Yth.
Direksi Pedagang Aset Keuangan Digital,
di tempat.

SALINAN
SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 16/SEOJK.07/2025
TENTANG
PENERAPAN PROGRAM ANTI PENCUCIAN UANG, PENCEGAHAN PENDANAAN TERORISME, DAN PENCEGAHAN PENDANAAN PROLIFERASI SENJATA PEMUSNAH MASSAL BAGI PEDAGANG ASET KEUANGAN DIGITAL

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 27 Tahun 2024 tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 38/OJK, Tambahan Lembaran Negara Republik Indonesia Nomor 108/OJK) dan untuk melaksanakan ketentuan Peraturan Otoritas Jasa Keuangan Nomor 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme, Dan Pencegahan Pendanaan Proliferasi Senjata Pemusnah Massal Di Sektor Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 11/OJK, Tambahan Lembaran Negara Republik Indonesia Nomor 36/OJK), perlu untuk mengatur lebih lanjut mengenai ketentuan pelaksanaan terkait tata cara, pelaporan dan mekanisme penerapan program anti pencucian uang, pencegahan pendanaan terorisme, dan pencegahan pendanaan proliferasi senjata pemusnah massal bagi Pedagang Aset Keuangan Digital dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

1. Dalam Surat Edaran Otoritas Jasa Keuangan ini yang dimaksud dengan:
   a. Aset Keuangan Digital adalah aset keuangan yang disimpan atau direpresentasikan secara digital, termasuk di dalamnya aset kripto.
   b. Aset Kripto adalah representasi digital dari nilai yang dapat disimpan dan ditransfer menggunakan teknologi yang memungkinkan penggunaan buku besar terdistribusi seperti *blockchain* untuk memverifikasi transaksinya dan memastikan keamanan dan validitas informasi yang tersimpan, tidak dijamin oleh otoritas pusat seperti bank sentral tetapi diterbitkan oleh pihak swasta, dapat ditransaksikan, disimpan, dan dipindahkan atau dialihkan secara elektronik, dan dapat berupa koin digital, token, atau representasi aset lainnya yang mencakup aset kripto terdukung (*backed crypto-asset*) dan aset kripto tidak terdukung (*unbacked crypto-asset*).
   c. Pedagang Aset Keuangan Digital yang selanjutnya disebut Pedagang adalah badan usaha yang melakukan perdagangan Aset Keuangan Digital, baik atas nama diri sendiri dan/atau memfasilitasi konsumen.

d. Direksi adalah organ Pedagang yang berwenang dan bertanggung jawab penuh atas pengurusan Pedagang untuk kepentingan Pedagang, sesuai dengan maksud dan tujuan Pedagang serta mewakili Pedagang, baik di dalam maupun di luar pengadilan sesuai dengan ketentuan anggaran dasar.
e. Dewan Komisaris adalah organ Pedagang yang bertugas melakukan pengawasan secara umum dan/atau khusus sesuai dengan anggaran dasar serta memberi nasihat kepada Direksi.
f. Pejabat Senior adalah pejabat setingkat kepala divisi atau kepala bagian di kantor pusat yang memiliki pengetahuan dan/atau pengalaman mengenai anti pencucian uang, pencegahan pendanaan terorisme, dan pencegahan pendanaan proliferasi senjata pemusnah massal.
g. Konsumen adalah setiap orang yang memiliki dan/atau memanfaatkan produk dan/atau layanan yang disediakan oleh Pedagang.
h. Nasabah adalah Konsumen sebagaimana dimaksud pada huruf g.
i. Pemilik Manfaat (*Beneficial Owner*) adalah orang perseorangan yang berhak atas dan/atau menerima manfaat tertentu yang berkaitan dengan rekening Nasabah, merupakan pemilik sebenarnya dari dana dan/atau Aset Keuangan Digital termasuk Aset Kripto yang ditempatkan pada Pedagang (*ultimately own account*), mengendalikan transaksi Nasabah, memberikan kuasa untuk melakukan transaksi, mengendalikan korporasi atau perikatan lainnya (*legal arrangement*), dan/atau merupakan pengendali akhir dari transaksi yang dilakukan melalui badan hukum atau berdasarkan suatu perjanjian.
j. *Travel Rule* adalah kewajiban untuk memperoleh, menyimpan, dan menyerahkan informasi pengirim dan penerima yang diperlukan terkait dengan jasa perpindahan atau transfer Aset Keuangan Digital guna mengidentifikasi dan melaporkan transaksi yang mencurigakan, melakukan pembekuan, dan melarang transaksi.
k. *Politically Exposed Person* yang selanjutnya disingkat PEP adalah orang yang diberi kewenangan untuk melakukan fungsi penting (*prominent function*), yang tidak dimaksudkan untuk tingkatan menengah atau tingkatan lebih rendah.
l. *Customer Due Diligence* yang selanjutnya disingkat CDD adalah kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Pedagang untuk memastikan transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi calon Nasabah, atau Nasabah.
m. *Enhanced Due Diligence* yang selanjutnya disingkat EDD adalah tindakan CDD lebih mendalam yang dilakukan Pedagang terhadap calon Nasabah, atau Nasabah, yang berisiko tinggi termasuk PEP dan/atau dalam area berisiko tinggi.
n. Tindak Pidana Pencucian Uang yang selanjutnya disingkat TPPU adalah TPPU sebagaimana dimaksud dalam undang-undang mengenai pencegahan dan pemberantasan tindak pidana pencucian uang.
o. Tindak Pidana Pendanaan Terorisme yang selanjutnya disingkat TPPT adalah TPPT sebagaimana dimaksud dalam

undang-undang mengenai pencegahan dan pemberantasan tindak pidana pendanaan terorisme.

p. Pendanaan Proliferasi Senjata Pemusnah Massal yang selanjutnya disingkat PPSPM adalah PPSPM sebagaimana diatur dalam peraturan pendanaan proliferasi senjata pemusnah massal.

q. Transaksi Keuangan Mencurigakan adalah transaksi keuangan mencurigakan terkait TPPU, TPPT, dan/atau PPSPM.

r. Daftar Terduga Teroris dan Organisasi Teroris yang selanjutnya disingkat DTTOT adalah daftar nama terduga teroris dan organisasi teroris sebagaimana dimaksud dalam peraturan perundang-undangan mengenai pencegahan dan pemberantasan TPPT.

s. Daftar Pendanaan Proliferasi Senjata Pemusnah Massal yang selanjutnya disingkat DPPSPM adalah daftar nama terduga pelaku PPSPM sebagaimana dimaksud dalam peraturan perundang-undangan mengenai pencegahan dan pemberantasan PPSPM.

t. Pemblokiran adalah pemblokiran sebagaimana diatur dalam peraturan perundang-undangan mengenai pencegahan dan pemberantasan TPPU, TPPT, dan/atau PPSPM.

u. Nasabah Berisiko Tinggi adalah Nasabah yang berdasarkan latar belakang, identitas, riwayatnya, dan/atau hasil penilaian risiko yang dilakukan Pedagang memiliki risiko tinggi melakukan kegiatan terkait TPPU, TPPT, dan/atau PPSPM.

v. Anti Pencucian Uang, Pencegahan Pendanaan Terorisme, dan Pencegahan Pendanaan Proliferasi Senjata Pemusnah Massal yang selanjutnya disingkat APU, PPT, dan PPPSPM adalah upaya pencegahan dan pemberantasan TPPU, TPPT, dan/atau PPSPM.

w. Rekomendasi *Financial Action Task Force* yang untuk selanjutnya disebut Rekomendasi FATF adalah standar pencegahan dan pemberantasan TPPU, TPPT, dan/atau PPSPM yang dikeluarkan oleh FATF.

x. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.

2. Pedagang sangat rentan terhadap kemungkinan digunakan sebagai media TPPU, TPPT, dan PPSPM, Pedagang dimungkinkan menjadi pintu masuk harta kekayaan yang merupakan hasil TPPU, TPPT, dan PPSPM ke dalam sistem keuangan yang selanjutnya dapat dimanfaatkan untuk kepentingan pelaku kejahatan. Misalnya untuk pelaku TPPU, harta kekayaan tersebut dapat ditarik kembali sebagai harta kekayaan yang seolah-olah sah dan tidak lagi dapat dilacak asal usulnya. Untuk pelaku TPPT, harta kekayaan tersebut dapat digunakan untuk membiayai kegiatan terorisme. Untuk pelaku PPSPM, harta kekayaan tersebut dapat digunakan untuk membiayai kegiatan proliferasi senjata pemusnah masal.

3. Semakin berkembangnya kompleksitas produk dan layanan jasa keuangan termasuk pemasarannya (*multichannel marketing*), serta semakin meningkatnya penggunaan teknologi informasi pada industri jasa keuangan, mengakibatkan semakin tinggi risiko Pedagang digunakan sebagai sarana TPPU, TPPT, dan PPSPM.

4. Dalam kaitan tersebut perlu adanya peningkatan kualitas penerapan program APU, PPT, dan PPPSPM yang didasarkan pada pendekatan berbasis risiko sesuai dengan prinsip-prinsip umum yang berlaku secara internasional, serta sejalan dengan penilaian risiko nasional (*national risk assessment*/NRA) dan penilaian risiko sektoral (*sectoral risk assessment*/SRA).
5. Pada dasarnya proses TPPU dapat dikelompokkan ke dalam 3 (tiga) tahap kegiatan yang meliputi:
   a. penempatan (*placement*), yaitu upaya menempatkan uang tunai yang berasal dari tindak pidana ke dalam sistem keuangan (*financial system*);
   b. pemisahan/pelapisan (*layering*), yaitu upaya untuk mengaburkan asal usul harta kekayaan yang berasal dari tindak pidana (*dirty money*) yang melibatkan Pedagang; dan/atau
   c. penggabungan (*integration*), yaitu upaya menggabungkan atau menggunakan harta kekayaan yang telah tampak sah, baik untuk dinikmati langsung, diinvestasikan ke dalam berbagai jenis produk/jasa/layanan keuangan dan bentuk material lainnya, dipergunakan untuk membiayai kegiatan bisnis yang sah, ataupun untuk membiayai kembali kegiatan tindak pidana.
6. Beberapa modus dan tipologi TPPU yang mungkin terjadi melalui sarana Pedagang antara lain:
   a. *structuring*, yaitu upaya untuk memecah transaksi dalam beberapa transaksi dengan masing-masing nilai transaksi yang relatif kecil yang dimaksudkan untuk menghindari pelaporan;
   b. *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;
   c. *mingling*, yaitu teknik mencampurkan atau menggabungkan hasil kejahatan dengan hasil usaha bisnis yang sah dengan tujuan untuk mengaburkan sumber dana hasil kejahatan;
   d. penyalahgunaan penggunaan jasa profesional seperti konsultan hukum, notaris, dan akuntan termasuk akuntan publik, dengan tujuan untuk mengaburkan identitas penerima manfaat dan sumber dana hasil kejahatan;
   e. penggunaan nama orang lain (*nominee*), anggota keluarga, dan/atau pihak ketiga oleh pihak-pihak yang berada dalam struktur kepengurusan Nasabah dan akan mewakili Nasabah dalam proses pembukaan hubungan usaha dengan Pedagang, yang dimaksudkan untuk mengaburkan identitas orang-orang yang melakukan tindak kejahatan dengan menggunakan identitas sah pihak lain;
   f. penggunaan identitas palsu oleh pihak-pihak yang berada dalam struktur kepengurusan Nasabah dan akan mewakili Nasabah dalam proses pembukaan hubungan usaha dengan Pedagang, yang dimaksudkan untuk mengaburkan identitas orang-orang yang melakukan tindak kejahatan, sehingga menghasilkan identitas baru yang seolah-olah asli dengan menggunakan identitas sah pihak lain. Adapun bentuk penggunaan identitas palsu antara lain melalui *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; dan

g. penggunaan atau kerja sama dengan perusahaan di negara/yurisdiksi *tax haven* yang tidak memiliki bisnis nyata (*paper company*), seperti diklasifikasikan oleh organisasi internasional yang kompeten, termasuk negara/yurisdiksi yang dikategorikan sebagai *high-risk and other monitored jurisdictions* oleh FATF.

7. 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.
8. Pada dasarnya proses TPPT dapat dikelompokkan ke dalam 3 (tiga) tahap kegiatan yang meliputi:
   a. pengumpulan dana (*collecting/raising funds*), yaitu aktivitas pengumpulan dana yang dilakukan oleh teroris, organisasi teroris, dan/atau pihak lain yang menjadi penyandang dana TPPT, dimana dana tersebut diperoleh dengan cara yang sah ataupun tidak sah.
   b. pemindahan dana (*moving/storing/transfering funds*), yaitu aktivitas menyediakan, memberikan, dan/atau meminjamkan dana dari pemilik dana kepada teroris dan/atau organisasi teroris.
   c. penggunaan dana (*using*), yaitu aktivitas penggunaan atau pemanfaatan dana yang telah dikumpulkan atau diterima oleh teroris dan/atau organisasi teroris untuk aktivitas tindak pidana terorisme.
9. Beberapa modus dan tipologi TPPT yang mungkin terjadi melalui sarana Pedagang, antara lain:
   a. penyalahgunaan dana investasi oleh Nasabah, dimana dana investasi disediakan, dikumpulkan, diberikan, dan/atau dipinjamkan kepada teroris dan/atau organisasi teroris, baik langsung maupun tidak langsung, dengan maksud digunakan seluruhnya atau sebagian untuk melakukan tindak pidana terorisme; dan
   b. pihak-pihak yang berada dalam struktur kepengurusan Nasabah dan akan mewakili Nasabah dan/atau pihak-pihak yang merupakan Pemilik Manfaat (*Beneficial Owner*) Nasabah tercantum dalam DTTOT.
10. PPSPM memiliki titik kritikal di mana kejahatan tidak hanya terbatas pada proses pembuatan suatu senjata pemusnah massal seperti nuklir, tetapi juga mencakup berbagai struktur pendukung lainnya, seperti penyediaan logistik bahan baku, pemanfaatan *shipping lines* tertentu untuk mendistribusikan logistik atau bahkan perangkat keras militer lainnya sampai dengan pembentukan *front company* untuk menutupi sejumlah transaksi yang digunakan sebagai upaya mendukung PPSPM.

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

1. Pedagang wajib menerapkan program APU, PPT, dan PPPSPM secara efektif dengan memperhatikan risiko TPPU, TPPT, dan/atau

PPSPM, serta skala usaha, kompleksitas usaha, dan/atau karakteristik usaha Pedagang, yang mencakup:

a. pengawasan aktif Direksi dan Dewan Komisaris;
b. kebijakan dan prosedur;
c. pengendalian intern;
d. sistem informasi manajemen; dan
e. sumber daya manusia dan pelatihan.

2. Penerapan program APU, PPT, dan PPPSPM sebagaimana dimaksud pada angka 1 dilakukan Pedagang dengan pendekatan berbasis risiko yang didasarkan pada hasil penerapan risiko APU, PPT, dan PPPSPM.
3. Dalam melakukan hubungan usaha dan transaksi dengan Nasabah, Pedagang harus menerapkan program APU, PPT, dan PPPSPM berbasis risiko (*risk-based approach*). Program tersebut antara lain mencakup hal yang diwajibkan dalam Rekomendasi FATF sebagai upaya untuk melindungi Pedagang agar tidak dijadikan sebagai sarana TPPU, TPPT, dan/atau PPSPM.

   Dalam Rekomendasi FATF dinyatakan bahwa Pedagang berkewajiban mengidentifikasi, menilai, dan memahami risiko TPPU, TPPT, dan/atau PPSPM terkait dengan Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*).

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

   Dalam penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk-based approach*), Pedagang 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 Pedagang harus tanggap dan mempertimbangkan perubahan risiko tersebut.
4. 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 TPPU, TPPT, dan PPSPM, risiko diartikan:

      1) pada tingkat nasional, adalah suatu ancaman dan kerentanan yang disebabkan oleh TPPU, TPPT, dan PPSPM yang membahayakan sistem keuangan nasional serta keselamatan dan keamanan nasional; dan
      2) pada tingkat Pedagang, adalah suatu ancaman dan kerentanan yang menempatkan Pedagang pada risiko dimana Pedagang digunakan sebagai sarana oleh TPPU, TPPT, dan PPSPM.

      Contoh matriks kemungkinan dan dampak *(Likelihood And Impact Matrix)* tercantum dalam Lampiran bagian A yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

Ancaman dapat berupa pihak atau objek yang dapat menyebabkan kerugian. Dalam konteks TPPU, TPPT dan PPSPM, 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, TPPT, dan/atau PPSPM, kerentanan diartikan pengendalian intern yang lemah dari Pedagang ataupun penawaran produk/jasa/transaksi yang berisiko tinggi.

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 TPPU, TPPT, dan/atau PPSPM, proses dimaksud mencakup pemahaman terhadap risiko TPPU, TPPT, dan/atau PPSPM, penilaian atas kedua risiko tersebut, dan pengembangan metode untuk mengelola dan melakukan mitigasi risiko yang telah diidentifikasi.

Dalam menerapkan manajemen risiko atas TPPU, TPPT, dan/atau PPSPM, Pedagang dapat mengembangkan metode manajemen risiko sesuai dengan kebutuhan Pedagang berdasarkan penilaian risiko TPPU, TPPT, dan/atau PPSPM, model bisnis, kegiatan usaha, skala usaha, kompleksitas usaha, karakteristik usaha, dan/atau peristiwa atau perkembangan besar dalam manajemen dan operasional Pedagang, dengan tetap mengacu pada peraturan perundang-undangan yang mengatur mengenai APU, PPT dan PPPSPM.

c. Risiko Bawaan (*Inherent Risk*) dan Risiko Residual (*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 TPPU, TPPT, dan/atau PPSPM 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

Dalam konteks TPPU, TPPT dan PPSPM, pendekatan berbasis risiko 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) Pedagang harus mempertimbangkan seluruh faktor risiko yang relevan termasuk risiko penggunaan teknologi informasi dan Sistem Elektronik.
3) Pedagang harus mengelola dan melakukan mitigasi risiko TPPU, TPPT, dan/atau PPSPM melalui pelaksanaan pengendalian intern dan melakukan langkah-langkah yang sesuai dengan risiko yang telah diidentifikasi, serta melakukan pemantauan transaksi sesuai dengan tingkat risiko TPPU, TPPT, dan/atau PPSPM yang telah dinilai.
Contoh tingkat risiko yang terkait dengan kegiatan usaha pedagang tercantum dalam Lampiran bagian B yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
4) Dalam melakukan penilaian, pengelolaan dan mitigasi risiko TPPU, TPPT dan PPSPM, Pedagang perlu memahami bahwa kegiatan penilaian dan mitigasi tersebut bukanlah sesuatu yang statis. Risiko yang telah diidentifikasi dapat berubah sejalan dengan perkembangan produk baru atau ancaman baru sehingga harus dilakukan pengkinian penilaian risiko secara berkala sesuai dengan kebutuhan dan penilaian risiko Pedagang.

5. Pedagang harus melakukan pengkinian penilaian risiko TPPU, TPPT dan/atau PPSPM secara berkala sesuai dengan kebutuhan Pedagang berdasarkan penilaian risiko TPPU, TPPT, dan/atau PPSPM, kegiatan, skala usaha, kompleksitas usaha, karakteristik usaha, dan/atau peristiwa atau perkembangan besar dalam manajemen dan operasional Pedagang.
Pengkinian penilaian risiko TPPU, TPPT dan/atau PPSPM terdiri atas:
a. Identifikasi, Pemahaman dan Penilaian terhadap Risiko Bawaan
1) Dalam melakukan identifikasi risiko bawaan (*inherent risk*), Pedagang harus mempertimbangkan kerentanan Pedagang untuk digunakan sebagai sarana TPPU, TPPT, dan/atau PPSPM. Langkah awal dalam melakukan penilaian risiko adalah dengan memahami kegiatan usaha Pedagang secara keseluruhan dengan perspektif yang luas. Pemahaman tersebut memungkinkan Pedagang untuk mempertimbangkan risiko TPPU, TPPT dan/atau PPSPM yang mungkin terjadi, apakah risiko terjadi pada sisi Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*).
2) Pedagang harus mempertimbangkan unsur yang memicu timbulnya risiko bagi Pedagang, baik dari sisi Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, dan/atau jaringan distribusi (*delivery channels*). Pedagang harus memahami unsur apa saja yang merupakan risiko bawaan (*inherent risk*) dan risiko residu (*residual risk*).
3) Risiko Nasabah
Pedagang harus memperhatikan risiko TPPU, TPPT, dan/atau PPSPM terkait profil calon Nasabah atau Nasabah. Pedagang perlu mengategorikan Nasabah berdasarkan tingkat risiko TPPU, TPPT, dan/atau PPSPM, dengan mengacu pada klasifikasi risiko yang ditetapkan oleh Pedagang.

4) Risiko Nasabah yang terkait dengan kekhasan bisnis proses Pedagang meningkat apabila memenuhi faktor:
   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 situs web/aplikasi Pedagang;
   c) nilai transaksi dari Nasabah memiliki nilai nominal yang besarnya tidak sesuai dengan profil Nasabah dimaksud (melewati batas kewajaran);
   d) intensitas transaksi oleh Nasabah melewati batas kewajaran termasuk yang berada di luar kebijakan yang normal/wajar atau yang berada di luar kebiasaan;
   e) Nasabah bertindak untuk Pemilik Manfaat (*Beneficial Owner*);
   f) Nasabah yang menggunakan produk dan/atau jasa Pedagang atau melakukan transaksi Aset Keuangan Digital termasuk Aset Kripto melalui Pedagang yang tidak sesuai dengan kebutuhan atau tidak menguntungkan Nasabah 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 antara lain akuntan, konsultan hukum, penilai, notaris, atau profesi lainnya yang bertindak mewakili Nasabah sehubungan dengan akun/rekening pada Pedagang;
   j) Nasabah 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 lembaga yang diawasi otoritas/ lembaga pengatur dan pengawas lain yang belum menerapkan program APU, PPT, dan PPPSPM secara efektif;
   l) Nasabah melakukan perubahan nomor rekening yang tercatat pada Pedagang;
   m) 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; dan/atau
   n) Terdapat perbedaan antara identitas atau data diri Nasabah yang dimiliki oleh Pedagang Aset Kripto

dengan identitas atau data diri Nasabah yang dimiliki oleh penyedia jasa pembayaran dan/atau rekening bank penyimpanan fiat.

5) Risiko Negara/Area Geografis/Yurisdiksi

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

Risiko TPPU, TPPT, dan/atau PPSPM terkait negara/area geografis/yurisdiksi meningkat apabila memenuhi ketentuan sebagai berikut:

a) Penerbit Aset Keuangan Digital termasuk Aset Kripto dari negara atau yurisdiksi berisiko tinggi;
b) Dana atau Aset Keuangan Digital termasuk Aset Kripto dari atau dikirim ke negara atau yurisdiksi berisiko tinggi;
c) Nasabah memiliki hubungan yang signifikan dengan negara atau yurisdiksi berisiko tinggi;
d) Nasabah berdomisili di wilayah yang berisiko tinggi;
e) Nasabah terdeteksi mengakses aplikasi/situs web Pedagang saat berada di wilayah atau di daerah perbatasan yang berisiko tinggi;
f) Nasabah berdomisili di wilayah daerah perbatasan antar negara yang berisiko tinggi;
g) Nasabah tidak diketahui wilayah domisili aslinya (menggunakan *IP address* palsu); dan/atau
h) Nasabah terdeteksi melakukan transaksi dengan Nasabah dari negara yang berisiko tinggi atau transaksi yang terhubung dengan Pedagang Aset Kripto pada negara yang berisiko tinggi.

Indikator yang menentukan suatu negara/area geografis/yurisdiksi berisiko tinggi terhadap TPPU, TPPT, dan/atau PPSPM 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/Layanan (Termasuk Transaksi)
Penilaian risiko secara keseluruhan harus mencakup penentuan risiko yang dapat terjadi atas berbagai produk/jasa/layanan (termasuk transaksi) yang ditawarkan. Hal-hal yang dapat meningkatkan risiko produk/jasa/ transaksi, antara lain:
a) produk atau jasa Aset Keuangan Digital termasuk Aset Kripto yang memungkinkan meningkatkan anonimitas, berkurangnya transparansi, dan mengaburkan arus keuangan, contoh: *anonymity-enhanced cryptocurrencies* (AECs), *mixers and tumblers, decentralized platforms and exchanges, privacy wallets*;
b) produk atau jasa Aset Keuangan Digital termasuk Aset Kripto yang terkait dengan aktivitas terlarang seperti digunakan untuk transaksi *darknet marketplace*, *ransomware*, dan *hacking*;
c) produk atau jasa yang memungkinkan pembayaran, penyaluran, atau pengelolaan dana dari pihak ketiga yang tidak dikenal atau tidak ada hubungan dengan Nasabah; dan/atau
d) transaksi yang berasal dari pembiayaan dan/atau *wallet* yang dimiliki oleh pihak yang dicurigai dan/atau ditetapkan oleh pihak yang berwenang sebagai pihak yang terafiliasi dengan kejahatan tertentu.

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 Pedagang 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, Pedagang 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 Pedagang 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 situs web di internet telah lumrah, namun hal tersebut tetap perlu dipertimbangkan sebagai bagian dari faktor yang dapat menyebabkan risiko TPPU, TPPT, dan/atau PPSPM menjadi lebih tinggi.
Beberapa indikator yang menyebabkan jaringan distribusi (*delivery channels*) berisiko tinggi, antara lain aplikasi daring yang tidak teruji keandalan dan keamanannya, khususnya terkait kerahasiaan data Nasabah.

8) Risiko Relevan Lainnya
Faktor lain yang relevan yang dapat memberikan dampak pada risiko TPPU, TPPT, dan/atau PPSPM antara lain:
   a) perkembangan modus dan tipologi risiko TPPU, TPPT dan/atau PPSPM;
   b) model bisnis, skala usaha, dan jumlah pegawai sebagai faktor risiko bawaan (*inherent risk*) Pedagang;
   c) total nilai dan intensitas transaksi yang tinggi sehingga memerlukan mitigasi risiko yang memadai;
   d) penggunaan teknologi informasi dalam seluruh rangkaian proses bisnis Pedagang;
   e) keamanan data dari risiko serangan siber (*cyberattacks*), dimana Pedagang sangat bergantung pada penggunaan *open communication network* (internet) sehingga pada proses penggunaan internet tersebut terdapat risiko besar terhadap serangan siber (*cyberattacks*);
   f) pelindungan data pribadi yang mencakup pelindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi sesuai dengan ketentuan peraturan perundang-undangan. Risiko paling besar bagi Pedagang adalah terkait dengan buruknya manajemen pelindungan data pribadi;
   g) rekam jejak transaksi dan penerimaan nasabah, dimana Pedagang diharuskan untuk menyediakan rekam jejak transaksi dan penerimaan nasabah terhadap seluruh kegiatannya di dalam Sistem Elektronik Pedagang. Rekam jejak transaksi dan penerimaan nasabah 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 pelindungan 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*), Pedagang tetap memiliki data cadangan (*back up data*) sehingga tidak mengulangi proses pengumpulan data kembali.

9) Pedagang 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 Pedagang.
11) Setelah melakukan identifikasi dan dokumentasi risiko bawaan (*inherent risk*), Pedagang perlu memberikan penilaian terkait tingkat pada setiap risiko dari calon Nasabah, misalnya rendah (*low*), sedang (*medium*), dan tinggi (*high*).
12) Dalam melakukan tahapan identifikasi dari risiko bawaan (*inherent risk*), Pedagang harus mampu menjelaskan seluruh proses identifikasi risiko yang telah dilakukan oleh Pedagang dan alasan atau pertimbangannya.
13) Setiap unsur risiko yang telah teridentifikasi sebagai risiko tinggi harus dimitigasi dan didokumentasikan. Pedagang harus dapat menjelaskan kepada Otoritas Jasa Keuangan langkah mitigasi terhadap unsur risiko tinggi, contohnya langkah dalam kebijakan dan prosedur atau program pelatihan.
14) Pedagang 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.
15) Pedagang harus menyediakan informasi yang telah terdokumentasi, yang menunjukkan bahwa Pedagang telah secara khusus memperhatikan indikator yang berisiko tinggi dalam penilaian risikonya.
16) Dalam rangka mengidentifikasi risiko TPPU, TPPT, dan/atau PPSPM dan menetapkan skala risiko dari calon Nasabah pada saat pembukaan hubungan usaha atau Nasabah pada saat melakukan transaksi, Pedagang dapat menggunakan *regulatory technology* seperti *big data analytic, artificial intelligence,* dan/atau *machine learning*.
17) Pemanfaatan *regulatory technology* dalam penerapan program APU, PPT, dan PPSPM bagi Pedagang dapat pula dilakukan oleh Pedagang 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 Pedagang, dimana risiko ini paling sedikit mencakup pemenuhan ketentuan sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan mengenai penerapan program anti pencucian uang, pencegahan pendanaan terorisme, dan pencegahan pendanaan proliferasi senjata pemusnah masal 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 Pedagang, baik dalam bentuk *risk taker* maupun *non-risk taker*.
   2) Pedagang harus menetapkan toleransi risiko sebelum mempertimbangkan mitigasi risiko.
   3) Pada saat mempertimbangkan ancaman, konsep toleransi risiko akan memberikan kemampuan kepada Pedagang untuk menentukan tingkat ancaman risiko yang dapat ditoleransi oleh Pedagang.
   4) Dalam menetapkan toleransi risiko, Pedagang perlu mempertimbangkan kategori risiko yang dapat memengaruhi Pedagang, paling sedikit:
      a) risiko operasional (*operational risk*); dan
      b) risiko TPPU, TPPT, dan/atau sesuai dengan ketentuan peraturan perundang-undangan.

c. Implementasi Penerapan program APU, PPT, PPPSPM Berbasis Risiko (*Risk-Based Approach*)
   1) Pedagang berkewajiban menerapkan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*) yang didasarkan pada hasil penilaian risiko TPPU, TPPT, dan/atau PPSPM.
   2) Penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk-based approach*) yang dimiliki Pedagang harus didokumentasikan untuk menunjukkan tingkat kepatuhan Pedagang. Kebijakan dan prosedur terkait penerapan program APU, PPT, dan PPPSPM 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 penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*) harus memenuhi persyaratan minimal sebagai berikut:
      a) identifikasi Nasabah berdasarkan tingkat risiko;
      b) pendeteksian Transaksi Keuangan Mencurigakan;
      c) penentuan intensitas pemantauan yang disesuaikan dengan tingkat risiko Nasabah, antara lain dari sisi frekuensi, tata cara pelaksanaan, dan evaluasi terhadap hasil pemantauan;
      d) penilaian risiko;
      e) tindakan khusus terhadap area berisiko tinggi;
      f) penatausahaan;

g) perencanaan dan pelaksanaan pengkinian data dan informasi Nasabah dan Pemilik Manfaat (*Beneficial Owner*) yang didasarkan pada tingkat risiko; dan
h) pelaporan.

4) Kebijakan dan prosedur dalam penerapan program APU, PPT, dan PPPSPM 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) Pedagang perlu melakukan pemantauan secara berkala terhadap seluruh hubungan usaha yang dilakukan, dan terhadap hubungan usaha yang berisiko tinggi terhadap TPPU, TPPT, dan PPSPM. Pedagang harus menerapkan langkah khusus yang lebih ketat terhadap Nasabah atau hubungan usaha yang berisiko tinggi.
6) Pedagang perlu memperhatikan bahwa dalam manajemen risiko dan mitigasi risiko dibutuhkan kepemimpinan dan keterlibatan Pejabat Senior. Pejabat Senior bertanggung jawab dalam pengambilan keputusan terkait kebijakan, prosedur, proses pengendalian intern, dan mitigasi risiko terhadap TPPU, TPPT, dan PPSPM dalam kegiatan/aktivitas usaha yang dimiliki Pedagang.
7) Dengan adanya penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*), Pedagang harus:
   a) memastikan bahwa penilaian risiko yang telah dilakukan menggambarkan proses penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*), frekuensi pemantauan Nasabah yang berisiko rendah dan berisiko tinggi, dan juga menggambarkan langkah pengendalian intern yang diberlakukan untuk mengurangi risiko tinggi yang telah diidentifikasi;
   b) menerapkan penerapan program APU, PPT, dan PPPSPM 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 TPPU, TPPT, dan/atau PPSPM;
   f) melakukan langkah tertentu terhadap Nasabah Berisiko Tinggi; dan
   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 intern untuk membatasi risiko TPPU, TPPT, dan/atau PPSPM yang telah diidentifikasi dalam penilaian risiko. Mitigasi risiko membantu Pedagang untuk memastikan kegiatan

usahanya tetap berada dalam batas toleransi risiko yang telah ditetapkan. Dalam hal hasil penilaian risiko menunjukkan bahwa Pedagang memiliki tingkat risiko tinggi, Pedagang 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, PPT, dan PPPSPM secara efektif dan memadai sebagaimana dimaksud pada angka 1.
3) Pedagang melaporkan kepada Otoritas Jasa Keuangan bahwa mitigasi risiko tersebut telah dilaksanakan secara efektif dalam laporan dokumen penilaian risiko TPPU, TPPT, dan/atau PPSPM yang telah disusun secara individual (*Individual Risk Assesment*/IRA).
4) Pengendalian intern dan mitigasi risiko pada area atau hubungan usaha yang berisiko tinggi didasarkan pada penerimaan risiko (*risk appetite*) dan toleransi risiko (*risk tolerance*).
5) Dalam semua situasi, kegiatan usaha Pedagang harus mempertimbangkan pengendalian intern 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 intern yang memadai serta didokumentasikan dengan baik.
7) Untuk semua Nasabah dan hubungan usaha, Pedagang 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, Pedagang 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, Pedagang harus:
   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 Pedagang secara proporsional berdasarkan tingkat risiko Nasabah, bagi Nasabah berisiko rendah dilakukan secara periodik dan bagi Nasabah Berisiko Tinggi dilakukan lebih sering dan/atau lebih dalam dibandingkan Nasabah berisiko rendah dan berisiko menengah,

      Contoh:

      Nasabah berisiko rendah dilakukan pemantauan tahunan dengan kedalaman *know your transaction*

umum, Nasabah berisiko menengah dilakukan pemantauan tiap 3 (tiga) bulan, atau semester dengan kedalaman *know your transaction* umum, dan Nasabah Berisiko Tinggi dilakukan pemantauan harian, mingguan, atau bulanan dengan kedalaman parameter *know your transaction* lebih khusus (*customized rules* menyesuaikan risiko).

c) melaksanakan mitigasi terhadap area berisiko tinggi. Strategi mitigasi risiko ini harus tercantum dalam kebijakan dan prosedur; dan

d) menerapkan prosedur pengendalian intern secara konsisten.

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

1) Risiko residu (*residual risk*) merupakan risiko yang tersisa setelah penerapan pengendalian intern dan mitigasi risiko. Pedagang perlu memperhatikan bahwa seketat apapun mitigasi risiko dan manajemen risiko yang dimiliki, Pedagang 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. Pedagang 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 intern dan mitigasi terhadap area berisiko tinggi tidak memadai, Pedagang 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 Pedagang. Risiko yang ditoleransi dapat meningkat dari waktu ke waktu. Sebagai contoh, ketika adanya ancaman baru TPPU, TPPT dan/atau PPSPM.

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 intern 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*), Pedagang harus:

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 Penerapan Program APU, PPT, dan PPPSPM Berbasis Risiko (*Risk Based Approach*)

1) Penilaian risiko TPPU, TPPT dan/atau PPSPM yang dimiliki oleh Pedagang harus dievaluasi berdasarkan kebutuhan untuk menguji efektivitas dari kepatuhan penerapan program APU, PPT, dan PPPSPM, yang meliputi:
   a) pengawasan aktif Direksi dan Dewan Komisaris;
   b) kebijakan dan prosedur;
   c) sistem informasi manajemen;
   d) pengendalian intern;
   e) kebutuhan sumber daya manusia yang memiliki pengetahuan dan kemampuan dibidang teknologi informasi serta bisnis proses Pedagang;
   f) program pelatihan sumber daya manusia bagi pegawai, Pejabat Senior serta Direksi dan Dewan Komisaris terkait penerapan program APU, PPT, dan PPPSPM; 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 intern.
3) Peninjauan atas penilaian risiko TPPU, TPPT dan/atau PPSPM 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 Pedagang 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 Pedagang. Pada akhirnya, prosedur peninjauan atas penilaian risiko dimaksud akan mempengaruhi efektivitas dari pelaksanaan penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*) dalam menerapkan program APU, PPT, dan PPPSPM.
4) Dengan adanya peninjauan pada penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*), Pedagang harus:
   a) melakukan peninjauan sesuai dengan kebutuhan Pedagang;
   b) menghasilkan tinjauan yang mencakup kepatuhan kebijakan dan prosedur, penilaian risiko terhadap TPPU, TPPT, dan PPSPM serta program pelatihan untuk menguji efektivitas penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*);
   c) melakukan penatausahaan terhadap proses peninjauan dan melaporkan kepada Pejabat Senior; dan
   d) melakukan penatausahaan hasil peninjauan dan penetapan langkah yang bersifat korektif untuk ditindaklanjuti.

III. PENGAWASAN AKTIF DIREKSI DAN DEWAN KOMISARIS

1. Pengawasan Aktif Direksi

Pengawasan aktif Direksi meliputi:

a. mengusulkan kebijakan dan prosedur tertulis mengenai penerapan program APU, PPT dan PPPSPM kepada Dewan Komisaris termasuk mitigasi risiko TPPU, TPPT, dan/atau PPSPM dengan memuat paling sedikit:
   1) identifikasi dan verifikasi calon Nasabah atau Nasabah;
   2) identifikasi dan verifikasi Pemilik Manfaat *(Beneficial Owner)*;
   3) penutupan hubungan usaha;
   4) pengelolaan risiko TPPU, TPPT, dan/atau PPSPM yang berkelanjutan terhadap Nasabah, area geografis (termasuk negara/yurisdiksi), produk/jasa/layanan, dan/atau jaringan distribusi *(delivery channels)*;
   5) pemeliharaan data yang akurat terkait dengan Transaksi, penatausahaan proses CDD, serta penatausahaan kebijakan dan prosedur;
   6) pengkinian dan pemantauan;
   7) pelaporan kepada Pejabat Senior, Direksi, dan Dewan Komisaris terhadap pelaksanaan kebijakan dan prosedur penerapan program APU, PPT, dan PPPSPM; dan
   8) pelaporan kepada Pusat Pelaporan dan Analisis Transaksi Keuangan.
b. memastikan penerapan program APU, PPT, dan PPPSPM dilaksanakan sesuai dengan kebijakan dan prosedur tertulis yang telah ditetapkan;
c. membentuk unit kerja khusus dan/atau menunjuk pejabat yang bertanggung jawab terhadap penerapan program APU, PPT dan PPPSPM;
d. melakukan pengawasan atas kepatuhan unit kerja dalam menerapkan program APU, PPT dan PPPSPM;
e. memastikan bahwa kebijakan dan prosedur tertulis mengenai penerapan program APU, PPT dan PPPSPM sejalan dengan perubahan dan pengembangan produk, jasa, dan teknologi di sektor jasa keuangan serta sesuai dengan perkembangan modus TPPU, TPPT, dan/atau PPSPM;
f. memastikan pejabat dan/atau pegawai, khususnya pegawai dari satuan kerja terkait (misalnya satuan kerja yang berhubungan baik secara langsung maupun tidak langsung dengan calon Nasabah, seperti petugas pelayanan Nasabah, petugas yang terkait pengelolaan dan pengembangan teknologi informasi, serta internal auditor) dan pegawai baru, telah mengikuti pelatihan yang berkaitan dengan penerapan program APU, PPT, dan PPPSPM sebanyak 1 (satu) kali dalam 1 (satu) tahun;
g. memastikan adanya pembahasan terkait penerapan program APU, PPT, dan PPPSPM dalam rapat Direksi.
   Hasil rapat pembahasan harus dituangkan dalam risalah rapat (*minute meeting*) yang ditanda tangani oleh Direksi dan pihak yang menghadiri rapat pembahasan tersebut;
h. memberikan arahan yang jelas atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko TPPU, TPPT, dan/atau PPSPM;
i. Dalam hal terdapat kebutuhan Pedagang berdasarkan penilaian risiko TPPU, TPPT, dan/atau PPSPM, kegiatan usaha,

skala usaha, kompleksitas usaha, karakteristik usaha, dan/atau peristiwa atau perkembangan besar dalam manajemen dan operasional Pedagang, pelatihan sebagaimana dimaksud pada huruf f dapat dilakukan lebih dari 1 (satu) kali dalam 1 (satu) tahun; dan

j. memastikan kerahasiaan data/informasi yang dikelola oleh Pedagang.

2. Pengawasan Aktif Dewan Komisaris.
   Dalam melakukan pengawasan aktif, Dewan Komisaris paling sedikit:
   a. memastikan Pedagang memiliki kebijakan dan prosedur penerapan program APU, PPT, dan PPPSPM;
   b. memberikan persetujuan atas kebijakan dan prosedur tertulis penerapan program APU, PPT, dan PPPSPM yang diusulkan Direksi;
   c. melakukan evaluasi atas kebijakan dan prosedur penerapan program APU, PPT, dan PPPSPM;
   d. melakukan pengawasan atas pelaksanaan tugas dan tanggung jawab Direksi terhadap penerapan program APU, PPT, dan PPPSPM; dan
   e. memastikan adanya pembahasan terkait penerapan program APU, PPT, dan PPPSPM dalam rapat Direksi dan Dewan Komisaris.
      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, PPT, dan PPPSPM, Direksi dan Dewan Komisaris harus:
   a. memiliki pemahaman yang memadai mengenai risiko TPPU, TPPT, dan/atau PPSPM yang melekat pada seluruh aktivitas operasional Pedagang 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, PPT, dan PPPSPM, termasuk memastikan penanggung jawab APU, PPT, dan PPPSPM berada dalam struktur organisasi; dan
   d. bertanggung jawab atas kebijakan dan prosedur, penerapan dan pengawasan penerapan program APU, PPT, dan PPPSPM, termasuk pengelolaan dan mitigasi risiko TPPU, TPPT, dan/atau PPSPM pada seluruh aktivitas operasional Pedagang.
4. Penanggung Jawab Penerapan Program APU, PPT, dan PPPSPM
   a. Pedagang harus memiliki penanggung jawab penerapan program APU, PPT, dan PPPSPM.
   b. Penanggung jawab penerapan program APU, PPT, dan PPPSPM harus berada dalam struktur organisasi Pedagang.
   c. Penentuan dan keberadaan penanggung jawab penerapan program APU, PPT dan PPPSPM didasarkan pada kebutuhan dan kompleksitas usaha Pedagang, artinya Pedagang dapat memiliki unit kerja khusus dan pejabat penanggung jawab

atau hanya memiliki unit kerja khusus saja atau hanya memiliki pejabat penanggung jawab saja.

d. Dalam hal penanggung jawab penerapan program APU, PPT, dan PPPSPM berupa unit kerja khusus 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) pimpinan dan pelaksana pada unit kerja khusus tidak merangkap fungsi lain;
   3) pimpinan unit kerja khusus ditetapkan dan diangkat oleh Direksi;
   4) berada dalam struktur organisasi Pedagang;
   5) berada di bawah koordinasi Direksi secara langsung dalam struktur organisasi Pedagang; dan
   6) bersifat independen dari fungsi lain.

e. Dalam hal penanggung jawab penerapan program APU, PPT, dan PPPSPM berupa pejabat penanggung jawab, maka pejabat penanggung jawab harus ditetapkan dan diangkat oleh Direksi dan hanya dapat merangkap fungsi kepatuhan dan/atau manajemen risiko.

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

g. Penanggung jawab penerapan program APU, PPT, dan PPPSPM melapor dan bertanggung jawab kepada Direksi yang memiliki tugas mengawasi penerapan program APU, PPT, dan PPPSPM.

h. Penanggung jawab penerapan program APU, PPT, dan PPPSPM pada Pedagang mempunyai tugas, sebagai berikut:
   1) menganalisis secara berkala penilaian risiko TPPU, TPPT, dan/atau PPSPM terkait dengan Nasabah, area geografis (termasuk negara/yurisdiksi), produk/jasa/layanan, dan/atau metode Transaksi/jaringan distribusi (*delivery channels*), sebanyak 1 (satu) kali dalam 1 (satu) tahun;
   2) menyusun, melakukan pengkinian, serta mengusulkan kebijakan dan prosedur penerapan program APU, PPT, dan PPPSPM yang telah disusun untuk mengelola dan memitigasi risiko berdasarkan penilaian risiko sebagaimana dimaksud dalam angka 1), untuk dimintakan pertimbangan Direksi;
   3) memastikan adanya sistem yang dapat mengidentifikasi, menganalisis, memantau, dan menyediakan laporan secara efektif mengenai Transaksi Keuangan Mencurigakan yang didasarkan pada adanya penyimpangan atas profil, karakteristik, atau kebiasaan pola transaksi Nasabah, seperti:
      a) Berdasarkan laporan keuangan, Nasabah tidak memiliki kemampuan keuangan untuk melakukan transaksi pembelian Aset Keuangan Digital di atas jumlah pendapatan, namun Nasabah dapat melakukan transaksi dengan jumlah jauh di atas pendapatan;

b) Nasabah melakukan transaksi dengan volume tidak wajar;
c) Direksi, Dewan Komisaris, pemegang saham, dan atau Pemilik Manfaat (*Beneficial Owner*) dari Nasabah diduga terkait dengan tindak pidana asal, TPPU, TPPT, dan/atau PPSPM;
d) Nasabah diduga terkait dengan TPPU, TPPT, dan/atau PPSPM;
e) aset yang dijadikan dasar penerbitan Aset Keuangan Digital diduga terkait dengan tindak pidana asal, TPPU, TPPT, dan/atau PPSPM; dan
f) Nasabah melakukan transaksi Aset Keuangan Digital dengan Pedagang yang berasal dari negara berisiko tinggi.

4) memastikan bahwa kebijakan dan prosedur yang disusun telah sesuai dengan perubahan dan/atau perkembangan produk/jasa/layanan, teknologi, dan/atau modus dan tipologi TPPU, TPPT, dan/atau PPSPM di sektor jasa keuangan, dan/atau sesuai dengan kebutuhan Pedagang berdasarkan penilaian risiko TPPU, TPPT, dan/atau PPSPM, model bisnis, kegiatan usaha, skala usaha, kompleksitas usaha, karakteristik usaha, dan/atau peristiwa atau perkembangan besar dalam manajemen dan operasional Pedagang;
5) memastikan bahwa formulir yang berkaitan dengan Nasabah telah mengakomodasi data yang diperlukan dalam penerapan program APU, PPT, dan PPPSPM;
6) memantau indikasi Transaksi Keuangan Mencurigakan sebagaimana dimaksud dalam angka 3);
7) melakukan evaluasi terhadap hasil pemantauan dan analisis transaksi Nasabah untuk memastikan ada atau tidak adanya Transaksi Keuangan Mencurigakan;
8) menatausahakan hasil pemantauan dan evaluasi;
9) memastikan pengkinian data dan profil Nasabah;
10) memastikan bahwa kegiatan usaha yang berisiko tinggi terhadap TPPU, TPPT, dan/atau PPSPM diidentifikasi secara efektif sesuai dengan kebijakan dan prosedur Pedagang serta ketentuan sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU, PPT, dan PPPSPM di sektor jasa keuangan;
11) memastikan adanya mekanisme komunikasi yang baik dari setiap satuan kerja terkait kepada unit kerja khusus atau pejabat yang bertanggung jawab terhadap penerapan program APU, PPT, dan PPPSPM dengan menjaga kerahasiaan informasi dan memperhatikan ketentuan *anti tipping-off*;
12) melakukan pengawasan terkait penerapan program APU, PPT, dan PPPSPM terhadap satuan kerja terkait, antara lain mengawasi satuan kerja terkait telah melakukan fungsi dan tugas untuk mempersiapkan laporan mengenai dugaan Transaksi Keuangan Mencurigakan sebelum menyampaikannya kepada unit kerja khusus atau pejabat yang bertanggung jawab terhadap penerapan program APU, PPT, dan PPPSPM;
13) memastikan adanya identifikasi area yang berisiko tinggi yang terkait dengan penerapan program APU, PPT, dan

PPPSPM dengan mengacu pada peraturan perundang-undangan dan sumber informasi yang memadai;

14) menerima, melakukan analisis, dan menyusun laporan Transaksi Keuangan Mencurigakan yang disampaikan oleh satuan kerja;
15) menyusun laporan Transaksi Keuangan Mencurigakan;
16) memantau secara berkala dan memastikan tindak lanjut terhadap DTTOT dan DPPSPM telah sesuai dengan peraturan perundang-undangan mengenai pencegahan dan pemberantasan TPPT dan peraturan mengenai pencegahan dan pemberantasan PPSPM;
17) memantau, menganalisis, dan merekomendasikan kebutuhan pelatihan tentang penerapan program APU, PPT, dan PPPSPM bagi pegawai Pedagang;
18) memastikan seluruh kegiatan untuk penerapan program APU, PPT, dan PPPSPM terlaksana dengan baik; dan
19) melakukan tugas lain untuk penerapan program APU, PPT, dan PPPSPM.
    Contoh:
    Memastikan pemenuhan terhadap permintaan data dan informasi terkait setiap pihak yang telah dilaporkan oleh PPATK kepada penyidik, tersangka, atau terdakwa kepada aparat penegak hukum.

i. Penanggung jawab penerapan program APU, PPT, dan PPPSPM memiliki wewenang sebagai berikut:
   1) memperoleh akses terhadap informasi yang dibutuhkan yang ada di seluruh unit organisasi Pedagang;
   2) melakukan koordinasi dan pemantauan terhadap penerapan program APU, PPT, dan PPPSPM oleh unit kerja terkait;
   3) mengusulkan pejabat dan/atau pegawai unit kerja terkait untuk membantu penerapan program APU, PPT, dan PPPSPM;
   4) melaporkan Transaksi Keuangan Mencurigakan, termasuk yang dilakukan oleh Direksi, Dewan Komisaris, dan/atau pihak terafiliasi dengan Direksi atau Dewan Komisaris, secara langsung kepada Pusat Pelaporan dan Analisis Transaksi Keuangan; dan
   5) melakukan kewenangan lain untuk penerapan program APU, PPT, dan PPPSPM.
      Contoh:
      Mengusulkan program tambahan untuk mendukung penerapan program APU, PPT, dan PPPSPM kepada satuan kerja terkait atau Direksi.

IV. KEBIJAKAN DAN PROSEDUR

1. Kebijakan dan prosedur penerapan program APU, PPT, dan PPPSPM berdasarkan pendekatan berbasis risiko meliputi:
   a. identifikasi dan verifikasi calon Nasabah atau Nasabah;
   b. identifikasi dan verifikasi Pemilik Manfaat (*Beneficial Owner*);
   c. penutupan hubungan usaha atau penolakan transaksi;
   d. pengelolaan risiko TPPU, TPPT dan PPSPM 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 Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK)dan Kepolisian.

2. Pedagang harus melakukan reviu atas kebijakan dan prosedur sebanyak 1 (satu) kali dalam 1 (satu) tahun. Dalam hal sesuai kebutuhan Pedagang berdasarkan penilaian risiko TPPU, TPPT, dan/atau PPSPM, kegiatan usaha, skala usaha, kompleksitas usaha, karakteristik usaha, dan/atau peristiwa atau perkembangan besar dalam manajemen dan operasional Pedagang, reviu atas kebijakan dan prosedur dapat dilakukan lebih dari 1 (satu) kali dalam 1 (satu) tahun.
   Apabila berdasarkan reviu yang telah dilakukan Pedagang memandang perlu untuk dilakukan perubahan terhadap kebijakan dan prosedur yang telah dimiliki, perubahan tersebut harus disusun paling lama 6 (enam) bulan sejak hasil reviu.
3. Kebijakan dan prosedur sebagaimana dimaksud pada angka 1 harus memperhatikan prinsip mengenali pengguna jasa (*Know Your Costumer* (KYC)).
4. PMPJ/KYC sebagaimana dimaksud pada angka 1 terdiri atas CDD dan EDD, melalui CDD atau EDD:
   a. Pedagang dapat memperoleh informasi secara detail mengenai calon Nasabah, Nasabah, transaksi Nasabah termasuk Transaksi Keuangan Mencurigakan;
   b. Pedagang dapat melindungi reputasi dan integritas Pedagang, memfasilitasi kepatuhan terhadap ketentuan, dan melindungi Pedagang dari ancaman eksternal yaitu digunakan sebagai sarana TPPU, TPPT, dan/atau PPSPM; dan
   c. Pedagang harus selalu berhati-hati dalam menerima calon Nasabah serta terus melakukan pemantauan terhadap transaksi Nasabah yang menggunakan jasa Pedagang. Apabila transaksi yang dilakukan tidak sesuai dengan profil, karakteristik, atau kebiasaan pola transaksi dari Nasabah yang bersangkutan, maka Pedagang berkewajiban menyampaikan laporan Transaksi Keuangan Mencurigakan kepada PPATK.
5. CDD dilakukan oleh Pedagang pada saat:
   a. melakukan hubungan usaha dengan calon Nasabah atau transaksi dengan Nasabah;
   b. terdapat transaksi keuangan dengan mata uang rupiah dan/atau mata uang asing yang nilainya paling sedikit atau setara dengan Rp100.000.000,00 (seratus juta rupiah);
   c. terdapat indikasi Transaksi Keuangan Mencurigakan yang terkait dengan TPPU, TPPT, dan/atau PPSPM; atau
   d. Pedagang meragukan kebenaran informasi yang diberikan oleh calon Nasabah, Nasabah, penerima kuasa, dan/atau Pemilik Manfaat (*Beneficial Owner*).
6. CDD ulang dapat dilakukan oleh Pedagang apabila Pedagang menilai terdapat perubahan tingkat risiko yang disebabkan antara lain:
   a. peningkatan nilai transaksi yang signifikan;
   b. perubahan profil Nasabah yang bersifat signifikan; dan/atau

c. informasi pada profil Nasabah yang tersedia dalam profil Nasabah secara terpadu (*single customer identification file*) belum dilengkapi dengan dokumen pendukung dalam rangka verifikasi.

7. Sebelum pengembangan produk/jasa/layanan dan praktik usaha baru termasuk metode transaksi/jaringan distribusi (*delivery channels*) dan/atau penggunaan teknologi baru atau pengembangan teknologi untuk produk/jasa/layanan yang telah ada diluncurkan atau digunakan, Pedagang wajib mengidentifikasi dan melakukan penilaian risiko TPPU, TPPT, dan/atau PPSPM, serta melakukan tindakan memadai untuk mengelola dan memitigasi risiko.
8. Identifikasi Calon Nasabah dan Nasabah;
   a. Pedagang berkewajiban mengidentifikasi dan mengklasifikasikan calon Nasabah atau Nasabah ke dalam kelompok orang perseorangan (*natural person*), korporasi (*legal person*), dan perikatan lainnya (*legal arrangement*).
   b. Pedagang 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 sebagai berikut:
      1) permintaan informasi mengenai calon Nasabah, bukti identitas serta informasi dan/atau dokumen pendukung dari calon Nasabah sebagaimana dimaksud dalam Pasal 25, Pasal 26, Pasal 27, Pasal 28, dan Pasal 29 Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU, PPT, dan PPPSPM 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. Pedagang dapat melakukan penerimaan dan identifikasi calon Nasabah atau Nasabah secara elektronik sepanjang Sistem Elektronik Pedagang mampu untuk mengidentifikasi identitas dari calon Nasabah atau Nasabah.
   e. Dalam pelaksanaan penerimaan dan identifikasi calon Nasabah atau Nasabah secara elektronik, Pedagang 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 25, Pasal 26, Pasal 27, Pasal 28, dan Pasal 29 Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU, PPT, dan PPPSPM di sektor jasa keuangan dalam bentuk *softcopy* melalui laman atau aplikasi Pedagang.

g. Selain salinan dokumen sebagaimana dimaksud dalam huruf f, Pedagang dapat meminta data, dokumen, dan informasi tambahan yang dibutuhkan dalam mengidentifikasi dan memverifikasi calon Nasabah atau Nasabah yang penyampaiannya dilakukan melalui laman atau aplikasi Pedagang. 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 Pedagang.
   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 Pedagang; 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 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 Pedagang.

9. Verifikasi Calon Nasabah atau Nasabah
   a. Dalam rangka melakukan hubungan usaha dengan calon Nasabah atau transaksi dengan Nasabah, Pedagang 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, tanda tangan elektronik, 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 pegawai 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) DTTOT yang diterbitkan oleh Kepolisian Negara Republik Indonesia;
      b) DPPSPM; 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 calon Nasabah atau Nasabah.

e. Dalam hal proses verifikasi diselesaikan kemudian setelah dilakukannya hubungan usaha atau transaksi sebagaimana dimaksud pada huruf d, maka Pedagang 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 Pedagang; dan/atau
3) Pedagang meminta calon Nasabah untuk melengkapi dokumen yang dipersyaratkan dalam jangka waktu tertentu.

f. Pedagang dapat melakukan proses verifikasi calon Nasabah atau Nasabah secara elektronik sepanjang Sistem Elektronik yang digunakan Pedagang mampu untuk memverifikasi kebenaran identitas dari calon Nasabah atau Nasabah.

g. Dalam hal Pedagang melaksanakan proses verifikasi secara elektronik, maka Pedagang harus memperhatikan hal-hal sebagai berikut:
   1) Pedagang 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 Pedagang atau milik pihak ketiga;
      b) dalam hal verifikasi *face to face* dilakukan melalui sarana elektronik milik Pedagang, maka pelaksanaannya menggunakan perangkat lunak milik Pedagang dengan perangkat keras milik Pedagang 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, PPT, dan PPPSPM di sektor jasa keuangan;
      d) verifikasi *face to face* melalui sarana elektronik milik Pedagang dilakukan dalam bentuk sarana elektronik yang setara dengan *video banking* secara *real time* dan daring mempertemukan secara elektronik pegawai/pejabat Pedagang dengan calon Nasabah atau Nasabah.

Contoh: Fitur *video call* pada aplikasi yang dimiliki Pedagang yang terhubung langsung secara *real time* dan daring dengan pegawai/pejabat Pedagang 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 yang setara dengan *video banking* secara *real time* dan daring mempertemukan secara elektronik pegawai/pejabat Pedagang dengan calon Nasabah atau Nasabah;

f) verifikasi *face to face* secara elektronik milik Pedagang 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 Pedagang dalam melaksanakan proses verifikasi *face to face* melalui sarana elektronik milik Pedagang atau pihak ketiga, Pedagang 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 Pedagang 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 Pedagang dengan perangkat keras milik Pedagang atau perangkat keras milik Nasabah atau calon Nasabah.

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

(1) aplikasi milik Pedagang yang dapat diakses dengan perangkat gawai (*mobile device*) antara lain *smartphone* dan/atau komputer tablet; dan/atau

(2) situs *web* (*website)* Pedagang yang dapat diakses melalui perangkat elektronik calon Nasabah atau Nasabah antara lain komputer dan/atau laptop.

Pedagang 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 Pedagang bekerjasama dengan Kementerian yang menyelenggarakan urusan pemerintahan di bidang kependudukan dan pencatatan sipil untuk memperoleh 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; dan

c) untuk memberikan tambahan keyakinan bagi Pedagang dalam proses verifikasi *non-face to face* sebagaimana dimaksud pada huruf b), Pedagang 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 Pedagang, verifikasi yang dilakukan secara elektronik oleh Pedagang dapat memanfaatkan teknologi *artificial intelligence* atau algoritma lainnya yang dipadankan dengan *database* Pedagang.

10. Identifikasi dan Verifikasi Calon Nasabah dan Nasabah Berisiko Tinggi atau PEP
    a. Identifikasi Calon Nasabah atau Nasabah Berisiko Tinggi atau PEP

1) Dalam hal Pedagang menilai calon Nasabah atau Nasabah Berisiko Tinggi atau PEP, maka Pedagang berkewajiban menerapkan EDD.
2) Pedagang harus memiliki kebijakan dan prosedur identifikasi Nasabah atau Nasabah Berisiko Tinggi atau PEP.
3) Kebijakan dan prosedur identifikasi Nasabah atau Nasabah Berisiko Tinggi atau PEP sebagaimana dimaksud pada angka 2) paling sedikit mencakup ketentuan sebagaimana dimaksud dalam ketentuan identifikasi calon Nasabah atau Nasabah sebagaimana dimaksud pada angka 8.
4) Identifikasi calon Nasabah atau Nasabah Berisiko Tinggi atau PEP dapat dilakukan secara elektronik, sepanjang Sistem Elektronik Pedagang mampu untuk mengidentifikasi identitas resmi dari calon Nasabah atau Nasabah Berisiko Tinggi atau PEP.
5) Dalam hal identifikasi calon Nasabah atau 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 25, Pasal 26, Pasal 27, Pasal 28, dan Pasal 29 Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU, PPT, dan PPPSPM di sektor jasa keuangan secara elektronik (*softcopy*) melalui laman atau aplikasi Pedagang.
6) Selain salinan dokumen sebagaimana dimaksud dalam angka 5), Pedagang dapat meminta data, dokumen, dan informasi tambahan yang dibutuhkan dalam mengidentifikasi dan memverifikasi calon Nasabah secara elektronik yang penyampaiannya dilakukan melalui laman atau aplikasi Pedagang. Adapun contoh data, dokumen, dan informasi tambahan tersebut antara lain dapat berupa data dan informasi sebagaimana dimaksud pada angka 8 huruf g mengenai identifikasi calon Nasabah atau Nasabah.

b. Verifikasi calon Nasabah atau Nasabah Berisiko Tinggi atau PEP
1) Verifikasi calon Nasabah atau Nasabah Berisiko Tinggi atau PEP dilaksanakan dengan memperhatikan ketentuan sebagaimana dimaksud pada angka 9 huruf a, huruf b, huruf c, huruf d, dan huruf e.
2) Selain memperhatikan ketentuan sebagaimana dimaksud dalam angka 1), Pedagang dapat melakukan verifikasi calon Nasabah atau Nasabah Berisiko Tinggi atau PEP dalam pelaksanaan EDD dengan cara antara lain:
a) meminta atau mencari informasi tambahan mengenai profil Nasabah, seperti pekerjaan, sumber dana, sumber kekayaan Nasabah;
b) melakukan pengkinian atas data identitas Nasabah;
c) meminta atau mencari informasi tambahan mengenai alasan atau dasar dari transaksi yang dilakukan oleh Nasabah;
d) memperoleh persetujuan dari Pejabat Senior untuk memulai dan/atau melanjutkan hubungan usaha dan/atau transaksi; dan/atau

e) melakukan pemantauan yang semakin diperketat terhadap transaksi yang dilakukan oleh Nasabah tersebut.

3) Verifikasi calon Nasabah atau Nasabah Berisiko Tinggi atau PEP sebagaimana dimaksud dalam angka 1) dapat dilakukan secara elektronik.

4) Dalam hal Pedagang melakukan verifikasi calon Nasabah atau Nasabah Berisiko Tinggi atau PEP secara elektronik, maka Pedagang harus memperhatikan ketentuan sebagaimana dimaksud pada angka 9 huruf g.

11. Identifikasi dan Verifikasi Pemilik Manfaat (*beneficial owner*)

a. Identifikasi Pemilik Manfaat *(Beneficial Owner)*

1) Pedagang 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, Pedagang 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) Pedagang 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, Pedagang 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 Pedagang. Namun Pedagang 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, Pedagang tetap melakukan identifikasi dan verifikasi terhadap Pemilik Manfaat (*Beneficial Owner*) dengan menggunakan data dan informasi yang tersedia di publik.
8) Pengecualian terhadap keharusan penyampaian dokumen dan/atau identitas pengendali akhir Pemilik Manfaat (*Beneficial Owner*) sebagaimana dimaksud pada angka 7) harus didokumentasikan oleh Pedagang.
9) Apabila Pedagang meragukan atau tidak dapat meyakini identitas Pemilik Manfaat (*Beneficial Owner*), Pedagang berkewajiban untuk menolak untuk melakukan hubungan usaha dengan calon Nasabah atau transaksi dengan Nasabah.
10) Terhadap calon Nasabah atau Pemilik Manfaat (*Beneficial Owner*) yang hubungan usahanya ditolak, Pedagang harus memperoleh paling sedikit informasi nama, nomor identitas, alamat, dan tempat tanggal lahir sesuai dengan salinan dokumen identitas yang diperoleh Pedagang untuk kepentingan pelaporan Transaksi Keuangan Mencurigakan.
11) Identifikasi Pemilik Manfaat (*Beneficial Owner*) dapat dilaksanakan secara elektronik sepanjang Sistem Elektronik Pedagang mampu untuk mengidentifikasi identitas resmi dari Pemilik Manfaat (*Beneficial Owner*).
12) Untuk mengetahui apakah calon Nasabah atau Nasabah bertindak untuk kepentingan Pemilik Manfaat (*Beneficial Owner*), pelaksanaannya dapat dilakukan antara lain melalui penambahan pertanyaan apakah calon Nasabah atau Nasabah bertindak untuk kepentingan Pemilik Manfaat (*Beneficial Owner*) pada pengisian formulir elektronik yang diisi melalui laman atau aplikasi Pedagang.
13) 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, PPT, dan PPPSPM di sektor jasa keuangan, secara elektronik (*softcopy*) melalui laman atau aplikasi Pedagang.

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, tanda tangan elektronik, 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 pegawai 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) DTTOT yang diterbitkan oleh Kepolisian Negara Republik Indonesia;
         (2) DPPSPM; 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 Pedagang, 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 Pedagang mampu untuk memverifikasi kebenaran identitas resmi dari Pemilik Manfaat (*Beneficial Owner*).
5) Dalam hal Pedagang melakukan verifikasi Pemilik Manfaat (*Beneficial Owner*) secara elektronik, maka Pedagang harus memperhatikan ketentuan sebagaimana dimaksud pada angka 9 huruf g.

12. CDD Sederhana (*Simplified CDD*)
    a. Dalam hal Pedagang menilai bahwa calon Nasabah atau Nasabah berdasarkan hasil penilaian risiko terjadinya TPPU, TPPT, dan/atau PPSPM, profil risiko calon Nasabah atau transaksi yang dilakukan oleh Nasabah tergolong rendah dan memenuhi kriteria calon Nasabah atau Nasabah dengan profil dan karakteristik sederhana, Pedagang dapat menerapkan CDD sederhana (*simplified CDD*).
    b. Dalam hal Pedagang melaksanakan CDD sederhana (*simplified CDD*), Pedagang 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 Pedagang, misalnya Nasabah Berisiko Tinggi atau PEP tidak dimasukkan sebagai calon Nasabah atau Nasabah dengan perlakuan CDD sederhana (*simplified CDD*);
       3) memastikan persyaratan CDD sederhana mampu mengelola dan memitigasi tingkat ancaman TPPU, TPPT, dan/atau PPSPM;
       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 dan waktu dimulainya penerapan prosedur CDD sederhana. Contoh: Setelah melakukan analisis risiko Nasabah, Pedagang memutuskan akan menerapkan CDD sederhana pada kelompok Nasabah tertentu dengan melakukan perubahan atas kebijakan dan prosedur APU, PPT, dan PPPSPM yang dimiliki. Berdasarkan perubahan atas kebijakan dan prosedur APU dan PPT, CDD sederhana akan diberlakukan sejak tanggal 30 Maret, maka Pedagang 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 di dalamnya 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 TPPU, TPPT, dan/atau PPSPM;
2) memiliki tingkat risiko yang meningkat; dan/atau
3) tidak sesuai dengan tujuan awal pada saat registrasi sebagai Nasabah.

d. Pedagang dapat melakukan identifikasi dan verifikasi calon Nasabah atau Nasabah dalam rangka CDD sederhana secara elektronik sepanjang Sistem Elektronik Pedagang 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 Pedagang melakukan identifikasi dan verifikasi calon Nasabah atau Nasabah dalam rangka CDD sederhana secara elektronik, maka pelaksanaannya harus memperhatikan ketentuan sebagaimana dimaksud pada angka 8 huruf d, huruf e, huruf f, dan huruf g, serta angka 9 huruf g.

13. CDD Pihak Ketiga

a. Pedagang 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 Pedagang sesuai dengan prosedur Pedagang dan tunduk pada kendali Pedagang yang mendelegasikan atas penerapan prosedur tersebut.

c. Dalam hal telah tersedia hasil CDD yang telah dilakukan oleh pihak ketiga terhadap calon Nasabah, Pedagang dapat

menggunakan hasil CDD yang telah dilakukan oleh pihak ketiga terhadap calon Nasabah tersebut.

d. Dalam hal Pedagang menggunakan hasil CDD Pihak ketiga:
   1) tanggung jawab CDD tetap berada pada Pedagang tersebut.
   2) Pedagang harus memahami maksud dan tujuan hubungan usaha serta mengidentifikasi dan memverifikasi Nasabah dan Pemilik Manfaat (*Beneficial Owner*).
   3) Pedagang harus sesegera mungkin mendapatkan informasi yang diperlukan terkait dengan prosedur CDD.
   4) Pedagang harus memiliki kerja sama dengan pihak ketiga dalam bentuk kesepakatan tertulis, dimana dalam kesepakatan tertulis harus dipastikan terdapat klausula yang menegaskan bahwa Pedagang 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, PPT, dan PPPSPM, dan bukan untuk kepentingan lainnya seperti pemasaran. Contoh: kepentingan penerapan program APU, PPT, dan PPPSPM adalah pemenuhan permintaan informasi, data dan salinan dokumen pendukung Nasabah dari Otoritas Jasa Keuangan, PPATK, atau aparat penegak hukum.
   5) Pedagang 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 Pedagang dalam rangka penerapan program APU, PPT, dan PPPSPM.
   6) Pedagang 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 Pedagang 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) Pedagang harus memperhatikan informasi terkait risiko negara tempat pihak ketiga tersebut berasal.
   8) Dalam hal Pedagang 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 Pedagang;
b. konglomerasi keuangan (*financial group*) tersebut telah menerapkan CDD, penatausahaan dokumen dan program APU, PPT, dan PPPSPM secara efektif sesuai dengan Rekomendasi FATF;
c. terhadap negara berisiko tinggi telah dilakukan mitigasi risiko secara memadai oleh unit APU, PPT, dan PPPSPM berdasarkan kebijakan program APU, PPT, dan PPPSPM di tingkat konglomerasi keuangan (*financial group*); dan
d. konglomerasi keuangan (*financial group*) tersebut diawasi oleh otoritas yang berwenang.

9) Pedagang memastikan bahwa pihak ketiga berada dalam negara yang patuh terhadap standar Rekomendasi FATF.

14. Travel *Rule*

Pedagang dalam memberikan jasa perpindahan atau transfer Aset Keuangan Digital, Pedagang wajib menerapkan prinsip *Travel Rule* sebagai berikut:

a. dalam perpindahan atau transfer Aset Keuangan Digital lebih dari atau sama dengan nilai dalam Rupiah yang setara dengan USD1.000,00 (seribu dolar Amerika), keterangan dan/atau informasi yang diperoleh:
   1) pengirim meliputi:
      a) nama pengirim, alamat *Wallet* pengirim, dan alamat pengirim;
      b) kartu tanda penduduk wajib bagi warga negara Indonesia; dan
      c) paspor, kartu identitas yang diterbitkan oleh negara asal Nasabah, kartu izin tinggal tetap atau kartu izin tinggal terbatas bagi warga negara asing jika dimungkinkan untuk diperoleh;
   2) penerima meliputi:
      a) nama penerima;
      b) alamat *wallet* penerima; dan
      c) alamat penerima; dan
b. dalam perpindahan atau transfer Aset Keuangan Digital kurang dari nilai dalam Rupiah yang setara dengan USD1.000,00 (seribu dolar Amerika),keterangan dan/atau informasi yang diperoleh:
   1) pengirim meliputi:
      a) nama pengirim; dan
      b) alamat *wallet* pengirim; dan
   2) penerima meliputi:
      a) nama penerima; dan
      b) alamat *wallet* penerima.

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

a. Pedagang berkewajiban memiliki sistem pengenalan dan pemantauan transaksi Aset Keuangan Digital, dengan menggunakan sistem berbasis *regulatory technology*, untuk memantau dan meninjau transaksi pengenalan dan pemantauan transaksi saat ini dan rekam jejaknya di masa lampau guna mengetahui ada tidaknya transaksi mencurigakan yang menyertai Aset Keuangan Digital. Contoh: Aplikasi analisis data *blockchain* (*blockchain analytic tools*)

merupakan aplikasi yang dapat mengumpulkan, memproses, dan menganalisis data dari *blockchain* baik yang berbayar maupun disediakan secara publik (*open source*).

b. Sistem pengenalan dan pemantauan transaksi Aset Keuangan Digital sebagaimana dimaksud pada huruf a, sedikitnya mampu mendeteksi hal sebagai berikut:
   1) transaksi Aset Keuangan Digital terindikasi dilakukan oleh Nasabah Berisiko Tinggi;
   2) transaksi Aset Keuangan Digital terkait TPPU, TPPT, dan/atau PPSPM;
   3) indikasi transaksi *red flag* berdasarkan Rekomendasi FATF; dan
   4) transaksi Aset Keuangan Digital terindikasi menggunakan metode, teknik, atau upaya meningkatkan anonimitas, berkurangnya transparansi, dan mengaburkan arus keuangan, contoh: *anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, privacy wallets*.

c. Dalam hal sistem pemantauan sebagaimana dimaksud pada huruf a mengindikasikan terdapat Transaksi Keuangan Mencurigakan Pedagang harus:
   1) menolak pemindahan atau transfer Aset Keuangan Digital Nasabah dari *wallet* Pedagang kepada *wallet* penerima yang terindikasi TPPU, TPPT, dan/atau PPPSPM;
   2) membekukan akun Nasabah yang menerima pemindahan atau transfer Aset Keuangan Digital dari *wallet* yang terindikasi TPPU, TPPT, dan/atau PPPSPM; dan/atau
   3) menutup/memutuskan hubungan usaha dengan Nasabah.

d. Pedagang dilarang membuka atau memelihara akun anonim atau rekening yang menggunakan nama fiktif.

e. Pedagang 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 Pedagang;
   2) Pedagang tidak dapat meyakini kebenaran identitas dan kelengkapan dokumen;
   3) transaksi masuk (*incoming transfer*) pada akun Nasabah, namun setelah Nasabah 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 DTTOT; dan/atau
   7) tercatat dalam DPPSPM.

f. Pedagang berkewajiban memberitahukan secara tertulis kepada Nasabah mengenai penutupan hubungan usaha.

g. Pemberitahuan tertulis dapat dilakukan dengan penyampaian surat yang ditujukan kepada Nasabah sesuai dengan alamat

yang tercantum dalam *database* Pedagang atau diumumkan melalui media cetak, media elektronik, maupun media lainnya.

h. Dalam hal Pedagang melakukan penolakan hubungan usaha dengan calon Nasabah atau penolakan transaksi atau penutupan/pemutusan hubungan usaha dengan Nasabah, maka Pedagang berkewajiban melaporkannya kepada PPATK mengenai tindakan penolakan hubungan usaha atau transaksi atau penutupan/pemutusan hubungan usaha tersebut sebagai Transaksi Keuangan Mencurigakan.

i. Dalam hal pemberitahuan tertulis telah dilakukan dan Nasabah tidak mengambil sisa dana yang tersimpan di Pedagang, 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.

j. Pedagang harus mendokumentasikan calon Nasabah atau Nasabah yang terkena penolakan transaksi atau penutupan hubungan usaha sebagaimana dimaksud pada huruf c dan huruf e dalam daftar tersendiri.

16. Pengelolaan risiko TPPU, TPPT, dan/atau PPSPM yang berkelanjutan

a. Pedagang harus memiliki kebijakan dan prosedur untuk mengelola risiko berkelanjutan terkait risiko TPPU, TPPT dan/atau PPSPM, dimana pengelolaan risiko tersebut tidak hanya dilakukan pada saat Pedagang melakukan pembukaan hubungan usaha dengan calon Nasabah atau transaksi dengan Nasabah.

b. Kebijakan dan prosedur untuk mengelola risiko TPPU, TPPT dan/atau PPSPM secara berkelanjutan mencakup:

1) Identifikasi risiko

Dalam melakukan identifikasi risiko, Pedagang harus menilai risiko TPPU, TPPT dan/atau PPSPM, 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 Pedagang terhadap peningkatan risiko TPPU, TPPT dan/atau PPSPM 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.

17. Pemeliharaan data yang akurat terkait dengan Nasabah dan transaksi Nasabah

a. Pemeliharaan data yang akurat terkait Nasabah dan transaksi Nasabah tidak hanya berguna bagi Pedagang dalam *risk management* dan pengembangan usaha, tetapi juga diperlukan sebagai upaya untuk membantu pihak yang berwenang dalam melakukan pengawasan kepatuhan, pemeriksaan dugaan TPPU, TPPT, dan/atau PPSPM, serta penyelidikan dan penyidikan terhadap dana yang diindikasikan berasal dari kejahatan sehingga dokumen yang disimpan oleh Pedagang harus memadai untuk dapat digunakan sebagai alat bukti (jika diperlukan) oleh aparat penegak hukum.
b. Pedagang 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. Pedagang 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 Transaksi Keuangan Mencurigakan.
d. dokumen sebagaimana disebutkan dalam huruf b dan huruf c dapat disimpan melalui format data atau dokumen elektronik dalam *database* Pedagang 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* Pedagang, Pedagang 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.

18. Pengkinian Data Nasabah
    a. Pedagang harus melakukan pengkinian data Nasabah sesuai dengan ketentuan sebagaimana dimaksud dalam Peraturan Otoritas Jasa Keuangan mengenai penerapan program APU, PPT, dan PPPSPM 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. Kegiatan pengkinian data, informasi, dan/atau dokumen pendukung Nasabah didasarkan pada tingkat risiko TPPU, TPPT, dan/atau PPSPM dari Nasabah tersebut dan difokuskan pada Nasabah berisiko lebih tinggi terlebih dahulu.

c. Pengkinian data berdasarkan tingkat risiko Nasabah sebagaimana dimaksud huruf b diperoleh dari hasil penilaian risiko Nasabah yang dituangkan dalam penggolongan Nasabah berdasarkan tingkat risiko dilakukan dengan memperhatikan skala usaha, kompleksitas usaha, karakteristik usaha, dan/atau peristiwa atau perkembangan besar dalam manajemen dan operasional Pedagang, sebagai contoh:
   1) Pedagang dengan kapasitas pengkinian data yang telah diotomatisasi dan mampu melaporkan seluruh tingkat risiko secara *real time*, dikinikan tiap tahun.
   2) Pedagang dengan kapasitas pengkinian data terbatas, dilakukan dengan:
      a) Nasabah Berisiko Tinggi, dikinikan paling sedikit 1 (satu) tahun sekali;
      b) Nasabah berisiko menengah, dikinikan paling sedikit 2 (dua) tahun sekali; dan
      c) Nasabah berisiko rendah, dikinikan paling sedikit 3 (tiga) tahun sekali.

d. Dalam melakukan pengkinian data, informasi, dan/atau dokumen pendukung Nasabah (pengkinian data Nasabah), Pedagang 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.

e. Dalam hal sumber daya yang dimiliki Pedagang 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 profil Nasabah secara terpadu (*single customer identification file*) tidak sesuai dengan profil Nasabah.

f. 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 TPPU, TPPT, dan/atau PPSPM;
   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 Nasabah;
   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 DTTOT;
9) tercantum dalam DPPSPM; dan/atau
10) transaksi yang diduga terkait dengan hasil TPPU, TPPT, dan/atau PPSPM.

g. 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.

h. Pedagang 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.

i. Berkaitan dengan pengkinian DTTOT dan DPPSPM, Pedagang:
1) harus memelihara DTTOT dan DPPSPM;
2) harus mencocokkan kesesuaian nama dan informasi Nasabah yang ada di Pedagang dengan nama dan informasi yang ada di dalam DTTOT dan DPPSPM yang disampaikan oleh Otoritas Jasa Keuangan;
3) harus mencocokkan kesesuaian nama dan informasi calon Nasabah yang akan menjadi Nasabah Pedagang dengan nama dan informasi yang ada di dalam DTTOT dan DPPSPM yang telah diterima oleh Pedagang; dan
4) dapat menjadikan DTTOT dan DPPSPM yang sudah dilakukan pengkinian sebagai alat *screening* pada saat melakukan hubungan usaha dengan calon Nasabah.

j. Pedagang dapat melakukan pengkinian data Nasabah secara elektronik. Dalam hal Pedagang melakukan proses pengkinian data secara elektronik maka:
1) Pedagang harus tetap memperhatikan hal-hal sebagaimana dimaksud dalam huruf a sampai dengan huruf j.
2) Pedagang 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, Pedagang memunculkan notifikasi dalam aplikasi atau situs web 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 Pedagang 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, Pedagang memunculkan fitur khusus yang bersifat *pop-up* untuk digunakan oleh Nasabah mengkinikan data pada saat Nasabah membuka aplikasi dan/atau situs web Pedagang dimana aplikasi akan terbuka setelah pengkinian data telah dilakukan oleh Nasabah.

k. Pedagang harus menatausahakan dan mendokumentasikan proses pengkinian data Nasabah.

l. 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* Pedagang.

19. Tindak Lanjut Terhadap DTTOT dan/atau DPPSPM

a. Pedagang harus memelihara dan mengkinikan DTTOT dan/atau DPPSPM yang disampaikan oleh Otoritas Jasa Keuangan melalui sistem yang disediakan oleh Otoritas Jasa Keuangan. Adapun pemeliharaan tersebut bertujuan untuk memastikan Pedagang tidak melakukan hubungan usaha dengan calon Nasabah atau melakukan Transaksi dengan Nasabah yang memiliki kesamaan identitas dan informasi dengan identitas dan informasi yang ada di dalam DTTOT dan DPPSPM.

b. Pedagang tidak diperbolehkan menyediakan, memberikan, atau meminjamkan dana kepada atau untuk kepentingan orang atau korporasi yang identitasnya tercantum dalam DTTOT dan/atau DPPSPM. Adapun yang dimaksud dengan dana adalah semua aset atau benda bergerak atau tidak bergerak, baik yang berwujud maupun yang tidak berwujud, yang diperoleh dengan cara apapun dan dalam bentuk apapun, termasuk dalam format digital atau elektronik, alat bukti kepemilikan, atau keterkaitan dengan semua aset atau benda tersebut, termasuk tetapi tidak terbatas pada kredit bank, cek perjalanan, cek yang dikeluarkan oleh bank, perintah pengiriman uang, saham, sekuritas, obligasi, bank draft, surat pengakuan utang, dan Aset Keuangan Digital.

c. Pedagang harus melakukan:

1) identifikasi dan memastikan kesesuaian identitas dan informasi lain (antara lain tempat tanggal lahir dan alamat Nasabah) mengenai Nasabah dengan identitas dan informasi lain yang tercantum dalam DTTOT dan/atau DPPSPM; dan

2) mitigasi risiko atas kemungkinan terjadinya *false positive* atau *false negative*, sejak Pedagang menerima DTTOT dan/atau DPPSPM.

Adapun yang dimaksud dengan *"false positive"* adalah kesalahan pelaksanaan Pemblokiran secara serta merta yang dilakukan oleh Pedagang yang dikarenakan sistem informasi Nasabah pada Pedagang menemukan adanya kesesuaian sebagian informasi Nasabah yang berada dalam *database* Nasabah yang ada di Pedagang dengan

identitas orang perseorangan atau korporasi yang tercantum dalam DTTOT dan/atau DPPSPM.

Yang dimaksud dengan *"false negative"* adalah kesalahan tidak dilakukannya Pemblokiran secara serta merta oleh Pedagang yang dikarenakan sistem informasi Nasabah pada Pedagang menemukan adanya kesesuaian atas sebagian informasi Nasabah yang berada dalam *database* Nasabah yang ada di Pedagang dengan identitas orang atau korporasi yang tercantum dalam DTTOT dan/atau DPPSPM, namun kurang memperhatikan adanya kesesuaian seluruh informasi.

d. Dalam hal terdapat kesesuaian identitas dan informasi lain terkait Nasabah atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT dan/atau DPPSPM, Pedagang harus melakukan Pemblokiran secara serta merta tanpa penundaan dan tanpa pemberitahuan sebelumnya kepada Nasabah atau Pemilik Manfaat (*Beneficial Owner*), dengan perlu mengacu pula pada peraturan perundang-undangan lain yang mengatur hal tersebut.

   Dalam hal dilakukan Pemblokiran secara serta merta tanpa penundaan, hak-hak bagi Nasabah yang diblokir tetap diberikan sesuai dengan ketentuan yang berlaku di Pedagang, namun hak-hak tersebut tetap termasuk dalam objek yang dilakukan Pemblokiran.

e. Pemblokiran dilakukan terhadap dana yang dimiliki atau dikuasai, baik secara langsung maupun tidak langsung, yang diperoleh dengan cara apapun dan dalam hal apapun, oleh Nasabah atau Pemilik Manfaat (*Beneficial Owner*), baik sepenuhnya maupun secara bersama-sama dengan pihak lain.

f. Dalam hal terdapat kesesuaian identitas dan informasi lain terkait calon Nasabah, Nasabah, dan/atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT dan/atau DPPSPM, Pedagang harus melaporkannya sebagai laporan Transaksi Keuangan Mencurigakan kepada PPATK.

g. Pedagang yang melakukan Pemblokiran secara serta merta tanpa penundaan terkait DTTOT harus:
   1) membuat berita acara Pemblokiran secara serta merta tanpa penundaan; dan
   2) menyampaikan laporan Pemblokiran secara serta merta dimaksud dengan melampirkan berita acara Pemblokiran secara serta merta tanpa penundaan kepada Kepolisian Negara Republik Indonesia dengan tembusan kepada Otoritas Jasa Keuangan.

h. Pedagang yang melakukan Pemblokiran secara serta merta tanpa penundaan terkait DPPSPM harus:
   1) membuat berita acara Pemblokiran secara serta merta tanpa penundaan; dan
   2) menyampaikan laporan Pemblokiran secara serta merta dimaksud dengan melampirkan berita acara Pemblokiran secara serta merta tanpa penundaan dimaksud kepada PPATK dengan tembusan kepada Otoritas Jasa Keuangan.

i. Dalam hal tidak ditemukan kesesuaian identitas dan informasi lain terkait Nasabah dengan identitas dan informasi lain yang tercantum dalam DTTOT, Pedagang harus membuat dan

menyampaikan laporan nihil kepada Kepolisian Negara Republik Indonesia dengan tembusan kepada Otoritas Jasa Keuangan.

j. Dalam hal tidak ditemukan kesesuaian identitas dan informasi lain terkait Nasabah dengan identitas dan informasi lain yang tercantum dalam DPPSPM, Pedagang harus membuat dan menyampaikan laporan nihil kepada PPATK dengan tembusan kepada Otoritas Jasa Keuangan.

k. Pedagang harus mengidentifikasi, menilai, memahami, dan memitigasi risiko penghindaran sanksi (*sanction evasion*) terkait DTTOT dan/atau DPPSPM yang dilakukan oleh Calon Nasabah, Nasabah, dan/atau Pemilik Manfaat (*Beneficial Owner*).

l. Adapun yang dimaksud dengan penghindaran sanksi (*sanction evasion*) adalah upaya penghindaran sanksi yang dilakukan pihak yang identitasnya tercantum dalam DTTOT dan/atau DPPSPM yang melakukan hubungan usaha dan/atau transaksi keuangan dengan atau atas nama pihak lain dengan tujuan untuk menghindari terdeteksinya Transaksi Keuangan Mencurigakan.

   Sebagai contoh, adanya calon Nasabah, Nasabah, dan/atau Pemilik Manfaat (*Beneficial Owner*) yang melakukan hubungan usaha dan/atau transaksi melalui modus:

   1) dilakukan untuk kepentingan dan/atau atas arahan, baik secara langsung maupun tidak langsung, dari pihak yang tercantum identitasnya dalam DTTOT dan/atau DPPSPM;
   2) dikendalikan oleh pihak yang tercantum identitasnya dalam DTTOT dan/atau DPPSPM; dan/atau
   3) dilakukan untuk membantu pihak yang tercantum identitasnya dalam DTTOT dan/atau DPPSPM dalam rangka penghindaran sanksi.

20. Pemantauan Nasabah dan Transaksi Nasabah

    a. Pedagang 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 Pedagang 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;
       3) apabila diperlukan, Pedagang dapat meminta informasi tentang latar belakang dan tujuan transaksi terhadap transaksi yang tidak sesuai dengan profil Nasabah dengan memperhatikan ketentuan *anti-tipping off*; dan
       4) Ketentuan *anti-tipping off* adalah ketentuan yang melarang Pedagang memberitahukan kepada Nasabah atau pihak lain manapun, baik secara langsung maupun tidak langsung, dengan cara apapun mengenai laporan Transaksi Keuangan Mencurigakan 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) DTTOT;
      b) DPPSPM; 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. Pedagang 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 Pedagang melakukan pemantauan profil dan transaksi Nasabah secara elektronik, Pedagang 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. Pedagang 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. Pedagang 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* Pedagang.

21. Rekam Jejak Transaksi dan Penerimaan Nasabah
    a. Pedagang harus memiliki rekam jejak atas kegiatan transaksi dan penerimaan Nasabah.
    b. Rekam jejak kegiatan transaksi dan penerimaan Nasabah digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya.

c. Pelaksanaan rekam jejak kegiatan transaksi dan penerimaan Nasabah mencakup paling sedikit:
   1) memelihara log transaksi sesuai kebijakan retensi data Pedagang, 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 kegiatan transaksi dan penerimaan Nasabah dilakukan oleh pihak ketiga, maka proses jejak kegiatan transaksi dan penerimaan Nasabah tersebut harus sesuai dengan standar yang ditetapkan kepada Pedagang sebagaimana dimaksud angka 1), 2), dan 3).

d. Proses rekam jejak transaksi dan penerimaan nasabah dapat dilakukan secara elektronik antara lain dengan:
   1) log atau rekaman elektronik transaksi dalam *database* Pedagang;
   2) notifikasi melalui *e-mail, short message service* (SMS), laman, atau aplikasi Pedagang kepada Nasabah apabila suatu transaksi telah berhasil dilakukan; dan
   3) sistem peringatan dini (*early warning system*) untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan.

22. 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 Pedagang;
       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 Pedagang 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, PPT, dan PPPSPM terkait jumlah calon Nasabah atau Nasabah 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, PPT, dan PPPSPM secara keseluruhan sebagaimana kebijakan dan prosedur tertulis yang telah ditetapkan oleh Pedagang; dan
6) Direksi dapat mengusulkan pembaruan kebijakan dan prosedur dalam hal terdapat perkembangan risiko yang perlu dimitigasi oleh Pedagang yang belum tercantum dalam kebijakan dan prosedur tertulis.

23. Kebijakan dan Prosedur Pelaporan kepada PPATK
    a. Pedagang harus memiliki kebijakan dan prosedur kewajiban pelaporan kepada PPATK sesuai dengan ketentuan dan tata cara pelaporan sebagaimana dimaksud dalam peraturan perundang-undangan mengenai pencegahan dan pemberantasan TPPU, TPPT, dan/atau PPSPM, 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 Transaksi Keuangan Mencurigakan, laporan terkait DPPSPM, dan laporan lain terkait penerapan program APU, PPT, dan PPPSPM dalam hal terdapat permintaan informasi dari PPATK.
24. Kebijakan dan Prosedur Pelaporan kepada Kepolisian Negara Republik Indonesia

    Pedagang harus memiliki kebijakan dan prosedur kewajiban pelaporan kepada Kepolisian Negara Republik Indonesia mengenai laporan terkait DTTOT, dan laporan lain terkait penerapan program APU, PPT, dan PPPSPM dalam hal terdapat permintaan informasi dari Kepolisian Negara Republik Indonesia.

V. PENGENDALIAN INTERN

1. Pengendalian Intern secara Umum
    a. Penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*) yang efektif harus diimplementasikan dalam pengendalian intern dan diinternalisasikan dalam proses bisnis Pedagang.
    b. Pedagang wajib memiliki sistem pengendalian intern yang efektif dan independen. Sistem dimaksud untuk memastikan kepatuhan Pedagang dalam menerapkan program APU, PPT, dan PPPSPM secara efektif dan untuk meminimalkan risiko TPPU, TPPT, dan/atau PPSPM yang dihadapi Pedagang.
    c. Dalam pengendalian intern, Pedagang harus memperhatikan hal-hal sebagai berikut:
        1) skala dan kompleksitas Pedagang;
        2) kegiatan usaha atau operasional Pedagang, termasuk aspek area geografis/negara, profil Nasabah, produk atau jasa, dan aktivitas transaksi Pedagang secara keseluruhan;
        3) jaringan distribusi (*delivery channels*) yang digunakan;
        4) volume dan intensitas transaksi;

5) tingkat penilaian risiko atas setiap kegiatan usaha Pedagang; dan/atau
6) hubungan usaha antara Pedagang dengan Nasabah baik secara langsung, koresponden, atau komunikasi tanpa pertemuan langsung (*non-face to face*).

d. Pedagang harus memiliki sistem pengendalian intern yang efektif dan independen untuk memastikan bahwa seluruh fungsi penerapan program APU, PPT, dan PPPSPM berjalan sesuai dengan kebijakan dan prosedur yang telah ditetapkan. Sistem pengendalian yang efektif dan independen dapat dibuktikan:
1) kebijakan, prosedur, dan pemantauan intern yang memadai yang mampu secara tepat waktu mendeteksi kelemahan dan penyimpangan yang terjadi dalam penerapan program APU, PPT, dan PPPSPM;
2) batasan wewenang dan tanggung jawab satuan kerja terkait dengan penerapan program APU, PPT, dan PPPSPM, dimana Pedagang harus memastikan adanya pemisahan tugas, wewenang dan tanggung jawab yang jelas antara unit khusus pengendalian intern, fungsi atau pejabat yang ditunjuk untuk melaksanakan fungsi pengendalian intern dengan unit bisnis Pedagang lainnya;
3) penunjukan unit kerja khusus dan/atau pejabat yang bertanggung jawab dalam penerapan program APU, PPT, dan PPPSPM;
4) pengkinian standar kepatuhan penerapan program APU, PPT, dan PPPSPM;
5) kebijakan, prosedur, dan pemantauan terkait penyaringan/rekrutmen pegawai Pedagang, untuk memastikan tidak digunakannya pegawai Pedagang sebagai sarana TPPU, TPPT, dan PPSPM melalui proses bisnis Pedagang;
6) pemantauan terhadap Nasabah, transaksi Nasabah, dan/atau penggunaan Sistem Elektronik dalam proses bisnis Pedagang khususnya yang memiliki risiko tinggi TPPU, TPPT, dan PPSPM 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;
7) penyediaan sistem yang dapat melakukan identifikasi, pemantauan, dan pelaporan Transaksi Keuangan Mencurigakan secara akurat;
8) melakukan tinjauan (*review*) atas penilaian risiko dan manajemen proses;
9) pengawasan yang memadai sebelum penawaran Aset Keuangan Digital, Aset Kripto, produk atau jasa baru, penggunaan teknologi baru atau penawaran produk/jasa yang dimodifikasi sedemikian rupa yang berpotensi terhadap peningkatan risiko TPPU, TPPT, dan/atau PPSPM;
10) penyampaian informasi secara cepat dan tepat dalam hal terdapat indikasi dan/atau dugaan terkait risiko TPPU, TPPT, dan/atau PPSPM, langkah perbaikan yang dilakukan, hasil identifikasi kelemahan atas peraturan yang dimiliki, rencana tindak lanjut untuk perbaikan, dan

pelaporan yang telah disampaikan kepada pihak berwenang;

11) kepatuhan terhadap ketentuan peraturan perundang-undangan, persyaratan pelaporan, serta rekomendasi terkait kepatuhan atas penerapan program APU, PPT, dan PPPSPM, dan melakukan pengkinian atas perubahan ketentuan peraturan perundangan-undangan;
12) penerapan kebijakan, prosedur, dan kontrol atas CDD dan EDD;
13) pengawasan yang memadai terkait Nasabah, transaksi dan produk yang berisiko tinggi, seperti batasan transaksi atau persetujuan manajemen;
14) pengawasan yang memadai terhadap pegawai Pedagang yang melengkapi laporan, menerima hibah, memantau aktivitas yang mencurigakan, atau terlibat dalam kegiatan lain yang merupakan bagian dari penerapan program APU, PPT, dan PPPSPM;
15) pengintegrasian kepatuhan terhadap penerapan program APU, PPT, dan PPPSPM dalam deskripsi pekerjaan dan evaluasi kinerja yang tepat;
16) pelatihan terkait penerapan program APU, PPT, dan PPPSPM yang tepat dan relevan untuk semua pegawai;
17) pengujian terhadap efektivitas dari pelaksanaan program APU, PPT, dan PPPSPM dengan mengambil contoh secara acak (*random sampling*) serta melakukan pendokumentasian atas pengujian yang dilakukan; dan
18) pemeriksaan secara independen untuk memastikan kepatuhan dan efektivitas penerapan APU, PPT, dan PPPSPM yang pelaksanaannya sesuai dengan kebutuhan dan kompleksitas usaha Pedagang.

e. Dalam melakukan pengendalian intern, Pedagang dapat menggunakan *regulatory technology* seperti algoritma, pemanfaatan teknologi *artificial intelligence*, dan/atau *machine learning*.
f. Dalam hal Pedagang melakukan pengendalian intern dengan menggunakan *regulatory technology* sebagaimana dimaksud dalam huruf e, Pedagang harus memastikan *regulatory technology* yang digunakan dalam sistem pengendalian intern:
   1) didasarkan pada hasil penilaian risiko yang di dalamnya memuat bagaimana Pedagang mengelola dan memitigasi risiko atas Sistem Elektronik yang digunakan;
   2) terjamin keandalannya dan telah tersertifikasi oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi; dan
   3) terjamin keamanan data dan informasinya, termasuk penggunaan *security tools* seperti teknologi enkripsi, penggunaan *anti virus*, dan *firewall*.
g. Penanggung jawab atas pelaksanaan pengendalian intern dalam rangka penerapan program APU, PPT, dan PPPSPM dapat dilaksanakan oleh penanggung jawab yang menjalankan fungsi kepatuhan atau fungsi audit internal.
h. Pedagang dapat memiliki sistem pelaporan dugaan terjadinya pelanggaran (*whistleblowing system*/WBS) yang dimaksudkan untuk menjaga integritas profesionalitas, dan akuntabilitas Pedagang. Sistem tersebut memungkinkan pihak internal perusahaan (pegawai) 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) Pedagang.

i. Sistem pelaporan dugaan terjadinya pelanggaran (*whistleblowing system*/WBS) paling sedikit mencakup:
   1) sistem pelaporan yang independen, bebas, dan rahasia;
   2) pelindungan kerahasiaan identitas pelapor;
   3) pelindungan terhadap pelapor dari tekanan, pemecatan, gugatan hukum hingga tindakan fisik. Pelindungan tidak hanya untuk pelapor tetapi juga dapat diperluas hingga ke anggota keluarga pelapor; dan
   4) informasi pelaksanaan tindak lanjut berupa kapan dan bagaimana serta kepada institusi mana tindak lanjut WBS.

j. Unit kerja independen yang mengelola sistem pelaporan dugaan terjadinya pelanggaran (*whistleblowing system*/WBS) dapat dirangkap oleh pejabat yang ditunjuk sebagai penanggung jawab fungsi penerapan program APU PPT PPPSPM sebagaimana dimaksud pada huruf d angka 3.

2. Pengendalian Intern atas Sistem Elektronik dalam Proses Bisnis Pedagang
   a. Pedagang harus memastikan bahwa pengendalian intern atas Sistem Elektronik dalam proses bisnis Pedagang cukup memadai dan efektif dalam penerapan program APU, PPT, dan PPPSPM, dan mampu mengantisipasi kemungkinan Sistem Elektronik yang digunakan Pedagang tidak dimanfaatkan sebagai sarana TPPU, TPPT, dan/atau PPSPM.
   b. Pedagang harus memastikan kelangsungan dan kestabilan operasional Sistem Elektronik serta melakukan mitigasi risiko yang berpotensi dapat mengganggu kegiatan operasional Pedagang.
   c. Dalam hal Pedagang menggunakan pihak penyedia jasa teknologi informasi yang digunakan dalam penerapan program APU, PPT, dan PPPSPM, Pedagang harus memastikan pihak penyedia jasa teknologi informasi tersebut telah menerapkan manajemen risiko penggunaan Sistem Elektronik. Sebagai contoh pihak penyedia jasa telah memiliki sertifikasi dari lembaga resmi.

VI. SISTEM INFORMASI MANAJEMEN

1. Pedagang wajib memiliki sistem informasi manajemen yang dapat mengidentifikasi, menganalisa, memantau, dan menyediakan laporan secara efektif mengenai karakteristik atau kebiasaan pola transaksi yang dilakukan oleh Nasabah.
2. Sistem informasi manajemen sebagaimana dimaksud pada angka 1 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 Pedagang, 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 Pedagang.

3. Pedagang harus memastikan sistem elektronik yang digunakan dalam sistem informasi manajemen terjamin keandalannya dan telah didasarkan pada hasil penilaian risiko yang di dalamnya memuat bagaimana Pedagang mengelola dan memitigasi risiko atas sistem elektronik yang digunakan.
4. Kebijakan dan prosedur tertulis yang dimiliki Pedagang diwajibkan untuk mempertimbangkan faktor sistem elektronik yang berpotensi disalahgunakan oleh pelaku TPPU, TPPT, dan/atau PPSPM, misalnya membuka akun melalui internet, atau perintah transfer dana melalui faksimili atau telepon, dan transaksi elektronik lainnya.
5. Pedagang 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.
6. Pedagang harus memelihara pangkalan data (*database)* PEP, DTTOT, dan DPPSPM.
7. Untuk memudahkan pemantauan dalam rangka menganalisis transaksi keuangan yang mencurigakan, Pedagang harus memiliki dan memelihara profil Nasabah secara terpadu (*single customer identification file*).
8. Informasi yang terdapat dalam profil Nasabah secara terpadu (*single customer identification file*) mencakup seluruh Aset Keuangan Digital, Aset Kripto, produk dan/atau layanan lainnya yang disediakan oleh Pedagang yang dimiliki oleh Nasabah.
9. Untuk memastikan sistem informasi manajemen tetap berjalan dengan baik dan efektif, Pedagang 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 Sistem Elektronik;
      2) menggunakan Sistem Elektronik yang sudah tersertifikasi sesuai dengan peraturan perundang-undangan;
      3) memiliki Sistem Elektronik yang saling terhubung dan saling mendukung;
      4) menggunakan perangkat lunak (*software*) yang legal;
      5) memiliki kebijakan dan prosedur internal terkait Sistem Elektronik 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 pelindungan data pribadi dan pencegahan serangan siber (*cyberattack*) dalam Sistem Elektronik yang dikelolanya;
7) mengadakan pelatihan pencegahan kegagalan pelindungan data pribadi dalam Sistem Elektronik yang dikelolanya;
8) melakukan audit atas Sistem Elektronik (IT audit) secara berkala dan/atau dalam hal diperlukan sesuai dengan kebutuhan Pedagang yang dimaksudkan untuk memastikan keandalan Sistem Elektronik yang digunakan dan untuk memastikan agar Sistem Elektronik tidak digunakan/dimanfaatkan oleh pelaku TPPU, TPPT, dan PPSPM; dan/atau
9) melakukan edukasi kepada Nasabah terkait keamanan data pribadi dan pencegahan serangan siber (*cyberattack*).

b. pelindungan 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 Pedagang melalui perangkat keras milik Nasabah (contohnya *smartphone*) dibatasi sesuai ketentuan peraturan perundang-undangan.

c. Apabila pemilik data pribadi tidak lagi menjadi Nasabah, Pedagang harus menyimpan data pribadi tersebut sesuai batas waktu sebagaimana dimaksud pada huruf b angka 3) terhitung sejak tanggal terakhir pemilik data pribadi menjadi Nasabah.
d. pusat data (*data center)* dan pusat pemulihan bencana (*disaster recovery center*) yang digunakan oleh Pedagang dijalankan sesuai dengan peraturan perundang-undangan.

VII. SUMBER DAYA MANUSIA DAN PELATIHAN

1. Sumber daya manusia
a. Untuk mencegah Pedagang digunakan sebagai media atau tujuan TPPU, TPPT, dan PPSPM yang melibatkan pihak internal, Pedagang berkewajiban melakukan:
1) prosedur penyaringan dalam rangka penerimaan pegawai baru (*pre-employee screening*) baik pegawai tetap maupun pegawai tidak tetap (pegawai dalam masa percobaan sebelum diangkat menjadi pegawai tetap, pegawai dalam masa pendidikan sebelum diangkat menjadi pegawai tetap, dan/atau pegawai kontrak), termasuk Pejabat Senior, tenaga ahli, dari mulai tingkat paling rendah sampai dengan 1 (satu) tingkat di bawah Direksi dan Dewan Komisaris; dan
2) pengenalan dan pemantauan terhadap profil pegawai (*know your employee*), baik pegawai tetap maupun

pegawai tidak tetap, termasuk tenaga ahli, dari mulai level paling rendah sampai dengan Direksi dan Dewan Komisaris. Pengenalan dan pemantauan terhadap profil pegawai (*know your employee*) mencakup karakter, perilaku, dan gaya hidup pegawai.

b. Prosedur penyaringan dalam rangka penerimaan pegawai baru (*pre-employee screening*) dilakukan dalam bentuk:
   1) metode *screening* yang dimaksudkan untuk memastikan profil calon pegawai tidak memiliki catatan kejahatan, antara lain mengharuskan calon pegawai membuat surat pernyataan dan/atau menyerahkan surat keterangan catatan kepolisian;
   2) melakukan verifikasi identitas dan pendidikan yang telah diperoleh calon pegawai antara lain melalui proses wawancara (*interview*) secara tatap muka ataupun secara virtual yang dimaksudkan untuk lebih memastikan kebenaran dari informasi dan data dari calon pegawai;
   3) melakukan penelitian melalui media atau informasi lainnya terhadap latar belakang dari calon pegawai antara lain riwayat pekerjaan dan/atau pengalaman kerja dari calon pegawai;
   4) memastikan rekam jejak (*track record*) yang baik dari calon pegawai antara lain dengan meminta surat rekomendasi dari perusahaan sebelumnya dimana calon pegawai pernah bekerja; dan
   5) memastikan kualitas kredit calon pegawai tidak tergolong kredit macet.

c. pengenalan dan pemantauan terhadap profil pegawai, mencakup perilaku dan gaya hidup pegawai, antara lain:
   1) melakukan verifikasi terhadap pegawai yang mengalami perubahan gaya hidup yang cukup signifikan;
   2) memastikan bahwa pegawai telah memahami dan menaati kode etik pegawai (*code of conduct*);
   3) mengevaluasi pegawai yang bertanggung jawab pada aktivitas yang tergolong berisiko tinggi antara lain memiliki akses ke data Pedagang dan/atau berhadapan dengan calon Nasabah atau Nasabah.

d. Prosedur penyaringan (*pre-employee screening*), pengenalan dan pemantauan terhadap profil pegawai dituangkan dalam kebijakan *know your employee* yang berpedoman pada ketentuan yang mengatur mengenai penerapan strategi anti *fraud*.

2. Pelatihan
   a. Pedagang wajib memberikan pelatihan tentang APU, PPT, dan PPPSPM kepada pejabat dan/atau pegawai sesuai dengan kebutuhan, yang berkesinambungan dan berkala, paling sedikit sebanyak 1 (satu) kali dalam 1 (satu) tahun.
   b. Pelatihan yang berkesinambungan dan berkala terkait penerapan program APU, PPT, dan PPPSPM harus diberikan kepada pegawai, khususnya pegawai dari satuan kerja terkait (misalnya satuan kerja yang berhubungan baik secara langsung maupun tidak langsung dengan calon Nasabah, seperti petugas pelayanan Nasabah, petugas yang terkait pengelolaan dan pengembangan teknologi informasi, serta internal auditor) dan pegawai baru.

Dalam hal sesuai kebutuhan Pedagang berdasarkan penilaian risiko TPPU, TPPT, dan/atau PPSPM, kegiatan usaha, skala usaha, kompleksitas usaha, karakteristik usaha, dan/atau peristiwa atau perkembangan besar dalam manajemen dan operasional Pedagang, pelatihan dapat dilakukan lebih dari 1 (satu) kali dalam 1 (satu) tahun.

c. Dalam menyelenggarakan pelatihan berkesinambungan sebagaimana dimaksud dalam huruf a, Pedagang dapat:
   1) menyelenggarakan secara mandiri;
   2) bekerja sama dengan pihak lain seperti asosiasi Pedagang PPATK, dan/atau otoritas berwenang yang terkait; dan/atau
   3) mengikutsertakan pegawainya dalam pelatihan antara lain yang diselenggarakan oleh asosiasi Pedagang, PPATK, Otoritas Jasa Keuangan, dan/atau otoritas berwenang lainnya.

d. Dalam menentukan peserta pelatihan, Pedagang mengutamakan pegawai yang tugas sehari-harinya memenuhi kriteria sebagai berikut:
   1) melakukan pengawasan pelaksanaan penerapan program APU, PPT, dan PPPSPM; dan/atau
   2) terkait dengan penyusunan pelaporan kepada PPATK dan Otoritas Jasa Keuangan.

e. Pegawai lainnya selain pegawai sebagaimana dimaksud pada huruf d harus mendapatkan pelatihan paling sedikit 1 (satu) kali dalam masa kerjanya, dimana pelatihan tersebut harus sudah dilakukan paling lama 1 (satu) tahun sejak pegawai tersebut pertama kali bekerja sebagai pegawai Pedagang.

f. Metode pelatihan, dapat dilakukan dengan cara:
   1) Pelatihan dapat dilakukan secara virtual (daring) maupun melalui tatap muka.
   2) Pelatihan secara virtual (daring) sebagaimana dimaksud dalam angka 1), dapat menggunakan media *e-learning* baik yang disediakan oleh otoritas berwenang seperti PPATK atau yang disediakan secara mandiri oleh Pedagang.
   3) Pelatihan melalui tatap muka dilakukan dengan menggunakan pendekatan antara lain:
      a) tatap muka secara interaktif (misalnya *workshop*) dengan topik pelatihan disesuaikan dengan kebutuhan peserta. Pendekatan ini digunakan untuk pegawai yang mendapatkan prioritas dan dilakukan secara berkesinambungan, misalnya setiap tahun; dan/atau
      b) atap muka satu arah (misalnya seminar) dengan topik pelatihan adalah berupa gambaran umum dari penerapan program APU, PPT, dan PPPSPM. Pendekatan ini diberikan kepada pegawai yang tidak mendapatkan prioritas dan dilakukan apabila terdapat perubahan ketentuan yang signifikan.

g. Materi dan evaluasi pelatihan dilakukan dengan cara:
   1) Pedagang dapat mengembangkan materi pelatihan terkait penerapan program APU, PPT, dan PPPSPM sesuai dengan kebutuhan. Beberapa topik yang dapat menjadi materi dalam pelatihan antara lain:

a) penerapan peraturan perundang-undangan yang terkait dengan program APU, PPT, dan PPPSPM;
b) modus dan tipologi TPPU, TPPT, dan/atau PPSPM;
c) kebijakan dan prosedur penerapan program APU, PPT, dan PPPSPM serta peran dan tanggung jawab pegawai dalam mencegah dan memberantas TPPU, TPPT, dan/atau PPSPM;
d) penggunaan teknologi informasi dalam penerapan program APU, PPT, dan PPPSPM serta mitigasi risiko atas penggunaan teknologi informasi dimaksud;
e) penilaian risiko dan penerapan program APU, PPT, dan PPPSPM berbasis risiko (*risk based approach*); dan
f) peran dan tanggung jawab pegawai dalam mencegah dan memberantas TPPU, TPPT, dan/atau PPSPM.

2) Kedalaman materi pelatihan disesuaikan dengan kebutuhan pegawai dan kesesuaian dengan tugas dan tanggung jawab pegawai.
3) Untuk mengetahui tingkat pemahaman pegawai dan kesesuaian materi pelatihan, Pedagang harus melakukan evaluasi terhadap setiap pelatihan yang telah diselenggarakan.
4) Evaluasi dapat dilakukan secara langsung melalui wawancara atau secara tidak langsung melalui tes.
5) Pedagang harus melakukan upaya tindak lanjut dari hasil evaluasi pelatihan melalui penyempurnaan materi dan metode pelatihan.

VIII. PELAPORAN

1. Laporan kepada Otoritas Jasa Keuangan
   a. Pedagang harus menyampaikan laporan penerapan program APU PPT, dan PPPSPM kepada Otoritas Jasa Keuangan, paling sedikit berupa:
      1) *Individual Risk Assessment*/IRA; dan
      2) Laporan rencana pengkinian data dan laporan realisasi kegiatan pengkinian data.
   b. Individual *Risk Assessment*/IRA
      1) *Individual Risk Assessment*/IRA disusun dengan format sebagai berikut:
         a) Bagian I: pendahuluan, yang paling sedikit terdiri atas:
            (1) latar belakang; dan
            (2) tujuan;
         b) Bagian II: landasan teori, yang paling sedikit terdiri atas:
            (1) metodologi;
            (2) kerangka kerja; dan
            (3) pembatasan ruang lingkup;
         c) Bagian III: profil Pedagang, yang berisi uraian mengenai gambaran umum Pedagang, baik dari sisi kelembagaan maupun operasional;
         d) Bagian IV: hasil penilaian risiko, yang paling sedikit terdiri atas:
            (1) peta risiko/kriteria TPPU secara umum, yang dipetakan dari sisi tindak pidana asal, bidang usaha Nasabah Korporasi, area geografis (dapat

berupa negara serta provinsi dan/atau kota/kabupaten di Indonesia), produk/jasa/layanan, dan metode Transaksi/jaringan distribusi (*delivery channels*);

(2) peta risiko/kriteria risiko TPPT secara umum, yang dipetakan dari sisi bidang usaha Nasabah Korporasi, area geografis (dapat berupa negara serta provinsi dan/atau kota/kabupaten di Indonesia), produk/jasa/layanan, dan metode Transaksi/jaringan distribusi (*delivery channels*);

(3) peta risiko/kriteria risiko PPSPM secara umum, yang dipetakan dari sisi bidang usaha Nasabah Korporasi, area geografis (dapat berupa negara serta provinsi dan/atau kota/kabupaten di Indonesia), produk/jasa/layanan, dan metode transaksi/jaringan distribusi (*delivery channels*);

(4) peta risiko seluruh Nasabah, yaitu pemetaan Nasabah berdasarkan tingkat risikonya; dan

(5) risiko akhir Pedagang secara agregat;

e) Bagian V: mitigasi risiko, yang berisi paling sedikit mengenai hal-hal yang telah dilakukan Pedagang dalam memitigasi risiko TPPU, TPPT, dan/atau PPSPM; dan

f) Bagian VI: kesimpulan dan tindak lanjut, yang merupakan ringkasan dari hasil penilaian risiko serta mitigasi risiko yang akan dilakukan.

2) Dokumen IRA disampaikan untuk pertama kalinya paling lama pada 12 (dua belas) bulan setelah Surat Edaran Otoritas Jasa Keuangan ini diterbitkan.

3) Pengkinan atas dokumen IRA disampaikan setiap tahun paling lambat akhir bulan Juni.

4) Dalam hal tanggal pelaporan IRA jatuh pada hari libur, penyampaian laporan dilakukan pada hari kerja berikutnya.

5) Penyampaian dokumen IRA disampaikan secara daring melalui sistem elektronik yang diselenggarakan oleh Otoritas Jasa Keuangan. Dalam hal sistem elektronik tersebut belum tersedia atau mengalami gangguan, maka penyampaian dokumen IRA disampaikan secara fisik atau melalui surat elektronik ke Otoritas Jasa Keuangan yang ditujukan kepada kepala satuan kerja pengawasan.

c. Laporan Rencana Pengkinian Data dan Laporan Realisasi Kegiatan Pengkinian Data

1) Laporan Rencana Pengkinian Data Nasabah dan Perubahannya;

a) Laporan rencana pengkinian data Nasabah harus mendapat persetujuan oleh Direksi.

b) Laporan rencana pengkinian data Nasabah memuat data kuantitatif (statistik jumlah Nasabah) dan data kualitatif (antara lain kendala, upaya yang telah dilakukan oleh Pedagang, serta kemajuan (*progress*) dari upaya tersebut).

c) Laporan rencana pengkinian data mencakup jumlah Nasabah dan tingkat risiko TPPU, TPPT, dan/atau PPSPM 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 tercantum dalam Lampiran bagian C yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

d) Laporan rencana pengkinian data Nasabah harus disampaikan kepada Otoritas Jasa Keuangan setiap tahun paling lama akhir bulan Desember sebelum periode pengkinian data.

Sebagai contoh, untuk pengkinian data Nasabah kurun waktu Januari sampai dengan Desember 2026, Pedagang menyampaikan laporan rencana pengkinian data Nasabah paling lambat tanggal 31 Desember tahun 2025.

e) Penyampaian laporan rencana pengkinian data Nasabah disampaikan secara daring melalui sistem elektronik yang diselenggarakan oleh Otoritas Jasa Keuangan. Dalam hal sistem elektronik tersebut belum tersedia atau mengalami gangguan, maka penyampaian laporan rencana pengkinian data Nasabah disampaikan secara fisik atau melalui surat elektronik ke Otoritas Jasa Keuangan yang ditujukan kepada kepala satuan kerja pengawasan.

f) Dalam hal tanggal pelaporan rencana pengkinian data Nasabah jatuh pada hari libur, penyampaian laporan dilakukan pada hari kerja berikutnya.

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

2) Laporan Realisasi Pengkinian Data;

a) Laporan realisasi pengkinian data Nasabah harus mendapat persetujuan oleh Direksi.

b) Laporan realisasi 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 tercantum dalam Lampiran bagian D yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

c) Laporan realisasi pengkinian data harus disampaikan kepada Otoritas Jasa Keuangan setiap tahun paling lama akhir bulan Januari setelah periode pengkinian data berakhir.

Sebagai contoh, untuk pengkinian data Nasabah yang telah dilakukan pada kurun waktu Januari sampai dengan Desember 2026, Pedagang menyampaikan laporan realisasi pengkinian data Nasabah paling lambat tanggal 31 Januari 2027.

d) Penyampaian laporan realisasi pengkinian data disampaikan secara daring melalui sistem elektronik yang diselenggarakan oleh Otoritas Jasa Keuangan. Dalam hal sistem elektronik tersebut belum tersedia atau mengalami gangguan, maka penyampaian laporan realisasi pengkinian data Nasabah disampaikan secara fisik atau melalui surat elektronik ke Otoritas Jasa Keuangan yang ditujukan kepada kepala satuan kerja pengawasan.

Dalam hal tanggal pelaporan realisasi pengkinian data Nasabah jatuh pada hari libur, penyampaian laporan dilakukan pada hari kerja berikutnya.

2. Tata cara penyampaian laporan penerapan program APU, PPT, dan PPPSPM
   a. Penyampaian laporan penerapan program APU, PPT, dan PPPSPM dilakukan secara daring melalui sistem pelaporan yang ditentukan oleh Otoritas Jasa Keuangan.
   b. Dalam hal Sistem Pelaporan Otoritas Jasa Keuangan sebagaimana dimaksud pada huruf a belum tersedia atau mengalami gangguan teknis, Pedagang menyampaikan laporan dalam bentuk dokumen elektronik melalui surat elektronik melalui alamat:
      1) mailingroomsumitro@ojk.go.id, dalam hal Sistem Pelaporan Otoritas Jasa Keuangan belum tersedia;
      2) mailingroommrp@ojk.go.id, dalam hal Sistem Pelaporan Otoritas Jasa Keuangan mengalami gangguan teknis; atau
      3) alamat lain yang ditetapkan oleh Otoritas Jasa Keuangan.
   c. Penyampaian laporan dalam bentuk dokumen elektronik melalui surat elektronik sebagaimana dimaksud pada huruf b ditujukan kepada:
      1) Kepala Departemen Pengawasan Inovasi Teknologi Sektor Keuangan, Aset Keuangan Digital dan Aset Kripto, dalam hal Sistem Pelaporan Otoritas Jasa Keuangan belum tersedia; atau
      2) Kepala Departemen Internasional dan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme dengan tembusan Kepala Departemen Pengawasan Inovasi Teknologi Sektor Keuangan, Aset Keuangan Digital dan Aset Kripto, dalam hal Sistem Pelaporan Otoritas Jasa Keuangan mengalami gangguan teknis.
   d. Dalam hal surat elektronik Otoritas Jasa Keuangan sebagaimana dimaksud pada huruf b mengalami gangguan teknis, penyampaian pelaporan disampaikan kepada Otoritas Jasa Keuangan secara luring dengan cara:
      1) diserahkan langsung; atau
      2) dikirim melalui perusahaan jasa pengiriman.
   e. Penyampaian laporan secara fisik sebagaimana dimaksud pada huruf d ditujukan kepada:
      1) Kepala Departemen Pengawasan Inovasi Teknologi Sektor Keuangan, Aset Keuangan Digital dan Aset Kripto
         Gedung Soemitro Djojohadikusumo

Jalan Lapangan Banteng Timur 2-4
Jakarta 10710, Indonesia,
dalam hal Sistem Pelaporan Otoritas Jasa Keuangan belum tersedia; atau

2) Kepala Departemen Internasional dan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme
Gedung Soemitro Djojohadikusumo
Jalan Lapangan Banteng Timur 2-4
Jakarta 10710, Indonesia,dengan tembusan kepada:
Kepala Departemen Pengawasan Inovasi Teknologi Sektor Keuangan, Aset Keuangan Digital dan Aset Kripto
dalam hal Sistem Pelaporan Otoritas Jasa Keuangan mengalami gangguan teknis.

f. Pedagang dinyatakan telah menyampaikan laporan dengan ketentuan:
   1) penyampaian melalui sistem pelaporan Otoritas Jasa Keuangan dibuktikan dengan bukti penerimaan dari Sistem Pelaporan Otoritas Jasa Keuangan;
   2) penyampaian melalui surat elektronik dibuktikan dengan tanda terima dari surat elektronik Otoritas Jasa Keuangan; atau
   3) penyampaian secara luring dibuktikan dengan tanda terima dari Otoritas Jasa keuangan.

3. Tembusan Laporan Pemblokiran Secara Serta Merta terkait DTTOT dan/atau DPPSPM;
   a. Dalam hal terdapat kesesuaian identitas dan informasi lain terkait Nasabah atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT dan/atau DPPSPM, Pedagang harus menyampaikan laporan Pemblokiran secara serta merta tanpa penundaan dan tanpa pemberitahuan sebelumnya kepada Nasabah atau Pemilik Manfaat (*Beneficial Owner*), dan melaporkannya kepada Kepolisian Negara Republik Indonesia (untuk DTTOT) atau kepada PPATK (untuk DPPSPM) dengan tembusan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja sejak Pedagang menerima DTTOT dan/atau DPPSPM.
   b. Penyampaian tembusan laporan Pemblokiran secara serta merta terkait DTTOT dan/atau DPPSPM harus disertai dengan melampirkan berita acara Pemblokiran secara serta merta.
   c. Penyampaian tembusan laporan Pemblokiran secara serta merta terkait DTTOT dan/atau DPPSPM disampaikan secara daring melalui sistem elektronik yang diselenggarakan oleh Otoritas Jasa Keuangan, yaitu Sistem Informasi Program APU PPT (SIGAP).
   d. Dalam hal sistem elektronik sebagaimana dimaksud pada huruf c belum tersedia atau mengalami gangguan teknis, maka tembusan laporan Pemblokiran secara serta merta terkait DTTOT dan/atau DPPSPM dimaksud disampaikan dalam bentuk dokumen elektronik melalui surat elektronik melalui alamat sebagaimana dimaksud pada angka 2 huruf b, yang ditujukan kepada kepala satuan kerja pengawasan sebagaimana dimaksud pada angka 2 huruf c.
   e. Dalam hal surat elektronik Otoritas Jasa Keuangan sebagaimana dimaksud pada huruf d mengalami gangguan teknis, penyampaian pelaporan disampaikan kepada Otoritas

Jasa Keuangan secara fisik sebagaimana dimaksud pada angka 2 huruf e.

f. Pedagang harus memastikan bahwa telah terdaftar sebagai pengguna (*user*) SIGAP dengan mengakses https://sigap.ojk.go.id.

g. Bagi Pedagang yang belum pernah melakukan registrasi pada SIGAP, dapat memilih tombol Register untuk melakukan pendaftaran. Adapun pada proses registrasi, dibutuhkan informasi mengenai akun SIPO (Sistem Informasi Penerimaan OJK), agar dapat memastikan bahwa Pedagang yang masuk ke dalam sistem SIGAP hanya Pedagang yang telah berizin di bawah kewenangan Otoritas Jasa Keuangan.

h. Secara lebih rinci, tata cara registrasi SIGAP serta mekanisme penyampaian tembusan laporan Pemblokiran secara serta merta terkait DTTOT dan/atau DPPSPM melalui SIGAP, dapat mengacu pada Surat Edaran Otoritas Jasa Keuangan mengenai pedoman Pemblokiran secara serta merta atas dana Nasabah yang identitasnya tercantum dalam DTTOT atau DPPSPM.

4. Tembusan Laporan Nihil terkait DTTOT dan/atau DPPSPM;

a. Dalam hal tidak ditemukan kesesuaian identitas dan informasi lain terkait Nasabah atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT dan/atau DPPSPM, Pedagang harus menyampaikan laporan nihil kepada Kepolisian Negara Republik Indonesia (untuk DTTOT) atau kepada PPATK (untuk DPPSPM) dengan tembusan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja sejak Pedagang menerima DTTOT dan/atau DPPSPM.

b. Penyampaian tembusan laporan nihil terkait DTTOT dan/atau DPPSPM disampaikan secara daring melalui sistem elektronik yang diselenggarakan oleh Otoritas Jasa Keuangan, yaitu Sistem Informasi Program APU PPT (SIGAP).

c. Dalam hal sistem elektronik sebagaimana dimaksud pada huruf b belum tersedia atau mengalami gangguan teknis, maka tembusan laporan nihil terkait DTTOT dan/atau DPPSPM dimaksud disampaikan dalam bentuk dokumen elektronik melalui surat elektronik melalui alamat sebagaimana dimaksud pada angka 2 huruf b, yang ditujukan kepada kepala satuan kerja pengawasan sebagaimana dimaksud pada angka 2 huruf c.

d. Dalam hal surat elektronik Otoritas Jasa Keuangan sebagaimana dimaksud pada huruf c mengalami gangguan teknis, penyampaian laporan nihil terkait DTTOT dan/atau DPPSPM disampaikan kepada Otoritas Jasa Keuangan secara fisik sebagaimana dimaksud pada angka 2 huruf e.

e. Pedagang harus memastikan bahwa telah terdaftar sebagai pengguna (*user*) SIGAP dengan mengakses https://sigap.ojk.go.id.

f. Bagi Pedagang yang belum pernah melakukan registrasi pada SIGAP, dapat memilih tombol Register untuk dapat melakukan pendaftaran. Adapun pada proses registrasi, dibutuhkan informasi mengenai akun SIPO (Sistem Informasi Penerimaan Otoritas Jasa Keuangan), agar dapat memastikan bahwa Pedagang yang masuk ke dalam sistem SIGAP hanya Pedagang

yang telah berizin di bawah kewenangan Otoritas Jasa Keuangan.

g. Secara lebih rinci, tata cara registrasi SIGAP serta mekanisme penyampaian tembusan laporan nihil terkait DTTOT dan/atau DPPSPM melalui SIGAP, dapat mengacu pada Surat Edaran Otoritas Jasa Keuangan mengenai pedoman Pemblokiran secara serta merta atas dana Nasabah yang identitasnya tercantum dalam DTTOT atau DPPSPM.

5. Laporan kepada PPATK.

Pedagang harus menyampaikan pelaporan kepada PPATK sesuai dengan ketentuan yang dimaksud dalam peraturan perundang-undangan mengenai pencegahan dan pemberantasan TPPU, TPPT, dan/atau PPSPM, termasuk peraturan pelaksanaannya, antara lain Peraturan Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan.

Beberapa laporan yang harus disampaikan kepada PPATK sesuai dengan model bisnis dan karakteristik usaha Pedagang, antara lain:

a. Laporan Transaksi Keuangan Mencurigakan;
   1) Pedagang harus menyampaikan laporan Transaksi Keuangan Mencurigakan, meliputi Transaksi dan/atau percobaan transaksi yang diduga terkait dengan tindak pidana asal, TPPU, TPPT, dan/atau PPSPM, termasuk dalam hal terdapat kesesuaian identitas dan informasi lain terkait calon Nasabah, Nasabah, dan/atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT dan/atau DPPSPM.
   2) Laporan Transaksi Keuangan Mencurigakan terkait dengan penyampaian laporan koreksi atas laporan Transaksi Keuangan Mencurigakan yang sebelumnya telah disampaikan.

      Contoh kriteria Transaksi Keuangan Mencurigakan tercantum dalam Lampiran bagian E yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

b. Laporan Pemblokiran Secara Serta Merta terkait DPPSPM;
   1) Dalam hal terdapat kesesuaian identitas dan informasi lain terkait Nasabah atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DPPSPM, Pedagang harus menyampaikan laporan Pemblokiran secara serta merta tanpa penundaan dan tanpa pemberitahuan sebelumnya kepada Nasabah atau Pemilik Manfaat (*Beneficial Owner* kepada PPATK paling lama 3 (tiga) hari kerja sejak Pedagang menerima DPPSPM.
   2) Penyampaian laporan Pemblokiran secara serta merta terkait DPPSPM harus disertai dengan melampirkan berita acara Pemblokiran secara serta merta.
   3) Penyampaian laporan Pemblokiran secara serta merta terkait DPPSPM disampaikan secara fisik kepada Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan u.p. Direktur Strategi dan Kerja Sama Dalam Negeri dengan alamat Jalan Ir. H. Juanda Nomor 35 Jakarta Pusat 10120 atau melalui surat elektronik pemblokiran.wmd@ppatk.go.id, atau melalui mekanisme lain yang diatur oleh Pusat Pelaporan dan Analisis Transaksi Keuangan.

c. Laporan Nihil DPPSPM;
   1) Dalam hal tidak ditemukan kesesuaian identitas dan informasi lain terkait Nasabah atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT dan/atau DPPSPM, Pedagang harus menyampaikan laporan nihil kepada PPATK paling lama 3 (tiga) hari kerja sejak Pedagang menerima DPPSPM.
   2) Penyampaian laporan Pemblokiran secara serta merta terkait DPPSPM disampaikan secara fisik kepada Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan u.p. Direktur Strategi dan Kerja Sama Dalam Negeri dengan alamat Jalan Ir. H. Juanda Nomor 35 Jakarta Pusat 10120 atau melalui surat elektronik pemblokiran.wmd@ppatk.go.id, atau melalui mekanisme lain yang diatur oleh Pusat Pelaporan dan Analisis Transaksi Keuangan.

6. Laporan kepada Kepolisian Negara Republik Indonesia.
   a. Laporan Pemblokiran Secara Serta Merta terkait DTTOT;
      1) Dalam hal terdapat kesesuaian identitas dan informasi lain terkait Nasabah atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT, Pedagang harus menyampaikan laporan Pemblokiran secara serta merta tanpa penundaan dan tanpa pemberitahuan sebelumnya kepada Nasabah atau Pemilik Manfaat (*Beneficial Owner* kepada Kepolisian Negara Republik Indonesia paling lama 3 (tiga) hari kerja sejak Pedagang menerima DTTOT.
      2) Penyampaian laporan Pemblokiran secara serta merta terkait DTTOT harus disertai dengan melampirkan berita acara Pemblokiran secara serta merta.
      3) Penyampaian laporan Pemblokiran secara serta merta terkait DTTOT disampaikan secara fisik kepada Kepolisian Republik Indonesia dengan alamat Jl. Trunojoyo No.3, RT.2/RW.1, Selong, Kec. Kby. Baru, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12110 atau melalui surat elektronik dttot.report@gmail.com/ dttot.report.2@gmail.com atau melalui mekanisme lain yang diatur oleh Kepolisian Negara Republik Indonesia.
   b. Laporan Nihil DTTOT;
      1) Dalam hal tidak ditemukan kesesuaian identitas dan informasi lain terkait Nasabah atau Pemilik Manfaat (*Beneficial Owner*) dengan identitas dan informasi lain yang tercantum dalam DTTOT, Pedagang harus menyampaikan laporan nihil kepada Kepolisian Negara Republik Indonesia paling lama 3 (tiga) hari kerja sejak Pedagang menerima DTTOT.
      2) Penyampaian laporan Pemblokiran secara serta merta terkait DTTOT disampaikan secara fisik kepada Kepolisian Republik Indonesia dengan alamat Jl. Trunojoyo No.3, RT.2/RW.1, Selong, Kecamatan Kebayoran Baru, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12110 atau melalui surat elektronik dttot.report@gmail.com dan dttot.report.2@gmail.com atau melalui mekanisme lain yang diatur oleh Kepolisian Negara Republik Indonesia.

IX. Rencana Tindak serta Kebijakan dan Prosedur

Penyampaian rencana tindak serta kebijakan dan prosedur Penerapan Program APU, PPT, dan PPPSPM serta Perubahannya

1. Rencana tindak serta kebijakan dan prosedur penerapan program APU, PPT, dan PPPSPM diusulkan oleh Direksi dan disetujui oleh Dewan Komisaris.

   Contoh format rencana tindak serta kebijakan dan prosedur tercantum dalam Lampiran bagian F yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
2. Pedagang harus menyampaikan rencana tindak serta kebijakan dan prosedur paling lama 9 Juli 2025.
3. Rencana tindak serta kebijakan dan prosedur disampaikan melalui sistem elektronik yang diselenggarakan oleh Otoritas Jasa Keuangan.
4. Dalam hal sistem elektronik sebagaimana dimaksud pada angka 3 belum tersedia atau mengalami gangguan teknis, maka rencana tindak serta kebijakan dan prosedur dimaksud disampaikan dalam bentuk dokumen elektronik melalui surat elektronik melalui alamat sebagaimana dimaksud pada romawi VIII angka 2 huruf b, yang ditujukan kepada kepala satuan kerja pengawasan sebagaimana dimaksud pada romawi VIII angka 2 huruf c.
5. Dalam hal surat elektronik Otoritas Jasa Keuangan sebagaimana dimaksud pada angka 4 mengalami gangguan teknis, penyampaian rencana tindak serta kebijakan dan prosedur disampaikan kepada Otoritas Jasa Keuangan secara fisik sebagaimana dimaksud pada romawi VIII angka 2 huruf e.
6. Dalam hal tanggal penyampaian rencana tindak serta kebijakan dan prosedur jatuh pada hari libur, penyampaian rencana tindak serta kebijakan dan prosedur dilakukan pada hari kerja berikutnya.
7. Dalam hal terdapat perubahan atas kebijakan dan prosedur yang telah disampaikan kepada Otoritas Jasa Keuangan, Pedagang harus menyampaikan perubahan tersebut paling lambat 7 (tujuh) hari kerja sejak perubahan dilakukan.

X. KETENTUAN LAIN-LAIN

1. Pedagang yang menggunakan jasa profesi penunjang yang menjadi pihak pelapor dalam rezim APU, PPT, dan PPPSPM di Indonesia, wajib memastikan profesi penunjang tersebut menerapkan program APU, PPT, dan PPPSPM serta telah terdaftar dalam sistem informasi pelaporan APU, PPT, dan PPPSPM yang dikelola oleh PPATK, yang dibuktikan dengan menunjukkan:
   a. surat elektronik konfirmasi dari PPATK yang disampaikan kepada profesi penunjang mengenai permohonan pendaftaran telah diterima; dan/atau
   b. bentuk lainnya sebagaimana dimaksud dalam peraturan perundang-undangan mengenai sistem informasi pelaporan APU, PPT, dan PPPSPM kepada PPATK.
2. Pedagang harus bekerja sama dengan aparat penegak hukum dan otoritas yang berwenang dalam pencegahan dan pemberantasan TPPU, TPPT, dan/atau PPSPM.

XI. PENUTUP

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

Ditetapkan di Jakarta
pada tanggal 3 Juli 2025

KEPALA EKSEKUTIF PENGAWAS INOVASI TEKNOLOGI SEKTOR KEUANGAN, ASET KEUANGAN DIGITAL DAN ASET KRIPTO
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

HASAN FAWZI

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd

Aat Windradi

LAMPIRAN
SURAT EDARAN OTORITAS JASA KEUANGAN
NOMOR 16/SEOJK.07/2025
TENTANG
PENERAPAN PROGRAM ANTI PENCUCIAN UANG, PENCEGAHAN PENDANAAN TERORISME, DAN PENCEGAHAN PENDANAAN PROLIFERASI SENJATA PEMUSNAH MASSAL BAGI PEDAGANG ASET KEUANGAN DIGITAL

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

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

      Kemungkinan *(likelihood)* mengacu pada potensi risiko pencucian uang dan pendanaan terorisme yang terjadi untuk setiap risiko tertentu yang dinilai.

      Dalam hal ini Pedagang dapat menggunakan skala risiko yang umum digunakan yaitu:

Peringkat	Kemungkinan (*Likelihood)* risiko TPPU, TPPT, dan PPPSPM
Tinggi	Kemungkinan risiko TPPU, TPPT, dan PPPSPM terjadi
Medium	Kemungkinan terjadinya risiko dapat diterima
Rendah	Tidak terdapat kemungkinan terjadinya risiko

   2. Dampak (*Impact*)

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

      Timbulnya dampak (*impact*) bergantung pada kondisi internal Pedagang. Dampak (*impact*) atas terjadinya risiko TPPU, TPPT, daqn PPPSPM dapat dilihat dari berbagai sudut pandang, antara lain:

      a. risiko reputasi dan dampaknya terhadap kegiatan usaha Pedagang;
      b. dampak regulasi;
      c. kerugian finansial bagi Pedagang; dan/atau
      d. risiko hukum.

      Dampak (*impact*) atas terjadinya risiko TPPU, TPPT, dan PPPSPM akan sangat spesifik untuk setiap Pedagang sehingga terdapat kesulitan dalam menghitung dampak (*impact*). Oleh karena itu, hanya Pedagang yang dapat menentukan dampak (*impact*) atas risiko yang terjadi.

      Skala yang digunakan untuk menghitung dampak (*impact*) tidak jauh berbeda dengan skala dalam menghitung kemungkinan (*likelihood*).

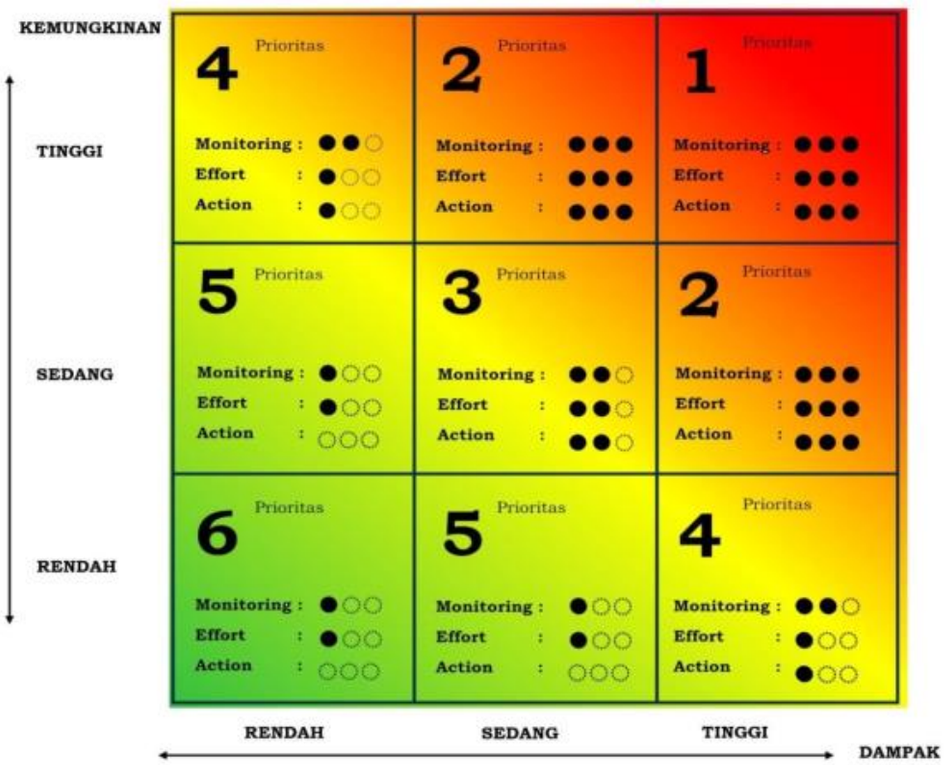
Peringkat	Konsekuensi atas risiko TPPU, TPPT, PPSPM
Tinggi	Risiko memiliki konsekuensi yang berat
Medium	Risiko memiliki konsekuensi yang moderat
Rendah	Risiko memiliki konsekuensi yang kecil atau tidak signifikan.

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

Matriks Kemungkinan dan Dampak

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

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



3. Cara membaca matriks prioritas
   1. Kotak 6
      Kondisi pada kotak 6 menunjukkan kemungkinan dan dampak terjadinya risiko TPPU, TPPT, dan PPSPM rendah sehingga Pedagang tidak perlu mengambil tindakan, upaya, atau pemantauan khusus.
   2. Kotak 5
      Kondisi pada kotak 5 menunjukkan kemungkinan dan dampak terjadinya risiko TPPU, TPPT, dan PPSPM tergolong rendah namun berpotensi meningkat dan menjadi skala menengah. Untuk kondisi pada kotak 5 diperlukan upaya dan monitoring untuk mencegah peningkatan risiko (tidak berubah menjadi kotak 4 atau kotak 3).
   3. Kotak 4
      Kondisi pada kotak 4 menunjukkan kemungkinan dan dampak terjadinya risiko TPPU, TPPT, dan PPSPM yang tergolong medium.

Pada kondisi ini, Pedagang perlu mengambil tindakan, upaya atau pemantauan. Tindakan, upaya, atau pemantauan yang memadai akan menurunkan kemungkinan dan dampak terjadinya risiko TPPU, TPPT, dan PPSPM, sebaliknya apabila tindakan, upaya, atau pemantauan tidak memadai maka akan meningkatkan risiko menjadi risiko tinggi.

4. Kotak 3
   Kondisi pada kotak 3 menunjukkan bahwa Pedagang perlu mengalokasikan sumber daya untuk melakukan tindakan, upaya, dan pemantauan. Terdapat kemungkinan terjadinya risiko TPPU, TPPT, dan PPSPM dengan dampak yang dapat
   dikategorikan moderat. Untuk itu, Pedagang perlu memperhatikan seluruh kegiatan usaha dan hubungan usaha yang ada, sehingga tidak menimbulkan peningkatan risiko (tidak berubah menjadi kotak 2 atau kotak 1).
5. Kotak 2
   Kondisi pada kotak 2 menunjukkan bahwa kemungkinan terjadinya risiko TPPU, TPPT, dan PPSPM tergolong tinggi. Pada kondisi ini, Pedagang perlu memperhatikan seluruh kegiatan usaha dan hubungan usaha dan mengerahkan sumber daya untuk menekan kemungkinan dan dampak risiko. Pedagang perlu menerapkan langkah mitigasi yang lebih ketat untuk mencegah peningkatan risiko menjadi sangat tinggi, atau menjadi kondisi pada kotak 1.
6. Kotak 1
   Kondisi pada kotak 1 menunjukkan bahwa kemungkinan terjadinya risiko TPPU, TPPT, dan PPSPM sangat tinggi termasuk besarnya dampak atas risiko tersebut. Pada kondisi tersebut dibutuhkan sumber daya yang lebih banyak, tindakan khusus, upaya khusus serta pemantauan berkala untuk meminimalisasi risiko tersebut.

B. CONTOH TINGKAT RISIKO YANG TERKAIT DENGAN KEGIATAN USAHA PEDAGANG

a. Sebagai contoh, tabel berikut menyajikan beberapa contoh faktor risiko yang mungkin dihadapi oleh Pedagang sebagai bagian dari penilaian risiko yang berhubungan dengan kegiatan usaha Pedagang. Tabel tersebut juga memaparkan alasan rasional yang dapat membantu Pedagang untuk membedakan setiap tingkat risiko.

b. Pedagang dapat memutuskan skala risiko yang digunakan oleh Pedagang. Pedoman ini tidak mewajibkan Pedagang untuk menentukan skala risiko tinggi, medium dan rendah. Pedagang dapat menggunakan skala tinggi dan rendah saja sesuai dengan kegiatan usaha, kebutuhan, dan kompleksitas Pedagang.

CONTOH TABEL TINGKAT RISIKO

FAKTOR	TINGKAT RISIKO		
	RENDAH	MEDIUM	TINGGI
Profil Nasabah Aset Keuangan Digital	Profil Nasabah teridentifikasi dan terverifikasi memiliki potensi rendah melakukan TPPU/TPPT/PPSPM	Nasabah memerlukan verifikasi lanjutan untuk memastikan Nasabah tidak terlibat TPPU/TPPT/PPSPM	Nasabah memenuhi kriteria terafiliasi melakukan TPPU/TPPT/PPSPM
Jaringan distribusi Aset Keuangan Digital	Jaringan distribusi Aset Keuangan Digital dilakukan dengan medium elektronik paling sedikit memenuhi: *cybersecurity maturity test* menunjukkan level 5, transparan, dapat dilacak, keamanan siber sesuai dengan *best practice*,	Jaringan distribusi Aset Keuangan Digital dilakukan dengan medium elektronik yang masih transparan dan dapat dilacak, namun *cybersecurity maturity test* menunjukkan level 4 ke bawah	Jaringan distribusi Aset Keuangan Digital memungkinkan peningkatan anonimitas dan mengaburkan keterlacakan, sehingga mempersulit identifikasi TPPU/TPPT/PPSPM

	enkripsi data, pelindungan data pribadi, pelindungan konsumen, dan berizin sesuai ketentuan peraturan perundangan.		
Produk atau Jasa Aset Keuangan Digital	Produk atau Jasa Aset Keuangan Digital telah sesuai dengan daftar aset kripto, memiliki izin produk/aktivitas/ layanan.	Produk atau Jasa Aset Keuangan Digital memiliki karakteristik yang berpotensi dimanfaatkan pelaku TPPU/TPPT/PPSPM.	Produk atau Jasa Aset Keuangan Digital memungkinkan meningkatkan anonimitas, berkurangnya transparansi, dan mengaburkan arus keuangan
Geografi negara berisiko tinggi	Pedagang tidak memiliki hubungan usaha dengan Nasabah Pedagang negara berisiko tinggi.	Nasabah atau mitra Pedagang berada di area geografi/perbatasan geografi yang berpotensi melakukan TPPU/TPPT/PPSPM.	Pedagang memiliki hubungan usaha yang frekuensi tinggi dan nilai transaksi yang signifikan dengan negara-negara berisiko tinggi.

C. CONTOH FORMAT LAPORAN RENCANA PENGKINIAN DATA NASABAH

LAPORAN RENCANA PENGKINIAN DATA NASABAH
(NAMA PEDAGANG)
TAHUN .....

No.	**Jenis Nasabah dan Tingkat risiko**	**Jumlah *single customer identification file***		**Informasi yang akan dikinikan**	**Metode atau strategi**	**Presentase target pemenuhan *Single User Identification* yang akan dikinikan pada priode tertentu**
		***Single customer identification file* yang akan dikinikan**	**% terhadap seluruh jumlah *single customer identification file***			
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1.	Nasabah orang perseorangan					
	a. Risiko tinggi					
	b. Risiko menengah					
	c. Risiko rendah					
2.	Nasabah Korporasi					
	a. Risiko tinggi					
	b. Risiko menengah					

	c. 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					
	3) Risiko rendah					
4.	Lembaga Negara, Instansi Pemerintah, Lembaga internasional, dan perwakilan negara asing					
	a. Risiko tinggi					
	b. Risiko menengah					
	c. Risiko rendah					

3. 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 customer identification file* dalam persen pada periode tertentu. Periode ditentukan dengan menyesuaikan kemampuan dan kondisi masing-masing Pedagang, misalnya secara triwulanan. Contoh: Triwulan I = 30%, Triwulan II=60%, Triwulan III=90%, Triwulan IV=100%.

4. Jumlah tingkat risiko dapat disesuaikan dengan kebijakan yang telah ditetapkan oleh Pedagang.

D. CONTOH FORMAT LAPORAN REALISASI PENGKINIAN DATA NASABAH

LAPORAN REALISASI PENGKINIAN DATA NASABAH
(NAMA PEDAGANG)
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. Risiko tinggi					
	b. Risiko menengah					
	c. 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					
	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 customer identification file* yang dikinikan.
   (d) Diisi dengan realisasi jumlah *single customer identification file* yang dikinikan.
   (e) Diisi dengan persentase selisih antara taget *single customer identification file* yang akan dikinikan (c) dengan (d) realisasi *single customer identification file* yang dikinikan.

(f) Kendala dapat diisi lebih dari satu.

(g) Diisi dengan upaya untuk mengatasi kendala dan dapat lebih dari satu.

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

E. CONTOH KRITERIA TRANSAKSI KEUANGAN MENCURIGAKAN

A. UMUM

1. Transaksi Keuangan yang menyimpang dari profil, karakteristik, atau kebiasaan pola Transaksi dari Nasabah yang bersangkutan;
2. Transaksi Keuangan oleh Nasabah yang patut diduga dilakukan dengan tujuan untuk menghindari pelaporan Transaksi yang bersangkutan yang wajib dilakukan oleh Pedagang sesuai dengan ketentuan peraturan perundang-undangan mengenai pencegahan dan pemberantasan TPPU, TPPT, dan/atau PPSPM;
3. Transaksi Keuangan yang dilakukan atau batal dilakukan dengan menggunakan harta kekayaan yang diduga berasal dari hasil tindak pidana; atau
4. Transaksi Keuangan yang diminta oleh PPATK untuk dilaporkan oleh Pihak Pelapor karena melibatkan Harta Kekayaan yang diduga berasal dari hasil tindak pidana.

B. KRITERIA TRANSAKSI KEUANGAN MENCURIGAKAN ASET KEUANGAN DIGITAL

1. Ukuran dan Frekuensi Transaksi menunjukkan indikasi transaksi keungan mencurigakan misalnya, transaksi, pertukaran atau transfer dalam jumlah kecil, atau dalam jumlah di bawah ambang batas *Travel Rule*. Transaksi dilakukan beberapa kali bernilai tinggi: dalam waktu singkat (misalnya, 24 jam), dalam pola bertahap dan teratur diikuti periode tidak ada transaksi, atau ke akun yang baru dibuat/tidak aktif.
2. Mentransfer Aset Keuangan Digital segera ke beberapa Pedagang, terutama yang terdaftar/beroperasi di yurisdiksi lain yang tidak relevan dengan profil Nasabah atau ke Pedagang di yurisdiksi dengan regulasi program APU PPT PPPSPM yang lemah.
3. Menyetor Aset Keuangan Digital di Pedagang dan kemudian segera menariknya tanpa aktivitas pertukaran tambahan, atau mengonversi Aset Keuangan Digital ke beberapa jenis Aset Keuangan Digital lain tanpa penjelasan bisnis yang logis.
4. Menerima dana yang dicurigai sebagai hasil curian atau penipuan dari alamat *wallet* yang teridentifikasi menyimpan dana curian.
5. Nasabah baru melakukan deposit awal yang besar untuk membuka akun baru dengan Pedagang, sementara jumlah dana tidak konsisten dengan profil Nasabah.
6. Menyetor seluruh deposit pada hari pertama akun dibuka dan segera memperdagangkan/menarik seluruhnya.
7. Nasabah baru mencoba memperdagangkan atau menarik seluruh saldo Aset Keuangan Digital keluar dari platform Pedagang.
8. Melakukan transfer sering dalam periode waktu tertentu ke akun Nasabah yang sama oleh lebih dari satu orang, dari alamat IP yang sama, atau melibatkan jumlah besar.

9. Transaksi masuk dari banyak *wallet* yang tidak terkait dalam jumlah relatif kecil (akumulasi dana) dengan transfer berikutnya ke *wallet* lain atau penukaran penuh ke mata uang fiat.
10. Melakukan pertukaran Aset Keuangan Digital dan fiat pada potensi kerugian (misalnya, terlepas dari biaya komisi yang sangat tinggi) tanpa penjelasan bisnis yang logis.
11. Mengonversi sejumlah besar mata uang fiat menjadi Aset Keuangan Digital, atau sejumlah besar satu jenis Aset Keuangan Digital ke jenis Aset Keuangan Digital lainnya, tanpa penjelasan bisnis yang logis.
12. Transaksi melibatkan lebih dari satu jenis Aset Keuangan Digital, meskipun ada biaya tambahan, terutama Aset Keuangan Digital yang memberikan anonimitas lebih tinggi seperti *anonymity-enhanced cryptocurrency* (AEC) atau *privacy coins*.
13. Memindahkan Aset Keuangan Digital yang beroperasi di blockchain publik, transparan (seperti Bitcoin) ke Pedagang terpusat dan kemudian segera memperdagangkannya untuk *anonymity-enhanced cryptocurrency* (AEC) atau *privacy coins*.
14. Aktivitas transaksi abnormal (tingkat dan volume) Aset Keuangan Digital yang dicairkan di Pedagang dari *wallet* terkait platform Pedagang tanpa penjelasan bisnis yang logis.
15. Aset Keuangan Digital ditransfer ke atau dari *wallet* yang menunjukkan pola aktivitas sebelumnya terkait dengan penggunaan Pedagang yang mengoperasikan layanan *mixing* atau *tumbling* atau platform P2P.
16. Transaksi yang menggunakan layanan pencampuran dan pengacakan (*mixing and tumbling services*), menunjukkan niat untuk mengaburkan aliran dana terlarang antara alamat *wallet* yang diketahui dan pasar gelap (*darknet marketplaces*).
17. Dana disetor atau ditarik dari alamat Aset Keuangan Digital atau *wallet* dengan tautan paparan langsung dan tidak langsung ke sumber mencurigakan yang diketahui (pasar gelap, layanan *mixing/tumbling*, situs perjudian yang dipertanyakan, aktivitas ilegal seperti ransomware, dan laporan pencurian).
18. Penggunaan *wallet* terdesentralisasi/tidak di-*hosting*, perangkat keras atau *wallet* kertas untuk mengangkut Aset Keuangan Digital melintasi batas negara dari negara berisiko tinggi.
19. Nasabah yang mendaftar nama domain Internet melalui *proxy* atau menggunakan DNS yang menekan/merahasiakan pemilik nama domain.
20. Nasabah memasuki platform Pedagang menggunakan alamat IP yang terkait dengan darknet atau perangkat lunak serupa yang memungkinkan komunikasi anonim (email terenkripsi, VPN).
21. Sejumlah besar *wallet* Aset Keuangan Digital yang tampaknya tidak terkait dikendalikan dari alamat IP yang sama, yang dapat melibatkan penggunaan *wallet* cangkang (*shell wallets*).
22. Penggunaan Aset Keuangan Digital yang desainnya tidak didokumentasikan secara memadai, atau terkait dengan

kemungkinan penipuan atau skema penipuan (misalnya, skema Ponzi).

23. Menerima atau mengirim dana ke Pedagang yang proses CDD/KYC-nya terbukti lemah atau tidak ada.
24. Nasabah telah memberikan dokumen palsu atau telah mengedit foto dan/atau dokumen identifikasi sebagai bagian dari proses *on-boarding*.
25. Nasabah memberikan identifikasi atau kredensial akun yang dibagikan oleh akun lain.
26. Timbul perbedaan antara alamat IP yang terkait dengan profil Nasabah dan alamat IP dari mana transaksi dimulai.
27. Nasabah membeli Aset Keuangan Digital dalam jumlah besar yang tidak didukung oleh kekayaan yang tersedia atau tidak konsisten dengan profil keuangan historisnya, yang dapat menunjukkan pencucian uang, *money mule*, atau korban scam.
28. Nasabah berulang kali melakukan transaksi dengan kumpulan individu yang terorganisir atau terafiliasi dengan keuntungan atau kerugian signifikan, yang dapat menunjukkan pengambilalihan akun atau skema TPPU.
29. Bertransaksi dengan alamat *wallet* atau kartu bank yang terhubung dengan penipuan yang diketahui, pemerasan, atau skema *ransomware*, alamat yang disanksi, pasar gelap, atau situs web terlarang lainnya.
30. Transaksi Aset Keuangan Digital yang berasal dari atau ditujukan ke layanan perjudian daring.
31. Deposit ke akun atau alamat Aset Keuangan Digital secara signifikan lebih tinggi dari biasanya dengan sumber dana yang tidak diketahui, diikuti oleh konversi ke mata uang fiat, yang dapat mengindikasikan pencurian dana.
32. Kurangnya transparansi atau informasi yang tidak memadai tentang asal dan pemilik dana (misalnya, penggunaan perusahaan cangkang, dana yang ditempatkan dalam penerbitan Aset Keuangan Digital di mana data pribadi investor mungkin tidak tersedia, atau transaksi masuk dari sistem pembayaran daring melalui kartu kredit/prabayar diikuti penarikan instan).
33. Sebagian besar sumber kekayaan Nasabah berasal langsung dari layanan *mixing* pihak ketiga atau *wallet tumblers*.
34. Sumber kekayaan Nasabah secara tidak proporsional berasal dari Aset Keuangan Digital yang berasal dari Pedagang lain yang tidak memiliki kontrol APU PPT PPPSPM.
35. Nasabah memanfaatkan Pedagang yang berlokasi di luar negeri di yurisdiksi berisiko tinggi yang tidak memiliki, atau diketahui tidak memadai, regulasi program APU PPT PPPSPM termasuk langkah-langkah CDD atau KYC yang tidak memadai.
36. Nasabah mengirim dana ke Pedagang yang beroperasi di yurisdiksi yang tidak memiliki regulasi Aset Keuangan Digital, atau belum menerapkan kontrol program APU PPT PPPSPM.

F. CONTOH FORMAT RENCANA TINDAK SERTA KEBIJAKAN DAN PROSEDUR

RENCANA TINDAK SERTA KEBIJAKAN DAN PROSEDUR
(NAMA PEDAGANG)
TANGGAL : .....

RENCANA TINDAK PROGRAM APU PPT PPPSPM PEDAGANG							
Item Tindakan	**Hal yang perlu dilakukan**	**Sumberdaya yang diperlukan**	**Penanggung jawab**	**Tanggal Mulai**	***Deadline***	**Hasil Kinerja yang diharapkan**	**Permasalahan yang dihadapi**
pengawasan aktif Direksi dan Dewan Komisaris							
pengendalian intern							
sistem informasi manajemen							
sumber daya manusia dan pelatihan							
KEBIJAKAN DAN PROSEDUR							
Kebijakan dan Prosedur	**Hal yang perlu dilakukan**	**Sumberdaya yang diperlukan**	**Penanggung jawab**	**Tanggal Mulai**	***Deadline***	**Hasil Kinerja yang diharapkan**	**Permasalahan yang dihadapi**
identifikasi dan verifikasi calon Nasabah atau Nasabah							
identifikasi dan verifikasi Pemilik							

Manfaat (*Beneficial Owner*)							
penutupan hubungan usaha atau penolakan transaksi							
travel rule							
pengelolaan risiko TPPU, TPPT dan PPSPM yang berkelanjutan terkait dengan Nasabah, negara/area geografis/yurisdiksi, produk/jasa/transaksi, atau jaringan distribusi (*delivery channels*);							
pemeliharaan data yang akurat terkait dengan transaksi, penatausahaan proses CDD, serta penatausahaan kebijakan dan prosedur							
pengkinian dan pemantauan							
pelaporan kepada pejabat senior, Direksi, dan Dewan Komisaris terhadap pelaksanaan kebijakan dan							

prosedur penerapan program APU, PPT, dan PPPSPM							
Pelaporan							

Ditetapkan di Jakarta
pada tanggal 3 Juli 2025

KEPALA EKSEKUTIF PENGAWAS INOVASI TEKNOLOGI SEKTOR KEUANGAN, ASET KEUANGAN DIGITAL DAN ASET KRIPTO
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

HASAN FAWZI

Salinan ini sesuai dengan aslinya
Kepala Direktorat Pengembangan Hukum
Departemen Hukum

ttd

Aat Windradi