Yth.
Penyelenggara Layanan Urun Dana
di tempat.

SALINAN

SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 17 /SEOJK.04/2022
TENTANG
PEDOMAN PENERAPAN PROGRAM ANTI PENCUCIAN UANG DAN PENCEGAHAN PENDANAAN TERORISME BAGI PENYELENGGARA LAYANAN URUN DANA BERBASIS TEKNOLOGI INFORMASI

Sehubungan dengan ketentuan Pasal 82 Peraturan Otoritas Jasa Keuangan Nomor 57/POJK.04/2020 tentang Penawaran Efek melalui Layanan Urun Dana Berbasis Teknologi Informasi (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 281, Tambahan Lembaran Negara Republik Indonesia Nomor 6594) sebagaimana telah diubah dengan Peraturan Otoritas Jasa Keuangan Nomor 16/POJK.04/2021 tentang Perubahan atas Peraturan Otoritas Jasa Keuangan Nomor 57/POJK.04/2020 Tentang Penawaran Efek Melalui Layanan Urun Dana Berbasis Teknologi Informasi (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 193, Tambahan Lembaran Negara Republik Indonesia Nomor 6714), perlu untuk mengatur ketentuan mengenai pedoman penerapan program anti pencucian uang dan pencegahan pendanaan terorisme bagi penyelenggara layanan urun dana 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. Penawaran Efek melalui Layanan Urun Dana Berbasis Teknologi Informasi yang selanjutnya disebut Layanan Urun Dana adalah penyelenggaraan layanan penawaran efek yang dilakukan oleh penerbit untuk menjual efek secara langsung kepada pemodal melalui jaringan sistem elektronik yang

bersifat terbuka.

b. Efek adalah surat berharga, yaitu surat pengakuan utang, surat berharga komersial, saham, obligasi, tanda bukti utang, unit penyertaan kontrak investasi kolektif, kontrak berjangka atas Efek, dan setiap derivatif dari Efek.

c. Penyelenggara Layanan Urun Dana yang selanjutnya disebut Penyelenggara adalah badan hukum Indonesia yang menyediakan, mengelola, dan mengoperasikan Layanan Urun Dana.

d. Pengguna Layanan Urun Dana yang selanjutnya disebut Pengguna adalah penerbit dan pemodal.

e. Penerbit adalah badan usaha Indonesia baik yang berbentuk badan hukum maupun badan usaha lainnya yang menerbitkan Efek melalui Layanan Urun Dana.

f. Pemodal adalah pihak yang melakukan pembelian Efek Penerbit melalui Layanan Urun Dana.

g. Calon Nasabah adalah calon Pengguna yang akan menggunakan jasa Penyelenggara.

h. Nasabah adalah Pengguna yang menggunakan jasa Penyelenggara.

i. Direksi:
   1) bagi Penyelenggara yang berbentuk badan hukum perseroan terbatas adalah Direksi sebagaimana dimaksud dalam Undang-Undang mengenai perseroan terbatas; atau
   2) bagi Penyelenggara yang berbentuk badan hukum koperasi adalah pengurus sebagaimana dimaksud dalam Undang-Undang mengenai perkoperasian.

j. Dewan Komisaris:
   1) bagi Penyelenggara yang berbentuk badan hukum perseroan terbatas adalah Dewan Komisaris sebagaimana dimaksud dalam Undang-Undang mengenai perseroan terbatas; atau
   2) bagi Penyelenggara yang berbentuk badan hukum koperasi adalah pengawas sebagaimana dimaksud dalam Undang-Undang mengenai perkoperasian.

k. Pencucian Uang adalah pencucian uang sebagaimana dimaksud dalam Undang-Undang mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang.

l. Pendanaan Terorisme adalah pendanaan terorisme sebagaimana dimaksud dalam Undang-Undang mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme.

m. Proliferasi Senjata Pemusnah Massal adalah penyebaran senjata nuklir, biologi, dan kimia.

n. 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.

o. Sistem Elektronik Layanan Jasa Keuangan yang selanjutnya disebut 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. Teknologi Informasi Layanan Jasa Keuangan yang selanjutnya disebut Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi di bidang layanan jasa keuangan.

q. Uji Tuntas Nasabah (*Customer Due Diligence*) yang selanjutnya disingkat CDD adalah kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Penyelenggara untuk memastikan transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi Calon Nasabah dan Nasabah.

r. Uji Tuntas Lanjut (*Enhanced Due Diligence*) yang selanjutnya disingkat EDD adalah tindakan CDD lebih mendalam yang dilakukan Penyelenggara terhadap Calon Nasabah atau Nasabah yang berisiko tinggi termasuk orang yang populer secara politis (*politically exposed person*) dan/atau dalam area berisiko tinggi.

s. 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.

t. Transaksi Keuangan Mencurigakan yang selanjutnya disingkat TKM adalah transaksi keuangan mencurigakan sebagaimana dimaksud dalam Undang-Undang mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Undang-Undang mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme.

u. 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 Penyelenggara (*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.

v. 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, deputi direktur, dan anggota dewan atau fungsi yang setara.

w. 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.

x. 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.

y. Pusat Pelaporan dan Analisis Transaksi Keuangan yang selanjutnya disingkat PPATK adalah PPATK sebagaimana dimaksud dalam Undang-Undang mengenai pencegahan dan pemberantasan TPPU.

z. Rekomendasi *Financial Action Task Force* yang untuk selanjutnya disebut Rekomendasi FATF adalah standar pencegahan dan pemberantasan Pencucian Uang dan/atau Pendanaan Terorisme yang dikeluarkan oleh FATF.

2. Penyelenggara sangat rentan terhadap kemungkinan digunakan sebagai sarana Pencucian Uang dan/atau Pendanaan Terorisme. Penyelenggara dimungkinkan menjadi pintu masuk harta kekayaan yang merupakan hasil TPPU dan/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 dan/atau Pendanaan Terorisme.
4. Dalam kaitan tersebut perlu adanya peningkatan kualitas penerapan program APU dan PPT 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*), yaitu upaya menempatkan uang tunai yang berasal dari tindak pidana ke dalam sistem keuangan (*financial system*).
      2) pemisahan/pelapisan (*layering*), yaitu upaya untuk mengaburkan asal usul harta kekayaan yang berasal dari tindak pidana (*dirty money*) yang telah berhasil ditempatkan pada Penyelenggara. 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*), yaitu 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 modus dan tipologi Pencucian Uang, antara lain:

1) pemanfaatan korporasi atau penggunaan perusahaan boneka, dimana 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 dana hasil kejahatan.

   Sebagai contoh: pelaku kejahatan melegalkan dana hasil kejahatannya dengan cara menjadikan perusahaan boneka sebagai Pemodal yang membeli Efek melalui Layanan Urun Dana atau sebagai Penerbit yang melakukan penawaran Efek melalui Layanan Urun Dana.

2) *structuring*, yaitu upaya untuk memecah transaksi dalam beberapa transaksi dengan masing-masing nilai transaksi yang relatif kecil yang dimaksudkan untuk menghindari pelaporan.

   Sebagai contoh: Pemodal memecah transaksi yang dananya berasal dari dana kejahatan melalui beberapa akun pada Penyelenggara.

3) *smurfing,* yaitu upaya memecah transaksi yang dananya berasal dari hasil kejahatan melalui beberapa rekening atas nama individu yang berbeda, baik terafiliasi atau tidak terafiliasi, untuk kepentingan satu orang atau Pemilik Manfaat (*Beneficial Owner*) tertentu.

   Sebagai contoh: Pemodal melakukan pembelian Efek melalui Layanan Urun Dana dimana dana yang digunakan berasal dari hasil kejahatan. Pembelian Efek dilakukan melalui beberapa akun Pemodal dengan nama dan identitas yang berbeda untuk menghindari transaksi pembelian Efek dengan nilai yang mencurigakan, dibandingkan apabila dilakukan hanya melalui 1 (satu) akun Pemodal.

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

Sebagai contoh:

a) Pemodal menggabungkan dana hasil kejahatannya dengan dana legal untuk selanjutnya diinvestasikan melalui Layanan Urun Dana dengan cara pembelian Efek Penerbit yang menjalankan kegiatan usaha yang sah; atau

b) Penerbit menggabungkan dana hasil kejahatannya dengan dana legal yang diterima dari Pemodal melalui Layanan Urun Dana, yang selanjutnya digunakan untuk menjalankan kegiatan usaha yang sah;

5) penggunaan jasa profesional seperti konsultan hukum, notaris, perencana keuangan, dan akuntan termasuk akuntan publik, dengan tujuan untuk mengaburkan identitas penerima manfaat dan sumber dana hasil kejahatan.

   Sebagai contoh: Pemodal atau Penerbit melakukan kerja sama dengan konsultan hukum, notaris, perencana keuangan atau akuntan termasuk akuntan publik dalam bentuk rekayasa atau manipulasi transaksi 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 Penerbit;

6) penggunaan nama orang lain (*nominee*), anggota keluarga atau pihak ketiga, yang dimaksudkan untuk mengaburkan identitas orang-orang yang mengendalikan dana hasil kejahatan dengan menggunakan identitas sah pihak lain, baik pada Pemodal maupun Penerbit;

7) pemalsuan foto wajah (swafoto) pada saat verifikasi *non-face to face* dalam rangka CDD;

8) Pemodal melakukan perubahan nomor rekening yang menunjukkan perubahan pemilik rekening pada saat Pemodal akan mendapatkan imbal hasil pendanaan;

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), dimana dana hasil kejahatan ditransfer ke perusahaan tersebut, dan perusahaan tersebut menjadi sumber dana Pemodal;

10) penggunaan identitas palsu di internet (pemanfaatan internet enkripsi dan akses terhadap identitas) dengan melakukan peretasan (akses secara tidak sah ke perangkat dan/atau akun orang lain) terhadap *e-mail*, situs web, dan/atau membuat situs web yang seolah-olah asli padahal palsu (*phishing*) dengan tujuan untuk 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;

11) Pemodal dan Penerbit merupakan pihak yang memiliki hubungan afiliasi, dimana dana yang digunakan untuk melakukan transaksi pembelian Efek melalui Layanan Urun Dana dari Pemodal kepada Penerbit tersebut merupakan dana yang berasal dari hasil kejahatan; dan/atau

12) penyetoran dana dalam rangka transaksi pembelian efek melalui Layanan Urun Dana oleh Pemodal dilakukan oleh pihak selain Pemodal dimaksud, dimana dana yang disetorkan merupakan dana 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.

Berdasarkan Undang-Undang mengenai pencegahan dan pemberantasan tindak pidana pendanaan terorisme, 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, obligasi, *bank draft*, dan surat pengakuan utang.

Dalam tindak pidana terorisme, uang atau dana diperuntukkan sebagai sarana untuk melakukan aksi terorisme 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, serta mobilisasi anggota dari atau ke suatu tempat demi terlaksananya aksi teror.

b. TPPT merupakan 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 mempunyai kesamaan, yaitu menggunakan jasa keuangan sebagai sarana untuk melakukan suatu tindak pidana.

c. Berbeda dengan TPPU yang tujuannya untuk menyamarkan asal-usul harta kekayaan, tujuan TPPT adalah membantu kegiatan terorisme, baik dengan harta kekayaan yang merupakan hasil dari suatu tindak pidana maupun 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 dan tipologi Pendanaan Terorisme, antara

lain:

1) perampokan atau pencurian oleh Penerbit yang berpendapat bahwa mengambil harta orang atau pihak lain adalah halal. Dalam kaitan tersebut:
   a) Penerbit melakukan penawaran Efek melalui Layanan Urun Dana dengan tujuan memperoleh dana yang dapat digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris, tanpa adanya niat untuk mengembalikan dana investasi, termasuk hasil investasi dalam bentuk dividen atau imbal hasil kepada Pemodal; atau
   b) pelaku kejahatan melakukan peretasan akun milik Penerbit dan menggunakan dana hasil penawaran Efek oleh Penerbit yang akunnya telah diretas untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris;
2) penggunaan dana oleh Penerbit yang tidak sesuai dengan tujuan penggunaan dana hasil penawaran Efek melalui Layanan Urun Dana.

   Sebagai contoh: dana hasil penawaran Efek awalnya dimaksudkan untuk pengembangan kegiatan usaha Penerbit, namun setelah dana diterima, dana tersebut digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris;
3) pelaku kejahatan bertindak selaku Penerbit yang memiliki hubungan afiliasi dengan:
   a) Pemodal yang berkedudukan di dalam maupun di luar negeri; dan/atau
   b) individu atau lembaga yang berkedudukan di dalam maupun di luar negeri dan melakukan investasi dengan memberikan dana secara langsung maupun tidak langsung kepada Pemodal, dimana dana yang diperoleh tersebut digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris;
4) penyamaran kegiatan usaha oleh Penerbit dengan menyerahkan dokumen dan/atau informasi kepada Penyelenggara yang menunjukkan bahwa kegiatan

usahanya merupakan kegiatan perdagangan barang dan/atau jasa yang legal. Namun demikian, setelah dana hasil penawaran Efek terkumpul digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris;

5) Penerbit melakukan perubahan nomor rekening yang menunjukkan perubahan pemilik rekening pada saat Penerbit akan menerima pendanaan dimana dana yang diterima digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris; dan/atau

6) penggunaan *nominee* sebagai pengendali pada Penerbit yang melakukan penawaran Efek melalui Layanan Urun Dana, dimana selanjutnya dana tersebut digunakan untuk mendanai pengelolaan jaringan teroris dan kegiatan teroris.

II. PENERAPAN PROGRAM APU DAN PPT BERBASIS RISIKO (*RISK BASED APPROACH*)

1. Penerapan program APU dan PPT berbasis risiko (*risk based approach*) mencakup paling sedikit:
   a. pengawasan aktif Direksi dan Dewan Komisaris;
   b. kebijakan dan prosedur;
   c. pengendalian internal;
   d. sistem informasi manajemen; dan
   e. sumber daya manusia serta pelatihan.
2. Penyelenggara berkewajiban menerapkan program APU dan PPT Berbasis Risiko (*Risk Based Approach*) dalam melakukan hubungan usaha dan transaksi dengan Pengguna. Program tersebut antara lain mencakup hal yang diwajibkan dalam Rekomendasi FATF sebagai upaya untuk melindungi Penyelenggara agar tidak dijadikan sebagai sarana Pencucian Uang dan/atau Pendanaan Terorisme.

   Dalam Rekomendasi FATF dinyatakan bahwa Penyelenggara berkewajiban mengidentifikasi, menilai, dan memahami risiko Pencucian Uang dan Pendanaan Terorisme terkait dengan Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*).

Penyelenggara harus melakukan penilaian sendiri (*self-assessment*) terkait risiko TPPU dan/atau TPPT, serta menerapkan proses kerangka kerja manajemen risiko yang efektif. Selain itu, Penyelenggara harus melakukan pendokumentasian dan pengkinian penilaian risiko terkait penerapan program APU dan PPT tersebut.

Penerapan program APU dan PPT berbasis risiko (*risk based approach*) mendukung Penyelenggara dalam menerapkan tindakan pencegahan dan mitigasi risiko yang sepadan dengan risiko TPPU dan/atau TPPT yang teridentifikasi. Penyelenggara selanjutnya dapat mengalokasikan sumber dayanya sesuai dengan profil risiko yang dihadapinya, mengelola pengendalian internal, struktur internal, dan implementasi kebijakan dan prosedur untuk mencegah serta mendeteksi Pencucian Uang dan/atau Pendanaan Terorisme.

Dalam penerapan program APU dan PPT 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 sehingga Penyelenggara harus tanggap dan mempertimbangkan perubahan risiko tersebut.

3. Konsep Risiko

   a. Definisi Risiko

      Risiko didefinisikan sebagai kemungkinan (*likelihood*) suatu kejadian dan dampak. Secara sederhana, risiko 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, risiko diartikan:

      1) pada tingkat nasional, adalah suatu ancaman dan kerentanan yang disebabkan oleh Pencucian Uang dan/atau Pendanaan Terorisme yang membahayakan sistem keuangan nasional serta keselamatan dan keamanan nasional; dan

      2) pada tingkat Penyelenggara, adalah suatu ancaman dan kerentanan yang menempatkan Penyelenggara pada risiko

dimana Penyelenggara digunakan sebagai sarana Pencucian Uang dan/atau Pendanaan Terorisme.

Ancaman dapat berupa pihak atau objek yang dapat menyebabkan kerugian. Dalam konteks Pencucian Uang dan Pendanaan Terorisme, 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/atau TPPT, kerentanan diartikan pengendalian internal 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/atau TPPT.

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, proses dimaksud mencakup pemahaman terhadap risiko Pencucian Uang dan/atau Pendanaan Terorisme, penilaian atas kedua risiko tersebut, dan pengembangan metode untuk mengelola dan melakukan mitigasi risiko yang telah diidentifikasi.

Dalam menerapkan manajemen risiko atas risiko Pencucian Uang dan/atau Pendanaan Terorisme, Penyelenggara dapat mengembangkan metode manajemen risiko sesuai dengan karakteristik Penyelenggara dengan tetap mengacu pada peraturan perundang-undangan yang mengatur mengenai APU dan PPT.

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 profil risiko Pencucian Uang dan/atau Pendanaan Terorisme dari Calon Nasabah atau Nasabah, yang mencakup paling sedikit 4 (empat) faktor risiko, yaitu Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*). 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/atau Pendanaan Terorisme, pendekatan berbasis risiko (*risk based approach*) adalah suatu proses yang meliputi hal sebagai berikut:

1) penilaian risiko yang mencakup paling sedikit 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 melakukan mitigasi risiko Pencucian Uang dan/atau Pendanaan Terorisme melalui pelaksanaan pengendalian internal dan melakukan langkah-langkah yang sesuai dengan risiko yang telah diidentifikasi, serta melakukan pemantauan transaksi sesuai dengan tingkat risiko Pencucian Uang dan/atau Pendanaan Terorisme yang telah dinilai.
4) Dalam melakukan identifikasi, penilaian, pengelolaan, dan mitigasi risiko Pencucian Uang dan/atau Pendanaan Terorisme, 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 Pencucian Uang dan/atau Pendanaan Terorisme secara berkala sesuai dengan kebutuhan Penyelenggara.

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 pembaruan Teknologi Informasi 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) menerapkan pendekatan berbasis risiko (*risk based approach*)

4) menyusun langkah mitigasi dan pengendalian risiko;

5) melakukan evaluasi atas risiko residu (*residual risk*); 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*) 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 R*isk)

1) Dalam melakukan identifikasi risiko bawaan (*inherent risk*), Penyelenggara harus mempertimbangkan kerentanan Penyelenggara untuk digunakan sebagai

sarana Pencucian Uang dan/atau Pendanaan Terorisme. Langkah awal dalam melakukan penilaian risiko adalah dengan memahami kegiatan usaha Penyelenggara secara keseluruhan dengan perspektif yang luas. Pemahaman tersebut memungkinkan Penyelenggara untuk mempertimbangkan risiko Pencucian Uang dan/atau Pendanaan Terorisme yang mungkin terjadi, apakah risiko terjadi pada sisi Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*).

2) Penyelenggara harus mempertimbangkan unsur yang memicu timbulnya risiko bagi Penyelenggara, baik dari sisi Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, dan/atau jaringan distribusi (*delivery channels*). Penyelenggara harus memahami unsur apa saja yang merupakan risiko bawaan (*inherent risk*) dan risiko residu (*residual risk*).

3) Risiko Nasabah

Penyelenggara harus memperhatikan risiko Pencucian Uang dan Pendanaan Terorisme terkait profil Calon Nasabah atau Nasabah. Penyelenggara perlu mengategorikan Nasabah berdasarkan tingkat risiko Pencucian Uang dan/atau Pendanaan Terorisme, dengan mengacu pada klasifikasi risiko yang ditetapkan oleh Penyelenggara.

4) Risiko Nasabah yang terkait dengan kekhasan bisnis proses Penyelenggara meningkat apabila:

a) Nasabah PEP, termasuk anggota keluarga atau pihak yang terkait (*close associates*) dari PEP;

b) Nasabah terdeteksi menggunakan *virtual private network* yang ditujukan untuk menyamarkan IP *address* pada saat mengakses aplikasi Penyelenggara;

c) Nilai investasi dari Pemodal memiliki nilai nominal yang besarnya tidak sesuai dengan profil Pemodal dimaksud (melewati batas kewajaran);

d) intensitas investasi oleh Pemodal melewati batas kewajaran termasuk yang berada di luar kebijakan yang normal/wajar atau yang berada di luar kebiasaan;

e) Pemodal atau Penerbit bertindak untuk Pemilik Manfaat (*Beneficial Owner*);

f) Pemodal yang mencari atau memilih penawaran Penerbit melalui Penyelenggara yang tidak sesuai dengan kebutuhan atau tidak menguntungkan Pemodal tersebut;

g) Nasabah atau Pemilik Manfaat (*Beneficial Owner*) memberikan informasi yang sangat minim atau informasi yang patut diduga sebagai informasi fiktif;

h) Nasabah atau Pemilik Manfaat (*Beneficial Owner*) mengaburkan atau tidak menyampaikan identitas yang sebenarnya;

i) *gatekeeper*, seperti profesi penunjang di pasar modal, antara lain akuntan, konsultan hukum, penilai, notaris, atau profesi lainnya yang bertindak mewakili Nasabah sehubungan dengan rekening pada Penyelenggara;

j) Pemodal berbentuk korporasi yang struktur kepemilikannya kompleks atau menimbulkan kesulitan untuk diidentifikasi siapa yang menjadi Pemilik Manfaat (*Beneficial Owner*), pemilik akhir (*ultimate owner*), atau pengendali akhir (*ultimate controller*) dari korporasi;

k) Nasabah merupakan organisasi amal atau organisasi non-profit lainnya yang tidak diatur dan diawasi oleh lembaga atau otoritas berwenang;

l) Pemodal merupakan lembaga yang diawasi otoritas/ lembaga pengatur dan pengawas lain yang belum menerapkan program APU dan PPT secara efektif;

m) Pemodal atau Penerbit melakukan perubahan nomor rekening yang tercatat pada Penyelenggara; dan/atau

n) risiko penggunaan identitas palsu dalam bentuk pemalsuan identitas, yaitu *impersonation identities*

(menirukan identitas) dan *synthetic identities* (menggabungkan identitas asli dan palsu). *Impersonation identities* 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.

5) Risiko Negara/Area Geografis/Yurisdiksi

Dalam melakukan penilaian risiko, Penyelenggara harus mengidentifikasi risiko terkait 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/atau Pendanaan Terorisme terkait negara/area geografis/yurisdiksi meningkat apabila:

a) Pemodal atau Penerbit memiliki hubungan afiliasi dengan orang perseorangan dan/atau korporasi dari negara atau yurisdiksi berisiko tinggi;
b) Pemodal atau Penerbit berdomisili di wilayah yang berisiko tinggi;
c) Pemodal atau Penerbit terdeteksi mengakses aplikasi Penyelenggara saat berada di wilayah yang berisiko tinggi;
d) Pemodal atau Penerbit terdeteksi mengakses aplikasi Penyelenggara saat berada di daerah perbatasan antar negara;
e) Pemodal berdomisili di wilayah daerah perbatasan antar negara; dan/atau
f) Pemodal atau Penerbit tidak diketahui wilayah domisili aslinya (menggunakan IP *address* palsu).

Indikator yang menentukan suatu negara/area geografis/yurisdiksi berisiko tinggi terhadap Pencucian Uang dan Pendanaan Terorisme antara lain:

a) yurisdiksi yang oleh organisasi yang melakukan *mutual assessment* terhadap suatu negara (seperti:

Financial Action Task Force (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), *Grupo de Accion Financiera de Sudamerica* (GAFISUD), *Inter Governmental Action Group Against Money Laundering in West 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); atau

g) negara atau yurisdiksi yang diidentifikasi oleh lembaga yang dipercaya, sebagai penyandang dana atau mendukung kegiatan terorisme, atau yang membolehkan kegiatan organisasi teroris di negaranya.

6) Risiko Produk/Jasa/Transaksi

Penilaian risiko secara keseluruhan harus mencakup penentuan risiko yang dapat terjadi atas berbagai produk/jasa/transaksi yang ditawarkan.

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

a) Efek bersifat ekuitas berupa saham yang terkait dengan pembiayaan usaha berisiko tinggi seperti pembiayaan properti, pembiayaan kredit konsumtif (kredit kendaraan bermotor), serta pembiayaan kegiatan ekspor dan impor; atau

b) Efek bersifat utang dan/atau sukuk yang berupa *project financing* berisiko tinggi.

7) 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.

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. Selain itu, Penyelenggara perlu pula memperhatikan risiko *borderless* sebagai bagian yang dapat meningkatkan risiko jaringan distribusi (*delivery channels*), dimana media yang digunakan untuk melakukan transaksi *borderless* memiliki risiko yang lebih tinggi dibanding dengan transaksi non-*borderless*.

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*) menggunakan aplikasi telepon genggam ataupun *website* di internet telah lumrah, namun hal tersebut tetap perlu

dipertimbangkan sebagai bagian dari faktor yang dapat menyebabkan risiko Pencucian Uang dan/atau Pendanaan Terorisme menjadi lebih tinggi.

Beberapa indikator yang menyebabkan jaringan distribusi (*delivery channels*) berisiko tinggi, antara lain aplikasi online yang tidak teruji kehandalan dan keamanannya, khususnya terkait kerahasiaan data Nasabah.

8) Risiko Relevan Lainnya

Faktor lain yang relevan yang dapat memberikan dampak pada risiko Pencucian Uang dan/atau Pendanaan Terorisme antara lain:

a) perkembangan modus dan tipologi Pencucian Uang dan/atau Pendanaan Terorisme;
b) model bisnis, skala usaha, dan jumlah karyawan sebagai faktor risiko bawaan (*inherent risk*) Penyelenggara;
c) total nilai dan intensitas transaksi yang tinggi sehingga memerlukan mitigasi risiko yang memadai;
d) penggunaan Teknologi Informasi dalam seluruh rangkaian proses bisnis Penyelenggara;
e) keamanan data dari risiko serangan siber (*cyberattacks*), dimana 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, dimana 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 lainya; dan/atau

h) pusat penyimpanan data (*data center*) dan pusat pemulihan bencana (*disaster recovery center*), dimana 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 mengulangi proses pengumpulan data kembali.

9) Penyelenggara perlu mempertimbangkan bahwa faktor risiko sebagaimana dimaksud pada angka 3) sampai dengan angka 8) di atas dapat saling terkait antara 1 (satu) faktor risiko dengan faktor risiko lainnya.

10) Indikator yang dapat meningkatkan risiko tidak terbatas pada indikator sebagaimana dimaksud pada angka 3) sampai dengan angka 8). Indikator yang dapat meningkatkan risiko tersebut dapat berkembang sesuai dengan kompleksitas kegiatan usaha Penyelenggara.

11) Setelah melakukan identifikasi dan dokumentasi risiko bawaan (*inherent risk*), Penyelenggara perlu memberikan penilaian terkait tingkat pada setiap risiko dari Calon Nasabah, misalnya rendah (*low*), sedang (*medium*), dan tinggi (*high*).

12) Untuk membantu Penyelenggara melakukan evaluasi penilaian risiko, Penyelenggara dapat menggunakan matriks kemungkinan (*likelihood*) dan dampak (*consequence*) sebagaimana tercantum dalam Lampiran

yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

13) 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.

14) 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.

15) 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.

16) Penyelenggara harus menyediakan informasi yang telah terdokumentasi, yang menunjukkan bahwa Penyelenggara telah secara khusus memperhatikan indikator yang berisiko tinggi dalam penilaian risikonya.

17) Dalam rangka mengidentifikasi risiko TPPU dan/atau TPPT dan menetapkan skala risiko dari Calon Nasabah pada saat pembukaan hubungan usaha atau Nasabah pada saat melakukan transaksi, Penyelenggara dapat menggunakan *regulatory technology* seperti *big data analytic*, *artificial intelligence*, *machine learning*, dan/atau *robo advisor*.

18) Pemanfaatan *regulatory technology* dalam penerapan program APU dan PPT bagi Penyelenggara dapat pula dilakukan oleh Penyelenggara pada saat verifikasi secara elektronik, pemantauan transaksi (*monitoring transaction*), dan penetapan *red flag alert*, dengan memperhatikan keamanan data dan informasi Nasabah.

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, dimana risiko ini paling sedikit mencakup pemenuhan ketentuan sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan mengenai penerapan program anti pencucian uang dan pencegahan pendanaan terorisme di sektor jasa keuangan 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) Penyelenggara harus menetapkan toleransi risiko sebelum mempertimbangkan mitigasi risiko.

3) Pada saat mempertimbangkan ancaman, konsep toleransi risiko akan memberikan kemampuan kepada Penyelenggara untuk menentukan tingkat ancaman risiko yang dapat ditoleransi oleh Penyelenggara.

4) Dalam menetapkan toleransi risiko, Penyelenggara perlu mempertimbangkan kategori risiko 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. Penerapan Pendekatan Berbasis Risiko (*Risk Based Approach*)

1) Penyelenggara berkewajiban menerapkan program APU dan PPT dengan pendekatan berbasis risiko (*risk based approach*) yang didasarkan pada hasil penilaian risiko Pencucian Uang dan/atau Pendanaan Terorisme.

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 seluruh pegawai, khususnya pegawai yang melakukan identifikasi dan penatausahaan

data dan informasi Nasabah serta pelaporan transaksi kepada otoritas terkait.

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/atau Pendanaan Terorisme. Penyelenggara harus 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 internal, dan mitigasi risiko Pencucian Uang dan/atau Pendanaan Terorisme 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 internal 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 terkait Pencucian Uang dan/atau Pendanaan Terorisme;

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).

d. Langkah Mitigasi dan Pengendalian Risiko

1) Mitigasi risiko merupakan penerapan pengendalian internal untuk membatasi risiko Pencucian Uang dan/atau Pendanaan Terorisme yang telah diidentifikasi dalam penilaian risiko. Mitigasi risiko membantu Penyelenggara untuk memastikan kegiatan usahanya 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 sebelumnya.

2) Mitigasi risiko dilakukan dalam penerapan 5 (lima) pilar penerapan program APU dan PPT secara efektif dan memadai yang mencakup paling sedikit:

a) pengawasan aktif Direksi dan Dewan Komisaris;

b) kebijakan dan prosedur;
c) pengendalian internal;
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.
4) Pengendalian internal 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 internal yang berpengaruh dalam melakukan mitigasi 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 internal yang memadai 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 verifikasi serta 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 internal secara konsisten.

e. Evaluasi atas Risiko Residu (*Residual risk)*

1) Risiko residu (*residual risk*) merupakan risiko yang tersisa setelah penerapan pengendalian internal 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 dari pada toleransi risiko, atau dalam hal pengendalian internal 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 risiko yang telah ditetapkan.

3) Ciri-ciri risiko residu (*residual risk*) adalah:

a) risiko telah ditoleransi/diterima:

Dalam risiko ini, risiko tetap ada meskipun telah dilakukan mitigasi risiko sesuai dengan toleransi risiko Penyelenggara. Risiko yang ditoleransi dapat meningkat dari waktu ke waktu. Sebagai contoh, ketika adanya ancaman baru Pencucian Uang dan/atau Pendanaan Terorisme.

b) risiko telah dimitigasi:

Dalam risiko ini, risiko tetap ada meskipun telah dimitigasi. Risiko ini telah dikurangi, tetapi tetap tidak dapat dihilangkan. Dalam praktiknya, pengendalian internal yang telah ditetapkan mungkin tidak dapat diterapkan. Sebagai contoh, 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.

f. Peninjauan dan Evaluasi Pendekatan Berbasis Risiko (*Risk Based Approach*)

1) Penilaian risiko Pencucian Uang dan/atau Pendanaan Terorisme yang dimiliki oleh Penyelenggara harus dievaluasi berdasarkan kebutuhan untuk menguji efektivitas dari kepatuhan penerapan program APU dan PPT, yang meliputi:

a) pengawasan aktif Direksi dan Dewan Komisaris;

b) kebijakan dan prosedur;

c) sistem informasi manajemen;

d) pengendalian internal;

e) kebutuhan sumber daya manusia yang memiliki pengetahuan dan kemampuan dibidang Teknologi Informasi serta bisnis proses Penyelenggaraan Layanan Urun Dana;

f) program pelatihan sumber daya manusia bagi karyawan, pejabat senior serta Direksi dan Dewan Komisaris terkait penerapan program APU dan PPT; dan/atau

g) profil pegawai termasuk pembuatan profil (*profiling*) data identitas serta kompetensi pegawai.

2) Dalam hal terdapat perubahan struktur kegiatan usaha, adanya penawaran atas produk dan jasa baru, dan teknologi baru, pengkinian atas penilaian risiko harus dilakukan untuk kebijakan dan prosedur, langkah mitigasi, dan pengendalian internal.
3) Peninjauan atas penilaian risiko Pencucian Uang dan/atau Pendanaan Terorisme harus mencakup seluruh unsur termasuk kebijakan dan prosedur terhadap penilaian risiko, mitigasi risiko dan pemantauan berkelanjutan yang lebih intensif. Peninjauan atas penilaian risiko 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 Penyelenggara. Pada akhirnya, prosedur peninjauan atas penilaian risiko dimaksud akan mempengaruhi efektivitas dari pelaksanaan pendekatan berbasis risiko (*risk based approach*) dalam menerapkan program APU dan PPT.
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 risiko terhadap Pencucian Uang dan/atau Pendanaan Terorisme 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

Dalam melakukan pengawasan aktif, Direksi paling sedikit:

a. memastikan Penyelenggara memiliki kebijakan dan prosedur penerapan program APU dan PPT;

b. mengusulkan kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT kepada Dewan Komisaris termasuk mitigasi risiko Pencucian Uang dan Pendanaan Terorisme 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 ditunjuk sebagai penanggung jawab penerapan program APU dan PPT;
   3) kebijakan dan prosedur program APU dan PPT;
   4) pengawasan atas penerapan program APU dan PPT; dan
   5) rencana pengendalian internal;

c. membentuk UKK dan/atau menunjuk pejabat yang bertanggung jawab terhadap penerapan program APU dan PPT;

d. memberikan arahan yang jelas atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme;

e. memastikan bahwa kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT sejalan dengan perubahan dan pengembangan produk, jasa, dan teknologi di sektor jasa keuangan serta sesuai dengan perkembangan modus Pencucian Uang dan/atau Pendanaan Terorisme;

f. memastikan dilaksanakannya program APU dan PPT sesuai dengan kebijakan dan prosedur tertulis yang telah ditetapkan;

g. melakukan pengawasan atas kepatuhan unit kerja dalam menerapkan program APU dan PPT, termasuk memantau pelaksanaan tugas UKK dan/atau pejabat yang bertanggung jawab atas penerapan program APU dan PPT;

h. melakukan pengawasan dan mitigasi risiko secara aktif, khususnya yang terkait dengan risiko Nasabah, risiko area/geografis/yurisdiksi, risiko produk/jasa/transaksi, dan risiko jaringan distribusi (*delivery channels*);

i. memastikan bahwa seluruh pegawai telah mengikuti pelatihan yang berkaitan dengan penerapan program APU dan PPT secara berkala;

j. memberikan persetujuan yang bersifat teknis atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan/atau Pendanaan Terorisme 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 Pencucian Uang dan/atau Pendanaan Terorisme; dan

l. memastikan kerahasiaan data/informasi yang dikelola oleh Penyelenggara.

2. Pengawasan Aktif Dewan Komisaris

Dalam melakukan pengawasan aktif, Dewan Komisaris paling sedikit:

a. memberikan persetujuan atas kebijakan dan prosedur tertulis penerapan program APU dan PPT yang diusulkan Direksi termasuk mitigasi risiko Pencucian Uang dan/atau Pendanaan Terorisme;

b. melakukan pengawasan atas pelaksanaan tugas dan tanggung jawab Direksi terhadap penerapan program APU dan PPT; dan

c. memastikan adanya pembahasan terkait Pencucian Uang dan/atau Pendanaan Terorisme dalam rapat Direksi dan Dewan Komisaris;

Rapat pembahasan Direksi dan Dewan Komisaris terkait Pencucian Uang dan/atau Pendanaan Terorisme harus memperhatikan:

1) intensitas pelaksanaan rapat pembahasan diserahkan kepada Penyelenggara sesuai dengan kebutuhan dan kompleksitas usaha Penyelenggara;

2) materi pembahasan dalam rapat Direksi dan Dewan Komisaris dapat berupa antara lain:

a) mitigasi risiko Pencucian Uang dan/atau Pendanaan Terorisme yang ada di Penyelenggara;

b) penanganan permasalahan dan/atau hambatan yang dihadapi Penyelenggara dalam menerapkan program APU dan PPT;

c) pembaruan ketentuan peraturan perundang-undangan dan modus atau tipologi terkait APU dan PPT;

d) efektivitas penerapan program APU dan PPT; dan

3) 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, Direksi dan Dewan Komisaris harus:

a. memiliki pemahaman yang memadai mengenai risiko Pencucian Uang dan/atau Pendanaan Terorisme yang melekat pada seluruh aktivitas operasional Penyelenggara sehingga Direksi dan Dewan Komisaris mampu mengelola dan memitigasi risiko tersebut secara memadai sesuai dengan ketentuan peraturan perundang-undangan;

b. memiliki pemahaman terkait risiko bawaan (*inherent risk)* yang meliputi 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, termasuk memastikan penanggung jawab APU dan PPT berada dalam struktur organisasi; dan

d. bertanggung jawab atas kebijakan dan prosedur, penerapan dan pengawasan penerapan program APU dan PPT, termasuk pengelolaan dan mitigasi risiko Pencucian Uang dan/atau Pendanaan Terorisme pada seluruh aktivitas operasional Penyelenggara.

4. Penanggung Jawab Penerapan Program APU dan PPT

a. Penyelenggara harus memiliki penanggung jawab penerapan program APU dan PPT.

b. Penanggung jawab penerapan program APU dan PPT harus berada dalam struktur organisasi Penyelenggara.

c. Penentuan dan keberadaan penanggung jawab penerapan program APU dan PPT 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 berupa UKK maka harus memenuhi ketentuan sebagai berikut:
   1) paling sedikit terdiri dari 2 (dua) orang yaitu 1 (satu) orang pimpinan dan 1 (satu) orang pelaksana;
   2) tidak merangkap fungsi lain; dan
   3) berada dalam struktur organisasi Penyelenggara.

e. Dalam hal penanggung jawab penerapan program APU dan PPT 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 melapor dan bertanggung jawab kepada Direksi yang memiliki tugas mengawasi penerapan program APU dan PPT.

g. Penanggung jawab penerapan program APU dan PPT dapat dilaksanakan oleh salah satu anggota Direksi. Dalam hal anggota Direksi ditunjuk sebagai penanggung jawab penerapan program APU dan PPT, anggota Direksi tersebut tidak boleh melaksanakan fungsi lainnya dan hanya dapat melaksanakan fungsi kepatuhan dan manajemen risiko.

h. UKK dan/atau pejabat penanggung jawab penerapan program APU dan PPT harus:
   1) independen terhadap kegiatan yang menjadi tanggung jawabnya;
   2) memiliki kemampuan yang memadai dalam menerapkan program APU dan PPT yang dibuktikan antara lain pernah mengikuti pelatihan APU dan PPT atau sertifikasi APU dan PPT;
   3) mampu memberikan informasi yang dibutuhkan oleh Direksi untuk mendapatkan gambaran tentang kondisi,

risiko, dan mitigasi risiko penerapan program APU dan PPT; dan

4) memiliki akses data dan informasi ke seluruh unit kerja untuk melihat, memperoleh, serta menganalisis dokumen terkait penerapan program APU dan PPT, seperti dokumen identifikasi Nasabah, rekening Nasabah, dan daftar transaksi Nasabah.

IV. KEBIJAKAN DAN PROSEDUR

1. Kebijakan dan prosedur penerapan program APU dan PPT berdasarkan pendekatan berbasis risiko memuat paling sedikit:
   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 yang berkelanjutan terkait dengan Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*);
   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 dalam angka 1 harus memperhatikan Prinsip Mengenali Pengguna Jasa (PMPJ/*Know Your Costumer* (KYC)).
3. PMPJ/KYC yang terdiri atas CDD dan EDD dilakukan tidak hanya kepada Calon Nasabah pada saat Calon Nasabah melakukan registrasi sebagai Pengguna, tetapi juga terhadap Nasabah melalui pemantauan transaksi Nasabah pada Penyelenggara.
4. Melalui CDD atau EDD:
   a. Penyelenggara dapat memperoleh informasi secara detail mengenai Calon Nasabah, Nasabah, transaksi Nasabah termasuk transaksi mencurigakan.

b. Penyelenggara dapat melindungi reputasi dan integritas Penyelenggara, memfasilitasi kepatuhan terhadap ketentuan, dan melindungi Penyelenggara dari ancaman eksternal yaitu digunakan sebagai sarana Pencucian Uang dan/atau Pendanaan Terorisme; dan

c. 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 berkewajiban menyampaikan laporan TKM kepada PPATK.

5. 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 TKM yang terkait dengan Pencucian Uang dan/atau Pendanaan Terorisme; atau
   d. Penyelenggara meragukan kebenaran informasi yang diberikan oleh Calon Nasabah, Nasabah, penerima kuasa, dan/atau Pemilik Manfaat (*Beneficial Owner*).
6. CDD ulang dapat dilakukan oleh Penyelenggara apabila Penyelenggara menilai terdapat perubahan tingkat risiko yang disebabkan antara lain terdapat:
   a. peningkatan nilai transaksi yang signifikan;
   b. perubahan profil Nasabah yang bersifat signifikan; dan/atau
   c. informasi pada profil Nasabah yang tersedia dalam nomor tunggal identitas pemodal *(single investor identification)* belum dilengkapi dengan dokumen pendukung dalam rangka verifikasi.
7. Identifikasi Calon Nasabah atau Nasabah
   a. Penyelenggara berkewajiban mengidentifikasi dan mengklasifikasikan Calon Nasabah atau Nasabah ke dalam kelompok orang perseorangan (*natural person*), korporasi (*legal person*), 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 harus 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 Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU dan PPT di sektor jasa keuangan;

2) penelitian atas kebenaran dokumen pendukung identitas Calon Nasabah sebagaimana dimaksud pada angka 1);

3) permintaan lebih dari satu jenis dokumen identitas Calon Nasabah 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 formulir elektronik dan penyampaian salinan dokumen sebagaimana dimaksud dalam Pasal 20, Pasal 21, Pasal 22, Pasal 23, dan Pasal 24 Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU dan PPT di sektor jasa keuangan dalam bentuk *softcopy* melalui laman atau aplikasi Penyelenggara.

g. Selain salinan dokumen sebagaimana dimaksud dalam huruf f, Penyelenggara dapat meminta data, dokumen, dan informasi tambahan yang dibutuhkan dalam mengidentifikasi dan memverifikasi Calon Nasabah atau Nasabah yang penyampaiannya dilakukan melalui laman atau aplikasi Penyelenggara. Adapun contoh data, dokumen, dan informasi tambahan tersebut antara lain untuk:

1) Calon Nasabah atau Nasabah orang perseorangan, antara lain alamat *e-mail*, *softcopy* dokumen identitas tambahan yang dikeluarkan oleh pihak atau yang berwenang, dan foto wajah (swafoto);
2) Calon Nasabah atau Nasabah korporasi, antara lain:
   a) alamat *e-mail* dan nomor telepon korporasi; dan
   b) nama, alamat *e-mail*, 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) Calon Nasabah atau Nasabah perikatan lainnya (*legal arrangement*), antara lain:
   a) perikatan lainnya berupa *trust,* data, informasi terkait nama, alamat *e-mail*, 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) perikatan lainnya dalam bentuk selain *trust* yakni data, informasi terkait nama, alamat *e-mail*, 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) Calon Nasabah yang merupakan Pemodal berupa lembaga negara, instansi pemerintah, lembaga internasional atau perwakilan negara asing, antara lain nama, alamat *e-mail*, 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.

8. 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 dilakukan dengan:

1) pertemuan langsung (*face to face*) dengan Calon Nasabah pada awal melakukan hubungan usaha;

2) mencocokkan kesesuaian profil Calon Nasabah, foto wajah (swafoto), dan foto identitas Nasabah;

3) mencocokkan kesesuaian dokumen identitas sidik jari, dan/atau foto wajah (swafoto) dengan dokumen identitas atau dokumen lainnya yang mencantumkan tanda tangan, sidik jari, dan/atau foto wajah (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) Dalam hal diperlukan, melakukan pengecekan silang 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 Negara 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;

c) dalam hal verifikasi *face to face* dilakukan menggunakan sarana elektronik milik pihak ketiga, maka pihak ketiga diwajibkan untuk mendapat persetujuan dari Otoritas Jasa Keuangan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU dan PPT di sektor jasa keuangan;

d) verifikasi *face to face* melalui sarana elektronik milik Penyelenggara dilakukan dalam bentuk sarana elektronik yang setara dengan *video banking* secara *real time* dan *online* mempertemukan secara elektronik pegawai/pejabat Penyelenggara dengan Calon Nasabah atau Nasabah.

   Contoh: Fitur *video call* pada aplikasi yang dimiliki Penyelenggara yang terhubung langsung secara *real time* dan *online* dengan pegawai/pejabat Penyelenggara melalui *smartphone,* komputer, dan/atau tablet milik Calon Nasabah atau Nasabah;

e) verifikasi *face to face* melalui sarana elektronik milik pihak ketiga dilakukan dalam bentuk *video banking* atau yang setara dengan *video banking* secara *real time* dan *online* mempertemukan secara elektronik pegawai/pejabat Penyelenggara dengan Calon Nasabah atau Nasabah;

f) verifikasi *face to face* secara elektronik milik Penyelenggara atau pihak ketiga tidak boleh

dilakukan dengan menggunakan provider yang secara umum menyediakan sarana elektronik, seperti *whatsapp call, line call*, dan *skype*; dan

g) untuk memberikan tambahan keyakinan bagi Penyelenggara dalam melaksanakan proses verifikasi *face to face* melalui sarana elektronik milik Penyelenggara atau pihak ketiga, 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 Calon Nasabah atau Nasabah dilengkapi dengan fitur pendukung verifikasi seperti kamera, pemindai, perekam, dan/atau pelacak lokasi;

b) verifikasi *non-face to face* diwajibkan untuk memanfaatkan data kependudukan yang memenuhi 2 (dua) faktor otentikasi yang 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 perundang-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 dimana *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) dimana 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), *e-mail* verifikasi, 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 lainnya yang dipadankan dengan *database* Penyelenggara.

9. Identifikasi Calon Nasabah atau Nasabah Berisiko Tinggi atau PEP

a. Dalam hal Penyelenggara menilai Calon Nasabah atau Nasabah Berisiko Tinggi atau PEP, maka Penyelenggara berkewajiban 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 identifikasi Calon Nasabah atau Nasabah sebagaimana dimaksud pada angka 7.

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 formulir elektronik dan penyampaian salinan dokumen sebagaimana dimaksud dalam Pasal 20, Pasal 21, Pasal 22, Pasal 23, dan Pasal 24 Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU dan PPT di sektor jasa keuangan secara elektronik (*softcopy*) melalui laman atau aplikasi Penyelenggara.

f. Selain salinan dokumen sebagaimana dimaksud dalam huruf e, Penyelenggara dapat meminta data, dokumen, dan informasi tambahan yang dibutuhkan dalam mengidentifikasi dan memverifikasi Calon Nasabah secara elektronik yang penyampaiannya dilakukan melalui laman atau aplikasi Penyelenggara. Adapun contoh data, dokumen, dan informasi tambahan tersebut antara lain dapat berupa data dan informasi sebagaimana dimaksud dalam angka 7 huruf g mengenai identifikasi Calon Nasabah atau Nasabah.

10. Verifikasi Calon Nasabah atau Nasabah Berisiko Tinggi atau PEP

a. Verifikasi Calon Nasabah dan Nasabah Berisiko Tinggi atau PEP dilaksanakan dengan memperhatikan ketentuan sebagaimana dimaksud dalam angka 8 huruf a, huruf b, huruf c, huruf d, dan huruf e.

b. Selain memperhatikan 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:

1) meminta atau mencari informasi tambahan mengenai profil Nasabah, seperti pekerjaaan, sumber dana, sumber kekayaan Nasabah;
2) melakukan pengkinian atas data identitas Nasabah;
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/atau
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 memperhatikan ketentuan sebagaimana dimaksud dalam angka 8 huruf g.

11. 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, dilakukan untuk kepentingan:
   a) Calon Nasabah atau Nasabah; atau
   b) 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 (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*) berdasarkan data dan/atau informasi yang disampaikan oleh Calon Nasabah.

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 yang dapat didasarkan pada ambang batas (*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.
   c) dalam hal tidak ditemukan pemegang saham perseroan yang paling mengendalikan perseroan, 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), huruf, b) dan 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 berkewajiban untuk 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 pada pengisian formulir 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 formulir elektronik dan pengunggahan salinan dokumen identitas sesuai dengan ketentuan mengenai kewajiban untuk melakukan identifikasi dan verifikasi identitas Pemilik Manfaat (*Beneficial Owner*) sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU dan PPT di sektor jasa keuangan, 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) Dalam hal diperlukan, melakukan pengecekan silang 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; atau

(4) melakukan analisis informasi geografis untuk melihat kondisi hutan melalui teknologi *remote sensing* terhadap Calon Nasabah perusahaan yang bergerak di bidang kehutanan; dan/atau

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 Negara Republik Indonesia;

(2) daftar pendanaan Proliferasi Senjata Pemusnah Massal; atau

(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 meliputi kondisi dimana:

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, 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 8 huruf g.

12. CDD Sederhana (*Simplified CDD)*

a. Dalam hal Penyelenggara menilai bahwa Calon Nasabah atau Nasabah berdasarkan hasil penilaian risiko terjadinya TPPU dan/atau TPPT, 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 paling sedikit:

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 dan/atau TPPT;

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 yang dimiliki. Berdasarkan perubahan atas kebijakan dan prosedur APU dan PPT, CDD sederhana akan diberlakukan sejak tanggal 30 Maret, maka Penyelenggara dapat menyampaikan pemberitahuan kepada Otoritas Jasa Keuangan rencana penerapan CDD sederhana tersebut sebelum tanggal 30 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); dan
7) memastikan pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan data dan informasi.

c. Nasabah yang telah mendapatkan perlakuan CDD sederhana (*simplified* CDD) harus dikeluarkan dari daftar Nasabah CDD sederhana (*simplified* CDD) apabila memenuhi kriteria:
   1) diidentifikasikan terkait dengan dugaan Pencucian Uang dan Pendanaan Terorisme;
   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 7 huruf d, huruf e, huruf f, dan huruf g, serta angka 8 huruf g.

13. 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. 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.

c. Dalam hal telah tersedia hasil CDD yang telah dilakukan oleh bank terhadap Calon Nasabah, Penyelenggara dapat menggunakan hasil CDD yang telah dilakukan oleh bank terhadap Calon Nasabah tersebut.

d. 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, dimana 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 dan bukan untuk kepentingan lainnya seperti pemasaran.

   Contoh: kepentingan penerapan program APU dan PPT 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 bersedia memenuhi permintaan informasi dan salinan dokumen pendukung segera pada kesempatan pertama apabila dibutuhkan oleh Penyelenggara dalam rangka penerapan program APU dan PPT.
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.

   Sebagai contoh Penyelenggara dapat menggunakan hasil CDD yang telah dilakukan oleh:
   a) penyedia jasa keuangan di sektor perbankan, pasar modal dan/atau industri keuangan non bank, dimana penyedia jasa keuangan memiliki prosedur CDD yang telah ditetapkan otoritas berwenang yang mengawasinya yaitu Otoritas Jasa Keuangan; atau
   b) perusahaan pialang berjangka komoditi dimana perusahaan pialang berjangka memiliki prosedur

CDD yang telah ditetapkan otoritas berwenang yang mengawasinya yaitu Badan Pengawas Perdagangan Berjangka Komoditi (BAPPEBTI).

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 secara efektif sesuai dengan Rekomendasi FATF;

c) terhadap negara berisiko tinggi telah dilakukan mitigasi risiko secara memadai oleh unit APU dan PPT berdasarkan kebijakan program APU dan PPT 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.

14. 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 yang mengatur 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 berkewajiban 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 berkewajiban melaporkannya kepada PPATK mengenai tindakan penolakan hubungan usaha atau transaksi atau penutupan/pemutusan hubungan usaha tersebut sebagai TKM.

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 tersebut 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.

15. Pengelolaan Risiko Berkelanjutan

a. Penyelenggara harus memiliki kebijakan dan prosedur untuk mengelola risiko berkelanjutan terkait risiko Pencucian Uang dan/atau Pendanaan Terorisme, dimana pengelolaan risiko tersebut tidak hanya dilakukan pada saat Penyelenggara melakukan pembukaan hubungan usaha dengan Calon Nasabah atau transaksi dengan Nasabah.

b. Kebijakan dan prosedur untuk mengelola risiko Pencucian Uang dan/atau Pendanaan Terorisme secara berkelanjutan mencakup:

1) Identifikasi risiko

Dalam melakukan identifikasi risiko, Penyelenggara harus menilai risiko Pencucian Uang dan/atau Pendanaan Terorisme yang melekat pada usahanya dengan mempertimbangkan risiko bawaan (*inherent risk*) seperti risiko 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 yang ada pada Nasabah, sumber dana yang digunakan untuk membeli produk/jasa/transaksi, dan pola transaksi Nasabah dalam membeli produk dan jasa; dan

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

16. 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 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 di dalamnya 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 undang-undang mengenai dokumen perusahaan;

3) dokumen yang ditatausahakan mencakup paling sedikit:

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 TKM.

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 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 PPATK dan/atau aparat penegak hukum.

17. Pengkinian Data Nasabah

a. Penyelenggara harus melakukan pengkinian data Nasabah sesuai dengan ketentuan sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU dan PPT di sektor jasa keuangan secara berkesinambungan dan memastikan bahwa data, informasi, dan/atau 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 terhadap informasi dan dokumen Nasabah sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU dan PPT di sektor jasa keuangan.

c. Kegiatan pengkinian data, informasi, dan/atau dokumen pendukung Nasabah didasarkan pada tingkat risiko Pencucian Uang dan/atau Pendanaan Terorisme 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 menengah, 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 di dalamnya memuat nama Nasabah, tanggal pengkinian Nasabah, cara pengkinian Nasabah (misalnya melalui *e-mail*, 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 nomor tunggal identitas pemodal *(single investor identification)* 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/atau Pendanaan Terorisme;

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 tempat dilakukannya transaksi termasuk *high risk countries*;
8) tercantum dalam daftar terduga teroris dan organisasi teroris;
9) tercantum dalam daftar pendanaan Proliferasi Senjata Pemusnah Massal; dan/atau
10) transaksi yang diduga terkait dengan hasil TPPU dan/atau TPPT.

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 dilakukan pembaruan dan tetap 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:
1) harus memelihara daftar terduga teroris dan organisasi teroris dan daftar pendanaan Proliferasi Senjata Pemusnah Massal;
2) harus 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;

3) harus 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; dan
4) dapat menjadikan daftar terduga teroris dan organisasi teroris dan daftar pendanaan Proliferasi Senjata Pemusnah Massal yang sudah dilakukan pengkinian sebagai alat *screening* pada saat melakukan hubungan usaha dengan Calon Nasabah.

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 j.
2) Penyelenggara dapat melakukan pengkinian melalui otomatisasi yang terkoneksi pada *big data* dengan sumber yang *reliable.*
3) Proses pengkinian data Nasabah dilakukan berdasarkan hasil penilaian risiko secara berkala melalui metode sebagai berikut:
a) menyampaikan notifikasi melalui *e-mail* 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, dimana 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 dimana 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.

18. Pemantauan Nasabah dan Transaksi Nasabah

a. Penyelenggara harus melakukan kegiatan pemantauan yang paling sedikit mencakup:

1) informasi dan dokumen Nasabah;
2) transaksi Nasabah; dan
3) hubungan usaha/transaksi dengan Nasabah Berisiko Tinggi atau PEP.

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*.

4) 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.

19. Rekam Jejak Audit

a. Penyelenggara berkewajiban 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 mencakup paling sedikit:
   1) memelihara log transaksi sesuai kebijakan retensi data Penyelenggara, sesuai peraturan perundang-undangan. Log transaksi berisi kegiatan transaksi yang bersifat utuh dan *real time.*
   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.

20. 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 atau PEP;

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 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 secara keseluruhan sebagaimana kebijakan dan prosedur tertulis yang telah ditetapkan oleh Penyelenggara; dan

6) Direksi dapat mengusulkan pembaruan kebijakan dan prosedur dalam hal terdapat perkembangan risiko yang perlu dimitigasi oleh Penyelenggara yang belum tercantum dalam kebijakan dan prosedur tertulis.

21. Kebijakan dan Prosedur Pelaporan kepada PPATK

a. Penyelenggara harus memiliki kebijakan dan prosedur 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 peraturan perundang-undangan yang mengatur mengenai pencegahan dan pemberantasan TPPT, termasuk peraturan pelaksanaannya antara lain Peraturan Kepala PPATK.

b. Kebijakan dan prosedur kewajiban pelaporan sebagaimana dimaksud pada huruf a paling sedikit mencakup kebijakan dan prosedur pelaporan TKM, laporan terkait daftar pendanaan Proliferasi Senjata Pemusnah Massal, dan laporan lain terkait

penerapan program APU dan PPT dalam hal terdapat permintaan informasi dari PPATK.

22. Kebijakan dan Prosedur Pelaporan kepada Kepolisian Negara Republik Indonesia

Penyelenggara harus memiliki kebijakan dan prosedur kewajiban pelaporan kepada Kepolisian Negara Republik Indonesia mengenai laporan terkait daftar terduga teroris dan organisasi teroris, dan laporan lain terkait penerapan program APU dan PPT dalam hal terdapat permintaan informasi dari Kepolisian Negara Republik Indonesia.

V. PENGENDALIAN INTERNAL

A. KETENTUAN UMUM PENGENDALIAN INTERNAL

1. Penerapan program APU dan PPT berbasis risiko (*risk based approach*) yang efektif harus diimplementasikan dalam pengendalian internal dan diinternalisasikan dalam proses bisnis Penyelenggara.
2. Penyelenggara harus memiliki sistem pengendalian internal untuk memastikan kepatuhan Penyelenggara dalam menerapkan program APU dan PPT secara efektif dan untuk meminimalkan risiko Pencucian Uang dan/atau Pendanaan Terorisme yang dihadapi Penyelenggara.
3. Dalam pengendalian internal, Penyelenggara harus memperhatikan hal-hal sebagai berikut:
   a. skala dan kompleksitas Penyelenggara;
   b. kegiatan usaha atau operasional Penyelenggara, termasuk aspek area geografis/negara, profil Nasabah, produk atau jasa, dan aktivitas transaksi Penyelenggara secara keseluruhan;
   c. jaringan distribusi (*delivery channels*) yang digunakan;
   d. volume dan intensitas 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 internal yang efektif dalam penerapan program APU dan PPT 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;
   b. batasan wewenang dan tanggung jawab satuan kerja terkait dengan penerapan program APU dan PPT, dimana Penyelenggara harus memastikan adanya pemisahan tugas, wewenang dan tanggung jawab yang jelas antara unit khusus pengendalian internal, fungsi atau pejabat yang ditunjuk untuk melaksanakan fungsi pengendalian internal dengan unit bisnis Penyelenggara lainnya;
   c. penunjukan UKK dan/atau pejabat yang bertanggung jawab dalam penerapan program APU dan PPT;
   d. pengkinian standar kepatuhan penerapan program APU dan PPT;
   e. kebijakan, prosedur, dan pemantauan terkait penyaringan/rekrutmen karyawan Penyelenggara, untuk memastikan tidak digunakannya karyawan Penyelenggara sebagai sarana TPPU dan/atau TPPT melalui proses bisnis Penyelenggara;
   f. pemantauan terhadap Nasabah, transaksi Nasabah, dan/atau penggunaan Teknologi Informasi dalam proses bisnis Penyelenggara khususnya yang memiliki risiko tinggi Pencucian Uang dan/atau Pendanaan Terorisme 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 TKM secara akurat;
   h. penyediaan tinjauan rutin atas penilaian risiko dan manajemen proses;
   i. pengawasan yang memadai sebelum penawaran produk atau jasa baru, penggunaan teknologi baru atau

penawaran produk/jasa yang dimodifikasi sedemikian rupa yang berpotensi terhadap peningkatan risiko Pencucian Uang dan/atau Pendanaan Terorisme;

j. penyampaian informasi secara cepat dan tepat dalam hal terdapat indikasi dan/atau dugaan terkait risiko Pencucian Uang dan/atau Pendanaan Terorisme, langkah perbaikan yang dilakukan, hasil identifikasi kelemahan atas peraturan yang dimiliki, rencana tindak lanjut 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 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;

o. pengintegrasian kepatuhan terhadap penerapan program APU dan PPT dalam deskripsi pekerjaan dan evaluasi kinerja yang tepat;

p. pelatihan terkait penerapan program APU dan PPT yang tepat dan relevan untuk semua pegawai;

q. pengujian terhadap efektivitas dari pelaksanaan program APU dan PPT dengan mengambil contoh secara acak (*random sampling*) serta melakukan pendokumentasian atas pengujian yang dilakukan; dan

r. audit independen secara internal untuk menguji kepatuhan dan efektivitas penerapan APU dan PPT yang

pelaksanaannya sesuai dengan kebutuhan dan kompleksitas usaha Penyelenggara.

5. Dalam melakukan pengendalian internal, Penyelenggara dapat menggunakan *regulatory technology* seperti *algoritma*, pemanfaatan teknologi *artificial intelligence*, dan/atau *machine learning*.
6. Dalam hal Penyelenggara melakukan pengendalian internal dengan menggunakan *regulatory technology* sebagaimana dimaksud dalam angka 5, Penyelenggara harus memastikan *regulatory technology* yang digunakan dalam sistem pengendalian internal:
   a. didasarkan pada hasil penilaian risiko yang di dalamnya 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. terjamin keamanan data dan informasinya, termasuk penggunaan *security tools* seperti teknologi enkripsi, penggunaan *anti virus*, dan *firewall*.
7. Penanggung jawab pengendalian internal terkait penerapan program APU dan PPT berbasis risiko sebagaimana dimaksud dalam angka 5 memiliki kewenangan mencakup paling sedikit:
   a. menyusun program dan prosedur audit berbasis risiko dengan prioritas audit pada unit kerja yang tergolong memiliki kompleksitas usaha yang tinggi;
   b. melakukan penilaian atas kecukupan proses yang berlaku di Penyelenggara dalam mengidentifikasi dan melaporkan TKM 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 internal harus:
   a. memastikan pengendalian internal dalam penerapan program APU dan PPT diterapkan dengan baik, tepat dan efektif sesuai dengan kebijakan dan prosedur yang telah ditetapkan serta mencakup kerangka pengendalian internal sebagaimana dimaksud dalam 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. Sistem tersebut memungkinkan pihak internal perusahaan (karyawan) ataupun eksternal seperti Calon Nasabah, Nasabah, atau masyarakat umum untuk 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 WBS.

11. Unit kerja independen yang mengelola sistem pelaporan dugaan terjadinya pelanggaran (WBS) dapat dirangkap oleh pejabat yang ditunjuk sebagai penanggung jawab pengendalian internal.

B. PENGENDALIAN INTERNAL ATAS PENGGUNAAN TEKNOLOGI INFORMASI DALAM PROSES BISNIS PENYELENGGARA.

1. Penyelenggara harus memastikan bahwa pengendalian internal atas penggunaan Teknologi Informasi dalam proses bisnis Penyelenggara cukup memadai dan efektif dalam penerapan program APU dan PPT, dan mampu mengantisipasi kemungkinan Teknologi Informasi yang digunakan Penyelenggara tidak dimanfaatkan sebagai sarana TPPU dan/atau TPPT.
2. Penyelenggara harus memiliki dan menerapkan sistem pengendalian internal secara efektif terhadap seluruh aspek penggunaan Teknologi Informasi yang digunakan dalam penerapan program APU dan PPT, yang memuat paling sedikit:
   a. memiliki dan menerapkan kebijakan, standar, dan prosedur penggunaan Teknologi Informasi yang digunakan dalam penerapan program APU dan PPT 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 keakuratan dokumen dan dokumen pendukung sebelum diinput ke dalam sistem;
   2) pengendalian atas pengolahan serta *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 internal maupun pihak lain.

3. Sistem pengendalian internal secara efektif terhadap seluruh aspek penggunaan Teknologi Informasi sebagaimana dimaksud dalam angka 2 merupakan bagian dari sistem pengendalian internal Penyelenggara secara menyeluruh.

4. Penyelenggara harus memastikan kelangsungan dan kestabilan operasional Teknologi Informasi serta melakukan mitigasi 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 kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*) informasi yang dikelola terjaga 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, 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 meliputi:
   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 yang mengatur mengenai 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 dan/atau kebutuhan informasi dari otoritas lain yang berwenang seperti PPATK dan/atau aparat penegak hukum.

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 memperhatikan kompleksitas usaha, volume transaksi, dan risiko yang dimiliki Penyelenggara, mencakup paling sedikit:
   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 diwajibkan untuk 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 di dalamnya memuat bagaimana Penyelenggara mengelola dan memitigasi risiko atas Teknologi Informasi yang digunakan.
3. Kebijakan dan prosedur tertulis yang dimiliki Penyelenggara diwajibkan untuk mempertimbangkan faktor Teknologi Informasi yang berpotensi disalahgunakan oleh pelaku Pencucian Uang

dan/atau Pendanaan Terorisme, 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 harus memiliki dan memelihara nomor tunggal identitas pemodal *(single investor identification).*
7. Informasi yang terdapat dalam nomor tunggal identitas pemodal *(single investor identification)* mencakup seluruh produk yang dimiliki oleh Pemodal melalui layanan yang diselenggarakan oleh Penyelenggara.
8. 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 di bidang 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 audit atas teknologi informasi (*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; 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 mengenai 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 digunakan oleh Penyelenggara dalam menjalankan kegiatan Layanan Urun Dana 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 dan/atau Pendanaan Terorisme yang melibatkan pihak internal, Penyelenggara berkewajiban melakukan:
   a. prosedur penyaringan dalam rangka penerimaan karyawan baru (*pre-employee screening*) sebagai bagian dari penerapan *know your employee*; 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;
   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 rekam jejak (*track record)* yang baik dari calon karyawan antara lain dengan meminta surat rekomendasi dari perusahaan sebelumnya dimana 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:
   a. melakukan verifikasi terhadap karyawan yang mengalami perubahan gaya hidup yang cukup signifikan;
   b. memastikan bahwa karyawan telah memahami dan menaati kode etik karyawan (*staff code of conduct*); dan
   c. 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 *know your employee* Penyelenggara dengan berpedoman pada ketentuan yang mengatur mengenai penerapan strategi *anti fraud*.

B. PELATIHAN
1. Penyelenggara berkewajiban menyelenggarakan pelatihan yang berkesinambungan tentang kebijakan dan prosedur penerapan program APU dan PPT serta peran dan tanggung jawab karyawan dalam mencegah dan memberantas TPPU dan/atau TPPT kepada seluruh karyawan.
2. Dalam menyelenggarakan pelatihan berkesinambungan sebagaimana dimaksud dalam huruf a, 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; 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, dimana 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. 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 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;
2) tren dan perkembangan profil risiko, teknik, metode, dan tipologi TPPU dan/atau TPPT, khususnya dalam kaitannya dengan proses bisnis Penyelenggara;
3) penggunaan Teknologi Informasi dalam penerapan program APU dan PPT serta mitigasi risiko atas penggunaan Teknologi Informasi dimaksud;
4) penilaian risiko dan penerapan program APU dan PPT berbasis risiko;
5) penerapan kebijakan dan prosedur program APU dan PPT;
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 dan/atau TPPT.

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) Laporan rencana kegiatan pengkinian data Nasabah dan

laporan realisasi kegiatan pengkinian data Nasabah diwajibkan untuk disetujui dan disampaikan oleh Direksi yang membawahi fungsi kepatuhan atau salah satu anggota Direksi yang bertanggung jawab terhadap penerapan program APU dan PPT.

2) 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.

3) Laporan realisasi kegiatan pengkinian Nasabah kepada 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.

4) Laporan rencana kegiatan pengkinian data Nasabah sebagaimana dimaksud dalam angka 2) diwajibkan untuk disampaikan kepada Otoritas Jasa Keuangan setiap tahun paling lambat pada akhir bulan Desember sebelum periode pengkinian data.

   Sebagai contoh, untuk pengkinian data Nasabah dalam kurun waktu Januari sampai dengan Desember 2024, Penyelenggara harus menyampaikan laporan rencana pengkinian data Nasabah paling lambat tanggal 31

Desember tahun 2023.

5) Laporan realisasi pengkinian data sebagaimana dimaksud dalam angka 3) diwajibkan untuk disampaikan kepada 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 2024, Penyelenggara harus menyampaikan laporan realisasi pengkinian data paling lambat tanggal 31 Januari tahun 2025.

6) Laporan rencana pengkinian data Nasabah sebagaimana dimaksud dalam angka 2) untuk pertama kalinya diwajibkan untuk disampaikan paling lambat pada akhir Desember 2023. Sementara Laporan realisasi pengkinian data sebagaimana dimaksud dalam angka 3) untuk pertama kalinya diwajibkan untuk disampaikan paling lambat pada akhir Januari 2025.

7) Dalam hal terdapat perubahan atas laporan rencana kegiatan pengkinian data, yang telah disampaikan kepada Otoritas Jasa Keuangan, Penyelenggara berkewajiban menyampaikan perubahan tersebut paling lambat 7 (tujuh) hari kerja sejak perubahan dilakukan.

8) Surat pengantar penyampaian laporan rencana kegiatan pengkinian data Nasabah sebagaimana dimaksud dalam angka 2) dan laporan realisasi kegiatan pengkinian data Nasabah sebagaimana dimaksud dalam angka 3) yang ditandatangani oleh Direksi serta 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.

9) Dalam hal sistem jaringan komunikasi data Otoritas Jasa Keuangan sebagaimana dimaksud dalam angka 8) belum tersedia, maka surat pengantar penyampaian laporan dan isi laporan dimaksud disampaikan melalui *e-mail*; dan

10) Dalam hal sistem jaringan komunikasi data Otoritas Jasa Keuangan sebagaimana dimaksud dalam angka 8) dan *e-*

mail sebagaimana dimaksud dalam angka 9) 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.

11) Laporan sebagaimana dimaksud dalam angka 2) dan angka 3) disampaikan oleh Penyelenggara kepada Kepala Eksekutif Pengawas Pasar Modal.

b. Laporan Penyesuaian Kebijakan dan Prosedur Penerapan Program APU dan PPT

1) Laporan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT memuat hal-hal perubahan atas penyesuaian kebijakan dan prosedur penerapan program APU dan PPT yang telah disampaikan sebelumnya kepada Otoritas Jasa Keuangan.

2) Laporan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT harus disetujui dan disampaikan oleh Direksi yang membawahi fungsi kepatuhan atau salah satu anggota Direksi yang bertanggung jawab terhadap penerapan program APU dan PPT.

3) Laporan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT diwajibkan untuk 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 pada Senin, 14 November 2023, Penyelenggara harus menyampaikan laporan perubahan penyesuaian kebijakan dan prosedur penerapan program APU dan PPT paling lambat pada 22 November 2023.

4) Laporan sebagaimana dimaksud dalam angka 1) disampaikan oleh Penyelenggara kepada Kepala Eksekutif Pengawas Pasar Modal Otoritas Jasa Keuangan.

2. Laporan kepada PPATK

a. Penyelenggara berkewajiban 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 peraturan perundang-undangan yang mengatur mengenai pencegahan dan pemberantasan TPPT, termasuk peraturan pelaksanaannya antara lain Peraturan Kepala PPATK.

b. Penyelenggara berkewajiban menyampaikan laporan TKM dalam hal ditemukan indikasi TKM.

   Berkaitan dengan TKM sebagai salah satu transaksi keuangan yang diwajibkan untuk 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.

c. Penyelenggara harus menyampaikan laporan terkait daftar pendanaan Proliferasi Senjata Pemusnah Massal berupa laporan pemblokiran secara serta merta dalam hal ditemukan adanya kesesuaian data dan informasi Nasabah dengan daftar pendanaan Proliferasi Senjata Pemusnah Massal atau laporan nihil dalam hal tidak ditemukan adanya kesesuaian data dan informasi Nasabah dengan daftar pendanaan Proliferasi Senjata Pemusnah Massal, dengan tembusan kepada Otoritas Jasa Keuangan.

d. Penyelenggara harus menyampaikan laporan lain terkait penerapan program APU dan PPT dalam hal terdapat permintaan informasi dari PPATK.

3. Laporan kepada Kepolisian Negara Republik Indonesia

   Penyelenggara harus menyampaikan laporan terkait daftar terduga teroris dan organisasi teroris berupa laporan pemblokiran secara serta merta dalam hal ditemukan adanya kesesuaian data dan informasi Nasabah dengan daftar terduga teroris dan organisasi teroris atau laporan nihil dalam hal tidak ditemukan adanya kesesuaian data dan informasi Nasabah dengan daftar terduga teroris dan organisasi teroris, dengan tembusan kepada Otoritas Jasa Keuangan.

IX. KETENTUAN LAIN-LAIN

Ketentuan terkait pencegahan pendanaan Proliferasi Senjata Pemusnah Massal dalam Surat Edaran Otoritas Jasa Keuangan ini bersifat himbauan sampai dengan diwajibkannya penerapan pencegahan pendanaan Proliferasi Senjata Pemusnah Massal bagi Penyelenggara berdasarkan Peraturan Otoritas Jasa Keuangan mengenai penerapan program anti pencucian uang dan pencegahan pendanaan terorisme di sektor jasa keuangan.

X. PENUTUP

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

Ditetapkan di Jakarta
pada tanggal 20 September 2022

KEPALA EKSEKUTIF
PENGAWAS PASAR MODAL
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

INARNO DJAJADI

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN

SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR 17 /SEOJK.04/2022

TENTANG

PEDOMAN PENERAPAN PROGRAM ANTI PENCUCIAN UANG DAN PENCEGAHAN PENDANAAN TERORISME BAGI PENYELENGGARA LAYANAN URUN DANA 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/ Yurisdiksi**	**Risiko Produk/ Jasa/ Transaksi**	**Risiko Jaringan Distribusi**
Nasabah dalam Layanan Urun Dana menggunakan sistem identitas digital dan layanan *non face to face* berdasarkan identifikasi risiko bawaan (*inherent risk*). Dalam kegiatan usaha Penyelenggara memiliki kekhasan, yaitu pengumpulan data pribadi dan verifikasi nasabah dilakukan dengan menggunakan sistem elektronik.	Risiko negara, risiko area geografis, atau risiko yurisdiksi bersama dengan faktor risiko lainnya menyediakan informasi yang bermanfaat untuk penilaian risiko pencucian uang dan pendanaan terorisme.	Produk, jasa atau transaksi yang mungkindapat terpapar risiko yang lebih tinggi terkait TPPU dan TPPT. Selain itu terdapat hal yang dapat meningkatkan profil risiko produk, jasa atau transaksi.	Salah satu ciri khas bisnis Penyelenggara Layanan Urun Dana adalah proses jaringan distribusi (*delivery channels*) yang dilakukan tanpa pertemuan langsung (*non face to face*)
Risiko relevan lainnya terutama yang berkaitan dengan penggunaan sistem elektronik.			

STEP 6 : PENINJAUAN PENDEKATAN BERBASIS RISIKO (*RISK BASED APPROACH*)
Melakukan evaluasi secara berkala atas pendekatan berbasis risiko (*Risk Based Approach*/RBA) untuk menilai efektivitas penerapan program APU dan PPT

STEP 2 : MENETAPKAN TOLERANSI RISIKO
Menetapkan tingkat dan jenis risiko yang dapat ditoleransi oleh Penyelenggara

STEP 5: EVALUASI RISIKO RESIDU
Memastikan risiko residu sesuai dengan toleransi risiko yang telah ditetapkan. (Risiko residu merupakan risiko yang tersisa setelah penerapan pengendalian internal dan mitigasi risiko)

STEP 3 : PENDEKATAN BERBASIS RISIKO
Menerapkan strategi mitigasi dan pengendalian untuk area berisiko tinggi terhadap risiko pencucian uang dan pendanaan terorisme

STEP 4: PENGURANGAN DAN PENGENDALIAN RISIKO
Menerapkan pengendalian internal untuk membatasi risiko pencucian uang dan pendanaan terorisme yang telah diidentifikasi pada saat melakukan penilaian risiko, serta mengembangkan dan menyusun dokumen strategi mitigasi untuk area berisiko tinggi

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

1. Dalam melakukan identifikasi risiko, salah satu alat bantu yang dapat digunakan oleh Penyelenggara adalah matriks kemungkinan dan dampak *(likehood and Consequence 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 yang terjadi untuk setiap risiko tertentu. Dalam hal ini Penyelenggara dapat menggunakan skala risiko yang digunakan secara umum, yaitu:

Peringkat	**Kemungkinan (*Likelihood*) risiko Pencucian Uang dan Pendanaan Terorisme**
Tinggi	Kemungkinan (*likelihood*) risiko Pencucian Uang dan Pendanaan Terorisme terjadi.
Sedang	Kemungkinan (*likelihood*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme dapat diterima.
Rendah	Tidak terdapat kemungkinan (*likelihood*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme.

b. Dampak (*Consequence*)

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

Timbulnya dampak (c*onsequence*) bergantung pada kondisi internal Penyelenggara. Dampak (c*onsequence*) atas terjadinya risiko Pencucian Uang dan Pendanaan Terorisme dapat dilihat dari berbagai sudut pandang, antara lain:

1) risiko reputasi dan dampaknya terhadap kegiatan usaha Penyelenggara;
2) dampak (c*onsequence*) regulasi;
3) kerugian finansial bagi Penyelenggara; dan/atau
4) risiko hukum.

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

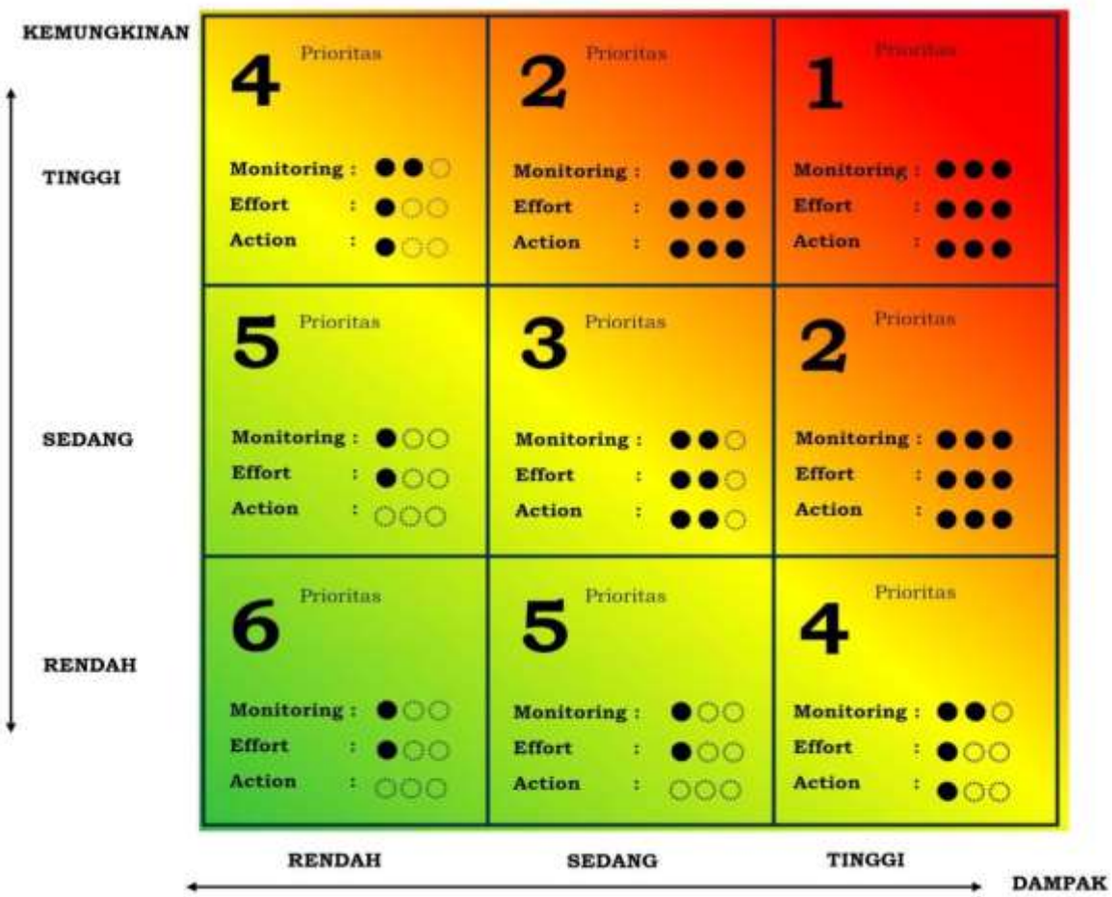
Peringkat	**Konsekuensi atas risiko Pencucian Uang dan Pendanaan Terorisme**
Tinggi	Risiko memiliki konsekuensi yang berat
Sedang	Risiko memiliki konsekuensi yang moderat
Rendah	Risiko memiliki konsekuensi yang kecil atau tidak signifikan.

2. Matriks kemungkinan (*likelihood*) dan dampak (c*onsequence*) 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:

1) *Action* (contoh: risiko perlu segera ditindaklanjuti)
2) *Effort* (contoh: tingkat upaya dalam melakukan mitigasi risiko)
3) *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 (c*onsequence*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme rendah sehingga Penyelenggara tidak perlu mengambil tindakan, upaya, atau pemantauan khusus.

   b. Kotak 5

      Kondisi pada kotak 5 menunjukkan kemungkinan dan dampak (c*onsequence*) terjadinya risiko Pencucian Uang dan Pendanaan Terorisme tergolong rendah, tetapi 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 yang tergolong menengah. Pada kondisi ini, Penyelenggara perlu mengambil tindakan, upaya atau pemantauan. Tindakan, upaya, atau pemantauan yang memadai akan menurunkan kemungkinan dan dampak (c*onsequence*) terjadinya risiko Pencucian Uang dan/atau Pendanaan Terorisme. 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/atau Pendanaan Terorisme dengan dampak (c*onsequence*) 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/atau Pendanaan Terorisme tergolong tinggi. Pada kondisi ini, Penyelenggara perlu memperhatikan seluruh kegiatan usaha dan hubungan usaha dan mengerahkan sumber daya untuk menekan kemungkinan (*likelihood*) dan dampak (c*onsequence*) 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/atau

Pendanaan Terorisme sangat tinggi termasuk besarnya dampak (c*onsequence*) 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 URUN DANA BERBASIS TEKNOLOGI INFORMASI

1. Pengguna diduga bertindak atas nama pihak ketiga, tetapi tidak memberitahu Penyelenggara.
2. Penyelenggara menyadari bahwa Pengguna adalah pelaku yang diduga melakukan TPPU dan/atau TPPT.
3. Penyelenggara menemukan adanya ketidaksesuaian antara profil Pengguna dengan nilai transaksi yang dilakukan.

   Contoh: Pelajar sebagai Pemodal melakukan investasi melalui Penyelenggara dengan nilai ratusan juga atau miliaran rupiah.
4. Penyelenggara menduga adanya keterlibatan antara Pemodal dan Penerbit atau memiliki hubungan afiliasi dalam kaitannya TPPU dan/atau TPPT.
5. Penyelenggara mendapatkan informasi dari sumber yang dapat dipercaya (PPATK, lembaga pengawas dan pengatur, termasuk Otoritas Jasa Keuangan, aparat penegak hukum, media massa, atau sumber lainnya) bahwa Pengguna diduga terlibat dalam aktivitas ilegal dan/ atau memiliki latar belakang tindak kriminal.
6. Pengguna mengubah atau membatalkan transaksi setelah Penyelenggara meminta dokumen identitas Pengguna.
7. Registrasi sebagai Pengguna atas nama badan usaha, yayasan, organisasi, dan/atau individu yang terlibat, diduga terlibat, atau terkait dengan kegiatan terorisme.
8. Transaksi Pengguna yang terkait dengan usaha menggunakan rekening perorangan.
9. Pengguna/pengurus atau pemilik Pengguna diduga menggunakan dana hasil tindak pidana

   Contoh: dana hasil tindak pidana digunakan oleh Pemodal untuk membeli efek yang diterbitkan oleh Penerbit atau dana hasil tindak pidana digunakan oleh Penerbit untuk membayar dividen ke Pemodal melalui Penyelenggara.
10. Pengurus atau pemilik Pengguna diduga melakukan suatu tindak pidana.
11. Transaksi melibatkan perusahaan fiktif atau *paper company*.

12. Transaksi keuangan yang diminta oleh PPATK karena Pengguna telah ditetapkan sebagai tersangka/terdakwa dalam kasus tindak pidana.

    Contoh: Pemodal telah ditetapkan sebagai tersangka/terdakwa.
13. Transaksi keuangan yang diminta oleh PPATK karena keterkaitannya dengan transaksi lain yang sedang dalam proses analisis maupun pemeriksaan oleh PPATK.
14. Transaksi Keuangan yang diminta oleh PPATK atas dasar penyelidikan atau penyidikan yang sedang dilakukan oleh aparat penegak hukum.
15. Pengguna/calon Pengguna memberikan informasi yang tidak benar mengenai hal-hal yang berkaitan dengan identitas, sumber penghasilan atau usahanya.

    Contoh: Penerbit tidak memberikan informasi yang benar mengenai pendapatan, alamat kantor, kegiatan usaha, dan lainnya.
16. Pengguna/calon Pengguna menggunakan dokumen identitas yang diragukan kebenarannya atau diduga palsu seperti tanda tangan yang berbeda atau foto yang tidak sama.
17. Pengguna/calon Pengguna enggan atau menolak untuk memberikan informasi/dokumen yang diminta oleh petugas Penyelenggara tanpa alasan yang jelas.
18. Pengguna tidak bersedia memberikan informasi yang benar atau segera memutuskan hubungan usaha/menutup rekening pada saat petugas Penyelenggara meminta informasi atas transaksi yang dilakukannya.
19. Pengguna enggan memberikan informasi sumber dana dan tujuan transaksi secara lengkap kepada Penyelenggara.
20. Pengguna menggunakan nama yang berbeda (ejaan yang berbeda) dari satu transaksi ke transaksi yang lain.
21. Transaksi melibatkan perusahaan fiktif dengan indikasi penggunaan dokumen palsu.
22. Pengguna berupaya untuk meyakinkan pegawai Penyelenggara untuk tidak melengkapi dokumentasi apapun yang diperlukan untuk melakukan transaksi.
23. 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).

24. Pengguna memberikan informasi yang diragukan atau tidak jelas.
25. Pengguna menolak untuk memberikan dokumen identitas pribadi.
26. Semua identitas yang disajikan tidak dapat diperiksa kebenarannya karena alasan tertentu.
27. Pengguna menyajikan dokumen identitas yang berbeda setiap kali transaksi dilakukan.
28. Terdapat fakta riwayat Pemodal dan Penerbit tercantum dalam kategori kolektibilitas 2 ke atas melalui data dari Sistem Layanan Informasi Keuangan (SLIK).
29. Terdapat fakta riwayat Pemodal dan Penerbit tercantum sebagai penarik cek dan/atau bilyet giro kosong melalui data Daftar Hitam Nasional (DHN).
30. Pengguna menggunakan alamat *Post Office Box* (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 *Single Investor Identification*		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan s*ingle investor identification* yang akan dikinikan pada periode tertentu
		s*ingle investor identification* yang akan dikinikan	% terhadap seluruh jumlah s*ingle investor identification*			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1	Nasabah orang perseorangan					
	a. Risiko tinggi					
	b. Risiko menengah					
	c. Risiko rendah					
2	Nasabah Korporasi					

No.	Jenis Nasabah dan tingkat risiko	Jumlah *Single Investor Identification*		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan s*ingle investor identification* yang akan dikinikan pada periode tertentu
		s*ingle investor identification* yang akan dikinikan	% terhadap seluruh jumlah s*ingle investor identification*			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	a. Non usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	b. Usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	c. PJK					
	1) Risiko tinggi					

No.	Jenis Nasabah dan tingkat risiko	Jumlah *Single Investor Identification*		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan s*ingle investor identification* yang akan dikinikan pada periode tertentu
		s*ingle investor identification* yang akan dikinikan	% terhadap seluruh jumlah s*ingle investor identification*			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	2) Risiko menengah					
	3) Risiko rendah					
	d. Yayasan					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	e. Selain perusahaan dan yayasan (berbadan hukum maupun tidak berbadan hukum)					
	1) Risiko tinggi					

No.	Jenis Nasabah dan tingkat risiko	Jumlah *Single Investor Identification*		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan s*ingle investor identification* yang akan dikinikan pada periode tertentu
		s*ingle investor identification* yang akan dikinikan	% terhadap seluruh jumlah s*ingle investor identification*			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	2) Risiko menengah					
	3) Risiko rendah					
3	Nasabah perikatan lainnya (*legal arrangement*)					
	a. *Trust*					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	b. Selain *trust*					
	1) Risiko tinggi					
	2) Risiko menengah					

No.	Jenis Nasabah dan tingkat risiko	Jumlah *Single Investor Identification*		Informasi yang akan dikinikan	Metode atau strategi	Persentase target pemenuhan s*ingle investor identification* yang akan dikinikan pada periode tertentu
		s*ingle investor identification* yang akan dikinikan	% terhadap seluruh jumlah s*ingle investor identification*			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	3) Risiko rendah					
4.	Lembaga Negara, Instansi Pemerintah, lembaga internasional, dan perwakilan negara asing					
	a. Risiko tinggi					
	b. Risiko menengah					
	c. Risiko rendah					

1. Keterangan kolom:

(a). Diisi dengan nomor.

(b). Sesuai kolom.

(c). Diisi dengan rencana jumlah 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 investor identification* 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 REALISASI 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)	(f)	(g)
1	Nasabah orang perseorangan					
	a. Risiko tinggi					
	b. Risiko menengah					
	c. Risiko rendah					
2	Nasabah Korporasi					
	a. Non usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	b. Usaha mikro dan kecil					
	1) Risiko tinggi					
	2) Risiko menengah					

No.	Jenis Nasabah dan tingkat risiko	Perkembangan			Kendala	Upaya yang akan dilakukan
		Target	Realisasi	Deviasi (%)		
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	3) Risiko rendah					
	c. PJK					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	d. Yayasan					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	e. Selain perusahaan dan yayasan (berbadan hukum maupun tidak berbadan hukum)					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
3	Nasabah perikatan lainnya (*legal arrangement*)					

No.	Jenis Nasabah dan tingkat risiko	Perkembangan			Kendala	Upaya yang akan dilakukan
		Target	Realisasi	Deviasi (%)		
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	a. *Trust*					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
	b. Selain *trust*					
	1) Risiko tinggi					
	2) Risiko menengah					
	3) Risiko rendah					
4.	Lembaga Negara, Instansi Pemerintah, lembaga internasional, dan perwakilan negara asing					
	a. Risiko tinggi					
	b. Risiko menengah					
	c. Risiko rendah					

1. Keterangan kolom:

   (a). Diisi dengan nomor.

(b). Sesuai kolom.

(c). Diisi dengan target jumlah *Single investor identification* yang dikinikan.

(d). Diisi dengan realisasi jumlah *Single investor identification* yang dikinikan.

(e). Diisi dengan persentase selisih antara taget *Single investor identification* yang akan dikinikan (c) dengan (d) realisasi jumlah *Single investor identification* 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 20 September 2022

KEPALA EKSEKUTIF
PENGAWAS PASAR MODAL
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

INARNO DJAJADI

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja