

**DAFTAR TANYA JAWAB LAZIM / FREQUENTLY ASKED QUESTIONS (FAQ)
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**

I. PENGATURAN UMUM

1. Apa latar belakang penerbitan PADK ini?

PADK ini diterbitkan sebagai ketentuan pelaksanaan dari Peraturan Otoritas Jasa Keuangan Nomor 34 Tahun 2025 tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah (POJK PTI BPR dan BPR Syariah), antara lain mengatur penjelasan lebih lanjut mengenai penerapan tata kelola serta kebijakan dan prosedur penyelenggaraan teknologi informasi, manajemen risiko penyelenggaraan teknologi informasi, pedoman ketahanan dan keamanan siber, pengelolaan data dan perlindungan data pribadi, serta format laporan penyelenggaraan teknologi informasi.

2. Kapan BPR dan BPR Syariah mulai menerapkan penyelenggaraan teknologi informasi ketentuan sesuai PADK ini?

BPR dan BPR Syariah mulai menerapkan penyelenggaraan teknologi informasi sesuai PADK ini setelah 1 (satu) tahun terhitung sejak tanggal ditetapkan.

II. PENERAPAN TATA KELOLA SERTA KEBIJAKAN DAN PROSEDUR PENYELENGGARAAN TI OLEH BPR DAN BPR SYARIAH

1. Apa saja cakupan dari penerapan tata kelola serta kebijakan dan prosedur penyelenggaraan TI oleh BPR dan BPR Syariah?

Cakupan penerapan tata kelola serta kebijakan dan prosedur penyelenggaraan TI oleh BPR dan BPR Syariah adalah:

- a. Penerapan tata kelola TI;
- b. Pengembangan dan pengadaan sistem elektronik;
- c. Operasional TI;
- d. Jaringan komunikasi;
- e. Pengamanan informasi;
- f. Rencana pemulihan bencana;
- g. Audit intern TI; dan
- h. Kerja sama dengan pihak penyedia jasa TI (PPJTI).

2. Apa saja hal-hal yang perlu dipertimbangkan BPR dan BPR Syariah dalam menerapkan tata kelola TI yang baik?

BPR dan BPR Syariah perlu 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 PPJT, 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, perlindungan data pribadi, kerahasiaan data nasabah, dan dokumen perusahaan

III. MANAJEMEN RISIKO PENYELENGGARAAN TI OLEH BPR DAN BPR SYARIAH

1. Apa saja yang perlu dilaksanakan dalam penerapan manajemen risiko layanan digital?

BPR dan BPR Syariah perlu menerapkan manajemen risiko layanan digital dengan melaksanakan proses:

- a. Identifikasi risiko
BPR dan BPR Syariah melakukan identifikasi risiko terkait layanan digital yang diselenggarakan, meliputi aspek teknologi, operasional, keamanan, hingga kepatuhan.
- b. Pengukuran risiko
Pengukuran dilakukan terhadap potensi kerugian yang terjadi (*loss event*) pada setiap jenis layanan digital sehingga perlu membuat Pangkalan Data (*database*) yang berisi data historis kerugian (*loss event database*) setiap jenis layanan perbankan elektronik.
- c. Pengendalian risiko layanan digital
Dalam rangka pengendalian risiko, BPR dan BPR Syariah harus melakukan mitigasi atas risiko yang mungkin terjadi dalam layanan digital dengan memperhatikan prinsip pengendalian pengamanan data nasabah dan transaksi layanan digital.

- d. Pengendalian risiko layanan digital tertentu
 - 1) Dalam menyediakan layanan digital misalnya pada *mobile banking* dan *internet banking*, BPR dan BPR Syariah perlu memperhatikan kenyamanan dan kemudahan nasabah dalam menggunakan fasilitas, serta menetapkan persyaratan atau melakukan pembatasan transaksi dalam rangka peningkatan pengamanan transaksi.
 - 2) 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, kerusakan, dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang.
 - 3) BPR dan BPR Syariah harus memastikan terdapatnya pengamanan atas aspek transmisi data, serta memastikan transfer dana secara elektronik dari rekening nasabah kepada rekening *acquirer* atau *merchant* untuk pembayaran suatu transaksi.
- e. Pengendalian risiko layanan digital yang diselenggarakan 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.

2. Apa saja yang perlu dilaksanakan dalam penerapan manajemen risiko kerja sama dengan PPJTI?

Manajemen risiko terkait kerja sama dengan PPJTI harus melaksanakan proses:

- a. Identifikasi risiko
Penggunaan PPJTI dalam menyelenggarakan TI dapat memberikan kontribusi terhadap beberapa jenis risiko, seperti risiko operasional, risiko reputasi, risiko stratejik, dan risiko kepatuhan.
- b. Pengukuran risiko
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.
- c. 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.
- d. Pengendalian risiko

BPR dan BPR Syariah harus memastikan pengendalian pengamanan untuk memitigasi risiko dan mencakup, antara lain penelitian latar belakang pegawai PPJTI, memastikan PPJTI melakukan pengendalian keamanan terhadap seluruh fasilitas TI yang digunakan dan data yang diproses serta informasi yang dihasilkan telah dicantumkan dalam perjanjian, memastikan PPJTI memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan BPR dan BPR Syariah, dan memastikan biaya yang dikeluarkan untuk masing-masing pengamanan sebanding dengan tingkat pengamanan yang dibutuhkan dan sesuai dengan tingkat toleransi risiko.

IV. PEDOMAN KETAHANAN DAN KEAMANAN SIBER BPR DAN BPR SYARIAH

1. Apa saja hal-hal yang diatur dalam PADK ini terkait ketahanan dan keamanan siber?

Sesuai PADK ini diatur antara lain mengenai pedoman penilaian tingkat maturitas keamanan siber, meliputi tata cara pengisian kertas kerja penilaian tingkat maturitas keamanan siber, kertas kerja penilaian tingkat maturitas keamanan siber dan kriteria penilaian parameter berdasarkan peringkat.

2. Apakah BPR dan BPR Syariah diharuskan menyampaikan hasil penilaian tingkat maturitas keamanan siber?

BPR dan BPR Syariah tidak diwajibkan menyampaikan hasil penilaian tingkat maturitas keamanan siber kepada Otoritas Jasa Keuangan, namun Otoritas Jasa Keuangan dapat sewaktu-waktu meminta hasil penilaian tingkat maturitas keamanan siber dimaksud.

Hasil penilaian tingkat maturitas keamanan siber dapat menjadi pertimbangan dalam penilaian manajemen risiko operasional BPR dan BPR Syariah.

3. Bagaimana periode penilaian tingkat maturitas keamanan siber dan kapan pertama kali dilakukan?

BPR dan BPR Syariah melakukan penilaian tingkat maturitas keamanan siber secara tahunan untuk posisi akhir bulan Desember. BPR dan BPR Syariah pertama kali melakukan penilaian tingkat maturitas keamanan siber untuk posisi Desember 2026.

V. PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI BPR DAN BPR SYARIAH

1. Apa saja yang harus diperhatikan dalam pengelolaan data?

BPR dan BPR Syariah dalam mengelola data harus memperhatikan:

- a. kualitas data;
- b. sistem pengelolaan data; dan
- c. sumber daya pendukung pengelolaan data.

2. Apa saja prinsip perlindungan data pribadi dalam melakukan pemrosesan data pribadi?

BPR dan BPR Syariah melaksanakan prinsip perlindungan 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.

VI. FORMAT LAPORAN PENYELENGGARAAN TI OLEH BPR DAN BPR SYARIAH

1. Apa saja format laporan yang tercakup dalam PADK ini?

Terdapat 4 (empat) format laporan yang tercakup dalam PADK ini, yaitu:

- a. Laporan kondisi terkini penyelenggaraan TI BPR dan BPR Syariah;
- b. Notifikasi awal insiden TI;
- c. Laporan insiden TI; dan
- d. Laporan realisasi penggunaan PPJTI.

2. Apakah notifikasi awal insiden TI dan laporan insiden TI termasuk untuk insiden siber?

Iya, format laporan notifikasi awal insiden TI dan laporan insiden TI termasuk untuk insiden siber. Notifikasi awal insiden TI disampaikan melalui sarana elektronik secara tertulis kepada Otoritas Jasa Keuangan berdasarkan informasi awal yang tersedia.

3. Apa saja laporan berkala yang harus disampaikan oleh BPR dan BPR Syariah?

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. Laporan disampaikan secara daring melalui Aplikasi Pelaporan *Online* Otoritas Jasa Keuangan (APOLO) kanal laporan penilaian tingkat kesehatan BPR dan BPR Syariah.

4. Apa saja laporan insidental yang harus disampaikan oleh BPR dan BPR Syariah?

BPR dan BPR Syariah menyampaikan laporan:

- a. tindakan dalam hal terdapat kondisi tertentu, sebagaimana dimaksud dalam Pasal 28 ayat (1) huruf a POJK PTI BPR dan BPR Syariah;
- b. penghentian penggunaan PPJTI, sebagaimana dimaksud dalam Pasal 28 ayat (1) huruf c POJK PTI BPR dan BPR Syariah;
- c. rencana tindak untuk melakukan upaya perbaikan sebagaimana dimaksud dalam Pasal 28 ayat (4) POJK PTI BPR dan BPR Syariah;
- d. kondisi terkini penyelenggaraan TI dalam hal terjadi perubahan mendasar dalam penyelenggaraan TI sebagaimana dimaksud dalam Pasal 44 POJK PTI BPR dan BPR Syariah;
- e. realisasi penggunaan PPJTI sebagaimana dimaksud dalam Pasal 45 POJK PTI BPR dan BPR Syariah; dan/atau
- f. 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.