SALINAN
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 43/PADK.03/2025
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH
BANK PEREKONOMIAN RAKYAT DAN
BANK PEREKONOMIAN RAKYAT SYARIAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

ANGGOTA DEWAN KOMISIONER OTORITAS JASA KEUANGAN,

Menimbang : bahwa untuk melaksanakan ketentuan sebagaimana dimaksud dalam Pasal 8, Pasal 12, Pasal 21, Pasal 25, Pasal 29, Pasal 33, Pasal 37, Pasal 41, dan Pasal 48 Peraturan Otoritas Jasa Keuangan Nomor 34 Tahun 2025 tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah, serta untuk mewujudkan peningkatan pemanfaatan teknologi informasi dan penguatan tata kelola, manajemen risiko, serta ketahanan dan keamanan siber dalam penyelenggaraan teknologi informasi bank perekonomian rakyat dan bank perekonomian rakyat syariah, perlu menetapkan Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah;

Mengingat : 1. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 5253) sebagaimana telah diubah 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. Peraturan Otoritas Jasa Keuangan Nomor 34 Tahun 2025 tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah (Lembaran Negara Republik Indonesia Tahun 2025 Nomor 46/OJK, Tambahan Lembaran Negara Republik Indonesia Nomor 175/OJK);

MEMUTUSKAN:

Menetapkan : PERATURAN ANGGOTA DEWAN KOMISIONER OTORITAS JASA KEUANGAN TENTANG PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH.

Pasal 1

Dalam Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini, yang dimaksud dengan:

1. Bank Perekonomian Rakyat yang selanjutnya disingkat BPR adalah jenis bank konvensional yang dalam kegiatannya tidak memberikan jasa dalam lalu lintas giral secara langsung.
2. Bank Perekonomian Rakyat Syariah yang selanjutnya disebut BPR Syariah adalah jenis bank syariah yang dalam kegiatannya tidak memberikan jasa dalam lalu lintas giral secara langsung.
3. Teknologi Informasi yang selanjutnya disingkat TI adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

Pasal 2

Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini mengatur pedoman penyelenggaraan TI oleh BPR dan BPR Syariah sebagai acuan standar minimum yang harus dipenuhi oleh BPR dan BPR Syariah dalam penyelenggaraan TI.

Pasal 3

Pedoman penyelenggaraan TI oleh BPR dan BPR Syariah sebagaimana dimaksud dalam Pasal 2 tercantum dalam:

a. Lampiran I yang memuat mengenai ketentuan mengenai penyelenggaraan TI oleh BPR dan BPR Syariah;
b. Lampiran II yang memuat mengenai penerapan tata kelola serta kebijakan dan prosedur penyelenggaraan TI oleh BPR dan BPR Syariah;
c. Lampiran III yang memuat mengenai manajemen risiko penyelenggaraan TI oleh BPR dan BPR Syariah;
d. Lampiran IV yang memuat mengenai pedoman ketahanan dan keamanan siber BPR dan BPR Syariah;
e. Lampiran V yang memuat mengenai pengelolaan data dan pelindungan data pribadi BPR dan BPR Syariah; dan
f. Lampiran VI yang memuat mengenai format laporan penyelenggaraan TI oleh BPR dan BPR Syariah,

yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

Pasal 4

BPR dan BPR Syariah menyesuaikan, menyempurnakan, dan menerapkan kebijakan, prosedur, dan pelaksanaan penyelenggaraan TI sesuai dengan Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

Pasal 5

BPR dan BPR Syariah menyusun dan mengembangkan pedoman penyelenggaraan TI sesuai dengan kebutuhan dan kompleksitas operasional usaha, strategi, serta visi dan misi masing masing BPR dan BPR Syariah dengan mengacu pada pedoman sebagaimana dimaksud dalam Pasal 2.

Pasal 6

Pada saat Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini mulai berlaku, Surat Edaran Otoritas Jasa Keuangan Nomor 15/SEOJK.03/2017 tentang Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah, dicabut dan dinyatakan tidak berlaku.

Pasal 7

Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini mulai berlaku setelah 1 (satu) tahun terhitung sejak tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 17 Desember 2025

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN I
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 43/PADK.03/2025
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH
BANK PEREKONOMIAN RAKYAT DAN
BANK PEREKONOMIAN RAKYAT SYARIAH

KETENTUAN MENGENAI PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH

DAFTAR ISI

I. TATA KELOLA TI BPR DAN BPR SYARIAH

1. Penerapan Tata Kelola TI yang Baik
   a. Sesuai dengan Pasal 2 POJK PTI BPR dan BPR Syariah, BPR dan BPR Syariah wajib menerapkan tata kelola TI yang baik.
   b. Dalam menerapkan tata kelola TI yang baik sebagaimana dimaksud dalam huruf a, BPR dan BPR Syariah mempertimbangkan faktor paling sedikit:
      1) strategi dan tujuan bisnis BPR dan BPR Syariah;
      2) skala usaha dan kompleksitas bisnis BPR dan BPR Syariah;
      3) peran TI bagi BPR dan BPR Syariah;
      4) metode pengadaan sumber daya TI;
      5) risiko dan permasalahan terkait TI;
      6) praktik atau standar yang berlaku secara nasional maupun internasional; dan
      7) ketentuan peraturan perundang-undangan.
2. Kebijakan dan Prosedur Penyelenggaraan TI
   a. Dalam menyusun kebijakan dan prosedur penyelenggaraan TI, BPR dan BPR Syariah mengacu pada strategi penyelenggaraan TI.
   b. Strategi penyelenggaraan TI memuat antara lain rencana pengembangan dan pengadaan TI serta pengembangan sumber daya manusia terkait penyelenggaraan TI sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai rencana bisnis bank perkreditan rakyat dan bank pembiayaan rakyat syariah.
   c. Penyusunan kebijakan dan prosedur penyelenggaraan TI dilakukan sesuai dengan kebutuhan dan kompleksitas usaha BPR dan BPR Syariah mencakup paling sedikit sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.
   d. Kebijakan dan prosedur penyelenggaraan TI meliputi paling sedikit:
      1) wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI;
      2) pengembangan dan pengadaan;
      3) operasional TI;
      4) jaringan komunikasi;
      5) pengamanan informasi;
      6) rencana pemulihan bencana;
      7) audit intern TI; dan
      8) penggunaan pihak penyedia jasa TI (PPJTI).
   e. BPR dan BPR Syariah melakukan kaji ulang dan menginikan kebijakan dan prosedur penyelenggaraan TI sebagaimana dimaksud pada huruf d secara berkala sesuai dengan kebutuhan, kondisi terkini, dan kepatuhan terhadap ketentuan peraturan perundang-undangan.
   f. Sesuai dengan Pasal 58 ayat (2) POJK Nomor 9 Tahun 2024 tentang Penerapan Tata Kelola bagi BPR dan BPR Syariah, Direksi dapat membentuk komite lain yang disesuaikan dengan permasalahan, skala usaha, dan/atau kompleksitas BPR dan BPR Syariah, misalnya BPR dan BPR Syariah memberikan layanan digital dan mempertimbangkan hasil penilaian tingkat maturitas keamanan siber. Komite lain dimaksud antara lain komite pengarah TI.

g. Komite pengarah TI beranggotakan:
   1) anggota Direksi yang membawahkan satuan kerja atau fungsi penyelenggaraan TI;
   2) anggota Direksi yang membawahkan fungsi manajemen risiko;
   3) pejabat tertinggi yang memimpin satuan kerja atau fungsi yang bertanggung jawab atas penyelenggaraan TI; dan
   4) pejabat tertinggi yang memimpin satuan kerja atau fungsi pengguna TI.

h. Komite pengarah TI diketuai oleh salah satu anggota Direksi yang merangkap sebagai anggota. Wewenang dan tanggung jawab komite pengarah TI tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

II. ARSITEKTUR TI BPR DAN BPR SYARIAH

1. BPR dan BPR Syariah yang menyediakan layanan digital menyusun arsitektur TI dalam dokumen tertulis disertai dengan penjelasan dari masing-masing domain.
2. Arsitektur TI merupakan dokumentasi BPR dan BPR Syariah yang menggambarkan topologi jaringan dan aplikasi yang dimiliki dan/atau dikelola oleh BPR dan BPR Syariah.
3. BPR dan BPR Syariah yang menyediakan layanan digital menyusun arsitektur TI secara komprehensif yang meliputi proses:
   a. Perencanaan
      BPR dan BPR Syariah menetapkan arah pengembangan penyelenggaraan TI, antara lain memuat visi, tujuan, dan ruang lingkup penyelenggaraan TI yang selaras dengan strategi bisnis.
   b. Desain
      BPR dan BPR Syariah menyusun desain arsitektur TI yang diharapkan termasuk rencana transisi dari arsitektur TI saat ini ke arsitektur TI yang diharapkan. Dalam menyusun desain arsitektur TI perlu mempertimbangkan, antara lain strategi dan kebutuhan bisnis, *gap analysis*, serta rencana tahapan implementasi.
   c. Implementasi
      BPR dan BPR Syariah menerapkan tahapan implementasi sesuai dengan desain arsitektur TI dan memastikan setiap tahapan selaras dengan arsitektur TI yang telah disusun.
   d. Kontrol
      BPR dan BPR Syariah memastikan kepatuhan terhadap visi, tujuan, dan ruang lingkup arsitektur TI serta mengevaluasi kendala selama tahapan implementasi termasuk melaporkan penyimpangan dan menyusun rekomendasi perbaikan.
4. Penyusunan arsitektur TI mempertimbangkan 3 (tiga) domain, yaitu:
   a. Arsitektur data
      Arsitektur data mendefinisikan jenis data, kebutuhan pengolahan data, serta alur data dan informasi yang diperlukan.
   b. Arsitektur aplikasi
      Arsitektur aplikasi mendefinisikan pengembangan setiap aplikasi, interaksi antar aplikasi, dan hubungan aplikasi dengan proses bisnis utama pada BPR dan BPR Syariah.

c. Arsitektur teknologi
Arsitektur teknologi mendefinisikan kapabilitas perangkat keras dan perangkat lunak untuk mendukung arsitektur data dan arsitektur aplikasi. Arsitektur teknologi mencakup, antara lain infrastruktur TI, *middleware*, jaringan, komunikasi, pengolahan, dan standar.

5. BPR dan BPR Syariah yang menyediakan layanan digital menginikan arsitektur TI secara berkala memperhatikan kebutuhan, kondisi terkini, dan kepatuhan terhadap ketentuan peraturan perundang-undangan, sesuai dengan prosedur dan kebijakan BPR dan BPR Syariah.

III. PENERAPAN MANAJEMEN RISIKO TI BPR DAN BPR SYARIAH

1. BPR dan BPR Syariah menerapkan manajemen risiko untuk seluruh penyelenggaraan TI, sesuai dengan kebijakan dan prosedur penyelenggaraan TI.
2. Kebijakan dan prosedur penyelenggaraan TI sebagaimana dimaksud dalam angka 1 diterapkan oleh BPR dan BPR Syariah untuk memitigasi risiko yang berhubungan dengan penyelenggaraan TI.
3. Penerapan manajemen risiko penyelenggaraan TI mengacu pada pedoman sebagaimana tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

IV. KETAHANAN DAN KEAMANAN SIBER BPR DAN BPR SYARIAH

1. BPR dan BPR Syariah menerapkan ketahanan dan keamanan siber untuk seluruh penyelenggaraan TI.
2. Ketahanan dan Keamanan Siber
   a. Ketahanan siber adalah kemampuan BPR dan BPR Syariah untuk tetap menjaga kelangsungan bisnisnya dengan melakukan tindakan antisipatif dan adaptif terhadap ancaman siber.
   b. Keamanan siber merupakan kondisi terjaganya kerahasiaan, keutuhan, serta ketersediaan informasi dan/atau sistem informasi yang saling terkoneksi satu sama lain melalui media siber dari serangan siber. Keamanan siber mencakup aspek, seperti keaslian, akuntabilitas, nirsangkal, dan keandalan.
   c. BPR dan BPR Syariah menjaga ketahanan dan keamanan siber dengan melakukan proses:
      1) Identifikasi aset, ancaman, dan kerentanan
         BPR dan BPR Syariah paling sedikit:
         a) menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta pencatatan konfigurasi secara efektif;
         b) melakukan identifikasi kerentanan dan pemantauan terhadap perkembangan siber terkini untuk mengidentifikasi ancaman siber; dan
         c) melakukan pengujian keamanan siber secara berkala.
      2) Pelindungan aset
         BPR dan BPR Syariah paling sedikit:
         a) menerapkan pengendalian keamanan (*security control*) yang komprehensif sesuai dengan hasil identifikasi aset, ancaman, dan kerentanan;

b) melakukan pemeliharaan dan perbaikan terhadap pengendalian keamanan atas aset TI;
c) menerapkan sistem pengamanan yang dikelola dengan baik;
d) melakukan penginian pengendalian keamanan secara berkala untuk memastikan kecukupan kontrol keamanan yang digunakan sesuai hasil terkini dari proses identifikasi;
e) menerapkan manajemen keamanan data dan informasi serta memastikan bahwa data dan/atau informasi dikelola sesuai strategi manajemen risiko organisasi untuk melindungi kerahasiaan, integritas, serta ketersediaan data dan informasi;
f) menerapkan manajemen pelindungan terhadap jaringan, perangkat keras, dan perangkat lunak;
g) menerapkan manajemen pelindungan terhadap akses dan pengguna untuk mencegah tindakan tidak terotorisasi pada perangkat, infrastruktur jaringan, dan komponen sistem yang dikelola BPR dan BPR Syariah;
h) menerapkan pelindungan yang memadai dalam kerja sama antara BPR dan BPR Syariah dengan PPJTI, termasuk dalam penggunaan *cloud*;
i) memastikan penerapan *secure coding* dalam pengembangan sistem dan aplikasi untuk meminimalisasi kerentanan sistem dan aplikasi; dan
j) memastikan pelaksanaan *patching* berjalan baik serta memastikan keandalan dan kemutakhiran komponen perangkat lunak, jaringan komunikasi, *database*, dan sistem operasi BPR dan BPR Syariah.

3) Deteksi insiden siber
BPR dan BPR Syariah paling sedikit:
a) memastikan ketersediaan dokumentasi kinerja dasar atas fungsi kritis BPR dan BPR Syariah dan sistem pendukung agar penyimpangan dideteksi tepat waktu serta aktivitas anomali dapat ditandai untuk ditindaklanjuti;
b) memantau aktivitas mencurigakan serta melakukan pengelolaan dan pengujian terhadap proses dan prosedur deteksi untuk memastikan aktivitas anomali dideteksi tepat waktu; dan
c) melakukan analisis ancaman dan kerentanan suatu insiden siber untuk memastikan penanganan insiden secara efektif sehingga dapat mencegah terjadinya gangguan pada layanan dan/atau operasional BPR dan BPR Syariah.

4) Penanggulangan dan pemulihan insiden siber
BPR dan BPR Syariah paling sedikit:
a) menetapkan rencana penanggulangan dan pemulihan insiden siber untuk memastikan penanggulangan dan pengembalian layanan tepat waktu sesuai risiko yang ditimbulkan, dengan dampak minimal;
b) menetapkan peran serta tugas dan tanggung jawab tim tanggap insiden siber untuk memastikan penanggulangan dan pemulihan insiden siber

dilaksanakan dengan dampak minimal terhadap layanan dan operasional BPR dan BPR Syariah;

c) menerapkan prosedur pemulihan dan upaya untuk mencegah penyebaran dampak dari insiden siber dengan memitigasi dampak dan menanggulangi insiden siber tersebut;

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

e) melakukan eskalasi dan pelaporan atas insiden siber sesuai dengan jalur komunikasi yang telah ditetapkan; dan

f) melakukan analisis pasca insiden sebagai bahan pelajaran terpetik (*lesson learned*) dalam penanggulangan dan pemulihan insiden siber untuk perbaikan berkelanjutan.

d. BPR dan BPR Syariah melakukan pengujian keamanan siber secara berkala atas keamanan jaringan, sistem, dan data sebagai langkah untuk memaksimalkan upaya menjaga keamanan siber BPR dan BPR Syariah. Pengujian keamanan siber terbagi menjadi 2 (dua), yaitu pengujian keamanan siber berdasarkan:
   1) analisis kerentanan; dan
   2) skenario.

e. Pengujian keamanan siber berdasarkan analisis kerentanan dilakukan dengan melihat titik lemah dari sistem BPR dan BPR Syariah.

f. Pengujian keamanan siber berdasarkan skenario dilakukan untuk memvalidasi proses penanggulangan dan pemulihan insiden siber pada BPR dan BPR Syariah termasuk rencana komunikasi BPR dan BPR Syariah dalam menghadapi ancaman siber.

g. Mekanisme pengujian keamanan siber mengacu pada pedoman sebagaimana tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

h. BPR dan BPR Syariah dapat melakukan pengujian keamanan siber secara mandiri atau menggunakan pihak ketiga. Dalam hal pengujian keamanan siber menggunakan pihak ketiga, BPR dan BPR Syariah harus:
   1) memastikan pihak ketiga memiliki kompetensi yang memadai sesuai dengan kebutuhan pengujian keamanan siber. Kompetensi dari pihak ketiga dibuktikan antara lain dengan adanya sertifikasi dan/atau pengakuan dari lembaga yang berwenang di Indonesia atau di luar negeri; dan
   2) tetap bertanggung jawab atas pelaksanaan pengujian keamanan siber.

i. BPR dan BPR Syariah melakukan dokumentasi dan pengamanan yang memadai atas hasil pengujian keamanan siber yang telah dilakukan untuk menjaga kerahasiaan hasil pengujian keamanan siber.

3. Fungsi yang Menangani Ketahanan dan Keamanan Siber
   a. BPR dan BPR Syariah membentuk fungsi yang bertugas menangani ketahanan dan keamanan siber BPR dan BPR Syariah.

b. Fungsi yang menangani ketahanan dan keamanan siber memiliki tugas untuk melaksanakan dan/atau mengoordinasikan:
   1) proses ketahanan siber;
   2) penilaian terhadap tingkat maturitas keamanan siber dan melaporkan secara berkala kepada Direksi;
   3) pengujian keamanan siber; dan
   4) tim tanggap siber termasuk inisiasi pembentukannya.

4. Penilaian Tingkat Maturitas Keamanan Siber
   a. BPR dan BPR Syariah melakukan penilaian tingkat maturitas keamanan siber. Penilaian tersebut dilakukan secara tahunan untuk posisi akhir bulan Desember. BPR dan BPR Syariah dapat melakukan penginian penilaian tersebut sewaktu-waktu apabila diperlukan.
   b. BPR dan BPR Syariah melakukan dokumentasi atas hasil penilaian maturitas keamanan siber.
   c. Otoritas Jasa Keuangan dapat sewaktu-waktu meminta hasil penilaian tingkat maturitas keamanan siber sebagaimana dimaksud pada huruf a.
   d. Hasil penilaian tingkat maturitas keamanan siber dapat menjadi pertimbangan dalam penilaian manajemen risiko operasional BPR dan BPR Syariah.
   e. Tata cara penilaian tingkat maturitas keamanan siber mengacu pada pedoman sebagaimana tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

V. PENGGUNAAN PPJTI DALAM PENYELENGGARAAN TI BPR DAN BPR SYARIAH
   1. BPR dan BPR Syariah dapat menggunakan PPJTI dalam penyelenggaraan TI.
   2. Mekanisme penggunaan PPJTI mengacu pada pedoman sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

VI. APLIKASI INTI PERBANKAN DAN PENEMPATAN SISTEM ELEKTRONIK
   1. Dalam pengembangan dan pemeliharaan Sistem Elektronik termasuk Aplikasi Inti Perbankan, BPR dan BPR Syariah melaksanakan tahapan sebagaimana dimaksud dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.
   2. BPR dan BPR Syariah menempatkan Sistem Elektronik berupa Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia.
   3. BPR dan BPR Syariah memastikan Pusat Data dan Pusat Pemulihan Bencana menjamin kelangsungan usaha BPR dan BPR Syariah.
      Yang dimaksud dengan “menjamin kelangsungan usaha” adalah memastikan bahwa kelangsungan usaha tetap dapat berjalan sebagaimana mestinya ketika terjadi bencana atau gangguan, termasuk menjamin kesiapan Sistem Elektronik yang terdapat pada Pusat Data dan Pusat Pemulihan Bencana.
      Contoh langkah yang dapat dilakukan untuk menjamin kelangsungan usaha BPR dan BPR Syariah, antara lain BPR dan BPR Syariah melakukan penilaian risiko atas Pusat Data dan Pusat Pemulihan Bencana, termasuk dengan mempertimbangkan

eksposur risiko yang berbeda dari masing-masing Pusat Data dan Pusat Pemulihan Bencana. Pusat Pemulihan Bencana termasuk Pusat Data yang beroperasi secara bersamaan dengan Pusat Data lainnya sehingga dapat saling menggantikan.

VII. PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI DALAM PENYELENGGARAAN TI BPR DAN BPR SYARIAH

1. Pengelolaan Data

   Pengelolaan data memperhatikan paling sedikit:
   a. kualitas data;
   b. sistem pengelolaan data; dan
   c. sumber daya pendukung pengelolaan data.

   Pelaksanaan pengelolaan data mengacu pada pedoman sebagaimana tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.
2. Pelindungan Data Pribadi

   BPR dan BPR Syariah melaksanakan prinsip pelindungan data pribadi dalam melakukan pemrosesan data pribadi yang mencakup aktivitas antara lain:
   a. pemerolehan dan pengumpulan;
   b. pengolahan;
   c. penyimpanan;
   d. transfer atau penyebarluasan; dan/atau
   e. penghapusan atau pemusnahan.

   Pelaksanaan pelindungan data pribadi mengacu pada pedoman sebagaimana tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

VIII. PENGENDALIAN DAN AUDIT INTERN BPR DAN BPR SYARIAH DALAM PENYELENGGARAAN TI BPR DAN BPR SYARIAH

1. BPR dan BPR Syariah melaksanakan sistem pengendalian intern secara efektif dalam penyelenggaraan TI.
2. Pengendalian intern dilakukan dalam rangka memastikan kepatuhan BPR dan BPR Syariah terhadap ketentuan intern dan peraturan perundang-undangan, efektivitas dan efisiensi kegiatan operasional, tersedianya informasi manajemen risiko yang lengkap, akurat, kini, dan utuh, serta efektivitas budaya manajemen risiko.
3. Pelaksanaan pengendalian intern terhadap penyelenggaraan TI dilakukan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank perkreditan rakyat dan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi bank pembiayaan rakyat syariah.
4. Dalam hal penyelenggaraan TI dilakukan oleh PPJTI, BPR dan BPR Syariah harus memiliki mekanisme pemantauan untuk memastikan PPJTI telah melaksanakan pekerjaan atau memberikan jasa sesuai dengan perjanjian.
5. BPR dan BPR Syariah memastikan pekerjaan PPJTI dilakukan sesuai dengan kebijakan dan prosedur.
6. BPR dan BPR Syariah melaksanakan audit intern terhadap penyelenggaraan TI, termasuk pengelolaan keamanan siber secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan pelaksanaan sebagai berikut:
   a. bagi BPR dan BPR Syariah, fungsi audit intern terhadap penyelenggaraan TI dilakukan sebagai bagian dari audit intern

BPR dan BPR Syariah sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan tata kelola bagi BPR dan BPR Syariah. Pelaksanaan fungsi audit intern terhadap penyelenggaraan TI tersebut dapat dilaksanakan sendiri oleh BPR dan BPR Syariah yang bersangkutan atau menggunakan jasa auditor ekstern.

b. bagi BPR Syariah, fungsi audit intern terhadap penyelenggaraan TI dilakukan dengan mengacu juga pada Peraturan Otoritas Jasa Keuangan mengenai penerapan tata kelola BPR Syariah dan ketentuan peraturan perundang-undangan terkait BPR Syariah lainnya.

7. Pelaksanaan audit intern penyelenggaraan TI mengacu pada pedoman sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

IX. PELAPORAN

1. Laporan Berkala
   a. BPR dan BPR Syariah menyampaikan laporan pelaksanaan dan pokok hasil audit intern kepada Otoritas Jasa Keuangan sebagai bagian dari laporan penilaian tingkat kesehatan BPR dan BPR Syariah.
   b. Laporan disampaikan secara daring melalui Aplikasi Pelaporan *Online* Otoritas Jasa Keuangan (APOLO) kanal laporan penilaian tingkat kesehatan BPR dan BPR Syariah.
   c. Tata cara penyampaian laporan sebagaimana dimaksud pada huruf a dilakukan sesuai dengan Surat Edaran Otoritas Jasa Keuangan mengenai pelaporan melalui sistem pelaporan Otoritas Jasa Keuangan dan transparansi kondisi keuangan bagi BPR dan BPR Syariah.
2. Laporan Insidental
   a. BPR dan BPR Syariah menyampaikan laporan:
      1) tindakan dalam hal terdapat kondisi tertentu, sebagaimana dimaksud dalam Pasal 28 ayat (1) huruf a POJK PTI BPR dan BPR Syariah;
      2) penghentian penggunaan PPJTI, sebagaimana dimaksud dalam Pasal 28 ayat (1) huruf c POJK PTI BPR dan BPR Syariah;
      3) rencana tindak untuk melakukan upaya perbaikan sebagaimana dimaksud dalam Pasal 28 ayat (4) POJK PTI BPR dan BPR Syariah;
      4) kondisi terkini penyelenggaraan TI dalam hal terjadi perubahan mendasar dalam penyelenggaraan TI sebagaimana dimaksud dalam Pasal 44 POJK PTI BPR dan BPR Syariah;
      5) realisasi penggunaan PPJTI sebagaimana dimaksud dalam Pasal 45 POJK PTI BPR dan BPR Syariah; dan/atau
      6) insiden TI yang berpotensi dan/atau telah mengakibatkan kerugian yang signifikan dan/atau mengganggu kelancaran operasional BPR dan BPR Syariah, berupa insiden siber dan insiden nonsiber, sebagaimana dimaksud dalam Pasal 46 ayat (1) huruf b POJK PTI BPR dan BPR Syariah,

      secara daring melalui APOLO kanal Laporan Insidental.
   b. BPR dan BPR Syariah menyampaikan laporan sebagaimana dimaksud dalam huruf a disertai dengan dokumen pendukung

sebagaimana tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

c. Tata cara penyampaian laporan sebagaimana dimaksud dalam huruf a dilakukan sesuai dengan Surat Edaran Otoritas Jasa Keuangan mengenai pelaporan melalui sistem pelaporan Otoritas Jasa Keuangan dan transparansi kondisi keuangan bagi BPR dan BPR Syariah.

d. BPR dan BPR Syariah menyampaikan notifikasi awal insiden TI yang berpotensi dan/atau telah mengakibatkan kerugian yang signifikan dan/atau mengganggu kelancaran operasional BPR dan BPR Syariah melalui sarana elektronik secara tertulis kepada Otoritas Jasa Keuangan berdasarkan informasi awal yang tersedia sesuai dengan format sebagaimana tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN II
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 43/PADK.03/2025
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH
BANK PEREKONOMIAN RAKYAT DAN
BANK PEREKONOMIAN RAKYAT SYARIAH

PENERAPAN TATA KELOLA SERTA KEBIJAKAN DAN PROSEDUR PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH

DAFTAR ISI

BAB I
PENERAPAN TATA KELOLA TI

Dalam penyelenggaraan TI, BPR dan BPR Syariah harus menerapkan tata kelola TI yang baik sebagai bagian dari penerapan tata kelola BPR dan BPR Syariah secara umum. Dalam rangka meminimalisasi terjadinya risiko yang terkait dengan penggunaan TI dan untuk melindungi kepentingan BPR dan BPR Syariah serta nasabah, BPR dan BPR Syariah perlu menerapkan tata kelola TI. Penerapan tata kelola TI bergantung pada pelaksanaan wewenang dan tanggung jawab Direksi, Dewan Komisaris, satuan kerja atau pegawai, baik penyelenggara maupun pengguna TI. Direksi dan Dewan Komisaris harus memastikan bahwa penyelenggaraan penerapan tata kelola TI dilakukan melalui penyelarasan Rencana Strategis TI dengan strategi bisnis BPR dan BPR Syariah, optimalisasi pengelolaan sumber daya, pemanfaatan TI, pengukuran kinerja, dan penerapan manajemen risiko yang efektif. Dalam rangka mewujudkan penyelenggaraan TI yang efektif dan efisien, Direksi dan Dewan Komisaris harus melibatkan seluruh jenjang organisasi BPR dan BPR Syariah.

Pengelolaan penyelenggaraan TI oleh BPR dan BPR Syariah secara efektif perlu dilakukan guna menghasilkan informasi yang diperlukan dalam pengambilan keputusan baik oleh BPR dan BPR Syariah maupun pemangku kepentingan BPR dan BPR Syariah. Sehubungan dengan hal tersebut, BPR dan BPR Syariah perlu memiliki dan menerapkan kebijakan dan prosedur penyelenggaraan TI, yang diantaranya meliputi wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI.

A. FAKTOR DALAM PENERAPAN TATA KELOLA TI YANG BAIK

Dalam menerapkan tata kelola TI yang baik, BPR dan BPR Syariah mempertimbangkan faktor paling sedikit:

a. strategi dan tujuan bisnis BPR dan BPR Syariah;
   Strategi dan tujuan bisnis BPR dan BPR Syariah yaitu strategi dan tujuan bisnis yang termuat dalam rencana bisnis BPR dan BPR Syariah.
b. skala usaha dan kompleksitas bisnis BPR dan BPR Syariah;
   Skala usaha dan kompleksitas bisnis BPR dan BPR Syariah yang tercermin dari antara lain modal inti dan kompleksitas kegiatan usaha yang dimiliki oleh BPR dan BPR Syariah.
c. peran TI bagi BPR dan BPR Syariah;
   Peran TI bagi BPR dan BPR Syariah dalam mendukung strategi dan mewujudkan tujuan bisnis BPR dan BPR Syariah, termasuk peningkatan peran TI terhadap produk dan layanan berbasis digital yang dimiliki oleh BPR dan BPR Syariah.
d. metode pengadaan sumber daya TI;
   Metode pengadaan sumber daya TI disesuaikan dengan kebutuhan dan kemampuan BPR dan BPR Syariah, antara lain pengadaan secara mandiri, pengadaan dengan menggunakan PPJTI, dan kombinasi antara keduanya.
e. risiko dan permasalahan terkait TI;
   Risiko dan permasalahan terkait TI mencerminkan antara lain risiko yang melekat maupun muncul terkait TI dan penerapan manajemen risiko dalam penyelenggaraan TI.
f. praktik atau standar yang berlaku secara nasional maupun internasional; dan
   Praktik atau standar yang berlaku secara nasional maupun internasional yang harus dipenuhi maupun digunakan sebagai

rujukan, seperti Standar Nasional Indonesia (SNI) dan standar internasional di bidang pengamanan informasi.

g. ketentuan peraturan perundang-undangan.
Ketentuan peraturan perundang-undangan yang perlu diperhatikan terkait dengan TI antara lain ketentuan peraturan perundang-undangan mengenai informasi dan transaksi elektronik, pelindungan data pribadi, kerahasiaan data nasabah, dan dokumen perusahaan.

B. TATANAN INSTITUSI TI

BPR dan BPR Syariah harus memperhatikan tatanan institusi TI yang baik dalam penerapan tata kelola TI. Tatanan institusi TI tersebut meliputi paling sedikit:

1. strategi dan perencanaan TI yang terintegrasi dengan strategi dan tujuan bisnis BPR dan BPR Syariah.
   Strategi dan perencanaan TI tersebut antara lain mempertimbangkan visi, misi, sasaran bisnis, analisis kondisi internal BPR dan BPR Syariah, dan lingkungan eksternal BPR dan BPR Syariah, dan memperhatikan faktor efisiensi, efektivitas, dan hal-hal lain, yaitu:
   a. peta jalan (*roadmap*) untuk mencapai kebutuhan TI yang mendukung strategi bisnis BPR dan BPR Syariah. Peta jalan (*roadmap*) terdiri dari kondisi saat ini (*current state*), kondisi yang ingin dicapai (*future state*), dan langkah-langkah yang akan dilakukan untuk mencapai kondisi yang ingin dicapai;
   b. sumber daya yang dibutuhkan. Dalam hal sumber daya yang dimiliki tidak memadai serta BPR dan BPR Syariah akan menggunakan jasa pihak lain dalam penyelenggaraan TI, BPR dan BPR Syariah memiliki kebijakan dan prosedur yang dibutuhkan;
   c. peran dan manfaat yang akan diperoleh saat rencana pengembangan dan pengadaan TI diterapkan;
   d. kendala yang mungkin timbul dalam penerapan rencana pengembangan dan pengadaan TI; dan
   e. strategi ketahanan dan keamanan siber selaras dengan visi dan misi BPR dan BPR Syariah, termasuk hasil kaji ulang strategi ketahanan dan keamanan siber secara berkala;
2. kebijakan, standar, dan prosedur TI yang utama, misalnya kebijakan TI yang utama yaitu kebijakan pengamanan TI dan manajemen risiko terkait penyelenggaraan TI;
3. wewenang dan tanggung jawab Direksi dan Dewan Komisaris dalam penerapan manajemen risiko;
4. kesesuaian antara proyek TI yang disetujui dengan Rencana Strategis TI;
5. kesesuaian antara pelaksanaan proyek TI dengan rencana proyek yang disepakati (*project charter*);
6. efektivitas langkah-langkah dalam meminimalisasi risiko atas investasi BPR dan BPR Syariah pada penyelenggaraan TI;
7. pemantauan atas kinerja TI dan upaya peningkatan kinerja TI; dan
8. upaya penyelesaian berbagai masalah terkait TI yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara TI secara efektif, efisien, dan tepat waktu.

C. WEWENANG DAN TANGGUNG JAWAB DIREKSI

Wewenang dan tanggung jawab Direksi dalam penyelenggaraan TI mencakup paling sedikit:

1. menetapkan rencana pengembangan dan pengadaan TI BPR dan BPR Syariah mencakup kegiatan:
   a. mengevaluasi, menyetujui, dan memantau proses pengembangan dan pengadaan TI BPR dan BPR Syariah; dan
   b. memastikan bahwa BPR dan BPR Syariah memiliki perjanjian kerjasama dengan pihak penyedia jasa TI (PPJTI) yang mengatur peran, hubungan, hak, kewajiban, tanggung jawab dari semua pihak yang terikat dengan perjanjian kerjasama tersebut, serta memastikan bahwa perjanjian kerjasama tersebut memenuhi syarat sahnya perjanjian dan dapat melindungi kepentingan BPR dan BPR Syariah apabila timbul permasalahan di kemudian hari dalam hal BPR dan BPR Syariah bekerjasama dengan PPJTI;
2. menetapkan kebijakan dan prosedur terkait penyelenggaraan TI, termasuk ketahanan dan keamanan siber (strategi, kebijakan, prosedur, dan limit) yang memadai dan mengomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna TI;
3. memantau kecukupan kinerja dan upaya peningkatan penyelenggaraan TI;
4. memastikan bahwa TI yang digunakan BPR dan BPR Syariah dapat mendukung perkembangan usaha, pencapaian tujuan bisnis, dan kelangsungan pelayanan terhadap nasabah BPR dan BPR Syariah mencakup kegiatan:
   a. penyediaan data dan informasi yang akurat untuk mendukung sistem informasi manajemen BPR dan BPR Syariah yang memadai;
   b. penyelenggaraan TI BPR dan BPR Syariah yang mampu mendukung perkembangan usaha BPR dan BPR Syariah yang berkelanjutan;
   c. penyelenggaraan TI BPR dan BPR Syariah yang mampu mendukung kelangsungan pelayanan kepada nasabah BPR dan BPR Syariah; dan
   d. memantau proses pengembangan dan pengadaan yang dilakukan oleh tim kerja sebagaimana dimaksud dalam Bab mengenai pengembangan dan pengadaan Sistem Elektronik.
5. Memastikan tersedianya sumber daya yang memadai dan terdapat peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan TI diantaranya melalui pendidikan, pelatihan, atau sertifikasi yang memadai, termasuk ketahanan dan keamanan siber, serta program edukasi untuk meningkatkan kesadaran atas pengamanan informasi.
6. memastikan tersedianya sistem pengelolaan pengamanan informasi (*information security management system*) yang efektif dan dikomunikasikan kepada satuan kerja penyelenggara dan pengguna TI;
7. memastikan tersedianya kebijakan dan prosedur penyelenggaraan TI yang memadai dan dikomunikasikan serta diterapkan secara efektif baik pada satuan kerja yang bertanggung jawab terhadap penyelenggaraan TI maupun satuan kerja pengguna TI paling sedikit meliputi kegiatan merumuskan kebijakan, rencana, dan anggaran penyelenggaraan TI;

Dalam pelaksanaan kewenangan dan tanggung jawab Direksi sebagaimana dimaksud dalam angka 1 sampai dengan angka 7, Direksi harus memperhatikan hal-hal sebagai berikut:

a. memastikan tersedianya kebijakan keamanan siber serta mengevaluasi kebijakan dimaksud secara berkala paling sedikit satu kali dalam satu tahun atau lebih dalam hal terdapat perubahan yang signifikan terhadap kegiatan usaha BPR dan BPR Syariah;
b. memastikan adanya dokumentasi terhadap setiap perubahan dan pengembangan yang dilakukan pada Sistem Elektronik termasuk perangkat lunak, baik yang dilakukan secara mandiri (*in-house*) maupun bekerjasama dengan PPJTI;
c. memastikan sumber daya manusia:
    1) tersedia dengan jumlah yang cukup dan kompeten sesuai dengan kebutuhan;
    2) memiliki peran dan tanggung jawab yang jelas termasuk terkait keamanan dan ketahanan siber; dan
    3) memahami risiko keamanan siber beserta strategi manajemen risikonya (*risk-appetite*, *zero risk-tolerance*, kerangka kerja) dan mampu mengomunikasikan serta menerapkannya secara konsisten.
d. Memastikan penerapan manajemen risiko dalam penyelenggaraan TI dilaksanakan secara memadai dan efektif;
e. mengembangkan budaya dan membangun serta memelihara kesadaran dan komitmen yang kuat mengenai tanggung jawab terkait keamanan siber bagi pegawai di semua level;
f. memastikan bahwa satuan kerja yang bertanggung jawab terhadap penyelenggaraan TI maupun satuan kerja pengguna TI memahami operasional TI yang digunakan;
g. memastikan kerja sama BPR dan BPR Syariah dengan pihak lain, misalnya kerja sama BPR dengan penyelenggara layanan pinjam meminjam uang berbasis TI telah memperhatikan prinsip manajemen risiko dan transparansi yang baik, termasuk memahami operasional TI yang digunakan oleh penyelenggara layanan pinjam meminjam uang berbasis TI; dan
h. memastikan tindak lanjut atas rekomendasi terkait dengan penyelenggaraan TI yang diberikan oleh audit intern, audit ekstern, dan otoritas.

D. WEWENANG DAN TANGGUNG JAWAB DEWAN KOMISARIS

Wewenang dan tanggung jawab Dewan Komisaris dalam penyelenggaraan TI mencakup paling sedikit:

1. mengarahkan dan memantau rencana pengembangan dan pengadaan TI BPR dan BPR Syariah yang bersifat mendasar antara lain:
    a. perubahan secara signifikan terhadap arsitektur TI atau Aplikasi Inti Perbankan;
    b. pengadaan Aplikasi Inti Perbankan baru;
    c. kerja sama dengan PPJTI; dan/atau
    d. pengembangan dan pengadaan TI mendasar lainnya yang dapat menambah dan/atau meningkatkan risiko BPR dan BPR Syariah;
2. mengevaluasi pertanggungjawaban Direksi terkait penyelenggaraan TI BPR dan BPR Syariah; dan
3. mengarahkan dan memantau penerapan tata kelola TI BPR dan BPR Syariah.

Dalam pelaksanaan kewenangan dan tanggung jawab Dewan Komisaris sebagaimana angka 1 sampai dengan angka 3, Dewan Komisaris harus memperhatikan hal-hal sebagai berikut:

a. mengevaluasi dan menyetujui kebijakan penyelenggaraan TI. Evaluasi kebijakan penyelenggaraan TI dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau sewaktu-waktu dalam hal terdapat perubahan yang memengaruhi kegiatan usaha BPR dan BPR Syariah secara signifikan;
   Contoh kebijakan penyelenggaraan TI, antara lain terkait manajemen risiko TI, keamanan informasi, dan pengelolaan SDM TI.
b. kebijakan manajemen risiko di bidang TI dan kesesuaian penerapannya dengan karakteristik, kompleksitas, dan profil risiko BPR dan BPR Syariah;
c. memberikan arahan perbaikan atas pelaksanaan kebijakan manajemen risiko di bidang TI;
d. mengevaluasi perencanaan dan pelaksanaan audit, memastikan audit dilaksanakan dengan frekuensi dan lingkup yang memadai, serta melakukan pemantauan atas tindak lanjut hasil audit yang terkait dengan sistem informasi; dan
e. mengevaluasi pengelolaan pengamanan yang andal dan efektif atas TI untuk menjamin ketersediaan, kerahasiaan, dan keakuratan informasi.

E. WEWENANG DAN TANGGUNG JAWAB KOMITE PENGARAH TI

Dalam hal BPR dan BPR Syariah memiliki Komite Pengarah TI sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan tata kelola bagi BPR dan BPR Syariah, wewenang dan tanggung jawab Komite Pengarah TI adalah memberikan rekomendasi kepada Direksi yang mencakup paling sedikit terkait dengan:

1. rencana pengembangan dan pengadaan TI BPR dan BPR Syariah yang sejalan dengan rencana bisnis BPR dan BPR Syariah. Dalam memberikan rekomendasi, komite pengarah TI harus memperhatikan faktor efisiensi, efektivitas, dan hal-hal lain, yaitu:
   a. peta jalan (*roadmap*) untuk mencapai kebutuhan TI yang mendukung strategi bisnis BPR dan BPR Syariah. Peta jalan (*roadmap*) terdiri dari kondisi saat ini (*current state*), kondisi yang ingin dicapai (*future state*), dan langkah-langkah yang akan dilakukan untuk mencapai kondisi yang ingin dicapai;
   b. manfaat yang akan diperoleh saat rencana pengembangan dan pengadaan TI BPR dan BPR Syariah diterapkan; dan
   c. kendala yang mungkin timbul dalam penerapan rencana pengembangan dan pengadaan TI BPR dan BPR Syariah.
2. perumusan kebijakan dan prosedur terkait penyelenggaraan TI, termasuk manajemen risiko penyelenggaraan TI;
3. kesesuaian antara pelaksanaan proyek TI dengan rencana pengembangan dan pengadaan TI BPR dan BPR Syariah;
4. kesesuaian antara TI dengan kebutuhan sistem informasi manajemen serta kebutuhan kegiatan usaha BPR dan BPR Syariah;
5. pemantauan atas kinerja TI dan upaya peningkatan kinerja TI, seperti pendeteksian keusangan infrastruktur TI dan pengukuran efektivitas dan efisiensi penerapan kebijakan pengamanan TI;
6. upaya penyelesaian masalah terkait TI yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara TI secara efektif, efisien, dan tepat waktu; dan
7. kecukupan dan alokasi sumber daya yang dimiliki BPR dan BPR Syariah. Dalam hal sumber daya yang dimiliki tidak memadai serta BPR dan BPR Syariah akan menggunakan jasa pihak lain dalam penyelenggaraan TI, komite pengarah TI harus memastikan BPR

dan BPR Syariah telah memiliki kebijakan dan prosedur yang dibutuhkan.

F. WEWENANG DAN TANGGUNG JAWAB SATUAN KERJA ATAU PEGAWAI YANG BERTANGGUNG JAWAB TERHADAP PENYELENGGARAAN TI

Wewenang dan tanggung jawab satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI paling sedikit:

1. membantu Direksi dan Dewan Komisaris dalam penyelenggaraan TI mencakup perencanaan, pelaksanaan dan pemantauan yang diwujudkan dalam kegiatan:
   a. memastikan kecukupan dan efektivitas kebijakan dan prosedur penyelenggaraan TI, serta penerapan manajemen risiko untuk mengidentifikasi, mengukur, menilai, dan mengawasi risiko TI;
   b. menerapkan seluruh kebijakan dan prosedur penyelenggaraan TI yang telah ditetapkan oleh Direksi;
   c. memastikan terdapatnya pengawasan yang memadai dalam setiap pengembangan dan pengadaan sistem TI;
   d. menyampaikan laporan penyelenggaraan TI secara periodik kepada Direksi dan mengusulkan tindakan untuk mengatasi kelemahan penyelenggaraan TI yang ditemukan; dan
   e. memastikan tindakan yang tepat telah dilakukan untuk memperbaiki temuan audit baik dari auditor intern maupun auditor ekstern atau berdasarkan laporan pemeriksaan Otoritas Jasa Keuangan.
2. mendukung pengembangan dan pengadaan TI paling sedikit:
   a. memastikan pengembangan dan pengadaan TI BPR dan BPR Syariah telah sesuai dengan kebijakan dan prosedur yang ditetapkan oleh Direksi;
   b. memastikan manajemen proyek terkait pengembangan dan pengadaan TI dilaksanakan secara konsisten dan memadai; dan
   c. memastikan bahwa perjanjian tertulis antara BPR dan BPR Syariah dengan PPJTI mencakup hal-hal yang telah diatur dalam POJK PTI BPR dan BPR Syariah dan Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini;
3. mendukung implementasi, operasional, dan pemeliharaan TI paling sedikit:
   a. memberikan dukungan dalam penyelesaian permasalahan terkait TI kepada satuan kerja pengguna secara responsif dan tepat waktu;
   b. memastikan setiap informasi yang dimiliki oleh satuan kerja pengguna TI mendapatkan perlindungan yang baik terhadap semua gangguan yang dapat menyebabkan kerugian akibat bocornya data atau informasi penting; dan
   c. memantau kinerja dari layanan TI di BPR dan BPR Syariah, antara lain persentase berapa lama sistem mati (*downtime error*), pelanggaran keamanan, penerapan perjanjian tingkat layanan (*Service Level Agreement*/SLA).
4. melakukan upaya penyelesaian permasalahan terkait TI yang tidak dapat diselesaikan oleh satuan kerja pengguna secara efektif, efisien, dan tepat waktu; dan
5. melakukan dokumentasi terhadap setiap perubahan dan pengembangan yang dilakukan pada Sistem Elektronik termasuk

perangkat lunak yang dilakukan secara mandiri (*in-house*) maupun bekerja sama dengan PPJTI.

BAB II
PENGEMBANGAN DAN PENGADAAN SISTEM ELEKTRONIK

Dalam rangka pengembangan dan pengadaan Sistem Elektronik yang dapat berupa pengembangan perangkat lunak secara intern, atau pembelian perangkat lunak, perangkat keras, dan/atau pengadaan jasa pengembangan Sistem Elektronik dari PPJTI, BPR dan BPR Syariah melakukan langkah-langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), serta mendukung pencapaian tujuan BPR dan BPR Syariah, paling sedikit:

a. menetapkan dan menerapkan prosedur pengembangan dan pengadaan Sistem Elektronik secara konsisten;
b. menerapkan manajemen proyek dalam pengembangan dan pengadaan Sistem Elektronik;
c. menetapkan pengaturan akses pengguna, termasuk akses pengguna berdasarkan peran (*role based access control*);
d. melakukan *testing* yang memadai pada saat pengembangan dan pengadaan Sistem Elektronik, termasuk uji coba dengan melibatkan satuan kerja pengguna, untuk memastikan keakuratan dan berfungsinya Sistem Elektronik sesuai dengan kebutuhan pengguna serta kesesuaian suatu sistem dengan sistem yang lain;
e. memiliki manajemen perubahan Sistem Elektronik;
f. memastikan dokumentasi terhadap pengadaan, pengembangan, manajemen perubahan, dan pemeliharaan Sistem Elektronik; dan
g. memastikan Sistem Elektronik BPR dan BPR Syariah mampu menampilkan kembali informasi secara utuh, baik dalam hal konversi, migrasi, dan kembali ke sistem awal (*roll back*).

Dalam rangka pengembangan dan pengadaan Sistem Elektronik, BPR dan BPR Syariah menerapkan manajemen proyek untuk memastikan Sistem Elektronik telah dikembangkan dengan struktur yang baik dan telah mengakomodasi kebutuhan pengguna serta sesuai dengan TI yang dimiliki BPR atau BPR Syariah. Penerapan manajemen proyek dilakukan oleh suatu tim kerja yang memiliki anggota paling sedikit berasal dari satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI dan satuan kerja pengguna TI. Tim kerja melaporkan setiap proses pengembangan dan pengadaan kepada Direksi. Sementara itu, satuan kerja audit intern atau pejabat eksekutif yang bertanggung jawab terhadap pelaksanaan fungsi audit intern merupakan pihak independen yang dapat memberikan masukan dan/atau pandangan sebagai pertimbangan bagi tim kerja dimaksud terkait kecukupan pengendalian dalam rangka pengembangan dan pengadaan Sistem Elektronik.

Dalam melaksanakan manajemen perubahan Sistem Elektronik selama dalam pengembangan aplikasi, seperti perubahan *user requirement*, perubahan teknologi pendukung yang digunakan, serta prosedur manajemen perubahan disusun, dilaksanakan, dan didokumentasikan dengan baik dan benar. Permintaan perubahan diteliti sebelum disetujui untuk menentukan metode lain dalam melakukan perubahan, biaya perubahan, serta waktu yang dibutuhkan untuk aktivitas pemrograman. Akar permasalahan (*root cause*) yang menyebabkan perubahan perlu diketahui dan didokumentasikan dengan baik dan benar. Jejak audit (*audit trail*) dari semua perubahan yang diminta wajib dipelihara.

A. KEBIJAKAN DAN PROSEDUR PENGEMBANGAN DAN PENGADAAN SISTEM ELEKTRONIK

Hal-hal yang harus diperhatikan dalam kebijakan dan prosedur pengembangan dan pengadaan Sistem Elektronik paling sedikit:

1. setiap pengembangan dan pengadaan Sistem Elektronik harus selalu melibatkan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI;
2. terhadap Sistem Elektronik yang dikembangkan dan diadakan oleh PPJTI, BPR dan BPR Syariah melakukan proses pemilihan PPJTI yang mengacu pada ketentuan mengenai pelaksanaan pekerjaan yang dialihdayakan. BPR dan BPR Syariah memastikan kecukupan pelatihan dan petunjuk pelaksanaan (*manual book*) yang disusun sebagai bagian dari perjanjian kerjasama antara BPR dan BPR Syariah dengan PPJTI;
3. kebijakan serta prosedur pengembangan dan pengadaan Sistem Elektronik mengacu pada tahapan pengembangan, kesesuaian spesifikasi dalam pengadaan, dan pelaksanaan aktivitas pemeliharaan;
4. kebijakan dan prosedur yang perlu dimiliki oleh BPR dan BPR Syariah dalam manajemen proyek antara lain:
   a. analisis atas biaya dan manfaat mencakup analisis terhadap manfaat yang akan diterima dari Sistem Elektronik yang akan dikembangkan dan diadakan berdasarkan pada permasalahan dan kendala penyelenggaraan Sistem Elektronik saat ini dibandingkan dengan biaya yang harus dikeluarkan, termasuk untuk menentukan apakah akan menggunakan sumber daya intern atau PPJTI;
   b. persyaratan pengamanan yang relevan sebelum Sistem Elektronik dikembangkan atau diadakan;
   c. pemisahan lingkungan (*environment*) untuk pengembangan, uji coba, dan operasional, termasuk pembatasan akses ke masing-masing lingkungan;
   d. analisis pemilihan perangkat lunak untuk memastikan terpenuhinya kebutuhan pengguna;
   e. perjanjian kerjasama antara BPR dan BPR Syariah dengan PPJTI yang memenuhi syarat sahnya perjanjian;
   f. penerapan manajemen pemeliharaan untuk semua proses pengembangan dan pengadaan Sistem Elektronik yang telah diimplementasikan;
   g. dokumentasi terhadap seluruh hasil pada setiap tahapan manajemen proyek; dan
   h. rencana proyek secara tertulis paling sedikit:
      1) identifikasi proyek dan manajer proyek;
      2) tujuan proyek, informasi latar belakang, dan strategi pengembangan dan pengadaan;
      3) deskripsi tanggung jawab utama dari tiap personel dalam manajemen proyek;
      4) prosedur untuk mengumpulkan dan menyebarkan informasi;
      5) kriteria hasil yang ditargetkan untuk masing-masing tahap pengembangan dan pengadaan (*acceptance criteria*);
      6) masalah keamanan dan pengendalian yang harus dipertimbangkan;
      7) *cut off date* untuk mengalihkan penggunaan sistem aplikasi dari versi lama ke versi terbaru;

8) standar pengembangan dan pengadaan yang akan digunakan untuk pengawasan proyek, pengendalian sistem, dan kendali mutu (*quality assurance*);
9) pendokumentasian yang dihasilkan di setiap tahap proyek;
10) jadwal tahapan proyek dan aktivitas yang akan diselesaikan dalam tiap tahap;
11) estimasi anggaran dari keseluruhan biaya proyek;
12) rencana uji coba (*testing plan*) yang mengidentifikasi kebutuhan uji coba (*testing requirement*) dan jadwal prosedur uji coba; dan
13) rencana pelatihan yang mengidentifikasikan kebutuhan pelatihan dan jadwal agar pengguna dapat menggunakan dan memelihara aplikasi pasca implementasi;

5. prosedur pengajuan pengubahan (*change request*) Sistem Elektronik yang harus dibuat BPR atau BPR Syariah paling sedikit:
   a. pertimbangan dan peninjauan ulang sebelum pengajuan pengubahan (*change request*) diotorisasi;
   b. pengujian hasil pengubahan (*change request*) dilakukan pada *testing environment* sebelum dilakukan *deployment*;
   c. prosedur rekam cadang (*back up*) data sebelum pengubahan (*change request*);
   d. dokumentasi yang terdiri atas:
      1) penjelasan pengubahan (*change request*);
      2) alasan penerapan atau penolakan pengubahan (*change request*) yang diusulkan;
      3) nama individu yang melakukan pengubahan (*change request*);
      4) tanggal dan waktu pengubahan (*change request*)dilakukan; dan
      5) salinan dari kode sumber (*source code*) yang diubah (jika ada).
   e. evaluasi setelah implementasi pengubahan (*change request*);
6. dokumentasi yang harus dibuat selama proses pengubahan (*change request*) berlangsung terdiri atas:
   a. informasi yang menjadi prioritas, antara lain pertimbangan dan hasil peninjauan ulang;
   b. identifikasi sistem, Pangkalan Data (*Database*) dan satuan kerja yang terpengaruh;
   c. nama dari individu yang bertanggung jawab dalam membuat pengubahan;
   d. kebutuhan sumber daya;
   e. prediksi biaya;
   f. prediksi tanggal penyelesaian;
   g. prediksi tanggal implementasi;
   h. pertimbangan potensi keamanan dan keandalan;
   i. kebutuhan uji coba;
   j. prosedur implementasi;
   k. perkiraan *downtime* pada saat implementasi;
   l. prosedur rekam cadang;

m. penginian dokumentasi, antara lain rancangan aplikasi dan *scripts*, topologi jaringan, petunjuk pelaksanaan bagi pengguna, dan rencana kontingensi;
n. dokumentasi persetujuan hasil pengubahan (*change request*) dari semua satuan kerja terkait (pengguna, teknologi, kendali mutu, keamanan, audit, dan lain-lain); dan
o. dokumentasi kaji ulang pasca implementasi (perbandingan antara rencana dan hasil).

B. TAHAPAN PENGEMBANGAN SISTEM ELEKTRONIK

Salah satu bentuk metodologi yang dapat digunakan oleh BPR dan BPR Syariah dalam melakukan pengembangan Sistem Elektronik adalah *System Development Life Cycle* (SDLC), yang terbagi menjadi tahapan inisiasi dan perencanaan, pendefinisian kebutuhan, desain, pemrograman, uji coba, implementasi, kaji ulang pasca implementasi, pemeliharaan, dan *disposal* dengan rincian sebagai berikut:

1. Tahap Inisiasi

   Inisiasi merupakan tahap perencanaan awal pengembangan Sistem Elektronik untuk mendefinisikan lingkup, tujuan, jadwal, dan anggaran awal yang diperlukan.

   Tahap inisiasi diawali dengan identifikasi kebutuhan untuk menambahkan, menyempurnakan, atau memperbaiki suatu sistem melalui usulan tertulis untuk mendapatkan persetujuan Direksi. Pengajuan dilakukan oleh satuan kerja pengguna bersama dengan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI.

   Tahap inisiasi terdiri atas langkah-langkah paling sedikit:

   a. Studi kelayakan proyek, antara lain pertimbangan bisnis BPR dan BPR Syariah, kebutuhan fungsional, rencana waktu pelaksanaan proyek, faktor-faktor yang mempengaruhi proyek serta analisis biaya dan manfaat.
   b. Pengajuan usulan tertulis yang berisi identifikasi kebutuhan pengguna untuk menambahkan, menyempurnakan, atau memperbaiki suatu sistem, tujuan, dan manfaat yang diharapkan, analisis biaya dan manfaat, serta manfaat dari Sistem Elektronik yang akan dikembangkan untuk mendukung strategi bisnis.

      Analisis atas biaya dan manfaat mencakup analisis terhadap manfaat yang akan diterima dari Sistem Elektronik yang akan dikembangkan dan diadakan berdasarkan pada kebutuhan penyelenggaraan Sistem Elektronik saat ini dibandingkan dengan biaya yang harus dikeluarkan, termasuk untuk menentukan apakah akan menggunakan sumber daya intern atau PPJTI.

      Dari analisis biaya dan manfaat tersebut BPR dan BPR Syariah dapat menentukan alternatif biaya dan sumber daya yang akan digunakan. Dalam hal digunakan Sistem Elektronik dari PPJTI, perlu pula diperhatikan kesesuaian spesifikasi dengan kebutuhan, pengaruh terhadap sistem yang telah ada, dukungan teknis purna jual, kondisi keuangan PPJTI, kelengkapan dokumentasi, dan pelatihan.
   c. Evaluasi dan persetujuan Direksi terhadap usulan tertulis mengenai pengembangan Sistem Elektronik baru atau perubahan Sistem Elektronik.

d. Penandatanganan dokumen pengembangan oleh semua pihak terkait, misalnya satuan kerja penyelenggara TI dan satuan kerja pengguna TI.

Setelah persetujuan pengembangan diperoleh pada tahap inisiasi, BPR dan BPR Syariah melakukan perencanaan untuk identifikasi lebih rinci atas aktivitas yang spesifik dan sumber daya yang dibutuhkan untuk menyelesaikan proyek. Tahap perencanaan ini menghasilkan suatu rencana proyek yang harus menjadi acuan dalam pelaksanaan proyek dan harus dilakukan penginian sesuai perkembangan proyek.

2. Tahap Pendefinisian Kebutuhan Pengguna (*User Requirement Definition*)

Pendefinisian Kebutuhan Pengguna (*User Requirement Definition*) adalah proses menganalisis kebutuhan pengguna terhadap Sistem Elektronik.

Berdasarkan usulan tertulis yang telah disetujui oleh Direksi, tim kerja dapat mulai menyusun *user requirement definition* secara detail sebagai dasar dimulainya pengembangan Sistem Elektronik. Pada tahap ini, seluruh kebutuhan pengguna Sistem Elektronik dikumpulkan berdasarkan contoh dokumen, spesifikasi proses dan sistem yang ada, wawancara dengan pengguna akhir serta analisis terhadap ketentuan yang berlaku.

Tahap pendefinisian kebutuhan pengguna ini terdiri atas:

a. Pengumpulan Kebutuhan (*Requirements Elicitation*) yang merupakan proses pengumpulan informasi mengenai tujuan pengembangan Sistem Elektronik, hasil yang diinginkan, kemampuan sistem dalam mengakomodasi kebutuhan bisnis proses dan cara penggunaan sistem.
b. Analisis Kebutuhan (*Requirements Analysis*) yang merupakan proses pemahaman permasalahan dan kebutuhan untuk menentukan solusi yang dapat dikembangkan. Pada tahap ini, ditentukan perkiraan umum dari waktu dan biaya pengembangan untuk tiap kebutuhan. Hasil analisis kebutuhan digunakan untuk menghasilkan alur bisnis proses yang dapat memperjelas pemahaman mengenai kebutuhan dan solusi, baik bagi satuan kerja pengguna maupun pengembang perangkat lunak (satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI dalam hal pengembangan dilakukan secara mandiri, atau PPJTI dalam hal pengembangan dilakukan melalui kerjasama).
c. Spesifikasi Kebutuhan (*Requirements Specification*) yang merupakan proses yang mendeskripsikan fungsional sistem yang akan dikembangkan, baik dari segi perangkat lunak maupun perangkat keras pendukung serta desain Pangkalan Data. Spesifikasi kebutuhan harus lengkap, komprehensif, dapat diuji, konsisten, jelas serta merinci kebutuhan input, proses, dan *output* yang dibutuhkan.
d. Pengelolaan Kebutuhan (*Requirements Management*) yang merupakan proses untuk mengidentifikasi, mengendalikan, dan menyimpan setiap perubahan terhadap kebutuhan pada saat proses pengembangan Sistem Elektronik.

3. Tahap Perancangan (Desain) Sistem Elektronik

Perancangan Sistem Elektronik merupakan proses konversi terhadap kebutuhan informasi, fungsi, dan jaringan teridentifikasi

selama tahap inisiasi menjadi spesifikasi rancangan/desain yang akan digunakan pengembang.
Salah satu teknik desain adalah dengan menggunakan purwarupa (*prototype*) yang mengembangkan desain maket dari bagian Sistem Elektronik seperti tampilan layar, struktur data, dan arsitektur sistem. Fungsi audit intern terhadap penyelenggaraan TI dan kendali mutu dapat dilibatkan sebagai narasumber terhadap desain yang akan digunakan.
Pada tahap desain diperlukan suatu standar pengendalian Sistem Elektronik yang mencakup kebijakan dan prosedur terkait dengan aktivitas pengguna dan pengendalian terintegrasi dalam Sistem Elektronik yang akan dikembangkan. Pada tahap ini, satuan kerja audit intern atau pejabat eksekutif yang bertanggungjawab terhadap pelaksanaan fungsi audit intern dapat memberikan masukan pengendalian yang dapat diterapkan dalam Sistem Elektronik. Tahap ini diperlukan untuk meningkatkan keamanan, integritas dan keandalan sistem dengan memastikan informasi input, proses, dan *output* yang terotorisasi, akurat, lengkap, dan aman.
Berdasarkan tujuannya, pengendalian terbagi atas pengendalian yang bersifat pencegahan, deteksi/temuan, atau koreksi. Pengendalian yang harus dilakukan paling sedikit:

a. Pengendalian Input
   Paling sedikit mencakup pemeriksaan terhadap validitas/kebenaran data, *range* data/parameter, dan duplikasi data yang diinput.
b. Pengendalian Proses
   Memastikan proses bekerja secara akurat dan dapat menyimpan atau menolak informasi. Pengendalian proses yang dapat dilakukan secara otomatis oleh Sistem Elektronik paling sedikit mencakup *Error Reporting*, *Transaction Log*, pemeriksaan urutan, dan rekam cadang *file*.
c. Pengendalian *Output*
   Memastikan sistem mengelola informasi dengan aman dan mendistribusikan informasi hasil proses dengan tepat serta menghapus informasi yang telah melewati masa retensi.

4. Tahap Pemrograman
   Pemrograman merupakan proses konversi dari desain yang telah disetujui ke dalam bahasa pemrograman.
   Dalam tahap ini tim kerja memperhatikan:
   a. Standar pemrograman, yang menjelaskan antara lain mengenai tanggung jawab *programmer*. Dalam rangka penerapan manajemen proyek, manajer proyek memahami secara keseluruhan mengenai proses pemrograman untuk memastikan tanggung jawab *programmer* telah sesuai, paling sedikit:
      1) Membatasi akses *programmer* terhadap data, aplikasi, utilitas, dan sistem di luar tanggung jawabnya. Pengendalian pengelolaan *library* dapat digunakan untuk mengelola akses tersebut; dan
      2) Pengendalian versi merupakan metode yang secara sistematis menyimpan kronologis dari salinan aplikasi yang disempurnakan serta menjadi salah satu dokumentasi aplikasi.

b. Dokumentasi
   1) Tim kerja mengelola dan memelihara dokumentasi yang detail untuk setiap aplikasi yang merupakan bagian dari Sistem Elektronik baik yang dikembangkan sendiri maupun yang dibeli atau dikembangkan oleh PPJTI yaitu mencakup:
      a) deskripsi detail aplikasi;
      b) dokumentasi pemrograman;
      c) format yang digunakan (basis data, tampilan, dan informasi);
      d) standar penamaan; dan
      e) petunjuk pelaksanaan bagi pengguna akhir.
   2) Dokumentasi harus dapat mengidentifikasi standardisasi pengembangan, seperti narasi sistem, alur sistem, pengkodean khusus sistem, dan pengendalian intern dalam dokumen aplikasi itu sendiri.
   3) Dalam hal aplikasi dibeli atau dikembangkan oleh PPJTI, tim kerja memastikan bahwa dokumentasi aplikasi dilakukan sesuai dengan standar minimum dokumentasi BPR atau BPR Syariah sebagaimana dimaksud pada angka 1).
c. Penginian rencana migrasi;
d. Implementasi dan pelatihan pengguna akhir;
e. Dokumentasi petunjuk pelaksanaan pemeliharaan; dan
f. Kebutuhan rencana uji coba yang harus dilakukan.

5. Tahap Uji Coba

Uji coba merupakan proses untuk menguji desain yang telah dikonversi menjadi bahasa pemrograman agar Sistem Elektronik berfungsi sesuai dengan kebutuhan pengguna serta hubungan dengan sistem aplikasi lain (*interoperability*) yang telah digunakan oleh BPR dan BPR Syariah.

Seluruh koreksi dan pengubahan (*change request*) yang dilakukan selama uji coba harus didokumentasikan untuk menjaga integritas keseluruhan dokumentasi Sistem Elektronik.

BPR dan BPR Syariah harus melengkapi petunjuk pelaksanaan bagi satuan kerja pengguna dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI, serta menyiapkan rencana implementasi dan pelatihan. Uji coba dilaksanakan dengan menggunakan skenario positif untuk memastikan sistem berfungsi sesuai dengan spesifikasi yang ditetapkan, serta skenario negatif untuk menilai respon sistem terhadap kesalahan input, kelemahan pengamanan, maupun potensi penyalahgunaan.

Uji coba yang dapat dilakukan oleh tim kerja atau PPJTI, yaitu:

a. *Unit Testing*

   Unit testing merupakan uji coba atas fungsional setiap unit atau sub modul dari Sistem Elektronik yang telah selesai dikembangkan. *Unit testing* dilakukan sebelum *system integration testing* sehingga apabila terjadi sesuatu, konfigurasi/kode pada unit perangkat lunak tersebut dapat diubah tanpa menimbulkan kekhawatiran berdampak pada sistem lainnya.

b. *System Integration Testing*

   System integration testing merupakan pengujian terhadap keseluruhan fungsional terhadap Sistem Elektronik setelah diintegrasikan menjadi satu kesatuan yang utuh. Pengujian ini

dilakukan untuk menghindari kesulitan penelusuran jika terjadi *error* atau *bug* pada integrasi tersebut.

c. *Stress Testing*

Stress testing merupakan uji ketahanan terhadap kemampuan Sistem Elektronik dalam menangani proses atau transaksi dalam skala/jumlah yang besar.

Stress Testing dilakukan setelah tim kerja atau PPJTI memberikan berita acara *system integration testing* kepada pengguna akhir.

d. *User Acceptance Test*

User Acceptance Test (UAT) merupakan proses uji coba akhir yang dilakukan oleh tim kerja atau PPJTI dengan pengguna akhir terhadap Sistem Elektronik yang telah selesai dikembangkan dalam rangka menguji fungsionalitas keseluruhan sistem telah sesuai dengan kebutuhan pengguna pada tahapan pendefinisian kebutuhan pengguna sebelum memutuskan implementasi dapat dilakukan. UAT hanya dapat dilakukan setelah tim kerja atau PPJTI memberikan berita acara atas hasil pengujian *system integration testing*. Pada tahap ini, satuan kerja audit intern atau pejabat eksekutif yang bertanggung jawab terhadap pelaksanaan fungsi audit intern dapat ikut melakukan pengujian dengan tetap menjaga independensi guna meyakini ketersediaan, kecukupan, dan efektivitas pengendalian yang ada di sistem.

Jika hasil UAT menunjukkan bahwa Sistem Elektronik telah sesuai dengan kebutuhan pengguna dan standar pengamanan BPR atau BPR Syariah, harus dibuat suatu berita acara UAT yang disetujui pengguna akhir.

6. Tahap Implementasi

Tim kerja perlu melakukan hal-hal utama yaitu pemberitahuan jadwal implementasi, pelatihan pada pengguna, dan instalasi Sistem Elektronik yang telah disetujui ke dalam lingkungan produksi. Hal-hal penting lainnya yang harus diperhatikan paling sedikit:

a. pemeriksaan integritas aplikasi berupa pengendalian yang memadai terhadap konversi dari kode sumber ke *object code* yang akan diimplementasikan;
b. migrasi data dari Sistem Elektronik lama ke Sistem Elektronik baru;
c. pemeriksaan akurasi dan keamanan data hasil migrasi pada sistem baru;
d. kemungkinan diberlakukannya *parallel run* antara sistem yang lama dengan yang baru, sampai dipastikan bahwa data pada sistem yang baru telah akurat dan andal;
e. integritas data, di mana BPR dan BPR Syariah harus memastikan keakuratan, dan keandalan dari Pangkalan Data dan integritas data;
f. pada saat implementasi, BPR dan BPR Syariah menghindari *patching data* karena dapat mempengaruhi integritas data pada Pangkalan Data di peladen (*server*) operasional;
g. pengaturan penyimpanan kode sumber dan Pangkalan Data dari sistem lama; dan
h. antisipasi adanya kelemahan sistem operasi, sistem yang dikembangkan, Pangkalan Data dan jaringan, termasuk ancaman dari *virus*, *trojan horse*, *worms*, *spyware*, *Denial-of-Service* (DoS), *wardriving*, *spoofing* dan *logic bomb*, dengan

menguji dan menerapkan pengendalian pengamanan atas sistem yang akan diimplementasikan.

7. Tahap Kaji Ulang Pasca Implementasi (*Post Implementation Review)*
   Satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI harus melakukan kaji ulang pasca implementasi Sistem Elektronik untuk mengetahui bahwa seluruh aktivitas dalam rencana proyek telah dilaksanakan dan tujuan proyek telah tercapai.
   Satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI harus menganalisis keefektifan aktivitas manajemen proyek dengan membandingkan antara lain rencana dan realisasi biaya, manfaat yang diperoleh, dan ketepatan jadwal proyek. Hasil analisis harus didokumentasikan dan dilaporkan kepada Direksi.
8. Tahap Pengoperasian
   Dalam pengoperasian Sistem Elektronik terdapat prosedur untuk pengawasan pelaksanaan pengoperasian, keamanan data, orisinalitas data, *inputing data*, dan pengaturan Pangkalan Data.
9. Tahap Pemeliharaan
   Pemeliharaan harus dilakukan terhadap perangkat keras, perangkat lunak, dan dokumentasi dalam rangka memastikan efektivitas operasional Sistem Elektronik. BPR dan BPR Syariah harus menetapkan prosedur pemeliharaan yang sesuai dengan karakteristik dan risiko tiap proyek dari Sistem Elektronik yang ada.
   Tahap pemeliharaan memperhatikan aspek antara lain:
   a. *Library*
      BPR dan BPR Syariah harus memiliki *library* untuk menyimpan program, menyimpan informasi dan/atau dokumen berupa data dan program yang berhubungan dengan peladen atau mesin produksi yang berasal dari pengembangan dan/atau pengujian dalam rangka menjamin ketersediaan program yang digunakan.
   b. Konversi
      Dalam hal terjadi penggabungan, peleburan, atau pengambilalihan BPR dan BPR Syariah yang memerlukan pengintegrasian sistem yang digunakan maka perlu dilakukan proses konversi. Dalam proses ini dilakukan modifikasi atau perubahan besar pada sistem yang ada dan pengembangan sistem baru apabila diperlukan. Dalam proses konversi ini, proses yang terstruktur seperti manajemen proyek dan siklus pengembangan sistem tetap harus diterapkan. Mengingat kompleksitas sistem di masing-masing BPR dan BPR Syariah yang terlibat penggabungan, peleburan, atau pengambilalihan, diperlukan analisis secara komprehensif terhadap dampak konversi pada kegiatan operasional BPR dan BPR Syariah khususnya pemrosesan transaksi. Agar proses konversi berlangsung secara efektif, BPR dan BPR Syariah perlu mengantisipasi peningkatan permintaan untuk *balancing*, *reconcilement*, *exception handling*, dukungan pengguna dan nasabah, penyelesaian masalah, keterhubungan jaringan, dan sistem administrasi.
   c. Pemeliharaan Dokumentasi
      Standar dokumentasi harus mengidentifikasikan dokumen utama dan dokumen detail yang telah disetujui dan sesuai format yang dibutuhkan. Dokumentasi tersebut berisi semua perubahan yang terjadi pada sistem baik dari perangkat lunak,

perangkat keras, dan jaringan, serta konfigurasi sesuai dengan standar yang ditentukan. Dokumentasi terkait sistem hanya dapat diakses oleh personel BPR dan BPR Syariah yang berhak dan/atau memiliki kewenangan untuk mengadministrasikan dokumentasi tersebut. BPR dan BPR Syariah harus memiliki lokasi penyimpanan khusus dokumentasi baik yang berupa *hardcopy* maupun *softcopy*, termasuk lokasi yang akan digunakan untuk kondisi darurat.

10. Tahap Pemusnahan (*Disposal*)

    Disposal merupakan proses terakhir dari pengembangan Sistem Elektronik termasuk data dengan cara menghapus atau menghancurkan sistem termasuk data. Setiap Sistem Elektronik hasil pengembangan dan pengadaan yang tidak digunakan dalam kegiatan operasional dan berdasarkan pertimbangan BPR atau BPR Syariah diyakini tidak diperlukan dan tidak akan dipelihara lagi, akan memasuki tahap terakhir dalam SDLC yaitu tahap *disposal*. Hal ini dilakukan untuk memastikan Sistem Elektronik yang digunakan dalam kegiatan operasional merupakan Sistem Elektronik yang paling akurat dan terkini, serta untuk menghindari penyalahgunaan oleh pihak yang tidak berwenang. Dalam melakukan *disposal*, BPR dan BPR Syariah memperhatikan paling sedikit:

    a. perencanaan untuk menghancurkan Sistem Elektronik;
    b. pemindahan data dari sistem lama ke sistem baru;
    c. memindahkan aplikasi Sistem Elektronik dari produksi dan memusnahkan seluruh infrastruktur sesuai dengan masa retensi aplikasi Sistem Elektronik;
    d. dokumentasi seluruh proses *disposal* agar dapat dipergunakan di kemudian hari; dan
    e. keberhasilan menampilkan kembali informasi secara utuh selama masa retensi.

C. PENGADAAN SISTEM ELEKTRONIK

Dalam proses pengadaan Sistem Elektronik, untuk memastikan bahwa Sistem Elektronik yang diadakan telah memenuhi kebutuhan fungsional, kriteria keamanan, dan keandalan, BPR dan BPR Syariah perlu memperhatikan hal-hal sebagai berikut:

1. Prosedur Pengadaan

   Prosedur pengadaan harus diterapkan untuk memastikan bahwa Sistem Elektronik yang diadakan memenuhi kebutuhan fungsional, kriteria keamanan, dan keandalan. Dalam pengadaan Sistem Elektronik, BPR dan BPR Syariah harus memperhatikan paling sedikit:

   a. pengadaan dimulai dengan pengajuan rencana kepada Direksi;
   b. evaluasi Direksi terhadap seluruh pengajuan rencana;
   c. pengajuan rencana harus didasarkan pada kebutuhan bisnis BPR dan BPR Syariah untuk:
      1) mendapatkan suatu produk, baik berupa perangkat lunak maupun perangkat keras;
      2) mengidentifikasi fitur sistem yang diinginkan; dan
      3) menggambarkan kebutuhan informasi, antarmuka jaringan (*network interface)*, serta komponen perangkat keras dan perangkat lunak;
   d. BPR dan BPR Syariah harus menyusun analisis kelayakan untuk menentukan kebutuhan pengadaan perangkat lunak

BPR dan BPR Syariah, baik yang dapat dimodifikasi sesuai kebutuhan maupun yang siap pakai (*off-the shelf*);

e. persetujuan dari seluruh pihak terkait atas analisis kelayakan tersebut harus didokumentasikan sebagai dasar pembuatan definisi kebutuhan;
f. BPR dan BPR Syariah menetapkan perencanaan pengadaan dan pemilihan metode pengadaan, yang meliputi penentuan anggaran, kriteria evaluasi, dan mekanisme pengadaan (tender terbuka, tender terbatas, atau penunjukan langsung);
g. setelah BPR dan BPR Syariah menerima penawaran, BPR dan BPR Syariah harus menganalisis dan membandingkan penawaran antar PPJTI terhadap kebutuhan yang ditetapkan BPR dan BPR Syariah. Proposal PPJTI harus membahas dengan jelas semua kebutuhan BPR dan BPR Syariah dan mengidentifikasi isu-isu lain yang dapat diterapkan;
h. BPR dan BPR Syariah harus memiliki prosedur untuk memastikan bahwa proses evaluasi penawaran telah dilaksanakan dengan benar. BPR dan BPR Syariah kemudian melakukan proses seleksi yang menghasilkan daftar PPJTI potensial;
i. Direksi harus mengkaji kembali kredibilitas, kestabilan kondisi keuangan, dan komitmen pelayanan dari PPJTI yang terpilih; dan
j. BPR dan BPR Syariah menentukan produk dan PPJTI serta menegosiasikan kontrak.

2. Analisis Kebutuhan Pengguna

   Analisis tentang kebutuhan pengguna merupakan hal yang perlu dilakukan sebelum dilaksanakannya evaluasi terhadap Sistem Elektronik yang akan diadakan. Dalam analisis ini perlu ditetapkan alasan untuk mengadakan Sistem Elektronik, kekurangan dari sistem yang digunakan saat ini, kebutuhan pengguna dan pemrosesan data, laporan yang dibutuhkan pengguna, keterkaitan Sistem Elektronik yang akan diadakan dengan sistem lainnya, serta sumber daya yang dibutuhkan untuk melakukan instalasi dan pemeliharaan Sistem Elektronik.

   Sistem Elektronik perlu ditelaah untuk memastikan tersedianya pengendalian pengamanan dan jejak audit, misalnya akses terhadap *file* data, proses otorisasi, pengendalian melalui *password*, catatan akses terhadap data, laporan tentang usaha menembus pengamanan, dan kemampuan *program utilities* untuk mengubah data.

3. Analisis Biaya dan Manfaat

   Dalam melakukan analisis biaya dan manfaat, tim kerja perlu melakukan perbandingan antara biaya yang dikeluarkan dengan manfaat yang diperoleh BPR dan BPR Syariah. Dalam pembuatan analisis biaya dan manfaat, BPR dan BPR Syariah perlu mempertimbangkan, antara lain perkembangan TI dan *cost efficiency* untuk melihat kelayakan secara ekonomis.

D. PEMELIHARAAN SISTEM ELEKTRONIK

Aktivitas pemeliharaan harus dilakukan oleh BPR dan BPR Syariah mencakup layanan rutin dan modifikasi terhadap perangkat keras, perangkat lunak dan informasi yang terkait untuk memastikan efektivitas penyelenggaraan TI bagi BPR atau BPR Syariah. Untuk itu diperlukan prosedur tentang Manajemen Perubahan (*change management*) guna memastikan perubahan yang terjadi selama tahap

pemeliharaan tidak mengganggu kegiatan operasional TI BPR dan BPR Syariah atau menurunkan kinerja/keamanan sistem. Manajemen perubahan mencakup modifikasi mayor (besar), minor (kecil), dan mendesak (darurat).

1. Manajemen Perubahan

   Direksi menetapkan prosedur pengendalian perubahan secara detail yang memuat prosedur otorisasi, uji coba, dokumentasi, implementasi, dan sosialisasi atas modifikasi teknologi tersebut.

   Modifikasi mencakup perangkat keras dan perangkat lunak. Modifikasi perangkat keras diperlukan untuk menggantikan peralatan yang lama, tidak berfungsi, atau untuk meningkatkan kinerja atau kapasitas penyimpanan. Modifikasi perangkat lunak dibutuhkan untuk memenuhi kebutuhan pengguna, memperbaiki permasalahan perangkat lunak, dan kelemahan pengamanan dalam penyelenggaraan TI, atau mengimplementasikan teknologi baru. BPR dan BPR Syariah harus mengoordinasikan modifikasi Sistem Elektronik melalui proses manajemen perubahan yang terpusat karena adanya keterkaitan antar Sistem Elektronik dan sistem operasional.

   Berdasarkan tingkat kepentingannya, modifikasi digolongkan menjadi:

   a. modifikasi besar (*major modification*), merupakan perubahan fungsional secara signifikan pada Sistem Elektronik yang antara lain disebabkan karena adanya konversi atau pengembangan sistem baru akibat adanya penggabungan, peleburan, atau perubahan kepemilikan BPR atau BPR Syariah. Modifikasi besar harus diterapkan mengikuti proses yang terstruktur seperti yang dilakukan dalam tahapan pengembangan Sistem Elektronik;
   b. modifikasi minor (*minor modification*), merupakan pelaksanaan perubahan pada Sistem Elektronik untuk meningkatkan kinerja, memperbaiki permasalahan, atau meningkatkan keamanan. Standar modifikasi minor harus mencakup permintaan perubahan, peninjauan kembali, dan prosedur persetujuan serta mensyaratkan BPR atau BPR Syariah untuk merencanakan, menguji coba, dan mendokumentasikan semua perubahan sebelum dilakukan implementasi. BPR dan BPR Syariah harus melakukan kaji ulang semua modifikasi yang diusulkan untuk memastikan kesesuaian modifikasi dengan sistem yang ada dan memastikan bahwa hanya modifikasi yang disetujui yang diimplementasikan. BPR dan BPR Syariah harus menetapkan standar persetujuan Sistem Elektronik yang mencakup prosedur untuk memverifikasi hasil uji coba, memeriksa kode yang diubah, dan memastikan kesesuaian kode sumber. Setelah modifikasi Sistem Elektronik selesai, semua kode sumber harus diamankan dalam *library* baik versi terkini maupun versi sebelum diubah;
   c. modifikasi darurat (*incidental modification*), dibutuhkan untuk memperbaiki permasalahan pada Sistem Elektronik atau mengembalikan proses operasional dengan cepat. Meskipun modifikasi tersebut harus diselesaikan dengan cepat, namun tetap harus diimplementasikan dan dikendalikan dengan baik. Modifikasi darurat juga harus diuji sebelum implementasi. Namun jika uji coba tidak dapat dilakukan secara menyeluruh pada modifikasi darurat sebelum implementasi, harus ada prosedur *roll back*. Hal ini penting agar BPR dan BPR Syariah

dapat membatalkan modifikasi jika modifikasi tersebut menyebabkan gangguan pada Sistem Elektronik.

2. *Patch Management*

   PPJTI mengembangkan dan mengeluarkan *patch* untuk memperbaiki permasalahan pada perangkat lunak, memperbaiki kinerja, dan meningkatkan keamanan. Jika terdapat *patch* baru, BPR dan BPR Syariah harus mengevaluasi dampak secara teknis dari instalasi *patch* tersebut terhadap bisnis dan keamanan. BPR dan BPR Syariah harus memiliki prosedur untuk mengidentifikasi ketersediaan *patch* dari sumber yang terpercaya. Pengaturan *patch* harus mencakup prosedur identifikasi, evaluasi, persetujuan, pengujian, instalasi, dan dokumentasi dari *patch*. BPR dan BPR Syariah harus meninjau ulang semua *security setting* dan *configuration parameter* setelah penggunaan *patch* baru untuk memastikan bahwa *setting* telah memenuhi kebijakan dan prosedur yang disetujui.

3. *Library*

   Untuk memastikan ketersediaan aplikasi yang digunakan, BPR dan BPR Syariah harus memiliki *Library* untuk menyimpan program. Selain itu perlu dilakukan penyimpanan atas informasi dan/atau dokumen berupa data dan aplikasi yang berhubungan dengan peladen yang berasal dari pengembangan dan/atau pengujian. Penjelasan lebih lanjut mengenai *library* dimuat pada bab yang mengatur mengenai operasional TI.

4. Konversi

   Dalam hal terjadi penggabungan, peleburan, atau perubahan kepemilikan BPR atau BPR Syariah yang memerlukan konversi Sistem Elektronik, perlu dilakukan modifikasi besar pada Sistem Elektronik yang ada dan pengembangan Sistem Elektronik baru apabila diperlukan. Dalam proses konversi ini, proses yang terstruktur seperti tahapan pengembangan Sistem Elektronik tetap harus diterapkan.

   Mengingat keragaman Sistem Elektronik di masing-masing BPR dan BPR Syariah yang terlibat penggabungan, peleburan, atau perubahan kepemilikan, diperlukan analisis secara komprehensif terhadap dampak konversi pada kegiatan operasional BPR atau BPR Syariah khususnya pemrosesan transaksi. Agar proses konversi berlangsung secara efektif, BPR dan BPR Syariah perlu mengantisipasi peningkatan permintaan untuk *balancing*, *reconcilement*, *exception handling*, dukungan pengguna dan nasabah (*help desk*), penyelesaian masalah (*troubleshooting*), keterhubungan jaringan dan sistem administrasi.

5. Pemeliharaan Dokumentasi

   BPR dan BPR Syariah harus mendokumentasikan semua perubahan yang terjadi pada sistem, aplikasi, dan konfigurasi sesuai dengan standar yang ditentukan.

BAB III
OPERASIONAL TI

Bab ini membahas aktivitas dan pengendalian dari operasional TI sebagai pedoman bagi BPR dan BPR Syariah dalam rangka menerapkan standar penyelenggaraan TI. Pengaturan atas operasional TI yang memadai sangat penting untuk memastikan informasi pada sistem komputer adalah lengkap, akurat, kini, terjaga integritasnya, dan andal, serta terhindar dari kesalahan, kecurangan, manipulasi, penyalahgunaan dan perusakan data.

Dalam penyelenggaraan TI, BPR dan BPR Syariah harus memastikan bahwa operasional TI stabil, aman, dan efisien secara keseluruhan, baik yang diselenggarakan sendiri maupun bekerjasama dengan PPJTI. BPR dan BPR Syariah harus menetapkan kebijakan dan prosedur operasional TI yang menjamin kesinambungan operasional TI dan memastikan penerapannya baik pada satuan kerja penyelenggara atau PPJTI. Operasional TI tidak hanya terkonsentrasi di Pusat Data (*Data Center*) tetapi juga pada aktivitas lainnya yang terkait dengan aplikasi yang terintegrasi, beragam media komunikasi, koneksi internet, dan berbagai *platform* komputer. Demikian juga dengan pemrosesan, dapat dilakukan di berbagai lokasi yang berjauhan namun saling terkait, baik secara *online*, *realtime*, maupun *offline*.

A. KEBIJAKAN DAN PROSEDUR OPERASIONAL TI

BPR dan BPR Syariah diwajibkan memiliki kebijakan dan prosedur yang mencakup setiap aspek operasional TI sesuai dengan POJK PTI BPR dan BPR Syariah. Kedalaman dan cakupan kebijakan dan prosedur tersebut disesuaikan dengan kompleksitas operasional BPR dan BPR Syariah. Kebijakan dan prosedur harus dijabarkan secara tertulis yang digunakan dalam pelaksanaan operasional TI. Kebijakan dan prosedur antara lain memuat rincian tugas, tanggung jawab, pemberian wewenang, dan pedoman pelaksanaan bagi satuan kerja penyelenggara TI, serta pengamanan dan dokumentasi akses ke sistem kritikal. Selain itu, BPR dan BPR Syariah harus menetapkan persyaratan yang harus dipenuhi terkait perangkat keras dan perangkat lunak yang digunakan di lingkungan produksi, pengujian, dan pengembangan dalam penyelenggaraan TI BPR dan BPR Syariah.

1. Kebijakan dan Prosedur Pengelolaan Data

   BPR dan BPR Syariah harus menjalankan kebijakan dan prosedur pengelolaan data atas penyelenggaraan TI yang mencakup:

   a. Kebijakan dan Prosedur Operasional Pusat Data

      Kebijakan dan prosedur yang diterapkan dalam aktivitas operasional Pusat Data mencakup aktivitas menjalankan tugas rutin maupun tidak rutin. Aktivitas yang terkait dengan operasional Pusat Data paling sedikit:

      1) penjadwalan tugas

         BPR dan BPR Syariah harus memiliki dan melaksanakan jadwal semua tugas yang harus dijalankan di Pusat Data operasional TI secara efektif dan aman;

      2) pengoperasian tugas

         Pemberian akses terbatas kepada operator TI sesuai kewenangan pada fungsi pengoperasian tugas yang telah ditentukan;

      3) pendistribusian laporan/*output*

         Hasil informasi yang diproduksi oleh sistem (*output*), dalam bentuk *softcopy* atau *hardcopy*, dapat merupakan informasi yang sensitif atau rahasia. BPR dan BPR Syariah harus memiliki prosedur pendistribusian

laporan/*output* yang meliputi penentuan informasi yang akan dihasilkan baik informasi umum atau rahasia, pendistribusian *output* baik secara *hardcopy* maupun *softcopy*, dan pemusnahan *output* yang sudah tidak diperlukan lagi. Prosedur tersebut diperlukan untuk menghindari terbukanya informasi yang bersifat rahasia, meningkatnya biaya akibat adanya *output* yang tidak diperlukan, dan memastikan keamanan *output*;

4) proses rekam cadang baik *on-site* maupun *off-site, restore,* unduh (*download*), dan unggah(*upload*) untuk data/Pangkalan Data;
5) pemantauan perangkat keras dan perangkat lunak serta lingkungan pusat data; dan
6) pengaktifan jejak audit (*audit trail*).

b. Kebijakan dan Prosedur Pengelolaan Pangkalan Data (*Database*)

Kegagalan dalam mengelola dan mengamankan Pangkalan Data dapat mengakibatkan perubahan, pemusnahan, atau pengungkapan informasi yang bersifat rahasia baik oleh pengguna secara sengaja maupun tidak sengaja ataupun oleh pihak lain yang tidak berhak. Pengungkapan informasi rahasia oleh pihak yang tidak berwenang dapat mengakibatkan risiko yang dapat menyebabkan kerugian finansial. BPR dan BPR Syariah harus membuat kategori jenis data pada Pangkalan Data yang termasuk dalam kategori informasi umum atau informasi rahasia. Pangkalan Data yang menyimpan informasi rahasia membutuhkan pengendalian yang lebih ketat dibandingkan Pangkalan Data yang menyimpan informasi yang bersifat umum. Untuk itu, BPR dan BPR Syariah harus memiliki fungsi *Database Administrator* (DBA) yang bertanggung jawab terhadap pengelolaan Pangkalan Data BPR atau BPR Syariah.

Kebijakan dan prosedur yang harus dimiliki BPR dan BPR Syariah terkait Pangkalan Data adalah pengaksesan, pemeliharaan, penanganan permasalahan, dan administrasi Pangkalan Data. Bagi BPR dan BPR Syariah yang memiliki *Data Warehouse* (DWH), BPR dan BPR Syariah harus menerapkan prosedur yang sama dengan kebijakan dan prosedur pengelolaan Pangkalan Data.

c. Kebijakan dan Prosedur Pengelolaan *Library*

Library merupakan kumpulan perangkat lunak atau data yang memiliki fungsi tertentu yang disimpan dan siap untuk digunakan. Dalam rangka pengelolaan *library*, BPR dan BPR Syariah harus melakukan inventarisasi dan menyimpan seluruh perangkat lunak dan data yang tersimpan dalam berbagai media, antara lain *tape* dan *disc*, termasuk salinan dari seluruh kebijakan dan prosedur seperti petunjuk instalasi dan penggunaan aplikasi.

BPR dan BPR Syariah harus memiliki kebijakan dan prosedur terkait pengelolaan *library* yang antara lain:

1) prosedur pengamanan akses data di *library*;
2) penanganan media penyimpan data (untuk data/Pangkalan Data dan jejak audit);
3) masa retensi dan pengujian media penyimpan data; dan
4) *log* akses terhadap media penyimpan data.

Dalam membuat kebijakan dan prosedur serta standar untuk *library*, BPR dan BPR Syariah harus memperhatikan kecukupan prosedur penyimpanan (*storage*), rekam cadang (*back-up),* pemulihan(*restore*), dan pemusnahan (*disposal*) media. BPR dan BPR Syariah harus selalu melakukan penginian rekam cadang data dan aplikasi untuk memastikan rekam cadang dimaksud dapat digunakan dalam rangka memulihkan sistem, aplikasi, dan data pada saat terjadi bencana atau gangguan lainnya.

2. Kebijakan dan Prosedur Perencanaan, Pengelolaan, Pemeliharaan, dan Penghapusan Perangkat Keras dan Perangkat Lunak

   BPR dan BPR Syariah harus memiliki kebijakan dan prosedur untuk operasional TI yang terkait dengan perangkat keras maupun perangkat lunak, antara lain dengan melakukan identifikasi serta pencatatan inventaris aset TI dan diperbarui secara berkala. Kebijakan dan prosedur operasional TI, mencakup:

   a. Kebijakan dan Prosedur Perencanaan Kapasitas

      BPR dan BPR Syariah harus memiliki kebijakan dan prosedur perencanaan kapasitas untuk dapat memastikan bahwa perangkat keras dan perangkat lunak yang digunakan BPR atau BPR Syariah telah sesuai dengan kebutuhan operasional bisnis dan mengantisipasi perkembangan usaha BPR atau BPR Syariah. Tanpa perencanaan kapasitas yang baik, BPR dan BPR Syariah menghadapi risiko kekurangan atau pemborosan sumber daya TI. Perencanaan kapasitas disusun secara berkala dan selalu dilakukan penginian untuk mengakomodasi perubahan yang ada.

   b. Kebijakan dan Prosedur Pengelolaan Konfigurasi Perangkat Keras dan Perangkat Lunak

      Dalam pengelolaan konfigurasi perangkat keras dan perangkat lunak, BPR dan BPR Syariah harus menetapkan prosedur terkait:

      1) proses instalasi perangkat keras dan perangkat lunak. Instalasi perangkat keras dan perangkat lunak BPR dan BPR Syariah hanya dapat dilakukan oleh Satuan Kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI atau pihak lain dengan otorisasi dari pihak penyelenggara TI;
      2) pengaturan parameter (*hardening*) perangkat keras dan perangkat lunak; dan

         Contoh:

         a) Seluruh perangkat komputer BPR dan BPR Syariah dilengkapi dengan anti-virus dan/atau anti-*malware* yang dikinikan secara otomatis dan berkala.
         b) *Port* USB terkait penyimpanan data pada perangkat komputer BPR dan BPR Syariah dibatasi penggunaannya.
         c) Perangkat komputer terkunci secara otomatis pada saat perangkat tidak aktif untuk beberapa saat.
         d) Seluruh perangkat komputer BPR dan BPR Syariah dipasang dengan *firewall* lokal (*host-based firewall*)

      3) inventarisasi dan penginian informasi perangkat keras, perangkat lunak, perangkat jaringan, media penyimpan, dan perangkat pendukung lainnya yang terdapat di Pusat Data.

Inventarisasi yang dilakukan meliputi:

a) perangkat keras
inventarisasi perangkat keras harus dilakukan secara menyeluruh termasuk inventarisasi terhadap perangkat keras yang dimiliki oleh pihak lain tetapi berada di BPR atau BPR Syariah. Informasi perangkat keras yang penting untuk dilakukan penginian antara lain nama PPJTI, model perangkat keras, tanggal pembelian dan instalasi, kapasitas *processor*, memori utama, kapasitas penyimpanan, sistem operasi, fungsi, dan lokasi.

b) perangkat lunak
BPR dan BPR Syariah harus melakukan inventarisasi atas informasi mengenai nama dan jenis perangkat lunak (peladen virtual, sistem operasi, sistem aplikasi, atau sistem utilitas). Informasi lain yang harus ada di dalam inventarisasi perangkat lunak meliputi nama pembuat atau PPJTI, tanggal instalasi, nomor versi dan keluaran (*release*), pemilik perangkat lunak, *setting parameter* dan *service* yang aktif, jumlah lisensi yang dimiliki, jumlah yang di-*install* dan jumlah pengguna (*user*).

c) perangkat jaringan
infrastruktur jaringan merupakan hal yang penting bagi operasional BPR atau BPR Syariah, sehingga satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI harus mendokumentasikan konfigurasi jaringan secara lengkap. Informasi dalam hasil dokumentasi mencakup antara lain:
(1) diagram jaringan;
(2) identifikasi seluruh koneksi intern dan ekstern BPR atau BPR Syariah;
(3) daftar dan kapasitas peralatan jaringan seperti *switch, router, hub, gateway, firewall*, dan lain-lain;
(4) identifikasi PPJTI terkait telekomunikasi di intern BPR atau BPR Syariah, antara BPR atau BPR Syariah dengan pihak lain, dan dengan internet;
(5) gambaran sistem pengamanan jaringan; dan
(6) klasifikasi antara jaringan untuk sistem kritikal dengan jaringan umum (contoh: surat elektronik) dan klasifikasi jaringan yang terpisah untuk layanan terminal perbankan elektronik antara lain ATM/CDM/EDC disertai dengan enkripsi *end-to-end* atau VPN.

d) media penyimpan
Informasi yang diperlukan dalam inventarisasi media penyimpan antara lain jenis dan kapasitas, lokasi penyimpanan baik *on-site* maupun *off-site*, tipe dan klasifikasi data yang disimpan, *source system,* serta frekuensi dan masa retensi rekam cadang.

e) perangkat pendukung Pusat Data
BPR dan BPR Syariah harus menginventarisasi perangkat pendukung Pusat Data antara lain

Uninterruptible Power Supply (UPS) dan *power control*, pendeteksi dan pemadam api (*fire detection and extinguisher*), pendingin udara (*air conditioning*), *generator set*, serta pengukur suhu dan kelembaban udara.

c. Kebijakan dan Prosedur Pemeliharaan Perangkat Keras dan Perangkat Lunak

1) Pemeliharaan Perangkat Keras dan Fasilitas Pusat Data

Pemeliharaan preventif secara berkala terhadap peralatan TI perlu dilakukan untuk meminimalkan kegagalan pengoperasian peralatan tersebut dan untuk mendeteksi secara dini permasalahan yang potensial. Untuk itu BPR dan BPR Syariah perlu memiliki kontrak pemeliharaan dengan PPJTI guna memastikan ketersediaan dukungan pemeliharaan dari PPJTI. Semua pemeliharaan yang dilakukan hendaknya didasarkan pada jadwal yang telah ditetapkan, didokumentasikan pada suatu *log*, dan dilakukan evaluasi secara berkala.

2) Pengamanan Fisik dan Pengendalian Lingkungan Pusat Data

a) Pengendalian Akses Fisik Pusat Data

Akses fisik ke Pusat Data harus dibatasi dan dikendalikan dengan baik. Pintu Pusat Data harus selalu terkunci, apabila perlu bisa dilengkapi dengan kartu akses dan/atau *biometric device*. Ruang Pusat Data tidak boleh diberi label atau papan petunjuk (*signing board*) sehingga orang mudah mengenalinya. BPR dan BPR Syariah harus memiliki *logbook* untuk mencatat tamu yang memasuki Pusat Data.

b) Pengendalian lingkungan Pusat Data

Dalam rangka penerapan pengendalian lingkungan Pusat Data, satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI harus melakukan paling sedikit:

(1) mengawasi dan memantau lingkungan Pusat Data, antara lain mencakup sumber listrik, api, air, suhu, dan kelembapan udara. Pengendalian lingkungan yang dapat diterapkan antara lain penggunaan *Uninterruptible Power Supply* (UPS), pengaturan suhu dan kelembaban udara (AC, termometer, dan higrometer), pendeteksi asap/api/panas, sistem pemadaman api, kamera *Closed Circuit Television* (CCTV), dan pengendali hama (*pest control*).

(2) memastikan tersedianya sumber listrik yang cukup, stabil, dan tersedianya sumber alternatif untuk mengantisipasi tidak berfungsinya sumber listrik utama. Untuk mengantisipasi putusnya arus listrik sewaktu-waktu, BPR dan BPR Syariah perlu memastikan pengatur voltase listrik, UPS, dan generator listrik dapat bekerja dengan baik pada saat diperlukan. BPR dan BPR Syariah sebaiknya menggunakan metode pemindahan secara otomatis (*automatic switching*) jika terjadi gangguan pada salah satu

sumber listrik untuk menjaga pasokan listrik yang sesuai dengan kebutuhan peralatan.

(3) memastikan Pusat Data memiliki alat pendeteksi api dan asap serta pipa pembuangan air. Selanjutnya, BPR dan BPR Syariah harus menyediakan sistem pemadam api yang memadai, baik yang dapat beroperasi secara otomatis maupun dioperasikan secara manual. Zat pemadam api dan sistem yang digunakan harus memperhatikan keamanan terhadap peralatan dan petugas pelaksana Pusat Data.

(4) mengamankan sistem perkabelan untuk menghindari efek *interference*di Pusat Data.

(5) menginventarisasi perangkat pendukung Pusat Data antara lain UPS dan *power control*, *fire detection and extinguisher*, *air conditioning*, termometer, dan higrometer.

c) Kinerja Perangkat Keras dan Perangkat Lunak

Pemantauan terhadap perangkat keras dan perangkat lunak minimal dilakukan setiap hari untuk memastikan seluruh perangkat tersebut beroperasi sebagaimana mestinya, misalnya peladen tetap dalam keadaan menyala, kapasitas Pangkalan Data dan utilitas peladen tidak melampaui limit, dan fasilitas pendukung berfungsi dengan baik. BPR dan BPR Syariah memiliki kebijakan TI tertulis dan memantau implementasi terkait siklus hidup perangkat keras dan/atau perangkat lunak, serta mengidentifikasi perangkat yang sudah masuk/mendekati masa *End-of-Life* (EOL) dan/atau *End-of-Support* (EOS).

d. Kebijakan dan Prosedur Penghapusan Perangkat Keras dan Perangkat Lunak (*Disposal*)

Disposal meliputi menghapus perangkat lunak, menghancurkan perangkat keras dan data yang sudah tidak digunakan lagi atau masa retensinya telah habis. Kode sumber versi lama yang sudah tidak dipakai lagi harus disimpan dengan indikasi yang jelas mengenai tanggal, waktu, dan informasi lain ketika digantikan dengan kode sumber versi terbaru. Kegiatan penghapusan yang dilakukan paling sedikit:

1) memindahkan data dari sistem produksi ke media rekam cadangdengan mekanisme sesuai prosedur, termasuk prosedur uji coba dan rekam cadang;
2) menyimpan dokumentasi sistem sebagai persiapan jika diperlukan untuk meng-*install* ulang suatu sistem ke peladen operasional;
3) mengelola arsip data sesuai masa retensi; dan
4) menghancurkan data yang habis masa retensinya.

3. Kebijakan dan Prosedur Pengelolaan Perubahan (*Change Management*)

Change Management adalah prosedur yang mengatur penambahan, penggantian, maupun penghapusan objek dilingkungan operasional. Objek dimaksud dapat berupa data, program, aplikasi, menu, perangkat komputer, perangkat jaringan, dan proses. BPR dan BPR Syariah harus memiliki kebijakan dan prosedur *Change Management* yang paling sedikit mencakup permintaan, analisis,

persetujuan perubahan, perubahan konfigurasi, daninstalasi perubahan termasuk pemindahan perangkat keras dan perangkat lunak dari lingkungan pengujian ke lingkungan operasional.

Change Management harus memperhatikan hal-hal sebagai berikut:

a. Pengendalian Perubahan

Ketergantungan antar Sistem Elektronik yang digunakan pada berbagai satuan kerja memerlukan penyelenggaraan TI yang terintegrasi. Oleh karena itu semua perubahan harus melalui fungsi pengawasan dalam *Change Management* yang terkoordinasi dan melibatkan perwakilan dari satuan kerja bisnis, satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI, dan keamanan informasi. Prosedur instalasi perubahan harus memperhatikan kelangsungan operasional pada lingkungan produksi, pengawasan, dan pengaturan pengamanan penyelenggaraan TI. Standar minimum yang diatur harus mencakup risiko, pengujian, otorisasi dan persetujuan, waktu implementasi, validasi setelah proses *install*, dan pemulihan (*recovery*).

b. *Patch Management*

Dalam *Change Management*, BPR dan BPR Syariah harus memiliki dokumentasi yang lengkap tentang instalasi *patch* yang dilakukan. Selain itu BPR dan BPR Syariah harus memastikan bahwa BPR atau BPR Syariah menggunakan versi perangkat lunak terbaru yang paling sesuai. BPR dan BPR Syariah juga harus memiliki informasi terkini mengenai perbaikan produk, masalah keamanan, *patch* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan.

c. Migrasi data

Migrasi data terjadi jika terdapat perubahan besar pada Sistem Elektronik BPR atau BPR Syariah, atau terjadi penggabungan data dari beberapa Sistem Elektronik yang berbeda. Dalam hal terdapat migrasi data, BPR dan BPR Syariah perlu memiliki kebijakan dan prosedur mengenai penanganan migrasi data. Tahap-tahap yang perlu dilalui dalam melakukan migrasi data dimulai dari rencana strategis, manajemen proyek, *Change Management*, pengujian, rencana kontinjensi, rekam cadang, manajemen PPJTI dan *post implementation review*.

4. Kebijakan dan Prosedur Penanganan Kejadian/Permasalahan

Prosedur penanganan kejadian/permasalahan harus mencakup perangkat keras, sistem operasi, sistem aplikasi, perangkat jaringan, dan peralatan keamanan.

BPR dan BPR Syariah harus memelihara sarana yang diperlukan untuk menangani permasalahan antara lain:

a. *Help desk*

BPR dan BPR Syariah harus memiliki fungsi *helpdesk* agar permasalahan yang dihadapi oleh pengguna dapat segera ditangani.

Hal-hal yang perlu diperhatikan dalam fungsi *helpdesk,* yaitu:

1) Tersedianya dokumentasi permasalahan yang lengkap yaitu dokumentasi permasalahan harus mencakup data pengguna, penjelasan masalah, dampak pada sistem (*platform*, aplikasi, atau lainnya), kode prioritas, status resolusi saat ini, pihak yang bertanggung jawab terhadap resolusi, akar permasalahan (jika teridentifikasi), target

waktu resolusi, dan *field* komentar untuk mencatat kontak pengguna dan informasi relevan lainnya.

2) BPR dan BPR Syariah dapat menggunakan sistem yang berbasis pengetahuan (*knowledge based system*) untuk memberikan dukungan kepada staf *help desk* tentang alternatif solusi permasalahan yang umum terjadi. BPR dan BPR Syariah secara berkala melakukan penginian terhadap sistem tersebut dengan informasi yang didapat dari PPJTI dan dari pengalaman staf *help desk*.

b. Penanganan Penggunaan *Superuser*

Superuser adalah *user-id* yang memiliki kewenangan sangat luas. Dalam rangka penanganan permasalahan, BPR dan BPR Syariah harus menetapkan prosedur penanganan *superuser* agar penggunaannya tidak disalahgunakan. Prosedur tersebut paling sedikit mengatur hal-hal sebagai berikut:

1) penetapan pihak yang memiliki hak akses *superuser* termasuk penerapan *dual custody* (pemecahan *password* kepada lebih dari 1 (satu) orang);
2) prosedur penyimpanan *password superuser*;
3) prosedur *break ID super user* pada keadaan darurat;
4) prosedur penggantian *password superuser* setelah digunakan;
5) pemantauan aktivitas yang dilakukan oleh *superuser*; dan
6) pendokumentasian penggunaan *superuser* dalam bentuk berita acara.

c. Rekam Cadang dan Uji *Restore*

Rekam cadang dan uji *restore* diperlukan untuk menjamin tersedianya data untuk kelangsungan operasional BPR atau BPR Syariah, baik dalam operasional secara rutin maupun apabila terjadi gangguan kerusakan terhadap data sehingga kerugian yang lebih besar dapat dihindarkan. Pengujian *restore* rekam cadang dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun. Dalam hal ini rekam cadangdan uji *restore* dimaksud meliputi data, *file*, aplikasi, sistem operasi, dan dokumen lainnya, harus disimpan di lokasi terpisah dari Pusat Data (*off site*) yang memenuhi standar pengamanan yang memadai. Hal-hal tersebut di atas adalah beberapa contoh kontrol dan teknologi yang dapat digunakan untuk membantu pengamanan informasi.

5. Kebijakan dan Prosedur Pengendalian Pertukaran Informasi (*Exchange of Information*)

Pengiriman informasi secara *online* maupun melalui media penyimpan harus dikelola secara memadai oleh BPR dan BPR Syariah untuk mencegah risiko terkait pengamanan informasi. BPR dan BPR Syariah harus memiliki prosedur pengelolaan transmisi informasi secara fisik dan *logic* paling sedikit:

a. permintaan dan pemberian informasi oleh pihak intern dan ekstern; dan
b. pengiriman informasi melalui berbagai media, seperti *hardcopy*, *disc*, surat elektronik, pos, dan internet.

BPR dan BPR Syariah harus mempertimbangkan pemisahan segmen WAN (*Wide Area Network*) dan LAN (*Local Area Network*) dengan perangkat pengamanan (seperti *firewall*) yang membatasi akses dan lalu lintas keluar masuknya data.

6. Kebijakan dan Prosedur Fungsi Kendali Mutu (*Quality Assurance)*
   BPR dan BPR Syariah perlu mempertimbangkan untuk memiliki fungsi kendali mutu atas operasional TI.
   Fungsi kendali mutu melakukan penilaian kualitas perangkat keras dan perangkat lunak sesuai dengan standar yang ditetapkan. Setiap pembuatan dan perubahan sistem harus melalui persetujuan fungsi kendali mutu sebelum diimplementasikan (*deployment*) ke lingkungan operasional sesuai dengan pedoman pengembangan Sistem Elektronik dan *change management.*
7. Kebijakan dan Prosedur Pengelolaan Hubungan dengan Pihak Penyedia Jasa
   Apabila penyelenggaraan TI BPR atau BPR Syariah dilakukan oleh PPJTI, BPR dan BPR Syariah harus memiliki fungsi pengelolaan hubungan dengan pihak ketiga yang bertugas memantau layanan PPJTI dengan menggunakan prosedur yang paling sedikit mencakup reputasi penyedia jasa, kelangsungan penyediaan layanan, pemantauan tingkat layanan (*service level agreement*), pelaporan permasalahan, dan dokumentasi yang terkait dengan layanan PPJTI.

B. KEBIJAKAN DAN PROSEDUR LAYANAN DIGITAL

Perkembangan pesat TI mendukung BPR dan BPR Syariah untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik atau dikenal dengan Layanan Perbankan Digital, yang selanjutnya disingkat Layanan Digital. Contoh Layanan Digital, antara lain *internet banking* dan *mobile banking*.

Seiring dengan peningkatan layanan nasabah, penggunaan Layanan Digital berpotensi meningkatkan risiko antara lain risiko operasional, risiko hukum, dan risiko reputasi. Oleh karena itu, penyediaan Layanan Digital harus memperhatikan prinsip kehati-hatian, prinsip pengamanan, dan perlindungan nasabah yang memadai serta searah dengan strategi bisnis BPR dan BPR Syariah.

Hal-hal yang perlu diperhatikan dalam cakupan kebijakan dan prosedur Layanan Digital adalah sebagai berikut:

1. Kebijakan dan prosedur secara tertulis untuk setiap layanan digital yang diterbitkan memuat paling sedikit:
   a. tanggung jawab dan kewenangan dalam pengelolaan produk dan aktivitas Layanan Digital;
   b. sistem informasi akuntansi produk dan aktivitas Layanan Digital termasuk keterkaitan dengan sistem informasi akuntansi BPR dan BPR Syariah secara menyeluruh; dan
   c. prosedur identifikasi, pengukuran, pemantauan, dan pengendalian berbagai risiko yang melekat pada produk dan aktivitas Layanan Digital.
2. Setiap kebijakan dan prosedur harus memenuhi prinsip pengendalian pengamanan data nasabah dan transaksi Layanan Digital, yaitu:
   a. prinsip kerahasiaan (*confidentiality*)
      BPR dan BPR Syariah memastikan bahwa metode dan prosedur yang digunakan dapat melindungi kerahasiaan data nasabah.
   b. prinsip integritas (*integrity*)
      BPR dan BPR Syariah memastikan bahwa metode dan prosedur yang digunakan mampu menjamin data yang digunakan akurat, andal, konsisten, dan terbukti kebenarannya sehingga terhindar

dari kesalahan, kecurangan, manipulasi, penyalahgunaan, dan perusakan data.

c. prinsip ketersediaan (*availability*)
BPR dan BPR Syariah memastikan ketersediaan Layanan Digital untuk digunakan oleh nasabah setiap saat.

d. prinsip keaslian (*authentication*)
BPR dan BPR Syariah harus dapat menguji keaslian identitas nasabah untuk memastikan informasi yang disampaikan dan/atau transaksi keuangan dilakukan oleh nasabah yang berhak.

e. prinsip tidak dapat diingkari (*non repudiation*)
BPR dan BPR Syariah harus menyusun, menetapkan, dan melaksanakan prosedur yang dapat memastikan bahwa transaksi yang telah dilakukan tidak dapat diingkari dan dapat dipertanggungjawabkan.

f. prinsip pengendalian otorisasi dalam sistem, Pangkalan Data (*database*), dan aplikasi (*authorization of control*)
BPR dan BPR Syariah memastikan antara lain:
1) adanya pengendalian terhadap hak akses dan otorisasi yang tepat terhadap sistem, Pangkalan Data (*database*) dan aplikasi yang digunakan dalam penyelenggaraan TI; dan
2) seluruh informasi dan data penyelenggaraan TI yang bersifat rahasia hanya dapat diakses oleh pihak yang telah memiliki otorisasi serta harus dipelihara secara aman dan dilindungi dari kemungkinan diketahui atau dimodifikasi oleh pihak yang tidak berwenang.

g. prinsip pemisahan tugas dan tanggung jawab (*segregation of duties*)
BPR dan BPR Syariah memastikan terdapat pemisahan tugas dan tanggung jawab terkait sistem, Pangkalan Data (*database*) dan aplikasi yang digunakan dalam penyelenggaraan TI untuk terlaksananya fungsi *check and balance*, misalnya terdapat pemisahan tugas antara pihak yang menginisiasi atau meng-input data dengan pihak yang bertanggung jawab untuk memverifikasi dan/atau mengotorisasi kebenaran data tersebut.

h. prinsip pemeliharaan jejak audit (*maintenance of audit trails*)
BPR dan BPR Syariah memastikan ketersediaan dan pemeliharaan *log* transaksi sesuai dengan kebijakan retensi data dan ketentuan peraturan perundang-undangan, agar terdapat jejak audit yang jelas untuk membantu pembuktian, penyelesaian perselisihan, dan pendeteksian usaha penyusupan pada Sistem Elektronik. BPR dan BPR Syariah harus menganalisis dan mengevaluasi fungsi jejak audit secara berkala.

Dalam menetapkan pengendalian pengamanan pada Layanan Digital, BPR dan BPR Syariah selain harus memperhatikan pengamanan layanan terhadap nasabah juga memperhatikan pengamanan serta hak dan kewajiban pihak lain yang terkait dan/atau yang bekerja sama dengan BPR dan BPR Syariah dalam menyelenggarakan Layanan Digital, khususnya terkait pengelolaan, penggunaan, dan penyimpanan data nasabah Layanan Digital. BPR dan BPR Syariah yang memberikan Layanan Digital menerapkan *Data Loss Prevention* (DLP) pada *endpoint* dan *gateway*.

BAB IV
JARINGAN KOMUNIKASI

Jaringan komunikasi merupakan hal yang sangat penting bagi industri keuangan. Hal tersebut dapat dilihat dari perkembangan produk dan aktivitas lembaga keuangan yang beragam dengan adanya jaringan komunikasi. Bahkan saat ini layanan perbankan sudah menjadi seperti tanpa batasan wilayah seiring berkembangnya jaringan komunikasi. BPR dan BPR Syariah dapat menyediakan Layanan Digital seperti *internet Banking* dan *mobile Banking*, baik yang diselenggarakan secara mandiri oleh BPR atau BPR Syariah maupun bekerja sama dengan PPJTI.

Jaringan komunikasi termasuk hal yang perlu dipastikan kesediaan, (*availability*), integritas, kerahasiaan, danakses kontrol dengan cara menerapkan kebijakan dan prosedur pengelolaan jaringan dengan baik, memaksimalkan kinerja jaringan, mendesain jaringan yang tahan terhadap gangguan, dan mendefinisikan layanan jaringan secara jelas serta melakukan pengamanan yang diperlukan.

A. KEBIJAKAN, STANDAR, DAN PROSEDUR JARINGAN KOMUNIKASI

BPR dan BPR Syariah harus memiliki kebijakan, standar, dan prosedur sebagai pedoman dalam menerapkan teknologi jaringan komunikasi untuk meyakinkan bahwa kelangsungan operasional dan keamanan jaringan komunikasi tetap terjaga.

Kebijakan jaringan komunikasi merupakan arah dan tujuan pengelolaan jaringan komunikasi yang akan diselenggarakan BPR dan BPR Syariah, misalnya terkait dengan penerapan enkripsi pada jaringan komunikasi.

Standar jaringan komunikasi merupakan sejumlah parameter yang ditetapkan oleh BPR dan BPR Syariah untuk memenuhi kebijakan jaringan komunikasi, misalnya penggunaan *Secure Socket Layer* (SSL) pada layer *Session*.

Prosedur jaringan komunikasi merupakan serangkaian langkah teknis yang akan dilakukan oleh BPR dan BPR Syariah untuk memenuhi standar jaringan komunikasi.

Kebijakan, standar, dan prosedur yang perlu ditetapkan paling sedikit:

1. pengukuran kinerja dan perencanaan kapasitas jaringan (*performance and capacity planning*);
2. pengamanan jaringan komunikasi (*network access controls*, termasuk *remote access*);
3. *change management* (*setting, configuration, and testing*);
4. *network management, logging* dan *monitoring*;
5. penggunaan *internet*, *intranet*, surat elektronik, dan *wireless* (termasuk mekanisme penggunaan jaringan komunikasi);
6. tersedianya prosedur penyelesaian masalah (*trouble shooting*);
7. tersedianya fasilitas untuk rekam cadang dan pemulihan; dan
8. kecukupan kontrak dan tersedianya SLA yang sesuai dengan kebutuhan BPR dan BPR Syariah dan harus dipantau secara berkala apabila jaringan komunikasi yang digunakan oleh BPR atau BPR Syariah diselenggarakan oleh PPJTI.

B. DESAIN JARINGAN KOMUNIKASI

Jaringan komunikasi harus didesain sedemikian rupa sehingga efisien tetapi juga dinamis untuk mengantisipasi pengembangan di masa yang akan datang. Pada tahap ini, terdapat beberapa hal yang diperhatikan, yaitu:

1. Penentuan Topologi Jaringan Komunikasi
   Penggunaan topologi direncanakan sesuai dengan kebutuhan, dalam hal ini kompleksitas sistem BPR dan BPR Syariah. Termasuk dalam hal ini memperhatikan konektivitas antar kantor dengan Pusat Data (DC) dan/atau Pusat Pemulihan Bencana (DRC).
2. Perencanaan kapasitas (*capacity planning*) jaringan komunikasi.
   Perencanaan kapasitas jaringan komunikasi data dilakukan dengan memperhatikan rencana strategi bisnis dan riwayat penggunaan jaringan komunikasi data BPR dan BPR Syariah.
3. Pemilihan media jaringan komunikasi, misalnya kabel dan nirkabel.
4. Rekam cadang perangkat keras, *alternative routing* (jalur alternatif), atau *provider* alternatif.
5. Pengamanan fisik dan *logic* paling sedikit terdiri atas:
   a. penempatan perangkat jaringan pada lokasi yang aman terhadap gangguan alam dan akses oleh orang yang tidak berhak; dan
   b. pengaturan parameter sistem perangkat jaringan, misal jaringan untuk publik dan jaringan untuk privat.
6. Tersedianya jejak audit, paling sedikit terhadap perubahan-perubahan pada *setting* parameter dan hak akses perangkat jaringan komunikasi dan juga penggunaan atas hak akses tersebut.

BAB V
PENGAMANAN INFORMASI

Informasi merupakan aset penting bagi BPR dan BPR Syariah, baik informasi yang terkait dengan nasabah, keuangan, laporan maupun informasi lainnya. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan, atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun non-finansial bagi BPR atau BPR Syariah. Selain itu juga memberikan dampak bagi nasabah maupun *stakeholder* lainnya, termasuk terhadap sistem perbankan nasional. Informasi harus dilindungi atau diamankan oleh seluruh personil di BPR atau BPR Syariah.

Pengamanan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen TI terkait, seperti perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC, dan lain-lain) dan sumber daya manusia (termasuk kualifikasi dan keterampilan).

A. PRINSIP PENGAMANAN INFORMASI

Pengamanan informasi paling sedikit memperhatikan prinsip-prinsip sebagai berikut:

1. Kerahasiaan (*confidentiality*) untuk menjamin bahwa informasi hanya diakses oleh pihak yang berwenang. Prinsip kerahasiaan dapat diperoleh antara lain melalui pengendalian akses (*access control*), enkripsi data saat disimpan dan ditransmisikan, autentikasi pengguna (*multi factor authentification* – MFA, *password policy*), dan kebijakan klasifikasi informasi. BPR dan BPR Syariah menerapkan pengendalian akses berbasis peran (*Role Based Access Control* – RBAC) terhadap seluruh sistem.
2. Integritas (*integrity*) untuk menjamin bahwa informasi akurat, lengkap, dan tidak dapat diubah selain oleh pihak yang berwenang. Prinsip integritas dapat diperoleh antara lain melalui *hashing*, *logging*, *change management*, dan *versioning* dokumen.
3. Ketersediaan (*availability*) untuk menjamin bahwa informasi dan sistemnya tersedia saat dibutuhkan oleh pengguna yang berwenang. Prinsip ketersediaan dapat diperoleh, antara lain melalui *backup* dan *recovery*, redundansi sistem, sistem proteksi terhadap serangan DDoS, serta pemeliharaan dan pemantauan infrastruktur TI.

Selain itu, pengamanan informasi juga wajib memperhatikan hal berikut:

1. aspek sumber daya manusia, proses, dan teknologi;
2. pengamanan informasi secara komprehensif dan berkesinambungan yaitu dengan menetapkan tujuan dan kebijakan pengamanan informasi, implementasi pengendalian pengamanan informasi, memantau dan mengevaluasi kinerja dan efektivitas kebijakan pengamanan informasi, serta melakukan penyempurnaan.

Untuk meningkatkan pengamanan informasi, BPR dan BPR Syariah dapat mempertimbangkan implementasi standar internasional di bidang pengamanan informasi, antara lain *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC), *National Institute of Standards and Technology* (NIST), *Information Technology Infrastructure Library* (IT-IL), dan standar nasional seperti Standar Nasional Indonesia (SNI), dengan memperhatikan kompleksitas usaha yang meliputi, antara lain keragaman dalam jenis transaksi/produk/jasa dan jaringan kantor serta teknologi pendukung

yang digunakan. Dalam hal penggunaan data penduduk, BPR dan BPR Syariah harus menerapkan ISO 27001 sebagaimana dipersyaratkan oleh otoritas terkait.

B. KEBIJAKAN PENGAMANAN INFORMASI

Direksi BPR dan BPR Syariah harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap pengamanan informasi. Kebijakan tersebut harus dikomunikasikan secara berkala kepada seluruh pegawai BPR atau BPR Syariah dan pihak ekstern yang terkait. Disamping itu, perlu dilakukan evaluasi secara berkala danpenginian apabila terdapat perubahan penting. Kebijakan tentang pengamanan informasi paling sedikit:

1. tujuan pengamanan informasi yang paling sedikit pengelolaan aset, sumber daya manusia, pengamanan fisik, pengamanan *logic* (*logical security*), pengamanan operasional TI, penanganan insiden, pengamanan jaringan komunikasi, dan pengamanan informasi dalam pengembangan sistem;
2. komitmen Direksi terhadap pengamanan informasi sejalan dengan strategi dan tujuan bisnis;
3. prinsip dan standar pengamanan informasi, termasuk kepatuhan terhadap ketentuan yang berlaku, pelatihan dan peningkatan kesadaran atas pentingnya pengamanan informasi (*security awareness program*), rencana kelangsungan bisnis dan sanksi atas pelanggaran;
4. analisis dampak pengamanan informasi terhadap kelangsungan bisnis;
5. tugas dan tanggung jawab pihak-pihak dalam pengamanan informasi; dan
6. dokumen atau ketentuan lain yang mendukung kebijakan pengamanan informasi.

C. STANDAR PENGAMANAN INFORMASI

Direksi BPR dan BPR Syariah harus menetapkan standar pengamanan informasi sesuai dengan kebijakan pengamanan informasi antara lain mengacu pada ketentuan peraturan perundangan-undangan dan *best practice*, sebagai dasar untuk mengimplementasikan pengamanan informasi. Standar pengamanan informasiantara lain standar *password*, standar enkripsi, standar pengamanan perangkat jaringan, standar pengamanan *end-point*, dan standar pengaman aplikasi.

D. PROSEDUR PENGAMANAN INFORMASI

1. Pengelolaan Aset
   a. aset BPR dan BPR Syariah yang terkait dengan informasi harus diidentifikasikan, ditentukan pemilik/penanggung jawabnya (*data owner*) dan dicatat agar dapat dilindungi secara tepat;
   b. aset yang terkait dengan informasi tersebut dapat berupa data (baik *hardcopy* maupun *softcopy*), perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC) dan sumber daya manusia yang kompeten;
   c. pengaturan penggunaan informasi dan aset harus diidentifikasi, didokumentasikan, dan diimplementasikan. Seluruh pegawai BPR dan BPR Syariah dan pihak ketiga harus mematuhi pengaturan tersebut, seperti pengaturan penggunaan surat elektronik, *internet*, *mobile devices*, *teleworking*, dan lainnya. Surat elektronik korporasi dilindungi sistem pengecekan otomatis spam, *phising*, dan *malware*; dan

d. informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya. Contoh dari klasifikasi tersebut antara lain:
   1) informasi rahasia, misalnya data simpanan nasabah, data pribadi nasabah;
   2) informasi intern, misalnya peraturan tentang gaji pegawai BPR atau BPR Syariah; dan
   3) informasi biasa, misalnya informasi tentang produk BPR atauBPR Syariah yang ditawarkan ke masyarakat.

   Klasifikasi dapat dibuat berdasarkan nilai, sensitivitas, hukum/ketentuan, dan tingkat kepentingan bagi BPR atau BPR Syariah.

2. Pengelolaan Sumber Daya Manusia (SDM)
   a. BPR dan BPR Syariah harus menerapkan pengendalian yang memadai sebelum mempekerjakan pegawai TI (pegawai tetap atau pegawai tidak tetap), konsultan, termasuk pegawai PPJTI pada posisi yang memiliki kerentanan atau dampak yang besar terhadap pengamanan informasi. Sebagai contoh yaitu melakukan *background check* catatan kriminal atau kejahatan lainnya seperti pencurian data, dan lain-lain saat melakukan rekrutmen untuk posisi *network administrator* atau *system administrator*;
   b. SDM baik pegawai BPR atau BPR Syariah, konsultan, pegawai tidak tetap dan pegawai PPJTI yang memiliki akses terhadap informasi harus memahami tanggung jawab terhadap pengamanan informasi, termasuk penggunaan *single* ID yang unik dan *password* pribadi untuk mengakses perangkat komputer;
   c. peran dan tanggung jawab SDM baik pegawai BPR atau BPR Syariah, konsultan, pegawai tidak tetap, dan pegawai PPJTI yang memiliki akses terhadap informasi harus didefinisikan dan didokumentasikan sesuai dengan kebijakan pengamanan informasi;
   d. dalam perjanjian kerja dengan pegawai BPR atauBPR Syariah (pegawai tetap dan pegawai tidak tetap) harus tercantum ketentuan-ketentuan mengenai pengamanan informasi yang sesuai dengan kebijakan pengamanan informasi BPR atau BPR Syariah. Sebagai contoh, perlu adanya klausula yang menyatakan bahwa pegawai BPR atau BPR Syariah (pegawai tetap dan pegawai tidak tetap) harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi;
   e. dalam hal BPR dan BPR Syariah bekerja sama dengan PPJTI dan/atau konsultan, perjanjian kerja sama antara BPR atauBPR Syariah dengan PPJTI dan/atau konsultan harus mencantumkan ketentuan mengenai pengamanan informasi, seperti klausul kerahasiaan informasi (*non-disclosure agreement*). Selain itu, semua pegawai yang ditugaskan PPJTI dan/atau konsultan di BPR atau BPR Syariah harus menandatangani suatu perjanjian menjaga kerahasiaan informasi dalam hal yang bersangkutan memiliki akses data BPR dan BPR Syariah;
   f. pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai BPR atau BPR Syariah, konsultan, pegawai tidak tetap, dan pegawai PPJTI. Pelatihan

dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab masing-masing pihak;

g. BPR dan BPR Syariah harus menetapkan sanksi atas pelanggaran terhadap kebijakan pengamanan informasi;

h. BPR dan BPR Syariah harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan perubahan/penutupan hak akses pegawai BPR atau BPR Syariah, konsultan, pegawai tidak tetapdan pegawai PPJTI yang disebabkan karena perubahan tugas atau selesainya masa kerja atau kontrak; dan

i. BPR dan BPR Syariah harus menetapkan pemisahan tugas dan tanggung jawab (*segregation of duties*), yaitu memastikan terdapat pemisahan tugas dan tanggung jawab antara sumber daya manusia di operasional BPR atau BPR Syariah.

3. Pengamanan Fisik dan Lingkungan

a. fasilitas pemrosesan informasi yang penting (misalnya *mainframe,* peladen, komputer, dan perangkat jaringan aktif) harus diberikan pengamanan fisik dan lingkungan yang memadai untuk mencegah akses yang tidak terotorisasi, kerusakan, serta gangguan lain;

b. pengamanan fisik dan lingkungan terhadap fasilitas pemrosesan informasi yang penting meliputi antara lain pembatas ruangan, pengendalian akses masuk (misalnya penggunaan *access control card*, *Personal Identification Number/*PIN, *biometrics*), kelengkapan alat pengamanan di dalam ruangan (misalnya alarm, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara) serta pemeliharaan kebersihan ruangan dan peralatan (misalnya dari debu, rokok, makanan/minuman, barang mudah terbakar);

c. fasilitas pendukung seperti AC, sumber daya listrik, dan pendeteksi dan pemadam api harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi;

d. pemisahan antara aset milik BPR atau BPR Syariah dengan PPJTI (misalnya peladen, *switching tools*) harus diidentifikasikan secara jelas dan diberikan perlindungan yang memadai seperti menerapkan pengamanan yang cukup, *dual control*, atau menempatkannya secara terpisah;

e. harus dilakukan pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan.

4. Pengamanan Logic (*Logic Security*)

a. BPR dan BPR Syariah harus memiliki prosedur formal secara tertulis yang telah disetujui oleh Direksi tentang pengadministrasian pengguna yang meliputi pendaftaran, perubahan dan penghapusan pengguna, baik untuk pengguna internal maupun eksternal BPR atau BPR Syariah, (misalnya PPJTI), antara lain terkait kebijakan dan prosedur penambahan/perubahan/penghapusan hak akses dalam hal terjadi perpindahan pegawai;

b. BPR dan BPR Syariah memiliki kebijakan dan melakukan kendali terhadap akses pengguna bagi seluruh pegawai, termasuk terkait kompleksitas *password*;

c. BPR dan BPR Syariah harus menerapkan metode identifikasi dan otentikasi (*authentication*) sesuai analisis risiko. Metode otentikasi yang digunakan, dapat berupa satu atau kombinasi

dari "*what you know*" (antara lain PIN dan *password*), "*what you have*" (antara lain OTP, *smart card*, dan token), "*what you are*" (antara lain *biometric* seperti retina dan sidik jari);

d. Pemberian akses mengacu pada prinsip berdasarkan kebutuhan bisnis dan dengan akses yang seminimal mungkin (*least privilege*).

e. BPR dan BPR Syariah harus menetapkan prosedur pengendalian melalui pemberian *password* atau PIN awal (*initial password* atau PIN) kepada pengguna dengan memperhatikan paling sedikit:
   1) *password* atau PIN awal harus diganti saat *login* pertama kali;
   2) *password* atau PIN awal diberikan secara aman, misalnya melalui amplop tertutup atau kertas berlapis dua;
   3) *password* atau PIN awal bersifat khusus (*unique*) untuk setiap pengguna dan tidak mudah ditebak;
   4) pemilik *user-id* terutama dari pegawai BPR atauBPR Syariah, pegawai tidak tetap, dan pegawai PPJTI harus menandatangani pernyataan tanggung jawab atau perjanjian penggunaan *user-id* dan *password* saat menerima *user-id* dan *password*;
   5) *password* atau PIN standar (*default password*atau PIN) yang dimiliki oleh sistem operasi, sistem aplikasi, *database management system*, dan perangkat jaringan, harus diganti oleh BPR atau BPR Syariah sebelum diimplementasikan dan sedapat mungkin mengganti *user-id* standar dari sistem (*default user-id*).

f. BPR dan BPR Syariah harus mewajibkan pengguna untuk:
   1) menjaga kerahasiaan *password*;
   2) menghindari penulisan *password* di kertas dan tempat lain tanpa pengamanan yang memadai;
   3) memilih *password* yang berkualitas, yaitu:
      a) panjang *password* yang memadai sehingga tidak mudah ditebak;
      b) mudah diingat dan terdiri dari paling sedikit kombinasi 2 tipe karakter (huruf, angka, atau karakter khusus);
      c) tidak didasarkan atas data pribadi pengguna seperti nama, nomor telepon, atau tanggal lahir;
      d) tidak menggunakan kata yang umum dan mudah ditebak oleh perangkat lunak (untuk menghindari *brute force attack*), misalnya kata 'pass', *'password'*, 'adm', '123', atau kata umum di kamus;
   4) mengubah *password* secara berkala; dan
   5) menghindari penggunaan *password* yang sama secara berulang.

g. BPR dan BPR Syariah harus menonaktifkan hak akses jika *user-id* tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan *password* (*failed login attempt*) dan menonaktifkan pengguna setelah mencapai jumlah maksimal kegagalan *password*. BPR dan BPR Syariah memiliki kebijakan dan prosedur penambahan/perubahan/penghapusan hak akses dalam hal terjadi perpindahan pegawai.

h. BPR dan BPR Syariah harus melakukan pemeriksaan/*review* berkala terhadap hak akses pengguna untuk memastikan

bahwa hak akses yang diberikan sesuai dengan wewenang yang diberikan.

i. sistem operasi, sistem aplikasi, Pangkalan Data, *utility,* dan perangkat lainnya yang dimiliki oleh BPR dan BPR Syariah sedapat mungkin membantu pelaksanaan pengamanan *password*, sebagai contoh:
   1) memaksa pengguna untuk mengubah *password* setelah jangka waktu tertentu dan menolak bila pengguna memasukkan *password* yang sama dengan yang digunakan sebelumnya saat mengganti *password*;
   2) menyimpan *password* secara aman (terenkripsi);
   3) memutuskan hubungan atau akses pengguna jika tidak terdapat respons selama jangka waktu tertentu (*session time-out*);
   4) menonaktifkan atau menghapus hak akses pengguna jika pengguna tidak melakukan *login* melebihi jangka waktu tertentu (*expiration interval*), misalnya karena cuti atau pindah bagian.

j. BPR dan BPR Syariah harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai dalam penggunaan perangkat *mobile computing* dan media penyimpan data seperti *notebook, hand phone, flash disk*, *external hard disk*, dan media lainnya, termasuk bila menggunakan *wireless access* atau *wireless network*.

k. BPR dan BPR Syariah harus memperhitungkan risiko dan menerapkan pengendalian pengamanan yang memadai terhadap titik akses (*access point*) ke dalam jaringan komputer dan/atau sarana pemrosesan informasi yang dapat dimanfaatkan oleh pihak yang tidak berwenang.

l. BPR dan BPR Syariah yang menggunakan *file sharing* harus menetapkan pembatasan akses paling sedikit melalui penggunaan *password* dan pengaturan pihak yang berwenang melakukan akses.

m. BPR dan BPR Syariah perlu memperhatikan penerapan standar konfigurasi pengamanan (*security hardening*) terhadap perangkat keras dan perangkat lunak, seperti *setting parameter* atau*patch*.

n. Pihak yang memiliki akses administrator di BPR dan BPR Syariah menggunakan akun yang berbeda dari akun harian (*daily use account*). Contoh: pihak yang memiliki akses administrator staf TI atau vendor.

5. Pengamanan Operasional TI

   Hal-hal yang harus diperhatikan dalam pengamanan operasional TI antara lain:

   a. informasi dan perangkat lunak harus dibuatkan rekam cadangdan prosedur pemulihan yang teruji sesuai dengan klasifikasi dan tingkat kepentingannya;
   b. BPR dan BPR Syariah perlu mengantisipasi dan menerapkan pengendalian pengamanan yang memadai atas kelemahan sistem operasi, sistem aplikasi, Pangkalan Data dan jaringan komunikasi, termasuk ancaman dari pihak yang tidak berwenang seperti *virus, trojan horse, worms, spyware, Denial-of-Service (*DoS*), war driving, spoofing,* dan *logic bomb*;
   c. BPR dan BPR Syariah harus membuat kebijakan dan prosedur yang mencakup identifikasi *patch* yang ada, evaluasi,

melakukan pengujian dan menginstalasinya jika memang dibutuhkan, antara lain sistem operasi dan antivirus;

d. BPR dan BPR Syariah harus memelihara catatan dari versi perangkat lunak yang digunakan dan memantau secara rutin informasi tentang penginian (*enhancement*) produk, masalah keamanan, *patch* atau *upgrade*, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan;

e. BPR dan BPR Syariah harus menetapkan penggunaan enkripsi dengan menggunakan teknik kriptografi tertentu dalam mengamankan proses transmisi informasi yang sensitif, khususnya yang melalui jaringan di luar jaringan komunikasi BPR atau BPR Syariah, sesuai dengan perkembangan teknologi terkini. Penggunaan teknik kriptografi tersebut antara lain ditujukan untuk menjaga dan memastikan kerahasiaan (*confidentiality*), integritas (*integrity*), keaslian (*authenticity*), dan nirsangkal (*non-repudiation*). Teknik yang dapat dipertimbangkan antara lain penggunaan enkripsi, seperti *Public Key Infrastructure*, *cipher text*, *hash function* dan *digital signatures*;

f. BPR dan BPR Syariah harus menyediakan dan melakukan evaluasi atas jejak audit/*log* baik di tingkat jaringan, sistem maupun aplikasi serta menetapkan jenis *log* (misalnya *administrator log, user log, system log*), informasi yang harus dimasukkan ke dalam *log*, jangka waktu penyimpanan atau kapasitas *log* dengan memperhatikan ketentuan yang berlaku untuk keperluan penelusuran masalah.

g. BPR dan BPR Syariah memiliki mekanisme sinkronisasi antar Sistem Elektronik dengan acuan yang disepakati, dalam hal ini mengimplementasikan *Network Time Protocol* (NTP).

h. Perangkat kerja BPR dan BPR Syariah memiliki perlindungan dengan sistem keamanan berbasis perilaku yang mampu mendeteksi perilaku mencurigakan dan serangan yang belum dikenal. Sistem keamanan berbasis perilaku misalnya *Endpoint Detection and Response* (EDR).

6. Prosedur Pemantauan Pengamanan Informasi

BPR dan BPR Syariah harus melakukan pemantauan dalam rangka mendeteksi berbagai upaya yang mengancam pengamanan informasi dengan metode yang ditentukan berdasarkan risiko atau tingkat kritikalitas informasi atau aset TI BPR dan BPR Syariah. Pemantauan dapat dilakukan secara *realtime* untuk memberikan *alert* ketika terjadi aktivitas yang tergolong mencurigakan berdasarkan tingkat risiko, misalnya *brute force* terhadap *password* administrator atau upaya mengakses peladen pada *port* yang tidak wajar atau dilakukan secara berkala, misalnya di luar jam kerja atau pada akhir hari.

7. Penanganan Insiden dalam Pengamanan Informasi

Hal-hal yang harus diperhatikan BPR dan BPR Syariah dalam melakukan penanganan insiden dalam pengamanan informasi antara lain:

a. tindakan saat terjadi insiden berupa:
   1) identifikasi serta validasi, untuk memastikan kebenaran insiden yang terjadi;
   2) klasifikasi dan kategorisasi berdasarkan tingkat kritikalitas (*high, medium, low*);
   3) tindakan respons, berupa *containment* (mengisolasi sistem terdampak agar tidak meluas), *eradication*

(menghilangkan sumber insiden), dan *recovery* (memulihkan sistem dan layanan ke kondisi normal dengan pengamanan tambahan);

4) pelaporan (*incident report*) kepada Direksi, regulator (jika diwajibkan), serta pihak terkait lainnya, dengan muatan laporan insiden paling sedikit memuat kronologi, penyebab, dampak, langkah penanganan, serta status terkini;
5) evaluasi dan kaji ulang pascainsiden (*post-incident review*), dengan melakukan *lessons learned* untuk mengidentifikasi kelemahan kontrol keamanan dan proses penanganan insiden, serta memberikan rekomendasi perbaikan mitigasi ke depan termasuk panduan penanganan insiden; dan
6) penutupan insiden, melalui dokumentasi insiden sebagai referensi audit dan bahan analisis risiko setelah semua tindakan respons, pelaporan, dan tindak lanjut perbaikan dilakukan.

b. BPR dan BPR Syariah harus menetapkan prosedur penanganan insiden dalam pengamanan informasi yang mengatur antara lain:
1) *awareness* bagi pegawai BPR atau BPR Syariah, pegawai tidak tetap, dan pegawai PPJTI untuk melaporkan insiden;
2) unit kerja atau personil yang harus dihubungi jika terjadi insiden pengamanan informasi (*Point of Contact/ PoC*);
3) jenis insiden yang harus dilaporkan;
4) mekanisme alur pelaporan dan penanganan insiden;
5) analisis atas insiden untuk mencegah terulangnya insiden; dan
6) pendokumentasian bukti terkait insiden dan tindak lanjutnya.

c. BPR dan BPR Syariah dapat mempertimbangkan pembentukan tim khusus yang menangani insiden pengamanan oleh TTIS (Tim Tanggap Insiden Siber) sesuai dengan skala usaha dan kompleksitas penyelenggaraan TI BPR atau BPR Syariah;

d. BPR dan BPR Syariah menetapkan hal-hal terkait penanganan insiden dalam pengamanan informasi sebagai berikut:
1) Anggota TTIS termasuk tugas dan tanggung jawab;
2) Panduan untuk melakukan *assessment* terhadap kebenaran laporan insiden termasuk klasifikasi insiden dalam pengamanan informasi yang disampaikan PoC;
3) Panduan penanganan insiden dalam pengamanan informasi yang akan dilakukan oleh TTIS. Contoh klasifikasi insiden adalah sebagai berikut:
a) *Denial of Service* (DoS);
b) akses fisik dan *logic* yang dilakukan oleh pihak yang tidak berwenang terhadap Sistem Elektronik;
c) penyebaran *malicious code* (misalnya virus, *worms*, dan *trojan horse*);
d) pelanggaran terhadap kebijakan pengamanan informasi dalam penggunaan *resource* TI oleh pegawai BPR dan BPR Syariah, pegawai tidak tetap, maupun PPJTI (misalnya penggunaan email kantor untuk tujuan *spamming*); dan
e) metode verifikasi oleh TTIS untuk meyakini bahwa laporan insiden dalam pengamanan informasi yang

disampaikan oleh PoC adalah benar termasuk dalam kejadian yang diklasifikasikan sebagai insiden dalam pengamanan informasi. Dalam hal insiden dalam pengamanan informasi yang dilaporkan tersebut benar merupakan insiden dalam pengamanan informasi maka TTIS harus menindaklanjuti insiden dalam pengamanan informasi tersebut sesuai panduan penanganan insiden dalam pengamanan informasi yang sesuai.

4) Panduan TTIS dalam melakukan penanganan terhadap insiden dalam pengamanan informasi sesuai jenisnya, mencakup langkah-langkah antara lain:
   a) dokumentasi semua informasi mengenai insiden dalam pengamanan informasi;
   b) identifikasi sistem TI yang terkena dampak insiden dalam pengamanan informasi;
   c) pengumpulan semua informasi yang tersimpan dalam sistem TI yang diidentifikasi terkena dampak insiden dalam pengamanan informasi. Dalam hal informasi tersebut akan dijadikan barang bukti digital (*digital evidence*) maka pengumpulan (*collection*) dan penyimpanan (*preservation*) informasi harus dilakukan dengan metode *digital forensically sound*;
   d) implementasi solusi terhadap insiden dalam pengamanan informasi sesuai dengan jenisnya dengan terlebih dahulu mendapat persetujuan Direksi;
   e) dalam hal TTIS mengidentifikasi bahwa insiden dalam pengamanan informasi tidak dapat dikendalikan, harus dilakukan eskalasi kepada Direksi untuk mengaktifkan prosedur penanganan krisis; dan
   f) penyusunan laporan lengkap atas aktivitas penanganan insiden dalam pengamanan informasi untuk disampaikan kepada Direksi baik saat masih dalam proses penanganan maupun setelah solusi diimplementasikan dan insiden dalam pengamanan informasi berstatus *closed*; dan
5) Penginian terhadap panduan penanganan insiden dalam pengamanan informasi menggunakan l*esson learned* dari aktivitas penanganan insiden dalam pengamanan informasi sebelumnya.

e. BPR dan BPR Syariah harus memelihara dokumentasi lengkap atas suatu insiden dalam pengamanan informasi;

f. BPR dan BPR Syariah secara berkala melakukan kaji ulang terhadap panduan penanganan insiden dalam pengamanan informasi untuk memastikan panduan tersebut relevan dengan kondisi sistem TI BPR dan BPR Syariah terkini;

g. BPR dan BPR Syariah dapat mempertimbangkan pemberian insentif kepada pegawai BPR dan BPR Syariah, pegawai tidak tetap, dan pegawai PPJTI yang melaporkan insiden atau *vulnerabilities* TI yang berisiko dieksploitasi dan mengancam pengamanan informasi, dalam rangka mendorong tercapainya pengamanan informasi yang kuat atau memadai.

8. Retensi Data
   Retensi data dilakukan untuk mempertahankan integritas data yang di rekam cadang dalam jangka waktu tertentu. Jangka waktu retensi data disesuaikan dengan ketentuan peraturan perundang-undangan yang mengatur mengenai dokumen perusahaan. BPR dan BPR Syariah memiliki kebijakan terkait penyimpanan *log* yang memiliki periode retensi untuk keperluan audit dan investigasi insiden siber.
9. Lainnya
   Pengamanan informasi juga perlu diterapkan dalam aspek lain seperti pengembangan dan pengadaan Sistem Elektronik, jaringan komunikasi data, rencana pemulihan bencana, dan kegiatan kerja sama dengan PPJTI.

BAB VI
RENCANA PEMULIHAN BENCANA

Kegiatan perbankan tidak dapat terhindar dari adanya gangguan/kerusakan yang disebabkan oleh alam maupun manusia, misalnya terjadinya gempa bumi, kebakaran, banjir, gangguan tenaga listrik (*power failure*), kesalahan teknis, kelalaian manusia, huru-hara dan sebagainya. Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi suatu BPR atau BPR Syariah, tetapi juga berdampak pada kegiatan operasional bisnis BPR atau BPR Syariah terutama pelayanan kepada nasabah. Bila tidak ditangani secara khusus, selain BPR atau BPR Syariah akan menghadapi risiko operasional, BPR dan BPR Syariah juga dapat menghadapi risiko reputasi yang berdampak pada menurunnya tingkat kepercayaan nasabah kepada BPR atauBPR Syariah.

Untuk meminimalisasi risiko tersebut, BPR dan BPR Syariah diharapkan memiliki *Business Continuity Management* (BCM) yaitu proses manajemen terpadu dan menyeluruh untuk menjamin operasional bisnis BPR atau BPR Syariah tetap dapat berfungsi walaupun menghadapi gangguan/bencana guna melindungi kepentingan para pemangku kepentingan. BCM yang efektif perlu didukung dengan beberapa hal salah satunya adalah penyusunan *Business Continuity Plan* (BCP).

Komponen prosedur BCP yang wajib dimiliki oleh BPR dan BPR Syariahadalah Rencana Pemulihan Bencana (*Disaster Recovery Plan*) sesuai dengan POJK PTI BPR dan BPR Syariah. Rencana Pemulihan Bencana lebih menekankan pada aspek teknologi dengan fokus pada pemulihan infrastruktur TI (*infrastructure recovery/restoration*) dan sistem informasi setelah gangguan atau bencana. Rencana Pemulihan Bencana memuat detail langkah teknis untuk *restore* data, aplikasi, jaringan, peladen, dan Aplikasi Inti Perbankan, termasuk mencakup prosedur *failover* dan penetapan parameter pemulihan, antara lain *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO).

A. KEBIJAKAN DAN PROSEDUR RENCANA PEMULIHAN BENCANA

Direksi BPR dan BPR Syariah harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap rencana pemulihan bencana yang mencakup:

1. Prinsip Penyusunan Rencana Pemulihan Bencana

   Dalam penyusunan kebijakan untuk menangani kondisi bencana, BPR dan BPR Syariah harus memastikan penerapan prinsip sebagai berikut:

   a. Rencana Pemulihan Bencana disusun berdasarkan analisis dampak bisnis (*business impact analysis*) dan *risk assessment* yang memadai;
   b. Rencana Pemulihan Bencana bersifat fleksibel untuk dapat merespons berbagai skenario ancaman dan gangguan serta bencana yang sifatnya tidak terduga yang bersumber dari kondisi internal dan/atau eksternal;
   c. Rencana Pemulihan Bencana bersifat spesifik, terdapat kondisi tertentu dan tindakan yang dibutuhkan segera untuk mengatasi kondisi tersebut;
   d. Rencana Pemulihan Bencana dilakukan uji coba secara berkala paling sedikit:
      1) 1 (satu) kali dalam 2 (dua) tahun, bagi BPR dan BPR Syariah yang menyediakan layanan digital; atau
      2) 1 (satu) kali dalam 3 (tiga) tahun, bagi BPR dan BPR Syariah yang tidak menyediakan layanan digital.

2. Analisis Dampak Bisnis (*Business Impact Analysis*)
   Efektivitas dari Rencana Pemulihan Bencana bergantung pada kemampuan manajemen untuk mengidentifikasi tingkat kepentingan (*criticality*) berbagai proses kerja atau aktivitas yang ada di BPR dan BPR Syariah sebelum Rencana Pemulihan Bencana disusun atau dikaji ulang. Dengan demikian, analisis dampak bisnis (*business impact analysis*) merupakan dasar dari penyusunan keseluruhan Rencana Pemulihan Bencana. Hal-hal yang harus dianalisis dalam analisis dampak bisnis (*business impact analysis*) meliputi:
   a. tingkat kepentingan (*criticality*) masing-masing proses bisnis dan ketergantungan antar proses bisnis serta skala prioritas yang diperlukan;
   b. tingkat ketergantungan terhadap pihak penyedia jasa baik TI maupun non TI;
   c. jangka waktu BPR dan BPR Syariah dapat beroperasi tanpa sistem atau fasilitas yang mengalami gangguan dan/atau toleransi jangka waktu pemulihan sistem atau fasilitas tersebut hingga dapat berfungsi kembali;
   d. kebutuhan minimal jumlah personel, data, kelengkapan sistem, dan fasilitas yang diperlukan agar bisnis dapat beroperasi (*minimum resources requirement*);
   e. dampak potensial dari kejadian yang bersifat tidak spesifik dan tidak dapat dikontrol terhadap proses bisnis dan pelayanan kepada nasabah;
   f. dampak gangguan dan/atau bencana terhadap seluruh satuan kerja dan fungsi bisnis, bukan hanya terhadap *data processing*;
   g. estimasi *downtime* maksimum yang dapat ditoleransi, tingkat toleransi atas kehilangan data dan terhentinya proses bisnis, dan dampak *downtime* terhadap kerugian finansial;
   h. jalur komunikasi yang dibutuhkan untuk berjalannya pemulihan; dan
   i. dampak hukum dan pemenuhan ketentuan yang terkait, seperti ketentuan peraturan perundang-undangan mengenai kerahasiaan data nasabah.

   Dalam melakukan analisis dampak bisnis (*business impact analysis*), baik satuan kerja TI maupun masing-masing unit bisnis perlu memperhatikan bahwa Rencana Pemulihan Bencana yang akan disusun bukan hanya untuk *total disaster*, melainkan juga untuk berbagai situasi bencana dan gangguan mulai dari yang bersifat *minor*, *major* sampai dengan *catastrophic*.
   Dampak yang harus diperhatikan bukan hanya yang dapat diukur dengan jelas (*tangible impact*) seperti penalti akibat keterlambatan pembayaran bunga atau biaya lembur pegawai, melainkan juga yang tidak dapat diukur secara jelas (*intangible impact*) seperti kesulitan nasabah memperoleh pelayanan.
3. *Risk Assessment*
   Risk Assessment yang terdiri dari identifikasi dan pengukuran risiko merupakan tahap kedua yang harus dilalui dalam penyusunan Rencana Pemulihan Bencana. Proses ini diperlukan untuk dapat mengetahui tingkat kemungkinan terjadi gangguan pada kegiatan BPR dan BPR Syariah yang penting (*critical*) serta dampaknya bagi kelangsungan usaha BPR dan BPR Syariah. *Risk assessment* mencakup hal-hal paling sedikit:

a. melakukan analisis atas dampak gangguan atau bencana terhadap BPR dan BPR Syariah, nasabah, dan industri keuangan;
b. melakukan *gap analysis* dengan membandingkan kondisi saat ini dengan langkah atau skenario yang seharusnya diterapkan; dan
c. membuat peringkat potensi gangguan bisnis berdasarkan tingkat kerusakan (*severity*) dan kemungkinan terjadinya (*likelihood*).

4. Penyusunan Rencana Pemulihan Bencana

Penyusunan Rencana Pemulihan Bencana dilakukan setelah proses analisis dampak bisnis (*business impact analysis*) dan *risk assessment*. Adapun tujuan dan sasaran dari penyusunan Rencana Pemulihan Bencana antara lain:

a. mengamankan aset penting BPR dan BPR Syariah;
b. meminimalisasi risiko akibat bencana, misalnya membatasi kerugian finansial, risiko kepatuhan, dan risiko reputasi;
c. memastikan operasional BPR dan BPR Syariah tetap berjalan;
d. meyakini ketersediaan layanan yang berkesinambungan kepada nasabah; dan
e. mempersiapkan alternatif lain agar fungsi bisnis yang kritikal tetap dapat berjalan untuk menjaga kelangsungan operasional BPR dan BPR Syariah.

Rencana Pemulihan Bencana terdiri dari kebijakan, strategi, dan prosedur yang diperlukan untuk dapat memastikan kelangsungan proses bisnis pada saat terjadinya gangguan atau bencana. Rencana Pemulihan Bencana harus memuat beberapa alternatif strategi yang dapat diambil BPR dan BPR Syariah untuk mengatasi masing-masing jenis dan ukuran gangguan atau bencana. Strategi pemulihan tersebut disesuaikan dengan hasil analisis dampak bisnis (*business impact analysis*), analisis risiko, sumber daya yang dimiliki, serta kapasitas dan tingkat teknologi BPR dan BPR Syariah. Setiap strategi yang dipilih hendaknya disertai analisis atau alasan yang melatarberlakangi dan harus didukung dengan sistem dan prosedur yang sesuai.

5. Analisis terhadap Rencana Pemulihan Bencana

Analisis terhadap kemungkinan timbulnya risiko yang dapat disebabkan oleh faktor antara lain:

a. faktor kebakaran;
b. faktor alam, seperti banjir dan gempa;
c. faktor teknis, seperti kerusakan perangkat keras/lunak, gangguan tenaga listrik, atau gangguan transmisi data; dan/atau
d. faktor manusia, seperti sabotase.

6. Jenis Prosedur Rencana Pemulihan Bencana

Adapun jenis prosedur dalam Rencana Pemulihan Bencana antara lain mencakup:

a. prosedur tanggap darurat (*emergency response - immediate steps*) untuk mengendalikan sistem pada saat terjadi gangguan/bencana, mengurangi dampak kerugian, serta menentukan status keadaan bencana;
b. prosedur pemulihan sistem yang memungkinkan kegiatan operasional BPR atauBPR Syariah dapat kembali ke kondisi normal; dan
c. prosedur sinkronisasi data digunakan untuk memastikan kesamaan antara data mesin yang digunakan untuk

operasional dengan data rekam cadang, serta untuk memastikan semua data hasil pemrosesan bisnis selama masa pemulihan telah masuk ke dalam sistem.

7. Komponen Prosedur Rencana Pemulihan Bencana
   Setiap prosedur Rencana Pemulihan Bencana mencakup komponen paling sedikit:
   a. Personel
      Rencana Pemulihan Bencana harus secara jelas mengemukakan komposisi, wewenang, dan tanggung jawab setiap personel yang berkaitan dengan penyelenggaraan TI dan memiliki alur komunikasi yang memadai.
   b. Teknologi dan Aplikasi Utama
      Prosedur yang disusun harus memperhatikan komponen teknologi yang dimiliki BPR atau BPR Syariah seperti perangkat keras, perangkat lunak, dan fasilitas komunikasi BPR atau BPR Syariah.
      Selanjutnya BPR dan BPR Syariah harus memiliki prosedur dan dokumentasi yang lengkap untuk memulihkan aplikasi-aplikasi utama, antara lain Aplikasi Inti Perbankan maupun operasional BPR atau BPR Syariah lainnya.
      Selain itu hal-hal yang berkaitan dengan data juga perlu diperhatikan seperti dokumentasi sistem dan data rekam cadang.
   c. Pusat Pemulihan Bencana (*Disaster Recovery Center*/DRC)
      Bagi BPR dan BPR Syariah yang memiliki Pusat Pemulihan Bencana, BPR dan BPR Syariah harus memastikan ketersediaan Pusat Pemulihan Bencana sebagai rekam cadangPusat Data yang dapat dioperasikan apabila Pusat Data tidak dapat beroperasi (dalam kondisi bencana). Sesuai dengan alternatif strategi yang dipilih BPR dan BPR Syariah, Pusat Pemulihan Bencana dapat dikelola sendiri maupun oleh PPJTI dengan memperhatikan hal-hal sebagai berikut:
      1) Pusat Pemulihan Bencana hendaknya ditempatkan pada lokasi yang terpisah dari lokasi Pusat Data, dengan memperhatikan karakteristik risiko berdasarkan:
         a) analisis risiko yang berkaitan dengan lokasi Pusat Pemulihan Bencana (tidak berlokasi di wilayah gempa, petir, banjir, huru hara, kerusuhan, dan gangguan lain) dan terhubung dengan infrastruktur komunikasi dan listrik yang berbeda dengan Pusat Data, serta fasilitas lain yang diperlukan untuk tetap berjalannya suatu sistem; dan
         b) jangkauan geografi atas suatu gangguan/bencana dan dampaknya terhadap kota atau wilayah tempat lokasi Pusat Pemulihan Bencana berada.
      2) Pusat Pemulihan Bencana harus memiliki pasokan listrik dan sarana telekomunikasi yang dapat menjamin beroperasinya Pusat Pemulihan Bencana;
      3) sistem di Pusat Pemulihan Bencana harus kompatibel dengan sistem yang digunakan pada Pusat Data dan harus disesuaikan jika terjadi perubahan pada Pusat Data;
      4) Pusat Pemulihan Bencana merupakan *restricted area*; dan
      5) memperhitungkan waktu tempuh untuk terjaminnya proses *recovery*.
   d. Rekam Cadang Dokumentasi, Sistem, dan Data

BPR dan BPR Syariah harus memastikan ketersediaan rekam cadang yang efektif dari informasi bisnis yang penting, perangkat lunak dan dokumentasi terkait sistem, dan pengguna untuk setiap proses fungsi bisnis yang penting (*critical*). Hal-hal yang harus diperhatikan dalam dokumentasi, sistem, dan data rekam cadangantara lain mencakup:

1) rekam cadang tersebut harus disimpan di lokasi terpisah dari Pusat Data (*off site*) yang memenuhi standar sistem pengamanan yang memadai, serta setiap perubahan dan modifikasi harus didokumentasikan dan salinannya juga harus diperbaharui;
2) media rekam cadang (*backup*) harus disimpan di lingkungan yang aman di lokasi *off site* dengan standar sistem pengamanan yang memadai;
3) rekam cadang sistem secara menyeluruh (*full system backup*) harus dilakukan secara periodik atau jika terjadi perubahan sistem yang mendasar, rekam cadang tersebut harus dilakukan sesegera mungkin;
4) seluruh media rekam cadang menggunakan standar penamaan (*labeling*) untuk dapat mengidentifikasi penggunaan, tanggal, dan jadwal retensi;
5) media rekam cadang harus dilakukan uji *restore* secara periodik untuk memastikan rekam cadang dapat digunakan pada saat diperlukan (keadaan *emergency*); dan
6) BPR dan BPR Syariah harus memiliki prosedur untuk *disposal* media rekam cadang.

e. Fasilitas Komunikasi

BPR dan BPR Syariah harus memastikan tersedianya alternatif jalur komunikasidi wilayah operasional BPR atau BPR Syariah yang dapat digunakan di lingkungan intern maupun dengan pihak ekstern pada saat gangguan/bencana.

8. Penetapan Kejelasan Tanggung Jawab bagi Pihak-Pihak Terkait dalam Penyelenggaraan Rencana Pemulihan Bencana

a. Tanggung jawab Direksi BPR dan BPR Syariah paling sedikit:
   1) menetapkan kebijakan dan prosedur tertulis mengenai Rencana Pemulihan Bencana;
   2) menelaah dan menyetujui Rencana Pemulihan Bencana;
   3) melakukan evaluasi terhadap kelayakan Rencana Pemulihan Bencana milik PPJTI dalam hal BPR atau BPR Syariah melakukan kerja sama dengan PPJTI;
   4) menetapkan tingkat gangguan dan bencana serta pemulihannya; dan
   5) mengambil tindakan yang diperlukan untuk memastikan Rencana Pemulihan Bencana berjalan dengan efektif.

b. Tanggung jawab satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI paling sedikit:
   1) bertanggung jawab penuh terhadap efektivitas penyelenggaraan Rencana Pemulihan Bencana;
   2) penentuan skenario pemulihan yang akan digunakan apabila terjadi gangguan atau bencana berdasarkan prioritisasi atas Sistem Elektronik yang dianggap kritis;
   3) pelaksanaan pengujian dan pelaksanaan Rencana Pemulihan Bencana sesuai dengan skenario pemulihan yang ditetapkan;

4) evaluasi setiap tahapan dalam pengujian dan pelaksanaan Rencana Pemulihan Bencana, termasuk pelajaran terpetik (*lesson learned*) dan rekomendasi untuk pengujian selanjutnya; dan
5) menyampaikan laporan kepada Direksi terkait hasil pengujian dan pelaksanaan Rencana Pemulihan Bencana.

B. DOKUMENTASI STRATEGI DAN PROSEDUR UNTUK PEMULIHAN BENCANA (*RECOVERY*)

BPR dan BPR Syariah harus mendokumentasikan strategi dan prosedur untuk proses pemulihan yang mencakup:
1. mekanisme penanganan dan eskalasi insiden TI;
2. langkah pemulihan atas infrastruktur TI, sistem, dan data yang terdampak;
3. rencana keberlangsungan layanan utama agar tetap dapat berjalan secara berkesinambungan; dan
4. tata cara koordinasi dan komunikasi dengan pihak internal, regulator, dan pemangku kepentingan terkait.

C. UJI COBA RENCANA PEMULIHAN BENCANA

Uji coba Rencana Pemulihan Bencana diperlukan untuk memastikan bahwa Rencana Pemulihan Bencana dapat dioperasikan dengan baik pada saat terjadi gangguan/bencana. BPR dan BPR Syariah melakukan uji coba terhadap Rencana Pemulihan Bencana paling sedikit:
1. 1 (satu) kali dalam 2 (dua) tahun, bagi BPR dan BPR Syariah yang menyediakan layanan digital; atau
2. 1 (satu) kali dalam 3 (tiga) tahun, bagi BPR dan BPR Syariah yang tidak menyediakan layanan digital.

Uji coba dilakukan terhadap seluruh sistem/aplikasi kritikal dan infrastruktur yang kritikal berdasarkan BIA serta melibatkan pengguna TI.

Yang dimaksud dengan sistem/aplikasi dan infrastruktur yang kritikal adalah aplikasi dan infrastruktur yang berdasarkan hasil analisis dampak bisnis BPR dan BPR Syariah memiliki potensi risiko bagi bisnis dan operasional BPR dan BPR Syariah.

BPR dan BPR Syariah melakukan kaji ulang secara berkala terhadap Rencana Pemulihan Bencana, dengan mempertimbangkan hasil uji coba, termasuk dalam hal BPR dan BPR Syariah melakukan perubahan yang signifikan terhadap sistem, aplikasi, atau infrastruktur TI, misalnya perubahan pada Aplikasi Inti Perbankan. Kaji ulang Rencana Pemulihan Bencana termasuk melakukan pengujian *failover*.

Dalam hal BPR dan BPR Syariah menggunakan PPJTI dalam kegiatan operasional, uji coba yang dilakukan juga perlu melibatkan PPJTI dimaksud.

1. Ruang Lingkup Uji Coba

   BPR dan BPR Syariah harus secara jelas menentukan fungsi, sistem, dan proses yang akan dilakukan uji coba. Hal-hal yang perlu diuji coba antara lain meliputi efektivitas dari:
   a. prosedur penetapan tingkatgangguan dan bencana;
   b. fasilitas Pusat Pemulihan Bencana yang disediakan oleh PPJTI baik yang digunakan untuk BPR dan BPR Syariah sendiri maupun yang digunakan bersama dengan BPR dan BPR Syariah lain;
   c. prosedur pemulihan operasional TI; dan
   d. pemulihan Pusat Data.

Uji coba yang dilakukan harus didokumentasikan secara tertib dan dievaluasi untuk memastikan efektivitas dan keberhasilan uji coba. Dalam hal terdapat kelemahan atas uji coba Rencana Pemulihan Bencana maka perlu disempurnakan.

2. Skenario Uji Coba

BPR dan BPR Syariah harus memiliki skenario uji coba yang menyeluruh dan mencakup seluruh kondisi yang mungkin terjadi untuk setiap uji coba yangakandilakukan. Pelaksanaan skenario tersebut tidak boleh mengganggu kegiatan operasional BPR atauBPR Syariah. Pelaksanaan skenario uji coba diharapkan dapat mendeteksi adanya kelemahan dari prosedur yang ada dalam rangka perbaikan Rencana Pemulihan Bencana.

Dalam hal ini, BPR dan BPR Syariah perlu melakukan validasi asumsi yang digunakan dalam skenario pengujian, antara lain mengenai:

a. kritikalitas fungsi proses bisnis atau sistem yang diuji;
b. volume transaksi, termasuk *concurrent user*; dan
c. strategi Rencana Pemulihan Bencana yang dipilih BPR dan BPR Syariah.

3. Analisis dan Laporan Hasil Uji Coba

Hasil uji coba dan analisis dari setiap permasalahan yang ditemukan pada saat uji coba harus dilaporkan kepada Direksi. Hal-hal yang dilaporkan paling sedikit:

a. penilaian ketercapaian tujuan uji coba;
b. penilaian atas validitas uji coba pemrosesan data;
c. tindakan korektif untuk mengatasi permasalahan yang terjadi;
d. deskripsi mengenai perbandingan antara hasil dari Rencana Pemulihan Bencana dengan sistem yang digunakan dan hasil uji coba serta usulan perubahannya apabila terdapat perbedaan; dan
e. pelajaran terpetik (*lesson learned*) dan rekomendasi untuk uji coba selanjutnya.

Dalam hal berdasarkan hasil uji coba ditemukan kegagalan, BPR dan BPR Syariah harus mengkaji penyebab kegagalan atau permasalahan yang terjadi dan melakukan uji coba ulang.

D. PEMELIHARAAN RENCANA PEMULIHAN BENCANA

BPR dan BPR Syariah harus memastikan bahwa Rencana Pemulihan Bencana dapat dijalankan setiap saat antara lain dengan meningkatkan pemahaman kepada satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI di BPR dan BPR Syariah maupun pegawai di PPJTIatas pentingnya Rencana Pemulihan Bencana dan berpartisipasi aktif dalam pelaksanaan Rencana Pemulihan Bencana.

BPR dan BPR Syariah harus melakukan penginian Rencana Pemulihan Bencana untuk memastikan kesesuaiannya dengan kondisi saat ini. Dalam melakukan penginian, hal-hal yang perlu diperhatikan antara lain perubahan yang ada dalam sistem, perangkat lunak, sistem operasi, perangkat keras, pihak-pihak lain terkait (*counter parties*), dan penyedia layanan (*services provider*). Perubahan tersebut harus dianalisis pengaruhnya terhadap Rencana Pemulihan Bencana yang ada saat ini dan menentukan perbaikan yang dibutuhkan untuk mengakomodasi perubahan tersebut. Selanjutnya Rencana Pemulihan Bencana hasil penginian tersebut harus didokumentasikan dan didistribusikan ke satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI BPR atau BPR Syariah.

E. AUDIT INTERN

Satuan kerja audit intern atau fungsi yang bertanggung jawab atas audit intern harus melakukan pemeriksaan terhadap:

1. kesesuaian Rencana Pemulihan Bencana dengan kebijakan manajemen risiko BPR dan BPR Syariah;
2. Rencana Pemulihan Bencana mencakup kegiatan kritikal berdasarkan analisis dampak bisnis (*business impact analysis*) yang telah dilakukan oleh BPR dan BPR Syariah;
3. kecukupan Rencana Pemulihan Bencana untuk mengendalikan dan memitigasi risiko yang telah ditetapkan dalam *risk assessment*;
4. kecukupan prosedur pengujian Rencana Pemulihan Bencana;
5. efektifitas pelaksanaan pengujian Rencana Pemulihan Bencana; dan
6. keterkinian Rencana Pemulihan Bencana sesuai perkembangan kegiatan operasional BPR dan BPR Syariah dan hasil pengujian terakhir.

Satuan kerja audit intern atau fungsi yang bertanggung jawab atas audit intern harus mengomunikasikan hasil pemeriksaan dan memberikan rekomendasi kepada Direksi. Direksi hendaknya melakukan tindak lanjut atas laporan hasil audit tersebut dan merencanakan penyempurnaan atau perbaikan.

BAB VII
AUDIT INTERN TI

Sistem pengendalian intern yang efektif merupakan komponen penting dalam pengelolaan BPR dan BPR Syariah serta menjadi dasar bagi kegiatan operasional BPR dan BPR Syariah yang sehat dan aman. Sistem pengendalian intern yang efektif dapat membantu BPR atau BPR Syariah dalam menjaga aset, menjamin tersedianya pelaporan keuangan dan manajerial yang dapat dipercaya, meningkatkan kepatuhan BPR dan BPR Syariah terhadap ketentuan dan peraturan perundang-undangan, serta mengurangi risiko terjadinya kerugian, penyimpangan, dan pelanggaran aspek kehati-hatian.

Penggunaan sarana TI disamping meningkatkan kemampuan BPR dan BPR Syariah dalam melaksanakan kegiatan operasional, juga mengandung risiko yang dapat mengakibatkan kerugian, baik yang bersifat finansial maupun non-finansial. Oleh karena itu, sistem pengendalian intern perlu diterapkan sebagai salah satu upaya meminimalkan kerugian dimaksud.

Fungsi audit intern merupakan salah satu bagian dari sistem pengendalian intern. Pelaksanaan fungsi audit intern dilakukan dalam rangka melakukan evaluasi terhadap penyelenggaraan TI secara independen dan objektif untuk meningkatkan efisiensi dan efektivitas, pengendalian intern, dan tata kelola yang baik.

A. ORGAN PELAKSANA FUNGSI AUDIT INTERN TERHADAP PENYELENGGARAAN TI

Fungsi audit intern terhadap penyelenggaraan TI harus dilakukan dengan pelaksanaan sebagai berikut:

1. bagi BPR dan BPR Syariah, fungsi audit intern terhadap penyelenggaraan TI dilakukan sebagai bagian dari audit intern BPR sesuai dengan Peraturan Otoritas Jasa Keuangan yang mengatur mengenai penerapan tata kelola bagi BPR dan BPR Syariah. Pelaksanaan fungsi audit intern terhadap penyelenggaraan TI tersebut dapat dilaksanakan sendiri oleh BPR dan BPR Syariah yang bersangkutan atau menggunakan jasa auditor ekstern;
2. bagi BPR Syariah, fungsi audit intern terhadap penyelenggaraan TI tetap dilakukan dengan mengacu pada ketentuan mengenai penerapan tata kelola BPR Syariah dan peraturan perundang-undangan terkait lainnya.

Pelaksanaan fungsi audit intern dilakukan oleh Satuan Kerja Audit Intern atau Pejabat Eksekutif yang melaksanakan fungsi audit intern, yang disebut dengan organ pelaksana fungsi audit intern terhadap penyelenggaraan TI.

B. PEDOMAN AUDIT INTERN TERHADAP PENYELENGGARAAN TI

1. Kebijakan Umum Audit

   Pedoman audit intern terhadap penyelenggaraan TI mencakup kebijakan umum paling sedikit:

   a. pernyataan visi dan misi fungsi audit intern penyelenggaraan TI;
   b. struktur organisasi dan sistem pelaporan;
   c. penentuan frekuensi dan jadwal audit yang paling sedikit akan diterapkan BPR atau BPR Syariah untuk audit intern penyelenggaraan TI dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun sebagai bagian dari pelaksanaan audit intern; dan
   d. pelaksanaan audit intern dilakukan terhadap aspek terkait TI sesuai kebutuhan, prioritas, dan hasil analisis risiko TI BPR

atau BPR Syariah mencakup aspek sebagai berikut:

1) Aplikasi Inti Perbankan, untuk memastikan kesesuaian Aplikasi Inti Perbankan telah memenuhi standar minimal sebagai berikut:
   a) menerapkan ketentuan peraturan perundang-undangan bagi BPR atau BPR Syariah;
   b) melakukan pembukuan transaksi antar jaringan kantor:
      (1) pada hari yang sama bagi BPR dan BPR Syariah yang tidak menyediakan layanan digital dan tidak melakukan kegiatan sebagai penerbit alat pembayaran menggunakan kartu (APMK); dan
      (2) secara *online* dan *real time* bagi BPR dan BPR Syariah yang menyediakan layanan digital dan/atau melakukan kegiatan sebagai penerbit alat pembayaran menggunakan kartu (APMK).
   c) menghasilkan data dan informasi yang digunakan dalam mendukung proses penyusunan laporan untuk kebutuhan intern dan ekstern;
   d) mengonsolidasikan fungsi-fungsi yang terdapat dalam Aplikasi Inti Perbankan untuk mendukung penyediaan data dan informasi yang lengkap, akurat, kini, dan utuh; dan
   e) memiliki log aktivitas sistem.

   Dalam memastikan kesesuaian Aplikasi Inti Perbankan telah memenuhi standar minimal sebagaimana huruf a) sampai dengan huruf e), BPR dan BPR Syariah harus memperhatikan bahwa Aplikasi Inti Perbankan mampu mengimplementasikan profil nasabah secara terpadu (*Single Customer Identification File*).
2) wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TIdilaksanakan sesuai dengan wewenang dan tanggung jawab sebagaimana dimaksud dalam Bab I;
3) pengembangan dan pengadaan TI, untuk memastikan pengembangan dan pengadaan TI telah memenuhi standar minimal sebagaimana dimaksud dalam POJK PTI BPR dan BPR Syariah;
4) operasional TI, untuk memastikan kesesuaian pelaksanaan penyelenggaraan TI dengan kebijakan dan prosedur;
5) jaringan komunikasi,untuk memastikan pengelolaan jaringan komunikasi telah sesuai dengan kebijakan dan prosedur;
6) pengamanan informasi, untuk memastikan pemenuhan pengamanan fisik dan pengamanan *logic* dalam penyelenggaraan TI;
7) rencana pemulihan bencana, untuk memastikan rencana pemulihan bencana dapat dijalankan setiap saat;
8) fungsionalitas dari seluruh perangkat TI yang digunakan, untuk menjamin terpenuhinya unsur kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dalam operasional BPR atau BPR Syariah; dan
9) hak akses pegawai berdasarkan klasifikasi data dan

informasi.

e. prosedur audit intern terhadap penyelenggaraan TI untuk setiap aktivitas TI dalam penyelenggaraan TI yang memerlukan audit.

2. Perencanaan Audit

Organ pelaksana fungsi audit intern terhadap penyelenggaraan TI harus memiliki rencana audit tahunan terkait penyelenggaraan TI terhadap satuan kerja yang bertanggung jawab terhadap penyelenggaraan TI. Dalam melakukan fungsi audit intern untuk menilai penyelenggaraan TI, fungsi audit intern paling sedikit melakukan hal-hal sebagai berikut:

a. mengidentifikasi data, aplikasi dan sistem operasi, teknologi, fasilitas dan personil;
b. mengidentifikasi kegiatan dan proses bisnis yang menggunakan TI; dan
c. mengidentifikasi tingkat dampak risiko TI dalam operasional BPR dan BPR Syariah serta mempertimbangkan skala prioritas berdasarkan tingkat risiko.

Rencana audit intern terhadap penyelenggaraan TI harus mendapat persetujuan dari Direksi.

3. Pelaksanaan Audit

Pelaksanaan audit bertujuan untuk:

a. memastikan kebijakan, standar, dan prosedur penyelenggaraan TI diterapkan secara efektif;
b. memastikan efektivitas penerapan manajemen risiko TI;
c. memastikan efektivitas standar pengelolaan informasi dan pengamanan penyelenggaraan TI;
d. menilai kecukupan kontrol yang diterapkan dalam penyelenggaraan TI;
e. memberikan rekomendasi perbaikan untuk mengatasi kekurangan dalam penyelenggaraan TI; dan
f. memastikan kepatuhan penyelenggaraan TI terhadap ketentuan peraturan perundang-undangan.

Dalam rangka melaksanakan rencana tahunan audit, program audit (*audit working plan* yang selanjutnya disebut "AWP") disusun untuk setiap penugasan audit, yang paling sedikit:

a. tujuan audit, jadwal, jumlah auditor, anggaran, dan pelaporan;
b. cakupan audit sesuai hasil penilaian risiko; dan
c. langkah-langkah teknis audit yang diperlukan untuk mencapai tujuan audit.

Dalam pelaksanaannya, audit intern terhadap penyelenggaraan TI harus memperhatikan aspek-aspek kerahasiaan terhadap data dan informasi yang diperoleh. Fungsi audit intern terhadap penyelenggaraan TI harus memperhatikan fleksibilitas AWP agar dapat disesuaikan dan dilengkapi sesuai dengan risiko yang diidentifikasi.

Auditor TI harus menjunjung tinggi kode etik dalam melaksanakan tugas, yaitu sebagai berikut:

a. integritas
    1) bekerja dengan jujur, tekun, dan bertanggung jawab;
    2) taat terhadap peraturan dan membuat pengungkapan yang sesuai dengan peraturan;
    3) tidak melakukan kegiatan yang ilegal; dan
    4) menghormati dan berperan dalam mendukung tujuan BPR dan BPR Syariah;
b. objektif

1) tidak ikut berperan dalam kegiatan yang dapat mempengaruhi objektivitas pelaksanaan tugas audit;
2) tidak menerima apapun yang dapat mempengaruhi pelaksanaan tugas audit dan bekerja sesuai keahliannya; dan
3) mengungkapkan fakta sebagaimana yang ditemukan dalam pelaksanaan tugas audit;

c. kerahasiaan
1) berhati-hati dalam penggunaan data atau informasi dan melindungi data atau informasi yang diperoleh dalam pelaksanaan tugas audit; dan
2) tidak menggunakan data atau informasi yang diperoleh untuk kepentingan pribadi ataupun bertentangan dengan hukum; dan

d. kompetensi
1) memiliki pengetahuan yang memadai;
2) melaksanakan tugas audit sesuai dengan standar yang ditetapkan oleh BPR dan BPR Syariah; dan
3) berusaha terus menerus meningkatkan kemampuan untuk meningkatkan kualitas audit.

Pernyataan mengenai kode etik auditor TI dapat dituangkan dalam bentuk surat pernyataan tertulis yang ditandatangani oleh masing-masing personel auditor TI, termasuk mencakup sanksi apabila yang bersangkutan melanggar etika tersebut.

Dalam pelaksanaan audit dilengkapi dengan kertas kerja, isi dan format laporan hasil audit, dokumentasi dan distribusi, serta pemantauan tindak lanjutnya. Temuan audit harus disertai dengan bukti-bukti dan kertas kerja pemeriksaan yang didokumentasikan dengan baik.

4. Pelaporan

Laporan pelaksanaan fungsi audit intern terhadap penyelenggaraan TI merupakan sarana bagi Direksi untuk melakukan penilaian terhadap kualitas dan kinerja satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI, serta memberikan saran perbaikan. Laporan tersebut disampaikan secara tepat waktu kepada Direktur Utama, dengan tembusan disampaikan kepada Dewan Komisaris dan/atau komite audit, anggota Direksi yang membawahkan fungsi kepatuhan, dan Dewan Pengawas Syariah bagi BPR Syariah. Laporan mengenai pelaksanaan fungsi audit intern terhadap penyelenggaraan TI disampaikan juga kepada Otoritas Jasa Keuangan sebagai bagian dari laporan pelaksanaan dan pokok hasil audit intern sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan tata kelola bagi BPR dan BPR Syariah.

5. Tindak Lanjut Audit

Auditee harus memberikan tanggapan terhadap hasil audit. Apabila temuan perlu ditindaklanjuti, *auditee* harus memberikan komitmen dan target waktu penyelesaiannya. Selanjutnya, fungsi audit intern terhadap penyelenggaraan TI harus memantau pelaksanaan komitmen *auditee* atas hasil audit secara berkala dan melakukan verifikasi terhadap kecukupan perbaikan yang telah dilakukan.

Fungsi audit intern terhadap penyelenggaraan TI harus memelihara dokumentasi atas hasil tindak lanjut tersebut. Laporan tindak lanjut hasil audit disampaikan kepada Direktur Utama, dengan tembusan kepada Dewan Komisaris dan/atau komite audit, anggota

Direksi yang membawahkan fungsi kepatuhan, dan Dewan Pengawas Syariah bagi BPR Syariah.

6. Pengembangan dan Pengujian Sistem Elektronik
   Fungsi audit intern terhadap penyelenggaraan TIdapat berperan dalam pengembangan Sistem Elektronik untuk memastikan bahwa Sistem Elektronik sesuai dengan kebutuhan BPR atau BPR Syariah serta ketentuan yang berlaku, memiliki kontrol yang memadai, dan memiliki sarana untuk penelusuran kembali (jejak audit), namun tidak dapat berperan sebagai penentu Sistem Elektronik diimplementasikan, melainkan berpartisipasi sebagai narasumber dalam aspek pengendalian khususnya mengenai standar pengamanan yang diperlukan. Peran ini diperlukan agar auditor dapat menjaga independensi dan obyektifitas dalam audit yang dilakukan apabila Sistem Elektronik diimplementasikan. Selain itu fungsi audit intern terhadap penyelenggaraan TI dapat memberikan rekomendasi kepada Direktur Utama atau anggota Direksi lainnya mengenai kontrol yang perlu diterapkan.

C. PELAKSANAAN FUNGSI AUDIT INTERN TERHADAP PENYELENGGARAAN TI YANG DILAKSANAKAN OLEH AUDITOR EKSTERN

Dalam hal terdapat keterbatasan kemampuan fungsi audit intern terhadap TI BPR dan BPR Syariah, pelaksanaan fungsi audit intern dapat dilakukan oleh auditor ekstern seperti Kantor Akuntan Publik atau Lembaga Audit TI Independen. Penggunaan jasa auditor ekstern untuk melaksanakan fungsi audit intern terhadap penyelenggaraan TI BPR atau BPR Syariah tidak mengurangi tanggung jawab fungsi audit intern terhadap penyelenggaraan TI atas temuan audit dan tindak lanjutnya.

Penggunaan jasa auditor ekstern tersebut harus mempertimbangkan ukuran dan kompleksitas usaha BPR atau BPR Syariah. Pelaksanaan fungsi audit intern terhadap penyelenggaraan TI oleh auditor ekstern tetap memperhatikan aspek kompetensi antara lain pengetahuan dan pengalaman yang memadai dan independensi serta didasari perjanjian kerja sama. Meskipun pelaksanaan fungsi audit intern dilakukan oleh auditor ekstern, prosedur audit terhadap penyelenggaraan TI harus tetap mengacu pada kebijakan dan prosedur audit intern terhadap penyelenggaraan TI yang dimiliki oleh BPR atau BPR Syariah.

D. PENGENDALIAN INTERN DAN AUDIT INTERN TERHADAP AKTIVITAS YANG DISELENGGARAKAN OLEH PPJTI

Pihak yang melaksanakan fungsi audit intern BPR dan BPR Syariah harus memastikan pengendalian yang dioperasikan oleh PPJTI. BPR dan BPR Syariah harus memastikan bahwa perjanjian dengan PPJTI mencakup klausul menyediakan data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan oleh BPR atau BPR Syariah, Otoritas Jasa Keuangan, dan/atau pihak lain sesuai dengan kewenangannya dalam ketentuan peraturan perundang-undangan, sertamenyatakan tidak berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang sesuai dengan ketentuan peraturan perundang-perundangan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan.

BAB VIII
PENGGUNAAN PPJTI DALAM PENYELENGGARAAN TI

Dalam rangka meningkatkan efektivitas dan efisiensi untuk mencapai tujuan strategis, BPR dan BPR Syariahdapat melakukankerja samadengan PPJTI. Kerja sama tersebut menyebabkan BPR dan BPR Syariah memiliki ketergantungan terhadap jasa yang diberikan secara berkesinambungan dan/atau dalam periode tertentu.

Kerja sama dengan PPJTI dapat memengaruhi risiko BPR dan BPR Syariah antara lain risiko operasional, kepatuhan, dan reputasi. Risiko tersebut dapat disebabkan antara lain karena adanya kegagalan PPJTI dalam menyediakan jasa, pelanggaran terhadap pengamanan, atau ketidakmampuan untuk mematuhi ketentuan dan peraturan perundang-undangan. BPR dan BPR Syariah tetapdiwajibkan bertanggung jawab terhadap penyelenggaraan TI yang dilakukan bekerjasama dengan PPJTI.

A. PROSES PEMILIHAN PPJTI

1. Penetapan Kebutuhan

   Dalam hal BPR dan BPR Syariah akan melakukan kerja sama dengan PPJTI, BPR dan BPR Syariah perlu melakukan penetapan kebutuhan dengan mempertimbangkan paling sedikit:
   a. hasil identifikasi fungsi atau aktivitas spesifik yang penyelenggaraannya akan dilaksanakan oleh PPJTI;
   b. hasil penilaian terhadap risiko yang dapat timbul akibat kerja sama yang akan dilaksanakan;
   c. penetapan dasar yang akan digunakan untuk mengidentifikasi pengukuran pengendalian yang memadai; dan
   d. penetapan pengendalian yang akan diimplementasikan.

   Tahap penetapan kebutuhan tersebut harus menghasilkan suatu dokumen yang berisi secara rinci mengenai kebutuhan BPR atau BPR Syariah terhadap jasa yang akan disediakan oleh PPJTI. Isi dari dokumen tersebut paling sedikit:
   a. lingkup dan karakteristik dari layanan, teknologi yang digunakan, dan dukungan kepada nasabah;
   b. standar dan tingkat layanan meliputi ketersediaan dan kinerja, manajemen perubahan, kualitas layanan, keamanan, dan kelangsungan usaha;
   c. karakteristik minimal yang harus dipenuhi oleh PPJTI yang akan digunakan antara lain pengalaman, tata kelola, kondisi keuangan, dan referensi mengenai reputasi;
   d. kriteria pelaporan yang dilakukan oleh PPJTI, antara lain dalam hal terdapat insiden TI;
   e. persyaratan yang harus dipenuhi antara lain terkait dengan sistem, data, maupun pelatihan personel, pada saat BPR atau BPR Syariah melakukan transisi atau migrasi ke sistem yang disediakan oleh PPJTI;
   f. jangka waktu perjanjian kerja sama, penghentian, dan cakupan minimal dari perjanjian kerja sama; dan
   g. perlindungan perjanjian kerja sama seperti pembatasan kewajiban, ganti rugi, dan asuransi.

   Dalam hal penyelenggaraan TI dipertimbangkan untuk dilakukan oleh pihak terkait BPR atau BPR Syariah, Direksi BPR atau BPR Syariah harus memastikan bahwa persiapan dan proses pelaksanaan yang dilakukan tidak berbeda dalam hal penyelenggaraan TI dilakukan oleh pihak tidak terkait BPR atau BPR Syariah (*arm's length principle*).

2. Analisis Biaya dan Manfaat

   Analisis biaya dan manfaat dilakukan untuk memastikan manfaat yang diterima BPR dan BPR Syariah atas kerjasama dengan PPJTI sepadan dengan biaya yang akan dikeluarkan.

   BPR dan BPR Syariah harus melakukan analisis terhadap biaya langsung maupun tidak langsung dalam penawaran tertulis oleh PPJTI dengan spesifikasi sesuai kebutuhan, jenis layanan, hal-hal yang diperlukan dalam menentukan efektivitas biaya, jangka waktu penyelesaian, pengamanan dan kelangsungan bisnis, SLA, serta solusi untuk masalah yang dihadapi.

   Pada saat BPR dan BPR Syariah melakukan analisis penawaran tertulis yang diajukan, terdapat kemungkinan ditemukannya ketidaksesuaian dengan kebutuhan BPR atau BPR Syariah. Oleh karena itu, BPR dan BPR Syariah harus mengevaluasi perbedaan tersebut dan dampaknya terhadap sasaran dan jasa yang diharapkan BPR atau BPR Syariah.

   Dalam rangka mengoptimalkan proses analisis biaya dan manfaat, selain menggunakan harga perkiraan sendiri (*owners estimate*), BPR dan BPR Syariah dapat melakukan perbandingan biaya dan manfaat yang ditawarkan antara PPJTI. Selanjutnya apabila penawaran tertulis tersebut telah memenuhi kebutuhan atau sesuai spesifikasi kebutuhan yang telah dibuat BPR atau BPR Syariah, BPR dan BPR Syariah perlu melakukan negosiasi dengan PPJTIsebelum pembuatan perjanjian kerja sama.

3. Uji Tuntas (*Due Diligence*) terhadap PPJTI

   Uji tuntas terhadap PPJTI dilakukan dalam rangka mendapatkan keyakinan bahwa PPJTI mampu memenuhi kebutuhan BPR atau BPR Syariah. Untuk mendapatkan keyakinan dimaksud, BPR dan BPR Syariah dapat melakukan evaluasi dan menilai informasi yang terkait dengan PPJTI antara lainmeliputi:

   a. eksistensi dan riwayat PPJTI;
   b. kualifikasi, latar belakang, dan reputasi pemilik PPJTI;
   c. perusahaan lain yang menggunakan jasa yang sama dari PPJTIsebagai referensi;
   d. kondisi keuangan, antara lain melalui analisis atas laporan keuangan yang telah diaudit;
   e. kemampuan dan efektivitas pemberian jasa, termasuk dukungan purna jual;
   f. teknologi dan arsitektur sistem;
   g. lingkungan pengendalian intern, riwayat pengamanan, dan cakupan audit;
   h. kepatuhan terhadap peraturan perundang-undangan;
   i. kepercayaan dan keberhasilan dalam melakukan hubungan dengan sub kontraktor;
   j. asuransi dan jaminan pemeliharaan;
   k. kemampuan untuk menyediakan pemulihan bencanadan keberlangsungan usaha (*business continuity*);
   l. penerapan manajemen risiko; dan/atau
   m. laporan hasil audit pihak independen terhadap kecukupan penerapan keamanan TI.

   Uji tuntas terhadap PPJTI yang dilakukan BPR atauBPR Syariah selama proses pemilihan harus didokumentasikan dengan baik dan dilakukan secara berkala sebagai bagian dari proses pemantauan dan kontrol. Dalam melakukan uji tuntas secara berkala terhadap PPJTI sebaiknya BPR dan BPR Syariah memperhatikan perubahan

atau perkembangan yang ada selama kurun waktu sejak uji tuntas terakhir dengan menggunakan informasi terkini.

4. Penentuan PPJTI

   Dalam menentukan PPJTI yang dipilih untuk digunakan oleh BPR atau BPR Syariah dalam menyelenggarakan TI, BPR dan BPR Syariah dapat memperhatikan hal-hal sebagai berikut:

   a. evaluasi atas penerapan manajemen risiko PPJTI secara berkala untuk memastikan penggunaan PPJTI tidak mengurangi tanggung jawab BPR dan BPR Syariah dalam menerapkan manajemen risiko;
   b. laporan-laporan yang pernah dibuat yang mencerminkan kinerja PPJTI sebelumnya yang diperlukan untuk menilai kinerja PPJTI telah memadai;
   c. kemampuan menyediakan informasi yang mencerminkan kinerja PPJTI yang diperlukan untuk memantau bahwa kinerja PPJTI memadai;
   d. hasil analisis terhadap biaya dan manfaat dari setiap pilihan PPJTI yang akan dipilih dan analisis terhadap pemenuhan jangka waktu penggunaan jasa sesuai dengan rencana bisnis BPR atau BPR Syariah;
   e. penerapan prinsip pengendalian TI secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen terhadap PPJTI, termasuk pengamanan *logic* dan fisik;
   f. informasi dari berbagai sumber termasuk laporan tahunan PPJTI dalam rangka mengevaluasi keandalan, kinerja, reputasi, dan kelangsungan penyediaan layanan dari PPJTI;
   g. menyediakan data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan oleh BPR atau BPR Syariah, Otoritas Jasa Keuangan, dan/atau pihak lain sesuai dengan kewenangannya dalam ketentuan peraturan perundang-undangan; dan
   h. dokumen penyeleksian yang memuat pertimbangan mengenai penerapan "hubungan kerja sama secara wajar (*arm's length principle*)", dalam hal PPJTI merupakan pihak terkait BPR atau BPR Syariah.

B. PERJANJIAN KERJA SAMA DENGAN PPJTI

Perjanjian kerja sama penyelenggaraan TI dengan PPJTI memuat paling sedikit:

1. cakupan pekerjaan atau jasa;
2. hak dan kewajiban BPR atau BPR Syariah maupun PPJTI;
3. kualifikasi dan kompetensi sumber daya manusia PPJTI yang memadai;
4. jaminan bahwa PPJTI menerapkan prinsip pengendalian TI secara memadai yang dibuktikan, antara lain penyediaan informasi secara berkala terkait dengan hasil audit TI terhadap penyelenggaraan Pusat Data dan/atau Pusat Pemulihan Bencana oleh pihak independen kepada Otoritas Jasa Keuangan melalui BPR dan BPR Syariah;
5. penyediaan data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan oleh BPR atau BPR Syariah, Otoritas Jasa Keuangan, dan/atau pihak lain sesuai dengan kewenangannya dalam ketentuan peraturan perundang-undangan termasuk untuk memastikan keberlangsungan operasional BPR dan BPR Syariah;

6. pernyataan tidak keberatan dari PPJTI dalam hal Otoritas Jasa Keuangan atau pihak lain yang berwenang sesuai dengan ketentuan peraturan perundang-undangan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan;
7. jaminan dari PPJTI untuk pengamanan dan kerahasiaan data terutama rahasia bank dan data pribadi nasabah termasuk bahwa Sistem Elektronik hanya bisa diakses oleh pemilik data (BPR dan BPR Syariah) serta Sistem Elektronik tersebut tidak mengandung *back door* yang memungkinkan akses oleh pihak yang tidak berwenang ke dalam Sistem Elektronik dan data BPR atau BPR Syariah;
8. tanggung jawab terus menerus dari PPJTI untuk menjaga keamanan dan kerahasiaan data/informasi BPR atau BPR Syariah;
9. kewajiban PPJTI untuk melaporkan setiap kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI yang dapat atau telah mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelangsungan operasional BPR atau BPR Syariah;
10. kewajiban PPJTI untuk menyediakan Rencana Pemulihan Bencana yang teruji dan memadai;
11. mekanisme penghentian kerja sama (*exit clause*) antara BPR atau BPR Syariah dengan PPJTI;
12. persetujuan BPR atau BPR Syariah secara tertulis dalam hal PPJTI melakukan pengalihan sebagian kegiatan (subkontrak) kepada subkontraktor. Selain itu, subkontraktor harus mempunyai standar penyelenggaraan TI yang memadai;
13. kemungkinan menghentikan, mengubah, membuat perjanjian baru, atau mengambil alih kegiatan yang diselenggarakan oleh PPJTI, serta mengakhiri perjanjian sebelum jangka waktu berakhirnya perjanjian,termasuk dalam hal ini atas permintaan Otoritas Jasa Keuangan;
14. pemenuhan tingkat pelayanan sesuai dengan perjanjian tingkat layanan (*service level agreement*) antara BPR dan BPR Syariah dan PPJTI;
15. biaya dan jangka waktu perjanjian kerja sama;
16. batasan risiko yang ditanggung oleh BPR atau BPR Syariah dan PPJTI yang diakibatkan perubahan antara lain:
    a. ruang lingkup perjanjian kerja sama;
    b. ruang lingkup bisnis dan organisasi perusahaan PPJTI; dan
    c. aspek hukum antara lain regulasi, hak cipta, paten, dan *trade mark*;
17. larangan bagi PPJTI untuk menggunakan atau mengungkapkan informasi yang dimiliki BPR dan BPR Syariah tanpa persetujuan BPR atau BPR Syariah;
18. pernyataan bahwa PPJTI memberikan jaminan keandalan Sistem Elektronik, termasuk tidak menggunakan fitur Sistem Elektronik yang dapat mengakibatkan Sistem Elektronik tersebut tidak berfungsi dengan baik;
19. standar spesifikasi dan kinerja Sistem Elektronik paling sedikit:
    a. kinerja dan fungsional yang diharapkan dari Sistem Elektronik;
    b. persyaratan dan infrastruktur yang diperlukan untuk menjalankan Sistem Elektronik;
    c. identifikasi kebutuhan uji coba guna menentukan pemenuhan standar kinerja Sistem Elektronik; dan

d. tindakan yang harus dilakukan PPJTI apabila Sistem Elektronik gagal pada saat uji coba.

20. kesediaan PPJTI untuk memberikan dokumen teknis kepada BPR atau BPR Syariah terkait dengan jasa yang dikerjakan oleh PPJTI antara lain, petunjuk pelaksanaan (*manual book*), dan aplikasi *online help* pada Sistem Elektronik yang bekerja secara interaktif;
21. kesediaan PPJTI membantu proses konversi perangkat lunak termasuk data dan format data pada saat penggantian sistem diperlukan di masa mendatang;
22. jaminan PPJTI bahwa Sistem Elektronik paling sedikit:
    a. tidak melanggar hak kekayaan intelektual dari pihak lain;
    b. tidak mengandung kode rahasia atau pembatasan secara otomatis yang tidak diungkapkan pada perjanjian;
    c. bekerja sesuai dengan spesifikasi dan PPJTI bertanggung jawab dalam hal terjadi permasalahan; dan
    d. dijamin pemeliharaannya oleh PPJTI selama jangka waktu perjanjian.
23. SLA yang memuat standar kinerja dari PPJTI antara lain mengenai tingkat pelayanan yang diperjanjikan (*service levels*) dan target kinerja;
24. klausula bahwa SLA tetap berlaku dalam hal terjadi perubahan kepemilikan pada PPJTI;
25. laporan hasil pemantauan kinerja PPJTI yang terkait dengan SLA;
26. kesediaan PPJTI tidak memodifikasi Sistem Elektronik yang telah disepakati dalam perjanjian tanpa persetujuan dari kedua belah pihak;
27. khusus untuk penyelenggaraan Pusat Data dan Pusat Pemulihan Bencana, PPJTI harus menyediakan informasi kepada BPR dan BPR Syariah laporan keuangan terkini yang telah diaudit setiap tahun.
28. Keharusan PPJTI untuk melakukan *transfer of knowledge* kepada BPR atau BPR Syariah dengan merencanakan pelatihan terhadap sumber daya manusia BPR atau BPR Syariah, antara lain mengenai jumlah sumber daya manusia yang dilatih, bentuk pelatihan, dan biaya yang diperlukan, yang bertujuan agar sumber daya manusia BPR atau BPR Syariah memahami TI yang digunakan terutama alur proses TI dan struktur Pangkalan Data dari Sistem Elektronik yang disediakan olehPPJTI tersebut;
29. sanksi dan/atau penalti terhadap pembatalan dan/atau pelanggaran perjanjian kerja sama;
30. kepatuhan pada ketentuan dan peraturan perundang-undangan termasuk penyelesaian sengketa dalam hal terjadi perselisihan;
31. kepemilikan dan hak cipta (*license*);
32. jaminan bahwa PPJTI tetap mendukung jasa yang diberikan kepada BPR atau BPR Syariah selama jangka waktu tertentu setelah implementasi;
33. ketersediaan sarana komunikasi *online*, pengamanan terhadap akses dan transmisi data dari dan ke Pusat Data serta Pusat Pemulihan Bencana, dan penyelenggaraan TI lainnya sesuai dengan ketentuan peraturan perundang-undangan;
34. pengaturan yang jelas mengenai rekam cadang, *contingency*, *record protection* termasuk perangkat keras, perangkat lunak, dan *data files*, untuk menjamin kelangsungan penyelenggaraan TI;
35. pengaturan mengenai pengamanan dalam pengiriman dokumen yang diperlukan dari dan ke Pusat Data serta Pusat Pemulihan Bencana, dan penyelenggaraan TI lainnya sesuai dengan ketentuan

peraturan perundang-undangan. Pihak yang bertanggung jawab sebaiknya dilindungi asuransi yang cukup;

36. tanggung jawab PPJTI dalam menyediakan tenaga ahli yang memadai sesuai dengan keperluan penyelenggaraan TI;
37. standar pengamanan sistem yang harus dipenuhi oleh PPJTI;
38. standar laporan pemantauan kinerja PPJTI;
39. standar perjanjian penyimpanan dokumen (*escrow agreement*);
40. aspek ketahanan dan keamanan siber; dan
41. tanggung jawab PPJTI atas kerugian yang dialami BPR dan BPR Syariah yang disebabkan oleh ketidakpatuhan terhadap perjanjian kerja sama dan/atau kelalaian PPJTI.

C. TINDAK LANJUT ATAS REALISASI PERJANJIAN KERJA SAMA DENGAN PPJTI

1. Antisipasi Risiko

   Dalam hal kerja sama dengan PPJTI telah direalisasikan, BPR dan BPR Syariah harus mengantisipasi risiko dari penyelenggaraan TI yang diserahkan kepada PPJTI. Dalam rangka mengantisipasi risiko tersebut, BPR dan BPR Syariah melakukan pemantauan untuk mengetahui secara dini apabila terdapat kondisi sebagai berikut:

   a. memburuknya kinerja penyelenggaraan TI oleh PPJTI yang berpotensi menimbulkan dan/atau mengakibatkan dampak yang signifikan pada kegiatan usaha dan/atau operasional BPR dan BPR Syariah;
   b. PPJTI mengalami kesulitan keuangan yang menyebabkan insolven, dalam proses menuju likuidasi, atau dipailitkan berdasarkan putusan pengadilan;
   c. terdapat pelanggaran oleh PPJTI terhadap ketentuan peraturan perundang-undangan;
   d. terdapat kondisi yang menyebabkan BPR atau BPR Syariah tidak dapat menyediakan data dan informasi yang diperlukan dalam rangka pengawasan oleh Otoritas Jasa Keuangan; dan/atau
   e. terdapat kondisi lain yang menyebabkan terganggunya atau terhentinya penyediaan jasa TI dari PPJTI kepada BPR dan BPR Syariah.

2. Tindak Lanjut Risiko

   Dalam hal BPR dan BPR Syariah menemukan kondisi sebagaimana dimaksud pada angka 1. diatas, BPR dan BPR Syariah wajib melakukan tindakan tertentu paling sedikit:

   a. melaporkan kepada Otoritas Jasa Keuangan paling lambat 3 (tiga) hari kerja setelah kondisi tersebut di atas diketahui oleh BPR atauBPR Syariah;
   b. memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian kerja sama dengan PPJTI apabila diperlukan; dan
   c. melaporkan kepada Otoritas Jasa Keuangan mengenai keputusan tindak lanjut yang telah dan/atau akan diambil, paling lambat 10 (sepuluh) hari kerja setelah tanggal laporan kondisi sebagaimana dimaksud dalam huruf a.

3. Rencana Darurat

   Dalam hal dilakukan penghentian kerja sama sebagaimana dimaksud pada angka 2 huruf b atau atas perintah Otoritas Jasa Keuangan sebelum berakhirnya jangka waktu perjanjian kerja sama, BPR dan BPR Syariah harus memiliki rencana darurat

(*contingency plan*) dalam rangka menjaga kelangsungan usaha BPR atau BPR Syariah.

4. Rencana Pemulihan Bencana
   BPR dan BPR Syariah harus memastikan bahwa ketergantungan pada PPJTI dapat dimitigasi sehingga BPR dan BPR Syariah tetap mampu menyelenggarakan TI dalam hal terjadi bencana, dengan cara:
   a. memastikan bahwa PPJTI memiliki Rencana Pemulihan Bencana sesuai dengan jenis, cakupan, dan kompleksitas aktivitas/jasa TI yang diberikan; dan
   b. secara aktif mendapatkan jaminan kesiapan Rencana Pemulihan Bencana milik PPJTI seperti pengujian secara berkala atas Rencana Pemulihan Bencana.
5. Jaminan Keberlangsungan Penyelenggaraan TI
   Dalam hal BPR dan BPR Syariah membeli sistem dari PPJTI dan menjaga keberlangsungan penyelenggaraan TI, BPR dan BPR Syariah perlu melakukan mitigasi terhadap ketergantungan pada PPJTI, antara lain:
   a. memperhatikan ketersediaan kode sumber oleh PPJTI pada saat diperlukan, dengan cara:
      1) menyerahkan kode sumber kepada BPR atau BPR Syariah; atau
      2) dalam hal PPJTI tidak menyerahkan kode sumber kepada BPR atau BPR Syariah, PPJTI menempatkan kode sumber pada pihak ketiga yang terpercaya yang dapat menjamin penyerahan kode sumber kepada BPR atau BPR Syariah.
   b. PPJTI harus memberikan jaminan kepada BPR dan BPR Syariah bahwa kelangsungan aplikasi didukung oleh *principal* pengembang perangkat lunak, dalam hal kode sumber tidak dimiliki oleh PPJTI.

Glosarium

1. **Akses (*Access*):**
   kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiriatau dalam jaringan

2. ***Administrator Log*:**
   file di komputer yang menyimpan informasi mengenai kegiatan administrator.

3. ***Arm's Length Principle*:**
   suatu prinsip kerjasama yang wajar dan saling menguntungkan dimana masing-masing pihak yang akan membuat perjanjian kerjasama memiliki daya tawar *(bargaining power)* yang sama walaupun pihak penyedia jasa merupakan pihak terkait.

4. ***Automated Teller Machine* (ATM):**
   suatu terminal/mesin komputer yang digunakan oleh BPR atau BPR Syariah yang dihubungkan dengan komputer lainnya melalui komunikasi data yang memungkinkan nasabah menyimpan dan mengambil uang di BPR atau BPR Syariah atau melakukan transaksi perbankan lainnya.

5. **Rekam Jejak Audit (*Audit Trail*):**
   file di komputer yang menyimpan informasi mengenai kegiatanpengguna atau komputer yang tersimpan secara kronologis, yang dapat digunakan untuk audit atau penelusuran.

6. ***Authentication*:**
   kemampuan dari setiap pihak dalam transaksi untuk menguji kebenaran dari pihak lain.

7. ***Back Door*:**
   metode untuk melewati otentikasi normal atau *remote access* yang aman dari suatu komputer terhadap pengaksesan suatu sistem namun tidak teridentifikasi melalui pemeriksaan biasa.

8. **Rekam Cadang (*Back Up*):**
   salinan dari dokumen asli atau cadangan dari mesin utama yang dapat digunakan apabila terjadi gangguan pada mesin utama. Rekam cadang dapat berupa rekam cadang data maupun rekam cadang *system*. Rekam cadang dapat ditempatkan secara *on site* di lokasi Pusat Data dan atau *off site* di lokasi alternatif.

9. ***Biometric Device:***
   perangkat atau sistem teknologi pengamanan informasi yang menggunakan bagian tubuh sebagai identitas dan otentikasi.

10. ***Business Continuity Management* (BCM):**
    proses manajemen terpadu dan menyeluruh untuk menjamin kegiatan operasional BPR dan BPR Syariah tetap dapat berfungsi walaupun terdapat gangguan/bencana guna melindungi kepentingan para pemangku kepentingan.

11. ***Business Continuity Plan*** **(BCP):**
suatu rangkaian proses yang dilakukan untuk memastikan terus berlangsungnya kegiatan dalam kondisi mendapatkan gangguan atau bencana.

12. ***Cost and Benefit Analysis*** **(Analisa Biaya dan Manfaat):**
suatu analisis perbandingan antara biaya investasi dan keuntungan yang diperoleh BPR atau BPR Syariah dari setiap alternatif pilihan penyedia jasa. Hasil analisis ini menjadi salah satu pertimbangan BPR atau BPR Syariah untuk mengambil keputusan outsourcing atau pemilihan penyedia jasa.

13. ***Pangkalan Data (Database)*****:**
sekumpulan data komprehensif dan disusun secara sistematis, dapat diakses oleh pengguna sesuai wewenang masing-masing, dan dikelola oleh administrator Pangkalan Data (*Database administrator*).

14. **Pusat Data (*Data Center*):**
suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

15. ***Denial of Service*** **(DoS):**
serangan terhadap sistem TI sehingga menjadi lambat atau tidak dapat berfungsi sama sekali misalnya dengan membuat kapasitas (*bandwidth*) jaringan atau kapasitas (*disk space*) komputer seolah-olah telah terpakai penuh, ganggguan pada peladenserta gangguan penyediaan jasa kepada sistem lain atau pengguna.

16. **Tanda Tangan Elektronik *(Digital signatures)*:**
tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

17. **Rencana Pemulihan Bencana (*Disaster Recovery Plan*):**
dokumen yang berisikan rencana dan langkah-langkah memulihkan kembali akses data, perangkat keras dan perangkat lunak yang diperlukan, agar BPR dan BPR Syariah dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana.

18. **Pusat Pemulihan Bencana(*Disaster Recovery Center*):**
suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting Sistem Elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia.

19. ***Downtime*****:**
lamanya sistem tidak dapat berfungsi dan digunakan oleh pengguna karena adanya gangguan *hardware, software* dan komunikasi.

20. **Enkripsi:**
alat untuk mencapai keamanan data dengan menerjemahkannya dengan menggunakan sebuat key (*password*). Enkripsi mencegah *password* atau *key* supaya tidak mudah dibaca pada file konfigurasi.

21. *Exception Handling*:
mekanisme untuk menangani munculnya kondisi yang tidak diharapkan yang dapat mengubah alur normal suatu sstem aplikasi.

22. *Firewall*:
peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian atas lalu lintas data/informasi melalui jaringan serta memisahkan jaringan privat dan publik.
Peralatan ini dapat digunakan untuk melindungi komputer yang telah dikoneksikan dengan jaringan dari serangan yang dapat mengkompromikan komputer internal yang dapat menyebabkan *data corruption* dan atau *Denial of Service* bagi pengguna yang diotorisasikan.

23. *Gateway*:
titik dalam suatu jaringan yang berfungsi sebagai pintu masuk ke jaringan lain atau menghubungkan satu jaringan dengan jaringan lain. *Gateway* dapat berupa komputer yang mengatur dan mengendalikan lalu lintas jaringan.

24. *Hardcopy*:
salinan data/informasi komputer dalam bentuk tercetak atau dikenal dengan *printout*.

25. *Hardening*:
merupakan proses/metode untuk mengamankan sistem dari berbagai ancaman atau gangguan. Metode yang digunakan termasuk antara lain menonaktifkan layanan yang tidak diperlukan, serta *username* atau *login* yang tidak diperlukan, mengembangkan *intrusion detection system, intrusion prevention system, firewall.*

26. *Hash Function*:
suatu cara untuk mengubah data (biasanya berbentuk pesan atau file) menjadi suatu angka tertentu yang dapat digunakan oleh komputer untuk menghasilkan data asalnya kembali.

27. *Hub*:
peralatan yang menghubungkan beberapa kabel pada jaringan dan meneruskan data/informasi ke seluruh *address* yang berupa titik jaringan atau peralatan yang dituju.

28. *Interoperability*:
a. kemampuan perangkat lunak atau perangkat keras pada berbagai jenis mesin dari banyak vendor untuk saling berkomunikasi.
b. kemampuan untuk saling bertukar dan menggunakan informasi (biasanya dalam suatu jaringan besar yang terdiri beberapa jaringan lokal yang bervariasi).

29. *System Integration Testing*:
pengujian terhadap keseluruhan fungsional terhadap Sistem setelah diintegrasikan menjadi satu kesatuan yang utuh.

30. *Library*:
kumpulan perangkat lunak atau data yang memiliki fungsi tertentu dan disimpan serta siap untuk digunakan.

31. *Logic Bomb*:
suatu kode yang sengaja dimasukkan di dalam suatu sistem perangkat lunak yang pada suatu kondisi tertentu akan melakukan serangkaian fungsi yang bersifat merusak.

32. *Mobile Banking*:
layanan yang memungkinkan nasabah BPR atau BPR Syariah melakukan transaksi perbankan melalui *handphone*. *Mobile banking* umumnya dilakukan melalui sms atau *mobile internet* namun dapat juga menggunakan program khusus yang di unduh melalui *handphone*.

33. Nirsangkal (*Non-repudiation*):
suatu cara untuk memastikan kebenaran pengirim dan penerima sehingga tidak ada pihak yang dapat menyangkal.

34. *Offline*:
sistem atau komputer yang tidak terdapat hubungan jaringan atau tidak dapat berkomunikasi dengan sistem atau komputer lain.

35. Alih Daya (*Outsourcing*):
penggunaan pihak lain (ekstern) dalam penyelenggaraan TI BPR atau BPR Syariah yang menyebabkan BPR atau BPR Syariah memiliki ketergantungan terhadap jasa yang diberikan pihak lain tersebut secara berkesinambungan dan atau dalam periode tertentu.

36. *Parallel Run*:
merupakan salah satu strategi implementasi sistem di mana kedua sistem lama dan baru berjalan berdampingan sampai pengguna yakin bahwa sistem baru tidak memiliki masalah. Setelah periode waktu ketika sistem baru terbukti bekerja dengan benar, sistem lama akan dihapus sepenuhnya dan pengguna akan tergantung hanya pada sistem baru.

37. *Password*:
angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya, yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.

38. *Patch*:
sekumpulan kode yang ditambahkan pada perangkat lunak untuk memperbaiki suatu kesalahan, biasanya merupakan koreksi yang bersifat sementara di antara dua keluaran versi perangkat lunak.

39. *Patch Management*:
manajemen sistem yang meliputi proses memperoleh, pengujian dan instalasi berbagai *patch* yang digunakan untuk memperbaiki suatu program.

40. Pengamanan Fisik:
suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap area komputerisasi serta peralatan/fasilitas pendukung.

41. Pengamanan *Logic*:
suatu sistem pengamanan untuk mencegah akses oleh pihak-pihak yang tidak berwenang terhadap sistem komputer dan informasi yang tersimpan di dalamnya yang meliputi penggunaan *user ID, password*, dan sebagainya.

42. *Personal Identification Number* (PIN):
rangkaian digit unik terdiri dari huruf, angka atau kode ASCII yang digunakan untuk mengidentifikasi pengguna komputer, pengguna ATM, *internet banking, mobile banking,* dan lain-lain.

43. *Platform*:
perangkat keras atau lunak seperti arsitektur komputer, sistem operasi atau bahasa pemrograman yang memungkinkan suatu aplikasi beroperasi.

44. *Super User*:
user id yang memiliki kewenangan sangat luas.

45. *Public Key Infrastructure*:
suatu pengolahan/pengaturan dimana suatu pihak ketiga yang dapat dipercayamenyediakanpemeriksaan secara seksama dan memastikan keabsahan suatu identitas.

46. *Quality Assurance*:
aktivitas yang memastikan produk atau jasa memenuhi standar yang ditetapkan termasuk keandalan, kegunaan, kinerja dan standar kualitas umum yang ditetapkan oleh perusahaan.

47. *Restore*:
mengembalikan pada fungsi atau kondisi semula sebelum terjadi *disaster*.

48. *Restricted Area*:
area yang hanya dapat dimasuki oleh orang yang telah mendapatkan hak akses.

49. *Router*:
peralatan jaringan yang meneruskan suatu paket data/informasi dan memilih rute terbaik untuk ditempuh untuk menyampaikan data/informasi tersebut.

50. *Service Level Agreement*:
bagiandari kontrak perjanjian dimana tingkat penyediaan layanan yang diharapkan para pihak ditetapkan biasanya mencakup pula standar kinerja seperti tingkat pelayanan yang diperjanjikan (*service levels)* atau target waktu penyediaan layanan.

51. *Softcopy*:
salinan data atau dokumen dalam bentuk *file* elektronik.

52. Kode Sumber(*Source Code*):
suatu rangkaian perintah, pernyataan, dan/atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang dapat dibaca dan dipahami orang.

53. *Spoofing*:
suatu keadaan dimana seseorang atau suatu program dapat menyerupai orang lain atau program lain dengan cara memalsukan data dengan tujuan untuk mendapatkan keuntungan-keuntungan tertentu.

54. *Spyware*:
perangkat lunak yang mengumpulkan informasi-informasi sensitif tentang pengguna tanpa sepengetahuan atau izin dari pengguna.

55. *Stress Testing*:
uji ketahanan terhadap kemampuan Sistem Elektronik atau Aplikasi Inti Perbankan dalam menangani proses atau transaksi dalam skala/jumlah yang besar.

56. *Switch*:
peralatan dalam jaringan yang meneruskan paket informasi kepada *address* atau peralatan yang dituju.

57. *System*:
suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran tertentu.

58. *System Development Life Cycle (SDLC)*:
siklus pengembangan sistem yang meliputi langkah-langkah paling sedikit sebagai berikut: (1) *system planning*, (2) *system analysis*, (3) *system design*, (4) *system selection*, (5*) system implementation*, (6) *system maintenance*, dan *(7) system disposal*.

59. *System Log*:
file di komputer yang menyimpan informasi mengenai kegiatan sistem atau komputer.

60. *Testing*:
uji coba yang dilakukan *quality assurance* untuk menguji fungsionalitas keseluruhan sistem aplikasi, termasuk tiap objek yang terdapat dalam sistem aplikasi tersebut.

61. *Trojan Horse*:
program yang bersifat merusak yang disusupkan oleh peretas (*hacker*) di dalam program yang sudah dikenal oleh pengguna replikasi atau distribusinya harus diaktivasi oleh program yang sudah dikenal oleh penggunanya melalui metode "*social engineering*".

62. *Unit Testing*:
uji coba atas fungsional setiap unit atau sub modul dari sistem yang telah selesai dikembangkan.

63. *Uninterruptible Power Supply* (UPS):
perangkat yang mempunyai fungsi utama sebagai penyedia listrik cadangan dengan jangka waktu tertentu bagi perangkat elektronik yang terpasang.

64. *Upload* dan *Download*:
transfer data elektronik antara dua komputer atau sistem yang sejenis.

65. *User Acceptance Test*:
uji coba akhir yang dilakukan oleh pengguna akhir terhadap Sistem yang telah selesai dikembangkan dalam rangka menguji fungsionalitas keseluruhan sistem apakah telah sesuai dengan kebutuhan pengguna pada tahapan pendefinisian kebutuhan pengguna sebelum memutuskan implementasi dapat dilakukan.

66. *User Log*:
file di komputer yang menyimpan informasi mengenai kegiatan user seperti waktu *login* dan *logout*.

67. Virus:
program yang bersifat merusak dan akan aktif dengan bantuan orang (dieksekusi), dan tidak dapat mereplikasi sendiri, penyebarannya karena dilakukan oleh orang, seperti *copy*, biasanya melalui *attachment* surat elektronik, *game*, program bajakan, dan lain-lain.

68. *War Driving*:
suatu tindakan untuk mendapatkan jaringan wi-fi (*wireless local area network*) dengan menggunakan perangkat yang dapat mendeteksi adanya jaringan wi-fi, seperti laptop atau *smartphone*.

69. *Worm*:
program komputer yang dirancang untuk memperbanyak diri secara otomatis dengan melekat pada surat elektronik atau sebagai bagian dari pesan jaringan. *Worm* menyerang jaringan dan berakibat kepada penuhnya *bandwith* yang terpakai sehingga menghambat laju pengiriman data pada jaringan.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN III
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 43/PADK.03/2025
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH
BANK PEREKONOMIAN RAKYAT DAN
BANK PEREKONOMIAN RAKYAT SYARIAH

MANAJEMEN RISIKO PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH

DAFTAR ISI

BAB I
MANAJEMEN RISIKO PENERAPAN TATA KELOLA TI

A. KEBIJAKAN, STANDAR, DAN PROSEDUR MANAJEMEN TI

Berdasarkan Pasal 14 POJK PTI BPR dan BPR Syariah, BPR dan BPR Syariah wajib menerapkan manajemen risiko secara efektif dalam penyelenggaraan TI. Dalam penerapan manajemen risiko, diperlukan kecukupan kebijakan, standar, dan prosedur penggunaan TI.

1. Kebijakan
   Kebijakan adalah ketentuan atau prinsip yang menggambarkan tekad, komitmen, atau rencana manajemen terhadap suatu masalah tertentu yang dinyatakan secara formal oleh manajemen dan menjadi landasan kerja organisasi.
   Contoh: kebijakan manajemen risiko TI, kebijakan keamanan informasi, dan kebijakan pengelolaan SDM TI.
2. Standar
   Standar adalah ketentuan teknis atau kriteria minimum yang harus dipenuhi untuk mendukung pelaksanaan kebijakan dan prosedur secara konsisten, aman, dan sesuai tujuan.
   Contoh: standar *hardening* OS *Windows*.
3. Prosedur
   Prosedur adalah urutan kegiatan dari suatu proses penyelenggaraan TI yang melibatkan satu atau beberapa unit kerja TI dalam BPR.
   Contoh: prosedur pengadaan TI, prosedur rekam cadang akhir hari, dan prosedur audit internal.

B. PROSES MANAJEMEN RISIKO TI

1. Identifikasi Jenis Risiko terkait Manajemen TI
   Dalam melakukan identifikasi dan penilaian risiko TI, BPR dan BPR Syariah terlebih dahulu harus memastikan adanya *risk awareness* di seluruh lini, yaitu:
   a. *risk awareness* dari Direksi dan pejabat eksekutif;
   b. pemahaman yang jelas mengenai *risk appetite* dari BPR dan BPR Syariah;
   c. pemahaman terhadap ketentuan peraturan perundang-undangan terkait TI; dan
   d. transparansi dan integrasi tanggung jawab mengenai risiko yang signifikan dari setiap aspek terkait penyelenggaraan TI.

   Untuk dapat memastikan hal tersebut, BPR dan BPR Syariah dapat menjalankan *risk awareness* program bagi seluruh pegawai dan pengurus BPR dan BPR Syariah atau menjalankan metode lain yang dapat meningkatkan kesadaran para pengguna TI akan risiko yang ada.
2. Risiko terkait TI
   BPR dan BPR Syariah harus memiliki pendekatan manajemen risiko dengan melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko secara efektif. Risiko terkait penyelenggaraan TI harus dikaji ulang bersamaan dengan risiko lainnya yang dimiliki BPR dan BPR Syariah untuk menentukan profil risiko BPR dan BPR Syariah secara keseluruhan.
3. Penilaian Risiko TI
   Penilaian risiko TI oleh BPR dan BPR Syariah perlu dilakukan secara berkesinambungan sebagai suatu siklus dan paling sedikit mencakup 4 (empat) langkah penting sebagai berikut:

a. Pengumpulan data atau dokumen atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko, baik dari kegiatan yang sedang maupun yang akan berjalan, antara lain:
   1) aset TI yang kritikal, dalam rangka mengidentifikasi titik-titik akses dan penyimpangan terhadap informasi nasabah yang bersifat rahasia;
   2) hasil kaji ulang rencana strategis bisnis, khususnya kaji ulang terhadap penilaian risiko potensial;
   3) hasil uji tuntas (*due diligence*) dan pemantauan terhadap kinerja PPJTI;
   4) hasil kaji ulang atas laporan atau keluhan yang disampaikan oleh nasabah dan/atau pengguna TI ke *call center* dan/atau *help desk*;
   5) hasil *self-assessment* yang dilakukan seluruh satuan kerja terhadap pengendalian yang dilakukan terkait TI; dan
   6) temuan audit terkait penyelenggaraan dan penggunaan TI.

b. Analisis risiko berkaitan dengan dampak potensial dari setiap risiko, seperti *fraud* pada pemrograman, virus komputer, kegagalan sistem, bencana alam, dan kesalahan pemilihan teknologi yang digunakan;

c. Penetapan prioritas pengendalian dan langkah mitigasi yang didasarkan pada hasil penilaian risiko BPR dan BPR Syariah secara keseluruhan; dan

d. Pemantauan kegiatan pengendalian dan mitigasi yang telah dilakukan atas risiko yang diidentifikasi dalam periode penilaian risiko sebelumnya, yang antara lain mencakup rencana tindak lanjut perbaikan, kejelasan akuntabilitas dan tanggung jawab, sistem pelaporan, serta pengendalian kualitas termasuk bentuk pengawasan lain atau *compensating controls*.

4. Pengukuran Risiko terkait TI

BPR dan BPR Syariah perlu memperhatikan signifikansi dampak risiko yang telah diidentifikasi terhadap kondisi BPR dan BPR Syariah dan frekuensi terjadinya risiko. Metode yang digunakan BPR dan BPR Syariah dapat berupa metode kuantitatif maupun kualitatif tergantung kompleksitas usaha dan TI yang digunakan. Dalam metode kualitatif, besarnya dampak dan kemungkinan keterjadian (*likelihood*) dapat dijelaskan secara naratif atau dengan pemberian peringkat.

Contoh metode kualitatif pengukuran yang sederhana berupa penggunaan *check list* atau *subjective risk rating* seperti *High*, *Medium*, atau *Low*.

Agar risiko yang telah diidentifikasi dan dinilai atau diukur dapat dipantau maka BPR dan BPR Syariah perlu memiliki dokumentasi risiko atau yang sering disebut sebagai *risk register*.

Contoh pembuatan *risk register* paling sedikit mencakup:

a. penetapan aset, proses, produk, atau kejadian yang mengandung risiko;

b. pengukuran atau pemeringkatan kemungkinan kejadian dan dampak (*inherent risk assessment*);

c. langkah-langkah penanganan terhadap risiko potensial (*potential risk treatment*), misalnya *Accept*, *Control*, *Avoid*, atau *Transfer* (ACAT).

Dalam dokumentasi penanganan terhadap risiko potensial (*potential risk treatment*), BPR dan BPR Syariah perlu memperhatikan antara lain *risk appetite*, fasilitas yang dapat digunakan sebagai *preventive control* atau *corrective control*, dan kesesuaian rencana mitigasi risiko dengan kondisi keuangan BPR dan BPR Syariah. Dokumentasi penanganan terhadap risiko potensial perlu dikinikan secara berkala.

Langkah-langkah penanganan risiko potensial yang dapat diambil BPR dan BPR Syariah sebagai berikut:

1) *Accept*: BPR dan BPR Syariah memutuskan untuk menerima risiko apabila besarnya dampak dan tingkat kecenderungan masih dalam batas toleransi organisasi.
   Contoh:
   a) Penetapan kriteria penerimaan risiko terkait dengan evaluasi dan penanganan risiko misalnya nilai risiko akhir "*Low*".
   b) Penetapan nilai risiko akhir "*Medium*" atau "*High*", namun telah diputuskan untuk diterima oleh BPR dan BPR Syariah dan dibuat suatu sistem prosedur untuk memantau risiko tersebut, misalnya dengan menyediakan tambahan modal sesuai besarnya potensi risiko.
2) *Control*: BPR dan BPR Syariah memutuskan mengurangi dampak maupun kemungkinan terjadinya risiko.
   Contoh: pemasangan *firewall* pada *Personal Computer* (PC) untuk mencegah akses yang tidak terotorisasi.
3) *Avoid*: BPR dan BPR Syariah memutuskan untuk tidak melakukan suatu aktivitas atau memilih alternatif aktivitas lain yang menghasilkan *output* yang sama untuk menghindari terjadinya risiko.
   Contoh: pengguna tidak diberikan hak *privilege* sebagai administrator untuk menghindari risiko TI berupa *malicious code* pada PC akibat dari perubahan konfigurasi dan pemasangan perangkat lunak pada PC yang dilakukan oleh pengguna.
4) *Transfer*: BPR dan BPR Syariah memutuskan untuk mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.
   Contoh: mengasuransikan fasilitas ruangan atau gedung yang mengandung risiko terjadi kebakaran; dan

d. pengukuran atau pemeringkatan kemungkinan kejadian dan dampak setelah ACAT (*residual risk assessment*).

5. Pemantauan Risiko terkait TI

BPR dan BPR Syariah melakukan pemantauan risiko TI dengan mengevaluasi kesesuaian, kecukupan, dan efektivitas kinerja penyelenggaraan TI.

a. Hal-hal yang dapat menjadi cakupan dalam evaluasi antara lain:
   1) hasil audit dan kajian terkait;
   2) umpan balik (*feedback*) yang diterima;
   3) kebijakan, standar, dan prosedur serta penerapannya;
   4) status dari tindakan preventif maupun korektif terkait risiko yang dihadapi BPR dan BPR Syariah;
   5) kelemahan dan ancaman baik yang telah ada maupun yang masih berupa potensi;
   6) hasil pengukuran atas efektivitas penyelenggaraan TI;

7) tindak lanjut atas hasil evaluasi sebelumnya;
8) perubahan kondisi yang mempengaruhi penyelenggaraan TI; dan
9) rekomendasi untuk perbaikan atau penyempurnaan.

b. Tindak lanjut atas hasil evaluasi dapat dituangkan dalam bentuk keputusan maupun tindakan untuk meningkatkan efektivitas penyelenggaraan TI, antara lain:
1) penginian profil risiko, pengukuran risiko, dan rencana penanganan risiko;
2) penyempurnaan kebijakan, standar, dan prosedur di bidang TI;
3) pemenuhan kebutuhan SDM;
4) penetapan dan pelaksanaan tindakan preventif dan korektif berdasarkan *assessment* atas ketidaksesuaian yang ada maupun yang masih bersifat potensi, dengan mempertimbangkan skala prioritas; dan
5) pemantauan dan evaluasi atas pelaksanaan tindakan preventif dan korektif.

c. Hasil evaluasi dan tindak lanjut sebagaimana dimaksud dalam huruf b didokumentasikan secara memadai.

6. Pengendalian Risiko terkait TI

BPR dan BPR Syariah menerapkan praktik-praktik pengendalian yang memadai, sebagai bagian dari strategi mitigasi risiko TI secara keseluruhan dengan memperhatikan paling sedikit:

a. hasil penilaian risiko;
b. kriteria penanganan risiko dan rekomendasi bentuk penanganan risiko;
c. ketentuan peraturan perundang-undangan dan persyaratan hukum atau kontrak lainnya;
d. praktik-praktik pengendalian antara lain:
1) penerapan kebijakan, standar, dan prosedur, serta struktur organisasi termasuk alur kerjanya;
2) pengendalian intern yang efektif yang dapat memitigasi risiko dalam proses TI. Cakupan dan kualitas pengendalian intern adalah kunci utama dalam proses manajemen risiko sehingga BPR dan BPR Syariah harus mengidentifikasi persyaratan spesifik pengendalian intern yang diperlukan dalam setiap kebijakan dan prosedur yang diterapkan;
3) penetapan kebijakan, standar, dan prosedur sistem pengelolaan pengamanan informasi yang diperlukan BPR dan BPR Syariah untuk melakukan pengamanan aset-aset terkait penyelenggaraan dan penggunaan TI termasuk data atau informasi;
4) evaluasi hasil kaji ulang dan pengujian atas Rencana Pemulihan Bencana (*Disaster Recovery Plan*/DRP) untuk setiap bagian operasional yang kritis;
5) penetapan kebijakan dan prosedur mengenai penggunaan PPJTI. Direksi harus memiliki pemahaman secara menyeluruh atas risiko yang berhubungan dengan penggunaan jasa PPJTI untuk sebagian atau semua operasional TI;
6) evaluasi kemampuan PPJTI untuk menjaga tingkat keamanan paling sedikit sama atau lebih ketat dari yang diterapkan oleh pihak intern BPR dan BPR Syariah baik

dari sisi kerahasiaan, integritas data, dan ketersediaan informasi. Pengawasan dan pemantauan yang ketat harus dilakukan karena tanggung jawab BPR dan BPR Syariah tidak hilang atau menjadi berkurang dengan melakukan alih daya (*outsourcing*) operasional TI kepada PPJTI; dan

7) pemakaian asuransi sebagai upaya untuk melengkapi mitigasi potensi kerugian dalam penyelenggaraan TI. Risiko yang perlu diasuransikan adalah *residual risk*. BPR dan BPR Syariah dapat melakukan kaji ulang sesuai kebutuhan, cakupan, dan nilai asuransi yang ditutup.

BAB II
MANAJEMEN RISIKO PENGEMBANGAN DAN PENGADAAN SISTEM ELEKTRONIK

Manajemen risiko pengembangan dan pengadaan TI harus memperhatikan:

1. Identifikasi risiko terkait pengembangan dan pengadaan

   Dalam melakukan identifikasi risiko terkait Pengembangan dan Pengadaan Sistem Elektronik, BPR dan BPR Syariah menginventarisasi, antara lain:

   a. kebutuhan pengguna untuk menghasilkan solusi yang tepat guna;
   b. pemilihan PPJTI yang sesuai kemampuan yang diperlukan;
   c. kompatibilitas produk dan jasa yang dikembangkan dengan sistem BPR dan BPR Syariah; dan
   d. dependensi terhadap sistem yang akan terdampak.

2. Pengukuran risiko terkait pengembangan dan pengadaan Sistem Elektronik

   Pengukuran tingkat risiko pada proses pengembangan dan pengadaan Sistem Elektronik tergantung pada faktor terkait antara lain:

   a. kesesuaian dengan rencana strategis bisnis dan ketentuan yang berlaku;
   b. adanya perubahan pada cakupan sistem atau proses;
   c. pemisahan lingkungan pengembangan, uji coba dan operasional, termasuk pengaturan aksesnya kepada pengembang, penguji, dan pengguna;
   d. rencana sistem aplikasi yang akan diperoleh melalui pembelian paket tanpa modifikasi, pembelian paket dengan modifikasi, pengembangan sendiri secara intern atau oleh PPJTI;
   e. cakupan dan tingkat kekritisan sistem atau banyaknya unit bisnis yang terpengaruh;
   f. kompleksitas tipe pemrosesan dari aplikasi yang akan dikembangkan (*batch*, *real-time*, *client* atau *server*, *parallel distributed*);
   g. volume dan nilai transaksi dari sistem aplikasi yang akan dikembangkan;
   h. klasifikasi dan sensitivitas data dari sistem yang akan dikembangkan;
   i. dampak pada data (baca (*read*), unduh (*download*), unggah (*upload*), pengkinian (*update*), atau ubah (*alter*));
   j. tingkat pengalaman dan kemampuan teknis, jika sistem dibeli atau dikembangkan oleh PPJTI;
   k. kecukupan jumlah dan kemampuan personel yang termasuk dalam tim pengembangan;
   l. kesesuaian *platform* dan aplikasi yang dipilih dengan arsitektur TI BPR dan BPR Syariah;
   m. ketergantungan sistem yang dikembangkan dengan sistem yang telah ada;
   n. ketidaksesuaian jumlah pengguna dengan rencana awal pengembangan atau terdapat perubahan struktur organisasi saat proses pengembangan;
   o. perubahan ketentuan;
   p. adanya risiko baru atau risiko yang dapat muncul dari teknologi yang sedang dikembangkan atau risiko keusangan teknologi;
   q. adanya kelemahan audit atau kelemahan yang ditemui dalam *self-assessment*; dan
   r. ketidaksesuaian pelaksanaan pengembangan dengan target waktu penyelesaian.

3. Pemantauan risiko pada pengembangan dan pengadaan
   BPR dan BPR Syariah melakukan pemantauan risiko TI dengan mengevaluasi kesesuaian, kecukupan, dan efektivitas pengembangan dan pengadaan Sistem Elektronik.
   a. pemantauan pelaksanaan proyek melalui proyek *management tools*;
   b. pemantauan hasil UAT dan SIT sebagai indikator *early warning*; dan
   c. melakukan review secara berkala atas kinerja PPJTI dan SLA yang diperjanjikan.
4. Pengendalian risiko pada pengembangan dan pengadaan Sistem Elektronik
   Pada setiap tahapan pengembangan dan pengadaan Sistem Elektronik, BPR dan BPR Syariah harus memitigasi risiko yang telah diidentifikasi dan diukur dengan beberapa cara pengendalian yang telah ditetapkan dalam kebijakan, standar, dan prosedur pengembangan dan pengadaan TI BPR dan BPR Syariah. Setelah melakukan mitigasi, BPR dan BPR Syariah harus memantau risiko yang dikendalikan dan *residual risk* karena setiap gangguan yang dapat mempengaruhi rencana dan proses pengembangan dan pengadaan TI, pada akhirnya dapat berdampak pada kegiatan operasional BPR dan BPR Syariah.
   a. Pengendalian Risiko pada Pengembangan
      Dalam rangka mengendalikan risiko terkait pengembangan TI, BPR dan BPR Syariah harus dapat memastikan bahwa pengembangan sistem yang dilakukan telah sesuai dengan kebijakan, standar, dan prosedur untuk setiap tahapan pengembangan. Hal ini dilakukan dengan memperhatikan:
      1) rencana pengembangan sistem telah sesuai dengan kebutuhan pengguna dan arah kebijakan bisnis BPR dan BPR Syariah;
      2) rancangan sistem yang dikembangkan telah mencakup kebutuhan pengguna pada tahap inisiasi dan perencanaan serta sesuai dengan standar pengendalian aplikasi yang melibatkan partisipasi dari audit intern.
         Berdasarkan tujuannya, pengendalian terbagi atas pengendalian yang bersifat pencegahan, deteksi atau temuan, atau koreksi. Pengendalian yang harus dilakukan paling sedikit meliputi:
         a) pengendalian *input*
            Paling sedikit mencakup pengecekan terhadap validitas atau kebenaran data, *range* data, parameter, dan duplikasi data yang di-*input*;
         b) pengendalian proses
            Memastikan proses bekerja secara akurat dan dapat menyimpan atau menolak informasi. Pengendalian proses yang dapat dilakukan secara otomatis oleh sistem mencakup paling sedikit *error reporting*, *transaction log*, pengecekan urutan, dan rekam cadang (*backup*) *file*; dan
         c) pengendalian *output*
            Memastikan sistem mengelola informasi dengan aman dan mendistribusikan informasi hasil proses dengan tepat serta menghapus informasi yang telah melewati masa retensi.
      3) hasil pemrograman dibangun berdasarkan spesifikasi desain dengan dilakukannya rencana uji coba yang didokumentasikan untuk mempermudah penelusuran pengubahan sistem aplikasi;
      4) pelaksanaan rangkaian uji coba dengan menetapkan ruang lingkup tes skenario, penilaian atas hasil uji coba, melakukan

perbaikan pada sistem sampai dengan mendapatkan pengesahan atas laporan hasil uji coba;

5) implementasi sistem yang baru dapat berjalan dengan sistem yang lama dengan adanya persiapan instalasi, migrasi file, konversi data, dokumen petunjuk teknis, dan pelatihan; dan
6) hasil implementasi dari sistem berjalan dengan baik secara berkesinambungan dengan dilakukannya kaji ulang secara berkala atas hasil efektivitas pemeliharaan.

b. Pengendalian Risiko pada Pengembangan dan Pengadaan Sistem Elektronik

Dalam rangka mengendalikan risiko pada pengadaan, BPR dan BPR Syariah harus membuat kriteria pemilihan PPJTI dan melakukan kaji ulang kemampuan PPJTI antara lain terkait dengan kondisi keuangan, tingkat dukungan (*support level*), dan pengendalian keamanan, sebelum menetapkan pilihan produk atau layanan dari PPJTI. BPR dan BPR Syariah harus melakukan kaji ulang perjanjian lisensi (*licensing agreement*) untuk memastikan hak dan tanggung jawab masing-masing pihak secara jelas dan wajar. BPR dan BPR Syariah harus melakukan konfirmasi bahwa jaminan kinerja (*performance guarantee*), akses terhadap kode sumber (termasuk melalui mekanisme *escrow agreement*), hak cipta, dan keamanan perangkat lunak atau data, telah diatur secara jelas sebelum pihak BPR dan BPR Syariah menandatangani perjanjian. Hal-hal yang perlu diperhatikan adalah:

1) memastikan proses pengadaan telah sesuai dengan kebijakan, standar, dan prosedur BPR dan BPR Syariah serta ketentuan berlaku terkait pengadaan; dan
2) melakukan segala perikatan yang memiliki kekuatan hukum secara memadai.

BAB III
MANAJEMEN RISIKO OPERASIONAL TI

A. MANAJEMEN RISIKO AKTIVITAS OPERASIONAL TI

Manajemen risiko aktivitas operasional TI harus memperhatikan:

1. Identifikasi risiko aktivitas operasional TI

   Dalam melakukan identifikasi aktivitas operasional TI, BPR dan BPR Syariah menginventarisasi kejadian atau aktivitas yang dapat mengganggu operasional, antara lain:

   a. kesalahan investasi teknologi termasuk penerapan yang tidak benar, kegagalan dari PPJTI, pendefinisian dari kebutuhan bisnis yang tidak tepat, ketidaksesuaian dengan sistem-sistem yang ada, atau keusangan perangkat lunak, termasuk hilangnya dukungan PPJTI terhadap perangkat keras dan perangkat lunak yang digunakan oleh BPR dan BPR Syariah;
   b. permasalahan pengembangan sistem dan implementasi termasuk ketidakcukupan manajemen proyek, biaya dan waktu yang melebihi batas, *error* pada pemrograman, kegagalan untuk mengintegrasikan atau migrasi dari sistem yang ada, atau kesalahan dari sebuah sistem untuk memenuhi kebutuhan pengguna;
   c. permasalahan pada kapasitas sistem seperti kekurangan pada perencanaan kapasitas, ketidakcukupan kapasitas untuk mengakomodasi fleksibilitas sistem, dan/atau ketidakcukupan perangkat lunak untuk mengakomodasi pengembangan bisnis;
   d. kegagalan sistem termasuk pada jaringan, *interface*, perangkat keras, perangkat lunak, atau kegagalan komunikasi intern; dan
   e. pelanggaran pada keamanan sistem termasuk pelanggaran pada keamanan, penipuan dalam pemrograman, atau virus pada komputer.

2. Pengukuran risiko aktivitas operasional TI

   BPR dan BPR Syariah perlu mengukur risiko aktivitas operasional TI dengan mempertimbangkan faktor terkait, antara lain:

   a. kesesuaian dengan rencana strategis bisnis dan regulasi yang berlaku;
   b. perubahan pada cakupan sistem atau proses;
   c. lokasi pengaksesan sistem (intern atau ekstern, termasuk internet, *dial-up*, atau WAN);
   d. perolehan aplikasi antara lain melalui pembelian paket tanpa modifikasi, pembelian paket dengan modifikasi, dan/atau pengembangan sendiri secara intern atau oleh pihak ketiga;
   e. cakupan dan tingkat kekritisan sistem atau banyaknya unit bisnis yang terpengaruh;
   f. kompleksitas tipe pemrosesan dari aplikasi (*batch*, *realtime*, *client* atau *server*, atau *parallel distributed*);
   g. volume transaksi dari sistem;
   h. klasifikasi dan sensitivitas data yang diproses atau digunakan;
   i. dampak pada data (baca (*read*), unduh (*download*), unggah (*upload*), penginian (*update*), atau ubah (*alter*));
   j. tingkat pengalaman dan kemampuan pengelola TI;
   k. kecukupan jumlah dan kemampuan tenaga pelaksana;
   l. keragaman *platform*, aplikasi, dan *delivery channel*;
   m. jumlah pengguna dan nasabah;
   n. perubahan ketentuan;

o. adanya risiko baru atau risiko yang dapat muncul dari teknologi yang sedang dikembangkan atau risiko keusangan teknologi; dan
p. adanya kelemahan audit atau kelemahan yang ditemui dalam *self-assessment*.

3. Pemantauan risiko aktivitas operasional TI
   BPR dan BPR Syariah melakukan pemantauan risiko TI dengan mengevaluasi kesesuaian, kecukupan, dan efektivitas aktivitas operasional TI.
   Hal-hal yang dapat menjadi cakupan dalam pemantauan risiko antara lain:
   a. pemantauan infrastruktur Sistem Elektronik;
   b. mengevaluasi aktivitas sistem terhadap *audit trail*; dan
   c. pemantauan kerentanan melalui *vulnerability assessment* dan *penetration testing*.
4. Pengendalian risiko aktivitas operasional TI
   BPR dan BPR Syariah menerapkan praktik-praktik pengendalian yang memadai, sebagai bagian dari strategi mitigasi risiko TI secara keseluruhan dengan memperhatikan paling sedikit:
   a. pengendalian secara *preventive* melalui implementasi *firewall*, *patch management*, *control access* pengguna, antivirus, dan pelatihan sumber daya manusia TI;
   b. pengendalian secara *detective* melalui IDS/IPS, *audit log*, dan monitoring *tools*; dan
   c. pengendalian secara *corrective* melalui prosedur *back up restore*, dan *incident respond plan*.

B. MANAJEMEN RISIKO LAYANAN DIGITAL

Manajemen risiko layanan digital harus memperhatikan:

1. Identifikasi Risiko
   BPR dan BPR Syariah wajib melakukan identifikasi risiko terkait Layanan Digital yang diselenggarakan, meliputi aspek teknologi, operasional, keamanan, hingga kepatuhan.
   a. risiko terkait keamanan siber, dapat berupa serangan *phishing*, *malware*, *ransomware*, DDoS, atau *credential theft*.
   b. risiko terkait operasional TI, dapat berupa kegagalan sistem/aplikasi, *bug software*, atau *downtime server*.
   c. risiko terkait data dan privasi, dapat berupa kebocoran data nasabah, penyalahgunaan akses.
   d. risiko terkait *fraud* digital, dapat berupa *social engineering*, transaksi palsu, atau akun fiktif.
   e. risiko terkait kepatuhan, dapat berupa pelanggaran regulasi OJK/BI, maupun regulasi lainnya terkait keamanan *digital banking*.
   f. risiko terkait reputasi, dapat berupa hilangnya kepercayaan nasabah akibat layanan gagal/insiden siber.
   g. risiko terkait pihak ketiga (PPJTI), dapat berupa kelemahan vendor teknologi, *cloud provider*, atau *fintech partner*.
2. Pengukuran Risiko
   Pengukuran dilakukan terhadap potensi kerugian yang terjadi (*loss event*) pada setiap jenis Layanan Digital. Untuk dapat memantau besar dan kecenderungan risiko dari setiap jenis Layanan Digital maka BPR dan BPR Syariah harus membuat Pangkalan Data (*database*) yang berisi data historis kerugian (*loss event database*) setiap jenis Layanan Perbankan Elektronik. Jenis risiko terkait Layanan Digital adalah sebagai berikut:

a. Risiko umum, antara lain:
   1) risiko operasional yaitu risiko yang timbul atau berasal dari *fraud*, kesalahan dalam proses, gangguan sistem atau kegiatan tidak terduga yang menyebabkan ketidakmampuan BPR dan BPR Syariah untuk menyediakan produk atau layanan serta menimbulkan kerugian bagi BPR dan BPR Syariah maupun nasabah. Risiko operasional juga dapat mencakup risiko terkait transaksi yang merupakan risiko yang dapat timbul dari kurang memadainya pelaksanaan prinsip pengendalian pengamanan;
   2) risiko kepatuhan yang timbul dari:
      a) ketidakpatuhan terhadap hukum dan/atau peraturan dari otoritas pengawas;
      b) ketidakpatuhan terhadap ketentuan peraturan perundang-undangan mengenai kerahasiaan data nasabah dan ketentuan peraturan perundang-undangan mengenai transparansi informasi produk; dan
      c) keterbatasan ketentuan peraturan perundang-undangan sebagai dasar hukum transaksi Layanan Perbankan Elektronik;
   3) risiko stratejik merupakan risiko yang dapat timbul dari:
      a) ketidaksesuaian dengan tujuan atau rencana bisnis BPR dan BPR Syariah;
      b) perencanaan investasi pada Layanan Digital yang kurang memadai dapat menyebabkan tidak optimalnya *return on investment* yang diperoleh dibandingkan dengan biaya yang dikeluarkan; dan
      c) pengelolaan hubungan (*relationship management*) dengan PPJTI yang kurang optimal;
   4) risiko reputasi yaitu risiko yang timbul dari kemungkinan menurunnya atau hilangnya kepercayaan nasabah karena *service level delivery* kepada nasabah tidak terjaga seperti kelambatan atau tidak tersedianya Layanan Perbankan Elektronik, kelambatan respons atas komplain nasabah, ketidakamanan sistem, dan adanya gangguan pada sistem;
   5) risiko likuiditas yaitu risiko yang timbul dalam hal BPR dan BPR Syariah tidak membatasi jumlah yang dapat ditransfer oleh nasabah korporasi melalui *internet banking*.

b. Risiko spesifik, antara lain:
   1) risiko operasional yang mungkin timbul dari transaksi Layanan Digital diantaranya adalah kecurangan, penyadapan, kesalahan, kerusakan, atau tidak berfungsinya sistem;
   2) risiko dalam penyelenggaraan *internet banking* meliputi:
      a) nasabah memperoleh informasi yang salah atau tidak akurat melalui internet;
      b) pencurian data finansial dari Pangkalan Data (*database*) BPR dan BPR Syariah melalui *informational and communicative internet banking* yang tidak terisolasi;
      c) terdapat ancaman atau serangan misalnya *defacing*, *cybersquatting*, *denial of service*, pemutusan jaringan

(*network interception*), *man-in-the middle-attack*, dan virus;

d) terjadi pencurian identitas (*identity theft*), misalnya *phising*, *keylogger*, *spoofing*, dan *cybersquatting*; dan

e) terjadi transaksi yang dilakukan oleh pihak yang tidak berwenang (*unauthorized transaction*) atau terjadi *fraud*;

3) ancaman keamanan pada produk yang menggunakan teknologi *wireless* misalnya *mobile banking* antara lain penyadapan komunikasi akibat belum semua transaksi melalui mobile banking dienkripsi, *denial of service attack*, virus, *worm*, *trojan*, dan penggandaan *sim card*; dan

4) ancaman keamanan pada produk *phone banking* yang rentan terhadap penyadapan.

3. Pengendalian risiko terkait Layanan Digital

Dalam rangka pengendalian risiko, BPR dan BPR Syariah harus melakukan mitigasi atas risiko umum dan risiko spesifik yang mungkin terjadi dalam Layanan Digital dengan memperhatikan prinsip pengendalian pengamanan data nasabah dan transaksi Layanan Digital, antara lain dengan:

a. melakukan langkah-langkah yang memadai untuk menguji keaslian (*authentication*) identitas dan kewenangan (*authorization*) nasabah yang melakukan transaksi melalui Layanan Perbankan Elektronik;

b. memiliki kebijakan dan prosedur tertulis untuk memastikan bahwa BPR dan BPR Syariah mampu menguji keaslian identitas dan kewenangan nasabah;

c. menggunakan berbagai metode untuk menguji keaslian yang didasarkan atas penilaian manajemen risiko Layanan Digital, sensitivitas, dan nilai data yang disimpan. Dalam menggunakan metode pengujian keaslian, BPR dan BPR Syariah memperhatikan hal-hal sebagai berikut:

1) menerapkan kombinasi paling sedikit 2 (dua) faktor otentikasi (*two factor authentication*) yaitu "*what you know*" (seperti PIN atau *password*), "*what you have*" (seperti antara lain OTP, *smart card*, dan token), dan/atau "*something you are*" (antara lain *biometric* seperti retina atau sidik jari);

2) persyaratan jumlah karakter minimum PIN. Khusus untuk PIN yang digunakan dalam alat pembayaran dengan menggunakan kartu, *mobile banking*, dan *internet banking*, panjang PIN harus paling sedikit terdiri dari 6 (enam) digit karakter;

3) adanya batasan maksimum kesalahan memasukkan PIN untuk menghambat upaya akses secara tidak sah;

4) BPR dan BPR Syariah harus memastikan penerapan prinsip kehati-hatian dalam penggunaan metode pengujian keaslian yang meliputi:

a) pembuatan, validasi, dan enkripsi PIN dan metode pengujian keaslian lainnya harus menggunakan metode yang diyakini keamanannya. Khusus untuk metode enkripsi yang digunakan pada alat pembayaran menggunakan kartu, metode enkripsi PIN harus paling sedikit menggunakan metode *Advanced Encryption Standard* (AES) atau

berdasarkan standar kartu dan/atau *chip* sesuai regulasi Otoritas terkait;

b) Pangkalan Data (*database*) pengujian keaslian yang menyediakan akses kepada rekening nasabah pada Layanan Digital dilindungi dari gangguan dan perusakan;

c) setiap penambahan, penghapusan, atau perubahan Pangkalan Data (*database*) dan pengujian keaslian telah diotorisasi dengan tepat oleh pihak yang berwenang;

d) khusus untuk Layanan Digital dengan menggunakan kartu, fungsi pembuatan dan pengiriman PIN harus terpisah dari fungsi pembuatan dan pengiriman kartu;

e) khusus untuk Layanan Digital dengan menggunakan kartu, fungsionalitas dan keamanan kartu harus diuji menggunakan standar kartu dan *chip* yang memenuhi standar;

f) terdapat sarana pengendalian yang tepat terhadap sistem Layanan Digital sehingga pihak ketiga yang tidak dikenal tidak dapat menggantikan nasabah yang telah dikenal; dan

g) terdapat kebijakan yang menyatakan bahwa jika terdapat indikasi telah terjadi pencurian data yang terkait dengan aspek otentikasi nasabah maka Bank harus melakukan penggantian data otentikasi nasabah dimaksud secepatnya;

5) BPR dan BPR Syariah harus menyusun dan menetapkan prosedur untuk menjamin bahwa transaksi tidak dapat diingkari oleh nasabah (*non-repudiation*) sehingga transaksi dapat dipertanggungjawabkan, yang meliputi antara lain:

a) sistem Layanan Digital telah dirancang untuk menghilangkan kemungkinan dilakukannya transaksi secara tidak sengaja oleh para pengguna yang berhak;

b) seluruh pihak yang melakukan transaksi telah diuji keasliannya;

c) data transaksi keuangan dilindungi dari kemungkinan pengubahan dan setiap pengubahan dapat dideteksi. Proses pencatatan transaksi keuangan harus dirancang sebaik mungkin agar dapat mencegah upaya pengubahan tidak sah. Setiap upaya pengubahan yang tidak sah perlu dicatat dan menjadi perhatian manajemen BPR dan BPR Syariah; dan

d) penerapan metode untuk menjamin dipenuhinya prinsip tidak dapat diingkari (*non-repudiation*), misalnya *digital signature* dan *Public Key Infrastructure* (PKI). Kunci-kunci (*keys*) yang digunakan untuk keperluan enkripsi harus dipelihara secara aman sehingga tidak ada yang mengetahui kombinasi kunci-kunci tersebut secara utuh;

d. memastikan terdapat pemisahan tugas dan tanggung jawab terkait penggunaan sistem, Pangkalan Data (*database*), dan

aplikasi Layanan Digital. BPR dan BPR Syariah harus memastikan terdapat *dual control* dan pemisahan tugas untuk memastikan terlaksananya fungsi *check and balance*. BPR dan BPR Syariah perlu memastikan terdapat pemisahan tugas antara pihak yang menginisiasi atau menginput data dan pihak yang bertanggung jawab untuk memverifikasi kebenaran data tersebut. Misalnya dalam suatu aplikasi perbankan, setiap penambahan atau perubahan Pangkalan Data (*database*) yang dilakukan oleh *data entry operator*, akan efektif sepanjang disetujui oleh penyelia (*supervisor*);

e. memastikan adanya pengendalian terhadap otorisasi dan hak akses (*privileges*) yang tepat terhadap sistem, Pangkalan Data (*database*), dan aplikasi Layanan Perbankan Elektronik. Seluruh arsip dan data BPR dan BPR Syariah yang bersifat rahasia hanya dapat diakses oleh pihak yang telah memiliki kewenangan dan otorisasi. Data BPR dan BPR Syariah yang bersifat rahasia harus dipelihara secara aman dan dilindungi dari kemungkinan diketahui atau dimodifikasi oleh pihak yang tidak berwenang;

f. memastikan metode dan prosedur diterapkan untuk melindungi integritas data, catatan, dan informasi terkait transaksi Layanan Digital dengan memperhatikan hal-hal sebagai berikut:
   1) BPR dan BPR Syariah harus menerapkan metode dan teknik yang tepat untuk mengurangi ancaman ekstern seperti serangan virus dan *malicious transaction*, yang meliputi:
      a) perangkat lunak – penyediaan *virus scanning* dan antivirus untuk seluruh *entry point* dan masing-masing komputer;
      b) perangkat lunak untuk mendeteksi adanya penyusupan (*intrusion detection system*); dan
      c) pengujian penetrasi (*penetration testing*) terhadap jaringan intern dan ekstern secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun;
   2) BPR dan BPR Syariah harus melakukan pengujian integritas data transaksi Layanan Digital; dan
   3) BPR dan BPR Syariah harus melakukan pengendalian untuk memastikan seluruh transaksi telah dilaksanakan dengan benar;

g. memastikan tersedianya mekanisme penelusuran (*audit trail*) yang jelas untuk seluruh transaksi Layanan Digital, yang mencakup hal-hal sebagai berikut:
   1) BPR dan BPR Syariah harus memelihara *log* transaksi berdasarkan kebijakan retensi data BPR dan BPR Syariah sesuai ketentuan peraturan perundang-undangan guna tersedianya jejak audit yang jelas serta membantu penyelesaian perselisihan. Data transaksi yang diperlukan mencakup paling sedikit data nasabah, nomor rekening, jenis, waktu, lokasi, dan jumlah transaksi;
   2) BPR dan BPR Syariah harus memberikan notifikasi kepada nasabah apabila suatu transaksi telah berhasil dilakukan. Apabila terdapat transaksi yang ditolak maka perlu didokumentasikan dan terdapat prosedur tindak lanjutnya; dan

3) BPR dan BPR Syariah harus memastikan tersedianya fungsi jejak audit untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan yang harus dikaji ulang atau dievaluasi secara berkala. Apabila sistem pemrosesan dan jejak audit merupakan tanggung jawab pihak ketiga maka proses jejak audit tersebut harus sesuai dengan standar yang ditetapkan oleh BPR dan BPR Syariah. BPR dan BPR Syariah harus memiliki kewenangan yang cukup untuk dapat mengakses jejak audit yang dipelihara oleh pihak ketiga tersebut;

h. melakukan pendeteksian berbasis perilaku, pemberitahuan *real-time*, dan pemantauan atas transaksi yang tidak sah atau tidak wajar (*unusual transaction*) misalnya melalui *Intrusion Detection System* (IDS) dan *fraud detection*. Selanjutnya BPR dan BPR Syariah harus memiliki prosedur penanganan masalah atau kejahatan yang terdeteksi;

i. menerapkan langkah-langkah untuk melindungi kerahasiaan informasi Layanan Perbankan Elektronik. Prosedur pengamanan disesuaikan dengan tingkat sensitivitas informasi;

j. memiliki standar dan pengendalian atas penggunaan dan perlindungan data apabila PPJTI memiliki akses terhadap data tersebut;

k. memiliki Rencana Pemulihan Bencana termasuk *contingency plan* yang efektif untuk memastikan tersedianya sistem dan jasa Layanan Digital secara berkesinambungan; dan

l. mengembangkan rencana penanganan kejadian (*incident response plan*) yang cepat dan tepat untuk mengelola, mengatasi, dan meminimalisasi dampak suatu insiden, *fraud*, kegagalan sistem (*intern* dan *ekstern*), yang dapat menghambat penyediaan sistem dan jasa Layanan Digital.

4. Pengendalian risiko untuk Layanan Digital tertentu

a. Dalam menyediakan Layanan Digital misalnya pada *mobile banking* dan *internet banking*, BPR dan BPR Syariah juga harus memperhatikan kenyamanan dan kemudahan nasabah dalam menggunakan fasilitas, termasuk efektivitas menu tampilan Layanan Digital, khususnya dalam melakukan pilihan pesan yang diinginkan nasabah agar tidak terjadi kesalahan dan kerugian dalam transaksi. Dalam rangka meningkatkan pengamanan, BPR dan BPR Syariah dapat menetapkan persyaratan atau melakukan pembatasan transaksi melalui Layanan Digital untuk menjamin keamanan dan keandalan transaksi, misalnya meminta nasabah melakukan registrasi rekening pihak ketiga yang merupakan tujuan transfer dalam *mobile banking* atau membatasi nominal jumlah dan jenis transaksi melalui *mobile banking* dan *internet banking*.

b. Dalam penyelenggaraan Layanan Digital yang menyediakan sarana fisik, BPR dan BPR Syariah harus melakukan pengendalian pengamanan fisik terhadap peralatan dan ruangan yang digunakan terhadap bahaya pencurian, perusakan, dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang. Pengamanan fisik antara lain menggunakan *seal* dan CCTV dan proteksi sistem antara lain anti-*Malware* dan *Operating System - OS Lock*. BPR dan BPR Syariah harus melakukan pemantauan secara rutin untuk menjamin

keamanan dan kenyamanan bagi nasabah pengguna Layanan Digital.

c. BPR dan BPR Syariah harus memastikan terdapatnya pengamanan atas aspek transmisi data antara terminal *Electronic Fund Transfer* (EFT) dengan *host computer*, terhadap risiko kesalahan transmisi, gangguan jaringan, akses oleh pihak yang tidak bertanggung jawab, dan lain-lain. Pengamanan mencakup pengendalian terhadap peralatan yang digunakan, pemantauan terhadap akses perangkat lunak *Controller* (*Host-Front End*), pemantauan kualitas dan akurasi kinerja perangkat jaringan serta saluran transmisi.

d. *Point of Sales* (POS) atau *Electronic Data Capture* (EDC) memungkinkan transfer dana secara elektronik dari rekening nasabah kepada rekening *acquirer* atau *merchant* untuk pembayaran suatu transaksi. Transaksi dilakukan melalui POS Terminal yang berlokasi di pusat perbelanjaan atau pasar swalayan umumnya menggunakan suatu alat pembayaran dengan menggunakan kartu. Penyediaan POS dapat dilakukan sendiri oleh BPR dan BPR Syariah penerbit maupun oleh *financial acquirer*, *technical acquirer*, dan perusahaan *switching*. Pihak penyedia POS Terminal harus selalu melakukan peningkatan pengamanan fisik di sekitar lokasi POS Terminal dan terhadap POS Terminal, antara lain dengan menggunakan POS Terminal yang dapat meminimalisasi kemungkinan adanya penyadapan baik di POS Terminal sendiri maupun dalam jaringan komunikasi.

e. Bagi BPR dan BPR Syariah yang menyediakan jasa *mobile banking* maka BPR dan BPR Syariah harus memastikan keamanan transaksi antara lain:
   1) menggunakan suatu SIM *Toolkit* dengan fitur enkripsi *end-to-end* dari *handphone* hingga *server mobile banking*, untuk melindungi pengiriman data pada *mobile banking*; dan
   2) melakukan *mutual authentication* yaitu pihak BPR dan BPR Syariah dan nasabah dapat melakukan proses otentifikasi dengan *digital certificate* atau *personal authentication message* yaitu untuk membantu nasabah memastikan bahwa pihak yang bertransaksi dengan nasabah adalah pihak yang benar.

5. Pengendalian risiko terkait Layanan Digital yang diselenggarakan melalui PPJTI

   Dalam hal sistem penyelenggaraan Layanan Digital dilakukan melalui kerja sama dengan PPJTI misalnya perusahaan *switching* dan *Internet Service Provider* (ISP), BPR dan BPR Syariah harus menetapkan dan menerapkan prosedur pengawasan dan *due diligence* yang menyeluruh dan berkelanjutan untuk mengelola hubungan BPR dan BPR Syariah dengan PPJTI tersebut. Untuk itu BPR dan BPR Syariah harus membuat suatu perjanjian tertulis dengan PPJTI terkait Layanan Perbankan Elektronik yang secara rinci mengatur hak dan kewajiban, aspek pengamanan, dan melakukan pemantauan kinerja PPJTI sesuai SLA.

BAB IV
MANAJEMEN RISIKO JARINGAN KOMUNIKASI

Manajemen risiko jaringan komunikasi harus memperhatikan:

1. Identifikasi Risiko

   BPR dan BPR Syariah perlu melakukan identifikasi risiko penggunaan jaringan komunikasi untuk menjamin kelangsungan operasional, antara lain meliputi:

   a. Identifikasi ketersediaan (*availability*) jaringan komunikasi, melalui identifikasi kebutuhan minimal *bandwidth*, jumlah kantor, dan hal terkait lainnya;
   b. Identifikasi potensi risiko yang melekat, antara lain berupa penyadapan data (*sniffing*), *man-in-the-middle-attack*, maupun penggunaan perangkat tidak sah; dan
   c. Identifikasi keandalan PPJTI, melalui pemilihan PPJTI yang memberikan SLA memadai.

2. Pengukuran Risiko

   BPR dan BPR Syariah perlu mengukur risiko jaringan komunikasi dengan mempertimbangkan faktor terkait, antara lain:

   a. kesesuaian kapasitas jaringan komunikasi dengan rencana strategis bisnis;
   b. implementasi jaringan komunikasi sesuai dengan kebijakan, standar, dan prosedur;
   c. kontrak dan SLA dengan pihak ketiga penyedia jasa fasilitas jaringan komunikasi;
   d. ketersediaan daftar permasalahan dan penanganannya;
   e. ketersediaan daftar pengguna dan wewenangnya; dan
   f. cakupan dan tingkat kekritisan sistem atau banyaknya unit bisnis yang terpengaruh.

3. Pemantauan Risiko

   Dalam pemantauan jaringan komunikasi yang digunakan oleh BPR dan BPR Syariah perlu diperhatikan antara lain:

   a. jejak audit yang tersedia harus dipantau secara teratur untuk dapat mendeteksi secara dini ada tidaknya penyimpangan;
   b. kinerja jaringan komunikasi diukur secara berkala berdasarkan tingkat ketersediaan (*availability*) dan *response time*;
   c. BPR dan BPR Syariah harus memantau kapasitas yang digunakan dan yang diperlukan untuk rencana pengembangan bisnis dibandingkan dengan kapasitas terpasang;
   d. BPR dan BPR Syariah harus memantau dan menindaklanjuti penyusupan/serangan terhadap jaringan komunikasi; dan
   e. BPR dan BPR Syariah harus melakukan kaji ulang pemberian akses ke pengguna secara berkala untuk meyakinkan bahwa akses yang diberikan masih sesuai dengan tugas dan wewenangnya, serta perlu dilakukan kaji ulang atas pengguna jaringan komunikasi di BPR atau BPR Syariah yang memiliki akses ke jaringan komunikasi di luar BPR atau BPR Syariah.

4. Pengendalian Risiko

   Dalam menerapkan pengendalian akses, terdapat beberapa hal yang harus diperhatikan oleh BPR dan BPR Syariah yaitu:

   a. akses ke jaringan komunikasi oleh pengguna didasarkan pada kebutuhan bisnis dengan memperhatikan aspek keamanan informasi;
   b. melakukan pemisahan jaringan komunikasi berdasarkan segmen baik secara *logic* maupun fisik, misalnya pemisahan antara

lingkungan pengembangan dan produksi tanpa berbagi data atau infrastruktur;

c. dalam hal pemisahan secara fisik tidak dapat dilakukan, BPR dan BPR Syariah harus memisahkan jaringan komunikasi secara *logic* dan memantau *security access* di jaringan komunikasi;
d. keputusan untuk terhubung ke jaringan komunikasi di luar BPR dan BPR Syariah harus sesuai dengan persyaratan pengamanan dan secara formal disetujui oleh Direksi sebelum pelaksanaan;
e. menerapkan pengendalian yang dapat membatasi *network traffic* yang tidak sah atau tidak diharapkan;
f. konfigurasi perangkat jaringan komunikasi harus diatur dengan baik, termasuk fungsi-fungsi atau layanan yang tidak dibutuhkan harus dinonaktifkan;
g. penggunaan perangkat pengamanan jaringan komunikasi, seperti *firewall*, *Intrusion Detection System* (IDS), dan *Intrusion Prevention System* (IPS);
h. penggunaan penambahan perangkat monitor jaringan komunikasi (*network management system*) dengan memperhatikan pengamanannya;
i. pengujian secara berkala terhadap keamanan jaringan komunikasi, misalnya dengan *penetration testing*;
j. perlu adanya mekanisme pemantauan secara cepat dan akurat untuk menjamin efektivitas dan efisiensi pengoperasian jaringan antara lain mencakup prioritas proses, *response time,* dan kapasitas perangkat keras/lunak;
k. tersedianya prosedur Rencana Pemulihan Bencana yang terutama mencakup rekam cadang terhadap perangkat keras/lunak, Pangkalan Data, serta mekanisme *restart/recovery*, yang membutuhkan pengujian secara berkala; dan
l. tersedianya alternatif sistem komunikasi untuk mengantisipasi jika sistem yang ada mengalami gangguan.

BAB V
MANAJEMEN RISIKO PENGAMANAN INFORMASI

Manajemen risiko pengamanan informasi harus memperhatikan:

1. Identifikasi Risiko

   Risiko terkait pengamanan informasi mencakup ancaman terhadap kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data serta sistem. BPR dan BPR Syariah perlu melakukan identifikasi risiko terkait pengamanan informasi, antara lain:
   a. Ancaman internal berupa *human error*, *insider threat*, atau penyalahgunaan wewenang;
   b. Ancaman eksternal berupa serangan siber (*malware, phishing*, DDoS, *ransomware*);
   c. Risiko kepatuhan berupa ketidakpatuhan pada regulasi OJK/BI, standar ISO 27001, atau regulasi lainnya yang terkait;
   d. Risiko operasional berupa kegagalan sistem, *downtime*, atau kerusakan infrastruktur TI; dan
   e. Risiko pihak ketiga (termasuk PPJTI) berupa kelemahan vendor/mitra (*outsourcing IT, cloud service*).
2. Pengukuran Risiko

   Risiko diukur dengan menilai kemungkinan (*likelihood*) dan dampak (*impact*), misalnya dengan matriks risiko (*Low, Medium, High, Critical*). Pengukuran risiko yang dilakukan BPR dan BPR Syariah dapat mempertimbangkan hal berikut:
   a. Penilaian kuantitatif berupa estimasi kerugian finansial akibat insiden siber (*fraud*, kehilangan data nasabah, denda regulator);
   b. Penilaian kualitatif berupa dampak reputasi, kepercayaan nasabah, dan potensi gangguan terhadap stabilitas BPR dan BPR Syariah;
   c. *Risk Scoring* yang memuat kombinasi nilai *likelihood* x *impact* untuk menentukan prioritas penanganan; dan
   d. *Risk Appetite* & *Tolerance* yang ditetapkan oleh manajemen BPR dan BPR Syariah sesuai kapasitas dan regulasi.
3. Pemantauan Risiko

   BPR dan BPR Syariah wajib melakukan pemantauan yang dilakukan secara berkelanjutan untuk memastikan risiko terkendali, berupa:
   a. Monitoring sistem keamanan, antara lain mengimplementasikan SIEM, IDS/IPS, *log server*, *audit trail* transaksi.
   b. *Early warning system*, berupa *dashboard* risiko yang mendeteksi anomali perilaku transaksi atau akses sistem.
   c. Pelaporan berkala berupa hasil monitoring disampaikan kepada manajemen, komite risiko, dan regulator (jika diperlukan).
   d. Audit internal dan eksternal yang melakukan evaluasi rutin kepatuhan terhadap standar keamanan informasi.
4. Pengendalian dan Mitigasi Risiko

   Berdasarkan hasil pengukuran risiko, BPR dan BPR Syariah harus menetapkan bentuk penanganan dan pengendalian risiko yang akan diterapkan untuk meminimalisasi risiko yang dihadapi BPR dan BPR Syariah. BPR dan BPR Syariah dapat menganalisis kelemahan dari bentuk pengendalian yang telah diterapkan dan bentuk pengendalian pengamanan yang dapat direkomendasikan untuk diterapkan kemudian. Pengendalian intern juga dilakukan untuk memastikan bahwa pengendalian pengamanan informasi telah diterapkan, memadai, dan berjalan secara efektif sesuai dengan kebijakan, standar, dan prosedur pengamanan informasi yang berlaku. Evaluasi dan penyempurnaan terhadap kebijakan, standar, prosedur, dan sistem

pengamanan informasi harus selalu dilakukan secara terencana, antara lain dengan melaksanakan pemantauan terhadap:

a. perkembangan teknik atau metode baru yang mengancam sistem pengamanan informasi BPR dan BPR Syariah;
b. laporan kinerja pengamanan informasi dalam rangka mengidentifikasi tren ancaman atau kelemahan pengendalian pengamanan;
c. tindak lanjut penanganan serangan atau insiden pengamanan informasi terhadap BPR dan BPR Syariah; dan
d. efektivitas penerapan kebijakan, standar, prosedur, dan pengendalian pengamanan informasi.

Pengendalian mencakup langkah preventif, detektif, dan korektif

a. *Preventive*, dapat berupa:
    1) Kebijakan keamanan informasi, termasuk klasifikasi data berdasarkan tingkat kritikalitas dan sensitivitas.
    2) Pengendalian akses berbasis *least privilege* dan *multi-factor authentication* terhadap seluruh sistem kritikal. BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk sistem kritikal.
    3) Pelatihan karyawan terkait literasi keamanan dan etika syariah dalam menjaga data.
b. *Detective*, dapat berupa:
    1) Pemanfaatan sistem deteksi ancaman, *penetration testing*, dan *vulnerability assessment*.
    2) Pengawasan aktivitas pengguna dan sistem secara *real-time*.
c. Korektif dan Mitigasi, dapat berupa:
    1) *Incident Response Plan* (IRP) dan *Disaster Recovery Plan* (DRP).
    2) Prosedur tindak lanjut insiden siber yang terintegrasi dengan *Business Continuity Plan* (BCP).
    3) Evaluasi pascainsiden (*lessons learned*) untuk meningkatkan ketahanan sistem.

BAB VI
MANAJEMEN RISIKO RENCANA PEMULIHAN BENCANA

Manajemen risiko terkait rencana pemulihan bencana harus memperhatikan:

1. Identifikasi Risiko
   BPR dan BPR Syariah harus dapat mengidentifikasi risiko yang berpotensi mengganggu kelangsungan operasional dan layanan, antara lain:
   a. Bencana alam, berupa gempa bumi, banjir, kebakaran, atau erupsi gunung berapi.
   b. Gangguan teknis, berupa kegagalan listrik, kerusakan *hardware*, atau kerusakan jaringan komunikasi.
   c. Serangan siber, berupa *ransomware*, DDoS, atau *data breach* yang melumpuhkan sistem inti (*core banking*).
   d. Gangguan eksternal, berupa huru-hara, sabotase, atau terputusnya layanan vendor kritikal (*cloud*, *data center*).
   e. Kesalahan manusia (*human error*), berupa salah konfigurasi, atau kelalaian dalam prosedur *backup/restore.*
2. Pengukuran Risiko
   BPR dan BPR Syariah dapat melakukan pengukuran risiko dengan menilai besarnya kemungkinan (*likelihood*) dan dampak (*impact*) atas faktor-faktor berikut, antara lain:
   a. Dampak Finansial, berupa potensi kerugian langsung (*fraud*, kerusakan aset) dan tidak langsung (denda regulator, *opportunity loss*).
   b. Dampak Operasional, berupa berapa lama sistem inti tidak berfungsi, pengaruh ke layanan nasabah, dan *settlement* antarbank.
   c. Dampak Reputasi dan Kepatuhan, berupa kehilangan kepercayaan nasabah, pelanggaran terhadap regulasi OJK/BI.
   d. *Risk Rating* dengan formulasi *Likelihood* × *Impact* yang digunakan untuk menentukan prioritas (*High/Medium/Low*).
   e. Penetapan RTO (*Recovery Time Objective*) dan RPO (*Recovery Point Objective*) sebagai tolok ukur kecepatan dan ketepatan pemulihan sistem, antara lain atas kritikalitas sistem penting BPR dan BPR Syariah.
3. Pemantauan Risiko
   BPR dan BPR Syariah dapat melakukan pemantauan secara berkala agar rencana pemulihan bencana selalu relevan dan siap dijalankan, melalui antara lain:
   a. Monitoring Infrastruktur TI, berupa penggunaan SIEM, IDS/IPS, dan monitoring *server/data center*.
   b. Uji coba DRP (*Disaster Recovery Test*) yang dilakukan secara periodik untuk memastikan prosedur dapat berjalan sesuai target RTO dan RPO.
   c. Pelaporan ke Direksi dan Regulator berupa hasil monitoring dan pengujian dilaporkan kepada Direksi, Komite Risiko, serta OJK/BI.
   d. Audit dan Review yang dilakukan oleh unit audit internal atau pihak eksternal untuk menilai efektivitas DRP.
   e. Evaluasi atas PPJTI dengan memastikan pihak ketiga (*cloud provider*, *data center*) juga memiliki DRP yang memadai.
4. Pengendalian Risiko
   a. Pengendalian *preventive*, berupa:
      1) Penetapan kebijakan BCM & DRP sebagai bagian dari manajemen risiko BPR dan BPR Syariah.

2) Infrastruktur redundan (*data center primer* & sekunder) dengan arsitektur *high availability*.
3) Proses *backup data* otomatis dan terenkripsi.

b. Pengendalian *mitigative*, berupa:
1) Penyusunan *Incident Response Plan* yang terintegrasi dengan DRP.
2) Latihan simulasi bencana untuk pegawai.
3) Penyediaan lokasi kerja alternatif (*work area recovery*).

c. Pengendalian *corrective*, berupa:
1) Aktivasi DRP saat insiden terjadi.
2) Pemulihan sistem sesuai prosedur untuk mencapai RTO dan RPO.
3) *Post-mortem review* untuk memperbaiki kelemahan dari insiden yang terjadi.

BAB VII
MANAJEMEN RISIKO KERJA SAMA DENGAN PPJTI

Manajemen risiko terkait kerja sama dengan PPJTI harus memperhatikan:

1. Identifikasi Risiko

   Identifikasi risiko paling sedikit memperhatikan hal-hal sebagai berikut:

   a. Penggunaan PPJTI lain dalam menyelenggarakan TI BPR dan BPR Syariah dapat memberikan kontribusi terhadap beberapa jenis risiko, yaitu:
      1) risiko operasional, yaitu ketidakmampuan PPJTI dalam memenuhi perjanjian;
      2) risiko reputasi, yaitu ketidakpuasan nasabah karena ketidakmampuan PPJTI memenuhi SLA;
      3) risiko stratejik, yaitu ketidakcocokan TI yang digunakan BPR dan BPR Syariah dengan tujuan dan rencana strategis BPR dan BPR Syariah yang dibuat untuk mencapai tujuan tersebut; dan
      4) risiko kepatuhan, yaitu ketidakmampuan BPR dan BPR Syariah memenuhi ketentuan peraturan perundang-undangan.
   b. Dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko, BPR dan BPR Syariah harus mempertimbangkan:
      1) terkait dengan aktivitas dan fungsi yang diselenggarakan oleh PPJTI meliputi sensitivitas data yang diakses, dilindungi, atau dikendalikan oleh PPJTI, volume transaksi, dan tingkat pentingnya aktivitas dan fungsi tersebut terhadap bisnis BPR dan BPR Syariah;
      2) terkait dengan PPJTI seperti misalnya kondisi keuangan, kompetensi tenaga kerja, perputaran manajemen dan tenaga kerja, pengalaman PPJTI, dan profesionalitas; dan
      3) terkait dengan teknologi yang digunakan meliputi keandalan (*reliability*), keamanan (*security*), ketersediaan (*availability*), dan ketepatan waktu (*timeliness*) serta kemampuan mengikuti perkembangan teknologi dan perubahan ketentuan peraturan perundang-undangan.

2. Pengukuran Risiko

   Setelah risiko diidentifikasi, BPR dan BPR Syariah harus mengukur risiko tersebut untuk mengetahui tingkat risiko yang dihadapi. Pengukuran risiko penggunaan PPJTI harus terintegrasi dengan pengukuran risiko terkait TI lainnya dengan menggunakan pendekatan pengukuran risiko yang sama.

   Hasil pengukuran risiko penggunaan PPJTI ini harus menghasilkan suatu tingkat risiko yang selanjutnya menjadi salah satu parameter untuk penilaian risiko TI BPR dan BPR Syariah secara keseluruhan.

3. Mitigasi Risiko

   Dari hasil pengukuran risiko, BPR dan BPR Syariah mengetahui tingkat risiko yang dihadapi. Selanjutnya, BPR dan BPR Syariah harus menetapkan strategi mitigasi risiko sesuai dengan tingkat risiko tersebut. Tindakan mitigasi risiko yang dilakukan BPR dan BPR Syariah harus efektif untuk mengendalikan risiko.

   a. Contoh tindakan mitigasi risiko yang dapat dilakukan BPR dan BPR Syariah antara lain menerapkan kontrol untuk mengurangi kemungkinan terjadinya risiko, seperti:
      1) perjanjian kerja sama dengan PPJTI yang memadai;
      2) memantau kinerja penyedia jasa secara berkala; dan
      3) pemilihan PPJTI yang andal.

b. Tindakan mitigasi risiko lainnya adalah mengurangi dampak kerugian apabila risiko yang telah diidentifikasi terjadi seperti asuransi dan Rencana Pemulihan Bencana.

c. BPR dan BPR Syariah harus memastikan bahwa risiko ketergantungan pada PPJTI dapat dimitigasi sehingga BPR dan BPR Syariah tetap mampu menjalankan bisnisnya apabila PPJTI mengalami wanprestasi, pemutusan hubungan, atau dalam proses likuidasi. Mitigasi risiko yang dapat dilakukan mencakup:
   1) memastikan bahwa PPJTI memiliki Rencana Pemulihan Bencana sesuai dengan jenis, cakupan dan kompleksitas aktivitas atau jasa yang diberikan;
   2) secara aktif mendapatkan jaminan kesiapan Rencana Pemulihan Bencana milik PPJTI seperti pengujian secara berkala atas Rencana Pemulihan Bencana;
   3) memiliki perjanjian penyimpanan program kode sumber (*escrow agreement*), jika BPR dan BPR Syariah tidak memiliki kode sumber dari program aplikasi yang diselenggarakan oleh PPJTI; dan
   4) pemberian jaminan dari PPJTI kepada BPR dan BPR Syariah bahwa kelangsungan aplikasi didukung oleh pejabat pengembang perangkat lunak dalam hal kode sumber tidak dimiliki oleh PPJTI.

d. Dalam rangka menjamin fungsi dan efektivitas Rencana Pemulihan Bencana, BPR dan BPR Syariah harus menyusun dan melakukan pengujian Rencana Pemulihan Bencana secara berkala, lengkap, dan mencakup hal-hal yang signifikan yang didasarkan atas jenis, cakupan, dan kompleksitas aktivitas atau kegiatan yang dilakukan oleh PPJTI. Disamping itu, PPJTI harus melakukan pengujian Rencana Pemulihan Bencana di pihak penyedia jasa sendiri untuk sistem atau fasilitas TI maupun pemrosesan transaksi yang diselenggarakan tanpa melibatkan pihak BPR dan BPR Syariah. Hasil pengujian Rencana Pemulihan Bencana oleh PPJTI tersebut digunakan BPR dan BPR Syariah untuk mengkinikan Rencana Pemulihan Bencana yang dimiliki BPR dan BPR Syariah.

4. Pengendalian Risiko Lainnya

Meskipun BPR dan BPR Syariah maupun PPJTI sudah menggunakan sistem yang canggih namun masih memungkinkan adanya penyimpangan misalnya kesalahan manusia, penerapan prosedur yang lemah dan pencurian oleh pegawai. BPR dan BPR Syariah harus memastikan adanya pengendalian pengamanan untuk memitigasi risiko dan mencakup hal-hal:

a. PPJTI harus melakukan penelitian latar belakang para pegawainya;

b. memastikan kewajiban PPJTI melakukan pengendalian keamanan terhadap seluruh fasilitas TI yang digunakan dan data yang diproses serta informasi yang dihasilkan telah dicantumkan dalam perjanjian;

c. memastikan PPJTI memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan BPR dan BPR Syariah untuk masing-masing jenis data berdasarkan sensitivitas kerahasiaan data; dan

d. memastikan biaya yang dikeluarkan untuk masing-masing pengamanan sebanding dengan tingkat pengamanan yang dibutuhkan dan sesuai dengan tingkat toleransi risiko yang telah ditetapkan oleh BPR dan BPR Syariah.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN IV
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 43/PADK.03/2025
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH
BANK PEREKONOMIAN RAKYAT DAN
BANK PEREKONOMIAN RAKYAT SYARIAH

PEDOMAN KETAHANAN DAN KEAMANAN SIBER BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH

DAFTAR ISI

BAB I
MANAJEMEN RISIKO KETAHANAN DAN KEAMANAN SIBER

A. PENERAPAN MANAJEMEN RISIKO KETAHANAN DAN KEAMANAN SIBER

1. BPR dan BPR Syariah menerapkan ketahanan dan keamanan siber untuk mengatur pelindungan keamanan terhadap seluruh aset TI serta memastikan keberlangsungan operasional. Dalam penerapan ketahanan dan keamanan siber, BPR dan BPR Syariah perlu menerapkan manajemen risiko secara efektif.
2. Dalam penerapan manajemen risiko terkait ketahanan dan keamanan siber, diperlukan kecukupan kebijakan, prosedur, dan limit. BPR dan BPR Syariah mendokumentasikan kebijakan, prosedur, dan limit tersebut secara memadai.
3. Kebijakan sebagaimana dimaksud pada angka 2 mengatur antara lain koordinasi dan komunikasi antarunit kerja yang memiliki tanggung jawab terkait ketahanan dan keamanan siber.
4. Prosedur sebagaimana dimaksud pada angka 2 mengatur antara lain manajemen risiko terkait ketahanan dan keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga yang rutin dievaluasi dan diperbarui.
5. Penerapan manajemen risiko terkait keamanan siber mencakup 4 (empat) aspek, yaitu:
   a. tata kelola risiko terkait ketahanan dan keamanan siber yang meliputi kecukupan pengawasan aktif oleh Direksi dan Dewan Komisaris, perumusan tingkat risiko terkait ketahanan dan keamanan siber yang akan diambil (*risk appetite*) dan toleransi risiko terkait ketahanan dan keamanan siber (*risk tolerance*), serta budaya dan kesadaran risiko terkait ketahanan dan keamanan siber;
   b. kerangka manajemen risiko terkait ketahanan dan keamanan siber, yang meliputi strategi manajemen risiko, kecukupan perangkat organisasi, serta kecukupan kebijakan, prosedur, dan penetapan limit risiko, terkait ketahanan dan keamanan siber;
   c. proses manajemen risiko, kecukupan sumber daya manusia (SDM), serta kecukupan sistem informasi manajemen risiko, terkait ketahanan dan keamanan siber; dan
   d. sistem pengendalian risiko terkait ketahanan dan keamanan siber yang meliputi kecukupan sistem pengendalian intern dan kecukupan kaji ulang.
6. Penerapan manajemen risiko terkait ketahanan dan keamanan siber disesuaikan dengan karakteristik dan kompleksitas bisnis BPR dan BPR Syariah serta penyelenggaraan TI secara menyeluruh oleh BPR dan BPR Syariah.
7. BPR dan BPR Syariah memiliki sistem informasi manajemen risiko termasuk ketahanan dan keamanan siber, pengembangan sistem informasi manajemen risiko sesuai kebutuhan BPR dan BPR Syariah, serta melakukan kaji ulang secara berkala atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko terkait ketahanan dan keamanan siber.
8. BPR dan BPR Syariah harus mendokumentasikan daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif.

9. Proses manajemen risiko terkait ketahanan dan keamanan siber:
   a. Identifikasi risiko ketahanan dan keamanan siber
      Dalam melakukan identifikasi dan penilaian risiko ketahanan dan keamanan siber, BPR dan BPR Syariah terlebih dahulu harus memastikan adanya *risk awareness* di seluruh lini.
      Untuk dapat memastikan hal tersebut, BPR dan BPR Syariah dapat menjalankan *risk awareness program* bagi seluruh pegawai dan pengurus BPR dan BPR Syariah atau menjalankan metode lain yang dapat meningkatkan kesadaran para pengguna TI akan risiko ketahanan dan keamanan siber yang ada.
      BPR dan BPR Syariah mengidentifikasi kondisi ekstern dan intern dari serangan siber melalui analisis dampak bisnis (*Business Impact Analysis*).
      BPR dan BPR Syariah mengidentifikasi risiko dan menentukan prioritas risiko terkait ketahanan dan keamanan siber berdasarkan fungsi kritis, aset TI, interkoneksi sistem (*interconnectivity*), serta dituangkan dalam dokumen inventaris risiko (*risk register*). Dokumen *risk register* diperbarui secara berkala.
   b. Pengukuran risiko ketahanan dan keamanan siber
      BPR dan BPR Syariah perlu memperhatikan signifikansi dampak risiko yang telah diidentifikasi terhadap kondisi BPR dan BPR Syariah dan frekuensi terjadinya risiko. BPR dan BPR Syariah juga perlu melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko, termasuk pengukuran tingkat kerentanan terhadap risiko ketahanan dan keamanan siber secara berkala.
   c. Pemantauan risiko ketahanan dan keamanan siber
      BPR dan BPR Syariah melakukan pemantauan risiko TI dengan mengevaluasi kesesuaian, kecukupan, dan efektivitas kinerja penyelenggaraan TI.
   d. Pengendalian risiko ketahanan dan keamanan siber
      BPR dan BPR Syariah menerapkan praktik-praktik pengendalian yang memadai sebagai bagian dari strategi mitigasi risiko TI secara keseluruhan.
10. BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait ketahanan dan keamanan siber secara berkala menyesuaikan dengan perkembangan teknologi, insiden yang terjadi, dan/atau perubahan kondisi terkini lainnya.

B. PENGUJIAN KEAMANAN SIBER

1. Pengujian Keamanan Siber Berdasarkan Analisis Kerentanan

   BPR dan BPR Syariah melakukan pengujian keamanan siber berdasarkan analisis kerentanan untuk melihat titik lemah dari sistem BPR dan BPR Syariah. Pengujian ini dilaksanakan secara berkala berdasarkan evaluasi intern BPR dan BPR Syariah. Contoh faktor yang dapat mendasari penentuan frekuensi pengujian ini yaitu tingkat kritikalitas sistem dari hasil identifikasi aset TI BPR dan BPR Syariah dan adanya perubahan pada Sistem Elektronik atau arsitektur TI pada BPR dan BPR Syariah yang mengakibatkan peningkatan eksposur risiko terkait keamanan siber.

   Pengujian ini diawali dengan pelaksanaan identifikasi kerentanan (*vulnerability assessment*) yang kemudian dilanjutkan dengan *penetration test*. *Penetration test* merupakan pengujian yang

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

2. Pengujian Keamanan Siber Skenario

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

   a. *Table-top Exercise*

      Table-top exercise merupakan suatu kegiatan berbasis diskusi dimana SDM dengan peran dan tanggung jawab tertentu pada BPR dan BPR Syariah bertemu dalam suatu forum untuk mendiskusikan peran masing-masing selama keadaan darurat dan penanggulangan yang dilakukan terhadap situasi darurat tertentu. Tujuan utama dari *table-top exercise* adalah memastikan setiap anggota tim memahami apa yang harus dilakukan saat terjadi keadaan darurat, serta mengidentifikasi kekurangan dalam rencana tanggap darurat organisasi.

   b. *Cyber Range Exercise*

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

   c. *Social Engineering Exercise*

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

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

1) Pengujian dalam bentuk simulasi serangan harus dilakukan secara terkendali di bawah pengawasan ketat untuk memastikan pengujian tersebut tidak mengganggu sistem BPR dan BPR Syariah di lingkungan produksi; dan
2) skenario ancaman harus dirancang dan didasarkan pada ancaman siber yang mungkin terjadi. BPR dan BPR Syariah juga dapat merancang skenario melalui proses pencarian ancaman siber secara proaktif yang menyeluruh, antara lain dengan menggunakan analisis data serangan yang relevan dengan lingkungan TI BPR dan BPR Syariah untuk mengidentifikasi potensi pelaku ancaman, tujuan, metode serangan, serta indikator dan dampak serangan, termasuk mengidentifikasi taktik, teknik, serta prosedur yang dapat digunakan dalam serangan tersebut.

BAB II
INSIDEN SIBER

A. INSIDEN SIBER

1. Insiden TI yaitu kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI, berupa:
   a. insiden siber; dan
   b. insiden nonsiber.
2. Insiden siber terjadi karena terganggunya keamanan siber. Insiden siber merupakan ancaman siber berupa upaya, kegiatan, dan/atau tindakan yang mengakibatkan Sistem Elektronik tidak berfungsi sebagaimana mestinya. Beberapa contoh ancaman siber:
   a. *Malware*
      Malware merupakan perangkat lunak dengan fitur atau kemampuan yang berpotensi mengganggu suatu sistem informasi. Gangguan dimaksud dapat menimbulkan kerugian bagi pemilik sistem informasi, baik secara langsung maupun tidak langsung.
   b. *Web defacement*
      Web defacement merupakan serangan yang dilakukan terhadap situs web dengan cara mengganti atau memodifikasi situs web sehingga isi dari situs web berubah sesuai dengan keinginan penyerang.
   c. *Denial of Service* (*DoS*) dan *Distributed Denial of Service* (*DDoS*)
      DoS dan DDoS merupakan serangan yang bertujuan untuk mengganggu keberlangsungan operasional (*availability*) suatu Sistem Elektronik dalam memproses transaksi atau akses yang sah, antara lain dengan cara membuat kapasitas jaringan atau kapasitas komputer seolah-olah telah terpakai penuh karena adanya permintaan akses dalam volume yang besar.
3. BPR dan BPR Syariah memiliki prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan yang diuji secara berkala.
4. BPR dan BPR Syariah memiliki prosedur notifikasi kepada regulator atau lembaga eksternal yang menetapkan batas waktu, media, dan tanggung jawab pelaporan setelah terjadinya insiden siber.
5. BPR dan BPR Syariah memiliki matriks eskalasi insiden siber yang mengategorisasikan kejadian berdasarkan tingkat keparahan/prioritas/dampak dan jalur komunikasi pelaporan.
6. BPR dan BPR Syariah memiliki prosedur tertulis ketahanan dan keamanan siber terkait pelaporan kejadian mencurigakan dan disosialisasikan kepada seluruh pegawai.
7. BPR dan BPR Syariah melaksanakan simulasi tanggap insiden siber secara berkala dan terdokumentasi.
8. BPR dan BPR Syariah menetapkan mekanisme untuk melakukan evaluasi kesesuaian prosedur dan *root cause analysis* serta dilakukan tindak lanjut pascainsiden siber.
9. BPR dan BPR Syariah memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber yang telah ditetapkan oleh Direksi. Prosedur didokumentasikan secara memadai dan dikomunikasikan kepada seluruh pegawai.
10. BPR dan BPR Syariah memiliki mekanisme komunikasi kepada nasabah dan publik ketika insiden siber terjadi.
    Mekanisme komunikasi mencakup, antara lain penetapan saluran resmi, proses persetujuan pesan, dan panduan pertanyaan-jawaban, serta melakukan pelatihan atas mekanisme tersebut.

11. BPR dan BPR Syariah memiliki dan menerapkan prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber.
12. Dalam hal terjadi insiden, BPR dan BPR Syariah menetapkan mekanisme proses eradikasi *malware* atau artefak serangan, termasuk pembersihan *file*, *patch* kerentanan, dan verifikasi bahwa sistem telah steril sebelum dikembalikan ke produksi.
13. BPR dan BPR Syariah perlu melakukan pemantauan atas insiden siber sebagai bentuk komunikasi kepada para pemangku kepentingan serta pengendalian atas pengelolaan ketahanan dan keamanan siber.
14. Kegiatan pemantauan insiden siber dapat bermanfaat bagi BPR dan BPR Syariah dalam melakukan penanggulangan dan pemulihan terhadap Sistem Elektronik BPR dan BPR Syariah sehingga kegiatan operasional BPR dan BPR Syariah tetap dapat berjalan sebagaimana mestinya.
15. BPR dan BPR Syariah melakukan kaji ulang secara berkala terhadap Rencana Pemulihan Bencana, termasuk Rencana Pemulihan Bencana insiden siber dengan mempertimbangkan hasil uji coba, termasuk dalam hal BPR dan BPR Syariah melakukan perubahan yang signifikan terhadap sistem, aplikasi, atau infrastruktur TI, misalnya perubahan pada Aplikasi Inti Perbankan. Kaji ulang Rencana Pemulihan Bencana termasuk melakukan pengujian *failover*.

B. TIM TANGGAP INSIDEN SIBER

Fungsi yang menangani ketahanan dan keamanan siber mengoordinasikan tim tanggap insiden siber, termasuk inisiasi pembentukannya, dengan memastikan bahwa:

1. pegawai yang terlibat dalam tim tanggap insiden siber memiliki pemahaman terkait penanganan insiden siber, yaitu dengan melakukan latihan respons insiden secara rutin, antara lain berupa pengujian saluran komunikasi, analisis insiden, pengambilan keputusan dan rekomendasi solusi, serta kemampuan teknis pelaporan insiden;
2. tim tanggap insiden siber dapat bekerja sama dengan unit atau fungsi terkait (seperti unit bisnis dan SDM) dan mampu mengakses informasi yang diperlukan dengan cepat (antara lain informasi dari penyedia jasa pihak ketiga atau informasi pendukung lainnya);
3. tim tanggap insiden siber memiliki kemampuan analisis insiden (antara lain daftar *host*, *packet sniffer*, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, perangkat forensik digital, dan sumber daya lain yang diperlukan);
4. tim tanggap insiden siber dapat bekerja sama dengan fungsi intelijen ancaman siber (*cyber threat intelligence*) dan *network operations* untuk menghasilkan penanganan insiden siber yang tepat dan proaktif terhadap potensi insiden siber di masa depan;
5. tim tanggap insiden siber dipimpin oleh pejabat yang berasal dari fungsi yang menangani ketahanan dan keamanan siber; dan
6. tim tanggap insiden siber menunjuk salah satu anggota tim tanggap insiden siber sebagai narahubung untuk mendukung koordinasi dalam pelaksanaan tugas.

C. LAPORAN INSIDEN SIBER

1. BPR dan BPR Syariah menyampaikan informasi mengenai insiden siber kepada Otoritas Jasa Keuangan berupa:
   a. notifikasi awal insiden siber; dan
   b. laporan insiden siber.
2. Notifikasi awal insiden siber disampaikan oleh BPR dan BPR Syariah dengan ketentuan sebagai berikut:
   a. Notifikasi awal disusun menggunakan format sebagaimana tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini. Notifikasi awal berisi informasi awal yang tersedia terkait insiden siber pada BPR dan BPR Syariah.
   b. Notifikasi awal disampaikan kepada Otoritas Jasa Keuangan paling lama 24 (dua puluh empat) jam setelah insiden siber diketahui oleh BPR dan BPR Syariah ditujukan kepada satuan kerja pengawasan dari BPR dan BPR Syariah yang bersangkutan melalui sarana elektronik secara tertulis. BPR dan BPR Syariah melakukan upaya untuk memastikan bahwa notifikasi awal telah diterima oleh Otoritas Jasa Keuangan.
3. Sebagai tindak lanjut dari notifikasi awal insiden siber yang telah disampaikan, BPR dan BPR Syariah melakukan analisis dan penanggulangan insiden siber lebih lanjut. Tindak lanjut ini disampaikan melalui laporan insiden siber kepada Otoritas Jasa Keuangan dengan ketentuan sebagai berikut:
   a. Laporan insiden siber disusun menggunakan format sebagaimana tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Anggota Dewan Komisioner Otoritas Jasa Keuangan ini. Laporan insiden siber berisi informasi yang lebih lengkap dari informasi yang telah disampaikan pada notifikasi awal.
   b. Laporan insiden siber disampaikan secara daring melalui sistem pelaporan Otoritas Jasa Keuangan paling lama 7 (tujuh) hari kerja setelah insiden siber diketahui.
4. Dalam hal terdapat pengaturan otoritas lain mengenai penyampaian notifikasi awal dan/atau laporan insiden siber, BPR dan BPR Syariah menyampaikan notifikasi awal dan/atau laporan insiden siber kepada Otoritas Jasa Keuangan dengan ketentuan sebagai berikut:
   a. dalam hal otoritas lain mengatur jangka waktu yang lebih cepat daripada jangka waktu sebagaimana diatur dalam POJK PTI BPR dan BPR Syariah maka BPR dan BPR Syariah menyampaikan notifikasi awal dan/atau laporan insiden siber kepada Otoritas Jasa Keuangan pada saat yang bersamaan sesuai dengan ketentuan peraturan perundang-undangan otoritas lain dimaksud.

      Contoh:

      Ketentuan otoritas “A”

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

      BPR “B” mengalami insiden siber pada tanggal 9 Februari 2026 pukul 13.00 WITA. Mengingat jangka waktu penyampaian

notifikasi awal dan/atau laporan insiden siber berdasarkan ketentuan otoritas "A" lebih cepat daripada yang diatur dalam POJK PTI BPR dan BPR Syariah, maka BPR "B" menyampaikan notifikasi awal dalam kurun waktu 1 (satu) jam setelah insiden siber diketahui. Apabila BPR "B" menyampaikan notifikasi awal insiden siber kepada otoritas "A" pada pukul 13.45 WITA maka BPR "B" juga menyampaikan notifikasi awal kepada Otoritas Jasa Keuangan pada saat yang bersamaan.

Hal yang sama juga berlaku untuk penyampaian laporan insiden siber. Apabila BPR "B" menyampaikan laporan insiden siber pada tanggal 12 Februari 2026 pukul 10.00 WITA kepada otoritas "A" maka BPR "B" juga menyampaikan laporan insiden siber kepada Otoritas Jasa Keuangan pada saat yang bersamaan.

b. dalam hal otoritas lain mengatur jangka waktu yang lebih lama daripada jangka waktu sebagaimana diatur dalam POJK PTI BPR dan BPR Syariah maka BPR dan BPR Syariah menyampaikan notifikasi awal dan/atau laporan insiden siber kepada Otoritas Jasa Keuangan sesuai dengan POJK PTI BPR dan BPR Syariah.

Contoh:

Ketentuan otoritas "C"

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

BPR Syariah "D" mengalami insiden siber pada tanggal 9 Februari 2026 pukul 13.00 WITA. Mengingat jangka waktu penyampaian notifikasi awal dan/atau laporan insiden siber berdasarkan ketentuan otoritas "B" lebih lama daripada yang diatur dalam POJK PTI BPR dan BPR Syariah, maka BPR Syariah "D" menyampaikan notifikasi awal kepada Otoritas Jasa Keuangan dalam kurun waktu 24 (dua puluh empat) jam setelah insiden siber diketahui.

Hal yang sama juga berlaku untuk penyampaian laporan insiden siber. BPR Syariah "D" menyampaikan laporan insiden siber kepada Otoritas Jasa Keuangan dalam kurun waktu 7 (tujuh) hari kerja setelah insiden siber diketahui, yaitu pada tanggal 18 Februari 2026.

BAB III
PEDOMAN PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER

A. PENJELASAN UMUM PEDOMAN PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER

1. Kertas kerja Penilaian Tingkat Maturitas Keamanan Siber terdiri atas 5 (lima) domain, yaitu:

No.	Domain	Tujuan Domain
1	Tata Kelola	Untuk memastikan bahwa tata kelola keamanan siber BPR dan BPR Syariah selaras dengan arah strategis, nilai-nilai, dan sasaran bisnis BPR dan BPR Syariah.
2	Identifikasi	Untuk memastikan BPR dan BPR Syariah telah membangun pemahaman yang menyeluruh mengenai risiko siber yang dihadapi, serta mengidentifikasi sumber daya penting (informasi, *software*, *hardware*, jaringan, SDM) yang harus dilindungi sehingga BPR dan BPR Syariah dapat mengelola risiko siber secara sistematis, menyeluruh, dan berkelanjutan.
3	Pelindungan	Untuk membatasi atau menahan dampak dari potensi insiden siber sehingga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dari data dan sistem BPR dan BPR Syariah tetap terjaga.
4	Deteksi	Untuk mengidentifikasi kejadian siber secara cepat melalui aktivitas pemantauan dan analisis yang berkelanjutan.
5	Penanggulangan dan Pemulihan	Untuk merespons insiden keamanan siber secara sistematis dan efektif, serta mengembalikan kondisi operasional normal dan meningkatkan ketahanan sistem di masa depan.

2. Penilaian terhadap 5 (lima) domain sebagai berikut:

No.	Domain	Subdomain	Tujuan Domain
1	Tata Kelola	Konteks Organisasi	untuk mengukur ketersediaan peran Direksi, Dewan Komisaris, dan unit/fungsi terkait lainnya terkait pengamanan siber, termasuk kebijakan dan prosedur perangkat kerja terkait pengamanan siber.
2	Identifikasi	Pengukuran risiko siber	untuk memastikan BPR dan BPR Syariah telah melakukan penilaian terhadap potensi

			ancaman dan kerentanan yang dapat mempengaruhi capaian tujuan bisnis.
3	Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	untuk memastikan bahwa kebijakan akses kontrol terhadap sistem, aset, dan data telah diterapkan secara konsisten, serta hak akses hanya diberikan kepada individu atau entitas yang berwenang.
		Keamanan data	untuk memastikan BPR dan BPR Syariah telah menerapkan mekanisme perlindungan terhadap data selama proses penyimpanan, pemrosesan, dan transmisi, termasuk enkripsi, pemantauan akses, dan klasifikasi data sesuai sensitivitasnya.
		Kesadaran dan pelatihan	untuk memastikan seluruh pegawai BPR dan BPR Syariah menerima pelatihan keamanan siber secara berkala guna meningkatkan kesadaran terhadap risiko dan tanggung jawab masing-masing dalam upaya mencegah terjadinya insiden siber.
4	Deteksi	Analisis Kejadian Mencurigakan	untuk memastikan agar BPR dan BPR Syariah melakukan analisis yang komprehensif terhadap setiap aktivitas mencurigakan yang berpotensi menyebabkan insiden siber, dengan cakupan karakteristik, sumber, metode serangan, dampak, dan proses eskalasi.
		Ketahanan Infrastruktur TI	untuk memastikan BPR dan BPR Syariah telah merancang dan memelihara infrastruktur teknologi

			yang tangguh, mampu beroperasi secara berkelanjutan, serta memiliki kemampuan adaptif terhadap gangguan atau serangan siber.
5	Penanggulangan dan Pemulihan	Analisis Insiden	untuk memastikan BPR dan BPR Syariah menganalisis insiden siber yang terjadi untuk menentukan akar penyebab, pola serangan, serta dampak terhadap aset dan operasional.
		Pelaksanaan Rencana Pemulihan Insiden Siber	untuk memastikan BPR dan BPR Syariah melaksanakan Rencana Pemulihan Bencana (*Disaster Recovery Plan* – DRP) terkait siber yang telah disusun, dengan cakupan kegiatan meliputi: pengaktifan DRC, pemulihan sistem, dan proses validasi atas integritas data/sistem sebelum kembali digunakan.

B. TATA CARA PENGISIAN KERTAS KERJA PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER

1. Setiap BPR dan BPR Syariah melakukan pengisian Kertas Kerja Penilaian Tingkat Maturitas Keamanan Siber yang terdiri atas 5 (lima) domain penilaian. Pengisian kertas kerja dilakukan sesuai dengan kompleksitas dan kegiatan usahanya dengan perincian sebagai berikut:

Kategori	Subjek	Jumlah Indikator
Kategori 1	BPR atau BPR Syariah yang Menyelenggarakan Layanan Digital dan/atau Terhubung dengan Sistem Aplikasi dan/atau Infrastruktur Teknologi Informasi Mitra Kerja	80
Kategori 2	BPR atau BPR Syariah yang Menyelenggarakan Layanan Perbankan Dasar	60

2. Tahap Penetapan Peringkat Maturitas Keamanan Siber
   a. Penilaian tingkat maturitas keamanan siber terdiri dari 5 (lima) domain dengan bobot setiap domain sebagai berikut:
      1) Tata Kelola, dengan bobot 25% (dua puluh lima persen);
      2) Identifikasi, dengan bobot 15% (lima belas persen);
      3) Pelindungan, dengan bobot 25% (dua puluh lima persen);
      4) Deteksi, dengan bobot 15% (lima belas persen); dan

5) Penanggulangan dan Pemulihan, dengan bobot 20% (dua puluh persen).

Setiap domain terdiri dari subdomain, dan setiap subdomain memiliki beberapa indikator.

b. Setiap BPR dan BPR Syariah menetapkan 1 (satu) peringkat pada setiap parameter berdasarkan data dan informasi yang sesuai dengan kondisi sebenarnya.

Peringkat parameter terdiri dari:

1) Peringkat 1 (sangat memadai);
2) Peringkat 2 (memadai);
3) Peringkat 3 (cukup memadai);
4) Peringkat 4 (kurang memadai); dan
5) Peringkat 5 (tidak memadai);

Peringkat 1 mencerminkan kondisi paling memadai yang ditunjukkan dengan keberadaan kebijakan, prosedur, dan dokumen terkait Ketahanan dan Keamanan Siber (KKS) secara formal dan dilakukan evaluasi dan/atau penginian secara berkala, serta pelaksanaan proses atau aktivitas dalam KKS yang telah dilaksanakan secara konsisten dan memadai.

Peringkat 5 mencerminkan kondisi paling tidak memadai dalam penerapan KKS yang ditunjukkan antara lain ketidakcukupan kebijakan, prosedur, dan dokumen terkait KKS secara formal, serta pelaksanaan proses dan/atau aktivitas dalam KKS yang tidak memadai.

c. Hasil rata-rata peringkat parameter dari setiap domain disebut dengan peringkat domain.

d. Penjumlahan dari peringkat domain sebagaimana huruf b) dikalikan dengan bobot setiap domain sebagaimana huruf a) disebut dengan nilai komposit. Penetapan peringkat komposit maturitas keamanan siber dilakukan berdasarkan rentang nilai komposit.

e. Penetapan peringkat komposit maturitas keamanan siber terdiri dari 5 (lima) peringkat dengan rentang nilai komposit sebagai berikut:

Peringkat Komposit	Nilai Komposit	Karakteristik
Peringkat 1 (Sangat Memadai)	1.00 – 1.80	• Kebijakan, prosedur, dan dokumen terkait KKS secara formal dan dilakukan evaluasi dan/atau penginian secara berkala. • Pelaksanaan proses atau aktivitas dalam KKS yang telah dilaksanakan secara konsisten dan sangat memadai. • Kerentanan rendah. • Kesadaran siber pegawai dan nasabah sangat memadai.
Peringkat 2 (Memadai)	1.81 – 2.60	• Kebijakan, prosedur, dan dokumen terkait KKS secara formal dan dilakukan evaluasi dan/atau penginian secara berkala.

		• Pelaksanaan proses atau aktivitas dalam KKS yang telah dilaksanakan secara konsisten dan memadai. • Kerentanan rendah. • Kesadaran siber pegawai dan nasabah memadai.
Peringkat 3 (Cukup Memadai)	2.61 – 3.40	• Kebijakan, prosedur, dan dokumen terkait KKS secara formal dan dilakukan evaluasi dan/atau penginian belum secara berkala. • Pelaksanaan proses atau aktivitas dalam KKS yang telah dilaksanakan, namun belum konsisten dan menyeluruh. • Kerentanan rendah. • Kesadaran siber pegawai dan nasabah cukup memadai.
Peringkat 4 (Kurang Memadai)	3.41 – 4.20	• Kebijakan, prosedur, dan dokumen terkait KKS secara formal dan dilakukan evaluasi dan/atau penginian dilakukan dalam hal terjadi insiden siber yang berdampak signifikan. • Pelaksanaan proses atau aktivitas dalam KKS yang telah dilaksanakan, namun belum konsisten dan menyeluruh. • Kerentanan cukup tinggi • Kesadaran siber pegawai dan nasabah kurang memadai.
Peringkat 5 (Tidak Memadai)	4.21 – 5.00	• Ketidakcukupan bahkan ketiadaan kebijakan, prosedur, dan dokumen terkait KKS secara formal. • Pelaksanaan proses atau aktivitas dalam KKS yang telah dilaksanakan belum memadai. • Kerentanan tinggi. • Kesadaran siber pegawai dan nasabah belum memadai.

C. KERTAS KERJA PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER

Tabel 1. Kertas Kerja Penilaian BPR dan BPR Syariah Kategori 1

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
1	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah menetapkan wewenang dan tanggung jawab Direksi dan Dewan Komisaris secara tertulis dalam penerapan manajemen risiko terkait keamanan siber.	
2	Tata Kelola	Konteks Organisasi	Direksi menetapkan tingkat risiko (*risk appetite*) terkait keamanan siber.	
3	Tata Kelola	Konteks Organisasi	Strategi ketahanan dan keamanan siber BPR dan BPR Syariah telah dirumuskan untuk mendukung serta selaras dengan visi dan misi BPR dan BPR Syariah (misalnya target pertumbuhan layanan digital, standar keamanan nasabah, dan *risk appetite* yang telah ditetapkan), termasuk melakukan kaji ulang strategi keamanan siber secara berkala untuk menentukan perlu atau tidaknya dilakukan perubahan.	
4	Tata Kelola	Konteks Organisasi	Direksi mengomunikasikan strategi, kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber secara efektif kepada seluruh satuan kerja dan pegawai agar dipahami secara jelas.	
5	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber.	
6	Tata Kelola	Konteks Organisasi	Direksi memastikan bahwa struktur organisasi serta strategi manajemen risiko keamanan siber BPR dan BPR Syariah telah mencantumkan peran dan tanggung jawab yang jelas terkait keamanan siber.	
7	Tata Kelola	Konteks Organisasi	Direksi memastikan seluruh SDM memahami risiko keamanan siber beserta strategi manajemen risikonya (*risk-appetite*, *zero risk-tolerance*, kerangka kerja) dan	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
			mampu mengomunikasikan serta menerapkannya secara konsisten.	
8	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki kebijakan ketahanan dan keamanan siber secara tertulis yang telah ditetapkan oleh Direksi. Kebijakan ketahanan dan keamanan siber dievaluasi secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau lebih dalam hal terdapat perubahan yang signifikan terhadap kegiatan usaha BPR dan BPR Syariah.	
9	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah menerapkan *baseline* kontrol proteksi pada seluruh aset TI (antara lain meliputi *hardening*, *patch*, *anti-malware*/EDR, *firewall* dan segmentasi jaringan, pengendalian akses, serta enkripsi), sesuai kebijakan dan prosedur, serta memantau dan mengevaluasi efektivitasnya secara berkala.	
10	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur koordinasi dan komunikasi antarunit kerja yang memiliki tanggung jawab terkait ketahanan dan keamanan siber.	
11	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga yang rutin dievaluasi dan diperbarui.	
12	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah mempunyai daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif, serta antara BPR dan BPR Syariah dan pihak ketiga terdapat perjanjian kerja sama yang mencakup aspek ketahanan dan keamanan siber.	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
13	Tata Kelola	Konteks Organisasi	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber harus didokumentasikan secara memadai.	
14	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko terkait keamanan siber secara berkala.	
15	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki sistem informasi manajemen risiko terkait keamanan siber dan mengembangkannya sesuai kebutuhan BPR dan BPR Syariah.	
16	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memastikan sistem informasi manajemen risiko terkait keamanan siber dan informasi yang dihasilkan telah sesuai dengan karakteristik dan kompleksitas kegiatan usaha BPR dan BPR Syariah serta adaptif terhadap perubahan.	
17	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melakukan kaji ulang secara berkala atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko terkait keamanan siber.	
18	Tata Kelola	Konteks Organisasi	Sebagai bagian dari sistem informasi manajemen risiko, laporan tingkat maturitas keamanan siber disusun secara berkala oleh fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber.	
19	Tata Kelola	Konteks Organisasi	Fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber menyampaikan laporan berkala kepada Direksi.	
20	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melaksanakan audit intern atas penyelenggaraan TI secara berkala, termasuk terhadap pengelolaan ketahanan dan keamanan siber.	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
21	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara berkala.	
22	Tata Kelola	Konteks Organisasi	Direksi mengembangkan budaya dan membangun serta memelihara kesadaran dan komitmen yang kuat mengenai tanggung jawab terkait keamanan siber bagi pegawai di semua level.	
23	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber secara berkala.	
24	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan penyimpanan *log* yang memiliki periode retensi untuk keperluan audit dan investigasi insiden siber sesuai dengan kebijakan/prosedur.	
25	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan klasifikasi data dan/atau informasi berdasarkan tingkat kritikalitas dan sensitivitas sesuai dengan kebijakan/prosedur.	
26	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah menerapkan pengamanan data dan/atau informasi berdasarkan klasifikasi data dan/atau informasi sesuai dengan kebijakan/prosedur.	
27	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melaksanakan analisis dampak bisnis (*Business Impact Analysis*) untuk mengidentifikasi kemungkinan kondisi ekstern dan intern dari serangan siber.	
28	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melaksanakan pengujian keamanan secara berkala, antara lain *vulnerability assessment* dan *penetration testing*, terhadap perangkat lunak dan perangkat keras yang digunakan dalam operasional BPR dan BPR Syariah maupun layanan kepada nasabah dan/atau pihak ketiga.	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
29	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan kaji ulang secara berkala terhadap kebijakan ketahanan dan keamanan siber untuk menyesuaikan dengan perkembangan teknologi, insiden yang terjadi, dan/atau perubahan kondisi terkini lainnya.	
30	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah mengidentifikasi risiko dan menentukan prioritas risiko terkait ketahanan dan keamanan siber berdasarkan fungsi kritis, aset TI, interkoneksi sistem (*interconnectivity*), serta dituangkan dalam dokumen inventaris risiko (*risk register*). Dokumen *risk register* diperbarui secara berkala.	
31	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan identifikasi aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta melakukan pencatatan dalam daftar inventaris TI, yang diperbarui secara berkala.	
32	MR Pelindungan	Kesadaran & Pelatihan	BPR dan BPR Syariah memberikan pelatihan ketahanan dan keamanan siber secara berkala kepada seluruh pegawai.	
33	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melakukan *hardening* atas perangkat kerja sesuai dengan kebijakan dan prosedur tertulis, antara lain: a. Seluruh perangkat komputer BPR dan BPR Syariah dilengkapi dengan *anti-malware* yang dikinikan secara otomatis dan berkala; b. *Port* USB terkait penyimpanan data pada perangkat komputer BPR dan BPR Syariah dibatasi penggunaannya; c. Perangkat komputer terkunci secara otomatis pada saat perangkat tidak aktif untuk beberapa saat; dan d. Seluruh perangkat komputer BPR dan BPR Syariah dipasang dengan *firewall* lokal (*host based firewall*).	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
34	MR Pelindungan	Konteks Organisasi	Surat elektronik (*email*) korporasi dilindungi sistem pengecekan otomatis *spam*, *phishing*, *dan malware*.	
35	MR Pelindungan	Kesadaran & Pelatihan	BPR dan BPR Syariah melakukan simulasi *phishing* dengan cara mengirimkan *emailblast* kepada seluruh pegawai untuk mengukur respons terhadap phishing dan serangan surat elektronik (*email*) serupa setidaknya sekali setiap tahun.	
36	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah menerapkan pengendalian akses berbasis peran (*Role Based Access Control*–RBAC) terhadap seluruh sistem.	
37	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	Setiap pegawai menggunakan *single* ID yang unik dan kata sandi pribadi untuk mengakses perangkat komputer.	
38	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah menerapkan kontrol operasional manajemen akses pengguna pada seluruh sistem, termasuk penegakan otomatis kompleksitas kata sandi, masa kedaluwarsa, riwayat, dan penguncian akun (*lockout*) sesuai dengan kebijakan/prosedur yang telah ditetapkan.	
39	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melakukan pemisahan jaringan dengan menggunakan *Service Set Identifier* (SSID) terpisah untuk pegawai dan tamu/pengunjung, serta menerapkan pengamanan teknis (misalnya *Virtual Local Area Network* - VLAN) untuk membatasi akses.	
40	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah menerapkan kontrol operasional siklus hidup aset TI yang meliputi inventarisasi dan	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
			identifikasi *End-of-Life* (EOL) dan *End-of-Support* (EOS), menjalankan *patching*/*upgrade* secara terjadwal, serta menarik atau mengisolasi dari produksi setiap perangkat yang mencapai EOL/EOS sesuai dengan kebijakan/prosedur yang telah ditetapkan.	
41	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah menerapkan kontrol akses operasional saat pegawai pindah/berhenti, yaitu hak akses disesuaikan atau dinonaktifkan tepat waktu, dan seluruh perubahan tercatat di *log* sesuai dengan kebijakan/prosedur yang ditetapkan.	
42	MR Pelindungan	Keamanan Data	BPR dan BPR Syariah menghapus (*wipe*) seluruh data pada perangkat kerja sebelum perangkat dimusnahkan/dialihkan. Selanjutnya hasilnya akan diverifikasi dan buktinya dicatat, sesuai dengan kebijakan/prosedur yang ditetapkan.	
43	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melindungi ruang *server*/pusat data (*data center*) dengan kontrol akses fisik, antara lain kunci, kartu akses, dan/atau biometrik, serta memiliki dokumentasi terhadap akses.	
44	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah memiliki prosedur persetujuan resmi terkait permintaan akses ke sistem kritikal yang disertai dengan dokumentasi.	
45	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	Pengguna dengan *role administrator* di BPR dan BPR Syariah (staf TI/vendor) memakai akun admin terpisah dari akun harian. Akun admin hanya untuk tugas *privileged*.	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
46	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	Seluruh sistem kritikal dilindungi dengan otentikasi multifaktor (*Multi Factor Authentication* - MFA).	
47	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah melakukan audit berkala terhadap hak akses pegawai berdasarkan klasifikasi data dan informasi.	
48	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah memiliki fitur yang secara otomatis memblokir koneksi dari atau ke alamat internet berbahaya (*firewall*), berdasarkan informasi dari penyedia *threat intelligence*.	
49	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	Instalasi perangkat lunak BPR dan BPR Syariah hanya dapat dilakukan oleh Satuan Kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI atau pihak lain dengan otorisasi dari pihak penyelenggara TI.	
50	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melakukan klasifikasi antara jaringan untuk sistem kritikal dengan jaringan umum (contoh: surat elektronik).	
51	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah menerapkan klasifikasi jaringan yang terpisah untuk layanan ATM/CDM/EDC disertai dengan enkripsi *end-to-end* atau VPN.	
52	MR Pelindungan	Konteks Organisasi	BPRdan BPR Syariah melakukan pembaruan (*update*) sistem dan aplikasi secara berkala, termasuk *patch* keamanan.	
53	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melindungi mesin ATM/CDM/EDC dengan proteksi fisik (antara lain *seal* dan CCTV) dan	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
			proteksi sistem (antara lain *anti-Malware* dan *Operating System* - OS *Lock*).	
54	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah memiliki prosedur tertulis terkait *change management* untuk meninjau seluruh perubahan konfigurasi.	
55	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah memisahkan lingkungan antara sistem produksi dengan pengembangan tanpa berbagi data atau infrastruktur.	
56	MR Pelindungan	Keamanan Data	BPR dan BPR Syariah melakukan enkripsi data penting (antara lain data transaksi, data nasabah, dan laporan internal) dengan menggunakan standar industri.	
57	MR Pelindungan	Keamanan Data	BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data termasuk namun tidak terbatas pada pelindungan data, transfer data, dan penghapusan data.	
58	MR Pelindungan	Kesadaran & Pelatihan	BPR dan BPR Syariah secara berkala melakukan edukasi kepada Nasabah mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi melalui berbagai kanal komunikasi.	
59	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk sistem kritikal.	
60	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut (*Attribute Based Access Control* - ABAC) untuk sistem kritikal (misalnya *Core Banking System*).	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
			Penerapan ABAC dilakukan dengan mempertimbangkan faktor antara lain lokasi, waktu, perangkat, dan tingkat risiko.	
61	MR Pelindungan	Keamanan Data	BPR dan BPR Syariah yang memberikan layanan digital menerapkan *Data Loss Prevention* (DLP) pada *endpoint* dan *gateway*.	
62	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah menerapkan pembatasan nominal transaksi dan jenis transaksi.	
63	MR Deteksi	Ketahanan Infrastruktur TI	Apabila terjadi percobaan *login* gagal, sistem kritikal BPR dan BPR Syariah akan memantau, mengirimkan *alert* otomatis ke Tim Keamanan, serta mengunci akun setelah ambang batas (*threshold*) percobaan terlampaui, guna mendeteksi lebih dini terhadap upaya serangan siber.	
64	MR Deteksi	Ketahanan Infrastruktur TI	Perangkat Kerja BPR dan BPR Syariah telah dilindungi dengan sistem keamanan berbasis perilaku yang mampu mendeteksi perilaku mencurigakan dan serangan yang belum dikenal. Sistem keamanan berbasis perilaku misalnya *Endpoint Detection and Response* (EDR).	
65	MR Deteksi	Analisis Kejadian Mencurigakan	Layanan *Mobile Banking* BPR dan BPR Syariah dilengkapi dengan mekanisme deteksi berbasis perilaku dan pemberitahuan *real-time* atas transaksi tidak biasa (*unusual transaction*).	
66	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan yang diuji secara berkala.	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
67	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki matriks eskalasi insiden siber yang mengategorisasikan kejadian berdasarkan tingkat keparahan/prioritas/dampak dan jalur komunikasi pelaporan.	
68	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki prosedur tertulis ketahanan dan keamanan siber terkait pelaporan kejadian mencurigakan dan disosialisasikan kepada seluruh pegawai.	
69	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah melaksanakan simulasi tanggap insiden siber secara berkala dan terdokumentasi.	
70	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah menetapkan mekanisme untuk melakukan evaluasi kesesuaian prosedur dan *root cause analysis* serta dilakukan tindak lanjut pascainsiden siber.	
71	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber yang telah ditetapkan oleh Direksi. Prosedur didokumentasikan secara memadai dan dikomunikasikan kepada seluruh pegawai.	
72	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki dan menerapkan prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber.	
73	MR Penanggulangan & Pemulihan	Analisis Insiden	Dalam hal terjadi insiden, BPR dan BPR Syariah segera membatasi dan mengisolasi (eradikasi) sistem yang diduga terinfeksi *malware* atau diserang, sesuai prosedur teknis yang diterapkan sebelum layanan dipulihkan.	
74	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah memiliki Rencana Pemulihan Bencana (*Disaster Recovery Plan*) dan mengimplementasikannya guna memulihkan layanan apabila terjadi insiden.	

No	Domain	Subdomain	Parameter Penilaian	Peringkat Parameter
75	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah wajib melakukan rekam cadang (*back up*) setiap akhir hari untuk seluruh data aktivitas BPR dan BPR Syariah.	
76	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah melakukan pengujian *restorebackup* data secara berkala paling sedikit 1 (satu) kali dalam 1(satu) tahun.	
77	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah melakukan analisis kritikalitas sistem penting dengan menetapkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	
78	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah melakukan kaji ulang terhadap rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) insiden siber secara berkala, termasuk melakukan pengujian *failover*.	
79	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah memiliki prosedur notifikasi kepada regulator ataupun lembaga eksternal (misal OJK, BI, dan lain-lain) yang menetapkan batas waktu, media, dan tanggung jawab pelaporan setelah terjadinya insiden siber.	
80	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah menetapkan mekanisme komunikasi kepada nasabah dan publik ketika insiden siber terjadi. Mekanisme komunikasi meliputi: penetapan saluran resmi, proses persetujuan pesan, dan panduan pertanyaan-jawaban, serta melakukan pelatihan atas mekanisme tersebut.	

Tabel 2. Kertas Kerja Penilaian BPR Kategori 2

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
1	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah menetapkan wewenang dan tanggung jawab Direksi dan Dewan Komisaris secara tertulis dalam penerapan manajemen risiko terkait keamanan siber.	
2	Tata Kelola	Konteks Organisasi	Direksi menetapkan tingkat risiko (*risk appetite*) terkait keamanan siber.	
3	Tata Kelola	Konteks Organisasi	Strategi ketahanan dan keamanan siber BPR dan BPR Syariah telah dirumuskan untuk mendukung serta selaras dengan visi dan misi BPR dan BPR Syariah (misalnya standar keamanan nasabah, dan *risk-appetite* yang telah ditetapkan), termasuk melakukan kaji ulang strategi keamanan siber secara berkala untuk menentukan perlu atau tidaknya dilakukan perubahan.	
4	Tata Kelola	Konteks Organisasi	Direksi mengomunikasikan strategi, kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber secara efektif kepada seluruh satuan kerja dan pegawai agar dipahami secara jelas.	
5	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber.	
6	Tata Kelola	Konteks Organisasi	Direksi memastikan bahwa struktur organisasi serta strategi manajemen risiko keamanan siber BPR dan BPR Syariah telah mencantumkan peran dan tanggung jawab yang jelas terkait keamanan siber.	
7	Tata Kelola	Konteks Organisasi	Direksi memastikan seluruh SDM memahami risiko keamanan siber beserta strategi manajemen risikonya (*risk-appetite*, *zero risk-tolerance*, kerangka kerja) dan	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
			mampu mengomunikasikan serta menerapkannya secara konsisten.	
8	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki kebijakan ketahanan dan keamanan siber secara tertulis yang telah ditetapkan oleh Direksi. Kebijakan ketahanan dan keamanan siber dievaluasi secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau lebih dalam hal terdapat perubahan yang signifikan terhadap kegiatan usaha BPR dan BPR Syariah.	
9	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah menerapkan *baseline* kontrol proteksi pada seluruh aset TI (antara lain meliputi *hardening*, *patch*, *anti-malware*/EDR, *firewall* dan segmentasi jaringan, pengendalian akses, serta enkripsi), sesuai kebijakan dan prosedur, serta memantau dan mengevaluasi efektivitasnya secara berkala.	
10	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur koordinasi dan komunikasi antarunit kerja yang memiliki tanggung jawab terkait ketahanan dan keamanan siber.	
11	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga yang rutin dievaluasi dan diperbarui.	
12	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah mempunyai daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif, serta antara BPR dan BPR Syariah dan pihak ketiga terdapat perjanjian kerja sama yang mencakup aspek ketahanan dan keamanan siber.	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
13	Tata Kelola	Konteks Organisasi	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber harus didokumentasikan secara memadai.	
14	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko terkait keamanan siber secara berkala.	
15	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memiliki sistem informasi manajemen risiko terkait keamanan siber dan mengembangkannya sesuai kebutuhan BPR dan BPR Syariah.	
16	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah memastikan sistem informasi manajemen risiko terkait keamanan siber dan informasi yang dihasilkan telah sesuai dengan karakteristik dan kompleksitas kegiatan usaha BPR dan BPR Syariah serta adaptif terhadap perubahan.	
17	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melakukan kaji ulang secara berkala atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko terkait keamanan siber.	
18	Tata Kelola	Konteks Organisasi	Sebagai bagian dari sistem informasi manajemen risiko, laporan tingkat maturitas keamanan siber disusun secara berkala oleh fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber dan disampaikan kepada Direksi.	
19	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melaksanakan audit intern atas penyelenggaraan TI secara berkala, termasuk terhadap pengelolaan ketahanan dan keamanan siber dan hak akses pegawai berdasarkan klasifikasi data dan informasi.	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
20	Tata Kelola	Konteks Organisasi	BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber secara berkala.	
21	Tata Kelola	Konteks Organisasi	Direksi mengembangkan budaya dan membangun serta memelihara kesadaran dan komitmen yang kuat mengenai tanggung jawab terkait keamanan siber bagi pegawai di semua level.	
22	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber secara berkala.	
23	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariahmelakukan penyimpanan *log* yang memiliki periode retensi untuk keperluan audit dan investigasi insiden siber sesuai dengan kebijakan/prosedur.	
24	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah menerapkan pengamanan data dan/atau informasi berdasarkan klasifikasi data dan/atau informasi berdasarkan tingkat kritikalitas dan sensitivitas sesuai dengan kebijakan/prosedur.	
25	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melaksanakan analisis dampak bisnis (*Business Impact Analysis*) untuk mengidentifikasi kemungkinan kondisi ekstern dan intern dari serangan siber.	
26	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melaksanakan pengujian keamanan secara berkala, antara lain *vulnerability assessment* dan *penetration testing*, terhadap perangkat lunak dan perangkat keras yang digunakan dalam operasional BPR maupun layanan kepada nasabah dan/atau pihak ketiga.	
27	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan kaji ulang secara berkala terhadap kebijakan ketahanan dan keamanan siber untuk menyesuaikan dengan perkembangan	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
			teknologi, insiden yang terjadi, dan/atau perubahan kondisi terkini lainnya.	
28	MR Identifikasi	Pengukuran Risiko Siber	BPR dan BPR Syariah melakukan identifikasi aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta melakukan pencatatan dalam daftar inventaris TI, yang diperbarui secara berkala.	
29	MR Pelindungan	Kesadaran & Pelatihan	BPR dan BPR Syariah memberikan pelatihan ketahanan dan keamanan siber secara berkala kepada seluruh pegawai, antara lain melakukan simulasi *phishing* dengan cara mengirimkan *emailblast* kepada seluruh pegawai untuk mengukur respons terhadap phishing dan serangan surat elektronik (*email*) serupa setidaknya sekali setiap tahun.	
30	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melakukan *hardening* atas perangkat kerja sesuai dengan kebijakan dan prosedur tertulis, antara lain: a. Seluruh perangkat komputer BPR dan BPR Syariah dilengkapi dengan antivirus yang dikinikan secara otomatis dan berkala; b. *Port* USB terkait penyimpanan data pada perangkat komputer BPR dan BPR Syariah dibatasi penggunaannya; c. Perangkat komputer terkunci secara otomatis pada saat perangkat tidak aktif untuk beberapa saat; dan d. Seluruh perangkat komputer BPR dan BPR Syariah dipasang dengan *firewall* lokal (*host based firewall*).	
31	MR Pelindungan	Konteks Organisasi	Surat elektronik (*email*) korporasi dilindungi sistem pengecekan otomatis *spam*, *phishing*, dan *malware*.	
32	MR Pelindungan	Manajemen Identitas,	BPR dan BPR Syariah memiliki kebijakan dan menerapkan pengendalian akses berbasis peran (*Role Based Access*	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
		Autentikasi, dan Kontrol Akses	*Control*/RBAC), terhadap seluruh sistem, seperti penggunaan single ID yang unik, dan kata sandi yang aman, dan penggunaan akun yang berbeda dari akun harian (*daily use account*). Contoh: pihak yang memiliki akses administrator staf TI atau vendor.	
33	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melakukan pemisahan jaringan dengan menggunakan *Service Set Identifier* (SSID) terpisah untuk pegawai dan tamu/pengunjung, serta menerapkan pengamanan teknis (misalnya *Virtual Local Area Network* - VLAN) untuk membatasi akses.	
34	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah menerapkan kontrol operasional siklus hidup aset TI yang meliputi inventarisasi dan identifikasi *End-of-Life* (EOL) dan *End-of-Support* (EOS), menjalankan *patching*/*upgrade* secara terjadwal, serta menarik atau mengisolasi dari produksi setiap perangkat yang mencapai EOL/EOS sesuai dengan kebijakan/prosedur yang telah ditetapkan.	
35	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariahmenerapkan kontrol akses operasional saat pegawai pindah/berhenti, yaitu hak akses disesuaikan atau dinonaktifkan tepat waktu, dan seluruh perubahan tercatat di *log* sesuai dengan kebijakan/prosedur yang ditetapkan.	
36	MR Pelindungan	Keamanan Data	BPR dan BPR Syariah menghapus (*wipe*) seluruh data pada perangkat kerja sebelum perangkat dimusnahkan/dialihkan. Selanjutnya hasilnya akan diverifikasi dan buktinya dicatat, sesuai dengan kebijakan/prosedur yang ditetapkan.	
37	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melindungi ruang *server*/pusat data (*data center*) dengan kontrol akses fisik, antara lain kunci,	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
			kartu akses, dan/atau biometrik, serta memiliki dokumentasi terhadap akses.	
38	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	Seluruh sistem kritikal dilindungi dengan otentikasi multi faktor (*Multi Factor Authentication* - MFA).	
39	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	Instalasi perangkat lunak BPR dan BPR Syariah hanya dapat dilakukan oleh Satuan Kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI atau pihak lain dengan otorisasi dari pihak penyelenggara TI.	
40	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah melakukan klasifikasi antara jaringan untuk sistem kritikal dengan jaringan umum (contoh: surat elektronik).	
41	MR Pelindungan	Konteks Organisasi	BPR dan BPR Syariah memiliki prosedur tertulis terkait *change management* untuk meninjau seluruh perubahan konfigurasi,	
42	MR Pelindungan	Keamanan Data	BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data termasuk namun tidak terbatas pada pelindungan data, transfer data, dan penghapusan data.	
43	MR Pelindungan	Kesadaran & Pelatihan	BPR dan BPR Syariah secara berkala melakukan edukasi kepada Nasabah mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi melalui berbagai kanal komunikasi.	
44	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk sistem kritikal.	
45	MR Pelindungan	Manajemen Identitas,	BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut (*Attribute Based Access*	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
		Autentikasi, dan Kontrol Akses	*Control* - ABAC) untuk sistem kritikal (misal *Core Banking System*). Penerapan ABAC dilakukan dengan mempertimbangkan faktor antara lain lokasi, waktu, perangkat, dan tingkat risiko.	
46	MR Pelindungan	Manajemen Identitas, Autentikasi, dan Kontrol Akses	BPR dan BPR Syariah menerapkan pembatasan nominal transaksi dan jenis transaksi.	
47	MR Deteksi	Ketahanan Infrastruktur TI	Apabila terjadi percobaan *login* gagal, sistem kritikal BPR dan BPR Syariah akan memantau, mengirimkan *alert* otomatis ke Tim Keamanan dan pemilik akun, serta mengunci akun setelah ambang batas (*threshold*) percobaan terlampaui, guna mendeteksi lebih dini terhadap upaya serangan siber.	
48	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan yang diuji secara berkala.	
49	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki matriks eskalasi insiden siber yang mengategorisasikan kejadian berdasarkan tingkat keparahan/prioritas/dampak dan jalur komunikasi pelaporan.	
50	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki prosedur tertulis ketahanan dan keamanan siber terkait pelaporan kejadian mencurigakan dan disosialisasikan kepada seluruh pegawai.	
51	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah melaksanakan simulasi tanggap insiden siber secara berkala dan terdokumentasi.	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
52	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah menetapkan mekanisme untuk melakukan evaluasi kesesuaian prosedur dan *root causeanalysis* serta dilakukan tindak lanjut pasca insiden siber.	
53	MR Penanggulangan & Pemulihan	Analisis Insiden	BPR dan BPR Syariah memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber yang telah ditetapkan oleh Direksi. Prosedur didokumentasikan secara memadai dan dikomunikasikan kepada seluruh pegawai.	
54	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah memiliki Rencana Pemulihan Bencana (*Disaster Recovery Plan*) dan mengimplementasikannya guna memulihkan layanan apabila terjadi insiden.	
55	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah wajib melakukan rekam cadang (*back up*) setiap akhir hari untuk seluruh data aktivitas BPR dan BPR Syariah.	
56	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah melakukan pengujian *restore backup data* secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun.	
57	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah melakukan analisis kritikalitas sistem penting dengan menetapkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	
58	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah melakukan kaji ulang terhadap rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) insiden siber secara berkala, termasuk melakukan pengujian *failover*.	

No	Domain	Sub Domain	Parameter Penilaian	Peringkat Parameter
59	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah memiliki prosedur notifikasi kepada regulator ataupun lembaga eksternal (misal OJK, BI, dan lain-lain) yang menetapkan batas waktu, media, dan tanggung jawab pelaporan setelah terjadinya insiden siber.	
60	MR Penanggulangan & Pemulihan	Pelaksanaan Rencana Pemulihan Insiden Siber	BPR dan BPR Syariah menetapkan mekanisme komunikasi kepada nasabah dan publik ketika insiden siber terjadi. Mekanisme komunikasi meliputi: penetapan saluran resmi, proses persetujuan pesan, dan panduan pertanyaan-jawaban, serta melakukan pelatihan atas mekanisme tersebut.	

D. KRITERIA PENILAIAN PARAMETER BERDASARKAN PERINGKAT

Tabel 3. Kriteria Penilaian Parameter Berdasarkan Peringkat

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
1	BPR dan BPR Syariah menetapkan wewenang dan tanggung jawab Direksi dan Dewan Komisaris secara tertulis dalam penerapan manajemen risiko terkait keamanan siber.	Wewenang dan tanggung jawab Direksi dan Dewan Komisaris terkait keamanan siber telah ditetapkan tertulis, disahkan, dan dievaluasi secara berkala serta konsisten.	Wewenang dan tanggung jawab Direksi dan Dewan Komisaris terkait keamanan siber telah ditetapkan tertulis, disahkan, dan dievaluasi namun belum secara konsisten atau belum mencakup seluruh aspek.	Wewenang dan tanggung jawab Direksi dan Dewan Komisaris terkait keamanan siber telah ditetapkan tertulis, namun belum pernah dievaluasi atau belum terdapat mekanisme evaluasi yang jelas.	Wewenang dan tanggung jawab Direksi dan Dewan Komisaris terkait keamanan siber masih berupa praktik lisan/*adhoc* tanpa dokumen formal.	Wewenang dan tanggung jawab Direksi Dewan Komisaris terkait keamanan siber belum pernah ditetapkan.
2	Direksi menetapkan tingkat risiko (*risk appetite*) terkait keamanan siber.	Strategi ketahanan dan keamanan siber disusun dengan sepenuhnya mengacu pada visi dan mendukung misi BPR dan BPR Syariah dan kaji ulang strategi dilakukan secara berkala namun	Tingkat risiko (*risk appetite*) terkait keamanan siber telah ditetapkan tertulis, disahkan, dan dievaluasi berkala namun belum secara konsisten atau belum mencakup seluruh aspek.	Tingkat risiko (*risk appetite*) terkait keamanan siber telah ditetapkan tertulis, namun belum dievaluasi secara berkala atau belum terdapat mekanisme evaluasi yang jelas.	Tingkat risiko (*risk appetite*) terkait keamanan siber masih berupa praktik lisan/*adhoc* tanpa dokumen tertulis.	Tingkat risiko (*risk appetite*) terkait keamanan siber belum pernah ditetapkan.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		belum secara konsisten atau belum mencakup seluruh aspek.				
3	Strategi ketahanan dan keamanan siber BPR dan BPR Syariah telah dirumuskan untuk mendukung serta selaras dengan visi dan misi BPR dan BPR Syariah (misalnya target pertumbuhan layanan digital, standar keamanan nasabah, dan *risk-appetite* yang telah ditetapkan), termasuk melakukan kaji ulang strategi keamanan siber secara berkala untuk menentukan perlu atau tidaknya dilakukan perubahan.	Strategi ketahanan dan keamanan siber disusun dengan sepenuhnya mengacu pada visi dan mendukung misi BPR dan BPR Syariah dan kaji ulang strategi dilakukan secara berkala serta konsisten.	Strategi ketahanan dan keamanan siber disusun dengan sepenuhnya mengacu pada visi dan mendukung misi BPR dan BPR Syariah dan kaji ulang strategi dilakukan secara berkala namun belum secara konsisten atau belum mencakup seluruh aspek.	Strategi ketahanan dan keamanan siber disusun, namun belum sepenuhnya selaras dan mendukung visi-misi BPR dan BPR Syariah dan kaji ulang dilakukan secara *adhoc* atau tidak terjadwal.	Strategi ketahanan dan keamanan sbier disusun, namun sepenuhnya tidak selaras dan mendukung visi-misi BPR dan BPR Syariah.	BPR dan BPR Syariah tidak memiliki strategi ketahanan dan keamanan siber.
4	Direksi mengomunikasikan strategi, kebijakan, prosedur, dan limit dalam penerapan	Direksi telah mengomunikasikan strategi, kebijakan, prosedur dan limit	Direksi telah mengomunikasikan strategi, kebijakan, prosedur dan limit manajemen risiko	Direksi telah mengomunikasikan strategi, kebijakan, prosedur dan limit manajemen risiko	Direksi telah mengomunikasikan strategi, kebijakan, prosedur dan limit	Direksi tidak mengomunikasikan strategi, kebijakan, prosedur dan

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	manajemen risiko terkait keamanan siber secara efektif kepada seluruh satuan kerja dan pegawai agar dipahami secara jelas.	manajemen risiko terkait keamanan siber secara efektif kepada seluruh jenjang organisasi dan seluruh jenjang organisasi mampu memahami manajemen risiko siber.	terkait keamanan siber secara efektif kepada seluruh jenjang organisasi namun tidak seluruh jenjang mampu memahami manajemen risiko siber	terkait keamanan siber secara efektif hanya kepada sebagian besar jenjang organisasi tertentu dan tidak seluruh jenjang mampu memahami manajemen risiko siber.	manajemen risiko terkait keamanan siber kepada sebagian besar jenjang organisasi dan sebagian besar jenjang organisasi tidak memahami perannya terkait manajemen risiko siber.	limit manajemen risiko terkait keamanan siber.
5	BPR dan BPR Syariah memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber.	Memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber dan fungsi dapat menjalankan perannya dengan sangat memadai.	Memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber dan fungsi dapat menjalankan perannya dengan memadai.	Memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber dan fungsi dapat menjalankan perannya dengan cukup memadai.	Memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber dan fungsi dapat menjalankan perannya dengan kurang memadai.	Tidak memiliki fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber.
6	Direksi memastikan bahwa struktur organisasi serta strategi manajemen risiko keamanan siber BPR dan BPR Syariah telah mencantumkan peran dan tanggung jawab	Direksi telah memastikan bahwa BPR dan BPR Syariah memiliki struktur organisasi serta strategi manajemen risiko	Direksi telah memastikan bahwa BPR dan BPR Syariah memiliki struktur organisasi serta strategi manajemen risiko keamanan siber	BPR dan BPR Syariah memiliki struktur organisasi serta strategi manajemen risiko keamanan siber namun belum sepenuhnya	BPR dan BPR Syariah memiliki struktur organisasi serta strategi manajemen risiko keamanan siber namun tidak dilengkapi dengan	BPR dan BPR Syariah tidak memiliki struktur organisasi serta manajemen risiko keamanan siber yang dilengkapi

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	yang jelas terkait keamanan siber.	keamanan siber yang dilengkapi dengan peran dan tanggung jawab yang jelas dalam dokumen tertulis.	namun belum sepenuhnya dilengkapi dengan peran dan tanggung jawab yang jelas dalam dokumen tertulis.	dilengkapi dengan peran dan tanggung jawab yang jelas dan belum dituangkan dalam dokumen tertulis.	peran dan tanggung jawab yang jelas dalam dokumen tertulis.	dengan peran dan fungis tanggung jawab yang jelas dalam dokumen tertulis.
7	Direksi memastikan seluruh SDM memahami risiko keamanan siber beserta strategi manajemen risikonya (*risk-appetite*, *zero risk-tolerance*, kerangka kerja) dan mampu mengomunikasikan serta menerapkannya secara konsisten.	BPR dan BPR Syariah melakukan *gap analysis* secara rutin, terdapat program pelatihan secara rutin, dan seluruh SDM sudah mampu memahami, mengomunikasi-kan, serta menerapkan strategi dan implikasi risiko keamanan siber.	BPR dan BPR Syariah melakukan *gap analysis* secara rutin, terdapat program pelatihan secara rutin, namun belum sepenuhnya SDM mampu memahami, mengomunikasi-kan, serta menerapkan strategi dan implikasi risiko keamanan siber.	BPR dan BPR Syariah melakukan *gap analysis* secara rutin, pelatihan tidak dilakukan secara rutin, dan belum sepenuhnya SDM mampu memahami, mengomunikasi-kan, serta menerapkan strategi dan implikasi risiko keamanan siber.	BPR dan BPR Syariah melakukan *gap analysis* dan pelatihan tidak secara rutin, sehingga pemahaman, kemampuan berkomunikasi, dan penerapan strategi keamanan siber baru tercapai pada sebagian SDM.	BPR dan BPR Syariah belum pernah melakukan *gap analysis* ataupun pelatihan terarah, sehingga sebagian besar SDM belum memahami, mengomunikasi-kan, maupun menerapkan strategi dan implikasi risiko keamanan siber.
8	BPR dan BPR Syariah memiliki kebijakan ketahanan dan keamanan siber secara tertulis yang telah	BPR dan BPR Syariah memiliki kebijakan ketahanan dan keamanan siber	BPR dan BPR Syariah memiliki kebijakan ketahanan dan keamanan siber	BPR dan BPR Syariah memiliki kebijakan ketahanan dan keamanan siber	BPR dan BPR Syariah dalam proses penyusunanan kebijakan	BPR dan BPR Syariah tidak memiliki kebijakan

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	ditetapkan oleh Direksi. Kebijakan ketahanan dan keamanan siber dievaluasi secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau lebih dalam hal terdapat perubahan yang signifikan terhadap kegiatan usaha BPR dan BPR Syariah.	yang telah ditetapkan oleh Direksi dan dievaluasi secara berkala paling sedikit dalam 1 (satu) tahun.	yang telah ditetapkan oleh Direksi dan dievaluasi secara berkala namun belum mencakup seluruh aspek.	yang telah ditetapkan oleh Direksi, namun belum dievaluasi secara berkala.	ketahanan dan keamanan siber.	ketahanan dan keamanan siber.
9	BPR dan BPR Syariah menerapkan *baseline* kontrol proteksi pada seluruh aset TI (antara lain meliputi *hardening*, *patch*, *anti-malware*/EDR, *firewall* dan segmentasi jaringan, pengendalian akses, serta enkripsi), sesuai kebijakan dan prosedur, serta memantau dan mengevaluasi efektivitasnya secara berkala.	BPR dan BPR Syariah telah menerapkan *baseline* kontrol pada seluruh aset, serta memantau dan mengevaluasi efektivitasnya secara berkala.	BPR dan BPR Syariah telah menerapkan *baseline* kontrol pada seluruh aset, namun belum memantau dan mengevaluasi efektivitasnya secara berkala.	BPR dan BPR Syariah telah menerapkan *baseline* kontrol pada sebagian aset, serta memantau dan mengevaluasi efektivitasnya secara berkala.	BPR dan BPR Syariah telah menerapkan *baseline* kontrol pada sebagian aset, namun belum memantau dan mengevaluasi efektivitasnya secara berkala.	BPR dan BPR Syariah belum menerapkan *baseline* kontrol dan belum memantau dan mengevaluasi efektivitasnya.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
10	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur koordinasi dan komunikasi antarunit kerja yang memiliki tanggung jawab terkait ketahanan dan keamanan siber.	BPR dan BPR Syariah memiliki kebijakan tertulis yang jelas dan komprehensif mengenai koordinasi dan komunikasi antar unit kerja dan dilaksanakan secara konsisten.	BPR dan BPR Syariah memiliki kebijakan tertulis yang jelas dan komprehensif mengenai koordinasi dan komunikasi antar unit kerja namun belum selalu konsisten dilaksanakan di seluruh unit kerja.	BPR dan BPR Syariah memiliki kebijakan tertulis, tetapi masih bersifat umum dan belum mengatur detail mekanisme koordinasi maupun komunikasi.	BPR dan BPR Syariah belum memiliki kebijakan tertulis mengenai koordinasi dan komunikasi antar unit kerja sehingga praktik koordinasi dan komunikatif bersifat *ad hoc*.	BPR dan BPR Syariah tidak memiliki kebijakan tertulis mengenai koordinasi dan komunikasi antarunit kerja.
11	BPR dan BPR Syariah memiliki kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga yang rutin dievaluasi dan diperbarui.	BPR dan BPR Syariah memiliki Kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga dan rutin dievaluasi serta diperbarui.	BPR dan BPR Syariah memiliki Kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga namun tidak semua aspek dievaluasi serta diperbarui.	Kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga dimiliki oleh BPR dan BPR Syariah, namun tidak rutin dievaluasi serta diperbarui.	BPR dan BPR Syariah dalam proses penyusunan kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga.	BPR dan BPR Syariah tidak memiliki Kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga.
12	BPR dan BPR Syariah mempunyai daftar pihak	BPR dan BPR Syariah memiliki	BPR dan BPR Syariah memiliki	BPR dan BPR Syariah memiliki	BPR dan BPR Syariah memiliki	BPR dan BPR Syariah tidak

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif, serta antara BPR dan BPR Syariah dan pihak ketiga terdapat perjanjian kerja sama yang mencakup aspek ketahanan dan keamanan siber.	daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif yang terdokumentasi dan dikinikan secara rutin, serta dilengkapi dengan perjanjian kerja sama yang mencakup seluruh aspek ketahanan dan keamanan siber.	daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif yang terdokumentasi dan dikinikan secara rutin, serta dilengkapi dengan perjanjian kerja sama yang mencakup sebagian aspek ketahanan dan keamanan siber.	daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif yang terdokumentasi dan dikinikan secara rutin, namun tidak dilengkapi dengan perjanjian kerja sama terkait aspek ketahanan dan keamanan siber.	daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi sensitif yang terdokumentasi, namun tidak dikinikan secara rutin dan tidak dilengkapi dengan perjanjian kerja sama terkait aspek ketahanan dan keamanan siber.	memiliki daftar pihak ketiga yang memiliki akses terhadap sistem internal dan/atau informasi yang sensitif dan tidak memiliki perjanjian kerja sama terkait ketahanan dan keamanan siber.
13	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko terkait keamanan siber harus didokumentasikan secara memadai.	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko ketahanan dan keamanan siber telah didokumentasikan secara konsisten dan dikomunikasikan	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko ketahanan dan keamanan siber telah didokumentasikan secara konsisten namun dikomunikasikan	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko ketahanan dan keamanan siber telah didokumentasikan sebagian dan telah dikomunikasikan kepada seluruh pegawai.	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko ketahanan dan keamanan siber telah didokumentasi-kan sebagian namun dikomunikasikan kepada sebagian pegawai.	Kebijakan, prosedur, dan limit dalam penerapan manajemen risiko ketahanan dan keamanan siber tidak didokumentasi-kan dan tidak dikomunikasikan

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		kepada seluruh pegawai.	kepada sebagian pegawai.			kepada seluruh pegawai.
14	BPR dan BPR Syariah melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko terkait keamanan siber secara berkala.	BPR dan BPR Syariah melakukan evaluasi atas sistem pengukuran risiko terkait keamanan siber secara berkala dan penyempurnaan dilakukan secara segera sesuai dengan hasil evaluasi.	BPR dan BPR Syariah melakukan evaluasi atas sistem pengukuran risiko terkait keamanan siber secara berkala namun tidak mencakup seluruh aspek dan penyempurnaan dilakukan secara segera sesuai dengan hasil evaluasi.	BPR dan BPR Syariah melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko terkait keamanan siber tidak terjadwal atau secara *adhoc*.	BPR dan BPR Syariah hampir tidak pernah melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko terkait keamanan siber.	BPR dan BPR Syariah tidak memiliki kebijakan untuk melakukan evaluasi dan penyempurnaan atas sistem pengukuran risiko terkait keamanan siber secara berkala.
15	BPR dan BPR Syariah memiliki sistem informasi manajemen risiko terkait keamanan siber dan mengembangkannya sesuai kebutuhan BPR dan BPR Syariah.	Sistem informasi manajemen risiko sangat mendukung dalam pembuatan laporan kepada Direksi dan BPR dan BPR Syariah secara berkala dan aktif melakukan evaluasi serta penyempurnaan	Sistem informasi manajemen risiko cukup mendukung dalam pembuatan laporan kepada Direksi dan BPR dan BPR Syariah secara berkala dan aktif melakukan evaluasi serta penyempurnaan terhadap sistem	Sistem informasi manajemen risiko kurang mendukung dalam pembuatan laporan kepada Direksi namun belum melakukan evaluasi secara berkala termasuk penyempurnaan terhadap sistem informasi	Sistem informasi manajemen risiko tidak sepenuhnya mendukung dalam pembuatan laporan kepada Direksi dan belum pernah melakukan evaluasi termasuk penyempurnaan terhadap sistem informasi	BPR dan BPR Syariah tidak mempunya sistem informasi manajemen risiko terkait keamanan siber.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		terhadap sistem informasi manajemen risiko keamanan siber.	informasi manajemen risiko keamanan siber.	manajemen risiko keamanan siber.	manajemen risiko keamanan siber.	
16	BPR dan BPR Syariah memastikan sistem informasi manajemen risiko terkait keamanan siber dan informasi yang dihasilkan telah sesuai dengan karakteristik dan kompleksitas kegiatan usaha BPR dan BPR Syariah serta adaptif terhadap perubahan.	Sistem informasi manajemen risiko keamanan siber dan informasi yang dihasilkan telah sesuai dengan karakteristik dan kompleksitas kegiatan usaha BPR dan BPR Syariah serta adaptif terhadap perubahan.	Sistem informasi manajemen risiko keamanan siber dan informasi yang dihasilkan telah sesuai dengan karakteristik dan kompleksitas kegiatan usaha BPR dan BPR Syariah namun kurang adaptif terhadap perubahan.	Sistem informasi manajemen risiko keamanan siber dan informasi yang dihasilkan telah sesuai dengan karakteristik dan kompleksitas kegiatan usaha BPR dan BPR Syariah namun tidak adaptif terhadap perubahan.	Sistem informasi manajemen risiko keamanan siber dan informasi yang dihasilkan tidak sepenuhnya sesuai dengan karakteristik dan kompleksitas kegiatan usaha BPR dan BPR Syariah dan kurang adaptif terhadap perubahan.	Sistem masih bersifat umum, belum disesuaikan dengan karakteristik dan kompleksitas usaha BPR dan BPR Syariah, serta tidak adaptif terhadap perubahan.
17	BPR dan BPR Syariah melakukan kaji ulang secara berkala atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko terkait keamanan siber.	BPR dan BPR Syariah melakukan kaji ulang atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi	BPR dan BPR Syariah melakukan kaji ulang atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko	BPR dan BPR Syariah melakukan kaji ulang atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi manajemen risiko	BPR dan BPR Syariah melakukan kaji ulang secara berkala atas kecukupan cakupan informasi yang dihasilkan dari sistem informasi	BPR dan BPR Syariah hampir tidak memiliki proses untuk melakukan kaji ulang atas kecukupan cakupan informasi yang

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		manajemen risiko terkait keamanan siber secara berkala.	terkait keamanan siber secara berkala namun tidak mencakup seluruh aspek.	terkait keamanan siber secara tidak terjadwal atau secara *adhoc*.	manajemen risiko terkait keamanan siber.	dihasilkan dari sistem informasi manajemen risiko terkait keamanan siber.
18	Sebagai bagian dari sistem informasi manajemen risiko, laporan tingkat maturitas keamanan siber disusun secara berkala oleh fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber.	Laporan tingkat maturitas keamanan siber disusun secara berkala, terdokumentasi dan disertai dengan dokumen pendukung yang memadai, dan digunakan sebagai dasar peningkatan kontrol serta pemenuhan ketentuan.	Laporan tingkat maturitas keamanan siber disusun secara berkala, terdokumentasi dan disertai dengan dokumen pendukung yang cukup memadai, dan digunakan sebagai dasar peningkatan kontrol serta pemenuhan ketentuan.	Laporan tingkat maturitas keamanan siber disusun secara berkala, terdokumentasi dan disertai dengan dokumen pendukung yang kurang memadai, dan digunakan sebagai dasar peningkatan kontrol serta pemenuhan ketentuan.	Laporan tingkat maturitas disusun namun belum dilakukan secara berkala dan belum dimanfaatkan sebagai dasar peningkatan kontrol serta pemenuhan ketentuan.	BPR dan BPR Syariah belum menyusun laporan tingkat maturitas keamanan siber.
19	Fungsi yang bertanggung jawab menangani ketahanan dan keamanan siber menyampaikan laporan berkala kepada Direksi.	Laporan berkala kepada Direksi disampaikan secara rutin dan disertai dengan dokumen	Laporan berkala kepada Direksi disampaikan secara rutin dan disertai dengan dokumen pendukung yang cukup memadai.	Laporan berkala kepada Direksi disampaikan secara rutin dan disertai dengan dokumen pendukung yang kurang memadai.	Laporan berkala kepada Direksi disampaikan namun tidak secara rutin dan tidak disertai	Laporan berkala tidak pernah disampaikan kepada Direksi.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		pendukung yang memadai.			dokumen pendukung.	
20	BPR dan BPR Syariah melaksanakan audit intern atas penyelenggaraan TI secara berkala, termasuk terhadap pengelolaan ketahanan dan keamanan siber.	BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara berkala.	BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara berkala namun tidak mencakup seluruh aspek.	BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara tidak terjadwal atau secara *adhoc*.	BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara tidak terjadwal atau secara *adhoc* dan hanya mencakup sebagian aspek.	BPR dan BPR Syariah tidak melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber.
21	BPR dan BPR Syariah melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara berkala.	Program budaya siber telah direncanakan, dipantau dan dievaluasi rutin, dan diperuntukkan bagi seluruh pegawai.	Program budaya siber telah direncanakan, dipantau dan dievaluasi rutin, dan hanya diimplementasikan pada pegawai tertentu.	Program budaya siber telah direncanakan, dipantau dan dievaluasi tidak secara rutin, dan diperuntukkan bagi seluruh pegawai.	Program budaya siber telah direncanakan, dipantau dan dievaluasi tidak secara rutin, dan hanya diimplementasi-kan pada pegawai tertentu.	Tidak terdapat program budaya siber.
22	Direksi mengembangkan budaya dan membangun serta	BPR dan BPR Syariah melakukan pengukuran	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan	BPR dan BPR Syariah tidak melakukan pengukuran

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	memelihara kesadaran dan komitmen yang kuat mengenai tanggung jawab terkait keamanan siber bagi pegawai di semua level.	tingkat kerentanan terhadap risiko terkait keamanan siber secara berkala.	terhadap risiko terkait keamanan siber secara berkala namun belum mencakup seluruh aspek.	terhadap risiko terkait keamanan siber secara tidak terjadwal atau secara *adhoc*.	terhadap risiko terkait keamanan siber secara tidak terjadwal atau secara *adhoc* dan hanya mencakup sebagian aspek.	tingkat kerentanan terhadap risiko terkait keamanan siber.
23	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber secara berkala.	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber secara berkala.	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber secara berkala namun belum mencakup seluruh aspek.	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber secara tidak terjadwal atau secara *adhoc*.	BPR dan BPR Syariah melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber secara tidak terjadwal atau secara *adhoc* dan hanya mencakup sebagian aspek.	BPR dan BPR Syariah tidak melakukan pengukuran tingkat kerentanan terhadap risiko terkait keamanan siber.
24	BPR dan BPR Syariah melakukan penyimpanan *log* yang memiliki periode retensi untuk keperluan audit dan investigasi insiden siber sesuai dengan kebijakan/prosedur.	BPR dan BPR Syariah menyimpan seluruh *log* dalam periode retensi sesuai kebijakan, dikelola dengan baik sehingga mudah ditelusuri, dan pemenuhan	BPR dan BPR Syariah menyimpan seluruh *log* dalam periode retensi sesuai kebijakan, dikelola dengan baik sehingga mudah ditelusuri, namun pemenuhan	BPR dan BPR Syariah menyimpan sebagian *log* dalam periode retensi sesuai kebijakan, dikelola dengan baik sehingga mudah ditelusuri, dan pemenuhan	BPR dan BPR Syariah menyimpan sebagian *log* dalam periode retensi sesuai kebijakan, dikelola dengan baik sehingga mudah ditelusuri, namun pemenuhan	BPR dan BPR Syariah tidak menyimpan *log* dalam periode retensi sesuai kebijakan, dan tidak memantau pemenuhan retensi secara berkala.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		retensi dipantau secara berkala.	retensi belum dipantau secara berkala.	retensi belum dipantau secara berkala.	retensi belum dipantau secara berkala.	
25	BPR dan BPR Syariah melakukan klasifikasi data dan/atau informasi berdasarkan tingkat kritikalitas dan sensitivitas sesuai dengan kebijakan/prosedur.	BPR dan BPR Syariah telah menerapkan klasifikasi atas seluruh data/informasi berdasarkan tingkat kritikalitas dan sensitivitas sesuai dengan kebijakan/ prosedur, serta melakukan kaji ulang atas klasifikasi tersebut secara berkala.	BPR dan BPR Syariah telah menerapkan klasifikasi atas seluruh data/informasi berdasarkan tingkat kritikalitas dan sensitivitas sesuai dengan kebijakan/ prosedur, namun belum melakukan kaji ulang atas klasifikasi tersebut secara berkala.	BPR dan BPR Syariah telah menerapkan klasifikasi atas sebagian data/informasi berdasarkan tingkat kritikalitas dan sensitivitas sesuai dengan kebijakan/ prosedur, serta melakukan kaji ulang atas klasifikasi tersebut secara berkala.	BPR dan BPR Syariah telah menerapkan klasifikasi atas sebagian data/informasi berdasarkan tingkat kritikalitas dan sensitivitas sesuai dengan kebijakan/ prosedur, namun belum melakukan kaji ulang atas klasifikasi tersebut secara berkala.	BPR dan BPR Syariah belum menerapkan klasifikasi atas data/informasi berdasarkan tingkat kritikalitas dan sensitivitas.
26	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur pengamanan data dan/atau informasi berdasarkan klasifikasi data dan/atau informasi.	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur pengamanan data dan/atau informasi berdasarkan	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur pengamanan data dan/atau informasi berdasarkan klasifikasi data	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur pengamanan data dan/atau informasi berdasarkan klasifikasi data	BPR dan BPR Syariah memiliki kebijakan tertulis yang mengatur pengamanan data dan/atau informasi berdasarkan klasifikasi data	BPR dan BPR Syariah tidak memiliki kebijakan tertulis yang mengatur pengamanan data dan/atau informasi

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		klasifikasi data dan/atau informasi, serta dievaluasi secara rutin, dan telah diimplementasikan secara menyeluruh.	dan/atau informasi, namun tidak dievaluasi secara rutin, dan telah diimplementasikan secara menyeluruh.	dan/atau informasi, serta dievaluasi secara rutin, namun belum diimplementasikan secara menyeluruh.	dan/atau informasi, namun tidak dievaluasi secara rutin dan belum diimplementasi-kan secara menyeluruh.	berdasarkan klasifikasi data dan/atau informasi.
27	BPR dan BPR Syariah melaksanakan analisis dampak bisnis (*Business Impact Analysis*) untuk mengidentifikasi kemungkinan kondisi ekstern dan intern dari serangan siber.	Pengujian dilakukan secara berkala dan mencakup seluruh komponen.	Pengujian dilakukan secara berkala namun hanya mencakup seluruh komponen.	Pengujian dilakukan secara tidak terjadwal atau secara *ad hoc* namun mencakup seluruh komponen.	Pengujian dilakukan secara tidak terjadwal atau secara *adhoc* namun hanya mencakup sebagian komponen.	Tidak terdapat pengujian keamanan secara berkala.
28	BPR dan BPR Syariah melaksanakan pengujian keamanan secara berkala, antara lain *vulnerability assessment* dan *penetration testing*, terhadap perangkat lunak dan perangkat keras yang digunakan dalam operasional BPR dan BPR Syariah	BPR dan BPR Syariah telah melakukan kaji ulang secara berkala terhadap kebijakan ketahanan dan keamanan siber dan disesuaikan dengan perkembangan teknologi, insiden	BPR dan BPR Syariah telah melakukan kaji ulang secara berkala terhadap kebijakan ketahanan dan keamanan siber namun tidak sepenuhnya disesuaikan dengan perkembangan	BPR dan BPR Syariah melakukan kaji ulang secara tidak terjadwal/*adhoc* terhadap kebijakan ketahanan dan keamanan siber.	BPR dan BPR Syariah melakukan kaji ulang secara tidak terjadwal/*adhoc* terhadap sebagian kecil kebijakan ketahanan dan keamanan siber.	Tidak terdapat proses kaji ulang atas kebijakan keamanan siber.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	maupun layanan kepada nasabah dan/atau pihak ketiga.	yang terjadi, dan/atau perubahan kondisi terkini lainnya.	teknologi, insiden yang terjadi, dan/atau perubahan kondisi terkini lainnya.			
29	BPR dan BPR Syariah melakukan kaji ulang secara berkala terhadap kebijakan ketahanan dan keamanan siber untuk menyesuaikan dengan perkembangan teknologi, insiden yang terjadi, dan/atau perubahan kondisi terkini lainnya.	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, serta dituangkan dalam dokumen inventaris risiko (*risk register*) yang diperbarui secara berkala.	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, namun tidak seluruhnya dituangkan dalam dokumen inventaris risiko (*risk register*) yang diperbarui secara berkala.	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, yang dituangkan dalam dokumen inventaris risiko (*risk register*) namun tidak diperbarui secara berkala.	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, namun tidak seluruhnya dituangkan dalam dokumen inventaris risiko (*risk register*) dan tidak diperbarui secara berkala.	BPR dan BPR Syariah tidak mengidentifikasi risiko ketahanan dan keamanan siber.
30	BPR dan BPR Syariah mengidentifikasi risiko dan menentukan prioritas risiko terkait ketahanan dan keamanan siber berdasarkan fungsi kritis, aset TI, interkoneksi sistem (*interconnectivity*), serta	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, serta dituangkan dalam dokumen inventaris risiko (*risk register*) yang	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, namun tidak seluruhnya dituangkan dalam dokumen inventaris risiko (*risk register*)	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, yang dituangkan dalam dokumen inventaris risiko (*risk register*) namun tidak	BPR dan BPR Syariah telah mengidentifikasi risiko ketahanan dan keamanan siber, namun tidak seluruhnya dituangkan dalam dokumen inventaris risiko	BPR dan BPR Syariah tidak mengidentifikasi risiko ketahanan dan keamanan siber.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	dituangkan dalam dokumen inventaris risiko (*risk register*). Dokumen *risk register* diperbarui secara berkala.	diperbarui secara berkala.	yang diperbarui secara berkala.	diperbarui secara berkala.	(*risk register*) dan tidak diperbarui secara berkala.	
31	BPR dan BPR Syariah melakukan identifikasi aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta melakukan pencatatan dalam daftar inventaris TI, yang diperbarui secara berkala.	BPR dan BPR Syariah telah melakukan identifikasi seluruh aset TI serta melakukan pencatatan dalam daftar inventaris TI, yang diperbarui secara berkala.	BPR dan BPR Syariah telah melakukan identifikasi seluruh aset TI serta melakukan pencatatan dalam daftar inventaris TI, namun tidak diperbarui secara berkala.	BPR dan BPR Syariah telah melakukan identifikasi sebagian aset TI serta melakukan pencatatan dalam daftar inventaris TI, yang diperbarui secara berkala.	BPR dan BPR Syariah telah melakukan identifikasi sebagian aset TI serta melakukan pencatatan dalam daftar inventaris TI, namun tidak diperbarui secara berkala.	BPR dan BPR Syariah tidak pernah melakukan identifikasi seluruh aset TI serta tidak melakukan pencatatan dalam daftar inventaris TI.
32	BPR dan BPR Syariah memberikan pelatihan ketahanan dan keamanan siber secara berkala kepada seluruh pegawai.	BPR dan BPR Syariah telah memberikan pelatihan dan keamanan siber secara berkala kepada seluruh pegawai dan sepenuhnya dapat diimplementasikan.	BPR dan BPR Syariah telah memberikan pelatihan dan keamanan siber secara berkala kepada seluruh pegawai dan tidak sepenuhnya dapat diimplementasikan.	BPR dan BPR Syariah telah memberikan pelatihan dan keamanan siber secara tidak berkala kepada seluruh pegawai dan dapat diimplementasikan sepenuhnya.	BPR dan BPR Syariah telah memberikan pelatihan dan keamanan siber secara tidak berkala kepada sebagian pegawai dan tidak sepenuhnya dapat.	BPR dan BPR Syariah tidak pernah memberikan pelatihan dan keamanan siber secara berkala kepada seluruh pegawai.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
33	BPR dan BPR Syariah melakukan hardening atas perangkat kerja sesuai dengan kebijakan dan prosedur tertulis, antara lain: a. Seluruh perangkat komputer BPR dan BPR Syariah dilengkapi dengan *anti-malware* yang dikinikan secara otomatis dan berkala; b. *Port* USB terkait penyimpanan data pada perangkat komputer BPR dan BPR Syariah dibatasi penggunaannya; c. Perangkat komputer terkunci secara otomatis pada saat perangkat tidak aktif untuk beberapa saat; dan d. Seluruh perangkat komputer BPR dan BPR Syariah dipasang dengan	BPR dan BPR Syariah telah menerapkan kontrol *hardening* pada seluruh perangkat kerja sesuai kebijakan secara otomatis.	BPR dan BPR Syariah telah menerapkan kontrol *hardening* pada seluruh perangkat kerja sesuai kebijakan secara manual.	BPR dan BPR Syariah telah menerapkan kontrol *hardening* pada sebagian perangkat kerja sesuai kebijakan secara otomatis.	BPR dan BPR Syariah telah menerapkan kontrol *hardening* pada sebagian perangkat kerja sesuai kebijakan secara manual.	BPR dan BPR Syariah tidak menerapkan kontrol *hardening* pada seluruh perangkat kerja.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	firewall lokal (*host based firewall*).					
34	Surat elektronik (*email*) korporasi dilindungi sistem pengecekan otomatis *spam*, *phishing*, *dan malware*.	Sistem pengecekan otomatis *spam*, *phishing*, dan *malware* terpasang pada *email* korporasi.	Sistem pengecekan *spam*, *phishing*, dan *malware* terpasang pada *email* korporasi, namun diperbarui secara manual.	BPR dan BPR Syariah hanya memiliki paling banyak 2 (dua) sistem pengecekan otomatis (*spam*/*phishing*/*malware*) terpasang pada *email* korporasi.	BPR dan BPR Syariah hanya memiliki paling banyak 2 (dua) sistem pengecekan (*spam*/*phishing*/*malware*) terpasang pada *email* korporasi, namun diperbarui secara manual.	Tidak terpasang sistem pengecekan otomatis *spam*, *phishing*, dan *malware* pada *email* korporasi.
35	BPR dan BPR Syariah melakukan simulasi *phishing* dengan cara mengirimkan *emailblast* kepada seluruh pegawai untuk mengukur respons terhadap *phishing* dan serangan surat elektronik (*email*) serupa setidaknya sekali setiap tahun.	Seluruh pegawai telah mengikuti simulasi *phishing* paling sedikit 1 (satu) kali setiap tahun.	Seluruh pegawai telah mengikuti simulasi *phishing* namun tidak dilakukan 1 (satu) kali setiap tahun.	Sebagian pegawai telah mengikuti simulasi *phishing* dan dilakukan paling sedikit 1 (satu) kali setiap tahun.	Sebagian pegawai telah mengikuti simulasi *phishing* namun tidak dilakukan 1 (satu) kali setiap tahun.	Belum ada simulasi *phishing* yang dilakukan BPR dan BPR Syariah.
36	BPR dan BPR Syariah menerapkan pengendalian akses berbasis peran (*Role*	BPR dan BPR Syariah telah menerapkan RBAC pada	BPR dan BPR Syariah telah menerapkan RBAC pada seluruh	BPR dan BPR Syariah telah menerapkan RBAC pada sebagian	BPR dan BPR Syariah telah menerapkan RBAC pada sebagian	Seluruh sistem BPR dan BPR Syariah tidak

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	Based Manajemen Identitas, Access Control – RBAC) terhadap seluruh sistem, termasuk administrator dan selevel administrator.	seluruh sistem BPR dan BPR Syariah dan dilakukan evaluasi secara berkala.	sistem BPR dan BPR Syariah namun tidak dilakukan evaluasi secara berkala.	sistem BPR dan BPR Syariah dan dilakukan evaluasi secara berkala.	sistem BPR dan BPR Syariah namun tidak dilakukan evaluasi secara berkala.	menerapkan RBAC.
37	Setiap pegawai menggunakan *single* ID yang unik dan kata sandi pribadi untuk mengakses perangkat komputer.	Setiap pegawai memiliki dan menggunakan *single* ID yang unik untuk mengakses perangkat komputer.	Sebagian pegawai memiliki dan menggunakan *single* ID yang unik untuk mengakses perangkat komputer.	Setiap pegawai memiliki dan menggunakan *single* ID yang unik untuk mengakses perangkat komputer namun masih terdapat praktik berbagi *user* ID antar pegawai.	Sebagian pegawai memiliki dan menggunakan *single* ID yang unik untuk mengakses perangkat komputer namun masih terdapat praktik berbagi *user* ID antar pegawai.	Tidak terdapat kebijakan *single* ID yang unik setiap pegawai.
38	BPR dan BPR Syariah menerapkan kontrol operasional manajemen akses pengguna pada seluruh sistem, termasuk penegakan otomatis kompleksitas kata sandi, masa kedaluwarsa, riwayat, dan penguncian akun	BPR dan BPR Syariah menerapkan kontrol sandi secara terpusat atas seluruh sistem yang meliputi kompleksitas, kedaluwarsa,	BPR dan BPR Syariah menerapkan kontrol sandi secara terpusat atas seluruh sistem yang meliputi kompleksitas, kedaluwarsa, riwayat, dan *lockout*	BPR dan BPR Syariah menerapkan kontrol sandi secara terpusat atas sebagian sistem yang meliputi kompleksitas, kedaluwarsa,	BPR dan BPR Syariah menerapkan kontrol sandi secara terpusat atas sebagian sistem yang meliputi kompleksitas, kedaluwarsa,	BPR dan BPR Syariah belum menerapkan kontrol sandi secara terpusat atas sistem yang dimiliki.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	(*lockout*) sesuai dengan kebijakan/prosedur yang telah ditetapkan.	riwayat, dan *lockout* sesuai dengan kebijakan, serta memantau kepatuhannya secara berkala.	sesuai dengan kebijakan, namun belum memantau kepatuhannya secara berkala.	riwayat, dan *lockout* sesuai dengan kebijakan, dan memantau kepatuhannya secara berkala.	riwayat, dan *lockout* sesuai dengan kebijakan, namun belum memantau kepatuhannya secara berkala.	
39	BPR dan BPR Syariahmelakukan pemisahan jaringan dengan menggunakan *Service Set Identifier* (SSID) terpisah untuk pegawai dan tamu/pengunjung, serta menerapkan pengamanan teknis (misalnya *Virtual Local Area Network* - VLAN) untuk membatasi akses.	BPR dan BPR Syariahtelah menerapkan *Service Set Identifier* (SSID) terpisah untuk pegawai dan tamu/pengunjung , serta melengkapinya dengan pengamanan teknis untuk membatasi akses terhadap seluruh jaringan.	BPR dan BPR Syariahtelah menerapkan *Service Set Identifier* (SSID) terpisah untuk pegawai dan tamu/pengunjung, serta melengkapinya dengan pengamanan teknis untuk membatasi akses terhadap sebagian jaringan.	BPR dan BPR Syariahtelah menerapkan *Service Set Identifier* (SSID) terpisah untuk pegawai dan tamu/pengunjung, namun belum dilengkapi dengan penerapan pengamanan teknis untuk membatasi akses jaringan.	BPR dan BPR Syariah belum memisahkan *Service Set Identifier* (SSID) dan hanya membatasi akses dengan sandi atau aturan manual.	BPR dan BPR Syariah belum menerapkan pemisahan jaringan.
40	BPR dan BPR Syariah menerapkan kontrol operasional siklus hidup aset TI yang meliputi inventarisasi dan	BPR dan BPR Syariahmenerapkan kontrol operasional siklus	BPR dan BPR Syariah menerapkan kontrol operasional	BPR dan BPR Syariah menginventarisasi dan identifikasi *End-of-Life* (EOL)	BPR dan BPR Syariah menginventarisasi dan identifikasi *End-of-Life* (EOL)	BPR dan BPR Syariah tidak kontrol operasional

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	identifikasi *End-of-Life* (EOL) dan *End-of-Support* (EOS), menjalankan *patching*/*upgrade* secara terjadwal, serta menarik atau mengisolasi dari produksi setiap perangkat yang mencapai EOL/EOS sesuai dengan kebijakan/prosedur yang telah ditetapkan.	hidup atas seluruh aset TI.	siklus hidup atas sebagian aset TI.	dan *End-of-Support* (EOS), menjalankan *patching*/*upgrade* secara terjadwal, namun tidak menarik atau mengisolasi dari produksi setiap perangkat yang mencapai EOL/EOS.	dan *End-of-Support* (EOS), namun tidak menjalankan *patching*/*upgrade* secara terjadwal dan tidak menarik atau mengisolasi dari produksi setiap perangkat yang mencapai EOL/EOS.	siklus hidup atas seluruh aset TI.
41	BPR dan BPR Syariah menerapkan kontrol akses operasional saat pegawai pindah/berhenti, yaitu hak akses disesuaikan atau dinonaktifkan tepat waktu, dan seluruh perubahan tercatat di *log* sesuai dengan kebijakan/prosedur yang ditetapkan.	BPR dan BPR Syariah mengintegrasikan sistem kepegawaian (HR) dengan *Identity and Access Management* (IAM). Sehingga apabila ada pegawai yang mutasi/berhenti, maka hak akses akan disesuaikan atau	BPR dan BPR Syariah mengintegrasikan sistem kepegawaian (HR) dengan *Identity and Access Management* (IAM). Apabila ada pegawai yang mutasi/berhenti, hak akses akan disesuaikan atau dinonaktifkan secara manual di hari yang sama,	BPR dan BPR Syariah mengintegrasikan sistem kepegawaian (HR) dengan *Identity and Access Management* (IAM). Apabila ada pegawai yang mutasi/berhenti, hak akses akan disesuaikan atau dinonaktifkan secara manual dalam 3 hari kerja,	Proses tidak konsisten dan sering terlambat. Pencatatan *log* tidak lengkap atau jarang ditinjau.	Tidak terdapat prosedur terkait kontrol akses. Akses sering tetap aktif setelah pegawai pindah/berhenti dan tidak ada pencatatan *log*.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		dinonaktifkan secara otomatis, dan seluruh perubahan terekam *log* lengkap dan ditinjau berkala.	dan seluruh perubahan terekam *log* lengkap dan ditinjau berkala.	dan seluruh perubahan terekam *log* lengkap dan ditinjau berkala.		
42	BPR dan BPR Syariah menghapus (*wipe*) seluruh data pada perangkat kerja sebelum perangkat dimusnahkan/dialihkan. Selanjutnya hasilnya akan diverifikasi dan buktinya dicatat, sesuai dengan kebijakan/prosedur yang ditetapkan.	BPR dan BPR Syariah melakukan *wipe* dengan metode/*tools* yang sesuai standar, memverifikasi hasilnya, dan mengadministrasikan secara tertib bukti pendukungnya (a.l. *log*, sertifikat penghapusan) atas seluruh perangkat kerja yang akan dimusnahkan/dialihkan.	BPR dan BPR Syariah melakukan *wipe* dengan metode/*tools* yang sesuai standar, memverifikasi hasilnya, namun belum mengadministrasikan secara tertib bukti pendukungnya (a.l. *log*, sertifikat penghapusan) atas seluruh perangkat kerja yang akan dimusnahkan/dialihkan.	BPR dan BPR Syariah melakukan *wipe* dengan metode/*tools* yang sesuai standar, memverifikasi hasilnya, dan mengadministrasikan secara tertib bukti pendukungnya (a.l. *log*, sertifikat penghapusan) atas sebagian perangkat kerja yang akan dimusnahkan/dialihkan.	BPR dan BPR Syariah melakukan *wipe* dengan metode/*tools* yang sesuai standar, memverifikasi hasilnya, namun belum mengadministrasikan secara tertib bukti pendukungnya (a.l. *log*, sertifikat penghapusan) atas sebagian perangkat kerja yang akan dimusnahkan/dialihkan.	BPR dan BPR Syariah tidak melakukan *wipe* perangkat kerja yang akan dimusnahkan/dialihkan.
43	BPR dan BPR Syariah melindungi ruang *server*/pusat data (*data*	BPR dan BPR Syariah memiliki ruang	BPR dan BPR Syariah memiliki ruang *server*/pusat	BPR dan BPR Syariah memiliki ruang *server*/pusat	BPR dan BPR Syariah memiliki ruang *server*/pusat	Server tidak ditempatkan di lokasi khusus.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	center) dengan kontrol akses fisik, antara lain kunci, kartu akses, dan/atau biometrik, serta memiliki dokumentasi terhadap akses.	*server*/pusat data yang hanya dapat diakses melalui kunci,kartu, dan/atau biometrik, terdapat pengamanan berlapis, dan terdapat dokumentasi terhadap akses.	data yang hanya dapat diakses melalui kunci,kartu, dan/atau biometrik, terdapat pengamanan minimal, dan terdapat dokumentasi terhadap akses.	data yang hanya dapat diakses melalui kunci manual dan tidak terdapat dokumentasi terhadap akses.	data, namun tidak terdapat kontrol akses.	
44	BPR dan BPR Syariah memiliki prosedur persetujuan resmi terkait permintaan akses ke sistem kritikal yang disertai dengan dokumentasi.	BPR dan BPR Syariah memiliki prosedur persetujuan resmi terkait permintaan akses ke sistem kritikal, diimplementasikan secara menyeluruh dan konsisten, serta terdapat dokumentasi yang memadai.	BPR dan BPR Syariah memiliki prosedur persetujuan resmi terkait permintaan akses ke sistem kritikal, diimplementasikan secara menyeluruh dan konsisten, serta terdapat dokumentasi yang cukup memadai.	BPR dan BPR Syariah memiliki prosedur persetujuan resmi terkait permintaan akses ke sistem kritikal, namun diimplementasikan tidak sepenuhnya diimpelementasikan secara menyeluruh, serta terdapat dokumentasi yang cukup memadai.	BPR dan BPR Syariah memiliki prosedur persetujuan resmi terkait permintaan akses ke sistem kritikal, namun diimplementasikan tidak sepenuhnya diimpelementasikan secara menyeluruh, serta terdapat dokumentasi yang kurang memadai.	BPR dan BPR Syariah tidak memiliki prosedur persetujuan resmi terkait permintaan akses ke sistem kritikal.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
45	Pengguna dengan *role administrator* di BPR dan BPR Syariah (staf TI/vendor) memakai akun admin terpisah dari akun harian. Akun admin hanya untuk tugas *privileged*.	Seluruh pengguna dengan *role administrator* telah menggunakan akun admin yang terpisah dari akun harian, dan aktivitasnya tercatat.	Seluruh pengguna dengan *role administrator* telah menggunakan akun admin yang terpisah dari akun harian, namun aktivitasnya belum sepenuhnya tercatat.	Sebagian pengguna dengan *role administrator* telah menggunakan akun admin yang terpisah dari akun harian, dan aktivitasnya tercatat.	Sebagian pengguna dengan *role administrator* telah menggunakan akun admin yang terpisah dari akun harian, namun aktivitasnya belum sepenuhnya tercatat.	Tidak ada pemisahan akun admin dan akun harian untuk pengguna dengan *role administrator*.
46	Seluruh sistem kritikal dilindungi dengan otentikasi multifaktor (*Multi Factor Authentication* - MFA).	Seluruh sistem kritikal menerapkan MFA dan dipantau secara berkala.	Sebagian besar sistem kritikal menerapkan MFA namun tidak dipantau secara berkala.	Sebagian kecil sistem kritikal menerapkan MFA dan dipantau secara berkala.	Sebagian kecil sistem kritikal menerapkan MFA namun tidak dipantau secara berkala.	Sistem kritikal BPR dan BPR Syariah tidak menerapkan MFA.
47	BPR dan BPR Syariahmelakukan audit berkala terhadap hak akses pegawai berdasarkan klasifikasi data dan informasi.	BPR dan BPR Syariah melakukan audit terhadap hak akses pegawai berdasarkan klasifikasi data dan informasi secara berkala.	BPR dan BPR Syariah melakukan audit terhadap hak akses pegawai berdasarkan klasifikasi data dan informasi secara berkala namun tidak mencakup seluruh aspek.	BPR dan BPR Syariah melakukan audit terhadap hak akses pegawai berdasarkan klasifikasi data dan informasi secara tidak terjadwal atau tidak secara berkala.	BPR dan BPR Syariah melakukan audit terhadap hak akses pegawai berdasarkan klasifikasi data dan informasi secara tidak terjadwal atau tidak secara berkala dan belum mencakup seluruh aspek.	Tidak dilakukan audit terhadap hak akses pegawai berdasarkan klasifikasi data dan informasi.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
48	BPR dan BPR Syariah memiliki fitur yang secara otomatis memblokir koneksi dari atau ke alamat internet berbahaya (*firewall*), berdasarkan informasi dari penyedia *threat intelligence*.	BPR dan BPR Syariah telah memiliki fitur yang secara otomatis memblokir seluruh koneksi dari atau ke alamat internet berbahaya (*firewall*) berdasarkan informasi dari penyedia *threat intelligence*.	BPR dan BPR Syariah telah memiliki fitur yang secara otomatis memblokir sebagian koneksi dari atau ke alamat internet berbahaya (*firewall*) berdasarkan informasi dari penyedia *threat intelligence* namun masih terdapat pemantauan berkala.	BPR dan BPR Syariah telah memiliki fitur yang secara otomatis memblokir sebagian koneksi dari atau ke alamat internet berbahaya (*firewall*) berdasarkan informasi dari penyedia *threat intelligence* namun tidak terdapat pemantauan berkala.	BPR dan BPR Syariah memblokir secara manual berdasarkan daftar alamat internet.	BPR dan BPR Syariah tidak memblokir koneksi dari atau ke alamat internet berbahaya.
49	Instalasi perangkat lunak BPR dan BPR Syariah hanya dapat dilakukan oleh Satuan Kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI atau pihak lain dengan otorisasi dari pihak penyelenggara TI.	BPR dan BPR Syariah menerapkan pembatasan instalasi perangkat lunak secara menyeluruh dan terdapat dokumentasi *log* instalansi.	BPR dan BPR Syariah menerapkan pembatasan instalasi perangkat lunak secara menyeluruh namun tidak terdapat dokumentasi *log* instalansi.	BPR dan BPR Syariah menerapkan pembatasan instalasi perangkat lunak pada sebagian perangkat dan terdapat dokumentasi *log* instalasi.	BPR dan BPR Syariah menerapkan pembatasan instalasi perangkat lunak pada sebagian perangkat dan tidak terdapat dokumentasi *log* instalasi.	Tidak terdapat pembatasan instalasi perangkat lunak BPR dan BPR Syariah.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
50	BPR dan BPR Syariah melakukan klasifikasi antara jaringan untuk sistem kritikal dengan jaringan umum (contoh: surat elektronik).	Jaringan kritikal dan jaringan umum dipisahkan secara ketat (segregasi fisik maupun logis) dan dilakukan pengujian. keamanan dan monitoring berkala untuk memastikan efektivitas pemisahan.	Jaringan kritikal dan jaringan umum dipisahkan secara ketat (segregasi fisik maupun logis) dan dilakukan pengujian keamanan dan monitoring namun tidak berkala untuk memastikan efektivitas pemisahan.	Pemisahan jaringan dilakukan secara minimal (lebih bersifat administratif daripada teknis) dan monitoring dilakukan namun bersifat *adhoc* dan tidak konsisten.	Pemisahan jaringan dilakukan secara minimal (lebih bersifat administratif daripada teknis) dan tidak pernah dilakukan monitoring.	Seluruh sistem (kritikal dan umum) berada dalam satu jaringan tanpa perlindungan khusus.
51	BPR dan BPR Syariah menerapkan klasifikasi jaringan yang terpisah untuk layanan ATM/CDM/EDC disertai dengan enkripsi *end-to-end* atau VPN.	BPR dan BPR Syariah menerapkan klasifikasi jaringan yang terpisah untuk layanan ATM/CDM/EDC dan seluruh komunikasi data menggunakan enkripsi *end-to-end* standar industri (misalnya AES-256) atau	BPR dan BPR Syariah menerapkan klasifikasi jaringan yang terpisah untuk layanan ATM/CDM/EDC serta enkripsi atau VPN sudah diterapkan untuk sebagian besar transaksi, dengan standar keamanan yang memadai.	Pemisahan jaringan dilakukan secara terbatas, sebagian layanan ATM/CDM/EDC masih berbagi infrastruktur dengan jaringan umum dan enkripsi atau VPN diterapkan namun hanya pada titik tertentu, tidak mencakup seluruh komunikasi.	Pemisahan jaringan dilakukan secara terbatas, sebagian layanan ATM/CDM/EDC masih berbagi infrastruktur dengan jaringan umum dan enkripsi tidak selalu digunakan.	Tidak terdapat klasifikasi jaringan ATM/CDM/EDC dan tidak terenkripsi.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		VPN dengan protokol aman.				
52	BPR dan BPR Syariahmelakukan pembaruan (*update*) sistem dan aplikasi secara berkala, termasuk *patch* keamanan.	BPR dan BPR Syariahmelakukan pembaruan seluruh sistem dan aplikasi secara berkala termasuk *patch* keamanan.	Sebagian besar sistem dan aplikasi kritikal diperbarui secara berkala.	Sebagian kecil sistem dan aplikasi kritikal diperbarui secara berkala.	Pembaruan sistem dan aplikasi kritikal hanya dilakukan dalam hal terdapat kendala atau temuan.	Tidak terdapat pembaruan sistem dan aplikasi kritikal.
53	BPR dan BPR Syariah melindungi mesin ATM/CDM/EDC dengan proteksi fisik (antara lain *seal* dan CCTV) dan proteksi sistem (antara lain *anti-Malware* dan *Operating System* - OS *Lock*).	BPR dan BPR Syariah melindungi mesin ATM/CDM/EDC dengan proteksi fisik secara ketat (antara lain *seal* dan CCTV) dan proteksi sistem secara ketat.	BPR dan BPR Syariah melindungi mesin ATM/CDM/EDC dengan proteksi fisik secara ketat dan proteksi sistem secara minimal.	BPR dan BPR Syariah melindungi mesin ATM/CDM/EDC dengan proteksi fisik secara minimal dan proteksi sistem secara minimal.	BPR dan BPR Syariah melindungi mesin ATM/CDM/EDC dengan proteksi fisik dan namun tidak terdapat proteksi sistem.	Tidak terdapat proteksi fisik dan sistem pada mesin ATM/CDM/EDC.
54	BPR dan BPR Syariah memiliki prosedur tertulis terkait *change management* untuk meninjau seluruh perubahan konfigurasi.	BPR dan BPR Syariah memiliki prosedur tertulis terkait *change management* untuk meninjau seluruh perubahan	BPR dan BPR Syariah memiliki prosedur tertulis terkait *change management* untuk meninjau seluruh perubahan konfigurasi namun	BPR dan BPR Syariah memiliki prosedur tertulis terkait *change management* untuk meninjau sebagian perubahan konfigurasi namun	BPR dan BPR Syariah memiliki prosedur tertulis terkait *change management* untuk meninjau sebagian perubahan konfigurasi dan	BPR dan BPR Syariah tidak memiliki prosedur tertulis terkait *change management* untuk meninjau seluruh

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		konfigurasi dan diterapkan secara konsisten.	belum diterapkan secara konsisten.	diterapkan secara konsisten.	diterapkan secara tidak konsisten.	perubahan konfigurasi.
55	BPR dan BPR Syariah memisahkan lingkungan antara sistem produksi dengan pengembangan tanpa berbagi data atau infrastruktur.	BPR dan BPR Syariah memisahkan penuh lingkungan antara sistem produksi dengan pengembangan, tidak ada data nyata (*real data*) yang digunakan di lingkungan pengembangan, hanya data *dummy* atau *anonymized* serta terdapat kebijakan, prosedur, dan monitoring ketat untuk mencegah kebocoran maupun perubahan tidak sah.	BPR dan BPR Syariah memisahkan lingkungan antara sistem produksi dengan pengembangan tetapi masih terdapat sebagian infrastruktur jaringan yang berbagi, tidak ada data nyata (*real data*) yang digunakan di lingkungan pengembangan, hanya data *dummy* atau *anonymized* serta terdapat kebijakan, prosedur, dan monitoring ketat untuk mencegah kebocoran maupun	BPR dan BPR Syariah memisahkan sebagian lingkungan antara sistem produksi dengan pengembangan, masih terdapat praktik berbagi infrastruktur/data dengan pengawasan yang ketat.	BPR dan BPR Syariah memisahkan sebagian lingkungan antara sistem produksi dengan pengembangan, masih terdapat praktik berbagi infrastruktur/data tanpa pengawasan yang ketat.	BPR dan BPR Syariah tidak memisahkan lingkungan antara sistem produksi dengan pengembangan, data produksi digunakan bebas di lingkungan pengembangan, tidak ada kebijakan, prosedur, maupun monitoring.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
			perubahan tidak sah.			
56	BPR dan BPR Syariah melakukan enkripsi data penting (antara lain data transaksi, data nasabah, dan laporan internal) dengan menggunakan standar industri.	BPR dan BPR Syariah telah melakukan enkripsi pada seluruh data penting (antara lain data transaksi, data nasabah, dan laporan internal) dengan menggunakan standar industri.	BPR dan BPR Syariah telah melakukan enkripsi pada seluruh data penting (antara lain data transaksi, data nasabah, dan laporan internal) dengan menggunakan standar lemah.	BPR dan BPR Syariah telah melakukan enkripsi pada sebagian data penting (antara lain data transaksi, data nasabah, dan laporan internal) dengan menggunakan standar industri.	BPR dan BPR Syariah telah melakukan enkripsi pada sebagian data penting (antara lain data transaksi, data nasabah, dan laporan internal) dengan menggunakan standar yang lemah.	BPR dan BPR Syariah tidak melakukan enkripsi pada seluruh data penting.
57	BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data termasuk namun tidak terbatas pada pelindungan data, transfer data, dan penghapusan data.	BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data dan seluruhnya diterapkan secara memadai.	BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data dan seluruhnya diterapkan secara cukup memadai.	BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data namun hanya sebagian besar diterapkan secara memadai.	BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data namun sebagian kecil diterapkan secara memadai.	BPR dan BPR Syariah tidak memiliki prosedur tertulis terkait metode manajemen data.
58	BPR dan BPR Syariah secara berkala melakukan edukasi kepada Nasabah	BPR dan BPR Syariah secara berkala melakukan	BPR dan BPR Syariah secara berkala melakukan edukasi kepada	BPR dan BPR Syariah tidak secara berkala melakukan edukasi	BPR dan BPR Syariah tidak secara berkala melakukan edukasi	BPR dan BPR Syariah tidak melakukan edukasi kepada

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi melalui berbagai kanal komunikasi.	edukasi kepada Nasabah mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi melalui berbagai kanal komunikasi dan materi edukasi komprehensif mencakup tren ancaman terbaru, tips keamanan, serta panduan praktis.	Nasabah mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi melalui kanal komunikasi terbatas dan materi edukasi yang terbatas.	kepada Nasabah mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi melalui berbagai kanal komunikasi dan materi edukasi masih bersifat umum.	kepada Nasabah mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi melalui kanal komunikasi yang terbatas dan materi edukasi yang minim.	Nasabah mengenai potensi risiko siber dalam penggunaan produk yang berbasis teknologi informasi.
59	BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk sistem kritikal.	BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk seluruh sistem kritikal dan dilakukan penginian secara berkala.	BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk seluruh sistem kritikal dan dilakukan penginian secara terbatas.	BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk sebagian sistem kritikal dan dilakukan penginian secara terbatas.	BPR dan BPR Syariah menerapkan metode autentikasi berbasis sertifikat digital untuk sebagian besar sistem kritikal dan tidak dilakukan penginian.	Sistem kritikal BPR dan BPR Syariah tidak dilakukan autentikasi berbasis sertifikat digital.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
60	BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut (*Attribute Based Access Control* - ABAC) untuk sistem kritikal (misalnya *Core Banking System*). Penerapan ABAC dilakukan dengan mempertimbangkan faktor antara lain lokasi, waktu, perangkat, dan tingkat risiko.	BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut ABAC pada seluruh sistem kritikal serta dilakukan penginian secara berkala.	BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut ABAC pada seluruh sistem kritikal serta dilakukan penginian secara terbatas.	BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut ABAC pada sebagian sistem kritikal serta dilakukan penginian secara terbatas.	BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut ABAC pada sebagian sistem kritikal serta tidak dilakukan penginian.	Sistem kritikal BPR dan BPR Syariah tidak menerapkan ABAC.
61	BPR dan BPR Syariah yang memberikan layanan digital menerapkan *Data Loss Prevention* (DLP) pada *endpoint* dan *gateway*.	BPR dan BPR Syariah yang memberikan layanan digital menerapkan *Data Loss Prevention* (DLP) pada seluruh *endpoint* dan *gateway* dan dimonitoring secara berkala.	BPR dan BPR Syariah yang memberikan layanan digital menerapkan *Data Loss Prevention* (DLP) pada seluruh *endpoint* dan *gateway* namun dimonitoring secara tidak berkala.	BPR dan BPR Syariah yang memberikan layanan digital menerapkan *Data Loss Prevention* (DLP) pada sebagian *endpoint* dan *gateway* dan dimonitoring secara berkala.	BPR dan BPR Syariah yang memberikan layanan digital menerapkan *Data Loss Prevention* (DLP) pada sebagian *endpoint* dan *gateway* namun dimonitoring secara tidak berkala.	*Endpoint* dan *gateaway* tidak menerapkan DLP.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
62	BPR dan BPR Syariah menerapkan pembatasan nominal transaksi dan jenis transaksi.	BPR dan BPR Syariah menerapkan pembatasan nominal transaksi dan jenis transaksi dan terdapat mekanisme reviu menyeluruh dan penyesuaian berkala terhadap batasan transaksi sesuai tren risiko.	BPR dan BPR Syariah menerapkan pembatasan nominal transaksi dan jenis transaksi dan terdapat mekanisme reviuterbatas dan penyesuaian berkala terhadap batasan transaksi sesuai tren risiko.	BPR dan BPR Syariah hanya menerapkan pembatasan nominal transaksi dan terdapat mekanisme reviudan penyesuaian berkala terhadap batasan transaksi sesuai tren risiko.	BPR dan BPR Syariah hanya menerapkan pembatasan nominal transaksi namun tidak terdapat mekanisme reviu.	BPR dan BPR Syariah tidak menerapkan pembatasan nominal dan jenis transaksi.
63	Apabila terjadi percobaan *login* gagal, sistem kritikal BPRdan BPR Syariah akan memantau, mengirimkan *alert* otomatis ke Tim Keamanan, serta mengunci akun setelah ambang batas (*threshold*) percobaan terlampaui, guna mendeteksi lebih dini terhadap upaya serangan siber	Seluruh sistem kritikal melakukan pemantauan *real-time*, terintegrasi dengan SIEM/SOAR, *alert* diteruskan ke SOC 24×7, ambang batas disesuaikan profil risiko, dan efektivitasnya diuji berkala.	Seluruh sistem kritikal melakukan pemantauan *real-time*, namun belum terintegrasi dengan SIEM/SOAR, *alert* diteruskan ke SOC 24×7, ambang batas disesuaikan profil risiko, dan efektivitasnya diuji berkala.	Sebagian besar sistem kritikal telah memantau *real-time* dan mengirim *alert* otomatis, namun belum seluruhnya terhubung ke SIEM/SOAR atau belum diuji secara berkala.	Pencatatan *login* gagal tersedia, tetapi pemantauan *real-time* dan *alert* masih bersifat manual/*adhoc*, dan akun tetap dikunci otomatis.	Tidak ada mekanisme pemantauan *real-time* atau alert otomatis atas percobaan-*login* gagal.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
64	Perangkat Kerja BPR dan BPR Syariah telah dilindungi dengan sistem keamanan berbasis perilaku yang mampu mendeteksi perilaku mencurigakan dan serangan yang belum dikenal Sistem keamanan berbasis perilaku misalnya *Endpoint Detection and Response* (EDR).	Seluruh perangkat kerja BPR dan BPR Syariah dilindungi oleh sistem keamanan berbasis perilaku dan terdapat dokumentasi *log* yang memadai.	Seluruh perangkat kerja BPR dan BPR Syariah dilindungi oleh sistem keamanan berbasis perilaku namun dokumentasi *log* kurang memadai.	Sebagian perangkat kerja BPR dan BPR Syariah dilindungi oleh sistem keamanan berbasis perilaku dan terdapat dokumentasi *log*.	Perangkat kerja BPR dan BPR Syariah tidak dilindungi oleh sistem keamanan berbasis perilaku, namun dilindungi menggunakan anti virus tradisional dan terdapat dokumentasi *log* yang minimal.	Seluruh perangkat kerja BPR dan BPR Syariah tidak dilindungi oleh sistem keamanan berbasis perilaku.
65	Layanan *Mobile Banking* BPR dan BPR Syariah dilengkapi dengan mekanisme deteksi berbasis perilaku dan pemberitahuan *real-time* atas transaksi tidak biasa (*unusual transaction*)	BPR dan BPR Syariah memiliki mekanisme deteksi berbasis perilaku dan pemberitahuan *real-time* atas transaksi tidak biasa (*unusual transaction*), monitoring dan pelaporan *real-time* dilakukan untuk mendeteksi anomali, terdapat	BPR dan BPR Syariah memiliki mekanisme deteksi berbasis perilaku dan pemberitahuan *real-time* atas transaksi tidak biasa (*unusual transaction*) dan monitoring dan pelaporan periodik dilakukan untuk mendeteksi anomali, terdapat	BPR dan BPR Syariah hanya memiliki pemberitahuan *real-time* atas transaksi tidak biasa (*unusual transaction*) berdasarkan aturan sederhana.	Pemberitahuan jarang diberikan atau hanya terbatas pada beberapa jenis transaksi.	BPR dan BPR Syariah tidak memiliki mekanisme deteksi berbasis perilaku dan pemberitahuan *real-time* atas transaksi tidak biasa (*unusual transaction*).

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		tindak lanjut otomatis.	tindak lanjut semimanual.			
66	BPR dan BPR Syariah memiliki prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan yang diuji secara berkala.	BPR dan BPR Syariah memiliki prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan yang diuji secara berkala.	BPR dan BPR Syariah memiliki prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan yang diuji secara berkala namun belum mencakup seluruh aspek.	BPR dan BPR Syariah memiliki prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan yang diuji secara tidak terjadwal.	BPR dan BPR Syariah dalam proses penyusunan prosedur respons insiden siber tertulis yang mencakup deteksi, pelaporan, eskalasi, penanganan, dan pemulihan.	Tidak terdapat prosedur respons insiden.
67	BPR dan BPR Syariah memiliki matriks eskalasi insiden siber yang mengategorisasikan kejadian berdasarkan tingkat keparahan/prioritas/dampak dan jalur komunikasi pelaporan.	BPR dan BPR Syariah memiliki matriks eskalasi insiden siber dan jalur komunikasi serta tanggung jawab setiap level ditetapkan secara detail dan tertulis, serta evaluasi efektivitas dilakukan rutin dan matriks	BPR dan BPR Syariah memiliki matriks eskalasi insiden siber dan jalur komunikasi pelaporan secara tertulis, namun belum diterapkan secara konsisten serta perubahan atau pembaruan matriks dilakukan hanya saat ada	BPR dan BPR Syariah memiliki matriks eskalasi insiden siber dan jalur komunikasi pelaporan secara tertulis, namun belum ada pengujian atau simulasi formal untuk memastikan efektivitas eskalasi.	BPR dan BPR Syariah memiliki matriks eskalasi insiden siber yang tidak jelas dan jalur komunikasi pelaporan secara lisan, dan belum ada pengujian atau simulasi formal untuk memastikan efektivitas eskalasi.	BPR dan BPR Syariah tidak memiliki matriks eskalasi insiden siber dan tidak terdapat jalur komunikasi pelaporan.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		diperbarui mengikuti perkembangan ancaman.	kebutuhan atau insiden besar.			
68	BPR dan BPR Syariah memiliki prosedur tertulis ketahanan dan keamanan siber terkait pelaporan kejadian mencurigakan dan disosialisasikan kepada seluruh pegawai.	BPR dan BPR Syariah memiliki dan menerapkan prosedur tertulis mengenai pelaporan kejadian mencurigakan serta disosialisasikan kepada seluruh pegawai dan terdapat pengukuran efektivitas atas pemahaman pegawai.	BPR dan BPR Syariah memiliki dan menerapkan prosedur tertulis mengenai pelaporan kejadian mencurigakan serta disosialisasikan kepada seluruh pegawai namun belum terdapat terdapat pengukuran efektivitas atas pemahaman pegawai.	BPR dan BPR Syariah memiliki dan menerapkan prosedur tertulis mengenai pelaporan kejadian mencurigakan serta disosialisasikan kepada satuan kerja/pegawai tertentu dan belum terdapat terdapat pengukuran efektivitas atas pemahaman pegawai.	BPR dan BPR Syariah tidak memiliki prosedur tertulis mengenai pelaporan kejadian mencurigakan, namun telah menerapkan pelaporan kejadian mencurigakan secara minimal.	BPR dan BPR Syariah tidak memiliki prosedur tertulis mengenai pelaporan kejadian mencurigakan.
69	BPR dan BPR Syariah melaksanakan simulasi tanggap insiden siber secara berkala dan terdokumentasi.	BPR dan BPR Syariah melaksanakan simulasi secara rutin yang disertai dengan	BPR dan BPR Syariah melaksanakan simulasi secara rutin namun dengan	BPR dan BPR Syariah melaksanakan simulasi, namun tidak secara berkala dan masih terdapat	BPR dan BPR Syariah melaksanakan simulasi, namun tidak secara berkala dan tidak terdapat	BPR dan BPR Syariah tidak melaksanakan simulasi tanggap darurat insiden siber.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		dokumentasi yang memadai.	dokumentasi yang cukup memadai.	dokumentasi yang kurang memadai.	dokumentasi yang memadai.	
70	BPR dan BPR Syariah menetapkan mekanisme untuk melakukan evaluasi kesesuaian prosedur dan *root cause analysis* serta dilakukan tindak lanjut pascainsiden siber.	BPR dan BPR Syariah telah menetapkan mekanisme untuk melakukan evaluasi kesesuaian prosedur dan *root cause analysis* secara menyeluruh dan dilakukan tindak lanjut pascainsiden siber.	BPR dan BPR Syariah telah menetapkan mekanisme untuk melakukan evaluasi kesesuaian prosedur dan *root cause analysis* secara terbatas dan dilakukan tindak lanjut pascainsiden siber.	BPR dan BPR Syariah menetapkan mekanisme evaluasi setiap terjadi insiden siber, namun tidak disertai mekanisme tindak lanjut.	BPR dan BPR Syariah hanya menetapkan mekanisme evaluasi apabila terjadi insiden siber yang signifikan atau berulang.	BPR dan BPR Syariah tidak menetapkan evaluasi dan tindak lanjut untuk setiap insiden siber.
71	BPR dan BPR Syariah memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber yang telah ditetapkan oleh Direksi. Prosedur didokumentasikan secara memadai dan dikomunikasikan kepada seluruh pegawai.	BPR dan BPR Syariah telah memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber yang telah ditetapkan oleh Direksi, didokumentasikan secara memadai,	BPR dan BPR Syariah telah memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber yang telah ditetapkan oleh Direksi, didokumentasikan secara cukup	BPR dan BPR Syariah telah memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber yang telah ditetapkan oleh Direksi, didokumentasikan secara kurang	BPR dan BPR Syariah sedang dalam proses penyusunan prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber dan praktik yang dilakukan	BPR dan BPR Syariah tidak memiliki prosedur komunikasi dalam penanggulangan dan pemulihan insiden siber.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		serta dikomunikasikan kepada seluruh pegawai.	memadai, serta dikomunikasikan kepada seluruh pegawai.	memadai, serta dikomunikasikan kepada pegawai tertentu.	berdasarkan *adhoc* atau lisan.	
72	BPR dan BPR Syariah memiliki dan menerapkan prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber.	BPR dan BPR Syariah telah memiliki dan menerapkan prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber dan dievaluasi secara berkala.	BPR dan BPR Syariah telah memiliki dan menerapkan prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber dan dievaluasi secara berkala namun belum mencakup seluruh aspek.	BPR dan BPR Syariah telah memiliki dan menerapkan prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber namun dievaluasi secara tidak terjadwal.	BPR dan BPR Syariah telah memiliki dan tidak sepenuhnya menerapkan prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber dan evaluasi hanya dilakukan ketika terdapat serangan siber.	BPR dan BPR Syariah tidak memiliki prosedur teknis *containment* dan isolasi sistem yang terindikasi terinfeksi *malware*/terkena serangan siber.
73	Dalam hal terjadi insiden, BPR dan BPR Syariah segera membatasi dan mengisolasi (eradikasi) sistem yang diduga terinfeksi *malware* atau diserang, sesuai	BPR dan BPR Syariah segera membatasi dan mengisolasi (eradikasi) sistem utama dan seluruh sistem terkait yang	BPR dan BPR Syariahsegera membatasi dan mengisolasi (eradikasi) sistem utama dan sebagian sistem terkait yang diduga	BPR dan BPR Syariah segera membatasi, namun tidak mengisolasi (eradikasi) sistem utama dan seluruh sistem terkait yang diduga terinfeksi	BPR dan BPR Syariah segera membatasi, namun tidak langsung mengisolasi (eradikasi) sistem utama dan sebagian sistem	BPR dan BPR Syariahtidak membatasi dan mengisolasi (eradikasi) baik sistem utamamaupun sistem terkait

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	prosedur teknis yang diterapkan sebelum layanan dipulihkan.	diduga terinfeksi *malware* atau diserang sebelum layanan dipulihkan.	terinfeksi *malware* atau diserang sebelum layanan dipulihkan.	*malware* atau diserang sebelum layanan dipulihkan.	terkait yang diduga terinfeksi *malware* atau diserang sebelum layanan dipulihkan.	yang diduga terinfeksi *malware* atau diserang sebelum layanan dipulihkan.
74	BPR dan BPR Syariah memiliki Rencana Pemulihan Bencana (*Disaster Recovery Plan* - DRP) dan mengimplementasikan-nya guna memulihkan layanan apabila terjadi insiden.	BPR dan BPR Syariah memiliki DRP yang terdokumentasi atas seluruh sistem secara komprehensif (a.l. mencakup skenario positif dan negatif, RTO dan RPO telah ditetapkan), dan mengimplementasi -kan DRP secara konsisten saat terjadi insiden siber.	BPR dan BPR Syariah memiliki DRP yang terdokumentasi atas sebagian sistem secara komprehensif (a.l. mencakup skenario positif dan negatif, RTO dan RPO telah ditetapkan), dan mengimplementasi kan DRP secara konsisten saat terjadi insiden siber.	BPR dan BPR Syariah memiliki DRP yang terdokumentasi atas seluruh sistem secara komprehensif (a.l. mencakup skenario positif dan negatif, RTO dan RPO telah ditetapkan), namun belum sepenuhnya mengimplementasi kan DRP secara konsisten saat terjadi insiden siber.	BPR dan BPR Syariah memiliki DRP yang terdokumentasi atas sebagian sistem secara komprehensif (a.l. mencakup skenario positif dan negatif, RTO dan RPO telah ditetapkan), namun belum sepenuhnya mengimplementa-sikan DRP secara konsisten saat terjadi insiden siber.	BPR dan BPR Syariah tidak memiliki DRP.
75	BPR dan BPR Syariah wajib melakukan rekam cadang (*back up*) setiap akhir hari untuk	BPR dan BPR Syariah melakukan rekam cadang (*back up*)	BPR dan BPR Syariah melakukan rekam cadang (*back up*) setiap akhir	BPR dan BPR Syariah melakukan rekam cadang (*backup*) dilakukan	BPR dan BPR Syariah melakukan rekam cadang (*backup*) tidak	Tidak terdapat mekanisme backup yang

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	seluruh data aktivitas BPR dan BPR Syariah.	setiap akhir hari untuk seluruh data aktivitas BPRdan BPR Syariah dan ditempatkan pada media yang terpisah (minimal 2 media yg berbeda).	hari untuk seluruh data aktivitas BPRdan BPR Syariah dan ditempatkan pada media yang terpisah.	setiap akhir hari, namun masih menggunakan proses manual.	setiap hari (misalnyadilakukan setiap minggu).	dilakukan secara berkala.
76	BPR dan BPR Syariah melakukan pengujian *restorebackup* data secara berkala paling sedikit 1 (satu) kali dalam 1(satu) tahun.	BPR dan BPR Syariah melakukan pengujian *restore backup data* secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan disertai dengan dokumen pendukung yang memadai.	BPR dan BPR Syariah melakukan pengujian *restore backup data* secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan disertai dengan dokumen pendukung yang cukup memadai.	BPR dan BPR Syariah melakukan pengujian *restore backupdata* secara tidak terjadwal dan disertai dengan dokumen pendukung yang cukup memadai.	BPR dan BPR Syariah melakukan pengujian *restore backup data* secara tidak terjadwal dan tidak disertai dengan dokumen pendukung.	Tidak dilakukan pengujian *restore backupdata*.
77	BPR dan BPR Syariah melakukan analisis kritikalitas sistem penting dengan menetapkan sasaran	BPR dan BPR Syariah melakukan analisis kritikalitas sistem	BPR dan BPR Syariah melakukan analisis kritikalitas sistem penting dengan	BPR dan BPR Syariah melakukan analisis kritikalitas sistem penting dengan	RTO dan RPO belum ditetapkan secara formal dan masih berupa asumsi teknis.	Tidak ditetapkan RTO dan RPO untuk sistem penting.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
	waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO).	penting dengan menetapkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO) serta diimplementasikan.pada seluruh sistem penting.	menetapkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO) serta diimplementasikan pada sebagian besar sistem penting.	menetapkan sasaran waktu pemulihan (*Recovery Time Objective* - RTO) dan sasaran titik pemulihan (*Recovery Point Objective* - RPO) serta diimplementasikan pada sebagian kecil sistem penting.		
78	BPR dan BPR Syariah melakukan kaji ulang terhadap Rencana Pemulihan Bencana (*Disaster Recovery Plan*/DRP) insiden siber secara berkala, termasuk melakukan pengujian *failover*.	BPR dan BPR Syariah melakukan kaji ulang terhadap rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) insiden siber secara berkala, termasuk melakukan pengujian *failover*, dan perbaikan	BPR dan BPR Syariah melakukan kaji ulang terhadap rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) insiden siber secara berkala, termasuk melakukan pengujian *failover*, dan namun perbaikan tidak dilakukan secara segera.	Melakukan kaji ulang terhadap rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) insiden siber namun tidak secara berkala, dan masih terdapat pengujian *failover*.	Melakukan kaji ulang terhadap rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) insiden siber namun tidak secara berkala dan tidak terdapat pengujian *failover*.	Tidak melakukan kaji ulang terhadap rencana pemulihan bencana (*Disaster Recovery Plan*/DRP).

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	**2 - Memadai**	**3 – Cukup Memadai**	**4 - Kurang Memadai**	**5 - Tidak Memadai**
		dilakukan secara segera.				
79	BPR dan BPR Syariah memiliki prosedur notifikasi kepada regulator ataupun lembaga eksternal (misal OJK, BI, dll) yang menetapkan batas waktu, media, dan tanggung jawab pelaporan setelah terjadinya insiden siber.	BPR dan BPR Syariah memiliki prosedur notifikasi yang dijalankan dengan konsisten, dimana seluruh notifikasi tercatat lengkap dan batas waktu pelaporan selalu terpenuhi.	BPR dan BPR Syariah memiliki prosedur notifikasi yang dijalankan dengan konsisten, namun belum semua notifikasi tercatat lengkap dan batas waktu pelaporan selalu terpenuhi.	BPR dan BPR Syariah memiliki prosedur notifikasi yang dijalankan kurang konsisten, dan belum semua notifikasi tercatat lengkap dan batas waktu pelaporan selalu terpenuhi.	BPR dan BPR Syariah memiliki prosedur notifikasi yang dijalankan kurang konsisten, dan belum semua notifikasi tercatat lengkap dan batas waktu pelaporan terkadang belum terpenuhi.	BPR dan BPR Syariah belum memiliki prosedur notifikasi insiden kepada regulator atau lembaga eksternal.
80	BPR dan BPR Syariah menetapkan mekanisme komunikasi kepada nasabah dan publik ketika insiden siber terjadi. Mekanisme komunikasi meliputi: penetapan saluran resmi, proses persetujuan pesan, dan panduan pertanyaan-jawaban, serta melakukan pelatihan	BPR dan BPR Syariah memiliki mekanisme komunikasi kepada nasabah dan publik dan terdokumentasi dengan memadai, melakukan simulasi (*table-top exercise*) minimal 1 (satu) tahun sekali.	BPR dan BPR Syariah memiliki mekanisme komunikasi kepada nasabah dan publik dan terdokumentasi dengan memadai, melakukan simulasi (*table-top exercise*) tidak secara berkala.	BPR dan BPR Syariah memiliki mekanisme komunikasi kepada nasabah dan publik dan terdokumentasi kurang memadai, melakukan simulasi (*table-top exercise*) tidak secara berkala.	BPR dan BPR Syariah memiliki mekanisme komunikasi kepada nasabah dan publik dan terdokumentasi dengan memadai, tidak pernah melakukan simulasi (*table-top exercise*).	BPR dan BPR Syariah belum memiliki mekanisme komunikasi kepada nasabah ataupun publik apabila insiden siber terjadi.

No	Parameter Penilaian	Kriteria Penilaian				
		1 - Sangat Memadai	2 - Memadai	3 – Cukup Memadai	4 - Kurang Memadai	5 - Tidak Memadai
	atas mekanisme tersebut.					

E. RINGKASAN PENILAIAN TINGKAT MATURITAS KEAMANAN SIBER

Periode Penilaian :
Nama BPR atau BPR Syariah :
Kategori BPRatau BPR Syariah* : Kategori 1 / Kategori 2

Domain	**Bobot**	**Peringkat Domain**	**Nilai Komposit**
	(a)	**(b)**	**(c) = (a) x (b)**
Tata Kelola	25%		
Identifikasi	15%		
Pelindungan	25%		
Deteksi	15%		
Penanggulangan dan Pemulihan	20%		
Nilai Komposit			
Peringkat Komposit			

Keterangan:
*coret yang tidak perlu.
(a) Bobot sesuai yang ditetapkan untuk setiap domain.
(b) Peringkat domain merupakan peringkat yang diperoleh dari nilai rata-rata peringkat parameter dari setiap domain.
(c) Nilai komposit merupakan hasil perkalian bobot (a) dengan peringkat domain (b)

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN V
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 43/PADK.03/2025
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH
BANK PEREKONOMIAN RAKYAT DAN
BANK PEREKONOMIAN RAKYAT SYARIAH

PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH

PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI

A. PENGELOLAAN DATA

Pengelolaan data memperhatikan paling sedikit:
a. kualitas data;
b. sistem pengelolaan data; dan
c. sumber daya pendukung pengelolaan data,
antara lain mencakup aktivitas:

1. melakukan pengembangan dan upaya menjaga dan/atau memperbaiki kualitas data
   a. BPR dan BPR Syariah menetapkan standar, persyaratan, dan spesifikasi penerapan kontrol kualitas data.
   b. BPR dan BPR Syariah melakukan identifikasi permasalahan terkait kualitas data.
   c. BPR dan BPR Syariah melakukan upaya peningkatan kualitas data yang diidentifikasi.
   d. BPR dan BPR Syariah melakukan evaluasi tingkat kualitas data.
2. memiliki kebijakan mengenai pembagian tugas dan kewenangan pengelolaan data
   a. BPR dan BPR Syariah memiliki kebijakan mengenai tugas dan tanggung jawab dalam pengelolaan data.
   b. BPR dan BPR Syariah menetapkan pembagian tugas dan wewenang pengelolaan data sesuai kompleksitas usaha BPR dan BPR Syariah.
   c. Direksi dan Dewan Komisaris BPR dan BPR Syariah memahami dan secara aktif menerapkan prinsip pemrosesan data dalam rangka pelindungan data di BPR dan BPR Syariah, serta bertanggung jawab atas kepatuhan terhadap prinsip-prinsip tersebut.
   d. BPR dan BPR Syariah menetapkan kebijakan dan prosedur pengelolaan data secara memadai.
3. memiliki kebijakan dan prosedur pengelolaan data
   a. BPR dan BPR Syariah memiliki kebijakan data yang memuat paling sedikit prinsip dan tujuan BPR dan BPR Syariah dalam pengelolaan data serta aturan dasar yang mengatur pembuatan, akuisisi, keamanan, kualitas, dan penggunaan data dan informasi, termasuk klasifikasi data, serta pemrosesan data nasabah dan calon nasabah.
   b. BPR dan BPR Syariah menetapkan klasifikasi data berdasarkan kritikalitas dan sensitivitas dari masing-masing jenis data.
   c. BPR dan BPR Syariah memiliki kebijakan kontrol akses pengelolaan data sesuai klasifikasi data.
      BPR dan BPR Syariah memiliki prosedur dan menerapkan kontrol akses berbasis atribut (*Attribute Based Access Control* - ABAC) untuk sistem kritikal (misal *Core Banking System*).
      Penerapan ABAC dilakukan dengan mempertimbangkan faktor antara lain lokasi, waktu, perangkat, dan tingkat risiko.
   d. BPR dan BPR Syariah memiliki kebijakan dan strategi pelindungan data sesuai peraturan perundang-undangan mengenai pelindungan data pribadi.
   e. BPR dan BPR Syariah memiliki kebijakan dan prosedur pemrosesan data yang memuat antara lain:
      1) pemrosesan data secara adil dan transparan, seperti data nasabah/calon nasabah diperoleh dengan cara yang sah

serta dipergunakan secara sah dan tidak dipergunakan untuk perbuatan melanggar hukum;
2) proses pengumpulan data nasabah atau calon nasabah;
3) informasi yang diberikan kepada individu dan pelaksanaan hak individu;
4) langkah teknis pengelolaan keamanan data;
5) prosedur penyelesaian perselisihan dengan nasabah terkait akurasi pencatatan data nasabah;
6) pengelolaan dokumentasi setiap tahap pemrosesan data;
7) pelaporan kebocoran data nasabah; dan
8) analisis dampak pemrosesan data.

4. melakukan pengelolaan data secara memadai
   a. BPR dan BPR Syariah memiliki arsitektur data sebagai bagian dari arsitektur TI.
   b. BPR dan BPR Syariah menerapkan pelindungan data dan informasi, mencakup:
      1) penetapan standar pengamanan data sesuai dengan klasifikasi data; dan
      2) implementasi kontrol dan prosedur pengamanan data dan informasi.
   c. BPR dan BPR Syariah mengelola integrasi dan interoperabilitas data. Integrasi data dan interoperabilitas menggambarkan proses terkait pergerakan dan konsolidasi data di dalam dan antara penyimpanan data, aplikasi, dan organisasi. Integrasi merupakan penggabungan data ke dalam bentuk yang konsisten, baik fisik maupun virtual. Interoperabilitas data merupakan kemampuan beberapa sistem untuk berkomunikasi. Penerapan integrasi dan interoperabilitas data memastikan BPR dan BPR Syariah dapat memperoleh data di manapun, kapanpun, dan dalam bentuk apapun sesuai kebutuhan.
   d. BPR dan BPR Syariah menerapkan pengelolaan data yang meliputi akuisisi, pembuatan, penyimpanan, pemrosesan, penggunaan, retensi, dan pemusnahan data.
   e. BPR dan BPR Syariah menerapkan pengelolaan referensi dan manajemen data master. Yang dimaksud pengelolaan referensi dan manajemen data master adalah berbagi data informasi lintas domain bisnis untuk memenuhi tujuan organisasi, mengurangi risiko yang terkait dengan redundansi data, memastikan kualitas data terjaga, dan mengurangi biaya integrasi data.
   f. BPR dan BPR Syariah memiliki prosedur tertulis terkait metode manajemen data termasuk namun tidak terbatas pada pelindungan data, transfer data, dan penghapusan data.
   g. BPR dan BPR Syariah mengelola gudang data (*data warehouse*) dan sistem aplikasi *Business Intelligence*.
   h. BPR dan BPR Syariah melakukan kegiatan perencanaan, implementasi, dan pengendalian untuk memungkinkan akses data kualitas tinggi dan/atau metadata terintegrasi.
   i. BPR dan BPR Syariah melakukan pengolahan berbagai jenis data untuk memperoleh informasi yang dapat memberikan nilai tambah terutama untuk pengambilan keputusan.
5. mengelola pangkalan data secara optimal
   a. BPR dan BPR Syariah menerapkan pengelolaan teknologi pangkalan data secara memadai, mencakup:
      1) perencanaan mengenai teknologi pangkalan data;

2) pengelolaan teknologi pangkalan data; dan
3) proses evaluasi.

b. BPR dan BPR Syariah menerapkan pengelolaan operasional pangkalan data secara memadai, paling sedikit:
1) identifikasi kebutuhan terkait pangkalan data, kebutuhan sistem penyimpanan *file*, kebutuhan penambahan kapasitas penyimpanan, dan kepatuhan terhadap regulasi serta metode dan *tools* yang sesuai untuk akses data;
2) merencanakan kelangsungan usaha (*business continuity*) apabila terjadi bencana yang berdampak pada sistem penyimpanan data. BPR dan BPR Syariah memastikan rencana pemulihan diterapkan pada seluruh pangkalan data dan peladen pangkalan data, mencakup skenario yang dapat mengakibatkan hilangnya atau rusaknya data termasuk membuat cadangan pangkalan data dan pengujian pemulihan data secara berkala; dan
3) melakukan pengujian terhadap pangkalan data.

B. PELINDUNGAN DATA PRIBADI

Dalam melindungi data pribadi nasabah, BPR dan BPR Syariah melakukan kontrol:

1. Pengembangan dan/atau penyelenggaraan TI dengan mempertimbangkan aspek pelindungan data pribadi;
2. Proses identifikasi dasar pemrosesan data pribadi nasabah dan/atau calon nasabah dilakukan secara memadai;
3. Proses permintaan persetujuan nasabah dalam rangka pemrosesan data pribadi nasabah dan/atau calon nasabah dilakukan secara memadai;
4. Proses rekam dan pengelolaan persetujuan nasabah dalam rangka pemrosesan data pribadi dilakukan secara memadai;
5. Kerja sama antara BPR dan BPR Syariah dan pihak ketiga untuk aktivitas pemrosesan data pribadi didukung oleh perjanjian kerja sama yang memadai;
6. Proses identifikasi, dokumentasi, dan evaluasi tujuan proses pengumpulan dan pemrosesan data pribadi secara memadai;
7. Prosedur penanganan permintaan nasabah untuk penginian, perbaikan, penghapusan, atau pemusnahan data pribadi nasabah dilakukan secara memadai;
8. Proses retensi data pribadi dilakukan secara memadai;
9. Proses pengamanan data pribadi dilakukan secara memadai;
10. Proses penilaian dampak atas penerapan pelindungan data pribadi dilakukan secara memadai;
11. Proses dokumentasi aktivitas pemrosesan data pribadi dilakukan secara memadai;
12. Prosedur pemberian informasi pemrosesan data kepada nasabah yang memadai;
13. Prosedur pemberian akses data pribadi dan informasi kepada nasabah yang memadai;
14. Proses penanganan permintaan nasabah untuk pembatasan pemrosesan data pribadi milik nasabah dilakukan secara memadai;
15. Proses penanganan permintaan nasabah untuk mentransfer data pribadi milik nasabah ke pihak ketiga dilakukan secara memadai; dan

16. Proses penanganan penolakan nasabah atas pemrosesan data pribadi dilakukan secara memadai.

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi

LAMPIRAN VI
PERATURAN ANGGOTA DEWAN KOMISIONER
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 43/PADK.03/2025
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH
BANK PEREKONOMIAN RAKYAT DAN
BANK PEREKONOMIAN RAKYAT SYARIAH

FORMAT LAPORAN PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH

DAFTAR ISI

BAB I

LAPORAN KONDISI TERKINI PENYELENGGARAAN TEKNOLOGI INFORMASI BPR DAN BPR SYARIAH

Nama BPR/BPR Syariah :
Alamat Kantor Pusat BPR/ BPR Syariah :
Nomor Telepon :
Nama Penanggung Jawab :
Jabatan Penanggung Jawab :
Tanggal Laporan :

A. SUMBER DAYA MANUSIA TERKAIT PENYELENGGARAAN TEKNOLOGI INFORMASI

1. Struktur organisasi BPR atau BPR Syariah yang menunjukkan posisi satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi.

	Terlampir	Tidak Terlampir	

2. Deskripsi kerja (*job description*) satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi.

	Terlampir	Tidak Terlampir	

3. Pelatihan dan/atau sertifikasi di bidang Teknologi Informasi yang pernah diikuti oleh anggota satuan kerja atau pegawai yang bertanggung jawab terhadap Teknologi Informasi.

	Terlampir	Tidak Terlampir	

B. PENGEMBANGAN DAN PENGADAAN SISTEM ELEKTRONIK

1. Kebijakan dan prosedur pengembangan dan pengadaan sistem elektronik BPR atau BPR Syariah.

	Terlampir	Tidak Terlampir	

2. Daftar Sistem Elektronik*) yang sudah diimplementasikan.
   a. Dikembangkan sendiri.

	Terlampir	Tidak Terlampir	

   b. Dikembangkan pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

3. Arsitektur Aplikasi

	Terlampir	Tidak Terlampir	

4. Daftar Sistem Elektronik*) dalam proses pengembangan dan pengadaan.
   a. Dikembangkan sendiri.

	Terlampir	Tidak Terlampir	

   b. Dikembangkan pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

5. BPR atau BPR Syariah melaksanakan fungsi manajemen proyek untuk Sistem Elektronik yang sedang dalam pengembangan dan pengadaan.

	Ya	Tidak	

6. BPR atau BPR Syariah memisahkan lingkungan untuk pengembangan, uji coba, dan operasional.

	Ya	Tidak	

*) Memuat informasi nama Sistem Elektronik termasuk aplikasi, perangkat keras/lunak atau Sistem Elektronik lainnya, kegunaan Sistem Elektronik tersebut, pihak pengembang (*in house* atau nama vendor), penyelenggara (intern/ekstern), *platform/operating system*, tanggal implementasi, dokumentasi teknis pengguna (*technical user documentation*), jenis sistem Pangkalan Data, lokasi peladen utama, dan lokasi peladen cadangan yang meng-*install* Sistem Elektronik termasuk aplikasi ini.

C. AKTIVITAS OPERASIONAL TEKNOLOGI INFORMASI*)

1. Informasi mengenai Pusat Data BPR atau BPR Syariah:
   a. Alamat
   b. Status kepemilikan

	Milik Sendiri	Milik pihak penyedia jasa Teknologi Informasi	

   c. Spesifikasi peladen utama dan perangkat keras lainnya.

	Terlampir	Tidak Terlampir	

   d. Kelengkapan pengamanan fisik pada Pusat Data.

	Terlampir	TidakTerlampir	

2. Terdapat peladen yang ditempatkan di luar Pusat Data.

	Ada	Tidak Ada	

3. Aplikasi khusus untuk pengamanan informasi (*access control software*).

	Ada	Tidak Ada	

4. Prosedur penanganan masalah (*problem handling* termasuk *helpdesk).*

	Ada	Tidak Ada	

5. Kebijakan dan prosedur manajemen perubahan.

	Ada	Tidak Ada	

6. Kebijakan dan prosedur pengelolaan hak akses pengguna sistem dan aplikasi.

	Ada	Tidak Ada	

7. Penetapan sistem & *data sensitivity.*

	Ada	Tidak Ada	

8. Ketersediaan jejak audit pada sistem dan data.

	Ada	Tidak Ada	

9. Kebijakan dan prosedur rekam cadang data.

	Ada	Tidak Ada	

*) Bila terdapat lebih dari 1 Pusat Data, agar dicantumkan pula kelengkapan informasi Pusat Data lainnya dari no. 1 sampai dengan no. 9 diatas.

D. JARINGAN KOMUNIKASI

1. Struktur/topologi Jaringan Komunikasi data (utama dan rekam cadang).

	Terlampir	Tidak Terlampir	

2. Kebijakan dan prosedur pengamanan Jaringan Komunikasi.

	Ada	Tidak Ada	

3. Daftar perangkat keras dan lunak yang digunakan untuk Jaringan Komunikasi.

	Terlampir	Tidak Terlampir	

4. Sistem pemantauan Jaringan Komunikasi (*network monitoring system*).

	Ada	Tidak Ada	

5. Kebijakan dan prosedur untuk pengaturan pengamanan Jaringan Komunikasi data (misalnya *firewall*).

	Ada	Tidak Ada	

E. PENGAMANAN INFORMASI*)

1. Kebijakan dan prosedur pengamanan informasi, mencakup antara lain:
   a. Pemberian, perubahan,dan penghapusan akses pengguna.

	Ada	Tidak Ada	

   b. *Security Awareness Program*.

	Ada	Tidak Ada	

   c. Tim penanganan insiden dalam pengamanan informasi (*Incident Response Team).*

	Ada	Tidak Ada	

   d. Klasifikasi data.

	Ada	Tidak Ada	

   e. Penggunaan *emergency user id*.

	Ada	Tidak Ada	

   f. Pencegahan penggunaan perangkat lunakilegal.

	Ada	Tidak Ada	

2. Pengelolaan aset
   a. Pengelolaan aset terkait informasi meliputi identifikasi, penentuan kepemilikan dan tanggung jawab, serta inventarisasi daftar aset.

	Terlampir	Tidak Terlampir	

   b. Klasifikasi informasi (misalnya rahasia, internal, biasa) dan prosedur pengamanannya.

	Terlampir	Tidak Terlampir	

   c. Pengamanan fisik termasuk penggunaan alat pengamanan (*access control card*, PIN, dan lain-lain) terhadap fasilitas pemrosesan informasi.

	Ada	Tidak Ada	

3. Pengamanan Akses
   a. Penerapan pengamanan *password* pada aplikasi, misalnya aplikasi telah memaksa pengguna untuk mengubah *password* secara berkala.

	Ada	Tidak ada	

   b. Pengelompokan hak akses yang diberikan kepada masing-masing penggunauntuk setiap aplikasi yang dimiliki BPR atau BPR Syariah.

	Ada	Tidak ada	

   c. Terdapat fungsi audit (*audit log*/jejak audit) untuk setiap aktivitas yang dilakukan oleh pengguna dan dilakukan analisis terhadap *audit log*/jejak audit tersebut.

	Ada	Tidak ada	

d. Evaluasi secara berkala terhadap kesesuaian antara pengguna berikut hak akses yang diberikan oleh pihak yang independen.

	Ada	Tidak ada	

4. Sumber Daya Manusia

a. Pencantuman ketentuan mengenai pengamanan informasi di dalam perjanjian dengan pegawai BPR atau BPR Syariah, pegawai kontrak, dan pihak ketiga.

	Ada	Tidak ada	

b. Adanya ketentuan mengenai sanksi atas pelanggaran terhadap kebijakan dan prosedur pengamanan informasi.

	Ada	Tidak ada	

c. Prosedur pengembalian atau perubahan hak akses terhadap aset terkait informasi saat terjadi mutasi atau selesainya perjanjian kerja atau masa tugas.

	Ada	Tidak ada	

5. Operasional Teknologi Informasi

Ketentuan tentang pengamanan dalam identifikasi dan otentikasi akses misalnya penggunaan, *password, token, biometric*, dan lain-lain.

	Ada	Tidak ada	

6. Penanganan Insiden Pengamanan Informasi

a. Ketentuan mengenai keharusan untuk melaporkan terjadinya insiden pengamanan informasi.

	Ada	Tidak ada	

b. Prosedur mengenai pelaporan, penanganan, pendokumentasian, dan tindak lanjut terjadinya insiden pengamanan informasi.

	Ada	Tidak ada	

*) Bila BPR dan BPRSyariah menggunakan pihak penyedia jasa Teknologi Informasi dalam penyelenggaraan Teknologi Informasi, pertanyaan-pertanyaan di atas berlaku juga untuk penyelenggaraan Teknologi Informasi tersebut.

F. RENCANA PEMULIHAN BENCANA

1. BPR dan BPR Syariah memiliki Rencana Pemulihan Bencana.

	Ada	Tidak Ada	

2. Pusat Pemulihan Bencana.
   a. Alamat

   b. Spesifikasi rekam cadang peladendan perangkat keras lainnya.

	Terlampir	Tidak Terlampir	

   c. Kelengkapan pengamanan fisik pada Pusat Pemulihan Bencana.

	Terlampir	Tidak Terlampir	

   d. Konfigurasi Pusat Pemulihan Bencana (topologi jaringan, perangkat keras, perangkat lunak, dan pendukung lainnya)

	Terlampir	Tidak Terlampir	

   e. Rekam cadang data (*hot, warm, cold back up*) untuk masing-masing aplikasi yang tersedia di Pusat Pemulihan Bencana.

	Terlampir	Tidak Terlampir	

3. Uji Coba Rencana Pemulihan Bencana.
   a. Kebijakan dan prosedur uji coba

	Ada	Tidak Ada	

   b. Pengujian menyeluruh (*overall testing*) untuk seluruh sistem/aplikasi kritikal dilakukan terakhir kali

	Pernah Tanggal:	Belum Pernah	

   c. Pengujian parsialatas sistem/aplikasi dalam 1 (satu) tahun terakhir

Aplikasi ..... Wilayah operasional	Tgl ..... Tgl .....

4. Kaji Ulang Rencana Pemulihan Bencana.

	Pernah Tanggal:	Belum Pernah	

5. Penginian Rencana Pemulihan Bencana.

	Pernah Tanggal:	Belum Pernah	

G. LAYANAN DIGITAL

1. BPR atau BPR Syariah memiliki kebijakan dan prosedur Layanan Digital.

	Ada	Tidak ada	

2. Daftar Layanan Digital dan tanggal penerbitan Layanan Digital.

	Terlampir	Tidak Terlampir	

3. BPR atau BPR Syariah melakukan kajian pasca implementasi Layanan Digital oleh pihak independen (produk baru) atau pihak intern (penambahan fitur produk).

	Pernah Tanggal:	Belum Pernah	

Jika pernah, lampirkan hasil kajian pasca implementasi.

	Terlampir	Tidak Terlampir	

H. AUDIT INTERN PENYELENGGARAAN TEKNOLOGI INFORMASI*)

1. BPR atau BPR Syariah memiliki organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi.

	Ya	Tidak	

Jika ya, lampirkan struktur organ pelaksana fungsi audit intern terhadap penyelenggaraan Teknologi Informasi dan lengkapi dengan riwayat hidup (*curriculum vitae)* auditor intern.

	Terlampir	Tidak Terlampir	

2. BPR atau BPR Syariah menggunakan auditor ekstern untuk melakukan fungsi audit intern terhadap penyelenggaraan Teknologi Informasi.

	Ya	Tidak	

Jika ya, lampirkan perjanjian kerja terkini.

	Terlampir	Tidak Terlampir	

3. BPR atau BPR Syariah memiliki pedoman audit intern terhadap penyelenggaraan Teknologi Informasi.

	Ada	Tidak Ada	

4. Audit intern terhadap penyelenggaraan Teknologi Informasi dilaksanakan paling sedikit 1 (satu) kali setahun.

	Ya	Tidak	

Sebutkan dua tanggal audit intern terhadap penyelenggaraan Teknologi Informasi terakhir.

Tanggal.....
Tanggal.....

Audit intern terhadap penyelenggaraan Teknologi Informasi tersebut di atas telah mencakup Aplikasi Inti Perbankan serta wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan Teknologi Informasi.

	Ya	Tidak	

5. Laporan audit intern terhadap penyelenggaraan Teknologi Informasi kepada Direktur Utama, Dewan Komisaris, Komite Audit

apabila ada, dan ditembuskan kepada anggota Direksi yang membawahkan fungsi kepatuhan.

	Ya	Tidak	

6. *Auditee* memberikan tanggapan/komitmen dan target waktu penyelesaian atas hasil audit intern, apabila ada.

	Ya	Tidak	

Jika ada, lampirkan tanggapan/komitmen dan target waktu penyelesaian atas hasil audit intern.

	Terlampir	Tidak Terlampir	

7. Organ pelaksana fungsi audit intern memantau pelaksanaan komitmen *auditee* atas hasil audit secara berkala dan melakukan verifikasi terhadap perbaikan yang telah dilakukan, apabila ada.

	Ya	Tidak	

Jika ada, lampirkan hasil pemantauan atas pelaksanaan komitmen *auditee*.

	Terlampir	Tidak Terlampir	

*) Informasi mencakup jenis layanan, data penyedia jasa (nama perusahaan, alamat *data center*, alamat perusahaan, pemilik/grup pemilik mayoritas), tanggal dan jangka waktu perjanjian, *contact person* di BPR atau BPR Syariah yang menangani jasa penyelenggaraan TI tersebut dan informasi penting lainnya.

I. KERJA SAMA DENGAN PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI

1. Tanggal mulai implementasi kerja sama Teknologi Informasi BPR atau BPR Syariah:
2. Uraikan nama dan alamat pihak penyedia jasa Teknologi Informasi.
   Nama :
   Alamat :
   Lokasi Pusat Data :
   Lokasi Pusat Pemulihan Bencana :

3. Daftar jasa Teknologi Informasi yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

4. Jaringan Komunikasi data yang digunakan oleh pihak penyedia jasa Teknologi Informasi BPR atau BPR atau BPR Syariah.

	Terlampir	Tidak Terlampir	

5. Salinan perjanjian kerja sama antara BPR atau BPR Syariah dengan pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

6. Hasil evaluasi terkini mengenai analisis biaya dan manfaat penyelenggaraan Teknologi Informasi oleh pihak penyedia jasa Teknologi Informasi.

	Ada	Tidak ada	

7. Analisis BPR atau BPR Syariah mengenai kecukupan Rencana Pemulihan Bencana milik pihak penyedia jasa Teknologi Informasi.

	Ada	Tidak ada	

J. PERUBAHAN MENDASAR

Huruf ini hanya diisi apabila BPR atau BPR Syariah menyampaikan laporan kondisi terkini apabila terjadi perubahan mendasar dalam penyelenggaraan Teknologi Informasi. Dalam hal terjadi perubahan mendasar, BPR atau BPR Syariah harus menyampaikan laporan kondisi terkini sebagaimana huruf A sampai dengan huruf I untuk menyampaikan keterangan dan alasan dari perubahan mendasar.

1. Tanggal efektif beroperasi sejak perubahan mendasar dalam penyelenggaraan Teknologi Informasi*):
2. Jenis perubahan mendasar dalam penyelenggaraan Teknologi Informasi:

Perubahan Mendasar**)	Keterangan dan Alasan***)
1.	
2.	
3.	
dst	

*) Perubahan dalam penyelenggaraan TI dilaporkan 10 (sepuluh) hari kerja sejak perubahan mendasar dalam penyelenggaraan TI sebagaimana dipersyaratkan pada POJK PTI BPR dan BPR Syariah dan Peraturan Anggota Dewan Komisioner ini.

**) Yang dimaksud dengan perubahan mendasar antara lain perubahan terhadap konfigurasi Teknologi Informasi atau Aplikasi Inti Perbankan, pengadaan Aplikasi Inti Perbankan, kerja sama dengan pihak penyedia jasa TI, serta pengembangan dan pengadaan TI mendasar lainnya yang dapat menambah dan/atau meningkatkan risiko BPR atau BPR Syariah.

***) Keterangan harus disertai dengan informasi lebih lanjut, antara lain berupa alasan dilakukannya perubahan mendasar dan teknis perubahan mendasar yang dilakukan oleh BPR atau BPR Syariah. Disertai dengan lampiran dokumen.

BAB II

NOTIFIKASI AWAL INSIDEN TEKNOLOGI INFORMASI (KEJADIAN KRITIS, PENYALAHGUNAAN, DAN/ATAU KEJAHATAN DALAM PENYELENGGARAAN TEKNOLOGI INFORMASI)*)

A. INFORMASI BPR DAN BPR SYARIAH

Nama BPR/BPR Syariah :
Alamat Kantor Pusat BPR/BPR Syariah :
Nomor Telepon :
Nama Penanggung Jawab :
Jabatan Penanggung Jawab :
Nomor Telepon Penanggung Jawab :
Tanggal Penyampaian Notifikasi :
Otoritas/Lembaga Penerima[1)] :

B. INFORMASI UMUM INSIDEN TI

1. Tanggal Terjadinya Insiden
   .....
2. Waktu Terjadinya Insiden
   .....
3. Jenis Insiden[2)]
   .....
4. Titik Serangan[3)]
   .....
5. Ringkasan Kronologis Penyebab Kejadian[4)]
   a. .....
   b. .....
   c. .....
6. Dampak/Akibat yang Ditimbulkan[5)]
   a. .....
   b. .....
   c. .....
7. Respons Awal BPR dan BPR Syariah Pasca Insiden[6)]
   a. .....
   b. .....
   c. .....
8. RencanaTindak Lanjut BPR dan BPR Syariah
   a. .....
   b. .....
   c. .....

Demikian notifikasi awal terkait insiden TI BPR/BPR Syariah ..... Selanjutnya, kami akan menyampaikan laporan insiden TI paling lama 7 (tujuh) hari kerja setelah insiden TI diketahui, yaitu tanggal ..... melalui APOLO Modul Laporan Insidental.

1) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang juga menerima pelaporan notifikasi awal ini (jika ada).
2) Memuat informasi mengenai jenis insiden TI, termasuk insiden siber. Contoh: *Malware*, *Hacking*, *Ransomware*, *Web Defacement*, *Denial of Services* (DoS)/*Distributed Denial of Services* (DDoS).
3) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
4) Memuat informasi mengenai kronologis kejadian insiden TI, termasuk insiden siber.
5) Memuat dampak insiden yang telah diidentifikasi (insiden siber dapat berdampak kepada antara lain produk, pihak ketiga, keuangan, dan reputasi BPR dan BPR Syariah).
6) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh BPR dan BPR Syariah setelah diketahui terjadinya insiden.

BAB III

LAPORAN INSIDEN TEKNOLOGI INFORMASI (KEJADIAN KRITIS, PENYALAHGUNAAN, DAN/ATAU KEJAHATAN DALAM PENYELENGGARAAN TEKNOLOGI INFORMASI)*)

A. INFORMASI BPR DAN BPR SYARIAH

Nama BPR/BPR Syariah :
Alamat Kantor Pusat BPR/BPR Syariah :
Nomor Telepon :
Nama Penanggung Jawab :
Jabatan Penanggung Jawab :
Nomor Telepon Penanggung Jawab :
Tanggal Penyampaian Notifikasi Awal :
Tanggal Laporan :

B. INFORMASI UMUM INSIDEN TI

1. Tanggal Terjadinya Insiden
   .....
2. Waktu Terjadinya Insiden
   .....
3. Jenis Insiden[2)]
   .....
4. Titik Serangan[3)]
   .....
5. Satuan Kerja Terkait atau Pegawai yang Dapat Dihubungi Lebih Lanjut.....
   .....
6. Respon Awal BPR dan BPR Syariah Pasca Insiden[4)]
   .....

C. PENILAIAN ATAS DAMPAK INSIDEN TI[5)]

1. Penilaian Dampak Insiden terhadap Bisnis BPR dan BPR Syariah[6)]
   .....
2. Penilaian Dampak Insiden terhadap Pihak Ketiga[7)]
   .....
3. Penilaian Dampak Finansial dari Insiden[8)]
   .....
4. Penilaian Dampak terhadap Reputasi BPR dan BPR Syariah[9)]
   .....
5. Penilaian Dampak terhadap Aspek Hukum dan Kepatuhan[10)]
   .....
6. Penilaian Dampak Lainnya yang Dapat Diidentifikasi oleh BPR dan BPR Syariah
   .....

D. INFORMASI KRONOLOGIS INSIDEN

1. Durasi terjadinya insiden.
2. Langkah eskalasi insiden yang dilakukan.
3. Langkah penanggulangan insiden yang dilakukan.
4. Langkah pemulihan insiden yang dilakukan.

5. Keterlibatan pihak ketiga dalam penanggulangan dan pemulihan insiden.
6. Pihak-pihak yang menerima informasi terkait insiden (*stakeholder* terkait, contoh: otoritas, mitra layanan, dan nasabah).
7. Informasi pendukung yang digunakan untuk mengidentifikasi serangan, apabila diketahui.
   (contoh: alamat IP yang mencurigakan, lalu lintas jaringan yang tidak biasa, tingkat kegagalan autentikasi yang tinggi, permintaan *file* secara berulang kali, dan sebagainya).

E. ANALISIS PENYEBAB TERJADINYA INSIDEN

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

F. ANALISIS FINAL

1. Kesimpulan
2. Langkah Perbaikan[15)]
3. Target Waktu Penyelesaian Insiden[16)]

Keterangan:

1) Berisi informasi yang sesuai dengan informasi yang telah disampaikan pada notifikasi awal, namun dapat ditambahkan atau disesuaikan dengan informasi tambahan bila ada.
2) Memuat informasi mengenai jenis insiden, termasuk insiden siber. Contoh: *Malware*, *Hacking*, *Ransomware*, *Web Defacement*, *Denial of Services* (DoS)/*Distributed Denial of Services* (DDoS).
3) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
4) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh BPR dan BPR Syariah setelah diketahui terjadinya insiden.
5) Pada bagian ini, informasi yang diberikan berupa penjelasan tambahan dari penilaian awal yang sudah dilakukan oleh BPR dan BPR Syariah saat pelaporan notifikasi awal insiden.
6) Diisi dalam hal terdapat dampak terhadap bisnis BPR dan BPR Syariah, termasuk dalam kaitannya dengan ketersediaan dan operasional layanan BPR dan BPR Syariah. Informasi paling sedikit memuat:
   a. Jenis layanan dan/atau nama produk yang terdampak (Contoh: layanan perbankan digital); dan
   b. Penjelasan mengenai dampak yang terjadi (jika layanan dan/atau produk yang terdampak lebih dari 1 (satu), maka penjelasan diberikan untuk seluruh layanan dan produk yang terdampak).
7) Diisi dalam hal terdapat dampak terhadap pihak ketiga dari BPR dan BPR Syariah. Informasi paling sedikit memuat:
   a. Kategori pihak ketiga (contoh: nasabah, pihak penyedia jasa, dan mitra kerja sama layanan); dan
   b. Penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) kategori mitra maka penjelasan diberikan untuk seluruh mitra terdampak).
8) Diisi dalam hal terdapat dampak finansial dari insiden. Informasi paling sedikit memuat:

a. Hal yang terdampak (contoh: nilai atau volume transaksi, penarikan dana, dan likuiditas BPR dan BPR Syariah); dan
b. Penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) hal, maka penjelasan diberikan untuk seluruh mitra terdampak).

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

BAB IV

LAPORAN REALISASI PENGGUNAAN PIHAK PENYEDIA JASA TEKNOLOGI INFORMASI

Nama BPR/BPRSyariah	:
Alamat Kantor Pusat BPR/BPRSyariah	:
Nomor Telepon	:
Nama Penanggung Jawab	:
Jabatan Penanggung Jawab	:
Tanggal Laporan	:

1. Tanggal mulai implementasi kerja sama Teknologi Informasi BPR atau BPR Syariah:

2. Uraikan nama dan alamat pihak penyedia jasa Teknologi Informasi.

Nama	:
Alamat	:
Lokasi Pusat Data	:
Lokasi Pusat Pemulihan Bencana	:

3. Daftar jasa Teknologi Informasi yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

4. Nilai nominal perjanjian kerja sama dengan pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

5. Jangka waktu perjanjian kerja sama dengan pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

6. Fotokopi perjanjian kerja sama dengan pihak penyedia jasa Teknologi Informasi.

	Terlampir	Tidak Terlampir	

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd.

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd.

Aat Windradi