

Yth.

Direksi Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi,  
di tempat.

SALINAN  
SURAT EDARAN OTORITAS JASA KEUANGAN  
REPUBLIK INDONESIA  
NOMOR 6 /SEOJK.05/2021  
TENTANG  
PEDOMAN PENERAPAN PROGRAM ANTI PENCUCIAN UANG DAN PENCEGAHAN  
PENDANAAN TERORISME BAGI PENYELENGGARA LAYANAN PINJAM MEMINJAM  
UANG BERBASIS TEKNOLOGI INFORMASI

Sehubungan dengan amanat ketentuan Pasal 68 Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 57, Tambahan Lembaran Negara Republik Indonesia Nomor 6035) sebagaimana telah diubah dengan Peraturan Otoritas Jasa Keuangan Nomor 23/POJK.01/2019 tentang Perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 178, Tambahan Lembaran Negara Republik Indonesia Nomor 6394), perlu untuk mengatur lebih lanjut mengenai penerapan program anti pencucian uang dan pencegahan pendanaan terorisme bagi Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

1. Dalam Surat Edaran Otoritas Jasa Keuangan ini yang dimaksud dengan:
  - a. Penyedia Jasa Keuangan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi adalah penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi sebagaimana dimaksud dalam Peraturan Otoritas Jasa

Keuangan mengenai layanan pinjam meminjam uang berbasis teknologi informasi.

- b. Penyelenggara Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang selanjutnya disebut Penyelenggara adalah badan hukum Indonesia yang menyediakan, mengelola, dan mengoperasikan layanan pinjam meminjam uang berbasis teknologi informasi.
- c. Penerima Pinjaman adalah orang dan/atau badan hukum yang mempunyai utang karena perjanjian layanan pinjam meminjam uang berbasis teknologi informasi.
- d. Pemberi Pinjaman adalah orang, badan hukum, dan/atau badan usaha yang mempunyai piutang karena perjanjian layanan pinjam meminjam uang berbasis teknologi informasi.
- e. Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi yang selanjutnya disebut Pengguna adalah Pemberi Pinjaman dan Penerima Pinjaman yang menggunakan layanan pinjam meminjam uang berbasis teknologi informasi.
- f. Nasabah adalah Pengguna sebagaimana dimaksud pada huruf e.
- g. Calon Nasabah adalah calon Pengguna yang akan menggunakan jasa Penyelenggara.
- h. Direksi:
  - 1) bagi Penyelenggara berbentuk badan hukum perseroan terbatas adalah Direksi sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai perseroan terbatas;
  - 2) bagi Penyelenggara yang berbentuk badan hukum koperasi adalah pengurus sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai perkoperasian.
- i. Dewan Komisaris:
  - 1) bagi Penyelenggara berbentuk badan hukum perseroan terbatas adalah dewan komisaris sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai perseroan terbatas;

- 2) bagi Penyelenggara yang berbentuk badan hukum koperasi adalah pengawas sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai perkoperasian.
- j. Pencucian Uang adalah pencucian uang sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang.
- k. Pendanaan Terorisme adalah pendanaan terorisme sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme.
- l. Proliferasi Senjata Pemusnah Massal adalah penyebaran senjata nuklir, biologi, dan kimia.
- m. Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme yang selanjutnya disingkat APU dan PPT adalah upaya pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Pendanaan Terorisme.
- n. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi di bidang layanan jasa keuangan.
- o. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik di bidang layanan jasa keuangan.
- p. Uji Tuntas Nasabah (*Customer Due Diligence*) yang selanjutnya disingkat CDD adalah kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh penyedia jasa keuangan untuk memastikan transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi Calon Nasabah, Nasabah, atau *walk-in customer*.
- q. Uji Tuntas Lanjut (*Enhanced Due Diligence*) yang selanjutnya disingkat EDD adalah tindakan CDD lebih mendalam yang dilakukan PJK terhadap Calon Nasabah, *walk-in customer*, atau Nasabah, yang berisiko tinggi termasuk orang yang populer secara politis (*politically exposed person*) dan/atau dalam area berisiko tinggi.

- r. Nasabah Berisiko Tinggi (*High Risk Customers*) adalah Nasabah yang berdasarkan latar belakang, identitas dan riwayatnya dianggap memiliki risiko tinggi melakukan kegiatan terkait tindak pidana Pencucian Uang dan/atau Pendanaan Terorisme.
- s. Transaksi Keuangan Mencurigakan selanjutnya disingkat TKM adalah transaksi keuangan mencurigakan sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme.
- t. Pemilik Manfaat (*Beneficial Owner*) adalah setiap orang yang:
  - 1) berhak atas dan/atau menerima manfaat tertentu yang berkaitan dengan rekening Nasabah;
  - 2) merupakan pemilik sebenarnya dari dana dan/atau efek yang ditempatkan pada penyedia jasa keuangan (*ultimately own account*);
  - 3) mengendalikan transaksi Nasabah;
  - 4) memberikan kuasa untuk melakukan transaksi;
  - 5) mengendalikan korporasi atau perikatan lainnya (*legal arrangement*); dan/atau
  - 6) merupakan pengendali akhir dari transaksi yang dilakukan melalui badan hukum atau berdasarkan suatu perjanjian.
- u. Orang yang Populer Secara Politis (*Politically Exposed Person*) yang selanjutnya disingkat PEP meliputi:
  - 1) PEP Asing adalah orang yang diberi kewenangan untuk melakukan fungsi penting (*prominent function*) oleh negara lain (asing), seperti kepala negara atau pemerintahan, politisi senior, pejabat pemerintah senior, pejabat militer atau pejabat di bidang penegakan hukum, eksekutif senior pada perusahaan yang dimiliki oleh negara, pejabat penting dalam partai politik;
  - 2) PEP Domestik adalah orang yang diberi kewenangan untuk melakukan fungsi penting (*prominent function*) oleh negara, seperti kepala negara atau pemerintahan, politisi senior, pejabat pemerintah senior, pejabat militer atau pejabat di bidang penegakan hukum, eksekutif senior pada perusahaan yang dimiliki oleh negara, pejabat penting

dalam partai politik; dan

- 3) Orang yang diberi kewenangan untuk melakukan fungsi penting (*prominent function*) oleh organisasi internasional, seperti senior manajer yang meliputi namun tidak terbatas pada direktur, deputy direktur, dan anggota dewan atau fungsi yang setara.
  - v. Tindak Pidana Pencucian Uang yang selanjutnya disingkat TPPU adalah tindak pidana pencucian uang sebagaimana dimaksud dalam Undang-Undang mengenai pencegahan dan pemberantasan tindak pidana pencucian uang.
  - w. Tindak Pidana Pendanaan Terorisme yang selanjutnya disingkat TPPT adalah tindak pidana pendanaan terorisme sebagaimana dimaksud dalam Undang-Undang mengenai pencegahan dan pemberantasan tindak pidana pendanaan terorisme.
  - x. Pusat Pelaporan dan Analisis Transaksi Keuangan yang selanjutnya disingkat PPATK adalah PPATK sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan TPPU.
2. Penyelenggara sangat rentan terhadap kemungkinan digunakan sebagai sarana Pencucian Uang, Pendanaan Terorisme, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal. Penyelenggara dimungkinkan menjadi pintu masuk harta kekayaan yang merupakan hasil TPPU atau TPPT ke dalam sistem keuangan yang selanjutnya dapat dimanfaatkan untuk kepentingan pelaku kejahatan. Misalnya untuk pelaku Pencucian Uang, harta kekayaan tersebut dapat ditarik kembali sebagai harta kekayaan yang seolah-olah sah dan tidak lagi dapat dilacak asal usulnya. Sedangkan untuk pelaku Pendanaan Terorisme atau pendanaan Proliferasi Senjata Pemusnah Massal, harta kekayaan tersebut dapat digunakan untuk membiayai kegiatan terorisme atau mendanai pengembangan senjata pemusnah massal.
  3. Semakin berkembangnya kompleksitas produk dan layanan jasa keuangan termasuk pemasarannya (*multi-channel marketing*), serta semakin meningkatnya penggunaan Teknologi Informasi pada industri jasa keuangan, mengakibatkan semakin tinggi risiko Penyelenggara digunakan sebagai sarana Pencucian Uang, Pendanaan Terorisme, dan/atau pendanaan Proliferasi Senjata

Pemusnah Massal.

4. Dalam kaitan tersebut perlu adanya peningkatan kualitas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal yang didasarkan pada pendekatan berbasis risiko (*risk based approach*) sesuai dengan prinsip umum yang berlaku secara internasional dan sejalan dengan penilaian risiko nasional (*national risk assessment* (NRA)) serta penilaian risiko sektoral (*sectoral risk assessment* (SRA)).
5. Gambaran Umum Pencucian Uang
  - a. Pada dasarnya proses Pencucian Uang dapat dikelompokkan ke dalam 3 (tiga) tahap kegiatan yang meliputi:
    - 1) penempatan (*placement*), adalah upaya menempatkan uang tunai yang berasal dari tindak pidana ke dalam sistem keuangan (*financial system*), atau upaya menempatkan uang giral (*cheque*, wesel bank, sertifikat deposito, dan lain-lain) kembali ke dalam sistem keuangan;
    - 2) pemisahan/pelapisan (*layering*), adalah upaya untuk mengaburkan asal usul harta kekayaan yang berasal dari tindak pidana (*dirty money*) yang telah berhasil ditempatkan pada pelaku jasa keuangan. Dalam kegiatan ini terdapat proses pemindahan harta kekayaan yang berasal dari tindak pidana dari beberapa rekening atau lokasi tertentu sebagai hasil *placement* ke tempat lain melalui serangkaian transaksi yang kompleks dan didesain untuk menyamarkan dan menghilangkan jejak sumber harta kekayaan tersebut; dan/atau
    - 3) penggabungan (*integration*) adalah upaya menggabungkan atau menggunakan harta kekayaan yang telah tampak sah, baik untuk dinikmati langsung, diinvestasikan ke dalam berbagai jenis produk keuangan dan bentuk material lainnya, dipergunakan untuk membiayai kegiatan bisnis yang sah, ataupun untuk membiayai kembali kegiatan tindak pidana.
  - b. Beberapa metode, teknis, skema, dan instrumen dalam Pencucian Uang, antara lain:
    - 1) pemanfaatan korporasi atau penggunaan perusahaan boneka, di mana dana hasil tindak pidana disalurkan ke

entitas/korporasi legal yang pada dasarnya merupakan perusahaan boneka untuk memfasilitasi aktivitasnya. Perusahaan boneka tersebut didirikan hanya untuk melakukan transaksi fiktif dan bertujuan untuk mengaburkan identitas orang-orang yang mengendalikan dana hasil kejahatan yang melakukan Pencucian Uang.

Contoh: dana hasil kejahatan dilegalkan menjadi dana milik Pemberi Pinjaman melalui Penyelenggara;

- 2) *structuring*, yaitu upaya untuk menghindari pelaporan dengan memecah transaksi pinjaman dana hasil kejahatan dengan menggunakan transaksi dalam jumlah relatif kecil namun dengan frekuensi yang tinggi di sektor keuangan.

Sebagai contoh: Pemberi Pinjaman memecah transaksi dana hasil kejahatan dalam beberapa kali transaksi dengan nilai transaksi yang relatif kecil ke Penerima Pinjaman;

- 3) *smurfing*, yaitu metode di mana transaksi dana hasil kejahatan dilakukan dengan menggunakan beberapa rekening atas nama individu yang berbeda-beda untuk kepentingan satu orang tertentu;

Sebagai contoh: Pemberi Pinjaman melakukan penyetoran dana pinjaman pada lebih dari 1 (satu) Penerima Pinjaman untuk menghindari nilai dana pinjaman yang mencurigakan pada 1 (satu) Penerima Pinjaman;

- 4) *mingling* (penyatuan uang haram dalam bisnis legal), yaitu teknik dengan mencampurkan atau menggabungkan hasil tindak kejahatan dengan hasil usaha bisnis yang sah dengan tujuan untuk mengaburkan sumber dana hasil kejahatan.

Sebagai contoh: dana hasil kejahatan digabungkan dengan dana Pemberi Pinjaman dan disampaikan ke Penerima Pinjaman untuk kegiatan usaha yang sah;

- 5) penggunaan jasa profesional, yaitu teknik dengan menggunakan jasa profesional seperti advokat, notaris, perencana keuangan, dan akuntan termasuk akuntan publik. Hal tersebut dilakukan dengan tujuan untuk mengaburkan identitas penerima manfaat dan sumber dana hasil kejahatan untuk menutupi kegiatan Pencucian Uang.

Contoh: Pemberi Pinjaman dan/atau Penerima Pinjaman melakukan kerja sama dengan advokat, notaris, perencana keuangan atau akuntan (termasuk akuntan publik) untuk bersama-sama melakukan rekayasa atau manipulasi untuk menyamarkan dana hasil kejahatan dalam *legal audit* dan *legal opinion*, anggaran dasar dan anggaran rumah tangga korporasi, proposal perencanaan keuangan, dan/atau laporan keuangan dari Pemberi Pinjaman maupun Penerima Pinjaman;

- 6) penggunaan nama orang lain (*nominee*), anggota keluarga atau pihak ketiga, yaitu teknik yang digunakan untuk mengaburkan identitas orang-orang yang mengendalikan dana hasil kejahatan, baik di Pemberi Pinjaman maupun Penerima Pinjaman;
- 7) pembelian aset berharga seperti perhiasan, logam mulia, dan/atau barang seni. Dalam kaitan ini, Penerima Pinjaman mengajukan pinjaman pada Penyelenggara untuk membeli perhiasan atau logam mulia, di mana saat melunasi pinjaman Penerima Pinjaman menggunakan dana hasil kejahatan;
- 8) penggunaan sektor nonkeuangan untuk melegalkan dana hasil kejahatan, di mana dana yang diperoleh Penerima Pinjaman digunakan untuk kegiatan sektor non keuangan seperti pertanian dan peternakan;
- 9) penggunaan perusahaan di negara-negara *tax haven* yang tidak memiliki bisnis nyata (*paper company*) seperti diklasifikasikan oleh organisasi internasional yang kompeten, termasuk negara-negara yang dikategorikan sebagai *High-risk and other Monitored Jurisdictions* oleh *Financial Action Task Force on Money Laundering* (FATF), di mana dana hasil kejahatan ditransfer ke perusahaan tersebut, dan perusahaan tersebut menjadi sumber dana Pemberi Pinjaman melalui Penyelenggara;
- 10) penggunaan dana hasil pinjaman yang tidak didasarkan pada kegiatan usaha Penerima Pinjaman yang jelas.

Contoh: dana hasil kejahatan dari Pemberi Pinjaman diberikan kepada Penerima Pinjaman untuk membiayai

kegiatan perdagangan umum, yang tidak jelas jenis komoditi yang diperdagangkan maupun mekanisme perdagangannya;

- 11) penggunaan identitas palsu di internet (enkripsi, akses terhadap identitas, perbankan internasional), dengan melakukan peretasan (akses secara tidak sah ke perangkat/akun orang lain) terhadap *e-mail*, atau situs web, dan/atau membuat situs web yang seolah-olah asli padahal palsu (*phishing*) untuk tujuan mengaburkan identitas dan/atau membuat identitas palsu dalam rangka Pencucian Uang.

Penggunaan identitas palsu dapat dilakukan dalam bentuk mencuri identitas orang lain atau menggabungkan identitas asli dengan identitas palsu sehingga menghasilkan identitas baru yang seolah-olah asli;

- 12) transfer internasional/penggunaan rekening bank asing, yaitu teknik yang digunakan untuk melakukan transfer dana hasil kejahatan antara lembaga keuangan dan sering kali ke yurisdiksi lain untuk menghindari deteksi dan penyitaan aset.

Contoh: Pemberi Pinjaman menyimpan dana di bank asing di mana dana Pemberi Pinjaman berasal dari hasil kejahatan;

- 13) penggunaan dana hasil kejahatan terkait obat-obatan terlarang, di mana uang hasil penjualan obat-obatan terlarang menjadi dana pinjaman oleh Pemberi Pinjaman;
- 14) Pemberi Pinjaman dan Penerima Pinjaman merupakan pihak yang saling memiliki hubungan afiliasi/terafiliasi, di mana dana pinjaman berasal dari hasil kejahatan. Contoh: Penerima Pinjaman menerima dana pinjaman dari Pemberi Pinjaman di mana dana pinjaman berasal dari hasil kejahatan dan antara Pemberi Pinjaman dengan Penerima Pinjaman memiliki hubungan afiliasi;

- 15) pada produk *purchase order financing*, pelaku kejahatan selaku Penerima Pinjaman menyusun proyek fiktif untuk dapat menerima pinjaman melalui Penyelenggara dan membayar pinjaman tersebut dengan dana dari hasil

kejahatan; dan

- 16) penyetoran dana pinjaman pada Penyelenggara oleh Pemberi Pinjaman dilakukan oleh pihak selain Pemberi Pinjaman dimaksud dan penyetoran dana pinjaman menggunakan dana hasil kejahatan.

6. Gambaran Umum Pendanaan Terorisme

- a. Setiap aksi terorisme yang dilakukan di Indonesia pada dasarnya membutuhkan dukungan, baik dalam bentuk persenjataan (senjata api, senjata tajam, dan bahan peledak), tempat tinggal, kendaraan untuk mobilisasi, fasilitas perang, dana dan penyediaan kebutuhan lainnya untuk melakukan aksi terorisme.

Dalam tindak pidana terorisme, uang atau dana diperuntukkan sebagai sarana untuk melakukan aksi dan bukan sebagai sasaran yang ingin dicari sehingga berbagai cara akan dilakukan oleh para pelaku tindak pidana terorisme untuk mendapatkan dana baik secara sah seperti menjual barang dan/atau jasa, maupun dengan aksi kejahatan seperti perampokan, penipuan, hingga peretasan situs investasi dalam jaringan (*online investment*). Dana yang terkumpul dipergunakan untuk mendapatkan persenjataan, membeli bahan peledak, membangun jaringan atau perekrutan anggota, pelatihan perang, mobilisasi anggota dari atau ke suatu tempat demi terlaksananya aksi teror.

Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme memuat definisi dana adalah semua aset atau benda bergerak atau tidak bergerak, baik yang berwujud maupun yang tidak berwujud, yang diperoleh dengan cara apapun dan dalam bentuk apapun, termasuk dalam format *digital* atau elektronik, alat bukti kepemilikan, atau keterkaitan dengan semua aset atau benda tersebut termasuk tetapi tidak terbatas pada kredit bank, cek perjalanan, cek yang dikeluarkan oleh bank, perintah pengiriman uang, saham, sekuritas, obligasi, bank draf, dan surat pengakuan utang.

- b. TPPT adalah penggunaan harta kekayaan secara langsung atau tidak langsung untuk kegiatan terorisme, organisasi teroris, atau teroris. Pendanaan Terorisme pada dasarnya merupakan jenis tindak pidana yang berbeda dari TPPU, namun demikian keduanya mengandung kesamaan yaitu menggunakan jasa keuangan sebagai sarana untuk melakukan suatu tindak pidana.
- c. Berbeda dengan TPPU yang tujuannya untuk menyamarkan asal-usul harta kekayaan, maka tujuan TPPT adalah membantu kegiatan terorisme, baik dengan harta kekayaan yang merupakan hasil dari suatu tindak pidana ataupun dari harta kekayaan yang diperoleh secara sah. Untuk mencegah Penyelenggara digunakan sebagai sarana TPPT, maka Penyelenggara perlu menerapkan program APU dan PPT secara memadai.
- d. Beberapa modus Pendanaan Terorisme antara lain:
  - 1) perampokan atau pencurian, di mana pelaku TPPT berpendapat bahwa adalah halal mengambil harta orang atau pihak lain. Dalam kaitan tersebut, pelaku TPPT melakukan:
    - a) pencurian dana untuk Pendanaan Terorisme dengan cara melakukan pinjaman kepada Penyelenggara tanpa adanya niat untuk membayar pinjaman tersebut. Dalam hal ini, pelaku menganggap bahwa dana hasil pencurian dengan meminjam kepada Penyelenggara tersebut merupakan dana yang dapat digunakan untuk aksi terorisme; dan/atau
    - b) tindak pidana kejahatan seperti perampokan di mana dana hasil kejahatan perampokan tersebut digabungkan dengan dana yang diperoleh Penerima Pinjaman melalui Penyelenggara untuk selanjutnya digunakan mendanai pengelolaan jaringan teroris dan kegiatan teroris;
  - 2) pelaku melakukan peretasan akun milik Nasabah yang terdaftar pada Penyelenggara untuk melakukan pinjaman dana melalui Penyelenggara yang dananya digunakan untuk kegiatan terorisme;

- 3) penyalahgunaan yayasan, di mana dana pinjaman yang diterima yayasan sebagai Penerima Pinjaman melalui Penyelenggara disalahgunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris;
- 4) penyamaran kegiatan usaha (barang/jasa) di mana Penerima Pinjaman pada saat melakukan pinjaman dana melalui Penyelenggara menyamarkan kegiatan usahanya seperti berdagang atau usaha jasa, namun dalam praktiknya dana pinjaman dimaksud digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris;
- 5) peminjaman dana melalui beberapa Penyelenggara yang dimaksudkan untuk memperoleh dana pinjaman yang maksimal untuk digunakan mendanai pengelolaan jaringan teroris dan kegiatan teroris, serta dimaksudkan untuk memecah transaksi untuk menghindari pelaporan;
- 6) pendanaan dari individu atau lembaga baik di dalam maupun luar negeri yang diberikan secara langsung maupun tidak langsung ke Pemberi Pinjaman untuk disalurkan ke Penerima Pinjaman yang terafiliasi dengan individu atau lembaga tersebut, di mana dana dimaksud digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris;
- 7) penggunaan alamat bisnis oleh Penerima Pinjaman yang tidak memiliki keterkaitan dengan pekerjaan dari Penerima Pinjaman, yang dimaksudkan agar dana pinjaman dapat disetujui dan diterima oleh Penerima Pinjaman dalam jumlah relatif besar, di mana dana yang diterima Penerima Pinjaman tersebut digunakan mendanai pengelolaan jaringan teroris dan kegiatan teroris. Contoh: ibu rumah tangga selaku Penerima Pinjaman yang beralamat di area bisnis menerima dana pinjaman yang nilainya relatif besar melalui Penyelenggara untuk selanjutnya digunakan mendanai pengelolaan jaringan teroris dan kegiatan teroris; dan
- 8) penggunaan pelajar/mahasiswa yang memenuhi syarat sebagai Penerima Pinjaman melalui Penyelenggara antara lain untuk keperluan sekolah Penerima Pinjaman yang

dilakukan secara rutin, di mana dana yang diterima oleh Pelajar tersebut digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris.

## II. PENERAPAN PROGRAM APU DAN PPT SERTA PENCEGAHAN PENDANAAN PROLIFERASI SENJATA PEMUSNAH MASSAL BERBASIS RISIKO (*RISK BASED APPROACH*)

1. Penerapan Program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berbasis risiko (*risk based approach*) paling sedikit meliputi:
  - a. pengawasan aktif Direksi dan Dewan Komisaris;
  - b. kebijakan dan prosedur;
  - c. pengendalian intern;
  - d. sistem informasi manajemen; dan
  - e. sumber daya manusia serta pelatihan.

2. Kewajiban Penerapan Program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal Berbasis Risiko (*Risk Based Approach*)

- a. Program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal merupakan program yang harus diterapkan Penyelenggara dalam melakukan hubungan usaha dan transaksi dengan Pengguna. Program tersebut antara lain mencakup hal yang diharuskan dalam Rekomendasi FATF sebagai upaya untuk melindungi Penyelenggara agar tidak dijadikan sebagai sarana atau sasaran pencucian uang, pendanaan terorisme serta pencegahan pendanaan serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.

Rekomendasi FATF menegaskan bahwa Penyelenggara wajib mengidentifikasi, menilai, dan memahami risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal terkait dengan Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*).

Penyelenggara melakukan penilaian sendiri dan menerapkan proses kerangka kerja manajemen risiko yang efektif. Penyelenggara harus melakukan pendokumentasian dan pengkinian penilaian risiko terkait

penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.

- b. Penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berbasis risiko (*risk based approach*) mendukung Penyelenggara dalam menerapkan tindakan pencegahan dan mitigasi risiko yang sepadan dengan risiko TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal yang teridentifikasi. Penyelenggara selanjutnya dapat mengalokasikan sumber dayanya sesuai dengan profil risiko yang dihadapinya, mengelola pengendalian intern, struktur internal, dan implementasi kebijakan dan prosedur untuk mencegah serta mendeteksi Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal.
- c. Dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berbasis risiko (*risk based approach*), Penyelenggara harus merujuk pada risiko yang tercantum dalam NRA dan SRA. Adapun risiko yang tercantum dalam NRA dan SRA tersebut dapat berkembang dan mengalami perubahan, karena itu Penyelenggara harus responsif terhadap perubahan risiko tersebut.

### 3. Konsep Risiko

#### a. Definisi Risiko

Risiko dapat didefinisikan sebagai kemungkinan (*likelihood*) suatu kejadian dan dampak. Secara sederhana, risiko dapat dilihat sebagai kombinasi peluang yang mungkin terjadi dan tingkat kerusakan atau kerugian yang mungkin dihasilkan dari suatu peristiwa. Dalam konteks Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, risiko diartikan:

- 1) pada tingkat nasional adalah suatu ancaman dan kerentanan yang disebabkan oleh Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang membahayakan sistem keuangan nasional serta keselamatan dan keamanan nasional; dan
- 2) pada tingkat Penyelenggara adalah ancaman dan kerentanan yang menempatkan Penyelenggara pada risiko di mana Penyelenggara digunakan sebagai sarana

Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal.

Ancaman dapat berupa pihak atau obyek yang dapat menyebabkan kerugian. Dalam konteks Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, ancaman dapat berupa pelaku tindakan kriminal, fasilitator (pihak yang membantu pelaksanaan tindakan kriminal), dana para pelaku kejahatan, atau bahkan kelompok teroris.

Kerentanan adalah unsur kegiatan usaha yang dapat dimanfaatkan oleh ancaman yang telah teridentifikasi. Dalam konteks TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal kerentanan dapat diartikan pengendalian intern yang lemah dari Penyelenggara ataupun penawaran produk/ jasa/transaksi yang berisiko tinggi.

Dampak mengacu pada tingkat kerusakan dan kerugian yang serius yang timbul jika terjadi TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal.

b. Manajemen Risiko

Manajemen risiko adalah proses yang secara luas digunakan pada sektor publik dan sektor privat untuk membantu dalam pembuatan keputusan. Dalam kaitannya dengan Pencucian Uang, dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, proses dimaksud mencakup pemahaman terhadap risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, penilaian atas kedua risiko tersebut, dan pengembangan metode untuk mengelola dan mitigasi risiko yang telah diidentifikasi.

Dalam menerapkan manajemen risiko atas risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, Penyelenggara dapat mengembangkan metode manajemen risiko sesuai dengan karakteristik Penyelenggara dengan tetap mengacu pada peraturan perundang-undangan mengenai APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.

c. Risiko Bawaan (*Inherent Risk*) dan Risiko Residu (*Residual Risk*)

Dalam melakukan penilaian risiko, penting untuk membedakan antara risiko bawaan (*inherent risk*) dan risiko residu (*residual risk*).

Risiko bawaan (*inherent risk*) adalah risiko yang melekat pada suatu peristiwa atau keadaan yang telah ada sebelum penerapan tindakan pengendalian. Risiko bawaan (*inherent risk*) ini terkait dengan kegiatan usaha dan Nasabah Penyelenggara. Pada sisi lain, risiko residu (*residual risk*) adalah tingkat risiko yang tersisa setelah implementasi langkah mitigasi risiko dan pengendalian.

d. Pendekatan Berbasis Risiko (*Risk based Approach*)

Dalam konteks Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, pendekatan berbasis risiko (*risk based approach*) adalah suatu proses yang meliputi hal sebagai berikut:

- 1) penilaian risiko yang mencakup 4 (empat) faktor risiko, yaitu:
  - a) Nasabah;
  - b) negara/area geografis/yurisdiksi;
  - c) produk/jasa/transaksi; dan
  - d) jaringan distribusi (*delivery channels*);
- 2) Penyelenggara harus mempertimbangkan seluruh faktor risiko yang relevan termasuk risiko penggunaan Teknologi Informasi;
- 3) Penyelenggara harus mengelola dan memitigasi risiko melalui pelaksanaan pengendalian intern dan melakukan langkah-langkah yang sesuai dengan risiko yang telah diidentifikasi, serta melakukan pemantauan transaksi dan hubungan bisnis sesuai dengan tingkat risiko yang telah dinilai;
- 4) dalam melakukan identifikasi, penilaian, pengelolaan, dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, Penyelenggara harus memahami bahwa kegiatan tersebut bukanlah sesuatu yang statis. Risiko yang telah diidentifikasi dapat berubah dari waktu ke waktu sejalan dengan perkembangan produk baru atau ancaman baru yang masuk dalam kegiatan usaha Penyelenggara;
- 5) Penyelenggara harus melakukan pengkinian penilaian risiko secara berkala sesuai dengan kebutuhan Penyelenggara; dan
- 6) Penyelenggara harus melakukan pembaruan Teknologi Informasi serta Sistem Elektronik yang dipergunakan sesuai dengan ketentuan peraturan perundang-undangan yang mengatur mengenai informasi dan transaksi elektronik (ITE). Pembaruan

Teknologi Informasi serta Sistem Elektronik mencakup standar minimum sistem Teknologi Informasi, pengelolaan risiko Teknologi Informasi, pengamanan Teknologi Informasi, ketahanan terhadap gangguan dan kegagalan sistem, serta alih kelola sistem Teknologi Informasi, sebagai contoh adalah penerapan ISO 27001 dalam pembaharuan TI dan sistem elektronik.

4. Siklus Pendekatan Berbasis Risiko (*Risk based Approach*)
  - a. Dalam melakukan pendekatan berbasis risiko (*Risk based Approach*), Penyelenggara harus melakukan 6 (enam) langkah kegiatan sebagai berikut:
    - 1) melakukan identifikasi terhadap risiko bawaan (*inherent risk*);
    - 2) menetapkan toleransi risiko;
    - 3) menyusun langkah pengurangan dan pengendalian risiko;
    - 4) melakukan evaluasi atas risiko residu (*residual risk*);
    - 5) menerapkan pendekatan berbasis risiko (*risk based approach*); dan
    - 6) melakukan tinjauan dan evaluasi atas pendekatan berbasis risiko (*risk based approach*) yang telah dimiliki.
  - b. Alur siklus pendekatan berbasis risiko (*risk based approach*) adalah sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
5. Langkah Pendekatan Berbasis Risiko (*Risk based Approach*)
  - a. Identifikasi Risiko Bawaan (*Inherent Risk*)
    - 1) Dalam melakukan identifikasi risiko bawaan (*inherent risk*), Penyelenggara harus mempertimbangkan kerentanan Penyelenggara untuk digunakan sebagai sarana Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal. Langkah awal dalam melakukan penilaian risiko ialah dengan memahami kegiatan usaha Penyelenggara secara keseluruhan dengan perspektif yang luas. Pemahaman tersebut akan memungkinkan Penyelenggara untuk mempertimbangkan risiko yang mungkin terjadi, apakah risiko terjadi pada kegiatan usaha, Nasabah, atau produk tertentu.
    - 2) Jumlah risiko aktual yang diinventarisasi oleh Penyelenggara akan bervariasi bergantung pada produk/jasa/transaksi yang ditawarkan.

- 3) Penyelenggara harus mempertimbangkan unsur yang memicu timbulnya risiko bagi Penyelenggara baik dari sisi Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*). Penyelenggara harus memahami unsur apa saja yang merupakan risiko bawaan (*inherent risk*) dan risiko residu (*residual risk*).
- 4) Risiko Nasabah  
Penyelenggara harus memperhatikan risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal terkait profil Calon Nasabah atau Nasabah. Penyelenggara perlu mengategorikan Nasabah berdasarkan dengan tingkat risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal. Pengkategorian tersebut dapat mengacu pada klasifikasi risiko yang ditetapkan oleh Penyelenggara, sesuai dengan peraturan perundang-undangan dan standar internasional.
- 5) Risiko Nasabah yang terkait dengan kekhasan bisnis proses Penyelenggara meningkat apabila:
  - a) pengumpulan data pribadi hingga transaksi Nasabah dilakukan secara elektronik;
  - b) pemberian dana dari Pemberi Pinjaman (*lender*) yang memiliki nilai nominal yang sangat besar;
  - c) intensitas pinjaman dana oleh Penerima Pinjaman (*borrower*) melewati batas kewajaran termasuk yang berada di luar kebijakan yang normal/wajar atau yang berada di luar jadwal pembayaran normal;
  - d) intensitas pemberian dana oleh Pemberi Pinjaman (*lender*) melewati batas kewajaran termasuk yang berada di luar kebijakan yang normal/wajar atau yang berada di luar jadwal pembayaran normal;
  - e) penerimaan dana dari Pemberi Pinjaman (*lender*) yang bertindak untuk Pemilik Manfaat (*Beneficial Owner*);
  - f) peminjaman dana oleh Penerima Pinjaman (*borrower*) yang bertindak untuk Pemilik Manfaat (*Beneficial Owner*);
  - g) Nasabah yang mencari atau menerima produk/jasa/transaksi Penyelenggara yang tidak sesuai dengan kebutuhan atau tidak menguntungkan

Nasabah tersebut;

- h) Nasabah atau Pemilik Manfaat (*Beneficial Owner*) tidak bersedia memberikan data dan informasi dalam proses identifikasi;
- i) Nasabah atau Pemilik Manfaat (*Beneficial Owner*) memberikan informasi yang sangat minim atau informasi yang patut diduga sebagai informasi fiktif;
- j) Nasabah atau Pemilik Manfaat (*Beneficial Owner*) mengaburkan atau tidak menyampaikan identitas yang sebenarnya;
- k) *gatekeeper* seperti akuntan, pengacara atau profesi lainnya yang bertindak mewakili Nasabah sehubungan dengan rekening/kontrak pada Penyelenggara;
- l) Nasabah yang termasuk dalam kategori PEP, termasuk anggota keluarga atau pihak yang terkait (*close associates*) dari PEP;
- m) Pemberi Pinjaman atau Penerima Pinjaman berbentuk korporasi yang struktur kepemilikannya kompleks dan menimbulkan kesulitan untuk diidentifikasi siapa yang menjadi Pemilik Manfaat (*Beneficial Owner*), pemilik akhir (*ultimate owner*), atau pengendali akhir (*ultimate controller*) dari korporasi;
- n) Nasabah merupakan organisasi amal atau organisasi non-profit lainnya yang tidak diatur dan diawasi;
- o) *institutional lender* merupakan lembaga jasa keuangan yang diawasi otoritas/lembaga pengatur dan pengawas lain seperti koperasi atau badan hukum di luar lembaga jasa keuangan yang tidak menerapkan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal secara efektif;
- p) *institutional lender* yang berasal dari lembaga non jasa keuangan yang pengurusnya merupakan Nasabah berisiko tinggi atau PEP atau terafiliasi dengan PEP; dan/atau
- q) risiko penggunaan identitas palsu, dalam bentuk pemalsuan identitas yaitu *impersonation identities* (menirukan identitas) dan *synthetic identities* (menggabungkan identitas asli dan palsu). *Impersonation*

dilakukan dengan cara orang tersebut mencuri identitas orang lain. Sedangkan *synthetic identities* menggunakan pemalsuan identitas dengan cara menggabungkan identitas asli dengan identitas palsu sehingga menghasilkan identitas baru yang seolah-olah asli.

6) Risiko Negara/Area Geografis/Yurisdiksi

Dalam melakukan penilaian risiko, Penyelenggara harus mengidentifikasi unsur risiko tinggi terkait dengan lokasi geografis, baik lokasi geografis Penyelenggara maupun lokasi geografis Nasabah, atau lokasi tempat terjadinya hubungan usaha, dan dampaknya pada keseluruhan risiko.

Risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal terkait negara/area geografis/yurisdiksi meningkat apabila:

- a) dana Pemberi Pinjaman (*lender*) diterima dari negara atau yurisdiksi yang berisiko tinggi;
- b) Pemberi Pinjaman (*lender*) memiliki hubungan afiliasi dengan orang perseorangan dan/atau korporasi dari negara atau yurisdiksi berisiko tinggi;
- c) Penerima Pinjaman (*borrower*) memiliki hubungan afiliasi dengan orang perseorangan dan/atau korporasi dari negara atau yurisdiksi berisiko tinggi;
- d) dana Pemberi Pinjaman (*lender*) diterima dari wilayah yang memiliki tingkat kejahatan yang tinggi;
- e) Penerima Pinjaman (*borrower*) berdomisili di wilayah yang memiliki tingkat kejahatan yang tinggi;
- f) dana Pemberi Pinjaman (*lender*) diterima dari wilayah di daerah perbatasan antar negara;
- g) Penerima Pinjaman (*borrower*) berdomisili di wilayah daerah perbatasan antar negara; dan/atau
- h) Penerima Pinjaman (*borrower*) dan/atau Pemberi Pinjaman (*lender*) tidak diketahui wilayah domisili aslinya (menggunakan *IP address* palsu).

Risiko yang terkait dengan domisili, kewarganegaraan, atau transaksi harus dinilai sebagai bagian dari risiko bawaan (*inherent risk*) dari Nasabah Penyelenggara.

Indikator yang menentukan suatu negara/area geografis/yurisdiksi berisiko tinggi terhadap Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, antara lain:

- a) yurisdiksi yang oleh organisasi yang melakukan *mutual assessment* terhadap suatu negara (seperti: *Financial Action Task Force on Money Laundering* (FATF) *on Money Laundering*, *Asia Pacific Group on Money Laundering* (APG), *Caribbean Financial Action Task Force* (CFATF), *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism* (MONEYVAL), *Eastern and Southern Africa Anti-Money Laundering Group* (ESAAMLG), *The Eurasian Group on Combating Money Laundering and Financing of Terrorism* (EAG), *The Grupo de Accion Financiera de Sudamerica* (GAFISUD), *Intergovernmental Anti-Money Laundering Group in Africa* (GIABA), atau *Middle East & North Africa Financial Action Task Force* (MENAFATF) diidentifikasi sebagai tidak secara memadai melaksanakan Rekomendasi FATF;
- b) negara yang diidentifikasi tidak kooperatif atau suaka pajak (*tax haven*) oleh *Organization for Economic Cooperation and Development* (OECD);
- c) negara yang memiliki tingkat tata kelola (*good governance*) yang rendah sebagaimana ditentukan oleh World Bank;
- d) negara yang memiliki tingkat risiko korupsi yang tinggi sebagaimana diidentifikasi dalam *Transparency International Corruption Perception Index*;
- e) negara yang diketahui secara luas sebagai tempat penghasil dan pusat perdagangan narkoba;
- f) negara yang dikenakan sanksi, embargo, atau yang serupa, oleh misalnya Perserikatan Bangsa Bangsa (PBB); dan
- g) negara atau yurisdiksi yang diidentifikasi oleh lembaga yang dipercaya, sebagai penyandang dana atau mendukung kegiatan terorisme, serta pendanaan Proliferasi Senjata Pemusnah Massal, atau yang membolehkan kegiatan organisasi teroris dan Proliferasi Senjata Pemusnah Massal di negaranya.

7) Risiko Produk/Jasa/Transaksi

Penilaian risiko secara keseluruhan harus mencakup penentuan risiko yang dapat terjadi atas berbagai produk/jasa/transaksi ditawarkan. Penyelenggara harus memperhatikan risiko yang berhubungan dengan produk/jasa/transaksi tertentu yang tidak secara khusus ditawarkan oleh Penyelenggara, namun memanfaatkan infrastruktur yang dimiliki Penyelenggara dalam menyediakan produk/jasa/transaksi.

Hal-hal yang dapat meningkatkan risiko produk/jasa/transaksi, antara lain:

- a) produk pinjaman multiguna yang tidak mewajibkan Nasabah untuk melampirkan/menyampaikan bukti pembelian barang dan jasa;
- b) produk pinjaman untuk pendanaan usaha produktif yang pada proses pendanaannya, Pemberi Pinjaman dapat memilih secara bebas pinjaman yang akan didanai. Hal ini berkaitan dengan adanya potensi adanya hubungan afiliasi antara Pemberi Pinjaman dengan Penerima Pinjaman untuk melakukan Pencucian Uang melalui Penyelenggara; dan
- c) produk pinjaman yang pembayarannya dimungkinkan untuk dilakukan oleh orang yang bukan merupakan Nasabah di mana Penyelenggara tidak dapat mendeteksi identitas dari rekening yang melakukan pembayaran.

8) Risiko Jaringan Distribusi (*Delivery Channels*)

Jaringan distribusi (*delivery channels*) merupakan media yang digunakan untuk memperoleh suatu produk/jasa/transaksi, atau media yang digunakan untuk melakukan suatu transaksi. Jaringan distribusi (*delivery channels*) harus dipertimbangkan sebagai risiko transaksi.

Salah satu ciri khas bisnis Penyelenggara adalah proses jaringan distribusi (*delivery channels*) yang dilakukan tanpa pertemuan langsung (*non face to face*), sebagai contoh penggunaan aplikasi pada telepon genggam (*mobile apps*) dan *website*, serta dapat diakses 24 (dua puluh empat) jam per hari, 7 (tujuh) hari dalam seminggu, dan dari manapun.

Dengan kekhasan yang dimiliki sangat mungkin Penyelenggara digunakan untuk mengaburkan identitas sebenarnya dari

Nasabah atau Pemilik Manfaat (*Beneficial Owner*) sehingga memiliki risiko yang lebih tinggi. Meskipun beberapa jaringan distribusi (*delivery channels*) dengan menggunakan aplikasi telepon genggam ataupun *website* di internet sudah lumrah, hal tersebut tetap perlu dipertimbangkan sebagai bagian dari faktor yang dapat menyebabkan risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal menjadi lebih tinggi.

Beberapa indikator yang dapat menyebabkan jaringan distribusi (*delivery channels*) berisiko tinggi, antara lain:

- a) aplikasi *online* yang digunakan dalam jaringan distribusi tidak tersertifikasi untuk mendapatkan alih kelola sistem Teknologi Informasi; dan
- b) penggunaan pihak lain dalam melakukan penyaluran dan/atau pembayaran pinjaman misalnya penggunaan agen lapangan.

9) Risiko Relevan Lainnya

Faktor lain yang relevan yang dapat memberikan dampak pada risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, antara lain:

- a) perkembangan tren tipologi, metode, teknik, dan skema Pencucian Uang dan Pendanaan Terorisme;
- b) model bisnis, skala usaha, jumlah cabang, dan jumlah karyawan sebagai faktor risiko bawaan (*inherent risk*) Penyelenggara;
- c) total nilai dan intensitas transaksi yang tinggi, yang memerlukan mitigasi risiko yang memadai;
- d) penggunaan Teknologi Informasi dalam seluruh rangkaian proses bisnis Penyelenggara;
- e) keamanan data dari risiko serangan siber (*cyberattacks*), di mana Penyelenggara sangat bergantung pada penggunaan *open communication network* (internet), sehingga pada proses penggunaan internet tersebut terdapat risiko besar terhadap serangan siber (*cyberattacks*);
- f) perlindungan data pribadi yang mencakup perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman,

pengiriman, penyebarluasan, dan pemusnahan data pribadi sesuai dengan ketentuan peraturan perundang-undangan. Risiko paling besar bagi Penyelenggara adalah terkait dengan buruknya manajemen perlindungan data pribadi;

- g) rekam jejak audit, di mana Penyelenggara diharuskan untuk menyediakan rekam jejak audit terhadap seluruh kegiatannya di dalam Sistem Elektronik Penyelenggara. Rekam jejak audit sangat penting karena digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian dan pemeriksaan lainnya; dan
- h) pusat penyimpanan data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*), di mana keberadaan pusat data dan pusat pemulihan bencana ditujukan untuk memudahkan proses perlindungan data pribadi dan untuk memulihkan kembali data atau informasi serta fungsi penting Sistem Elektronik yang terganggu atau rusak akibat bencana yang disebabkan oleh alam dan/atau manusia.

Melalui pusat penyimpanan data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*), Penyelenggara tetap memiliki data cadangan (*back up data*), sehingga tidak mengulang proses pengumpulan data kembali.

- 10) Penyelenggara perlu mempertimbangkan bahwa faktor risiko sebagaimana dimaksud pada angka 4) sampai dengan 9) di atas dapat saling terkait antara 1 (satu) faktor risiko dengan faktor risiko lainnya.
- 11) Indikator yang dapat meningkatkan risiko tidak terbatas pada indikator sebagaimana dimaksud pada angka 4) sampai dengan angka 9). Indikator yang dapat meningkatkan risiko tersebut dapat berkembang sesuai dengan kompleksitas Penyelenggara.
- 12) Penentuan Skala Risiko
  - a) Setelah melakukan identifikasi dan dokumentasi risiko bawaan (*inherent risk*), Penyelenggara perlu memberikan skala pada setiap risiko.
  - b) Skala risiko disusun dengan mempertimbangkan karakteristik dan kompleksitas kegiatan usaha.

- c) Untuk kegiatan usaha dengan karakteristik dan kompleksitas usaha rendah, Penyelenggara dapat mengkategorikan risiko dalam 2 (dua) kategori yaitu rendah dan tinggi.
  - d) Untuk kegiatan usaha dengan karakteristik dan kompleksitas usaha tinggi, Penyelenggara dapat mengkategorikan risiko dalam beberapa level, misalnya rendah (*low*), sedang (*medium*), dan tinggi (*high*).
- 13) Untuk membantu Penyelenggara melakukan evaluasi penilaian risiko, Penyelenggara dapat menggunakan matriks kemungkinan (*likelihood*) dan dampak (*impact*) sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
  - 14) Dalam melakukan tahapan identifikasi dari risiko bawaan (*inherent risk*), Penyelenggara harus mampu menjelaskan seluruh proses identifikasi risiko yang telah dilakukan oleh Penyelenggara dan alasan atau pertimbangannya.
  - 15) Setiap unsur risiko yang telah teridentifikasi sebagai risiko tinggi, harus dimitigasi dan didokumentasikan.  
Penyelenggara harus dapat menjelaskan kepada Otoritas Jasa Keuangan langkah mitigasi terhadap unsur risiko tinggi, contohnya langkah dalam kebijakan dan prosedur atau program pelatihan.
  - 16) Penyelenggara juga harus dapat menunjukkan kepada Otoritas Jasa Keuangan bahwa langkah mitigasi risiko tersebut telah dilaksanakan secara efektif, misalnya ditunjukkan melalui hasil audit internal atau audit independen.
  - 17) Penyelenggara harus menyediakan informasi yang telah terdokumentasi, yang menunjukkan bahwa Penyelenggara telah secara khusus memperhatikan indikator yang berisiko tinggi dalam penilaian risikonya.
  - 18) Dalam rangka mengidentifikasi risiko TPPU, TPPT, dan/atau pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dan menetapkan skala risiko (*risk ranking*) dari Calon Nasabah pada saat pembukaan hubungan atau Nasabah pada saat melakukan transaksi, Penyelenggara dapat menggunakan

*regulatory technology* seperti *big data analytic*, *machine learning*, dan/atau *robo advisor*.

b. Menetapkan Toleransi Risiko

- 1) Toleransi risiko (*risk tolerance*) merupakan tingkat dan jenis risiko yang secara maksimum dapat ditoleransi atau dilaksanakan dan ditetapkan oleh Penyelenggara, di mana risiko ini paling sedikit mencakup pemenuhan ketentuan sebagaimana dimaksud dalam POJK APU dan PPT serta peraturan pelaksanaannya. Toleransi risiko merupakan penjabaran dari tingkat risiko yang akan diambil (*risk appetite*).

Sementara *risk appetite* adalah risiko yang ingin diambil oleh Penyelenggara, baik dalam bentuk *risk taker* maupun *non risk taker*.

- 2) Toleransi risiko adalah komponen penting dari manajemen risiko yang efektif.
- 3) Penyelenggara harus menetapkan toleransi risiko sebelum mempertimbangkan mitigasi risiko.
- 4) Pada saat mempertimbangkan ancaman, konsep toleransi risiko akan memungkinkan Penyelenggara untuk menentukan tingkat ancaman risiko yang dapat ditoleransi oleh Penyelenggara.
- 5) Dalam menetapkan toleransi risiko, Penyelenggara perlu mempertimbangkan kategori risiko di bawah ini yang dapat memengaruhi Penyelenggara, antara lain:
  - a) risiko kepatuhan (*compliance risk*);
  - b) risiko reputasi (*reputational risk*);
  - c) risiko hukum (*legal risk*);
  - d) risiko operasional (*operational risk*); dan
  - e) risiko fraud (*fraud risk*).

c. Langkah Pengurangan dan Pengendalian Risiko

- 1) Mitigasi risiko adalah penerapan pengendalian internal untuk membatasi Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang telah diidentifikasi dalam melakukan penilaian risiko. Mitigasi risiko akan membantu agar kegiatan usaha Penyelenggara tetap berada dalam batas toleransi risiko yang telah ditetapkan. Dalam hal hasil penilaian risiko menunjukkan bahwa Penyelenggara memiliki tingkat risiko tinggi, Penyelenggara harus

mengembangkan strategi mitigasi risiko secara tertulis (berupa kebijakan dan prosedur untuk memitigasi risiko tinggi) dan menerapkannya pada area atau hubungan usaha yang berisiko tinggi sebagaimana yang telah diidentifikasi.

- 2) Mitigasi risiko dilakukan dalam penerapan 5 (lima) pilar penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal secara efektif dan memadai yang paling sedikit meliputi:
  - a) pengawasan aktif Direksi dan Dewan Komisaris;
  - b) kebijakan dan prosedur;
  - c) pengendalian intern;
  - d) sistem informasi manajemen; dan
  - e) sumber daya manusia dan pelatihan.
- 3) Penyelenggara harus menunjukkan kepada Otoritas Jasa Keuangan bahwa mitigasi risiko tersebut telah dilaksanakan secara efektif, misalnya ditunjukkan dengan bukti surat izin/sertifikasi sebagai penyedia Sistem Elektronik yang diperoleh dari Kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
- 4) Pengendalian intern dan mitigasi risiko pada area atau hubungan usaha yang berisiko tinggi didasarkan pada penerimaan risiko (*risk appetite*) dan toleransi risiko (*risk tolerance*).
- 5) Dalam semua situasi, kegiatan usaha Penyelenggara harus mempertimbangkan pengendalian intern yang akan berpengaruh dalam memitigasi keseluruhan risiko yang telah diidentifikasi.
- 6) Dalam penilaian risiko, semua area berisiko tinggi yang telah diidentifikasi sebagai bagian dari penilaian risiko harus dimitigasi dengan pengendalian intern serta didokumentasikan dengan baik.
- 7) Untuk semua Nasabah dan hubungan usaha, Penyelenggara harus:
  - a) melakukan pemantauan terhadap seluruh hubungan usaha; dan
  - b) mendokumentasikan informasi terkait dan langkah yang telah dilakukan.

- 8) Untuk Nasabah dan hubungan usaha yang berisiko tinggi, Penyelenggara harus:
    - a) melakukan pemantauan yang lebih sering terhadap hubungan usaha tersebut; dan
    - b) mengambil langkah yang lebih ketat dalam melakukan identifikasi dan pengkinian data.
  - 9) Dengan adanya kegiatan mitigasi risiko, Penyelenggara dapat:
    - a) melakukan pengkinian dan penatausahaan terhadap informasi Nasabah dan Pemilik Manfaat (*Beneficial Owner*);
    - b) menetapkan dan melaksanakan kegiatan pemantauan berkelanjutan pada setiap tingkatan hubungan usaha Penyelenggara (bagi Nasabah berisiko rendah dilakukan secara periodik dan bagi Nasabah berisiko tinggi dilakukan lebih sering dibandingkan Nasabah berisiko rendah);
    - c) melaksanakan mitigasi terhadap area berisiko tinggi. Strategi mitigasi risiko ini harus tercantum dalam kebijakan dan prosedur; dan
    - d) menerapkan prosedur pengendalian intern secara konsisten.
- d. Evaluasi atas Risiko Residu (*Residual Risk*)
- 1) Risiko residu (*residual risk*) merupakan risiko yang tersisa setelah penerapan pengendalian intern dan mitigasi risiko. Penyelenggara perlu memperhatikan bahwa seketat apapun mitigasi risiko dan manajemen risiko yang dimiliki, Penyelenggara tetap akan memiliki risiko residu (*residual risk*) yang harus dikelola secara baik.
  - 2) Risiko residu (*residual risk*) harus sesuai dengan toleransi risiko yang telah ditetapkan. Penyelenggara harus memastikan bahwa risiko residu (*residual risk*) tidak lebih besar dari toleransi risiko yang telah ditetapkan. Dalam hal risiko residu (*residual risk*) masih lebih besar daripada toleransi risiko, atau dalam hal pengendalian intern dan mitigasi terhadap area berisiko tinggi tidak memadai, Penyelenggara harus kembali melakukan langkah pengurangan dan pengendalian risiko, serta meningkatkan level atau kuantitas dari langkah mitigasi yang telah ditetapkan.

- 3) Ciri-ciri risiko residu (*residual risk*) adalah:
  - a) risiko telah ditoleransi/diterima:

Dalam risiko ini, risiko tetap ada melebihi batas yang telah ditoleransi. Penerimaan terhadap risiko yang ditoleransi diartikan bahwa upaya yang dilakukan oleh Penyelenggara untuk mengurangi risiko tidak memberikan pengaruh dalam usaha mengurangi risiko. Namun demikian, risiko yang ditoleransi tersebut dapat meningkat dari waktu ke waktu. Sebagai contoh, ketika adanya ancaman baru Pencucian Uang dan Pendanaan Terorisme;
  - b) risiko telah dimitigasi:

Dalam risiko ini, risiko tetap ada meskipun telah dimitigasi. Risiko ini telah dikurangi, namun tetap tidak dapat dihilangkan. Dalam praktiknya, pengendalian intern yang telah ditetapkan mungkin tidak dapat diterapkan (misalnya, sistem pemantauan atau proses pemantauan transaksi gagal, sehingga menyebabkan beberapa transaksi tidak dilaporkan).
- 4) Dengan adanya kegiatan evaluasi terhadap risiko residu (*residual risk*), Penyelenggara dapat:
  - a) melakukan evaluasi terhadap risiko residu yang dimiliki; dan
  - b) melakukan penyesuaian tingkat risiko yang dimiliki dengan risiko yang ditoleransi/diterima.
- e. Penerapan Pendekatan Berbasis Risiko (*Risk Based Approach*)
  - 1) Penyelenggara menerapkan pendekatan berbasis risiko (*risk based approach*) yang didasarkan pada hasil penilaian risiko terhadap kegiatan/aktivitas usaha sehari-hari termasuk identifikasi, verifikasi, dan pemantauan, yang tetap perlu dilakukan sebagai persyaratan minimal.
  - 2) Pendekatan berbasis risiko (*risk based approach*) yang dimiliki Penyelenggara harus didokumentasikan untuk menunjukkan tingkat kepatuhan Penyelenggara. Kebijakan dan prosedur terkait pendekatan berbasis risiko (*risk based approach*) harus dikomunikasikan, dipahami, dan dipatuhi oleh semua pegawai, khususnya pegawai yang melakukan identifikasi dan penatausahaan data dan informasi Nasabah serta pelaporan

transaksi kepada otoritas terkait. Penyelenggara harus menyediakan informasi yang cukup untuk memproses dan melengkapi transaksi, sesuai dengan identifikasi dan penatausahaan data dan informasi Nasabah sebagaimana dipersyaratkan.

- 3) Prosedur dan kebijakan pendekatan berbasis risiko (*risk based approach*) harus memenuhi persyaratan minimal sebagai berikut:
  - a) identifikasi Nasabah;
  - b) penilaian risiko;
  - c) tindakan khusus terhadap area berisiko tinggi;
  - d) penatausahaan; dan
  - e) pelaporan.
- 4) Kebijakan dan prosedur dalam pendekatan berbasis risiko (*risk based approach*) juga mencakup hal terkait pendeteksian transaksi mencurigakan dan penentuan jenis pemantauan yang disesuaikan dengan tingkat risiko Nasabah atau hubungan usaha, serta aspek pemantauan baik dari sisi frekuensi, tata cara pelaksanaan, dan evaluasi terhadap hasil pemantauan.
- 5) Penyelenggara perlu melakukan pemantauan secara berkala terhadap seluruh hubungan usaha yang dilakukan, dan terhadap hubungan usaha yang berisiko tinggi terhadap Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal. Penyelenggara menerapkan langkah khusus yang lebih ketat terhadap Nasabah atau hubungan usaha yang berisiko tinggi.
- 6) Penyelenggara perlu memperhatikan bahwa dalam manajemen risiko dan mitigasi risiko dibutuhkan kepemimpinan dan keterlibatan pejabat senior. Pejabat senior bertanggung jawab dalam pengambilan keputusan terkait kebijakan, prosedur, proses pengendalian intern, dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal dalam kegiatan/aktivitas usaha yang dimiliki Penyelenggara.
- 7) Dengan adanya pendekatan berbasis risiko (*risk based approach*), Penyelenggara dapat:
  - a) memastikan bahwa penilaian risiko yang telah dilakukan menggambarkan proses pendekatan berbasis risiko (*risk*

- based approach*), frekuensi pemantauan Nasabah yang berisiko rendah dan berisiko tinggi, dan juga menggambarkan langkah pengendalian intern yang diberlakukan untuk mengurangi risiko tinggi yang telah diidentifikasi;
- b) menerapkan pendekatan berbasis risiko (*risk based approach*);
  - c) melakukan pengkinian data dan informasi terhadap Nasabah dan Pemilik Manfaat (*Beneficial Owner*);
  - d) melakukan pemantauan terhadap seluruh hubungan usaha yang dimiliki;
  - e) melakukan pemantauan yang lebih sering terhadap hubungan usaha yang berisiko tinggi;
  - f) melakukan langkah tertentu terhadap Nasabah berisiko tinggi; dan/atau
  - g) melibatkan pejabat senior dalam menghadapi situasi atau area berisiko tinggi (misalnya untuk PEP, pemberian persetujuan melakukan hubungan usaha diberikan oleh pejabat senior).
- f. Peninjauan dan Evaluasi Pendekatan Berbasis Risiko (*Risk based Approach*)
- 1) Penilaian risiko yang dimiliki oleh Penyelenggara harus dievaluasi berdasarkan kebutuhan untuk menguji efektivitas dari kepatuhan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, yang meliputi:
    - a) penilaian risiko terkait Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal;
    - b) pengawasan aktif Direksi dan Dewan Komisaris;
    - c) kebijakan dan prosedur;
    - d) kebutuhan sumber daya manusia yang memiliki pengetahuan dan kemampuan di bidang Teknologi Informasi serta bisnis proses Penyelenggaraan;
    - e) program pelatihan sumber daya manusia bagi karyawan, pejabat senior serta Direksi dan Dewan Komisaris terkait

- penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal; dan
- f) profil pegawai termasuk *profiling* data identitas serta kompetensi pegawai.
- 2) Dalam hal terhadap perubahan struktur kegiatan usaha dan adanya penawaran atas produk dan jasa baru, pengkinian atas penilaian risiko harus dilakukan untuk kebijakan dan prosedur, langkah mitigasi, dan pengendalian intern.
  - 3) Peninjauan atas penilaian risiko terkait Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal harus mencakup seluruh unsur termasuk kebijakan dan prosedur terhadap penilaian risiko, mitigasi risiko dan pemantauan berkelanjutan yang lebih intensif. Peninjauan dapat membantu Penyelenggara dalam mengevaluasi penyempurnaan kebijakan dan prosedur yang ada, atau untuk pembentukan kebijakan dan prosedur yang baru. Risiko yang telah diidentifikasi dapat berubah atau berkembang seiring dengan pengembangan produk baru atau timbulnya ancaman baru terhadap kegiatan usaha. Pada akhirnya, prosedur peninjauan dimaksud akan memengaruhi efektivitas dari pelaksanaan pendekatan berbasis risiko (*risk based approach*).
  - 4) Dengan adanya peninjauan pada pendekatan berbasis risiko (*risk based approach*), Penyelenggara dapat:
    - a) melakukan peninjauan sesuai dengan kebutuhan Penyelenggara;
    - b) menghasilkan tinjauan yang mencakup kepatuhan kebijakan dan prosedur, penilaian terhadap risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal serta program pelatihan untuk menguji efektivitas pendekatan berbasis risiko (*risk based approach*);
    - c) melakukan penatausahaan terhadap proses peninjauan dan melaporkan kepada pejabat senior; dan
    - d) melakukan penatausahaan hasil peninjauan bersama dengan penetapan langkah yang bersifat korektif untuk ditindaklanjuti.

### III. PENGAWASAN AKTIF DIREKSI DAN DEWAN KOMISARIS

#### 1. Pengawasan Aktif Direksi

Pengawasan aktif Direksi paling sedikit meliputi:

- a. memastikan Penyelenggara memiliki kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
- b. mengusulkan kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal kepada Dewan Komisaris termasuk mitigasi risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal dengan memuat paling sedikit:
  - 1) latar belakang penyusunan kebijakan dan prosedur;
  - 2) struktur, tugas, wewenang dan tanggung jawab unit kerja khusus (UKK) dan/atau pejabat yang tunjuk sebagai penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - 3) kebijakan dan prosedur program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - 4) pengawasan atas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal; dan
  - 5) rencana pengendalian internal;
- c. membentuk unit kerja khusus dan/atau menunjuk pejabat yang bertanggung jawab terhadap penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
- d. memberikan arahan yang jelas atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal;
- e. memastikan dilaksanakannya program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal sesuai dengan kebijakan dan prosedur tertulis yang sudah ditetapkan;

- f. melakukan pengawasan atas kepatuhan unit kerja dalam menerapkan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, termasuk memantau pelaksanaan tugas UKK dan/atau pejabat yang bertanggung jawab atas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - g. melakukan pengawasan dan mitigasi risiko secara aktif khususnya yang terkait dengan risiko Nasabah, risiko area/geografis/yuridis, risiko produk/jasa/transaksi, dan risiko jaringan distribusi;
  - h. memastikan bahwa kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal sejalan dengan perubahan dan pengembangan produk, jasa dan teknologi di sektor jasa keuangan serta sesuai dengan perkembangan modus Pencucian Uang dan/atau Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal;
  - i. memastikan bahwa seluruh pegawai telah mengikuti pelatihan yang berkaitan dengan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal secara berkala;
  - j. memberikan persetujuan yang bersifat teknis atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal yang berkaitan dengan teknis pelaksanaan tugas Direksi;
  - k. memberikan persetujuan yang bersifat teknis atas kebijakan, prosedur, rencana bisnis dan/atau perubahan Sistem Elektronik dengan mempertimbangkan risiko TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal; dan
  - l. memastikan pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan.
2. Pengawasan Aktif Dewan Komisaris
- Pengawasan aktif Dewan Komisaris paling sedikit meliputi:
- a. memberikan persetujuan atas kebijakan dan prosedur tertulis penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal yang diusulkan Direksi

- termasuk mitigasi risiko TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal;
- b. melakukan pengawasan atas pelaksanaan tugas dan tanggung jawab Direksi terhadap penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - c. memastikan adanya pembahasan terkait Pencucian Uang, Pendanaan Terorisme, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal dalam rapat Direksi dan Dewan Komisaris; dan
  - d. rapat pembahasan Direksi dan Dewan Komisaris terkait Pencucian Uang, Pendanaan Terorisme dan/atau pendanaan Proliferasi Senjata Pemusnah Massal harus memperhatikan hal-hal sebagai berikut:
    - 1) intensitas pelaksanaan rapat pembahasan diserahkan kepada Penyelenggara sesuai dengan kebutuhan dan kompleksitas usaha Penyelenggara; dan
    - 2) materi pembahasan dalam rapat Direksi dan Dewan Komisaris dapat berupa antara lain:
      - a) mitigasi risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang ada di Penyelenggara;
      - b) penanganan permasalahan dan/atau hambatan yang dihadapi Penyelenggara dalam menerapkan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
      - c) pembaruan ketentuan peraturan perundang-undangan dan tipologi atau modus terkait APU dan PPT;
      - d) efektivitas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal; dan
      - e) hasil rapat pembahasan harus dituangkan dalam risalah rapat (*minute meeting*) yang ditanda tangani oleh Direksi dan Dewan Komisaris yang menghadiri rapat pembahasan tersebut.
3. Dalam mendukung efektivitas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, Direksi, dan Dewan Komisaris harus:

- a. memiliki pemahaman yang memadai mengenai risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang melekat pada seluruh aktivitas operasional Penyelenggara sehingga Direksi dan Dewan Komisaris mampu mengelola dan memitigasi risiko tersebut secara memadai sesuai dengan ketentuan peraturan perundangan undangan;
  - b. memiliki pemahaman terkait risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal terutama risiko Nasabah, risiko negara/area geografis/yurisdiksi, risiko produk/jasa/transaksi, risiko jaringan distribusi (*delivery channels*), dan risiko relevan lainnya;
  - c. memastikan struktur organisasi yang memadai untuk penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal; dan
  - d. bertanggung jawab atas kebijakan, prosedur, penerapan dan pengawasan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, termasuk pengelolaan dan mitigasi risiko TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal pada seluruh aktivitas operasional Penyelenggara.
4. Penanggung Jawab Penerapan Program APU dan PPT
- a. Penyelenggara harus memiliki penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.
  - b. Penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal harus berada dalam struktur organisasi Penyelenggara.
  - c. Penentuan dan keberadaan penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal didasarkan pada kebutuhan dan kompleksitas usaha Penyelenggara, artinya Penyelenggara dapat memiliki UKK dan pejabat penanggung jawab atau hanya memiliki UKK saja atau hanya memiliki pejabat penanggung jawab saja.
  - d. Dalam hal penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah

Massal berupa UKK, maka harus memenuhi ketentuan sebagai berikut:

- 1) terdiri paling sedikit 2 (dua) orang yaitu 1 (satu) orang pimpinan dan 1 (satu) orang pelaksana;
  - 2) tidak merangkap fungsi lain; dan
  - 3) berada di bawah koordinasi Direksi secara langsung.
- e. Dalam hal penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berupa pejabat penanggung jawab, maka pejabat penanggung jawab hanya dapat merangkap fungsi kepatuhan dan manajemen risiko.
- f. UKK dan/atau pejabat penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal melapor dan bertanggung jawab kepada Direksi yang memiliki tugas mengawasi penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.
- g. Penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dapat dilaksanakan oleh salah satu anggota Direksi. Dalam hal anggota Direksi ditunjuk sebagai penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, anggota Direksi tersebut tidak boleh melaksanakan fungsi lainnya dan hanya dapat melaksanakan fungsi kepatuhan dan manajemen risiko.
- h. Dalam hal Penyelenggara memiliki kantor cabang, Penyelenggara harus memiliki penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal di kantor pusat dan kantor cabang. Penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal di kantor cabang dapat dirangkap oleh penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal di kantor pusat sepanjang penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berada dalam rentang kendali penanggung jawab di kantor pusat.

- i. UKK dan/atau pejabat penanggung jawab penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal harus:
  - 1) independen terhadap kegiatan yang menjadi tanggung jawabnya;
  - 2) memiliki kemampuan yang memadai dalam menerapkan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal yang dibuktikan antara lain pernah mengikuti pelatihan APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal atau sertifikasi APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - 3) mampu memberikan informasi yang dibutuhkan oleh Direksi untuk mendapatkan gambaran tentang kondisi, risiko dan mitigasi risiko penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal; dan
  - 4) memiliki akses yang tepat dan tidak dibatasi untuk melihat dan menganalisis dokumen identifikasi Nasabah, rekening terdaftar, catatan akuntansi lain, dan informasi terkait lainnya.

#### IV. KEBIJAKAN DAN PROSEDUR

1. Kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berdasarkan pendekatan berbasis risiko dimaksud paling sedikit meliputi:
  - a. identifikasi dan verifikasi Calon Nasabah atau Nasabah;
  - b. identifikasi dan verifikasi Pemilik Manfaat (*Beneficial Owner*);
  - c. penutupan hubungan usaha atau penolakan transaksi;
  - d. pengelolaan risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang berkelanjutan terkait dengan Nasabah, negara area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi;

- e. pemeliharaan data yang akurat terkait dengan transaksi, penatausahaan proses CDD, dan penatausahaan kebijakan dan prosedur;
  - f. pengkinian dan pemantauan;
  - g. pelaporan kepada pejabat senior, Direksi, dan Dewan Komisaris; dan
  - h. pelaporan kepada PPATK.
2. Kebijakan dan prosedur sebagaimana dimaksud pada angka 1 harus memperhatikan Prinsip Mengenali Pengguna Jasa (PMPJ/*Know Your Costumer* (KYC)).
  3. PMPJ/KYC yang terdiri atas *Customer Due Diligence* (CDD) dan *Enhanced Due Diligence* (EDD) dilakukan tidak hanya kepada Calon Nasabah pada saat Calon Nasabah melakukan registrasi sebagai Pengguna, tetapi juga terhadap Nasabah melalui pemantauan transaksi Nasabah.
  4. CDD mencakup kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Penyelenggara, dengan tujuan untuk memastikan hubungan usaha atau transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi Calon Nasabah dan Nasabah. Sementara EDD merupakan tindakan CDD lebih mendalam yang dilakukan Penyelenggara terhadap Calon Nasabah atau Nasabah yang berisiko tinggi termasuk PEP dan/atau dalam area berisiko tinggi.
  5. Melalui CDD atau EDD:
    - a. Penyelenggara dapat memperoleh informasi secara detail mengenai Calon Nasabah, mengenal Nasabah dan memahami transaksi yang dilakukan Nasabah, mengetahui transaksi Nasabah yang tidak normal atau mencurigakan, melindungi reputasi dan integritas Penyelenggara, memfasilitasi kepatuhan terhadap ketentuan, dan melindungi Penyelenggara dari ancaman eksternal yaitu digunakan sebagai sarana Pencucian Uang, Pendanaan Terorisme, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal; dan
    - b. Penyelenggara harus selalu berhati-hati dalam menerima Calon Nasabah serta terus melakukan pemantauan terhadap transaksi Nasabah yang menggunakan jasa Penyelenggara. Apabila transaksi yang dilakukan tidak sesuai dengan profil,

karakteristik, atau kebiasaan pola transaksi dari Nasabah yang bersangkutan, maka Penyelenggara wajib menyampaikan laporan TKM kepada PPATK.

6. CDD dilakukan oleh Penyelenggara pada saat:
  - a. melakukan hubungan usaha dengan Calon Nasabah atau transaksi dengan Nasabah;
  - b. terdapat transaksi keuangan dengan mata uang rupiah dan/atau mata uang asing yang nilainya paling sedikit atau setara dengan Rp100.000.000,00 (seratus juta rupiah);
  - c. terdapat indikasi transaksi keuangan mencurigakan yang terkait dengan Pencucian Uang, Pendanaan Terorisme, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal; atau
  - d. Penyelenggara meragukan kebenaran informasi yang diberikan oleh Calon Nasabah, Nasabah, penerima kuasa, dan/atau Pemilik Manfaat (*Beneficial Owner*).
7. CDD ulang dapat dilakukan oleh Penyelenggara apabila Penyelenggara menilai terdapat perubahan tingkat risiko yang disebabkan antara lain:
  - a. terdapat peningkatan nilai transaksi yang signifikan;
  - b. terdapat perubahan profil Nasabah yang bersifat signifikan; dan
  - c. informasi pada profil Nasabah yang tersedia dalam *customer identification file* (CIF) belum dilengkapi dengan dokumen dalam rangka verifikasi.
8. Identifikasi Calon Nasabah atau Nasabah
  - a. Penyelenggara wajib mengidentifikasi dan mengklasifikasikan Calon Nasabah atau Nasabah ke dalam kelompok orang perseorangan (*natural person*), korporasi, dan perikatan lainnya (*legal arrangement*).
  - b. Penyelenggara harus memiliki kebijakan tentang penerimaan dan identifikasi Calon Nasabah atau Nasabah.
  - c. Kebijakan penerimaan dan identifikasi Calon Nasabah sebagaimana dimaksud pada huruf b paling sedikit mencakup hal-hal sebagai berikut:
    - 1) permintaan informasi mengenai Calon Nasabah, bukti identitas, serta informasi dan/atau dokumen pendukung dari Calon Nasabah sebagaimana dimaksud dalam Pasal 20, Pasal 21, Pasal 22, Pasal 23, dan Pasal 24 POJK APU

- dan PPT;
- 2) penelitian atas kebenaran dokumen pendukung identitas Calon Nasabah sebagaimana dimaksud pada angka 1);
  - 3) permintaan dokumen identitas Calon Nasabah lebih dari satu yang dikeluarkan pihak yang berwenang, jika terdapat keraguan terhadap kartu identitas yang ada;
  - 4) apabila diperlukan dapat dilakukan wawancara dengan Calon Nasabah untuk memperoleh keyakinan atas kebenaran informasi, bukti identitas dan dokumen pendukung Calon Nasabah;
  - 5) larangan untuk membuka atau memelihara nama user/pengguna anonim atau nama fiktif; dan
  - 6) identifikasi terhadap transaksi atau hubungan usaha dengan Calon Nasabah yang berasal atau terkait dengan negara yang belum memadai dalam melaksanakan rekomendasi FATF yang dapat dilihat dari rilis resmi pada laman (*website*) FATF yang diterbitkan secara berkala.
- d. Penyelenggara dapat melakukan penerimaan dan identifikasi Calon Nasabah atau Nasabah secara elektronik sepanjang Sistem Elektronik Penyelenggara mampu untuk mengidentifikasi identitas dari Calon Nasabah atau Nasabah.
- e. Dalam pelaksanaan penerimaan dan identifikasi Calon Nasabah atau Nasabah secara elektronik, Penyelenggara tetap harus memperhatikan pedoman penerimaan dan identifikasi Calon Nasabah atau Nasabah sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c.
- f. Dalam hal penerimaan dan identifikasi Calon Nasabah dilakukan secara elektronik, pelaksanaannya dapat dilakukan antara lain melalui pengisian *form* elektronik dan penyampaian salinan dokumen sebagaimana dimaksud dalam Pasal 20, Pasal 21, Pasal 22, Pasal 23, dan Pasal 24 POJK APU dan PPT dalam bentuk *softcopy* melalui laman atau aplikasi Penyelenggara.
- g. Selain salinan dokumen sebagaimana dimaksud dalam huruf f, Penyelenggara dapat meminta sejumlah data, dokumen dan informasi tambahan yang dibutuhkan dalam mengidentifikasi dan memverifikasi Calon Nasabah atau Nasabah yang penyampaiannya dilakukan melalui laman atau melalui aplikasi

Penyelenggara. Adapun contoh data, dokumen, dan informasi tambahan tersebut antara lain sebagai berikut:

- 1) untuk Calon Nasabah atau Nasabah orang perseorangan antara lain alamat email, *softcopy* dokumen identitas tambahan yang dikeluarkan oleh pihak atau yang berwenang, dan foto wajah (swafoto);
- 2) untuk Calon Nasabah atau Nasabah korporasi antara lain:
  - a) alamat *email* dan nomor telepon korporasi; dan
  - b) nama, alamat *email*, nomor telepon, foto wajah (swafoto), serta dokumen identitas pihak yang ditunjuk mempunyai wewenang bertindak untuk dan atas nama korporasi dalam melakukan hubungan usaha dengan Penyelenggara.
- 3) untuk Calon Nasabah atau Nasabah perikatan lainnya (*legal arrangement*) antara lain:
  - a) bagi perikatan lainnya berupa *trust*, data, informasi terkait nama, email, nomor telepon, foto wajah (swafoto), serta dokumen identitas orang perseorangan dari pihak yang ditunjuk mempunyai wewenang bertindak untuk dan atas nama perikatan lainnya, penitip harta (*settlor*), penerima dan pengelola harta (*trustee*), penjamin/*protector* (apabila ada), penerima manfaat, dan orang perseorangan yang menjadi pengendali akhir dari *trust* dalam melakukan hubungan usaha dengan Penyelenggara.
  - b) bagi perikatan lainnya dalam bentuk selain *trust* yakni data, informasi terkait nama, *email*, nomor telepon, foto wajah (swafoto), serta dokumen identitas orang perseorangan yang mempunyai posisi yang sama atau setara dengan pihak dalam *trust* sebagaimana dimaksud dalam huruf a).
- 4) untuk Calon Nasabah berupa lembaga negara, instansi pemerintah, lembaga internasional atau perwakilan negara asing antara lain nama, *email*, nomor telepon, foto wajah (swafoto), serta dokumen identitas pihak yang ditunjuk mempunyai wewenang bertindak untuk dan atas nama lembaga negara, instansi pemerintah, lembaga

internasional, dan perwakilan negara asing tersebut dalam melakukan hubungan usaha dengan Penyelenggara.

9. Verifikasi Calon Nasabah atau Nasabah

- a. Dalam rangka melakukan hubungan usaha dengan Calon Nasabah atau transaksi dengan Nasabah, Penyelenggara harus melakukan verifikasi atas informasi yang telah diberikan pada saat identifikasi melalui dokumen pendukung Calon Nasabah atau Nasabah.
- b. Dalam rangka meyakini kebenaran identitas Calon Nasabah, verifikasi dapat dilakukan dengan:
  - 1) melakukan wawancara melalui telepon, atau *video conference* dengan Calon Nasabah apabila diperlukan;
  - 2) mencocokkan kesesuaian profil Calon Nasabah, foto diri dan foto identitas Nasabah;
  - 3) mencocokkan kesesuaian dokumen identitas sidik jari, dan/atau foto diri (swafoto) dengan dokumen identitas atau dokumen lainnya yang mencantumkan tanda tangan, sidik jari, dan/atau foto diri (swafoto);
  - 4) meminta kepada Calon Nasabah untuk memberikan lebih dari satu dokumen identitas yang dikeluarkan oleh pihak yang berwenang apabila timbul keraguan terhadap dokumen identitas yang ada;
  - 5) melakukan pengecekan silang (apabila perlu) untuk memastikan adanya konsistensi dari berbagai informasi yang disampaikan. Pengecekan silang dilakukan dengan cara, antara lain:
    - a) menghubungi Calon Nasabah melalui telepon (rumah atau kantor);
    - b) menghubungi pejabat sumber daya manusia tempat Calon Nasabah bekerja apabila pekerjaan Calon Nasabah adalah karyawan suatu perusahaan atau instansi;
    - c) melakukan konfirmasi atas penghasilan Calon Nasabah dengan mensyaratkan rekening koran dari bank atau penyedia jasa keuangan lain; atau
    - d) melakukan analisis informasi geografis untuk melihat kondisi hutan melalui teknologi *remote sensing*

terhadap Calon Nasabah perusahaan yang bergerak di bidang kehutanan; dan/atau

- 6) memastikan bahwa Calon Nasabah tidak memiliki rekam jejak negatif dengan melakukan verifikasi identitas Calon Nasabah menggunakan sumber independen lainnya antara lain:
  - a) daftar terduga teroris dan organisasi teroris yang diterbitkan oleh Kepolisian Republik Indonesia;
  - b) daftar pendanaan Proliferasi Senjata Pemusnah Massal; atau
  - c) data lainnya seperti identitas pemberi kerja dari Calon Nasabah, rekening telepon dan rekening listrik.
- c. Penyelesaian proses verifikasi identitas Calon Nasabah atau Nasabah dilakukan sebelum membuka hubungan usaha dengan Calon Nasabah atau transaksi dengan Nasabah.
- d. Dalam kondisi tertentu, proses verifikasi dapat diselesaikan kemudian setelah dilakukannya hubungan usaha atau transaksi.

Contoh: dokumen identitas yang dipersyaratkan masih dalam proses pengurusan sehingga tidak dapat dipenuhi pada saat akan melakukan hubungan usaha dengan Penyelenggara.
- e. Dalam hal proses verifikasi diselesaikan kemudian setelah dilakukannya hubungan usaha atau transaksi sebagaimana dimaksud pada huruf d, maka Penyelenggara harus melakukan mitigasi risiko yang memadai, contohnya dengan melakukan hal-hal sebagai berikut:
  - 1) meminta dokumen yang dapat membuktikan bahwa kelengkapan dokumen yang dipersyaratkan masih dalam proses pengurusan.

Contoh:

    - a) untuk Nasabah korporasi dan perikatan lainnya berupa dokumen bukti pengurusan izin usaha yang dikeluarkan dari instansi yang berwenang, dan/atau dokumen bukti pengurusan nomor pokok wajib pajak dari instansi pemerintah yang berwenang menyelenggarakan urusan pemerintahan di bidang pajak; atau

- b) untuk Nasabah orang perseorangan berupa dokumen yang membuktikan bahwa akta pewarisan atau akta jual beli sebagai dokumen sumber dana sedang dalam proses pengurusan oleh notaris/pejabat pembuat akta tanah;
  - 2) memberlakukan pembatasan layanan dan/atau transaksi yang diberikan oleh Penyelenggara; dan/atau
  - 3) Penyelenggara meminta Calon Nasabah untuk melengkapi dokumen yang dipersyaratkan dalam jangka waktu tertentu.
- f) Penyelenggara dapat melakukan proses verifikasi Calon Nasabah atau Nasabah secara elektronik sepanjang Sistem Elektronik yang digunakan Penyelenggara mampu untuk memverifikasi kebenaran identitas dari Calon Nasabah atau Nasabah.
- g) Dalam hal Penyelenggara melaksanakan proses verifikasi secara elektronik, maka Penyelenggara harus memperhatikan hal-hal sebagai berikut:
- 1) Penyelenggara dapat melakukan verifikasi secara elektronik dengan cara pertemuan langsung tatap muka (verifikasi *face to face*) dengan ketentuan sebagai berikut:
    - a) verifikasi *face to face* secara elektronik dapat dilakukan melalui sarana elektronik milik Penyelenggara atau milik pihak ketiga;
    - b) dalam hal verifikasi *face to face* dilakukan melalui sarana elektronik milik Penyelenggara, maka pelaksanaannya menggunakan perangkat lunak milik Penyelenggara dengan perangkat keras milik Penyelenggara atau perangkat keras milik Nasabah atau Calon Nasabah.  
Contoh: Fitur *video call* pada aplikasi yang dimiliki Penyelenggara yang terhubung langsung secara *real-time* dan *online* dengan pegawai/pejabat Penyelenggara melalui *smarphone*, komputer, dan/atau tablet milik Nasabah atau Calon Nasabah;
    - c) dalam hal verifikasi *face to face* dilakukan menggunakan sarana elektronik milik pihak ketiga, maka pihak ketiga wajib mendapat persetujuan dari

Otoritas Jasa Keuangan; dan

- d) untuk memberikan tambahan keyakinan bagi Penyelenggara dalam melaksanakan proses verifikasi *face to face* melalui sarana elektronik sebagaimana dimaksud pada huruf a), Penyelenggara dapat menambahkan penggunaan mekanisme dan/atau teknologi pendeteksi gerak untuk memastikan bahwa Calon Nasabah atau Nasabah adalah subjek yang hidup dan tidak terdapat upaya penipuan identitas.

Contoh: mekanisme pendeteksi gerak pada proses verifikasi *face to face* secara elektronik antara lain pejabat/pegawai Penyelenggara meminta Calon Nasabah atau Nasabah bergerak secara acak ke berbagai arah (misalnya menggerakkan wajah 45 derajat atau 90 derajat ke kiri atau ke kanan), meminta Calon Nasabah atau Nasabah untuk memperlihatkan area sekitar tempat Calon Nasabah atau Nasabah pada saat melakukan verifikasi, dan/atau menyampaikan pertanyaan yang sifatnya konfirmasi kebenaran informasi atau identitas kepada Calon Nasabah atau Nasabah.

- 2) Proses verifikasi *face to face* dapat dikecualikan dengan proses verifikasi tanpa tatap muka (verifikasi *non-face to face*) dengan ketentuan sebagai berikut:

- a) verifikasi *non-face to face* dilakukan dengan menggunakan perangkat lunak milik Penyelenggara dengan perangkat keras milik Penyelenggara atau perangkat keras milik Nasabah atau Calon Nasabah.

Contoh: perangkat lunak milik Penyelenggara dan perangkat keras milik Nasabah atau Calon Nasabah yang digunakan untuk verifikasi *non-face to face* antara lain:

- (1) aplikasi milik Penyelenggara yang dapat diakses dengan perangkat gawai (*mobile device*) antara lain *smartphone* dan/atau komputer tablet; dan/atau
- (2) situs web (*website*) Penyelenggara yang dapat diakses melalui perangkat elektronik Calon

Nasabah atau Nasabah antara lain komputer dan/atau laptop.

Penyelenggara harus memastikan perangkat keras milik Nasabah atau Calon Nasabah dilengkapi dengan fitur pendukung verifikasi seperti kamera, pemindai, perekam, dan/atau pelacak lokasi;

b) verifikasi *non-face to face* wajib memanfaatkan data kependudukan yang memenuhi 2 (dua) faktor otentikasi. Yang dimaksud dengan “2 (dua) faktor otentikasi” mencakup:

(1) *what you have*, yaitu dokumen identitas yang dimiliki oleh Calon Nasabah yaitu Kartu Tanda Penduduk (KTP) Elektronik; dan

(2) *what you are*, yaitu data biometrik antara lain dalam bentuk sidik jari, iris mata milik Calon Nasabah, dan/atau teknologi pengenalan wajah.

Akses data kependudukan dapat diperoleh dengan mengacu kepada peraturan perundangan-undangan yang mengatur mengenai pemberian hak akses dan pemanfaatan data kependudukan, yang dapat diakses melalui *web service*, *web portal*, dan *card reader*.

Akses data kependudukan melalui *web service* dan *web portal* contohnya adalah melalui *platform* bersama di mana *platform* bersama dimaksud bertindak selaku perantara yang tidak memiliki hak akses data kependudukan dan tidak menyimpan data perseorangan.

Contoh akses data kependudukan lainnya adalah melalui pihak yang memanfaatkan data administrasi kependudukan yang memenuhi 2 (dua) faktor otentikasi sebagaimana dimaksud pada angka (1) dan angka (2) di mana pihak tersebut memperoleh sertifikasi dari Kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi;

c) untuk memberikan tambahan keyakinan bagi Penyelenggara dalam proses verifikasi *non face to face*

sebagaimana dimaksud pada huruf b), Penyelenggara dapat:

- (1) menambahkan faktor otentikasi lain yaitu *what you know*, yang antara lain dapat berupa *personal identification number (PIN)*, *password*, *onetime password (OTP)*, dan/atau *challenge-response*; dan/atau
- (2) menambahkan penggunaan teknologi pendeteksi gerak untuk memastikan bahwa Calon Nasabah atau Nasabah adalah subjek yang hidup dan tidak terdapat upaya penipuan identitas.
- 3) Untuk memberikan tambahan keyakinan bagi Penyelenggara, verifikasi yang dilakukan secara elektronik oleh Penyelenggara dapat memanfaatkan teknologi *artificial intelligence*, atau algoritma yang dipadankan dengan *database* Penyelenggara.

10. Identifikasi Calon Nasabah atau Nasabah Berisiko Tinggi atau PEP

- a. Dalam hal Penyelenggara menilai Calon Nasabah atau Nasabah berisiko tinggi atau PEP, maka Penyelenggara wajib menerapkan EDD.
- b. Penyelenggara harus memiliki kebijakan dan prosedur identifikasi Calon Nasabah atau Nasabah Berisiko Tinggi atau PEP.
- c. Kebijakan dan prosedur identifikasi Calon Nasabah dan Nasabah berisiko tinggi atau PEP sebagaimana dimaksud pada huruf b paling sedikit mencakup ketentuan sebagaimana dimaksud dalam ketentuan angka 8 huruf b, huruf c, dan huruf e.
- d. Identifikasi Calon Nasabah dan Nasabah berisiko tinggi atau PEP dapat dilakukan secara elektronik sepanjang Sistem Elektronik Penyelenggara mampu untuk mengidentifikasi identitas resmi dari Calon Nasabah atau Nasabah berisiko tinggi atau PEP.
- e. Dalam hal identifikasi Calon Nasabah dan Nasabah berisiko tinggi atau PEP dilakukan secara elektronik, pelaksanaannya dapat dilakukan antara lain melalui pengisian *form* elektronik dan penyampaian salinan dokumen sebagaimana dimaksud dalam Pasal 20, Pasal 21, Pasal 22, Pasal 23, dan Pasal 24 POJK

APU dan PPT secara elektronik (*softcopy*) melalui laman atau aplikasi Penyelenggara.

- f. Selain salinan dokumen sebagaimana dimaksud dalam huruf e, Penyelenggara dapat meminta sejumlah data, dokumen dan informasi tambahan yang dibutuhkan dalam mengidentifikasi dan memverifikasi Calon Nasabah secara elektronik yang penyampaiannya dilakukan melalui laman atau melalui aplikasi Penyelenggara. Adapun contoh data, dokumen, dan informasi tambahan tersebut antara lain sebagai berikut:
- 1) untuk Calon Nasabah atau Nasabah orang perseorangan antara lain alamat email, *softcopy* dokumen identitas tambahan yang dikeluarkan oleh pihak atau yang berwenang, dan foto wajah (swafoto);
  - 2) untuk Calon Nasabah atau Nasabah korporasi antara lain:
    - a) alamat *email* dan nomor telepon korporasi; dan
    - b) nama, alamat *email*, nomor telepon, foto wajah (swafoto), serta dokumen identitas pihak yang ditunjuk mempunyai wewenang bertindak untuk dan atas nama korporasi dalam melakukan hubungan usaha dengan Penyelenggara;
  - 3) untuk Calon Nasabah atau Nasabah perikatan lainnya (*legal arrangement*) antara lain:
    - a) bagi perikatan lainnya berupa *trust*, data, informasi terkait nama, email, nomor telepon, foto wajah (swafoto), serta dokumen identitas orang perseorangan dari pihak yang ditunjuk mempunyai wewenang bertindak untuk dan atas nama perikatan lainnya, penitip harta (*settlor*), penerima dan pengelola harta (*trustee*), penjamin/*protector* (apabila ada), penerima manfaat, dan orang perseorangan yang menjadi pengendali akhir dari *trust* dalam melakukan hubungan usaha dengan Penyelenggara; dan
    - b) bagi perikatan lainnya dalam bentuk selain *trust* yakni data, informasi terkait nama, email, nomor telepon, foto wajah (swafoto), serta dokumen identitas orang perseorangan yang mempunyai posisi yang sama atau setara dengan pihak dalam *trust* sebagaimana

dimaksud dalam huruf a); dan

- 4) untuk Calon Nasabah berupa lembaga negara, instansi pemerintah, lembaga internasional, dan perwakilan negara asing antara lain nama, email, nomor telepon, foto wajah (swafoto), serta dokumen identitas pihak yang ditunjuk mempunyai wewenang bertindak untuk dan atas nama lembaga negara, instansi pemerintah, lembaga internasional, dan perwakilan negara asing tersebut dalam melakukan hubungan usaha dengan Penyelenggara apabila orang perseorangan tersebut berisiko tinggi atau PEP.

11. Verifikasi Calon Nasabah atau Nasabah Berisiko Tinggi atau PEP

- a. Verifikasi Calon Nasabah dan Nasabah berisiko tinggi atau PEP dilaksanakan dengan memerhatikan ketentuan sebagaimana dimaksud dalam angka 9 huruf a sampai dengan huruf e.
- b. Selain memerhatikan ketentuan sebagaimana dimaksud dalam huruf a, Penyelenggara dapat melakukan verifikasi Calon Nasabah dan Nasabah berisiko tinggi atau PEP dalam pelaksanaan EDD dengan cara antara lain sebagai berikut:
  - 1) meminta atau mencari informasi tambahan tentang Nasabah bersangkutan (misalnya pekerjaan, dan besaran aset yang dimiliki) dan melakukan pengkinian atas data identitas Nasabah;
  - 2) meminta atau mencari informasi tambahan mengenai sumber dana atau sumber kekayaan Nasabah tersebut;
  - 3) meminta atau mencari informasi tambahan mengenai alasan atau dasar dari transaksi yang dilakukan oleh Nasabah;
  - 4) memperoleh persetujuan dari pejabat senior untuk memulai dan/atau melanjutkan hubungan usaha dan/atau transaksi; dan
  - 5) melakukan pemantauan yang semakin diperketat terhadap transaksi yang dilakukan oleh Nasabah tersebut.
- c. Verifikasi Calon Nasabah atau Nasabah berisiko tinggi atau PEP sebagaimana dimaksud dalam huruf a dapat dilakukan secara elektronik.
- d. Dalam hal Penyelenggara melakukan verifikasi Calon Nasabah atau Nasabah berisiko tinggi atau PEP secara elektronik, maka

Penyelenggara harus memerhatikan ketentuan sebagaimana dimaksud dalam angka 9 huruf g.

12. Identifikasi dan Verifikasi Pemilik Manfaat (*Beneficial Owner*).

a. Identifikasi Pemilik Manfaat (*Beneficial Owner*)

- 1) Penyelenggara harus memastikan apakah hubungan usaha dengan Calon Nasabah atau transaksi dengan Nasabah untuk kepentingan Calon Nasabah atau Nasabah atau untuk kepentingan pihak lain atau Pemilik Manfaat (*Beneficial Owner*).
- 2) Apabila Calon Nasabah mewakili Pemilik Manfaat (*Beneficial Owner*) untuk membuka hubungan usaha atau melakukan transaksi, Penyelenggara harus melakukan prosedur CDD terhadap Pemilik Manfaat (*Beneficial Owner*) yang sama ketatnya dengan prosedur CDD bagi Calon Nasabah.
- 3) Dalam hal Pemilik Manfaat (*Beneficial Owner*) tergolong Nasabah berisiko tinggi atau PEP, maka prosedur yang diterapkan adalah prosedur CDD yang lebih ketat atau uji tuntas lanjut (*Enhanced Due Dilligence/EDD*).
- 4) Penyelenggara harus meneliti kebenaran informasi yang disampaikan oleh Calon Nasabah dengan melakukan verifikasi terhadap dokumen pendukung berdasarkan dokumen dan/atau sumber independen lainnya serta memastikan kekinian informasi tersebut.
- 5) Dalam melakukan identifikasi terhadap Calon Nasabah korporasi, Penyelenggara harus menetapkan Pemilik Manfaat (*Beneficial Owner*).
- 6) Identifikasi Pemilik Manfaat (*Beneficial Owner*) dari korporasi berbentuk perseroan terbatas dapat dilakukan antara lain melalui penelusuran informasi sebagai berikut:
  - a) orang perseorangan yang memiliki persentase mayoritas kepemilikan saham. Kepemilikan saham mayoritas bergantung pada struktur kepemilikan dari perseroan terbatas, di mana dapat didasarkan pada *threshold* contohnya pihak yang memiliki saham dengan persentase lebih dari 25 (dua puluh lima) persen;

- b) dalam hal tidak ditemukan mayoritas kepemilikan saham (pemegang saham memiliki persentase kepemilikan yang sama), maka identifikasi pemegang saham perseroan yang paling mengendalikan perseroan dilakukan melalui bentuk lain misalnya orang perseorangan yang memiliki kemampuan dalam penentuan atau penunjukan anggota Direksi; dan
- c) dalam hal tidak ditemukan pemegang saham perseroan yang paling mengendalikan perseroan karena misalnya keputusan diambil secara kolektif oleh seluruh pemegang saham perseroan, maka identifikasi Pemilik Manfaat (*Beneficial Owner*) didasarkan pada anggota Dewan Komisaris atau Direksi yang paling mengendalikan perseroan terbatas dimaksud.

Langkah penelusuran informasi dalam rangka identifikasi Pemilik Manfaat (*Beneficial Owner*) sebagaimana dimaksud pada huruf a) sampai dengan huruf c) di atas, bukan merupakan langkah yang bersifat pilihan alternatif, tetapi merupakan langkah berjenjang yang masing-masing akan digunakan apabila langkah sebelumnya telah diterapkan oleh Penyelenggara, namun Penyelenggara belum dapat mengidentifikasi Pemilik Manfaat (*Beneficial Owner*) melalui langkah tersebut.

- 7) Bagi Pemilik Manfaat (*Beneficial Owner*) berupa lembaga negara atau instansi pemerintah, perusahaan yang mayoritas sahamnya dimiliki oleh negara, atau perusahaan publik atau emiten, Calon Nasabah tidak memiliki keharusan untuk menyampaikan dokumen dan/atau identitas pengendali akhir. Namun demikian, Penyelenggara tetap melakukan identifikasi dan verifikasi terhadap Pemilik Manfaat (*Beneficial Owner*) dengan menggunakan data, dan informasi yang tersedia di publik. Pengecualian terhadap keharusan penyampaian dokumen dan/atau identitas pengendali akhir Pemilik Manfaat (*Beneficial Owner*) harus didokumentasikan oleh Penyelenggara.

- 8) Apabila Penyelenggara meragukan atau tidak dapat meyakini identitas Pemilik Manfaat (*Beneficial Owner*), Penyelenggara wajib menolak untuk melakukan hubungan usaha dengan Calon Nasabah atau transaksi dengan Nasabah.
  - 9) Terhadap Calon Nasabah atau Pemilik Manfaat (*Beneficial Owner*) yang hubungan usahanya ditolak, Penyelenggara harus memperoleh paling sedikit informasi nama, nomor identitas, alamat, dan tempat tanggal lahir sesuai dengan salinan dokumen identitas yang diperoleh Penyelenggara untuk kepentingan pelaporan TKM.
  - 10) Identifikasi Pemilik Manfaat (*Beneficial Owner*) dapat dilaksanakan secara elektronik sepanjang Sistem Elektronik Penyelenggara mampu untuk mengidentifikasi identitas resmi dari Pemilik Manfaat (*Beneficial Owner*).
  - 11) Untuk mengetahui apakah Calon Nasabah atau Nasabah bertindak untuk kepentingan Pemilik Manfaat (*Beneficial Owner*), pelaksanaannya dapat dilakukan antara lain melalui penambahan pertanyaan apakah Calon Nasabah atau Nasabah bertindak untuk kepentingan Pemilik Manfaat (*Beneficial Owner*) pada pengisian *form* elektronik yang diisi melalui laman atau aplikasi Penyelenggara.
  - 12) Dalam hal Identifikasi Pemilik Manfaat (*Beneficial Owner*) dilaksanakan secara elektronik, pelaksanaannya dapat dilakukan antara lain melalui pengisian *form* elektronik dan penggugahan salinan dokumen identitas sebagaimana dimaksud pada Pasal 28 POJK APU dan PPT secara elektronik (*softcopy*) melalui laman atau aplikasi Penyelenggara.
- b. Verifikasi Pemilik Manfaat (*Beneficial Owner*)
- 1) Dalam rangka meyakini kebenaran identitas Pemilik Manfaat (*Beneficial Owner*), verifikasi dapat dilakukan dengan:
    - a) melakukan wawancara melalui telepon, atau *video conference* dengan Pemilik Manfaat (*Beneficial Owner*) apabila diperlukan;

- b) mencocokkan kesesuaian cap jempol, sidik jari, atau foto wajah (swafoto) dengan dokumen identitas atau dokumen lainnya yang mencantumkan tanda tangan, cap jempol, sidik jari, atau foto wajah (swafoto) Pemilik Manfaat (*Beneficial Owner*);
- c) meminta untuk memberikan lebih dari satu dokumen identitas Pemilik Manfaat (*Beneficial Owner*) yang dikeluarkan oleh pihak yang berwenang apabila timbul keraguan terhadap dokumen identitas yang ada;
- d) melakukan pengecekan silang (apabila perlu) untuk memastikan adanya konsistensi dari berbagai informasi yang disampaikan. Pengecekan silang dilakukan dengan cara, antara lain:
  - (1) menghubungi Calon Nasabah melalui telepon (rumah atau kantor);
  - (2) menghubungi pejabat sumber daya manusia tempat Calon Nasabah bekerja apabila pekerjaan Calon Nasabah adalah karyawan suatu perusahaan atau instansi;
  - (3) melakukan konfirmasi atas penghasilan Calon Nasabah dengan mensyaratkan rekening koran dari bank atau penyedia jasa keuangan lain; dan
  - (4) melakukan analisis informasi geografis untuk melihat kondisi hutan melalui teknologi *remote sensing* terhadap Calon Nasabah perusahaan yang bergerak di bidang kehutanan;
- e) memastikan bahwa Calon Nasabah tidak memiliki rekam jejak negatif dengan melakukan verifikasi identitas Calon Nasabah menggunakan sumber independen lainnya antara lain:
  - (1) daftar terduga teroris dan organisasi teroris yang diterbitkan oleh Kepolisian Republik Indonesia;
  - (2) daftar pendanaan Proliferasi Senjata Pemusnah Massal; dan
  - (3) data lainnya seperti identitas pemberi kerja dari Calon Nasabah, rekening telepon dan rekening listrik.

- 2) Penyelesaian proses verifikasi identitas Pemilik Manfaat (*Beneficial Owner*) dilakukan sebelum membuka hubungan usaha dengan calon Nasabah atau transaksi dengan Nasabah yang bertindak untuk dan atas nama kepentingan Pemilik Manfaat (*Beneficial Owner*).
- 3) Dalam kondisi tertentu, proses verifikasi dapat diselesaikan kemudian setelah dilakukannya hubungan usaha atau transaksi. Kondisi tertentu tersebut adalah apabila:
  - a) kelengkapan dokumen tidak dapat dipenuhi pada saat hubungan usaha atau transaksi akan dilakukan, misalnya karena dokumen masih dalam proses pengurusan. Untuk itu, Pemilik Manfaat (*Beneficial Owner*) dapat menyampaikan dokumen setelah melakukan hubungan usaha, dengan jangka waktu sebagaimana yang ditetapkan Penyelenggara yang diikuti dengan mitigasi risiko yang memadai, dan/atau
  - b) tingkat risiko Pemilik Manfaat (*Beneficial Owner*) perorangan tergolong rendah.
- 4) Verifikasi Pemilik Manfaat (*Beneficial Owner*) dapat dilaksanakan secara elektronik sepanjang Sistem Elektronik Penyelenggara mampu untuk memverifikasi kebenaran identitas resmi dari Pemilik Manfaat (*Beneficial Owner*).
- 5) Dalam hal Penyelenggara melakukan verifikasi Pemilik Manfaat (*Beneficial Owner*) secara elektronik, maka Penyelenggara harus memperhatikan ketentuan sebagaimana dimaksud dalam angka 9 huruf g.

13. CDD Sederhana (*Simplified CDD*)

- a. Dalam hal Penyelenggara menilai bahwa Calon Nasabah atau Nasabah berdasarkan hasil penilaian risiko terjadinya TPPU, TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal, profil risiko Calon Nasabah atau transaksi yang dilakukan oleh Nasabah tergolong rendah dan memenuhi kriteria Calon Nasabah atau Nasabah dengan profil dan karakteristik sederhana, Penyelenggara dapat menerapkan CDD sederhana (*simplified CDD*).

- b. Dalam hal Penyelenggara melaksanakan CDD sederhana (*simplified CDD*), Penyelenggara harus:
- 1) memastikan informasi dan dokumen pendukung CDD sederhana (*simplified CDD*) paling sedikit memuat identitas diri, sumber dana, dan tujuan transaksi;
  - 2) menetapkan kriteria Nasabah dengan profil dan karakteristik sederhana yang mendapat perlakuan CDD sederhana (*simplified CDD*) dan dilengkapi dengan alasan atau dasar penetapan yang jelas dan konsisten dengan penilaian risiko yang dilakukan oleh Penyelenggara, misalnya Nasabah berisiko tinggi atau PEP tidak dimasukkan sebagai Calon Nasabah atau Nasabah dengan perlakuan CDD sederhana (*simplified CDD*);
  - 3) memastikan persyaratan CDD sederhana mampu mengelola dan memitigasi tingkat ancaman TPPU, TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal;
  - 4) memastikan persyaratan CDD sederhana tidak mencakup Nasabah yang berdasarkan peraturan perundang-undangan dikategorikan sebagai Nasabah yang berisiko tinggi atau PEP;
  - 5) memberitahukan kepada Otoritas Jasa Keuangan rencana penerapan prosedur CDD sederhana termasuk kriteria Nasabah dengan profil dan karakteristik sederhana yang mendapat perlakuan CDD sederhana (*simplified CDD*) dan waktu dimulainya penerapan prosedur CDD sederhana. Contoh: Setelah melakukan analisis risiko Nasabahnya, Penyelenggara memutuskan akan menerapkan CDD sederhana pada kelompok Nasabah tertentu dengan melakukan perubahan atas kebijakan dan prosedur APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal yang dimiliki. Berdasarkan perubahan atas kebijakan dan prosedur APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, CDD sederhana akan diberlakukan sejak tanggal 30 Maret, maka Penyelenggara dapat menyampaikan pemberitahuan kepada Otoritas Jasa Keuangan rencana penerapan CDD sederhana tersebut pada tanggal 20 Maret;

- 6) mendokumentasikan Nasabah yang mendapat perlakuan CDD sederhana (*simplified* CDD) dalam daftar yang didalamnya juga memuat informasi mengenai alasan penetapan risiko Nasabah sehingga digolongkan sebagai Nasabah berisiko rendah dan mendapat perlakuan CDD sederhana (*simplified* CDD);
  - 7) meminta informasi kepada calon Nasabah dengan berpedoman kepada ketentuan yang berlaku; dan
  - 8) memastikan pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan.
- c. Nasabah yang telah mendapatkan perlakuan CDD sederhana (*simplified* CDD) harus dikeluarkan dari daftar Nasabah CDD sederhana (*simplified* CDD) apabila memenuhi kriteria:
- 1) diidentifikasi terkait dengan dugaan Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal;
  - 2) memiliki tingkat risiko yang meningkat; dan/atau
  - 3) tidak sesuai dengan tujuan awal pada saat registrasi sebagai pengguna.
- d. Penyelenggara dapat melakukan identifikasi dan verifikasi Calon Nasabah atau Nasabah dalam rangka CDD sederhana secara elektronik sepanjang Sistem Elektronik Penyelenggara mampu untuk mengidentifikasi identitas resmi dari Calon Nasabah atau Nasabah berisiko rendah dan memenuhi kriteria Calon Nasabah atau Nasabah dengan profil dan karakteristik sederhana tersebut serta mampu untuk memverifikasi kebenaran identitas resmi Calon Nasabah atau Nasabah dimaksud.
- e. Dalam hal Penyelenggara melakukan identifikasi dan verifikasi Calon Nasabah atau Nasabah dalam rangka CDD sederhana secara elektronik, maka pelaksanaannya harus memperhatikan ketentuan sebagaimana dimaksud dalam angka 8 huruf d sampai dengan huruf g, serta angka 9 huruf g.
14. CDD Pihak Ketiga
- a. Penyelenggara dapat menggunakan hasil CDD yang telah dilakukan oleh pihak ketiga terhadap Calon Nasabah yang telah menjadi Nasabah pada pihak ketiga tersebut.

- b. Mengingat salah satu persyaratan menggunakan layanan Penyelenggara adalah bahwa calon Pemberi Pinjaman dan Penerima Pinjaman wajib telah menjadi Nasabah Bank, Penyelenggara dapat menggunakan hasil CDD yang telah dilakukan oleh Bank terhadap Calon Nasabah yang telah menjadi Nasabah Bank tersebut.
- c. Dalam hal Penyelenggara menggunakan hasil CDD Pihak ketiga (termasuk hasil CDD Bank):
  - 1) tanggung jawab CDD tetap berada pada Penyelenggara tersebut;
  - 2) Penyelenggara harus memahami maksud dan tujuan hubungan usaha serta mengidentifikasi dan memverifikasi Nasabah dan Pemilik Manfaat (*Beneficial Owner*);
  - 3) Penyelenggara harus sesegera mungkin mendapatkan informasi yang diperlukan terkait dengan prosedur CDD;
  - 4) Penyelenggara harus memiliki kerja sama dengan pihak ketiga dalam bentuk kesepakatan tertulis, di mana dalam kesepakatan tertulis harus dipastikan terdapat klausula yang menegaskan bahwa Penyelenggara memiliki hak untuk memperoleh informasi, data, atau salinan dokumen pendukung Nasabah dari pihak ketiga yang CDD atas Nasabah tersebut telah dilakukan oleh pihak ketiga, sepanjang informasi, data, atau salinan dokumen pendukung Nasabah tersebut diperlukan semata-mata untuk kepentingan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dan bukan untuk kepentingan lainnya seperti pemasaran.

Contoh: kepentingan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal adalah pemenuhan permintaan informasi, data dan salinan dokumen pendukung Nasabah dari Otoritas Jasa Keuangan, PPATK atau aparat penegak hukum;
  - 5) Penyelenggara harus mengambil langkah yang memadai untuk memastikan bahwa pihak ketiga (termasuk Bank) bersedia memenuhi permintaan informasi dan salinan dokumen pendukung segera pada kesempatan pertama

apabila dibutuhkan oleh Penyelenggara dalam rangka penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;

- 6) Penyelenggara harus memastikan bahwa pihak ketiga merupakan lembaga keuangan dan/atau penyedia barang dan/atau jasa dan profesi tertentu yang memiliki prosedur CDD dan tunduk pada pengawasan dari otoritas berwenang sesuai dengan ketentuan yang berlaku.

Contoh:

Penyelenggara dapat menggunakan hasil CDD yang telah dilakukan oleh:

- a) penyedia jasa keuangan di sektor perbankan, pasar modal dan/atau industri keuangan nonbank, di mana penyedia jasa keuangan memiliki prosedur CDD yang telah ditetapkan otoritas berwenang yang mengawasinya yaitu Otoritas Jasa Keuangan; atau
  - b) perusahaan pialang berjangka komoditi di mana perusahaan pialang berjangka memiliki prosedur CDD yang telah ditetapkan otoritas berwenang yang mengawasinya yaitu Badan Pengawas Perdagangan Berjangka (BAPPEPTI);
- 7) Penyelenggara harus memperhatikan informasi terkait risiko negara tempat pihak ketiga tersebut berasal;
  - 8) Dalam hal Penyelenggara bermaksud menggunakan hasil CDD Pihak ketiga yang berkedudukan di negara berisiko tinggi (*high risk countries*), maka hal itu dapat dilakukan apabila:
    - a) pihak ketiga berada dalam konglomerasi keuangan (*financial group*) yang sama dengan Penyelenggara;
    - b) konglomerasi keuangan (*financial group*) tersebut telah menerapkan CDD, penatausahaan dokumen, dan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal secara efektif sesuai dengan Rekomendasi FATF;
    - c) terhadap negara berisiko tinggi telah dilakukan mitigasi risiko secara memadai oleh unit APU dan PPT serta pencegahan pendanaan Proliferasi Senjata

Pemusnah Massal berdasarkan kebijakan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal di tingkat konglomerasi keuangan (*financial group*); dan

d) konglomerasi keuangan (*financial group*) tersebut diawasi oleh otoritas yang berwenang.

9) Penyelenggara memastikan bahwa pihak ketiga berada dalam negara yang patuh terhadap standar FATF; dan

10) CDD pihak ketiga tidak berlaku untuk hubungan keagenan atau *outsourcing*. Hal ini dikarenakan pada hubungan keagenan atau *outsourcing* dalam melakukan CDD dilakukan untuk kepentingan Penyelenggara sesuai dengan prosedur Penyelenggara dan tunduk pada kendali Penyelenggara yang mendelegasikan atas penerapan prosedur tersebut.

15. Penolakan Hubungan Usaha atau Transaksi dan Penutupan/Pemutusan Hubungan Usaha

a. Penyelenggara dilarang membuka atau memelihara rekening anonim atau rekening yang menggunakan nama fiktif.

b. Penyelenggara harus menolak hubungan usaha atau transaksi atau menutup/memutuskan hubungan usaha dengan Calon Nasabah atau Nasabah dalam hal:

1) tidak bersedia memberikan informasi dan/atau melengkapi dokumen yang dipersyaratkan Penyelenggara;

2) Penyelenggara tidak dapat meyakini kebenaran identitas dan kelengkapan dokumen;

3) transaksi masuk (*incoming transfer*) pada rekening nasabah, namun setelah Penyelenggara menerima dan melakukan CDD ulang dan berdasarkan dari pengirim diketahui bahwa rekening Nasabah penerima merupakan rekening penampungan tindak pidana sebagaimana dimaksud dalam peraturan perundang-undangan mengenai pencegahan dan pemberantasan TPPU.

4) memberikan informasi dan/atau dokumen yang tidak sesuai atau patut diduga sebagai dokumen palsu atau informasi yang diragukan kebenarannya;

- 5) sumber dana transaksi yang dimiliki diketahui dan/atau patut diduga berasal dari hasil tindak pidana;
  - 6) tercatat dalam daftar terduga teroris dan organisasi teroris; dan/atau
  - 7) tercatat dalam daftar pendanaan Proliferasi Senjata Pemusnah Massal.
- c. Penyelenggara wajib memberitahukan secara tertulis kepada Nasabah mengenai penutupan hubungan usaha.
  - d. Pemberitahuan tertulis dapat dilakukan dengan penyampaian surat yang ditujukan kepada Nasabah sesuai dengan alamat yang tercantum dalam *database* Penyelenggara atau diumumkan melalui media cetak, media elektronik, maupun media lainnya.
  - e. Dalam hal Penyelenggara melakukan penolakan hubungan usaha dengan Calon Nasabah atau penolakan transaksi atau penutupan/pemutusan hubungan usaha dengan Nasabah, maka Penyelenggara wajib melaporkannya kepada PPATK mengenai tindakan penolakan hubungan usaha atau transaksi atau penutupan/pemutusan hubungan usaha tersebut sebagai transaksi keuangan mencurigakan.
  - f. Dalam hal pemberitahuan tertulis telah dilakukan dan Nasabah tidak mengambil sisa dana yang tersimpan di Penyelenggara, maka penyelesaian terhadap sisa dana Nasabah tersebut dilakukan sesuai peraturan perundang-undangan yang berlaku, antara lain dengan menyerahkan sisa dana ke Balai Harta Peninggalan.
  - g. Penyelenggara harus mendokumentasikan Calon Nasabah atau Nasabah yang terkena penolakan transaksi atau penutupan hubungan usaha sebagaimana dimaksud pada huruf b dalam daftar tersendiri.
16. Pengelolaan Risiko Berkelanjutan
- a. Penyelenggara harus memiliki kebijakan dan prosedur untuk mengelola risiko berkelanjutan terkait risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, di mana pengelolaan risiko tersebut tidak hanya dilakukan pada saat melakukan registrasi sebagai Pengguna pada saat Nasabah melakukan transaksi.

b. Kebijakan dan prosedur untuk mengelola risiko Pencucian Uang dan/atau Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal secara berkelanjutan mencakup:

1) Identifikasi risiko.

Dalam melakukan identifikasi risiko, Penyelenggara harus menilai risiko Pencucian Uang dan/atau Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang melekat pada usahanya dengan mempertimbangkan risiko yang disebabkan oleh Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, dan jaringan distribusi (*delivery channels*).

2) Pengendalian dan mitigasi risiko

Pengendalian dan mitigasi risiko yang dapat diterapkan meliputi:

a) mengidentifikasi dan memverifikasi Calon Nasabah dan memantau transaksi Nasabah;

b) meningkatkan frekuensi pengawasan dan melakukan peninjauan kembali atas hubungan usaha secara berkelanjutan;

c) meningkatkan CDD menjadi EDD yang dilakukan Penyelenggara terhadap peningkatan risiko Pencucian Uang dan/atau Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang ada pada Nasabah, sumber dana yang digunakan untuk membeli produk/jasa/transaksi, dan perilaku Nasabah dalam membeli produk dan jasa; dan

d) eskalasi atau persetujuan berjenjang untuk pembukaan hubungan usaha atau transaksi melalui persetujuan pejabat senior.

17. Pemeliharaan data yang akurat terkait Nasabah dan transaksi Nasabah

a. Pemeliharaan data yang akurat terkait Nasabah dan transaksi Nasabah tidak hanya berguna bagi Penyelenggara dalam *risk management* dan pengembangan usaha, tetapi juga diperlukan sebagai upaya untuk membantu pihak yang berwenang dalam melakukan pengawasan kepatuhan, pemeriksaan dugaan TPPU dan/atau TPPT serta pendanaan Proliferasi Senjata Pemusnah

Massal, serta penyelidikan dan penyidikan terhadap dana yang diindikasikan berasal dari kejahatan, sehingga dokumen yang disimpan oleh Penyelenggara harus memadai untuk dapat digunakan sebagai alat bukti (jika diperlukan) oleh aparat penegak hukum.

- b. Penyelenggara harus menatausahakan atau mendokumentasikan data Nasabah termasuk didalamnya data yang diperoleh dari proses identifikasi dan verifikasi Calon Nasabah atau pemantauan transaksi Nasabah termasuk yang berisiko tinggi atau PEP dalam rangka EDD, Pemilik Manfaat (*Beneficial Owner*), atau yang tergolong berisiko rendah dan memenuhi kriteria Calon Nasabah atau Nasabah dengan profil dan karakteristik sederhana dalam rangka CDD Sederhana.
- c. Penyelenggara harus memiliki kebijakan dan prosedur jangka waktu penatausahaan dokumen yang mencakup:
  - 1) dokumen yang terkait dengan data Nasabah ditatausahakan dengan jangka waktu paling sedikit 5 (lima) tahun sejak:
    - a) berakhirnya hubungan usaha dengan Nasabah; dan/atau
    - b) ditemukannya ketidaksesuaian transaksi dengan tujuan ekonomis dan/atau tujuan usaha;
  - 2) dokumen terkait transaksi keuangan Nasabah dengan jangka waktu sebagaimana diatur dalam peraturan perundang-undangan; dan
  - 3) dokumen yang ditatausahakan paling sedikit mencakup:
    - a) identitas Nasabah beserta dokumen pendukungnya;
    - b) informasi transaksi yang dilakukan;
    - c) hasil analisis yang telah dilakukan;
    - d) korespondensi dengan Nasabah; dan
    - e) dokumen lain yang terkait dengan pelaporan transaksi keuangan mencurigakan.
- d. Dokumen sebagaimana disebutkan dalam huruf b dan huruf c dapat disimpan melalui format data atau dokumen elektronik dalam *database* Penyelenggara dengan tetap memperhatikan sistem pengamanan data atau dokumen elektronik.

- e. Dalam hal dokumen sebagaimana disebutkan dalam huruf b dan huruf c disimpan melalui format data atau dokumen elektronik dalam *database* Penyelenggara, Penyelenggara harus memastikan mampu menampilkan kembali data atau dokumen elektronik secara utuh sesuai dengan peraturan perundang-undangan, apabila diminta oleh Otoritas Jasa Keuangan dan/atau otoritas lain yang berwenang seperti PPAK dan/atau aparat penegak hukum.

#### 18. Pengkinian Data Nasabah

- a. Penyelenggara harus melakukan pengkinian data Nasabah secara berkesinambungan dan memastikan bahwa data, informasi, dokumen yang dikumpulkan melalui proses CDD dan/atau EDD merupakan data terkini yang dimaksudkan untuk mengidentifikasi kesesuaian antara transaksi Nasabah dengan profil Nasabah.
- b. Kewajiban pengkinian data Nasabah oleh Penyelenggara sebagaimana dimaksud dalam huruf a, mencakup:
  - 1) data, informasi, dan/atau dokumen pendukung Nasabah;
  - 2) daftar terduga teroris dan organisasi teroris; dan
  - 3) daftar pendanaan Proliferasi Senjata Pemusnah Massal.
- c. Kegiatan pengkinian data, informasi, dan/atau dokumen pendukung Nasabah didasarkan pada tingkat risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal dari Nasabah tersebut dan difokuskan pada Nasabah berisiko lebih tinggi terlebih dahulu.
- d. Tingkat risiko Nasabah diperoleh dari hasil penilaian risiko Nasabah yang dituangkan dalam penggolongan Nasabah berdasarkan tingkat risiko, yang dapat terbagi menjadi:
  - 1) Nasabah berisiko tinggi, yang harus dikinikan paling sedikit 1 (satu) tahun sekali;
  - 2) Nasabah berisiko sedang, yang harus dikinikan paling sedikit 2 (dua) tahun sekali; dan
  - 3) Nasabah berisiko rendah, yang harus dikinikan paling sedikit 3 (tiga) tahun sekali.
- e. Dalam melakukan pengkinian data, informasi, dan/atau dokumen pendukung Nasabah (pengkinian data Nasabah), Penyelenggara harus mendokumentasikan upaya pengkinian

Nasabah dalam bentuk kertas kerja yang didalamnya memuat nama Nasabah, tanggal pengkinian Nasabah, cara pengkinian Nasabah (misalnya melalui email, telepon, surat, berita di media massa dan elektronik termasuk internet atau sumber lain yang dapat dipercaya), hasil pengkinian data Nasabah dan tindak lanjut hasil pengkinian khususnya terhadap data Nasabah yang tidak berhasil dikinikan.

- f. Dalam hal sumber daya yang dimiliki Penyelenggara terbatas, kegiatan pengkinian Nasabah dilakukan dengan skala prioritas, antara lain didasarkan pada:
- 1) tingkat risiko Nasabah tergolong Nasabah berisiko tinggi;
  - 2) transaksi dengan jumlah yang signifikan dan/atau menyimpang dari profil transaksi atau profil Nasabah;
  - 3) terdapat perubahan saldo yang nilainya signifikan; dan
  - 4) informasi yang ada pada CIF tidak sesuai dengan profil Nasabah.
- g. Kriteria Nasabah berisiko tinggi dapat dilihat dari:
- 1) latar belakang atau profil Nasabah berisiko tinggi (*high risk customers*);
  - 2) produk sektor jasa keuangan yang berisiko tinggi untuk digunakan sebagai sarana Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal;
  - 3) transaksi dengan pihak yang berasal dari high risk countries atau nasabah memiliki hubungan yang signifikan dengan high risk countries;
  - 4) transaksi tidak sesuai dengan profil;
  - 5) termasuk dalam kategori PEP;
  - 6) bidang usaha termasuk high risk business;
  - 7) negara atau teritori asal, domisili, atau dilakukannya transaksi termasuk high risk countries;
  - 8) tercantum dalam daftar terduga teroris dan organisasi teroris; dan/atau
  - 9) transaksi yang dilakukan diduga terkait dengan hasil tindak pidana kejahatan dan/atau terkait dengan Pendanaan Terorisme.

- h. Pelaksanaan pengkinian data Nasabah yang tercantum dalam laporan rencana pengkinian data dapat dilakukan antara lain pada saat:
  - 1) penggantian dokumen data dan identitas Nasabah; atau
  - 2) penutupan hubungan usaha.
- i. Penyelenggara harus memastikan bahwa dokumen, data atau informasi yang dihimpun dalam proses CDD selalu diperbaharui dan relevan dengan melakukan pemeriksaan kembali terhadap data yang ada, khususnya yang terkait dengan Nasabah berisiko tinggi atau PEP.
- j. Berkaitan dengan pengkinian daftar terduga teroris dan organisasi teroris dan daftar pendanaan Proliferasi Senjata Pemusnah Massal, Penyelenggara harus:
  - 1) memelihara daftar terduga teroris dan organisasi teroris dan daftar pendanaan Proliferasi Senjata Pemusnah Massal;
  - 2) mencocokkan kesesuaian nama dan informasi Nasabah yang ada di Penyelenggara dengan nama dan informasi yang ada di dalam daftar terduga teroris dan organisasi teroris dan daftar pendanaan Proliferasi Senjata Pemusnah Massal yang disampaikan oleh Otoritas Jasa keuangan; dan
  - 3) mencocokkan kesesuaian nama dan informasi Calon Nasabah yang akan menjadi Nasabah Penyelenggara dengan nama dan informasi yang ada di dalam daftar terduga teroris dan organisasi teroris dan daftar pendanaan Proliferasi Senjata Pemusnah Massal yang telah diterima oleh Penyelenggara.
- k. Penyelenggara dapat melakukan pengkinian data Nasabah secara elektronik. Dalam hal Penyelenggara melakukan proses pengkinian data secara elektronik maka:
  - 1) Penyelenggara harus tetap memperhatikan hal-hal sebagaimana dimaksud dalam huruf a sampai dengan huruf h, dan huruf j.
  - 2) proses pengkinian data Nasabah dilakukan berdasarkan hasil penilaian risiko secara berkala melalui metode sebagai berikut:
    - a) menyampaikan notifikasi melalui email agar Nasabah mengkinikan data dan informasinya;

- b) dalam hal sesuai hasil penilaian risiko terdapat Nasabah yang telah mencapai waktu untuk dikinikan datanya, Penyelenggara memunculkan notifikasi dalam aplikasi agar Nasabah mengkinikan data dan informasinya;
  - c) dalam hal sesuai hasil penilaian risiko terdapat Nasabah yang telah mencapai waktu untuk dikinikan datanya, sebelum Nasabah melakukan transaksi maka Penyelenggara memunculkan fitur khusus yang bersifat *pop-up* untuk digunakan oleh Nasabah mengkinikan data dan informasinya, di mana transaksi dapat dilanjutkan setelah proses pengkinian data telah dilakukan oleh Nasabah; dan/atau
  - d) dalam hal sesuai hasil penilaian risiko terdapat Nasabah yang telah mencapai waktu untuk dikinikan datanya, Penyelenggara memunculkan fitur khusus yang bersifat *pop-up* untuk digunakan oleh Nasabah mengkinikan data pada saat Nasabah membuka aplikasi Penyelenggara di mana aplikasi akan terbuka setelah pengkinian data telah dilakukan oleh Nasabah.
- l. Penyelenggara harus menatausahakan dan mendokumentasikan proses pengkinian data Nasabah.
  - m. Penatausahaan dan pendokumentasian pengkinian data Nasabah dapat dilakukan secara manual dalam bentuk tertulis melalui dokumen formal seperti memo, nota, atau catatan yang juga dapat disimpan melalui format data atau dokumen elektronik dalam *database* Penyelenggara.
19. Pemantauan Nasabah dan Transaksi Nasabah
- a. Penyelenggara harus melakukan kegiatan pemantauan yang paling sedikit mencakup:
    - 1) informasi dan dokumen Nasabah;
    - 2) transaksi Nasabah;
    - 3) hubungan usaha/transaksi dengan Nasabah berisiko tinggi atau PEP;
    - 4) daftar terduga teroris dan organisasi teroris; dan
    - 5) daftar pendanaan Proliferasi Senjata Pemusnah Massal.

b. Pemantauan yang dilakukan oleh Penyelenggara sebagaimana dimaksud dalam huruf a, harus memperhatikan hal-hal sebagai berikut:

- 1) pemantauan dilakukan secara berkesinambungan untuk mengidentifikasi kesesuaian antara transaksi Nasabah dengan profil risiko Nasabah;
- 2) pemantauan mencakup analisis terhadap seluruh transaksi yang tidak sesuai dengan profil risiko Nasabah; dan
- 3) apabila diperlukan, Penyelenggara dapat meminta informasi tentang latar belakang dan tujuan transaksi terhadap transaksi yang tidak sesuai dengan profil Nasabah dengan memperhatikan ketentuan *anti-tipping off*.

Ketentuan *anti-tipping off* adalah ketentuan yang melarang Penyelenggara memberitahukan kepada Nasabah atau pihak lain manapun, baik secara langsung maupun tidak langsung, dengan cara apapun mengenai laporan TKM yang sedang disusun atau telah disampaikan kepada PPATK.

c. Kegiatan pemantauan profil dan transaksi Nasabah dilakukan secara berkesinambungan meliputi kegiatan:

- 1) memastikan kelengkapan informasi dan dokumen Nasabah;
- 2) meneliti kesesuaian antara profil transaksi dengan profil Nasabah; dan
- 3) meneliti kemiripan atau kesamaan nama dan informasi dengan nama dan informasi yang tercantum dalam:
  - a) daftar terduga teroris dan organisasi teroris;
  - b) daftar pendanaan Proliferasi Senjata Pemusnah Massal; dan
  - c) dokumen atau informasi yang memuat nama tersangka atau terdakwa yang dipublikasikan dalam media massa atau oleh otoritas yang berwenang.

d. Sumber informasi yang dapat digunakan untuk memantau Nasabah yang ditetapkan sebagai tersangka atau terdakwa dapat diperoleh antara lain melalui:

- 1) data yang dikeluarkan oleh pihak berwenang seperti PPATK;

- 2) data publik yang dikeluarkan oleh Kementerian/Lembaga yang menyelenggarakan urusan pemerintahan di bidang terkait; atau
  - 3) data publik yang tercantum dalam media massa seperti koran, majalah, televisi, dan internet.
- e. Penyelenggara harus melakukan klasifikasi transaksi dan Nasabah yang membutuhkan pemantauan khusus. Pemantauan terhadap transaksi Nasabah harus lebih ketat apabila terdapat Nasabah berisiko tinggi.
- f. Dalam hal Penyelenggara melakukan pemantauan profil dan transaksi Nasabah secara elektronik, Penyelenggara harus memastikan bahwa Sistem Elektronik yang digunakan dapat:
- 1) mengidentifikasi, menganalisis, memantau, dan menyediakan laporan secara efektif mengenai profil, karakteristik dan/atau kebiasaan pola transaksi yang dilakukan oleh Nasabah; dan
  - 2) menelusuri setiap transaksi, apabila diperlukan, termasuk antara lain penelusuran atas identitas Nasabah, bentuk transaksi, tanggal transaksi, jumlah, dan denominasi transaksi, serta sumber dana transaksi.
- g. Penyelenggara dapat melakukan pemantauan profil dan transaksi secara elektronik dengan menggunakan *regulatory technology* antara lain dengan memanfaatkan algoritma, parameter tertentu, *artificial intelligence*, dan *machine learning*.
- h. Penyelenggara harus menatausahakan dan mendokumentasikan proses pemantauan profil dan transaksi Nasabah.
- i. Penatausahaan dan pendokumentasian pemantauan profil dan transaksi Nasabah dapat dilakukan secara manual dalam bentuk tertulis melalui dokumen formal seperti memo, nota, atau catatan maupun melalui format data atau dokumen elektronik dalam *database* Penyelenggara.

## 20. Rekam Jejak Audit

- a. Penyelenggara wajib memiliki rekam jejak audit atas seluruh kegiatannya.
- b. Rekam jejak audit digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya.

- c. Pelaksanaan rekam jejak audit paling sedikit mencakup:
    - 1) memelihara log transaksi sesuai kebijakan retensi data Penyelenggara, sesuai peraturan perundang-undangan;
    - 2) memberikan notifikasi kepada Nasabah apabila suatu transaksi telah berhasil dilakukan;
    - 3) memastikan tersedianya fungsi jejak audit untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan yang harus dianalisis atau dievaluasi secara berkala; dan
    - 4) dalam hal sistem pemrosesan dan jejak audit dilakukan oleh pihak ketiga, maka proses jejak audit tersebut harus sesuai dengan standar yang ditetapkan oleh Penyelenggara.
  - d. Proses rekam jejak audit dapat dilakukan secara elektronik antara lain dengan:
    - 1) log atau rekaman elektronik transaksi dalam *database* Penyelenggara;
    - 2) notifikasi melalui *e-mail*, *short message service* (SMS), laman, atau aplikasi Penyelenggara kepada Nasabah apabila suatu transaksi telah berhasil dilakukan; dan
    - 3) sistem peringatan dini (*early warning system*) untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan.
21. Pelaporan kepada Pejabat Senior, Direksi, dan Dewan Komisaris
- a. Pejabat senior, Direksi dan/atau Dewan Komisaris harus dilibatkan secara berjenjang dalam persetujuan dan pengawasan terhadap kondisi khusus yang mencakup:
    - 1) adanya Calon Nasabah yang berisiko tinggi atau PEP yang ingin melakukan hubungan usaha dengan Penyelenggara;
    - 2) adanya Calon Nasabah yang berasal dari negara berisiko tinggi; dan/atau
    - 3) adanya transaksi yang dilakukan oleh Nasabah berisiko tinggi atau PEP.
  - b. Pelaporan atas perkembangan persetujuan dan pengawasan terhadap kondisi khusus tersebut dilaporkan secara berjenjang dari pejabat senior, Direksi, dan Dewan Komisaris.
  - c. Kebijakan dan prosedur pelaporan kepada pejabat senior, Direksi, dan Dewan Komisaris mencakup:
    - 1) dalam hal proses CDD menunjukkan adanya Calon Nasabah atau Nasabah yang dikategorikan berisiko tinggi

atau PEP maka pegawai Penyelenggara yang melaksanakan CDD melapor kepada pejabat senior. Pejabat senior bertanggung jawab terhadap penerimaan dan/atau penolakan hubungan usaha dengan Calon Nasabah atau Nasabah yang berisiko tinggi;

- 2) dalam hal pejabat senior menyetujui hubungan usaha dengan Nasabah berisiko tinggi atau PEP maka pejabat senior bertanggung jawab dalam memantau transaksi Nasabah berisiko tinggi atau PEP;
- 3) pejabat senior harus melaporkan kepada Direksi yang membawahi fungsi penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal terkait jumlah Calon Nasabah atau Nasabah yang berisiko tinggi atau PEP termasuk jumlah Nasabah berisiko tinggi atau PEP yang ditolak, diterima atau dilakukan penutupan hubungan usaha.
- 4) Direksi harus memberikan arahan atas laporan yang disampaikan pejabat senior dan menetapkan langkah-langkah mitigasi risiko.
- 5) Direksi melaporkan kepada Dewan Komisaris terkait hasil pemantauan atas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal secara keseluruhan sebagaimana kebijakan dan prosedur tertulis yang telah ditetapkan Penyelenggara.
- 6) Direksi dapat mengusulkan pengkinian kebijakan dan prosedur dalam hal terdapat perkembangan risiko yang perlu dimitigasi oleh Penyelenggara, yang belum tercantum dalam kebijakan dan prosedur tertulis.

## 22. Kebijakan dan Prosedur Pelaporan kepada PPATK

- a. Penyelenggara harus menyampaikan kewajiban pelaporan kepada PPATK sesuai dengan ketentuan dan tata cara pelaporan sebagaimana dimaksud dalam peraturan perundang-undangan yang mengatur mengenai pencegahan dan pemberantasan TPPU dan TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal, termasuk peraturan pelaksanaannya antara lain Peraturan Kepala PPATK.

Berkaitan dengan TKM sebagai salah satu transaksi keuangan yang wajib dilaporkan oleh Penyelenggara, Penyelenggara dapat melihat contoh-contoh transaksi keuangan sebagaimana dimaksud pada Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

- b. Penyelenggara harus menyampaikan laporan lain terkait penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dalam hal terdapat permintaan informasi dari PPATK.

## V. PENGENDALIAN INTERN

### A. PENGENDALIAN INTERN

1. Penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berbasis risiko (*risk based approach*) yang efektif harus diimplementasikan dalam pengendalian intern dan diinternalisasikan dalam proses bisnis Penyelenggara.
2. Penyelenggara harus memiliki sistem pengendalian intern untuk memastikan kepatuhan Penyelenggara dalam menerapkan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal secara efektif dan untuk meminimalkan risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang dihadapi Penyelenggara.
3. Dalam pengendalian intern, Penyelenggara harus memperhatikan hal-hal sebagai berikut:
  - a. skala dan kompleksitas Penyelenggara;
  - b. keragaman kegiatan usaha atau operasional Penyelenggara, termasuk keragaman negara/area geografis/yurisdiksi, profil Nasabah, produk atau jasa, dan aktivitas transaksi Penyelenggara secara keseluruhan;
  - c. jaringan distribusi (*delivery channels*) yang digunakan;
  - d. volume dan skala transaksi;
  - e. tingkat penilaian risiko atas setiap kegiatan usaha Penyelenggara; dan/atau
  - f. hubungan usaha antara Penyelenggara dengan Nasabah baik secara langsung atau melalui agen, pihak ketiga, koresponden, atau komunikasi tanpa pertemuan langsung

*(non-face to face).*

4. Penyelenggara harus memiliki kerangka pengendalian intern yang efektif dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berbasis risiko, yang meliputi paling sedikit:
  - a. kebijakan, prosedur, dan pemantauan internal yang memadai, yang mampu secara tepat waktu mendeteksi kelemahan dan penyimpangan yang terjadi dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - b. batasan wewenang dan tanggung jawab satuan kerja terkait dengan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, di mana Penyelenggara harus memastikan adanya pemisahan tugas, wewenang dan tanggung jawab yang jelas antara unit khusus pengendalian, fungsi atau pejabat yang ditunjuk untuk melaksanakan fungsi pengendalian intern dengan unit bisnis Penyelenggara;
  - c. penunjukan UKK dan/atau pejabat yang bertanggung jawab dalam mengelola penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - d. pengkinian standar kepatuhan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - e. kebijakan, prosedur, dan pemantauan terkait penyaringan/rekrutmen karyawan Penyelenggara, untuk memastikan tidak digunakannya karyawan Penyelenggara sebagai sarana TPPU dan/atau TPPT serta pendanaan Proliferasi Senjata Pemusnah Massal melalui proses bisnis Penyelenggara;
  - f. pemantauan terhadap Nasabah, transaksi Nasabah, dan/atau penggunaan Teknologi Informasi dalam proses bisnis Penyelenggara khususnya yang memiliki risiko tinggi terkait risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal termasuk pemantauan terhadap hal tertentu yang

perlu mendapat perhatian khusus yang didasarkan antara lain pada saran dan informasi dari asosiasi industri, regulator, atau aparat penegak hukum;

- g. penyediaan sistem yang dapat melakukan identifikasi, pemantauan, dan pelaporan transaksi keuangan mencurigakan secara akurat;
- h. penyediaan tinjauan rutin atas penilaian risiko dan manajemen proses;
- i. pengawasan yang memadai sebelum penawaran produk atau jasa baru atau penggunaan teknologi baru atau penawaran produk atau jasa yang dimodifikasi sedemikian rupa yang berpotensi terhadap peningkatan risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal;
- j. penyampaian informasi secara cepat dan tepat dalam hal terdapat indikasi dan/atau dugaan terkait risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, langkah perbaikan yang dilakukan, hasil identifikasi kelemahan atas peraturan yang dimiliki, rencana tindak untuk perbaikan, dan pelaporan yang telah disampaikan kepada pihak berwenang;
- k. kepatuhan terhadap ketentuan peraturan perundangan-undangan, persyaratan pelaporan serta rekomendasi terkait kepatuhan atas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dan melakukan pengkinian atas perubahan ketentuan peraturan perundangan-undangan;
- l. penerapan kebijakan, prosedur, dan kontrol atas uji tuntas Nasabah (CDD) dan uji tuntas lanjut (EDD);
- m. pengawasan yang memadai terkait Nasabah, transaksi dan produk yang berisiko tinggi, seperti batasan transaksi atau persetujuan manajemen;
- n. pengawasan yang memadai terhadap pegawai Penyelenggara yang melengkapi laporan, menerima hibah, memantau aktivitas yang mencurigakan, atau terlibat dalam kegiatan lain yang merupakan bagian dari

- penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
- o. pengintegrasian kepatuhan terhadap penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dalam deskripsi pekerjaan dan evaluasi kinerja yang tepat;
  - p. pelatihan terkait penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal yang tepat dan relevan untuk semua pegawai;
  - q. pengujian terhadap keefektifan dari pelaksanaan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dengan mengambil contoh secara acak (*random sampling*) dan melakukan pendokumentasian atas pengujian yang dilakukan; dan
  - r. audit independen secara internal untuk menguji kepatuhan dan efektivitas penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, yang pelaksanaannya sesuai dengan kebutuhan dan kompleksitas usaha Penyelenggara.
5. Dalam melakukan pengendalian intern, Penyelenggara dapat menggunakan *regulatory technology* seperti algoritma, pemanfaatan teknologi *artificial intelligence*, atau *machine learning*.
6. Dalam hal Penyelenggara melakukan pengendalian intern dengan menggunakan *regulatory technology* sebagaimana dimaksud pada angka 5, Penyelenggara harus memastikan *regulatory technology* yang digunakan dalam sistem pengendalian intern:
- a. didasarkan pada hasil penilaian risiko yang didalamnya memuat bagaimana Penyelenggara mengelola dan memitigasi risiko atas Teknologi Informasi yang digunakan;
  - b. terjamin keandalannya dan telah tersertifikasi oleh Kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika; dan
  - c. menggunakan pengamanan, termasuk penggunaan *security tools* seperti teknologi enkripsi, penggunaan *anti virus*, dan *firewall*.

7. Penanggung jawab pengendalian intern terkait penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berbasis risiko sebagaimana dimaksud pada angka 5 memiliki kewenangan paling sedikit mencakup:
  - a. menyusun program dan prosedur audit berbasis risiko dengan prioritas audit pada unit kerja atau kantor cabang yang tergolong memiliki kompleksitas usaha yang tinggi;
  - b. melakukan penilaian atas kecukupan proses yang berlaku di Penyelenggara dalam mengidentifikasi dan melaporkan transaksi keuangan yang mencurigakan dengan memperhatikan ketentuan *anti-tipping off*;
  - c. membantu Direksi dan Dewan Komisaris Penyelenggara dalam melakukan pengawasan dengan cara menjabarkan secara operasional baik perencanaan, pelaksanaan, maupun pemantauan hasil audit;
  - d. membuat analisis dan penilaian di bidang keuangan, akuntansi, operasional, dan kegiatan lain melalui audit;
  - e. mengidentifikasi segala kemungkinan untuk memperbaiki dan meningkatkan efisiensi penggunaan sumber daya dan sumber dana; dan
  - f. memberikan saran perbaikan dan informasi yang objektif tentang kegiatan yang diperiksa pada semua tingkatan manajemen Penyelenggara.
8. Penanggung jawab pengendalian intern harus:
  - a. memastikan pengendalian intern dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal diterapkan dengan baik, tepat dan efektif sesuai dengan kebijakan dan prosedur yang telah ditetapkan serta mencakup kerangka pengendalian intern sebagaimana dimaksud pada angka 4;
  - b. menciptakan budaya manajemen risiko dan kepatuhan; dan
  - c. memastikan bahwa pegawai taat terhadap kebijakan dan prosedur yang telah ditetapkan.
9. Penyelenggara dapat memiliki sistem pelaporan dugaan terjadinya pelanggaran (*whistleblowing system/WBS*) yang dimaksudkan untuk menjaga integritas profesionalitas, dan akuntabilitas Penyelenggara, di mana sistem tersebut

memungkinkan pihak internal perusahaan (karyawan) ataupun eksternal seperti Calon Nasabah, Nasabah, atau masyarakat umum, melaporkan dugaan pelanggaran etik, perilaku, prosedur kerja, dan/atau peraturan perundang-undangan yang dilakukan oleh sumber daya manusia (termasuk Direktur dan Dewan Komisaris) Penyelenggara.

10. Sistem pelaporan dugaan terjadinya pelanggaran (WBS) paling sedikit mencakup:
  - a. sistem pelaporan yang independen, bebas, dan rahasia;
  - b. perlindungan kerahasiaan identitas pelapor;
  - c. perlindungan terhadap pelapor dari tekanan, pemecatan, gugatan hukum hingga tindakan fisik. Perlindungan tidak hanya untuk pelapor tetapi juga dapat diperluas hingga ke anggota keluarga pelapor; dan
  - d. informasi pelaksanaan tindak lanjut berupa kapan dan bagaimana serta kepada institusi mana tindak lanjut diserahkan.
11. Unit kerja independen yang mengelola sistem pelaporan dugaan terjadinya pelanggaran (WBS) dapat dirangkap oleh pejabat yang ditunjuk sebagai penanggung jawab pengendalian intern.

**B. PENGENDALIAN INTERN ATAS PENGGUNAAN TEKNOLOGI INFORMASI DALAM PROSES BISNIS PENYELENGGARA**

1. Penyelenggara harus memastikan bahwa pengendalian intern atas penggunaan Teknologi Informasi dalam proses bisnis Penyelenggara cukup memadai dan efektif dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, dan mampu mengantisipasi kemungkinan Teknologi Informasi yang digunakan Penyelenggara tidak dimanfaatkan sebagai sarana TPPU, TPPT, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal
2. Dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, Penyelenggara harus memiliki dan menerapkan sistem pengendalian intern secara efektif terhadap seluruh aspek penggunaan Teknologi Informasi yang digunakan dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, yang meliputi paling sedikit:

- a. memiliki dan menerapkan kebijakan, standar, dan prosedur penggunaan Teknologi Informasi yang digunakan dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal secara konsisten dan berkesinambungan yang dimaksudkan untuk mengurangi risiko terjadinya kesalahan atau kegagalan sistem informasi yang digunakan, paling sedikit meliputi aspek:
  - 1) manajemen;
  - 2) pengembangan dan pengadaan;
  - 3) operasional Teknologi Informasi;
  - 4) pemeliharaan sistem informasi yang digunakan secara berkala;
  - 5) jaringan komunikasi;
  - 6) pengamanan informasi;
  - 7) rencana pemulihan bencana; dan
  - 8) penggunaan pihak penyedia jasa Teknologi Informasi.
- b. pengkajian ulang dan pengkinian kebijakan, standar dan prosedur sebagaimana dimaksud dalam huruf a secara berkala, sesuai dengan kebutuhan dan kompleksitas usaha Penyelenggara;
- c. pengendalian menyeluruh (*general control*) atas aktivitas Teknologi Informasi yang meliputi:
  - 1) pengendalian organisasi dan manajemen;
  - 2) pengendalian terhadap pengembangan dan pemeliharaan sistem aplikasi;
  - 3) pengendalian terhadap sistem operasi;
  - 4) pengendalian terhadap sistem perangkat lunak; dan
  - 5) pengendalian terhadap sistem *entry* data dan program.
- d. pengendalian atas aplikasi (*application control*), yang digunakan untuk memberikan keyakinan memadai bahwa semua transaksi telah diotorisasi dan dicatat, serta diolah seluruhnya, dengan cermat dan tepat waktu yang meliputi:
  - 1) pengendalian atas masukan (*input*), yang dimaksudkan untuk memastikan keabsahan, validitas, dan keakurasian dokumen dan dokumen pendukung sebelum diinput ke dalam sistem;

- 2) pengendalian atas pengolahan dan *file* data komputer; dan
  - 3) pengendalian atas keluaran (*output*), yang dimaksudkan untuk memastikan agar *output* sistem dapat diverifikasi dengan baik.
- e. pengawasan oleh manajemen dan adanya budaya pengendalian;
  - f. identifikasi dan penilaian risiko;
  - g. pemisahan fungsi; dan
  - h. kegiatan pemantauan dan koreksi penyimpangan, yang dilakukan oleh satuan kerja operasional, satuan kerja audit intern maupun pihak lain.
3. Sistem pengendalian intern secara efektif terhadap seluruh aspek penggunaan Teknologi Informasi sebagaimana dimaksud pada angka 2 merupakan bagian dari sistem pengendalian intern Penyelenggara.
  4. Penyelenggara harus memastikan kelangsungan dan kestabilan operasional Teknologi Informasi serta memitigasi risiko yang berpotensi dapat mengganggu kegiatan operasional Penyelenggara.
  5. Penyelenggara harus memastikan pengamanan informasi dilaksanakan secara efektif dengan memperhatikan paling sedikit:
    - a. pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*) secara efektif dan efisien dengan memperhatikan kepatuhan terhadap ketentuan; dan
    - b. pengamanan informasi yang dilakukan terhadap aspek teknologi, sumber daya manusia, dan proses dalam penggunaan Teknologi Informasi.
  6. Dalam hal Penyelenggara menggunakan pihak penyedia jasa Teknologi Informasi yang digunakan dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal, Penyelenggara harus memastikan pihak penyedia jasa Teknologi Informasi tersebut telah menerapkan manajemen risiko penggunaan Teknologi Informasi. Sebagai

contoh pihak penyedia jasa telah memiliki sertifikasi dari lembaga resmi.

7. Dalam hal Penyelenggara menggunakan jasa penyedia Teknologi Informasi, maka Penyelenggara harus melakukan tindakan tertentu sebagai bentuk mitigasi risiko dalam hal terdapat kondisi berupa:
  - a. memburuknya kinerja penyelenggaraan Teknologi Informasi oleh penyedia jasa Teknologi Informasi yang dapat berdampak signifikan pada kegiatan usaha Penyelenggara;
  - b. pihak penyedia jasa Teknologi Informasi menjadi insolven, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan;
  - c. terdapat pelanggaran oleh pihak penyedia jasa Teknologi Informasi terhadap ketentuan rahasia Penyelenggara dan kewajiban merahasiakan data pribadi Nasabah; dan/atau
  - d. terdapat kondisi yang menyebabkan Penyelenggara tidak dapat menyediakan data yang diperlukan dalam rangka pengawasan oleh Otoritas Jasa Keuangan.

## VI. SISTEM INFORMASI MANAJEMEN

1. Sistem informasi manajemen ditujukan untuk mengidentifikasi, menganalisis, memantau, dan menyediakan laporan secara efektif mengenai karakteristik transaksi yang dilakukan Nasabah dengan menggunakan parameter yang disesuaikan secara berkala dan memerhatikan kompleksitas usaha, volume transaksi, dan risiko yang dimiliki Penyelenggara, termasuk antara lain:
  - a. transaksi keuangan yang menyimpang dari profil, karakteristik, atau kebiasaan pola transaksi dari Nasabah yang bersangkutan;
  - b. transaksi keuangan oleh Nasabah yang patut diduga dilakukan dengan tujuan untuk menghindari pelaporan transaksi yang bersangkutan yang wajib dilakukan oleh pihak pelapor sesuai dengan peraturan perundang-undangan;
  - c. transaksi keuangan yang dilakukan atau batal dilakukan dengan menggunakan harta kekayaan yang diduga berasal dari hasil tindak pidana;
  - d. transaksi keuangan yang diminta oleh PPATK untuk dilaporkan oleh pihak pelapor karena melibatkan harta kekayaan yang

- diduga berasal dari hasil tindak pidana;
- e. transaksi Nasabah yang tidak memenuhi ketentuan CDD; dan
  - f. transaksi Nasabah yang kebenaran informasinya diragukan oleh Penyelenggara.
2. Penyelenggara harus memastikan Teknologi Informasi yang digunakan dalam sistem informasi manajemen terjamin keandalannya, dan telah didasarkan pada hasil penilaian risiko yang didalamnya memuat bagaimana Penyelenggara mengelola dan memitigasi risiko atas Teknologi Informasi yang digunakan.
  3. Kebijakan dan prosedur tertulis yang dimiliki Penyelenggara wajib mempertimbangkan faktor Teknologi Informasi yang berpotensi disalahgunakan oleh pelaku Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, misalnya pembukaan rekening melalui *internet*, atau perintah transfer dana melalui faksimili atau telepon, dan transaksi elektronik lainnya.
  4. Penyelenggara harus memiliki sistem informasi manajemen yang memungkinkan untuk menelusuri setiap transaksi (*individual transaction*) dan menanggapi secara penuh, cepat dan tepat permintaan informasi, data dan dokumen baik untuk keperluan internal dan/atau Otoritas Jasa Keuangan, maupun dalam kaitannya dengan upaya penegakan hukum dan kepentingan peradilan.
  5. Penyelenggara harus memelihara pangkalan data (*database*) PEP, daftar terduga teroris dan organisasi teroris, dan daftar Proliferasi Senjata Pemusnah Massal.
  6. Untuk memudahkan pemantauan dalam rangka menganalisis transaksi keuangan yang mencurigakan, Penyelenggara wajib memiliki dan memelihara profil Nasabah secara terpadu (*single CIF*).
  7. Informasi yang terdapat dalam *single CIF* mencakup seluruh produk atau jasa yang digunakan oleh Nasabah pada suatu Penyelenggara.
  8. Untuk rekening bersama (jika ada) maka CIF dibuat atas masing-masing pihak pemilik rekening bersama (*joint account*). Contohnya rekening bersama (*joint account*) atas nama A dan B, maka CIF yang dibuat adalah 2 (dua) CIF yaitu CIF atas nama A dan B dengan menginformasikan bahwa baik A maupun B memiliki rekening bersama (*joint account*).

9. Untuk keperluan pemeliharaan *single* CIF, Penyelenggara harus menetapkan kebijakan bahwa untuk setiap penambahan rekening dan/atau produk atau jasa oleh Nasabah yang sudah ada, Penyelenggara harus mengkaitkan rekening, produk atau jasa tambahan tersebut dengan nomor informasi Nasabah dari Nasabah yang bersangkutan.
10. Untuk memastikan sistem informasi manajemen tetap berjalan dengan baik dan efektif, Penyelenggara harus melakukan mitigasi risiko antara lain terhadap:
  - a. keamanan data dari serangan siber (*cyberattacks*) dan penggunaan identitas digital, yang dapat dilakukan dengan:
    - 1) melakukan identifikasi dan penilaian risiko terkait penggunaan Teknologi Informasi;
    - 2) menggunakan Teknologi Informasi yang sudah tersertifikasi sesuai dengan peraturan perundang-undangan;
    - 3) memiliki Teknologi Informasi yang saling terhubung dan saling mendukung;
    - 4) menggunakan perangkat lunak (*software*) yang legal;
    - 5) memiliki kebijakan dan prosedur internal terkait Penyelenggaraan Teknologi Informasi termasuk penggunaan *security tools* seperti teknologi enkripsi, *anti-virus* dan *firewall* termasuk pembaruannya dengan merujuk ketentuan yang dikeluarkan oleh Kementerian atau Lembaga yang menyelenggarakan urusan pemerintahan dibidang siber dan sandi negara;
    - 6) meningkatkan kesadaran sumber daya manusia di lingkungannya untuk memberikan perlindungan data pribadi dalam Teknologi Informasi yang dikelolanya;
    - 7) mengadakan pelatihan pencegahan kegagalan perlindungan data pribadi dalam Teknologi Informasi yang dikelolanya;
    - 8) melakukan informasi teknologi audit (IT audit) secara berkala dan/atau dalam hal diperlukan sesuai dengan kebutuhan Penyelenggara yang dimaksudkan untuk memastikan keandalan Teknologi Informasi yang digunakan dan untuk memastikan agar Teknologi Informasinya tidak digunakan/dimanfaatkan oleh pelaku Pencucian Uang

- dan/atau Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal; dan/atau
- 9) melakukan edukasi kepada Nasabah terkait keamanan data pribadi dan pencegahan serangan siber (*cyberattack*).
- b. perlindungan data pribadi, yang dapat dilakukan sebagai berikut:
- 1) data pribadi yang disimpan telah diverifikasi kebenarannya;
  - 2) data pribadi disimpan dalam bentuk data terenkripsi;
  - 3) penyimpanan data pribadi dilakukan sesuai dengan peraturan perundang-undangan yang mengatur jangka waktu penyimpanan data pribadi; dan
  - 4) penggunaan akses data pribadi oleh Penyelenggara melalui perangkat keras milik Nasabah (contohnya *smartphone*) dibatasi sesuai ketentuan peraturan perundang-undangan. Apabila pemilik data pribadi tidak lagi menjadi Nasabah, Penyelenggara harus menyimpan data pribadi tersebut sesuai batas waktu sebagaimana dimaksud dalam angka 3) terhitung sejak tanggal terakhir pemilik data pribadi menjadi Pengguna Jasa.
- c. pusat data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*) yang dapat dilakukan Penyelenggara dengan membuat dan menyimpan tempat penyimpanan internal sebagai pusat data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*) sesuai dengan peraturan perundang-undangan.

## VII. SUMBER DAYA MANUSIA DAN PELATIHAN

### A. SUMBER DAYA MANUSIA

1. Untuk mencegah digunakannya Penyelenggara sebagai media atau tujuan Pencucian Uang, Pendanaan Terorisme, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal yang melibatkan pihak intern. Penyelenggara wajib melakukan:
  - a. prosedur penyaringan dalam rangka penerimaan karyawan baru (*pre-employee screening*) sebagai bagian dari penerapan *know your employee* (KYE); dan
  - b. Pengenalan dan pemantauan terhadap profil karyawan.

2. Prosedur penyaringan dalam rangka penerimaan karyawan baru (*pre-employee screening*) dilakukan dalam bentuk:
  - a. metode screening yang dimaksudkan untuk memastikan profil calon karyawan tidak memiliki catatan kejahatan, antara lain mengharuskan calon karyawan membuat surat pernyataan dan/atau menyerahkan surat keterangan catatan kepolisian (SKCK);
  - b. melakukan verifikasi identitas dan pendidikan yang telah diperoleh calon karyawan antara lain melalui proses wawancara (interview) secara tatap muka ataupun secara virtual yang dimaksudkan untuk lebih memastikan kebenaran dari informasi dan data dari calon karyawan;
  - c. melakukan penelitian melalui media atau informasi lainnya terhadap latar belakang dari calon karyawan antara lain riwayat pekerjaan, dan/atau pengalaman kerja dari calon karyawan;
  - d. memastikan track record yang baik dari calon karyawan antara lain dengan meminta surat rekomendasi dari perusahaan sebelumnya di mana calon karyawan pernah bekerja; dan
  - e. memastikan kualitas kredit calon karyawan tidak tergolong kredit macet.
3. Pengenalan dan pemantauan terhadap profil karyawan, mencakup perilaku dan gaya hidup karyawan, antara lain:
  - 1) melakukan verifikasi terhadap karyawan yang mengalami perubahan gaya hidup yang cukup signifikan;
  - 2) memastikan bahwa karyawan telah memahami dan menaati kode etik karyawan (*staff code of conduct*); dan
  - 3) mengevaluasi karyawan yang bertanggung jawab pada aktivitas yang tergolong berisiko tinggi antara lain memiliki akses ke data Penyelenggara, dan/atau berhadapan dengan Calon Nasabah atau Nasabah.
4. Prosedur penyaringan (*pre-employee screening*), pengenalan dan pemantauan terhadap profil karyawan dituangkan dalam kebijakan dan prosedur tertulis KYE Penyelenggara dengan berpedoman pada ketentuan yang mengatur mengenai penerapan strategi *anti fraud*.

## B. PELATIHAN

1. Penyelenggara wajib menyelenggarakan pelatihan yang berkesinambungan tentang kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal serta peran dan tanggung jawab karyawan dalam mencegah dan memberantas TPPU, TPPT, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal kepada seluruh karyawan.
2. Dalam menyelenggarakan pelatihan berkesinambungan sebagaimana dimaksud dalam angka 1, Penyelenggara dapat:
  - a. bekerja sama dengan pihak lain seperti asosiasi Penyelenggara, PPATK, dan/atau otoritas berwenang yang terkait; dan/atau
  - b. mengikutsertakan karyawannya dalam pelatihan antara lain yang diselenggarakan oleh asosiasi Penyelenggara, PPATK, Otoritas Jasa Keuangan, dan/atau otoritas berwenang lainnya.
3. Dalam menentukan peserta pelatihan, Penyelenggara mengutamakan karyawan yang tugas sehari-harinya memenuhi kriteria sebagai berikut:
  - a. melakukan pengawasan pelaksanaan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal; dan/atau
  - b. terkait dengan penyusunan pelaporan kepada PPATK dan Otoritas Jasa Keuangan.
4. Karyawan yang tugas sehari-harinya sebagaimana dimaksud pada angka 3 harus mendapatkan pelatihan secara berkesinambungan.
5. Karyawan lainnya selain karyawan sebagaimana dimaksud pada angka 3 harus mendapatkan pelatihan paling sedikit 1 (satu) kali dalam masa kerjanya, di mana pelatihan tersebut harus sudah dilakukan paling lama 1 (satu) tahun sejak karyawan tersebut pertama kali bekerja sebagai karyawan Penyelenggara.
6. Metode pelatihan
  - a. Pelatihan dapat dilakukan secara virtual atau dalam jaringan maupun melalui tatap muka.

- b. Pelatihan secara virtual atau dalam jaringan sebagaimana dimaksud dalam huruf a, dapat menggunakan media *e-learning* baik yang disediakan oleh otoritas berwenang seperti PPATK, Otoritas Jasa Keuangan atau yang disediakan secara mandiri oleh Penyelenggara.
  - c. Pelatihan melalui tatap muka sebagaimana dimaksud dalam huruf a, dilakukan dengan menggunakan pendekatan antara lain:
    - 1) tatap muka secara interaktif (misalnya *workshop*) dengan topik pelatihan disesuaikan dengan kebutuhan peserta. Pendekatan ini digunakan untuk karyawan yang mendapatkan prioritas dan dilakukan secara berkesinambungan, misalnya setiap tahun; dan/atau
    - 2) tatap muka satu arah (misalnya seminar) dengan topik pelatihan adalah berupa gambaran umum dari penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal. Pendekatan ini diberikan kepada karyawan yang tidak mendapatkan prioritas dan dilakukan apabila terdapat perubahan ketentuan yang signifikan.
7. Materi dan Evaluasi Pelatihan
- a. Penyelenggara dapat mengembangkan materi pelatihan terkait penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal sesuai dengan kebutuhan. Beberapa topik yang dapat menjadi materi dalam pelatihan antara lain:
    - 1) pelatihan implementasi peraturan perundang-undangan yang terkait dengan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
    - 2) tren dan perkembangan profil risiko, teknik, metode, dan tipologi TPPU, TPPT, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal, khususnya dalam kaitannya dengan proses bisnis Penyelenggara;
    - 3) penggunaan Teknologi Informasi dalam penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;

- 4) penilaian risiko dan penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal berbasis risiko;
  - 5) penerapan kebijakan dan prosedur program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal;
  - 6) ketentuan *sharing information* dalam konglomerasi keuangan dengan memperhatikan ketentuan anti *tipping off*; dan/atau
  - 7) peran dan tanggung jawab pegawai dalam mencegah dan memberantas TPPU, TPPT, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal.
- b. Kedalaman materi pelatihan disesuaikan dengan kebutuhan karyawan dan kesesuaian dengan tugas dan tanggung jawab karyawan.
  - c. Untuk mengetahui tingkat pemahaman karyawan dan kesesuaian materi pelatihan, Penyelenggara harus melakukan evaluasi terhadap setiap pelatihan yang telah diselenggarakan.
  - d. Evaluasi dapat dilakukan secara langsung melalui wawancara atau secara tidak langsung melalui tes.
  - e. Penyelenggara harus melakukan upaya tindak lanjut dari hasil evaluasi pelatihan melalui penyempurnaan materi dan metode pelatihan.

## VIII. PELAPORAN

1. Laporan kepada Otoritas Jasa Keuangan
  - a. Laporan Rencana Kegiatan Pengkinian Data dan Laporan Realisasi Kegiatan Pengkinian Data
    - 1) Pengkinian data Nasabah difokuskan pada Nasabah yang memiliki risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal lebih tinggi terlebih dahulu, di mana pengkinian data Nasabah berisiko tinggi dilakukan lebih sering dibandingkan Nasabah yang memiliki tingkat risiko lebih rendah. Pengkinian Nasabah berisiko tinggi dilakukan paling kurang 1 (satu) tahun sekali, Nasabah berisiko sedang 2 (dua)

tahun sekali, Nasabah berisiko rendah dilakukan 3 (tiga) tahun sekali.

- 2) Laporan rencana kegiatan pengkinian data Nasabah dan laporan realisasi kegiatan pengkinian data Nasabah harus disetujui dan disampaikan oleh Direksi yang membawahkan fungsi kepatuhan atau salah satu anggota Direksi yang bertanggung jawab terhadap penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.
- 3) Laporan rencana kegiatan pengkinian data Nasabah memuat jumlah Nasabah dan tingkat risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal dari Nasabah yang akan dikinikan, informasi yang akan dikinikan, metode atau strategi pengkinian, dan persentase pemenuhan Nasabah yang akan dikinikan pada periode tertentu.

Contoh format laporan rencana pengkinian data nasabah terdapat pada Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

- 4) Laporan realisasi kegiatan pengkinian Nasabah ke Otoritas Jasa Keuangan, memuat hasil pengkinian Nasabah berupa jumlah target Nasabah yang harus dikinikan, jumlah Nasabah yang berhasil dikinikan, jumlah Nasabah yang tidak berhasil dikinikan yang tercermin dari selisih target dengan realisasi, kendala yang dihadapi, serta upaya tindak lanjut yang akan dilakukan atas Nasabah yang tidak berhasil dikinikan.

Contoh format laporan realisasi pengkinian data nasabah terdapat pada Lampiran yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

- 5) Penyampaian laporan rencana kegiatan pengkinian data Nasabah sebagaimana dimaksud dalam angka 3) harus disampaikan ke Otoritas Jasa Keuangan setiap tahun paling lambat akhir bulan Desember.

Sebagai contoh, untuk pengkinian data Nasabah kurun waktu Januari sampai dengan Desember 2022, Penyelenggara harus menyampaikan laporan rencana

pengkinian data Nasabah paling lambat tanggal 31 Desember tahun 2021.

- 6) Penyampaian laporan realisasi pengkinian data sebagaimana dimaksud dalam angka 4) disampaikan ke Otoritas Jasa Keuangan setiap tahun paling lambat 1 (satu) bulan setelah periode pelaporan berakhir.  
Sebagai contoh, pengkinian data Nasabah yang telah dilakukan pada kurun waktu Januari sampai dengan akhir Desember 2021, Penyelenggara harus menyampaikan laporan realisasi pengkinian data paling lambat tanggal 31 Januari tahun 2022.
- 7) Penyampaian laporan rencana pengkinian data Nasabah sebagaimana dimaksud dalam angka 3) untuk pertama kalinya disampaikan paling lambat akhir Desember 2022. Sementara penyampaian laporan realisasi pengkinian data sebagaimana dimaksud dalam angka 4) untuk pertama kalinya disampaikan paling lambat akhir Januari 2023.
- 8) Dalam hal terdapat perubahan atas laporan rencana kegiatan pengkinian data, yang telah disampaikan kepada Otoritas Jasa Keuangan, Penyelenggara wajib menyampaikan perubahan tersebut paling lambat 7 (tujuh) hari kerja sejak perubahan dilakukan.
- 9) Surat pengantar penyampaian laporan rencana kegiatan pengkinian data Nasabah sebagaimana dimaksud dalam angka 3) dan laporan realisasi kegiatan pengkinian data Nasabah sebagaimana dimaksud dalam angka 4) yang ditandatangani oleh Direksi dan isi laporan rencana kegiatan pengkinian data Nasabah dan laporan realisasi kegiatan pengkinian data Nasabah tersebut disampaikan secara *online* melalui sistem jaringan komunikasi data Otoritas Jasa Keuangan.
- 10) Dalam hal sistem jaringan komunikasi data Otoritas Jasa Keuangan sebagaimana dimaksud dalam angka 9) belum tersedia maka surat pengantar penyampaian laporan dan isi laporan dimaksud disampaikan melalui surat elektronik (*email*); dan

- 11) Dalam hal sistem jaringan komunikasi data Otoritas Jasa Keuangan sebagaimana dimaksud dalam angka 9) dan surat elektronik (*email*) sebagaimana dimaksud dalam angka 10) mengalami gangguan atau permasalahan teknis maka surat pengantar penyampaian laporan dan isi laporan dimaksud dapat dilakukan secara *offline* dalam bentuk *hardcopy* dan/atau media penyimpanan elektronik.
  - 12) Laporan sebagaimana dimaksud dalam angka 3) dan angka 4) disampaikan oleh Penyelenggara kepada:  
Kepala Eksekutif Pengawas Industri Keuangan Nonbank Otoritas Jasa Keuangan  
u.p. Direktur Pengaturan, Perizinan, dan Pengawasan Financial Technology  
Gedung Wisma Mulia 2 Lantai 12  
Jalan Jenderal Gatot Subroto Kav 42  
Jakarta Selatan 12710.
  - 13) Dalam hal terdapat perubahan alamat Kantor Otoritas Jasa Keuangan untuk penyampaian laporan sebagaimana dimaksud dalam angka 12), Otoritas Jasa Keuangan akan menyampaikan pemberitahuan mengenai perubahan alamat melalui surat atau pengumuman.
- b. Laporan Perubahan Penyesuaian Kebijakan dan Prosedur Penerapan Program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.
- 1) Laporan perubahan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal memuat hal-hal perubahan atas penyesuaian kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal yang telah disampaikan sebelumnya kepada Otoritas Jasa Keuangan.
  - 2) Laporan perubahan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal harus disetujui dan disampaikan oleh Direksi yang membawahkan fungsi kepatuhan atau salah satu anggota Direksi yang

bertanggung jawab terhadap penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal.

- 3) Penyampaian laporan perubahan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal harus disampaikan paling lambat 7 (tujuh) hari kerja sejak perubahan dilakukan.

Sebagai contoh, Penyelenggara telah melakukan perubahan atas penyesuaian kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal pada Senin, 14 November 2022, Penyelenggara harus menyampaikan laporan perubahan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT serta pencegahan pendanaan Proliferasi Senjata Pemusnah Massal paling lambat pada 22 November 2022.

- 4) Laporan sebagaimana dimaksud pada angka 1) disampaikan oleh Penyelenggara kepada  
Kepala Eksekutif Pengawas Industri Keuangan Nonbank  
Otoritas Jasa Keuangan  
u.p. Direktur Pengaturan, Perizinan, dan Pengawasan  
Financial Technology  
Gedung Wisma Mulia 2 Lantai 12  
Jalan Jenderal Gatot Subroto Kav 42  
Jakarta Selatan 12710.
- 5) Dalam hal terdapat perubahan alamat Kantor Otoritas Jasa Keuangan untuk penyampaian laporan sebagaimana dimaksud dalam angka 4), Otoritas Jasa Keuangan akan menyampaikan pemberitahuan mengenai perubahan alamat melalui surat atau pengumuman.

## 2. Laporan kepada PPATK

Penyelenggara harus menyampaikan laporan kepada PPATK sebagaimana diatur dalam peraturan perundang-undangan yang mengatur mengenai pencegahan dan pemberantasan TPPU, termasuk peraturan pelaksanaannya.

IX. PENUTUP

Ketentuan dalam Surat Edaran Otoritas Jasa Keuangan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta  
pada tanggal 29 Januari 2021

KEPALA EKSEKUTIF PENGAWAS  
PERASURANSIAN, DANA PENSIUN,  
LEMBAGA PEMBIAYAAN, DAN  
LEMBAGA JASA KEUANGAN LAINNYA  
OTORITAS JASA KEUANGAN  
REPUBLIK INDONESIA,

ttd

RISWINANDI

Salinan ini sesuai dengan aslinya  
Direktur Hukum 1  
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 6 /SEOJK.05/2021

TENTANG

PEDOMAN PENERAPAN PROGRAM ANTI PENCUCIAN UANG DAN PENCEGAHAN  
PENDANAAN TERORISME BAGI PENYELENGGARA LAYANAN PINJAM MEMINJAM  
UANG BERBASIS TEKNOLOGI INFORMASI

A. SIKLUS PENDEKATAN BERBASIS RISIKO (*RISK BASED APPROACH*)

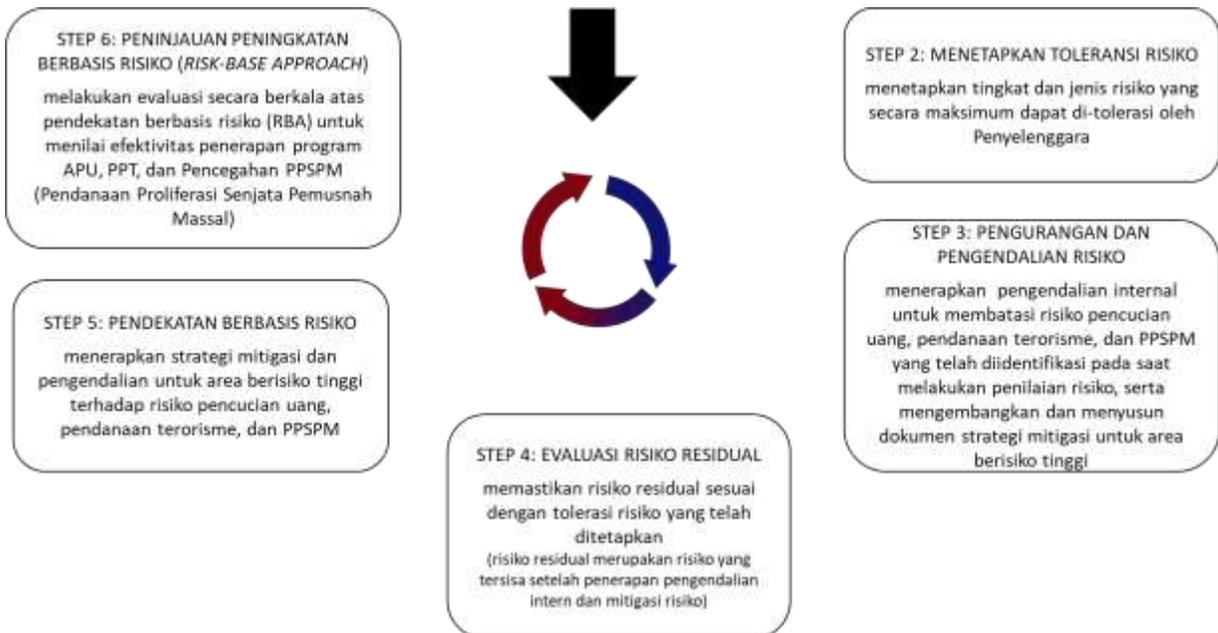
STEP 1: IDENTIFIKASI RISIKO BAWAAN (INHERENT RISK)

Jenis-Jenis Risiko



Risiko Nasabah	Risiko Negara/ Geografis/Yuridiksi	Risiko Produk/Jasa/ Transaksi	Risiko Jaringan Distribusi
Nasabah dalam layanan pinjam meminjam uang berbasis teknologi informasi, menggunakan sistem identitas digital dan layanan non <i>face to face</i> berdasarkan identifikasi risiko bawaan ( <i>inherent risk</i> ) dalam kegiatan usaha PJK memiliki kekhasan yaitu pengumpulan data pribadi nasabah dilakukan dengan menggunakan sistem elektronik, verifikasi nasabah dilakukan melalui sistem elektronik.	Risiko negara, risiko area geografis, atau risiko yuridiksi bersama dengan faktor risiko lainnya, menyediakan informasi yang sangat bermanfaat untuk penilaian risiko pencucian uang, pendanaan terorisme, dan pendanaan proliferasi senjata pemusnah massal.	Produk, jasa, atau transaksi yang mungkin dapat terpapar risiko yang lebih tinggi terkait APU, PPT, dan pendanaan proliferasi senjata pemusnah massal. Selain itu terdapat hal yang meningkatkan profil risiko produk, jasa, atau transaksi.	Salah satu ciri khas bisnis PJK layanan pinjam meminjam uang berbasis teknologi informasi adalah proses jaringan distribusi ( <i>delivery channels</i> ) yang dilakukan tanpa pertemuan langsung ( <i>non face to face</i> ).

Risiko relevan lainnya terutama yang berkaitan dengan penggunaan sistem elektronik



B. MATRIKS KEMUNGKINAN DAN DAMPAK (*LIKELIHOOD AND IMPACT MATRIX*)

1. Dalam melakukan identifikasi risiko, salah satu alat bantu yang dapat digunakan oleh Penyelenggara ialah matriks kemungkinan dan dampak (*likelihood and impact matrix*). Matriks tersebut membantu Penyelenggara dalam menetapkan seberapa besar upaya atau pemantauan yang perlu dilakukan untuk mengidentifikasi risiko bawaan (*inherent risk*). Perlu diperhatikan bahwa matriks tersebut hanya merupakan contoh. Penyelenggara dapat menggunakan alat bantu lain atau bentuk matriks lain yang sesuai dengan skala usaha, kebutuhan, karakteristik dan kompleksitas kegiatan usaha Penyelenggara sehingga benar-benar dapat menggambarkan risiko yang dihadapi Penyelenggara.

a. Kemungkinan (*likelihood*)

Kemungkinan (*likelihood*) mengacu pada potensi risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang terjadi untuk setiap risiko tertentu yang dinilai. Dalam hal ini Penyelenggara dapat menggunakan skala risiko yang umum digunakan yaitu:

**PERINGKAT KEMUNGKINAN (*LIKELIHOOD*)**

<b>TINGGI</b>	TPPU, TPPT, dan/atau pendanaan Proliferasi Senjata Pemusnah Massal terjadi
<b>SEDANG</b>	Kemungkinan ( <i>likelihood</i> ) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal dapat diterima
<b>RENDAH</b>	Tidak terdapat kemungkinan ( <i>likelihood</i> ) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal

b. Dampak (*Impact*)

Dampak (*impact*) dalam hal ini merujuk pada tingkat keseriusan atau konsekuensi dari suatu kerusakan atau kerugian yang terjadi apabila terjadi risiko.

Timbulnya dampak (*impact*) bergantung pada kondisi internal Penyelenggara. Dampak (*impact*) atas terjadinya risiko Pencucian

Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal dapat dilihat dari berbagai sudut pandang, antara lain:

- a. risiko reputasi dan dampaknya terhadap kegiatan usaha Penyelenggara;
- b. dampak (*impact*) regulasi;
- c. kerugian finansial bagi Penyelenggara; dan/atau
- d. risiko hukum.

Dampak (*impact*) atas terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal akan sangat spesifik untuk setiap Penyelenggara sehingga terdapat kesulitan dalam menghitung dampak (*impact*). Oleh karena itu, hanya Penyelenggara yang dapat menentukan dampak (*impact*) atas risiko yang terjadi. Skala yang digunakan untuk menghitung dampak (*impact*) tidak jauh berbeda dengan skala dalam menghitung kemungkinan (*likelihood*).

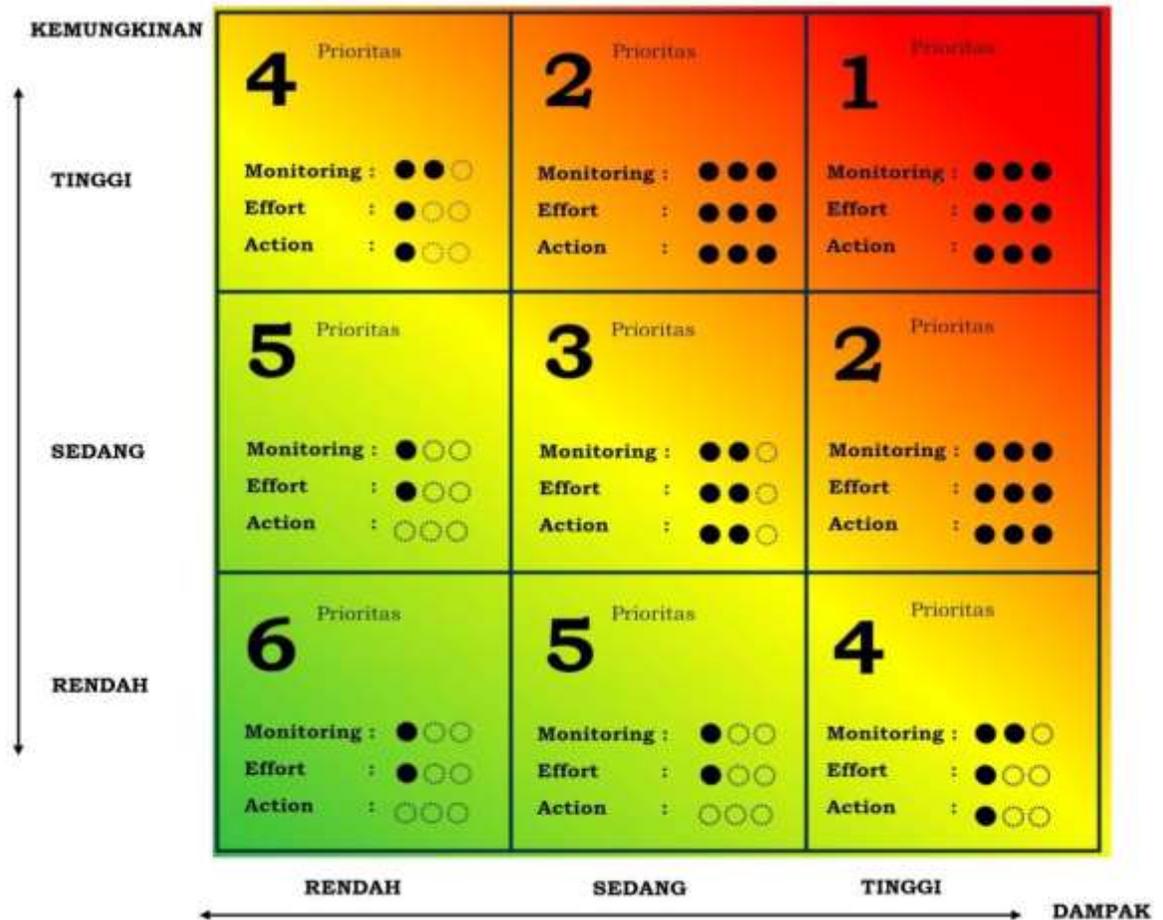
<b>Peringkat</b>	<b>Konsekuensi atas risiko Pencucian Uang dan Pendanaan Terorisme serta Pendanaan Proliferasi Senjata Pemusnah Massal</b>
<b>Tinggi</b>	Risiko memiliki konsekuensi yang berat
<b>Sedang</b>	Risiko memiliki konsekuensi yang moderat
<b>Rendah</b>	Risiko memiliki konsekuensi yang kecil atau tidak signifikan

- 2. Matriks kemungkinan (*likelihood*) dan dampak (*impact*) akan membantu Penyelenggara untuk memutuskan hal yang perlu dilakukan dengan mempertimbangkan risiko secara keseluruhan. Seperti yang telah disebutkan sebelumnya, pendekatan berbasis risiko merupakan proses yang memungkinkan Penyelenggara untuk menerapkan langkah-langkah yang sepadan dengan risiko yang teridentifikasi sebagai bagian dari penilaian risiko.

### Matriks Kemungkinan dan Dampak

Setiap kotak dalam matriks menunjukkan sumber daya yang dibutuhkan untuk melakukan:

- *Action* (contoh: risiko perlu segera ditindaklanjuti)
- *Effort* (contoh: tingkat upaya dalam melakukan mitigasi risiko)
- *Monitoring* (contoh: tingkat pemantauan yang perlu dilakukan Penyelenggara)



### 3. Cara membaca matriks prioritas

#### a. Kotak 6

Kondisi pada kotak 6 menunjukkan kemungkinan (*likelihood*) dan dampak (*impact*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal rendah sehingga Penyelenggara tidak perlu mengambil tindakan, upaya, atau pemantauan khusus.

#### b. Kotak 5

Kondisi pada kotak 5 menunjukkan kemungkinan dan dampak (*impact*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal

tergolong rendah namun berpotensi meningkat dan menjadi skala sedang. Untuk kondisi pada kotak 5 diperlukan upaya dan monitoring untuk mencegah peningkatan risiko (tidak berubah menjadi kotak 4 atau kotak 3).

c. Kotak 4

Kondisi pada kotak 4 menunjukkan kemungkinan (*likelihood*) dan dampak (*impact*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal yang tergolong medium. Pada kondisi ini, Penyelenggara perlu mengambil tindakan, upaya atau pemantauan. Tindakan, upaya, atau pemantauan yang memadai akan menurunkan kemungkinan dan dampak (*impact*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal, sebaliknya apabila tindakan, upaya, atau pemantauan tidak memadai maka akan meningkatkan risiko menjadi risiko tinggi.

d. Kotak 3

Kondisi pada kotak 3 menunjukkan bahwa Penyelenggara perlu mengalokasikan sumber daya untuk melakukan tindakan, upaya, dan pemantauan. Terdapat kemungkinan (*likelihood*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal dengan dampak (*impact*) yang dapat dikategorikan moderat. Untuk itu, Penyelenggara perlu memperhatikan seluruh kegiatan usaha dan hubungan usaha yang ada, sehingga tidak menimbulkan peningkatan risiko (tidak berubah menjadi kotak 2 atau kotak 1).

e. Kotak 2

Kondisi pada kotak 2 menunjukkan bahwa kemungkinan (*likelihood*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal tergolong tinggi. Pada kondisi ini, Penyelenggara perlu memperhatikan seluruh kegiatan usaha dan hubungan usaha dan mengerahkan sumber daya untuk menekan kemungkinan (*likelihood*) dan dampak (*impact*) risiko. Penyelenggara perlu menerapkan langkah mitigasi yang lebih ketat untuk mencegah

peningkatan risiko menjadi sangat tinggi, atau menjadi kondisi pada kotak 1.

f. Kotak 1

Kondisi pada kotak 1 menunjukkan bahwa kemungkinan (*likelihood*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal sangat tinggi termasuk besarnya dampak (*impact*) atas risiko tersebut. Pada kondisi tersebut dibutuhkan sumber daya yang lebih banyak, tindakan khusus, upaya khusus serta pemantauan berkala untuk meminimalisasi risiko tersebut.

C. CONTOH TRANSAKSI KEUANGAN MENCURIGAKAN TERKAIT PENCUCIAN UANG DALAM PENYELENGGARAAN LAYANAN PINJAM MEMINJAM UANG BERBASIS TEKNOLOGI INFORMASI

1. Pengguna Jasa diduga bertindak atas nama pihak ketiga, tetapi tidak memberitahu Penyelenggara.
2. Penyelenggara menyadari bahwa Pengguna Jasa adalah pelaku yang diduga melakukan tindak pidana Pencucian Uang dan/atau Pendanaan Terorisme serta pendanaan Proliferasi Senjata Pemusnah Massal.
3. Penyelenggara mendapatkan informasi dari sumber yang dapat dipercaya (PPATK, lembaga pengatur dan pengawas termasuk Otoritas Jasa Keuangan, aparat penegak hukum, media massa, atau sumber lainnya) bahwa Pengguna Jasa diduga terlibat dalam aktivitas ilegal dan/ atau memiliki latar belakang tindak kriminal.
4. Pengguna Jasa mengubah atau membatalkan transaksi setelah Penyelenggara meminta dokumen identitas Pengguna Jasa.
5. Registrasi sebagai Pengguna atas nama badan usaha, yayasan, organisasi, dan atau individu yang terlibat, diduga terlibat atau terkait dengan kegiatan terorisme.
6. Transaksi Pengguna Jasa yang terkait dengan usaha menggunakan rekening perorangan.
7. Pengguna Jasa/pengurus atau pemilik Pengguna Jasa diduga menggunakan dana hasil tindak pidana  
Contoh: dapat digunakan oleh Pemberi Pinjaman untuk menyalurkan dana ke Penerima Pinjaman atau Penerima Pinjaman saat membayar pinjaman ke Pemberi Pinjaman melalui Penyelenggara.
8. Pengurus atau pemilik Pengguna Jasa diduga melakukan suatu tindak pidana.
9. Transaksi melibatkan perusahaan fiktif atau *paper company*.  
Contoh: Dapat terjadi apabila Penyelenggara memiliki produk *Invoice Financing* atau Pemberi Pinjaman yang bersifat institusi yang menggunakan *paper company*.
10. Transaksi keuangan yang diminta oleh PPATK karena Pengguna Jasa telah ditetapkan sebagai tersangka/terdakwa dalam kasus tindak pidana.  
Contoh: Pemberi Pinjaman telah ditetapkan sebagai tersangka/terdakwa.

11. Transaksi keuangan yang diminta oleh PPATK karena keterkaitannya dengan transaksi lain yang sedang dalam proses analisis maupun pemeriksaan oleh PPATK.
12. Transaksi Keuangan yang diminta oleh PPATK atas dasar penyelidikan atau penyidikan yang sedang dilakukan oleh aparat penegak hukum.
13. Pengguna Jasa/calon Pengguna Jasa memberikan informasi yang tidak benar mengenai hal-hal yang berkaitan dengan identitas, sumber penghasilan atau usahanya.  
Contoh: Penerima Pinjaman yang tidak memberikan informasi dengan benar seperti penghasilan, alamat kantor, usaha dan sebagainya.
14. Pengguna Jasa/calon Pengguna Jasa menggunakan dokumen identitas yang diragukan kebenarannya atau diduga palsu seperti tanda tangan yang berbeda atau foto yang tidak sama.  
Contoh: Penerima Pinjaman atau Pemberi Pinjaman yang tidak memberikan informasi dengan benar.
15. Pengguna Jasa/calon Pengguna Jasa enggan atau menolak untuk memberikan informasi/dokumen yang diminta oleh petugas Penyelenggara tanpa alasan yang jelas.
16. Pengguna Jasa tidak bersedia memberikan informasi yang benar atau segera memutuskan hubungan usaha/menutup rekening pada saat petugas Penyelenggara meminta informasi atas transaksi yang dilakukannya.
17. Pengguna Jasa enggan memberikan informasi sumber dana dan tujuan transaksi secara lengkap kepada Penyelenggara.
18. Pengguna Jasa menggunakan nama yang berbeda (ejaan yang berbeda) dari satu transaksi ke transaksi yang lain.
19. Transaksi melibatkan perusahaan fiktif dengan indikasi menggunakan dokumen palsu.
20. Pengguna Jasa berupaya untuk meyakinkan pegawai Penyelenggara untuk tidak melengkapi dokumentasi apapun yang diperlukan untuk melakukan transaksi.
21. Ditemukan ketidak-konsistenan identifikasi atau verifikasi yang tidak dapat dijelaskan (misalnya perbedaan negara tempat tinggal terdahulu, perbedaan negara yang mengeluarkan paspor terdahulu, perbedaan negara yang pernah dikunjungi sesuai dengan paspor,

atau perbedaan dokumen-dokumen yang terkait dengan nama, alamat, dan tanggal lahir).

22. Pengguna Jasa memberikan informasi yang diragukan atau tidak jelas.
23. Pengguna Jasa menolak untuk memberikan dokumen identitas pribadi.
24. Semua identitas yang disajikan tidak dapat diperiksa kebenarannya karena alasan tertentu.
25. Pengguna Jasa menyajikan dokumen identitas yang berbeda setiap kali transaksi dilakukan.
26. Pengguna Jasa menggunakan alamat PO BOX dan berasal dari negara yang berisiko tinggi.

D. Contoh Format Laporan Rencana Pengkinian Data Nasabah

**LAPORAN RENCANA PENGKINIAN DATA NASABAH  
(NAMA PENYELENGGARA)  
TAHUN .....**

No.	Jenis Nasabah dan tingkat risiko	Jumlah profil Nasabah secara terpadu ( <i>Single Customer Identification File</i> )		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan <i>Single Customer Identification File</i> yang akan dikinikan pada periode tertentu
		Yang akan dikinikan <i>Single Customer Identification File</i>	% terhadap seluruh jumlah <i>Single Customer Identification File</i>			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1	Nasabah orang perseorangan					
	a. Risiko tinggi					
	b. Risiko sedang					
	c. Risiko rendah					
2	Nasabah Korporasi					
	a. Non usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	b. Usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	c. Penyedia Jasa					

No.	Jenis Nasabah dan tingkat risiko	Jumlah profil Nasabah secara terpadu ( <i>Single Customer Identification File</i> )		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan <i>Single Customer Identification File</i> yang akan dikinikan pada periode tertentu
		Yang akan dikinikan <i>Single Customer Identification File</i>	% terhadap seluruh jumlah <i>Single Customer Identification File</i>			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	Keuangan					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	d. Yayasan					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	e. Selain perusahaan dan yayasan (berbadan hukum maupun tidak berbadan hukum)					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
3	Nasabah perikatan lainnya ( <i>legal arrangement</i> )					
	a. <i>Trust</i>					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	b. Selain <i>trust</i>					

No.	Jenis Nasabah dan tingkat risiko	Jumlah profil Nasabah secara terpadu ( <i>Single Customer Identification File</i> )		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan <i>Single Customer Identification File</i> yang akan dikinikan pada periode tertentu
		Yang akan dikinikan <i>Single Customer Identification File</i>	% terhadap seluruh jumlah <i>Single Customer Identification File</i>			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
4.	Lembaga Negara, Instansi Pemerintah, lembaga internasional, dan perwakilan negara asing					
	a. Risiko tinggi					
	b. Risiko sedang					
	c. Risiko rendah					

1. Keterangan kolom:

- (a). Diisi dengan nomor.
- (b). Sesuai kolom.
- (c). Diisi dengan rencana jumlah *Single Customer Identification File* yang akan dikinikan untuk 1 (satu) tahun berikutnya.
- (d). Diisi dalam persentase.
- (e). Informasi dapat diisi lebih dari satu, seperti pengkinian alamat tempat tinggal atau pekerjaan.
- (f). Metode atau strategi dapat diisi lebih dari satu, seperti korespondensi melalui surat atau surat elektronik.
- (g). Diisi dengan target pemenuhan pengkinian *Single Customer Identification File* dalam persen pada periode tertentu. Periode ditentukan dengan menyesuaikan kemampuan dan kondisi masing-masing Penyelenggara, misalnya secara triwulanan. Contoh: Triwulan I = 30%, Triwulan II=60%, Triwulan III=90%, Triwulan IV=100%.

2. Jumlah tingkat risiko dapat disesuaikan dengan kebijakan yang telah ditetapkan oleh Penyelenggara.

E. Contoh Format Laporan Rencana Pengkinian Data Nasabah

**LAPORAN REALISASI PENGKINIAN DATA NASABAH  
(NAMA PENYELENGGARA)  
TAHUN .....**

No.	Jenis Nasabah dan tingkat risiko	Perkembangan			Kendala	Upaya yang akan dilakukan
		Target	Realisasi	Deviasi (%)		
(a)	(b)	(c)	(d)	(e)	(a)	(b)
1	Nasabah orang perseorangan					
	a. Risiko tinggi					
	b. Risiko sedang					
	c. Risiko rendah					
2	Nasabah Korporasi					
	a. Non usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	b. Usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	c. Penyedia Jasa Keuangan					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	d. Yayasan					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					

No.	Jenis Nasabah dan tingkat risiko	Perkembangan			Kendala	Upaya yang akan dilakukan
		Target	Realisasi	Deviasi (%)		
(a)	(b)	(c)	(d)	(e)	(a)	(b)
	e. Selain perusahaan dan yayasab (berbadan hukum maupun tidak berbadan hukum)					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
3	Nasabah perikatan lainnya ( <i>legal arrangement</i> )					
	a. <i>Trust</i>					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
	b. Selain <i>trust</i>					
	1) Risiko tinggi					
	2) Risiko sedang					
	3) Risiko rendah					
4.	Lembaga Negara, Instansi Pemerintah, lembaga internasional, dan perwakilan negara asing					
	a. Risiko tinggi					
	b. Risiko sedang					
	c. Risiko rendah					

1. Keterangan kolom:

(a). Diisi dengan nomor.

(b). Sesuai kolom.

(c). Diisi dengan target jumlah *Single Customer Identification File* yang dikinikan.

(d). Diisi dengan realisasi jumlah *Single Customer Identification File* yang dikinikan.

(e). Diisi dengan persentase selisih antara taget *Single Customer Identification File* yang akan dikinikan (c) dengan (d) realisasi jumlah *Single Customer Identification File* yang dikinikan.

- (f). Kendala dapat diisi lebih dari satu.
  - (g). Diisi dengan upaya untuk mengatasi kendala dan dapat lebih dari satu.
2. Jumlah tingkat risiko dapat disesuaikan dengan kebijakan yang telah ditetapkan oleh Penyelenggara.

Ditetapkan di Jakarta  
pada tanggal 29 Januari 2021

KEPALA EKSEKUTIF PENGAWAS  
PERASURANSIAN, DANA PENSIUN,  
LEMBAGA PEMBIAYAAN, DAN  
LEMBAGA JASA KEUANGAN LAINNYA  
OTORITAS JASA KEUANGAN  
REPUBLIK INDONESIA,

ttd

RISWINANDI

Salinan ini sesuai dengan aslinya  
Direktur Hukum 1  
Departemen Hukum

ttd

Mufli Asmawidjaja