EVALUASI PEMANFAATAN *REGULATORY TECHNOLOGY* DALAM SISTEM ANTI-PENCUCIAN UANG UNTUK ASET VIRTUAL DI INDONESIA

TESIS

Magister Akuntansi

Disusun Oleh:

Nama: Kharisma Fatmalina Fajri

No. Mahasiswa: 20919050

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2024

EVALUASI PEMANFAATAN *REGULATORY TECHNOLOGY* DALAM SISTEM ANTI-PENCUCIAN UANG UNTUK ASET VIRTUAL DI INDONESIA

TESIS

Disusun dan diajukan untuk memenuhi sebagai salah satu syarat untuk mencapai derajat Magister (Strata-2) Program Studi Akuntansi pada Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia

Oleh:

Nama: Kharisma Fatmalina Fajri

No. Mahasiswa: 20919050

MAGISTER AKUNTANSI

FAKULTAS BISNIS DAN EKONOMIKA

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

PERNYATAAN BEBAS PLAGIARISME

"Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya yang pernah diajukan untuk gelar kemagisteran di suatu perguruan tinggi dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam referensi ini. Apabila di kemudian hari terbukti bahwa pernyataan ini tidak benar maka saya sanggup menerima hukuman/sanksi apapun sesuai peraturan yang berlaku."

Yogyakarta, 29 Desember 2023

Peneliti,

(Kharisma Fatmalina Fajri)

HALAMAN PENGESAHAN

"Evaluasi Pemanfaatan *Regulatory Technology* dalam Sistem Anti-Pencucian Uang untuk Aset Virtual di Indonesia"

Yogyakarta, 12 Januari 2024

Telah Diterima dan Disetujui dengan Baik Oleh:

Dosen Pembimbing

Dekar Urumsah, S.E., S.Si., M.Com(IS), Ph.D., CFrA.

BERITA ACARA UJIAN TESIS

Pada hari Jumat tanggal 5 Januari 2024 Program Studi Akuntansi Program Magister, Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia telah mengadakan ujian tesis yang disusun oleh:

KHARISMA FATMALINA FAJRI

No. Mahasiswa : 20919050

Konsentrasi : Audit Forensik

Dengan Judul:

EVALUASI PEMANFAATAN *REGULATORY TECHNLOGY* DALAM SISTEM ANTI-PENCUCIAN UANG UNTUK ASET VIRTUAL DI INDONESIA

Berdasarkan penilaian yang
diberikan oleh Tim Penguji, maka
tesis tersebut dinyatakan **LULUS**

Penguji I	Penguji II
Dekar Urumsah, S.E., S.Si., M.Com(IS), Ph.D.	Hendi Yogi Prabowo, S.E., M.For.Accy, Ph.D.

Mengetahui
Ketua Program Studi,

Ariel Rahmah, S.E., S.I.P., M.Com., Ph.D.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Assalamu'alaikum Warahmatullahi Wabarakaatuh

Segala puji syukur peneliti tunjukan ke hadirat Allah SWT karena atas petunjuk, berkah, rahmat dan karunia-Nya, peneliti dapat menyelesaikan penyusunan tesis ini dengan baik. Tidak lupa junjungan shalawat serta salam peneliti haturkan kepada Nabi Muhammad SAW yang telah menyampaikan risalah Allah SWT serta menjadi suri teladan yang baik bagi umat manusia, menjadi penerang dikala gelap menghampiri, membimbing umat manusia dengan keimanan dan ketaqwaan untuk melihat kebesaran dan keagungan Allah SWT.

Penyusunan tesis yang berjudul **"Evaluasi Pemanfaatan *Regulatory Technology* dalam Sistem Anti-Pencucian Uang untuk Aset Virtual di Indonesia"** dilakukan guna memenuhi salah satu syarat dalam menyelesaikan Pendidikan Program Magister (S-2) pada Program Studi Akuntansi Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia. Dalam penyusunan tesis ini tentunya tidak terlepas dari do'a, dukungan dan bantuan berbagai pihak. Oleh karena itu, peneliti mengucapkan syukur dan terima kasih kepada:

1. Allah SWT yang tidak pernah berhenti untuk selalu mengasihi, menyayangi dan mengampuni hamba-Nya, memberikan takdir terbaik bagi hamba-Nya.
2. Nabi Muhammad SAW sebagai perantara kepada umat manusia untuk dapat mengenal kebesaran dan keagungan Allah SWT, mengajarkan keimanan dan ketaqwaan yang seakan tidak pernah ada habisnya.

3. Ayah, Mama, Kakak, dan Adik peneliti yang selalu mendo'akan dan memberikan dukungan kepada peneliti. Semoga selalu dalam lindungan, penjagaan, dan keberkahan Allah SWT.
4. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D. selaku Rektor Universitas Islam Indonesia Periode 2022-2026.
5. Bapak Johan Arifin, S.E., M.Si., Ph.D., CFrA., CertIPSAS selaku Dekan Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia Periode 2022-2026.
6. Bapak Dekar Urumsah, S.E., S.Si., M.Com(IS), Ph.D., CFrA selaku Ketua Jurusan Akuntansi Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia Periode 2022-2026 dan Dosen Pembimbing Tesis yang telah meluangkan banyak waktu dan tenaganya untuk membimbing peneliti serta memberikan banyak ilmu bagi peneliti. Terima Kasih, semoga Bapak selalu sehat dan selalu dalam lindungan Allah SWT.
7. Bapak Arief Rahman, S.E., S.I.P., M.Com., Ph.D., CertDA selaku Ketua Program Studi Magister Akuntansi Fakultas Bisnis dan Ekonomika Universitas Islam Indonesia Periode 2022-2026.
8. Seluruh partisipan wawancara, terima kasih telah membantu dan bekerjasama dengan peneliti agar peneliti dapat menyelesaikan penelitian ini.
9. Seluruh Sivitas Akademika dan Staff Universitas Islam Indonesia, khususnya Program Studi Magister Akuntansi yang telah memberikan ilmu dan pengalaman kepada peneliti.

10. Seluruh pihak yang pernah hadir untuk mendukung, mendo'akan dan membantu peneliti. Terima kasih, semoga Allah SWT mengganti dan membalas dengan sesuatu yang jauh lebih baik.

Peneliti berharap bahwa penelitian yang masih jauh dari kata sempurna ini dapat memberikan kontribusi bagi perkembangan ilmu pengetahuan, khususnya di bidang akuntansi forensik serta bagi siapapun yang membacanya. Kritik dan saran yang membangun sangat diharapkan oleh peneliti.

Wassalamu'alaikum Warahmatullahi Wabarakaatuh

Yogyakarta, 26 Desember 2023

Peneliti

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Di Indonesia, pemanfaatan RegTech dalam mencegah *crypto laundering* masih terus berkembang. Namun, efektivitasnya belum menunjukkan hasil yang siginifikan sehingga perlu dilakukan eksplorasi penyebab mengenai tidak efektifnya pemanfaatan RegTech. Penelitian ini bertujuan untuk mengetahui regulasi mekanisme pencegahan *crypto laundering*, penyebab tidak efektifnya pemanfaatan RegTech, serta rekomendasi perbaikan yang dapat diterapkan oleh para pemangku kepentingan. Peneliti menggunakan data sekunder dan data primer. Data sekunder diperoleh dengan mengumpulkan dokumen regulasi yang relevan. Sedangkan data primer diperoleh melalui wawancara semi-terstruktur dengan partisipan yang berkompetensi dalam *anti-money laundering operating system*. Analisis data dilakukan dengan pendekatan analisis isi *(content analysis)* untuk data sekunder dan analisis tematik *(thematic analysis)* untuk data primer. Hasil analisis data dengan analisis isi mengungkapkan bahwa mekanisme pencegahan *crypto laundering* dilakukan melalui proses KYC *(know your customer)* dan pemantauan transaksi *(transaction monitoring)* berdasarkan pendekatan berbasis risiko *(risk-based approach)*. Sedangkan hasil analisis data dengan analisis tematik mengungkapkan bahwa penyebab tidak efektifnya pemanfaatan RegTech disebabkan karena terdapat beberapa kekurangan dalam regulasi pencegahan *crypto laundering* dan implementasi regulasi melalui RegTech. Rekomendasi perbaikan kepada para pemangku kepentingan dibagi ke dalam dua jenis, yaitu perbaikan dalam pencegahan *crypto laundering* dan pemanfaatan RegTech.

Kata Kunci: *Crypto Laundering*, Pencegahan *Crypto Luandering*, RegTech

ABSTRACT

In Indonesia, the use of RegTech in preventing crypto laundering is still developing. However, its effectiveness has not shown significant results, so it is necessary to explore the causes of the ineffective use of RegTech. This research aims to determine the regulation of crypto laundering prevention mechanisms, the causes of ineffective use of RegTech, and recommendations for improvements which can be implemented by stakeholders. Researcher used secondary and primary data. Secondary data was obtained by collecting relevant regulatory documents. Meanwhile, primary data was obtained through semi-structured interviews with participants who have an anti-money laundering operating system background. Data analysis was conducted using content analysis for secondary data and thematic analysis for primary data. The results of content analysis reveal that the crypto laundering prevention mechanism is carried out through the KYC (know your customer) and transaction monitoring, which conducted based on a risk-based approach. While the results of thematic analysis reveal that the cause of ineffective use of RegTech is due several lacks of the regulation of crypto laundering and implementation of regulations through RegTech. Recommendations for improvement to stakeholders are divided into two, namely improvement in the prevention of crypto laundering and the use of RegTech.

Keywords: *Crypto Laundering, Crypto Laundering Prevention, RegTech*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Money laundering (ML) merupakan proses tidak berwujud yang digunakan untuk menyamarkan asal mula atas keuntungan yang dihasilkan melalui kegiatan kriminal (Gottschalk, 2010) atau dengan kata lain, ML berarti mengamankan hasil tindak pidana yang dilakukan oleh pelaku (Pontes *et al*., 2022). Aktivitas ML menjadi aktivitas yang penting dalam tindak kejahatan keuangan (Gottschalk, 2010) karena terdiri atas proses penyembunyian *(concealment)* (Pickett & Pickett, 2002) dan konversi *(conversion)* (Albrecht *et al.*, 2012) dari tindak kejahatan keuangan asal *(predicate crime)*, seperti: kecurangan *(fraud)*, korupsi *(corruption*) dan pencurian *(theft)*. Hasil dari proses ML diintegrasikan dengan proses ekonomi yang sah menurut hukum agar para pelaku dapat menggunakannya secara aman karena tujuan dari ML adalah mengubah hasil yang tidak sah menjadi seolah-olah sah menurut hukum (Gottschalk, 2010). Dalam melakukan aktivitasnya, pelaku menggunakan berbagai media untuk 'mencuci' uang tersebut. Institusi keuangan—terutama Bank—memiliki probabilitas yang tinggi sebagai media yang digunakan untuk ML (Haryono & Sofwan, 2020) karena Bank menjadi tempat yang aman bagi para pelaku dalam menyembunyikan uangnya (Go & Benarkah, 2019).

ML mengakibatkan rusaknya tatanan *financial market* dan mengikis kepercayaan publik terhadap sistem keuangan global (Pramod *et al*., 2012), stabilitas serta perkembangan ekonomi dan politik (Aluko & Bagheri, 2012).

Rata-rata kerugian global per tahun akibat dari tindak pidana ML berkisar antara 2% hingga 5% dari produk domestik bruto dunia *(world's gross domestic product)* atau berkisar antara USD 590 Miliar hingga USD 1.5 Triliun (FATF, 2022). Jika tidak ditangani secara efektif maka ML dapat menguasai sistem ekonomi yang lebih besar melalui skema investasi atau menawarkan suap kepada pejabat publik atau bahkan pemerintah untuk menyempurnakan aktivitasnya (Albrecht et al., 2019).

Pelaku ML cenderung mencari negara dengan risiko rendah untuk terdeteksi karena hal tersebut mengindikasikan tidak efektifnya sistem *anti-money laundering* (AML) di negara tersebut (FATF, 2022). Negara berkembang menjadi tempat yang 'hijau' bagi para pelaku ML dalam melakukan aktivitasnya karena sistem AML di negara berkembang cenderung tidak selektif (Aluko & Bagheri, 2012), seperti beberapa contoh dari hasil penelitian pada beberapa negara sebagaimana yang disajikan pada Tabel 1.1:

Tabel 1.1 Kompilasi Penerapan *Anti-Money Laundering* di Negara Berkembang

Negara	Penerapan AML	Kekurangan	Implikasi
Malaysia (Zolkaflil *et al*., 2019)	Prosedur investigasi ML dilaksanakan cukup baik oleh aparat penegak hukum	Undang-Undang AML belum mendukung rangkaian proses investigasi yang seharusnya	AML tidak efektif
Myanmar (Thompson, 2018)	Pengembangan AML *Framework*	Keahlian teknis serta sumber daya keuangan dan manusia untuk memastikan kepatuhan dan penegakkan hukum	Risiko ML belum menurun secara signifikan

Tabel 1.1 Kompilasi Penerapan *Anti-Money Laundering* di Negara Berkembang (Lanjutan)

Negara	Penerapan AML	Kekurangan	Implikasi
Vietnam (Nguyen Le, 2013)	Pengembangan AML *Framework* sejak tahun 2005	Para penyidik masih berfokus pada *predicate crime* dan belum memiliki keinginan untuk melakukan investigasi mendalam terhadap aliran dana dari *predicate crime*	Tingkat kerentanan ML masih tinggi
India (Viritha *et al*., 2015)	Implementasi AML sudah dilakukan oleh Bank	Implementasi tidak merata di setiap cabang	Probabilitas signifikan pada Bank sebagai media ML
Qatar (Truby, 2016)	Kepatuhan AML terbukti secara berkelanjutan	Masih jauh dengan rekomendasi *Financial Action Task Force* (FATF)	Pengawasan ML tidak efektif

Sumber: Peneliti, Diolah

Pada umumnya, hampir semua negara berkembang memiliki mekanisme AML, namun tidak seefektif sistem yang diimplementasikan oleh negara maju (Aluko & Bagheri, 2012). Penegakkan hukum melalui undang-undang AML sangat penting dan pelaksanannya harus efektif. Namun, penegakkan hukum pada ML relatif bersifat *post factum* (setelah peristiwa) yang menunjukkan bahwa masih adanya kemungkinan kerugian atau kerusakan atas tindak pidana ML sehingga sistem AML harus bersifat preventif atau dapat mencegah terjadinya ML (Basel Institue of Governance, 2021) karena aktivitas ML sangat dipengaruhi oleh gaya hidup manusia dan kemajuan teknologi sehingga selalu bersifat dinamis (Wronka, 2022b).

Sifat dinamis atas aktivitas ML yang dipengaruhi oleh kemajuan teknologi, perkembangan dunia digital, dan penggunaan internet tersebut menjadi pemicu aktivitas ML dengan teknik terbaru (Mugarura & Ssali, 2020). Penggunaan internet dimanfaatkan oleh para pelaku ML untuk melakukan ML melalui transaksi daring atau disebut sebagai *cyber-laundering* dengan menggunakan pembayaran digital dan mata uang virtual *(virtual currencies)* atau *cryptocurrencies* agar terhindar dan tidak mudah terdeteksi oleh aparat penegak hukum (Wronka, 2022a; Wronka, 2022b; Mardiansyah, 2021). Sulitnya pendeteksian ini disebabkan karena *cyber-laundering* menggunakan lebih dari satu mata uang *(multiple currencies)* dimana para pelaku menggunakan *cryptocurrencies* yang mudah digunakan, relatif anonim, sulit ditelusuri dan penggunaannya tidak dibatasi oleh peraturan perundang-undangan (van Wegberg *et al*., 2018; Leuprecht *et al*., 2022). *Cryptocurrencies* digunakan oleh para pelaku ML pada tahap penempatan *(placement)* dan transfer *(layering)*, kemudian menggunakan mata uang yang sah *(fiat currencies)* pada tahap integrasi *(integration)* (Leuprecht *et al*., 2022). Penggunaan *cryptocurrencies* dalam aktivitas ML semakin bertambah yang ditandai oleh meningkatnya kasus secara eksponensial (Dyntu & Dykyi, 2019) dengan kenaikan sebesar 30% pada tahun 2021 (Chainalysis, 2022). Sulitnya pendeteksian pada aktivitas ML yang melibatkan *cryptocurrencies* dan atau *cryptocurrencies* yang diintegrasikan dengan *fiat currencies* disebabkan karena kelemahan bawaan dari sistem regulasi nasional dan internasional yang belum dapat mencegah aktivitas ML transnasional (Mugarura & Ssali, 2020; Pavlidis, 2020).

Di Indonesia—sebagai salah satu negara berkembang dengan 29.6% penduduk tercatat oleh Kementerian Komunikasi dan Informatika sebagai pengguna internet per tahun 2021—pengguna dan pemilik *cryptocurrency* mencapai 15% dari jumlah penduduk per Bulan Oktober 2022, yang mana jumlah ini lebih tinggi dari rata-rata global sebesar 14% dari jumlah penduduk (Finder, 2022). *Cryptocurrency* dan *crypto asset* ditetapkan sebagai komoditi yang dapat diperdagangkan di Bursa Berjangka (Jakfar, 2022), namun bukan merupakan alat pembayaran yang sah di Indonesia karena sifatnya yang tidak dikendalikan oleh otoritas moneter atau bank sentral setempat (Kementerian Keuangan RI, 2022). Mata uang virtual atau *cryptocurrency* diketahui sebagai *emerging threat* pada tindak pidana pencucian uang (TPPU) sejak tahun 2015 yang digunakan dalam transaksi *digital money network* pada pasar gelap daring sebagai hasil dari tindak pidana perpajakan dan aktivitas perjudian daring dengan risiko TPPU pada tingkat menengah (Mardiansyah, 2021). Aktivitas TPPU ini dikategorikan oleh hukum pidana Indonesia sebagai perbuatan pidana dimana pelaku beserta aset virtualnya dapat dijerat secara hukum (Utami, S., 2021).

Menanggapi berbagai tantangan tersebut yang berpengaruh terhadap sistem AML dan meningkatkan ancaman terhadap stabilitas perekonomian regional maupun global, maka *Financial Action Task Force* (FATF) merekomendasikan kepada negara anggotanya untuk memastikan bahwa penyedia layanan aset virtual harus terdaftar pada otoritas moneter setempat serta patuh terhadap sistem anti-pencucian uang yang efektif sebagai upaya mitigasi risiko dan pencegahan pencucian uang melalui aset virtual (FATF, 2022). Penggunaan aset virtual dalam

aktivitas ilegal mencapai lebih dari 37 Juta transaksi per tahun (Leuprecht *et al.*, 2022) sehingga menghasilkan data dalam jumlah yang besar. Besarnya jumlah serta proliferasi dari data tersebut menyebabkan kepatuhan terhadap sistem AML menjadi lebih mahal dan rumit (Teichmann *et al.*, 2022). Untuk itu, pengadopsian sistem otomatisasi digital *(digital automation)* melalui *regulatory technology* (RegTech) menjadi solusi yang efektif dalam mencegah ML dengan melibatkan aset dan atau mata uang virtual (Teichmann *et al*., 2022).

RegTech dengan versi terbaru (RegTech 3.0) berpindah fokus dari *know your customer* (KYC) menjadi *know your data* (KYD) (Umalkar, 2021) melalui pengaplikasian *data analytics* untuk memperkirakan risiko potensial yang muncul (Teichmann et al., 2022). RegTech membantu organisasi dalam mencegah ML dengan mengendalikan dan menganalisis transaksi serta verifikasi identitas secara cepat dan akurat (Zabelina *et al*., 2018). Beberapa teknologi terbaru dalam RegTech yang terbukti dapat membantu pengendalian dan analisis tersebut, yaitu *machine learning* (Ruiz & Angelis, 2021), *artificial intelligence* (Kurum, 2020), dan *cloud computing* (Kurum, 2020).

Beberapa penelitian mengenai *crypto laundering* (Leuprecht *et al*., 2022; Wronka, 2022c; Akartuna *et al*., 2022; Albrecht *et al*., 2019; Dyntu & Dykyi, 2019; van Wegberg *et al.*, 2018), dan pemanfaatan RegTech (Utami & Septivani, 2022b; Utami & Septivani, 2022a; Meiryani *et al*., 2022; Kurum, 2020; Naheem, 2018; Anagnostopoulos, 2018) sudah dilakukan. Sedangkan penelitian yang secara khusus memaparkan mengenai pemanfaatan RegTech dalam mencegah *crypto laundering* hanya dilakukan oleh Ruiz dan Angelis (2021). Di Indonesia,

terdapat beberapa penelitian mengenai pemanfaatan RegTech dalam mencegah pencucian uang yang berfokus pada pengujian tingkat efektivitas dari pemanfaatan RegTech melalui studi kuantitatif (Utami & Septivani, 2022a; Utami & Septivani, 2022b; Meiryani *et al*., 2022). Hasilnya, ditemukan bahwa efektivitas pemanfaatan RegTech di Indonesia tidak menunjukkan hasil yang signifikan. Maka dari itu, penelitian ini bertujuan untuk mengeksplorasi penyebab atas temuan penelitian sebelumnya, yaitu mengenai tidak signifikannya efektivitas pemanfaatan RegTech, khususnya dalam pencegahan *crypto laundering*. Dengan fokus yang berbeda serta pengaplikasian pendekatan kualitatif, penelitian ini berkontribusi terhadap penelitian terdahulu dalam memberikan tambahan temuan, sehingga hasil penelitian mengenai tidak efektifnya pemanfaatan RegTech dalam mencegah *crypto laundering* dapat disajikan secara integral.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan maka penelitian ini memiliki rumusan masalah sebagai berikut:

1. *Bagaimana mekanisme sistem AML untuk crypto asset di Indonesia?*

   Pertanyaan ini bertujuan untuk mengetahui mekanisme, pedoman penerapan, dan pemanfaatan RegTech yang berlaku di Indonesia dalam mencegah tindak pidana pencucian uang virtual atau *cryptocurrencies*.

2. *Mengapa pemanfaatan RegTech tidak signifikan?*

   Pertanyaan ini bertujuan untuk mengetahui penyebab tidak signifikannya pemanfaatan RegTech dalam mencegah ML yang melibatkan penggunaan *cryptocurrencies* dan *crypto asset*.

3. *Bagaimana rekomendasi perbaikan untuk menurunkan risiko penyebab dan tantangan dalam pemanfaatan RegTech untuk mencegah crypto laundering?*
   Pertanyaan ini bertujuan untuk memberikan rekomendasi perbaikan yang dapat digunakan oleh para pemangku kepentingan untuk meningkatkan pemanfaatan RegTech dalam mencegah ML yang melibatkan penggunaan *cryptocurrencies* dan *crypto asset*.

1.3 Tujuan Penelitian

Sebagaimanana latar belakang dan rumusan masalah yang telah dipaparkan maka penelitian ini memiliki tujuan sebagai berikut:

1. Mengetahui mekanisme pencegahan tindak pidana pencucian uang virtual atau *cyber-money laundering* yang melibatkan *cryptocurrencies* dan *crypto asset* di Indonesia;
2. Menganalisis penyebab dan tantangan yang dihadapi oleh Indonesia dalam pemanfaatan RegTech untuk mencegah *crypto laundering*;
3. Memberikan rekomendasi solusi atau saran perbaikan dalam pemanfaatan RegTech untuk *crypto laundering*.

1.4 Fokus Penelitian

Agar hasil yang diperoleh dapat menjawab rumusan masalah dan sesuai dengan tujuan penelitian, maka peneliti menentukan fokus penelitian sebagai berikut:

1. Aspek Penelitian : Mekanisme dan pedoman penerapan sistem AML untuk *cryptocurrencies* dan *crypto asset* di Indonesia.
2. Objek Penelitian : Dokumen dan pihak yang berkaitan dengan

pemanfaatan RegTech dalam mencegah *crypto laundering*.

1.5 Manfaat Penelitian

Hasil Penelitian ini diharapkan dapat memberikan manfaat dan kontribusi sebagai berikut:

1. Manfaat Akademis

   Menambah kontribusi literatur pada bidang kepatuhan dan akuntansi forensik digital mengenai pemanfaatan RegTech dalam mencegah ML yang melibatkan *virtual asset* atau *cryptocurrencies* atau *crypto asset* di Indonesia serta menjadi acuan bagi penelitian selanjutnya yang membahas mengenai *crypto laundering*, baik di Indonesia maupun negara lain.

2. Manfaat Praktis

   Memberikan kontribusi pengetahuan dan rekomendasi kepada para pemangku kepentingan dan atau pihak berwenang dalam meningkatkan pemanfaatan RegTech guna mencegah ML yang melibatkan *cryptocurrencies* dan *crypto asset* di Indonesia.

1.6 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang dari dilakukannya penelitian ini. Kemudian, dari latar belakang tersebut dipaparkan mengenai rumusan dan tujuan penelitian, fokus penelitian, serta manfaat penelitian. Pada Sub-Bab terakhir, dipaparkan mengenai sistematika penulisan dalam penelitian ini.

BAB II KAJIAN PUSTAKA

Bab ini berisi telaah pustaka untuk mendapatkan landasan teori yang dapat digunakan oleh peneliti dalam membantu menjawab rumusan masalah. Selanjutnya, pada bab ini juga dipaparkan mengenai beberapa penelitian terdahulu yang relevan dengan penelitian ini. Pada bagian terakhir dari bab ini, digambarkan kerangka penelitian untuk membantu peneliti dalam melakukan analisis.

BAB III METODOLOGI PENELITIAN

Bab ini memaparkan langkah-langkah yang dilakukan peneliti dalam melakukan penelitian. Bab ini berisi pemaparan mengenai jenis dan instrumen penelitian yang digunakan oleh peneliti, prosedur penelitian, sumber dan pengumpulan data, teknik analisis data, teknik pengujian keabsahan data, serta penyajian data.

BAB IV HASIL DAN PEMBAHASAN

Bab ini memaparkan jawaban atas rumusan masalah yang diperoleh dari hasil analisis data dan diskusi temuan dalam penelitian. Hasil analisis data dan diskusi temuan disusun secara sistematis berdasarkan rincian pada rumusan masalah.

BAB V PENUTUP

Bab ini memaparkan kesimpulan dari penelitian yang dilakukan, kontribusi dan implikasi penelitian, serta keterbatasan dan saran untuk penelitian selanjutnya.

BAB II

KAJIAN PUSTAKA

2.1 *Money Laundering*

Istilah *"Money Laundering"* pertama kali digunakan pada tahun 1930-an oleh para mafia Amerika yang mendirikan tempat 'pencucian' untuk melegitimasi hasil kriminal mereka (Schneider & Windischbauer, 2008). *Money laundering* (ML) merupakan salah satu sub-kategori dari *financial crime* dan menjadi aktivitas yang penting bagi sebagian besar tindakan kriminal karena ML memiliki motif untuk mendapatkan keuntungan ekonomis dari beberapa aktivitas ilegal, seperti: *embezzlement* (penggelapan), *fraud* (penipuan), *misappropriation* (penyalahgunaan), *corruption* (korupsi), *robbery* (perampokan), *distribution of narcotic drugs* (peredaran narkotika) dan *human trafficking* (perdagangan manusia) (Gottschalk, 2010; Lukito, 2016). Peningkatan perdagangan narkoba di seluruh dunia, korupsi dan kejahatan yang terorganisir telah meningkatkan kecenderungan para pelaku untuk melakukan pencucian hasil yang berasal dari aktivitas ilegal mereka (Fabre, 2003). Secara umum, ML dapat dikatakan sebagai proses menyembunyikan hasil kejahatan atau berasal dari hal yang bersifat ilegal kemudian mengubahnya menjadi aset yang sah dan legal (CAMS, 2012).

Proses ML terbagi atas tiga tahap yang disebut sebagai *three-stage process* (Gottschalk, 2010), yaitu:

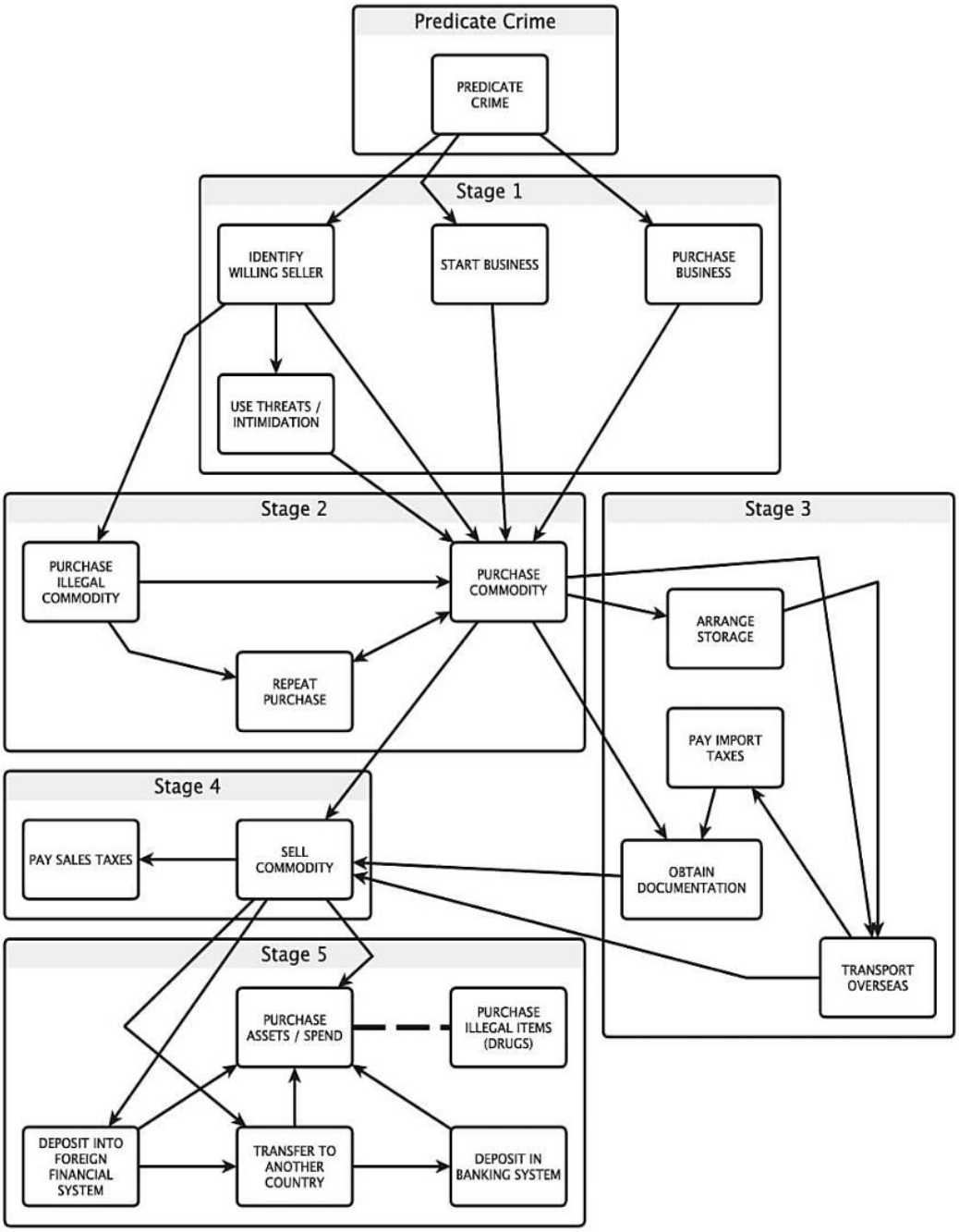
1. *Placement Stage*, memindahkan dana yang berasal dan berhubungan langsung dengan aktivitas kriminal;

2. *Layering Stage,* menyamarkan jejak untuk mempersulit pihak yang berwenang dalam mendeteksi;
3. *Integration Stage*, melegitimasi hasil sehingga dapat digunakan dengan bebas oleh pelaku untuk kepentingan pribadi dengan membeli aset atau berinvestasi di bisnis yang legal.

Namun, *three-stage process* dinilai masih menggunakan pendekatan dasar dalam menjelaskan proses ML sehingga Gilmour (2014) mengembangkannya menjadi lima tahap *(five-stage process)* melalui pendekatan *crime script* untuk memahami proses ML dalam praktik, sebagai berikut:

1. *Identification Stage*, mengidentifikasi bisnis atau komoditas yang bernilai tinggi di masa depan;
2. *Placement Stage*, memindahkan dana dari aktivitas ilegal ke dalam komoditas yang bernilai tinggi di masa depan—seperti: barang mewah—dengan menggunakan uang tunai untuk mempersulit pendeteksian;
3. *Further Preparatory Work*, mempersiapkan dan memfasilitasi pelaku agar proses ML dapat berjalan lebih efektif, namun proses ini tidak diperlukan di setiap keadaan;
4. *Layering Stage*, komoditas dari hasil ilegal dijual secara sah dan memiliki catatan transaksi keuangan untuk menghindari kecurigaan dari pihak berwenang;
5. *Integration Stage*, dana yang dapat dipertanggungjawabkan secara sah digunakan untuk pembelian kepentingan pribadi.

Five-stage process dari ML digambarkan oleh Gilmour (2014) melalui skema pembelian komoditas bernilai tinggi *(high-value commodities)* yang disajikan pada Gambar 2.1.



Gambar 2.1 *Five-Stage Process*: Skema Pembelian Komoditas

Sumber: Gilmour (2014)

Proses ML bersifat dinamis, dimana para pelaku secara aktif mengidentifikasi lokasi dengan tingkat deteksi ML yang rendah, beradaptasi dengan perubahan kondisi situasional serta melibatkan eksploitasi produk dan jasa sehingga membuatnya sulit untuk ditetapkan dan dituntut sebagai aktivitas tindak pidana pencucian uang dan atau tindakan melawan hukum (Gilmour, 2016).

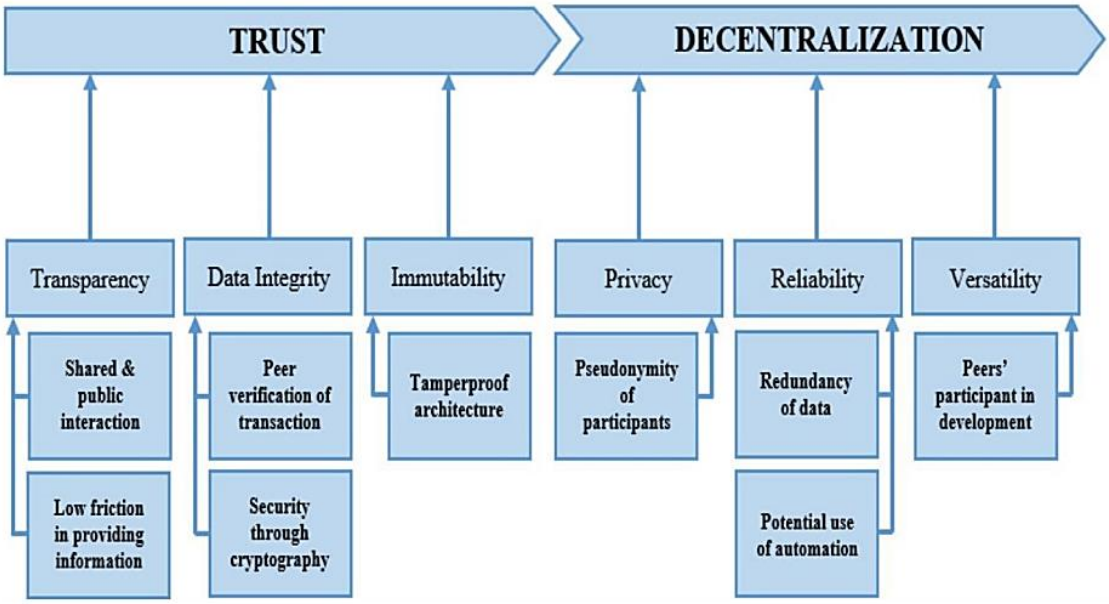
2.1.1 *Money Laundering* melalui *Cryptocurrency*

2.1.1.1 *Cryptocurrency*

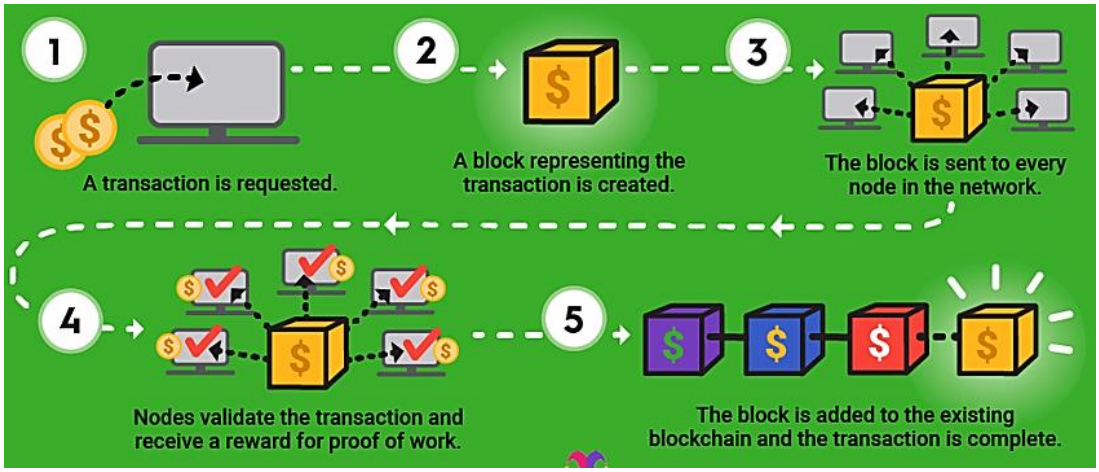
Cryptocurrencies merupakan mata uang virtual yang pertama kali diperkenalkan oleh Satoshi Nakamoto pada tahun 2009 dengan menciptakan bitcoin sebagai salat satu jenis mata uang dalam *cryptocurrencies* (Albrecht *et al.*, 2019). Berbeda dengan *fiat currencies* yang dikeluarkan secara sah oleh suatu negara, mata uang virtual ini tidak dikeluarkan dan tidak terikat oleh suatu negara *(stateless)* serta tidak berwujud *(intangible)* dengan mengandalkan *blockchain* sebagai *virtual ledger* untuk menjamin stabilitas nilai mata uang (Adachi & Aoyagi, 2020). Stabilitas nilai mata uang dapat terjamin karena setiap transaksi *cryptocurrencies* yang berisi serangkaian kode dalam *virtual ledger* dienkripsi dan diverifikasi oleh *blockchain* (Litchfield, 2015). *Blockchain* bersifat terbuka *(open public)* sehingga transaksi yang dienkripsi dan diverifikasi adalah semua transaksi dalam *cryptocurrencies* dengan tujuan untuk menyusun *'block-chain'*, bukan untuk menyusun transaksi milik masing-masing individu atau organisasi (Albrecht *et al*., 2019). Setiap *block* menyimpan *hash* (sekumpulan kode) kriptografi dari *block* sebelumnya yang menyusun sebuah rantai *(chain)*, dimana *hash* kriptografi juga mengambil data dari *block* sebelumnya dan mengubahnya

menjadi sebuah *string* yang ringkas (Zaman *et al.*, 2023). *String* tersebut tidak dapat diprediksi sehingga koneksi *block* menjadikan rantai *(chain)* aman dan bersifat terdesentralisasi (Zaman *et al*., 2023) atau tidak terdapat *sever* terpusat yang memegang transaksi sehingga setiap *block* harus memenuhi persyaratan rantai *(chain)* agar tidak terdapat transaksi yang dapat menggantikan transaksi sebelumnya (Moore, 2018).

Selain memiliki karakteristik terdesentralisasi, teknologi *blockchain* juga memiliki karakteristik *trust* (Seebacher & Schüritz, 2017). Masing-masing karakeristik memiliki sub-atribut yang disajikan melalui Gambar 2.2. Sedangkan proses pencatatan transaksi yang terjadi dalam teknologi *blockchain* sehingga membentuk *'block-chain'* disajikan melalui Gambar 2.3.



Gambar 2.2 Karakteristik Teknologi *Blockchain*
Sumber: Seebacher dan Schüritz (2017)



Gambar 2.3 Proses Pencatatan Transaksi dalam *Blockchain*
Sumber: Bylund, 2023

Jika *cryptocurrencies* dibandingkan dengan *fiat currencies* maka terdapat beberapa perbedaan mendasar (Wronka, 2022a; Wronka, 2022c) yang disajikan pada Tabel 2.1.

Tabel 2.1 Perbedaan antara *Fiat Currencies* dengan *Cryptocurrencies*

	Fiat Currencies	***Cryptocurrencies***
Financial institution	*Banks and payment institutions*	*No institution involved, but crypto platforms instead*
Storage of the transactions	*Central at the institute*	*Decentralized on the blockchain*
Business partner	*Known person*	*Pseudonym, known person if applicable*
Customer	*Identified person*	*Pseudonym, identified person if applicable*
Storage and disposal	*Banknotes and cards*	*Wallet with the public keys*
Access to the assets	*PIN/signature/cheque*	*Private key*
Allocation of the payment	*IBAN with Bank Identification Code (BIC)*	*Public key*
Monitoring of the transactions	*Accounts and payment transactions*	*Blockchain*

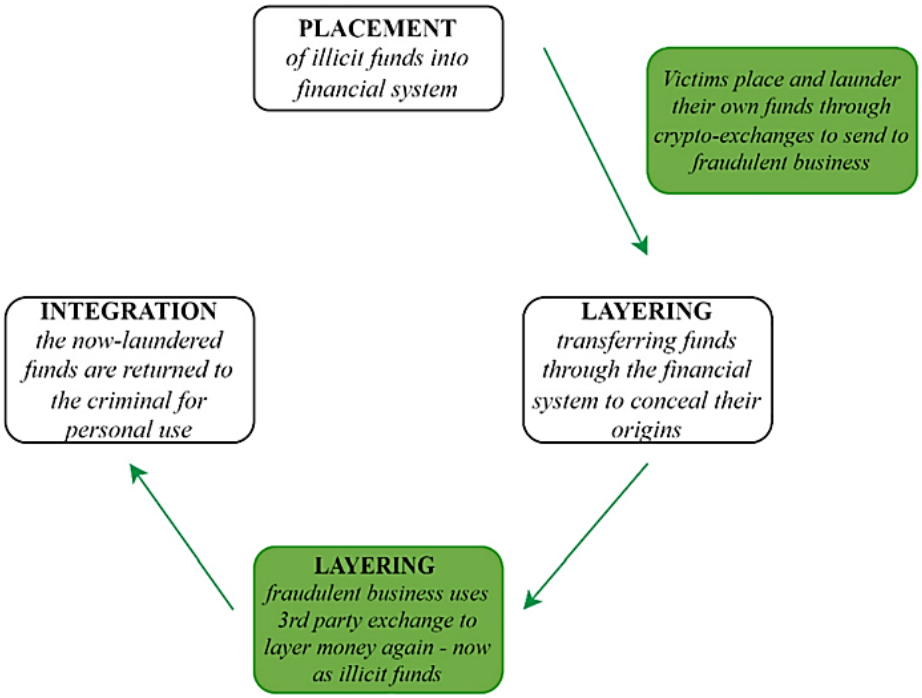
Sumber: Wronka (2022c)

Dengan sifatnya yang demikian, *cryptocurrencies* tidak membutuhkan Bank atau lembaga intermediasi lain dalam melakukan transaksi keuangan (Peters *et al*., 2015) dan pemilik dari transaksi keuangan tersebut sulit diidentifikasi karena relatif anonim (van Wegberg *et al*., 2018; Albrecht *et al*., 2019; Leuprecht *et al*., 2022; Al-Tawil, 2022) sehingga para pelaku kejahatan keuangan mulai menggunakan *cryptocurrencies* selama proses ML (Albrecht *et al.,* 2019). Para pelaku dapat dengan mudah memindahkan dana dari satu negara ke negara lainnya dalam jaringan *cryptocurrencies* hanya dengan koneksi internet karena sifatnya yang *stateless* serta tidak terdapat otoritas pusat yang mengatur (Albrecht *et al*., 2019). Dengan kemudahan tersebut, *cryptocurrencies* menjadi ancaman bagi keamanan sistem keuangan global (Al-Tawil, 2022). Data terkini menujukkan bahwa terdapat kenaikan sebesar 30% dari tahun 2020 ke tahun 2021 dalam penggunaan *cryptocurrencies* untuk aktivitas ML pada *darknet market* dan belum termasuk aktivitas ML melalui *cryptocurrencies* yang diintegrasikan dengan *fiat currencies* (Chainalysis, 2022). Penggunaan *cryptocurrencies* yang diintegrasikan dengan *fiat currencies* melalui konversi *fiat currencies* ke *cryptocurrencies* ataupun sebaliknya dilakukan oleh para pelaku untuk menyulitkan pendeteksian (Leuprecht *et al*., 2022).

2.1.1.2 *Crypto Laundering*

Sebagaimana proses ML secara konvensional, proses ML melalui *cryptocurrencies* juga terdiri atas tiga tahapan utama, yaitu penempatan *(placement)*, transfer *(layering)* dan integrasi *(integration)*. *Placement* menjadi tahapan yang sangat penting karena melalui tahapan ini, penelusuran transaksi

keuangan dapat ditelusuri (Albrecht *et al.*, 2019) sehingga para pelaku ML menggunakan *cryptocurrencies* yang bersifat anonim dan sulit didentifikasi pada tahapan ini (Leuprecht *et al.*, 2022). *Cryptocurrencies* juga digunakan pada tahapan *layering* karena sifatnya yang virtual dan *stateless* sehingga dana dapat ditempatkan oleh para pelaku ML pada yurisdiksi manapun melalui perdagangan, investasi atau pertukaran koin dengan *cryptocurrency* jenis lain (Leuprecht *et al.*, 2022). Sedangkan pada tahap *integration*, biasanya pada pelaku ML melakukan pertukaran *cyptocurrencies* dengan *fiat currencies* (Leuprecht *et al.*, 2022; Albrecht et *al.*, 2019). Penggunaan dan pertukaran *cryptocurrencies* dalam aktivitas ML digambarkan melalui skema pada Gambar 2.4 (Leuprecht *et al.*, 2022).



Gambar 2.4 Skema *Money Laundering* melalui *Cryptocurrencies*
Sumber: Leuprecht et al. (2022)

2.1.2 *Money Laundering* di Indonesia

Risiko terbesar dari ML yang terjadi di Indonesia berasal dari tindak pidana asal *(predicate crime)* narkotika, korupsi, perpajakan serta kejahatan pada bidang kehutanan/lingkungan *(forestry* atau *environmental crime)* dimana para pelaku melakukannya dengan sistem *self-laundering*. Hasil dari berbagai tindak pidana tersebut disalurkan melalui perbankan, pasar modal serta bisnis sektor perkebunan dalam negeri *(foreign inward)* maupun lintas yurisdiksi *(foreign outward* atau *laundering off-shore)* (APGML, 2018). Indonesia—melalui lembaga PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan)—telah melaksanakan pengkinian penilaian risiko nasional Tindak Pidana Pencucian Uang (TPPU) pada tahun 2019 (Mardiansyah, 2021) dengan temuan yang disajikan pada Tabel 2.2.

Tabel 2.2 Risiko Utama Nasional Tindak Pidana Pencucian Uang

No.	Jenis Penilaian	Temuan
1.	Penilaian Risiko Nasional Tindak Pidana Pencucian Uang (TPPU)	Risiko TPPU berdasarkan: 1. **Tindak Pidana**: Narkotika, Korupsi, Perbankan, Kehutanan, Pasar Modal 2. **Ancaman dari Luar Negeri**: Perpajakan, Perbankan, Kehutanan 3. ***Foreign Predicate Crime****:* Korupsi, Penipuan, Narkotika 4. ***Laundering Offshore***: Narkotika, Korupsi, Perpajakan 5. **Wilayah**: DKI Jakarta 6. **Kelompok Industri**: Perbankan, Pasar Modal, Perusahaan Properti, Perdagangan Kendaraan Bermotor 7. **Profil Perorangan**: Pengusaha dan Pegawai Swasta 8. **Profil Perorangan berdasarkan *Legal Persons***: Perusahaan Penanaman Moda Asing (PMA) 9. **Profil Korporasi**: PT, Yayasan, Koperasi Non-UMKM 10. ***Emerging Threat***: Penggunaan *virtual currency*

Tabel 2.2 Risiko Utama Nasional Tindak Pidana Pencucian Uang (Lanjutan)

No.	Jenis Penilaian	Temuan
2.	*White Papers* Perpajakan Direktorat Jenderal Pajak (DJP), Kementerian Keuangan	Perubahan risiko TP perpajakan dari risiko tinggi tindak pidana asal (TPA) menjadi TPPU menjadi risiko menengah yang disebabkan oleh penguatan rezim pajak di Indonesia berupa *Tax Amnesty*

Sumber: Mardiansyah (2021)

Lembaga PPATK juga merangkum berbagai kasus ML atau TPPU yang ditindak pidana sejak tahun 2016 sampai dengan tahun 2020, baik yang dilakukan oleh perseorangan maupun oleh korporasi (Mardiansyah, 2021), beberapa di antaranya, yaitu:

1. Kasus Pencucian Uang Hasil Tindak Pidana Korupsi (Perseorangan)

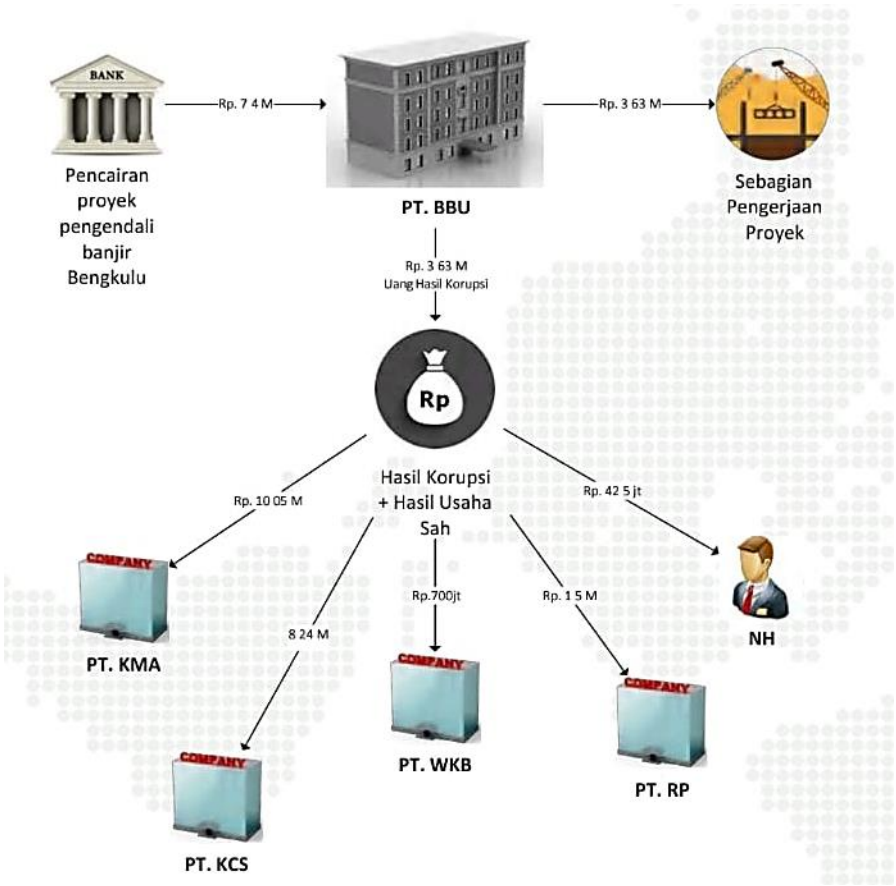
   Kasus terpidana atas nama ES yang merupakan Direktur Utama PT Garuda Indonesia (Persero) telah terbukti melakukan tindak pidana korupsi berupa suap atas pengadaan pesawat dan mesin pesawat di PT GI senilai Rp 49.3 Miliar dan tindak pidana pencucian uang senilai Rp 87.46 Miliar. Berikut skema kasus terpidana atas nama ES yang disajikan pada Gambar 2.5.

Gambar 2.5 Skema Kasus Terpidana Atas Nama ES

Sumber: Mardiansyah (2021)

2. Kasus Pencucian Uang Hasil Tindak Pidana Korupsi (Korporasi)

   Terdakwa PT BBU ditetapkan sebagai penyedia barang dan atau jasa untuk Pekerjaan Pengendali Banjir Air Bengkulu Kota Bengkulu Tahun Anggaran 2014. Atas pekerjaan tersebut, PT BBU telah memperkaya diri selaku korporasi dan merugikan keuangan negara sejumlah Rp 3,750,170,883.36. Berikut skema kasus yang melibatkan PT BBU selaku korporasi yang disajikan pada Gambar 2.6.

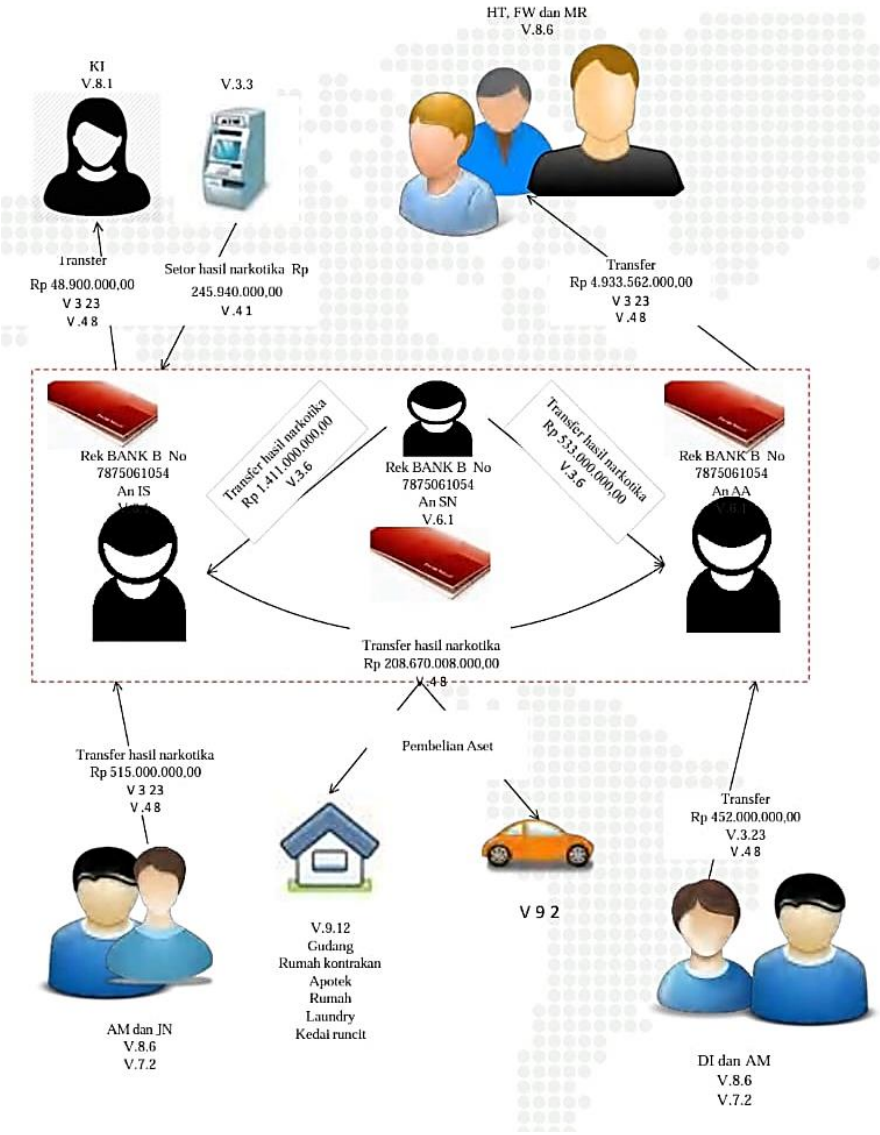


Gambar 2.6 Skema Kasus Terpidana Atas Nama PT BBU selaku Korporasi

Sumber: Mardiansyah (2021)

3. Kasus Pencucian Uang Hasil Tindak Pidana Narkotika

   Kasus terpidana atas nama AA sebagai sindikat narkotika jaringan internasional asal Malaysia yang masuk ke Negara Indonesia melalui Provinsi Nanggroe Aceh Darussalam untuk melakukan peredaran narkotika jenis shabu seberat 30 Kg di Medan. Berikut skema kasus terpidana atas nama AA yang disajikan melalui Gambar 2.7.

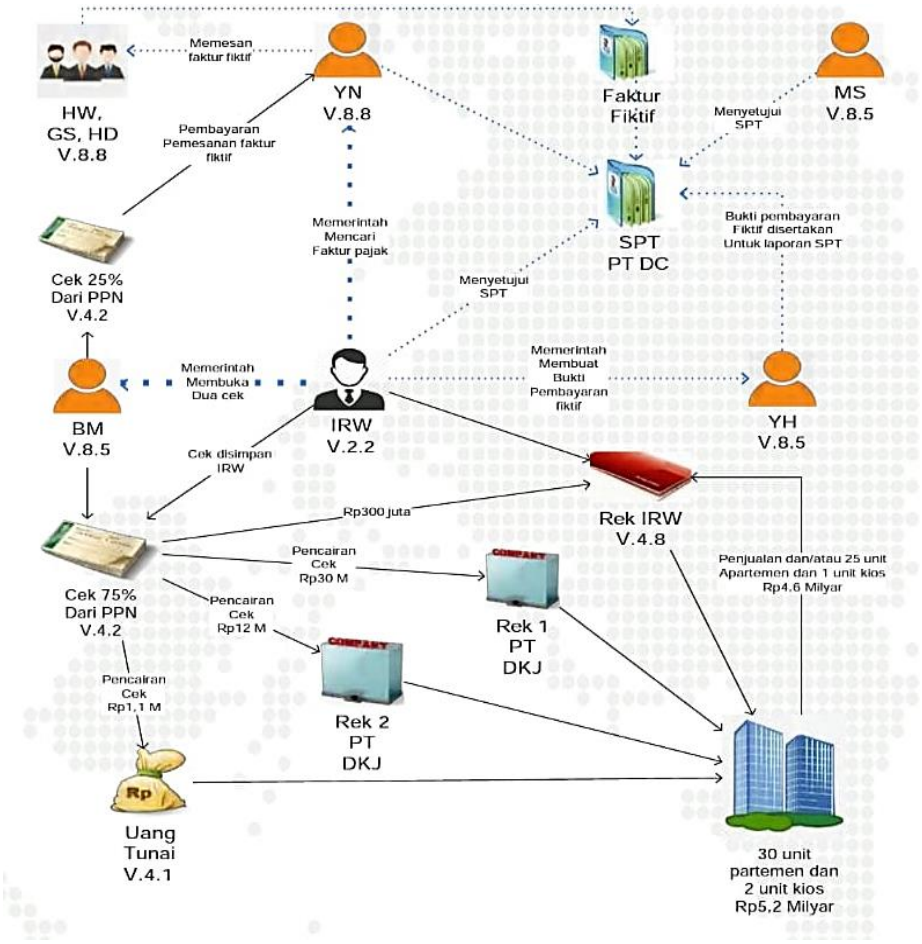


Gambar 2.7 Skema Kasus Terpidana Atas Nama AA

Sumber: Mardiansyah (2021)

4. Kasus Pencucian Uang Hasil Tindak Pidana Pajak

Terpidana kasus atas nama IRW selaku Direktur Keuangan dan Operasional PT DC (penyedia jasa konstruksi dan sebagai sub kontraktor) telah melakukan pembelian dan penggunaan faktur pajak yang tidak sesuai dengan transaksi sebenarnya. Terdakwa IRW terbukti merugikan pendapatan negara sebesar Rp 10,254,308,910. Berikut skema kasus pencucian uang terpidana atas nama IRW yang disajikan pada Gambar 2.8.



Gambar 2.8 Skema Kasus Terpidana Atas Nama IRW

Sumber: Mardiansyah (2021)

Selain itu, lembaga PPATK juga merangkum secara khusus TPPU yang menggunakan *virtual currency* atau *cryptocurrencies* sebagai *emerging threat* TPPU di Indonesia. Berdasarkan hasil analisis pada Penilaian Risiko Nasional 2021, penggunaan mata uang virtual dalam TPPU yang sudah diidentifikasi adalah sebagai berikut (Mardiansyah, 2021):

1. Praktik Jual Beli dan Penggunaan Akun Rekening atas nama Orang Lain

   Aktivitas ini dilakukan oleh sindikat yang bekerja untuk mencari akun orang lain dengan memanfaatkan *social engineering* dan *money mule network*. Kemudian akun rekening dijual kembali kepada para pelaku tindak pidana yang membutuhkan. Penjualan akun rekening tersebut dilakukan secara swa-mandiri dengan motif ekonomi.

2. Penyalahgunaan *E-Commerce* dalam Transaksi Hasil Kejahatan

   Penyalahgunaan ini dilakukan oleh para pelaku karena *platform e-commerce* memiliki kerterbatasan dalam proses identifikasi pihak *originator name* (pemiliki akun *platform e-commerce*). Dalam aktivitas TPPU, *e-commerce* digunakan sebagai media suap *(bribery)* melalui pembelian barang bernilai tinggi *(high end)* dan pembelian barang atau jasa (*travel* atau penginapan) dengan nilai besar kepada suatu *merchant* yang bertujuan untuk perpindahan dana, namun tidak ada pengiriman barang.

3. Praktik Teknologi Finansial *Peer to Peer Lending* Tidak Berizin

   Praktik yang tidak berizin menyulitkan otoritas berwenang untuk melakukan identifikasi dan penelusuran transaksi pinjam meminjam sehingga meningkatkan potensi TPPU melalui teknologi finansial jenis ini.

2.2 Pencegahan *Money Laundering*

Pencegahan ML menjadi permasalahan internasional yang utama karena upaya internasional untuk memberantas ML seringkali berbenturan dengan adanya tindak kejahatan yang terorganisir serta perbedaan dinamika kejahatan dan yurisdiksi dari masing-masing negara (Bin Belaisha & Brooks, 2014). Tantangan tersebut semakin sulit dengan berkembangnya teknik terbaru dari ML (Mugarura & Ssali, 2020) yang melibatkan *virtual currencies* atau *cyrptocurrencies* (Wronka, 2022a; Wronka, 2022b; Mardiansyah, 2021). Kegagalan dari pencegahan ML dapat memberikan *catastrophic concequences* bagi para korban (Truby, 2016). Oleh karena itu, berbagai bentuk eksploitasi terhadap produk, jasa dan atau teknologi baru untuk tujuan ML harus segera dicegah (Akartuna *et al*., 2022; Gilmour, 2016).

2.2.1 *Regulatory Technology*

Regulatory Technology (RegTech) merupakan teknologi informasi yang dapat membantu organisasi dalam memenuhi kepatuhan terhadap persyaratan hukum dengan menggabungkan regulator perdagangan, pajak dan keuangan melalui solusi yang andal *(reliable)*, aman *(safe)* dan ekonomis *(economical)* (Zabelina *et al*., 2018) untuk meningkatkan efisiensi dan efektivitas kinerja organisasi (Anagnostopoulos, 2018). Secara khusus, RegTech digunakan oleh organisasi untuk mencegah ML yang melibatkan penggunaan mata uang virtual karena RegTech meningkatkan kemampuan institusi dan regulator dalam melawan kejahatan keuangan (Kurum, 2020) dengan mengoptimalkan pemetaan

risiko serta melakukan investigasi pada sistem keuangan melalui analisis data dan pertukaran informasi (Zabelina *et al*., 2018).

RegTech berkembang dengan cepat yang terbagi ke dalam tiga fase (KPMG, 2018), yaitu: (1) RegTech 1.0 yang dimulai pada tahun 1990-an sampai dengan 2000-an sebelum krisis global pada tahun 2008 dan berfokus pada *risk assessment*; (2) RegTech 2.0 dimulai pada tahun 2010-an dengan berfokus pada *know your customer* (KYC) untuk kepatuhan AML; dan (3) RegTech 3.0 dimulai pada tahun 2018-an dan berfokus pada *know your data* (KYD) dalam *financial crime compliance* (FCC).

Proses analisis data dan pertukaran informasi yang cepat dan akurat pada RegTech dapat dilakukan karena RegTech menggunakan teknologi *big data* dan *cloud* dalam mengumpulkan serta menyimpan data-data tidak terstruktur dengan jumlah yang besar. RegTech juga membantu organisasi dalam melakukan otomatisasi pelaporan serta deteksi dari adanya transaksi mencurigakan *(suspicious tranasaction)* (Zabelina *et al*., 2018). Pemanfaatan RegTech membantu organisasi dalam melaksanakan upaya pencegahan ML dan atau *crypto laundering* sebagaimana yang disajikan pada Tabel 2.3.

Tabel 2.3 Peran RegTech dalam Pencegahan *Money Laundering*

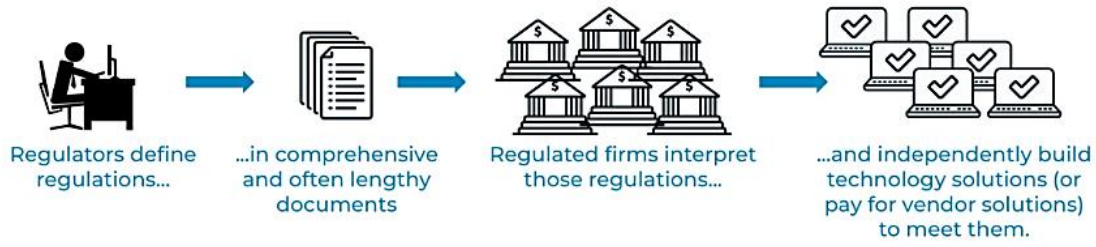
Pencegahan *Money Laundering*	**Tujuan**	**Peran RegTech**	**Referensi**
Risk Assessment	Mengidentifikasi dan meningkatkan pemahaman mengenai risiko ML pada organisasi	Digitalisasi sistem pengawasan untuk memetakan potensi risiko	Juntunen & Teittinen (2022); (Zabelina *et al.*, 2018)

Tabel 2.3 Peran RegTech dalam Pencegahan *Money Laundering* (Lanjutan)

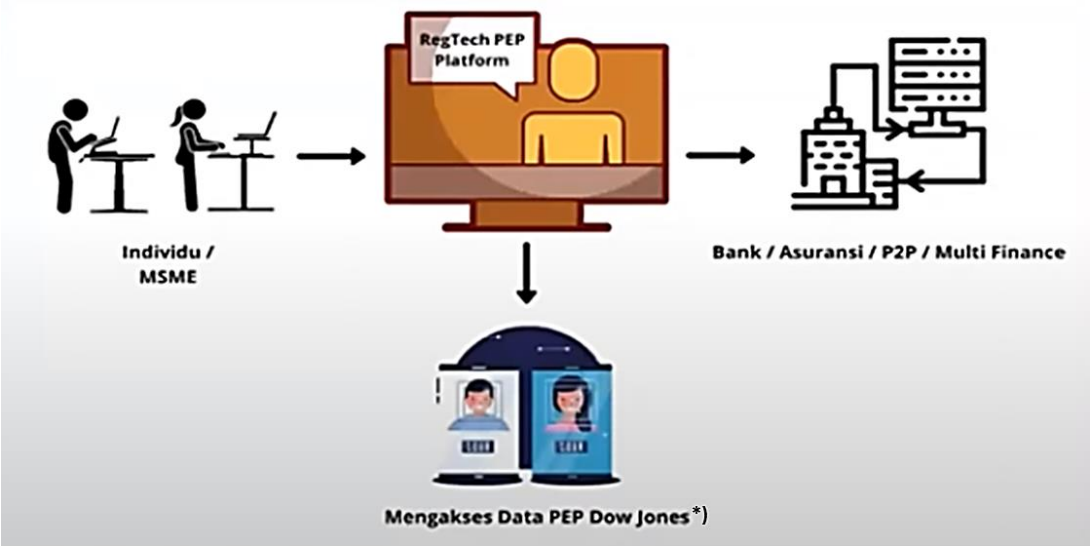
Pencegahan *Money Laundering*	Tujuan	Peran RegTech	Referensi
Electronic Know Your Customer (eKYC)	Memeroleh informasi mengenai *customer* sebelum melakukan kerjasama	Digitalisasi pengumpulan informasi untuk meningkatkan akurasi dan reliabilitas dari informasi yang diperoleh	Juntunen & Teittinen (2022); Meiryani *et al.* (2022)
Transaction Monitoring	Mengawasi setiap transakasi yang dilakukan oleh *customer*	Identifikasi dan prediksi transaksi keuangan mencurigakan *(suspicious transaction)*	Akartuna *et al.* (2022); Meiryani *et al.* (2022)
Cost and Time Efficiencies	-	Mengakselarasi proses dan menurunkan biaya pencegahan ML	Meiryani *et al.* (2022)

Sumber: Peneliti, Diolah

Skema pengembangan RegTech berdasarkan regulasi yang disusun oleh regulator disajikan melalui Gambar 2.9. Adapun salah satu skema penerapan RegTech, yaitu proses eKYC disajikan melalui Gambar 2.10.



Gambar 2.9 Skema Pengembangan RegTech
Sumber: FINOS (2020)



Gambar 2.10 Skema Penerapan RegTech (eKYC)
Sumber: Otoritas Jasa Keuangan (2022)

2.2.2 *Financial Intelligence*

ML menjadi risiko sistemik *(systematic risk)* terhadap keuangan dan ekonomi internasional sehingga penggunaan RegTech perlu dilengkapi dengan *financial monitoring* untuk mencegah terjadinya ML dan atau *cyber-laundering* (Reznik *et al.*, 2021). *Financial monitoring* harus dipertimbangkan sebagai bagian integral dari *financial control* dalam aspek ekonomi suatu negara. Bentuk khusus dari pendekatan *financial control* adalah melalui penerapan *financial intelligence* (Reznik *et al*., 2021) dengan ruang lingkup yang disajikan pada Tabel 2.4.

*) *Dow Jones: Global Sanction List, Global Politically Exposed Person, Relative & Close Associate, Special Interest Person (Financial Crime)*

Tabel 2.4 Ruang Lingkup *Financial Intelligence*

Controller	***Controlled***	***Controlled Object***	***Purpose***
Lembaga dengan fungsi *financial control* yang ditunjuk negara	Semua jenis entitas bisnis, institusi, organisasi dan individu	Legalitas, penggunaan, keandalan dan efisiensi ekonomi dari aktivitas keuangan	Mencegah transaksi yang mungkin berkaitan dengan aktivitas ML

Sumber: Reznik et al., Diolah (2021)

Penerapan *financial intelligence* dilakukan oleh lembaga *(controller)* yang ditunjuk atau dibentuk oleh negara. Penyebutan dan penamaan lembaga tersebut dapat berbeda dari setiap negara, namun secara umum disebut sebagai *Financial Intelligence Unit* (FIU) (Reznik *et al*., 2021) dan bertindak sebagai koordinator dalam AML di negara tersebut (Sultana, 2020; Naheem, 2018).

Fungsi utama atau fungsi internal dari FIU adalah mengumpulkan, menganalisis dan menyebarluaskan laporan atas entitas atau individu kepada lembaga berwenang (Reznik *et al*., 2021) yang berkaitan dengan adanya aktivitas keuangan mencurigakan (Sultana, 2020) berdasarkan indikator atau regulasi yang berlaku (Williams, 2014). Sedangkan fungsi eksternal dimana FIU bekerjasama dengan berbagai FIU dari negara lain memberikan efektivitas terhadap pencegahan ML pada tingkat internasional (Williams, 2014). FIU berperan dalam melakukan pertukaran informasi *(information exchange)* dari FIU satu negara dengan FIU negara lain *(FIU-to-FIU)* melalui penerapan *opened database* berdasarkan perjanjian bilateral dan atau multilateral dari masing-masing negara yang melakukan pertukaran informasi *FIU-to-FIU* (FATF, 2003).

2.3 *Anti-Money Laundering*

Dampak negatif dari ML terhadap stabilitas keuangan global mendorong FATF untuk memperkenalkan AML/CFT *(Anti-Money Laundering/Counter-Financing of Terrorism) Framework* dalam rangka memerangi tindak pidana pencucian uang (Zolkaflil *et al*., 2019). FATF memiliki peranan penting dalam mengembangkan aturan dan rekomendasi yang diperlukan oleh lembaga keuangan dalam menghadapi ML (Alexander, 2001). Topik yang disarankan oleh FATF diwujudkan dalam "*The FATF Recommendations"* yang berisi 40 rekomendasi (FATF, 2003). Rekomendasi tersebut mengalami beberapa perubahan pada tahun 2012 untuk memperkuat sistem AML/CFT dalam menghadapi tingginya risiko ML/TF (FATF, 2022) sehingga 40 topik yang direkomendasikan oleh FATF disajikan melalui Tabel 2.5.

Tabel 2.5 *The FATF Recommendations*

No.	FATF Recommendation	Measurement
1	Assesing risks and applying risk-based approach	AML/CFT Policies and Coordination
2	National cooperation and coordination	
3	Money laundering offence	Money Laundering and Confiscation
4	Confiscationand provisional measures	
5	Terrorist financing offence	Terrorist Financing and Financing of Proliferation
6	Tergeted financial sanctions related to terrorism and terrorist financing	
7	Tergeted financial sanctions related to proliferation	
8	Non-profit organisations	

Tabel 2.5 *The FATF Recommendations* (Lanjutan)

No.	FATF Recommendation	Measurement
9	Financial institution secrecy laws	Preventive Measures
10	Customer due dilligence	
11	Record keeping	
12	Politicaly exposed persons	
13	Correspondent banking	
14	Money or value transfer services	
15	New technologies	
16	Wire transfers	
17	Reliance on third parties	
18	Internal controls and foreign branches and subsidiaries	
19	Higher-risk countries	
20	Reporting of suspicious transaction	
21	Tipping-off and confidentially	
22	Customer due dilligence (non-financial business and professions)	
23	Other measures (non-financial business and professions)	
24	Transparency and beneficial ownership of legal persons	Transparency and Beneficial Ownership of Legal Persons and Arrangements
25	Transparency and beneficial ownership of legal arrangements	
26	Regulation and supervision of financial institutions	Powers and Responsibilities of Competent Authorities and Other Institutional Measures
27	Powers of supervisors	
28	Regulation and supervision (non-financial business and professions)	
29	Financial intelligence unit	
30	Responsibilities of law enforcement and investigative authorities	
31	Powers of law enforcement and investigative authorities	
32	Cash couriers	

Tabel 2.5 *The FATF Recommendations* (Lanjutan)

No.	FATF Recommendation	Measurement
33	Statistics	Powers and Responsibilities of Competent Authorities and Other Institutional Measures
34	Guidance and feedback	
35	Sanctions	
36	International instruments	International Cooperation
37	Mutual legal asisstance	
38	Mutual legal asisstance: freezing and confiscation	
39	Extradition	
40	Other forms of international cooperation	

Sumber: FATF, 2022

2.3.1 *Anti-Money Laundering* untuk *Cryptocurrency*

Secara khusus, FATF merekomendasikan penerapan AML untuk *virtual asset* atau *crypto asset* melalui *FATF Recommendations* nomor 15, yaitu *new technologies*. Berdasarkan rekomendasi ini, *virtual asset* meliputi properti *(property),* keuntungan atau pendapatan *(proceeds),* dana *(funds),* aset lain *(other assets)* dan hal-hal lain yang memiliki keterkaitan dengan *virtual asset (corresponding value)* (FATF, 2022). Selanjutnya, FATF (2022) merekomendasikan kepada masing-masing negara untuk menyesuaikan sistem AML untuk *virtual asset* berdasarkan rekomendasi-rekomendasi yang telah disusun oleh FATF dengan penjelasan sebagai berikut (FATF, 2022):

1. Berdasarkan rekomendasi nomor 1 *(applying risk-based approach)* maka setiap negara harus mengidentifikasi, menilai dan memahami risiko ML dari aktivitas aset virtual dan penyedian layanan aset virtual *(virtual asset service provider/VASP)* dengan menerapkan pendekatan berbasis risiko *(risk-based approach)* untuk mencegah ML yang melibatkan aset virtual;

2. VASP harus terlisensi atau terdaftar pada otoritas yang berwenang berdasarkan yurisdiksi dimana VASP bertempat atau menjalankan aktivitas bisnisnya serta diawasi dan dipantau oleh otoritas berwenang;
3. VASP harus patuh dan menerapkan rekomendasi FATF dan sistem AML nasional yang relevan untuk mencegah atau memitigasi risiko ML;
4. Pengawasan kepatuhan terhadap sistem AML nasional dilakukan oleh otoritas setempat yang berwenang;
5. Melakukan *preventive measures* berdasarkan rekomendasi nomor 10 sampai dengan nomor 21 dengan *threshold* USD/EUR 1,000;
6. Menetapkan sanksi sebagaimana rekomendasi nomor 35;
7. Bergerak secara cepat, konstruktif dan efektif dalam kerjasama internasional yang berkaitan dengan pencucian uang, tindak pidana asal *(predicate crime)* dan pembiayaan yang berkaitan dengan aset virtual berdasarkan rekomendasi nomor 37 sampai dengan nomor 40.

Adapun rincian secara umum dari *FATF Recommendations* yang diterapkan untuk *virtual asset* disajikan pada Tabel 2.6.

Tabel 2.6 *The FATF Recommendations for Virtual Asset*

No.	FATF Recommendation	Measurement
1	Assesing risks and applying risk-based approach	AML/CFT Policies and Coordination
2	National cooperation and coordination	
10	Customer due dilligence	Preventive Measures
11	Record keeping	
12	Politicaly exposed persons	
13	Correspondent banking	
14	Money or value transfer services	

Tabel 2.6 ***The FATF Recommendations for Virtual Asset*** **(Lanjutan)**

No.	FATF Recommendation	Measurement
15	New technologies	Preventive Measures
16	Wire transfers	
17	Reliance on third parties	
18	Internal controls and foreign branches and subsidiaries	
19	Higher-risk countries	
20	Reporting of suspicious transaction	
21	Tipping-off and confidentially	
24	Transparency and beneficial ownership of legal persons	Transparency and Beneficial Ownership of Legal Persons and Arrangements
25	Transparency and beneficial ownership of legal arrangements	
26	Regulation and supervision of financial institutions	Powers and Responsibilities of Competent Authorities and Other Institutional Measures
27	Powers of supervisors	
28	Regulation and supervision (non-financial business and professions)	
29	Financial intelligence unit	
30	Responsibilities of law enforcement and investigative authorities	
31	Powers of law enforcement and investigative authorities	
33	Statistics	
34	Guidance and feedback	
35	Sanctions	
37	Mutual legal asisstance	International Cooperation
38	Mutual legal asisstance: freezing and confiscation	
39	Extradition	
40	Other forms of international cooperation	

Sumber: FATF (2022)

2.3.2 *Anti-Money Laundering* di Indonesia

Menindaklanjuti rekomendasi FATF nomor 1 yang dikeluarkan pada tahun 2003 *(money laundering offence)*, Indonesia melalui Komite TPPU (Tindak Pidana Pencucian Uang) yang dibentuk pada tahun 2004 menyusun Strategi Nasional Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (STRANAS TPPU) dengan tujuan untuk memitigasi risiko dalam melaksanakan pencegahan dan pemberantasan TPPU di Indonesia karena dalam penerapannya belum sepenuhnya diimbangi dengan langkah yang seragam antar para pemangku kepentingan (Mardiansyah, 2021). STRANAS telah disusun selama empat periode berkelanjutan sebagaimana yang disajikan pada Tabel 2.7.

Tabel 2.7 Strategi Nasional Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang

Langkah Strategis	STRANAS 2007-2011	STRANAS 2012-2016	STRANAS 2017-2019	STRANAS 2020-2024
Strategi I	Pembuatan *single identity number* bagi semua WNI untuk memudahkan pencegahan dan pemberantasan tindak pidana	Penerapan dan pengawasan penggunaan NIK	Menurunkan tingkat pidana narkotika, korupsi dan tindak pidana perpajakan melalui optimalisasi penegakan hukum TPPU	Meningkatkan kemampuan sektor privat dalam mendeteksi indikasi dan atau potensi TPPU, TPPT serta pendanaan proliferasi senjata pemusnah massal
Strategi II	Pengundangan RUU Pencegahan dan Pemberantasan TPPU secepatnya agar Indonesia memiliki UU APU yang lebih komprehensif dan efektif untuk mencegah dan memberantas TPPU yang sesuai dengan standar internasional	Implementasi UU PP TPPU dengan percepatan penyelesaian peraturan pelaksananya	Mewujudkan mitigasi risiko yang efektif dalam mencegah terjadinya TPPU dan pendanaan terorisme di Indonesia	Meningkatkan upaya pencegahan terjadinya TPPU, TPPT serta pendanaan proliferasi senjata pemusnah massal dengan penerapan pendekatan berbasis risiko
Strategi III	Pengelolaan *database* secara elektronis dan ketersambungan *(connectivity)* antar instansi terkait agar kebutuhan informasi setiap instansi terkait dapat terpenuhi secepatnya	Pengelolaan *database* secara elektronis dan ketersambungan *database* yang dimiliki oleh beberapa instansi terkait	Optimalisasi upaya pencegahan dan pemberantasan tindak pidana pendanaan terorisme	Meningkatkan upaya pemberantasan terjadinya TPPU, TPPT serta pendanaan proliferasi senjata pemusnah massal dengan penerapan pendekatan berbasis risiko

Tabel 2.7 Strategi Nasional Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (Lanjutan)

Langkah Strategis	STRANAS 2007-2011	STRANAS 2012-2016	STRANAS 2017-2019	STRANAS 2020-2024
Strategi IV	Peningkatan pengawasan kepatuhan PJK agar PJK memiliki kesadaran yang lebih tinggi untuk memenuhi kewajibannya sebagai pihak pelapor	Peningkatan pengawasan kepatuhan Penyedia Jasa Keuangan (PJK)	Menguatkan koordinasi dan kerjasama antar instansi pemerintah dan atau lembaga swasta	Mengoptimalisasi *asset recovery* dengan pendekatan berbasis risiko
Strategi V	Mengefektifkan penerapan *asset tracing and recovery* agar harta kekayaan hasil kejahatan yang kembai ke negara lebih maksimal dan sekaligus dapat memberikan kontribusi yang signifikan bagi pembangunan perekonomian nasional	Percepatan penyusunan peraturan pelaksana dan persiapan implementasi kewajiban pelaporan bagi PJK	Meningkatkan pemanfaatn instrument kerjasama internasional dalam rangka optimalisasi *asset recovery* yang berada di negara lain	Meningkatkan efektivitas *targeted financial sanction* dalam rangka mendisrupsi aktivitas terorisme, teroris, organisasi teroris dan aktivitas pendanaan proliferasi senjata pemusnah massal
Strategi VI	Peningkatan peran serta masyarakat melalui kampanye publik untuk mendukung rezim anti-pencucian uang di Indonesia	Pengefektifan penerapan penyitaan aset *(asset forfeiture)* dan pengembalian aset *(aset recovery)*	Meningkatkan kedudukan dan posisi Indonesia di forum internasional di bidang pencegahan dan pemberantasan TPPU dan PT	-

Tabel 2.7 Strategi Nasional Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (Lanjutan)

Langkah Strategis	STRANAS 2007-2011	STRANAS 2012-2016	STRANAS 2017-2019	STRANAS 2020-2024
Strategi VII	Percepatan ratifikasi UN *Convention* dan *Regional Convention/Treaty* karena konvensi-konvensi tersebut sangat mendukung dan mendukung penanganan TPPU	Pengungkapan kasus-kasus terkait dengan TPPU dan kejahatan terorganisir	Penguatan regulasi dan peningkatan pengawasan pembawaan uang tunai dan *Bearer Negotiable Instrument* (BNI) lintas batas negara sebagai media PT	-
Strategi VIII	Penguatan peraturan tentang *Alternative Remittance System* dan *Wire Transfer*	Peningkatan peran serta masyarakat melalui kampanye publik	-	-
Strategi IX	-	Peningkatan kerjasama internasional	-	-
Strategi X	-	Percepatan penyelesaian RUU Pendanaan Terorisme dan penyusunan peraturan pelaksanaannya	-	-

Tabel 2.7 Strategi Nasional Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (Lanjutan)

Langkah Strategis	STRANAS 2007-2011	STRANAS 2012-2016	STRANAS 2017-2019	STRANAS 2020-2024
Strategi XI	-	Penanganan sektor remitansi secara komprehensif (implementasi UU Transfer Dana)	-	-
Strategi XII	-	Penanganan sektor *non-profit organization* secara komprehensif	-	-

Sumber: Mardiansyah (2021)

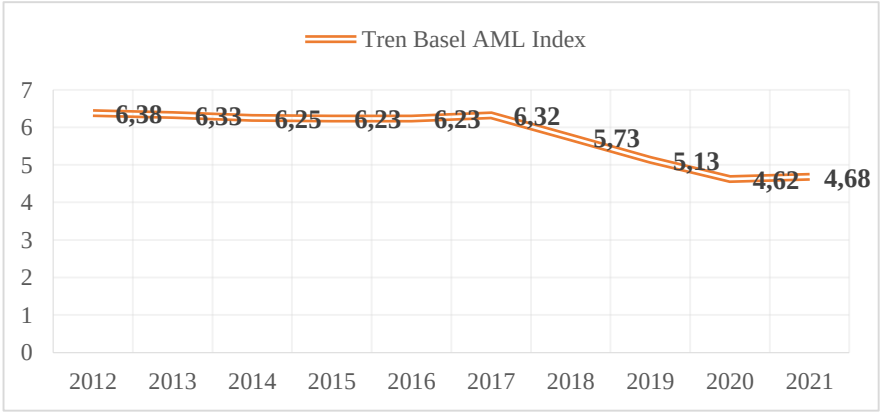
Sebagai bentuk implementasi untuk mencapai keberhasilan STRANAS tersebut maka Pemerintah Indonesia melalui PPATK dan para pemangku kepentingan—seperti: regulator, lembaga pengawas dan pengatur, lembaga penegak hukum, pihak swasta atau pihak pelapor serta asosiasi, ahli dan akademisi serta mitra strategis di luar negeri—melakukan pemutakhiran penilaian risiko nasional *(National Risk Assessment*/NRA*)* terhadap TPPU melalui proses identifikasi, analisis dan evaluasi risiko yang bertujuan untuk memberikan evaluasi terhadap kecenderungan dan dampak terhadap risiko yang dimiliki dalam menentukan prioritas penanganan risiko, langkah strategis mitigasi untuk mereduksi risiko yang dimiliki serta pengalokasian sumber daya yang efektif (Mardiansyah, 2021).

Pada skala regional, Indonesia tergabung dalam *Asia/Pasific Group on Money Laundering* (APGML)—yang merupakan representatif dari FATF—dimana para anggota dalam APGML berkomitmen untuk mengimplementasikan AML secara efektif di negaranya masing-masing. APGML telah melakukan penilaian terkait implementasi AML/CFT di Indonesia pada tahun 2008 dan 2018. APGML menilai berdasarkan analisa kepatuhan terhadap 40 rekomendasi dari FATF dan efektivitas implementasi dari sistem AML/CFT (APGML, 2018). Menurut APGML (2018), STRANAS Indonesia telah menggabungkan berbagai aksi untuk memperkuat sistem AML/CFT melalui penilaian risiko sektoral, keputusan dan kebijakan mengenai alokasi anggaran, waktu dan sumber daya serta pelaporan daring terintegrasi melalui Sistem Informasi Pelaporan dan Pemantauan STRANAS TPPU (SIPPENAS).

Adapun pada skala internasional, penilaian risiko ML diwujudkan oleh *Basel Institute on Governance* melalui *Basel AML Index* yang dilakukan setiap tahun sejak tahun 2012. *Basel AML Index* mencerminkan risiko keseluruhan atas paparan ML/TF dari suatu negara. Penilaian risiko tersebut bersumber pada data dari FATF, *Transparency International*, *World Bank* dan *World Economic Forum* yang didasarkan pada lima hal penilaian (Basel Institute on Governance, 2020), yaitu:

1. *Quality of ML/TF Framework* (Kualitas Kerangka Kerja APU/PPT);
2. *Bribery and Corruption* (Penyuapan dan Korupsi);
3. *Financial Transparency Standards* (Transparansi dan Standar Keuangan);
4. *Public Transparency and Accountability* (Transparansi dan Akuntabilitas Publik);
5. *Legal and Political Risks* (Risiko Hukum dan Politik).

Tren risiko ML/TF di Indonesia dari tahun 2012 sampai dengan tahun 2021 (Basel Institue of Governance, 2021; 2020; 2019; 2018; 2017; 2016; 2015; 2014; 2013) berdasarkan *Basel AML Index* ditunjukkan melalui Gambar 2.11.



Gambar 2.11 Indeks Indonesia Berdasarkan *Basel AML Index*

Sumber: Basel Institute of Governance (2013-2021)

Adapun sistem AML untuk *cryptocurrencies* di Indonesia diatur dan ditetapkan oleh Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) yang memiliki tugas pokok untuk melakukan pembinaan, pengaturan, pengembangan, dan pengawasan terhadap perdagangan berjangka (Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 11 Lampiran: Pedoman Penerapam Program Anti Pencucian Uang Dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka, 2017). Bappebti menetapkan bahwa penerapan program AML untuk *cryptocurrencies* harus dilaksanakan berdasarkan pendekatan berbasis risiko *(risk-based approach)* sebagaimana rekomendasi FATF nomor 1, yaitu *assesing risks and applying risk-based approach*. Pendekatan berbasis risiko ini menjadi dasar untuk melaksanakan sistem AML selanjutnya, seperti: *know your customer* melalui *customer due diligence* dan atau *enhanced due diligence*, *transaction monitoring* melalui *record keeping*, dan pelaporan atas transaksi mencurigakan kepada Bappebti dan PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan).

Penerapan sistem AML harus dilaksanakan secara cepat dan akurat sehingga Bappebti menetapkan bahwa setiap aktivitas AML dalam ekosistem perdagangan *crypto aset* harus diselenggarakan dengan berbasis *regulatory technology* (RegTech) melalui pengaplikasian *face recognition* yang terintegrasi dengan data *biometric* untuk aktivitas *know your customer* dan *blockchain analytic tools* untuk aktivitas *transaction monitoring*. Penetapan penggunaan teknologi ini dilaksanakan oleh Bappebti sebagaimana rekomendasi FATF nomor 15 *(new technologies)* dalam mencegah aktivitas ML yang melibatkan mata uang virtual.

2.4 Evaluasi Pemanfaatan Teknologi dalam Sistem *Anti-Money Laundering*

Money laundering memberikan tantangan unik bagi pemerintah dan aparat penegak hukum karena para pelaku ML terus berupaya dan beradaptasi dengan sistem AML. Para pelaku ML mengubah berbagai tindakan mereka dalam menyamarkan hasil dari tindak pidana yang dilakukan untuk mempersulit pendeteksian (Gilmour, 2022). Pencegahan ML semakin rumit dengan adanya peningkatan globalisasi masyarakat (Gilmour, 2022), kurangnya landasan dan kepastian hukum (Meiryani & Warganegara, 2022) serta berkembangnya berbagai jenis teknologi baru (Wronka, 2022b; Anagnostopoulos, 2018) yang tidak diimbangi dengan perkembangan sistem AML (Turner, 2011).

Pemanfaatan teknologi melalui RegTech secara relatif dapat membantu regulasi, pengawasan, dan kepatuhan dalam sistem AML atau pencegahan ML (McCarthy, 2022). Namun, ditemukan bahwa sebanyak 29% RegTech tidak secara eksplisit membantu dan mendukung kepatuhan terhadap regulasi sehingga berimplikasi pada adopsi pemanfaatan RegTech di masa mendatang (Freij, 2020). Selain itu, evolusi peraturan juga sangat mungkin terjadi di masa mendatang yang akan berpengaruh pada pemanfaatan RegTech (Freij, 2020). Jika adopsi pemanfaatan RegTech saat ini masih belum optimal maka sangat dimungkinkan adanya peningkatkan biaya dan keterbatasan manfaat dari RegTech di masa mendatang (Freij, 2020).

Oleh karena itu, perlunya analisis terhadap pemanfaatan teknologi (RegTech) dalam mekanisme AML untuk mengoptimalkan penggunaan RegTech yang berperan dalam efisiensi implementasi sistem AML. Efisiensi dari

implementasi sistem AML bergantung dengan desain yang tepat dan *personal willingness* dari masing-masing individu dan atau regulator (Azevedo Araujo, 2010) sehingga ketepatan regulasi dan pemangku kepentingan yang berperan dalam implementasi pemanfaatan RegTech menjadi bagian penting dari evaluasi pemanfaatan RegTech (Sarabdeen, 2023).

2.5 Penelitian Terdahulu

Telaah pustaka yang disajikan pada tabel 2.8 memberikan wawasan awal mengenai *money laundering* dan *anti-money laundering* di berbagai negara dengan sub-topik sebagai berikut:

1. Implementasi AML (Juntunen & Teittinen, 2022; Naheem, 2020);
2. Efektivitas AML (Pontes *et al*., 2022; Hassan *et al*., 2022);
3. Kepatuhan AML (Viritha *et al*., 2015);
4. Pencegahan ML (Lukito, 2016; Meiryani & Warganegara, 2022; Truby, 2016; Bin Belaisha & Brooks, 2014);
5. Pencegahan ML melalui pemanfaatan RegTech atau teknologi terbaru (Meiryani *et al*., 2022; Utami & Septivani, 2022a; Pettersson Ruiz & Angelis, 2021);
6. Pengembangan *AML Framework* (Salehi & Imeny, 2019; Thompson, 2018);
7. *Cryptocurrency* sebagai sarana ML (Wronka, 2022c);
8. AML untuk *cryptocurrency* (Al-Tawil, 2022).

Sebagian besar penelitian terdahulu berfokus pada ruang lingkup dimana sistem AML diimplementasikan, baik dari aspek keberhasilan (efektivitas) maupun aspek kepatuhan. Namun, penelitian yang berfokus pada ML dengan

media terkini melalui *cryptocurrency*, pemanfaatan RegTech atau terknologi terbaru untuk mencegah *crypto-laundering* serta evaluasi terhadap pemanfaatan RegTech dalam mencegah *crypto-laundering* masih terbatas.

Tabel 2.8 Telaah Pustaka yang Berkaitan dengan *Anti-Money Laundering*

No.	Penulis	Sub-Topik	Pendekatan	Variabel Independen	Variabel Dependen	Sampel	Hasil
1.	Meiryani *et al*., (2022)	Pencegahan ML melalui RegTech	Kuantitatif	• *Electronic Know Your Customer* (eKYC) • *Transaction Monitoring* ™ • *Cost & Time Effectiveness* (CT)	• *Customer Due Dilligence* • *Enhanced Due Dilligence* • *Suspicious Transaction Reporting* • *Targeted Financial Sanctions* • *Record-Keeping*	160 Staff Perbankan di Indonesia	• eKYC berpengaruh, tidak signifikan • TM berpengaruh, signifikan • CT berpengaruh, tidak signifikan
2.	Salehi & Imeny (2019)	Integrasi *AML Framework*	Kuantitatif-Deskriptif	• *Gender* • *Age* • *Educational Level* • *Work Experience* • *Level Familiarity with Iranian AML Rules & Regulations* • *Level Familiarity with FATF Recommendations* • *Level Familiarity with Wolfsberg Group Standars*	*AML Status*	24 Staff Anti-Pencucian Uang di Perbankan Iran	Jumlah dan pengalaman kerja staff perbankan berpengaruh positif terhadap kontrol AML

Tabel 2.8 Telaah Pustaka yang Berkaitan dengan *Anti-Money Laundering* (Lanjutan)

No.	Penulis	Sub-Topik	Pendekatan	Variabel Independen	Variabel Dependen	Sampel	Hasil
3.	Juntunen & Teittinen (2022)	Implementasi Akuntabilitas dalam AML	Kualitatif Studi Kasus	-	-	Perbankan di Finlandia	Penerapan akuntabilitas melalui pelaporan *suspicious transaction* antar-Bank memudahkan Bank untuk melaksanakan KYC dalam rangka mencegah ML
4.	Pontes *et al.*, (2022)	Efektivitas Rezim AML	Kualitatif dengan Wawancara Semi-Terstruktur	-	-	Praktisi Sektor Publik dan Privat di United Kingdom	• Peraturan dan pengawasan terkait ML dengan *risk-based approach* tidak efektif • Pihak berwenang memiliki keterbatasan dalam menghentikan pelaporan yang tidak sesuai dengan indikator
5.	Thompson (2018)	Pengembangan *AML Framework*	Kualitatif	-	-	Myanmar	Kurangnya keahlian teknis serta sumber daya keuangan dan manusia untuk memastikan kepatuhan dan penegakkan hukum sehingga risiko ML masih tinggi

Tabel 2.8 Telaah Pustaka yang Berkaitan dengan *Anti-Money Laundering* (Lanjutan)

No.	Penulis	Sub-Topik	Pendekatan	Variabel Independen	Variabel Dependen	Sampel	Hasil
6.	Viritha *et al*., (2015)	Kepatuhan AML	Kuantitatif	• *Bank's AML Policy* • *Customer Identification* • *Dealing with Wire Transfer* • *Reporting* • *KYC* • *Record Maintenance*	Regulasi AML	392 Staff Perbankan di India	Kapatuhan Bank terhadap regulasi AML tidak menunjukkan hasil yang signifikan
7.	Lukito (2016)	Pencegahan ML dengan *Financial Intelligence*	Kualitatif-Telaah Pustaka	-	-	Regulasi Pencegahan dan Pemberantasan TPPU di Indonesia	*Financial intelligence* menjadi hal yang penting dalam memberantas ML
8.	Meiryani & Warganegara (2022)	Pencegahan ML	Kualitatif-Telaah Pustaka	-	-	Legislasi dan Regulasi TPPU di Indonesia	Pencegahan ML melalui penilaian validitas suatu kepemilikan yang terdiri dari: • Status/pendaftaran resmi usaha • Pelaporan PPh dan PPN • Perizinan usaha

Tabel 2.8 Telaah Pustaka yang Berkaitan dengan *Anti-Money Laundering* (Lanjutan)

No.	Penulis	Sub-Topik	Pendekatan	Variabel Independen	Variabel Dependen	Sampel	Hasil
9.	Naheem (2020)	Implementasi AML	Kualitatif-Telaah Pustaka	-	-	Kuwait	Mekanisme 50egislative dan regulasi AML telah disusun berdasarkan rekomendasi dari FATF
10.	Bin Belaisha & Brooks (2014)	Pencegahan ML	Kualitatif dengan Wawancara Semi-Terstruktur	-	-	*Central Bank Staff* di Dubai	Lembaga berwenang menyadari bahwa strategi pencegahan ML di masa depan diperlukan
11.	Truby (2016)	Pencegahan ML	Kualitatif-Telaah Pustaka	-	-	Qatar	Kepatuhan AML terbukti secara berkelanjutan, namun masih jauh dengan rekomendasi dari FATF
12.	Hassan *et al*., (2022)	Efektivitas AML	Kualitatif dengan Wawancara Semi-Terstruktur	-	-	Bank Negara di Pakistan	Pembaruan UU yang ketat tidak disertai dengan efektivitas koordinasi antara lembaga berwenang dengan lembaga perbankan

Tabel 2.8 Telaah Pustaka yang Berkaitan dengan *Anti-Money Laundering* (Lanjutan)

No.	Penulis	Sub-Topik	Pendekatan	Variabel Independen	Variabel Dependen	Sampel	Hasil
13.	Al-Tawil (2022)	AML untuk *cryptocurrency*	Kualitatif-Telaah Pustaka	-	-	Uni Arab Emirates (UAE)	• Regulasi AML belum mengatur mengenai keuangan terdesentralisasi sehingga meningkatkan peluang terjadinya ML melalui *cryptocurrency* • Diperlukan regulasi yang responsif terhadap berbagai kemungkinan negatif dari *cryptocurrency*
14.	Wronka (2022c)	ML melalui *cryptocurrency*	Kualitatif Telaah Pustaka dan Wawancara Ahli	-	-	Uni Eropa	• *Crypto asset* memiliki risiko konkrit terhadap ML • Pencegahan ML melalui *crypto asset* masih dalam tahap diskusi
15.	Utami & Septivani (2022a)	Pencegahan ML melalui RegTech	Kuantitatif	• *Electronic Know Your Customer* (eKYC) • *Transaction Monitoring* (TM) • *Cost & Time Effectiveness* (CT)	*Money Laundering Prevention*	77 Staff Perbankan Konvensional di Indonesia	• eKYC tidak berpengaruh, • TM berpengaruh, signifikan • CT berpengaruh, signifikan

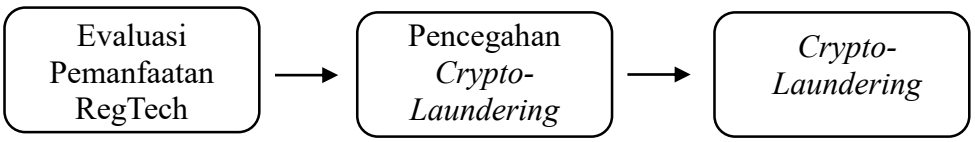
Tabel 2.8 Telaah Pustaka yang Berkaitan dengan *Anti-Money Laundering* (Lanjutan)

No.	Penulis	Sub-Topik	Pendekatan	Variabel Independen	Variabel Dependen	Sampel	Hasil
16.	Pettersson Ruiz & Angelis (2021)	Pencegahan ML melalui *cryptocurrency* dengan *machine learning*	Campuran (Kuantitatif dan Kualitatif-Wawancara)	Learning algorithms	• *F1-Score* • *Recall* • *Precision*	*Elliptic Bitcoin Data Set*	Implementasi *machine learning* dalam mencegah ML melalui pertukaran cryptocurrency masih terlalu lambat dan perlu dioptimalkan

Sumber: Peneliti, Diolah

2.5 Kerangka Pemikiran

Berdasarkan penjelasan yang telah dipaparkan maka kerangka pemikiran dalam penelitian ini digambarkan melalui diagram alir yang disajikan pada Gambar 2.12.



Gambar 2.12 Kerangka Pemikiran

Sumber: Peneliti (2023)

BAB III

METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Penelitian ini memiliki rumusan masalah yang diawali dengan kata tanya "bagaimana" dan "mengapa" sehingga penelitian ini memerlukan pendekatan kualitatif untuk menjawab rumusan masalah tersebut. Pendekatan kualitatif dapat membantu peneliti untuk menjawab pertanyaan yang kompleks, seperti: bagaimana dan mengapa implementasi dari suatu *best practices* dapat berhasil atau mengalami kegagalan (Hamilton & Finley, 2020).

Biasanya, penelitian kualitatif menggunakan pendekatan berupa wawancara terhadap individu dan *focus group*, observasi, etnografi dan beberapa pendekatan lainnya karena hal tersebut menjadi media dengan kredibilitas paling baik dalam memahami fenomena yang dipikirkan oleh sumber data (Hamilton & Finley, 2020) sehingga memudahkan peneliti dalam melakukan *reality reconstruction* (Khalid, 2009). Penelitian kualitatif sangat bergantung dengan *reality reconstruction* atau *social contrucrionism* dalam menjawab pertanyaan penelitian (Saunders *et al*., 2012).

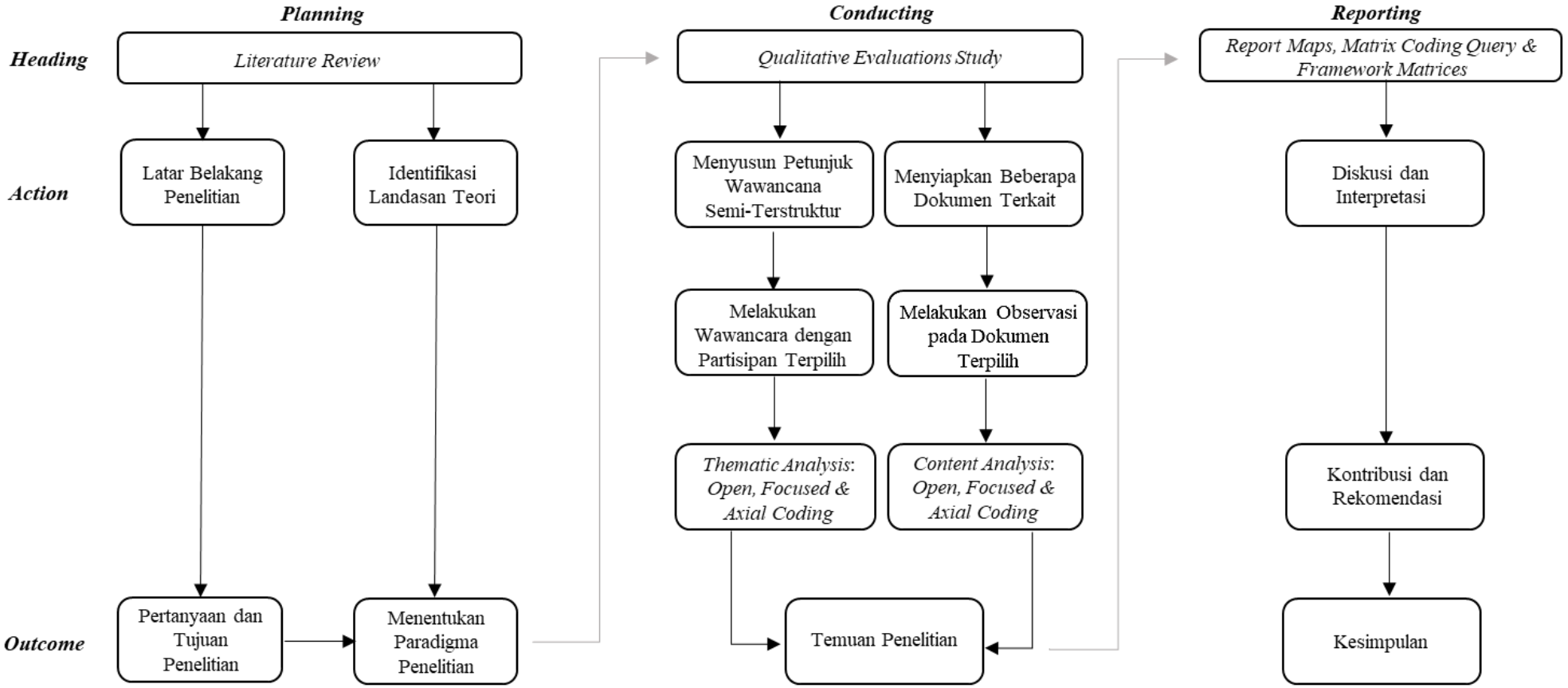
3.2 Instrumen Penelitian

Dalam penelitian kualitatif, peneliti menjadi instrumen penelitian (Patton, 2003) dimana semua proses penelitian dimediasi dan diinterpretasikan oleh peneliti (Khalid, 2009) sehingga kredibilias, validitas dan signifikansi dari penelitian bergantung dengan kemampuan peneliti (Patton, 2003).

Peneliti sebagai *human instrument* bukanlah pengamat yang netral dan objektif, maka tindakan dan peran peneliti dalam melakukan penelitian perlu dievaluasi karena *'critical self scrunity'* dan *'active reflexivity'* dari peneliti menjadi salah satu kriteria penentu dari keberhasilan penelitian kualitatif, dimana *active reflexivity* meningkatkan *critical self scrunity* dari peneliti (Mason, 2002) serta menjadi *key role* peneliti dalam konstruksi pengetahuan *(knowledge construction)* (Khalid, 2009). Melalui *active reflexivity*, peneliti merefleksikan bagaimana teori, metode dan hal lainnya dapat membantu peneliti untuk memahami wawasan yang muncul dalam penelitian serta peneliti dapat menerima fakta bahwa dirinya merupakan bagian yang tidak terpisahkan dari dunia sosial yang sedang ditelitinya (Bolam *et al.*, 2003; Patton, 2003).

3.3 Prosedur Penelitian

Prosedur penelitian merupakan serangkaian tahapan yang dilakukan oleh peneliti dalam melakukan penelitian, mulai dari rencana penelitian sampai dengan penarikan kesimpulan. Prosedur dari setiap penelitian dapat berbeda, bergantung dengan topik, data dan teknik analisis yang digunakan oleh peneliti. Dalam penelitian ini, peneliti membagi prosedur penelitian ke dalam tiga tahapan, yaitu *planning* (perencanaan), *conducting* (pelaksanaan) dan *reporting* (pelaporan) yang disajikan melalui Gambar 3.1.



Gambar 3.1 Prosedur Penelitian

Sumber: Peneliti (2023)

Planning, pada tahapan ini peneliti melakukan perencanaan penelitian melalui *literature review* sehingga peneliti dapat mengidentifikasi *research gap* dan pertanyaan penelitian. *Literature review* juga membantu peneliti dalam mengidentifikasi landasan teori yang digunakan dalam penelitian sehingga peneliti dapat menentukan paradigma untuk menjawab pertanyaan penelitian. Paradigma dapat membantu peneliti dalam memeroleh pemahaman mengenai fenomena yang terjadi (Saunders *et al*., 2012). Dalam penelitian ini, paradigma yang digunakan adalah *functionalist paradigm* yang disusun oleh dimensi objektivitis dan regulasi. Penelitian yang dilakukan dalam *functionalist paradigm* akan menjadi studi evaluasi untuk menilai efektivitas dari suatu fenomena dan menyusun rekomendasi untuk memperbaiki efektivitas dari fenomena tersebut (Saunders *et al*., 2012).

Conducting, tahapan ini dapat terlaksana jika langkah-langkah dalam tahapan *planning* sudah selesai dilakukan. Dalam tahapan ini, peneliti melaksanakan penelitian kualitatif berdasarkan paradigma studi evaluasi *(functionalist paradigm)* untuk menjawab pertanyaan penelitian melalui wawancara dengan partisipan terpilih sebagai sumber data primer dan observasi dokumen yang terkait dengan pertanyaan penelitian sebagai sumber data sekunder. Data-data yang dihasilkan menjadi dasar bagi peneliti untuk melakukan analisis dengan *content analysis* melalui pendekatan *open coding* (Corbin & Strauss, 2008), *focused coding* (Charmaz, 2006) dan *axial coding* (Corbin & Strauss, 2008) sehingga temuan dalam penelitian dapat tersusun secara fleksibel dan komprehensif (Saunders *et al.*, 2012).

Reporting, merupakan tahapan terakhir dari prosedur dalam penelitian ini. Temuan-temuan dalam penelitian berdasarkan hasil coding yang dilakukan oleh peneliti disajikan ke dalam *report maps, matrix coding query,* dan *framework matrices* untuk memudahkan peneliti dalam mendiskusikan dan menginterpretasikan hasil temuan sehingga peneliti dapat memberikan kontribusi dan rekomendasi perbaikan (jika diperlukan) kepada objek penelitian. Dengan demikian, peneliti dapat menyusun kesimpulan untuk menjawab pertanyaan penelitian berdasarkan hasil studi evaluasi yang diperoleh.

3.4 Sumber dan Pengumpulan Data

Sumber dan pengumpulan data pada penelitian kualitatif dapat diperoleh melalui data non-numerik yang tidak terstandar sehingga prosedur penelitian dapat berubah selama proses penelitian yang bersifat naturalistik dan interaktif. Data non-numerik dapat bersumber dari data primer, seperti: wawancara, survei dan etnografi, ataupun berasal dari dokumen sebagai data sekunder (de Villiers *et al.*, 2019). Penggunanaan kombinasi dari kedua jenis sumber data tersebut banyak digunakan oleh para peneliti dalam menjawab pertanyaan penelitian (Saunders *et al*., 2012).

3.4.1 Sumber Data Sekunder

Untuk menjawab pertanyaan dan memenuhi tujuan penelitian, peneliti dapat melakukan analisis terhadap data yang sudah dikumpulkan sebelumnya (Saunders *et al.,* 2012). Data tersebut merupakan data sekunder dimana analisis lebih mendalam terhadap data bertujuan untuk memberikan pengetahuan, interpretasi

dan atau kesimpulan tambahan yang berbeda dari sebelumnya (Bulmer *et al.*, 2009).

Pada penelitian ini, data sekunder digunakan untuk menjawab pertanyaan penelitian nomor 1 (satu), yaitu beberapa dokumen yang berkaitan dengan mekanisme pencegahan ML untuk *virtual currency* di Indonesia dan sudah dipublikasikan oleh lembaga yang berwenang. Daftar dokumen yang digunakan disajikan melalui Tabel 3.1.

Tabel 3.1 Sumber Data Sekunder

No.	Jenis Peraturan	Pembahasan	Sumber
1.	Undang-Undang Nomor 7 Tahun 2011	Penggunaan Mata Uang	Republik Indonesia
2.	Peraturan Menteri Perdagangan Nomor 99 Tahun 2018	Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	Kementerian Perdagangan
3.	Peraturan Kepala Bappebti Nomor 8 Tahun 2021	Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto	Badan Pengawas Perdagangan Berjangka Komoditi
4.	Peraturan Bappebti Nomor 5 Tahun 2019	Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto di Bursa Berjangka	
5.	Peraturan Bappebti Kepala Nomor 11 Tahun 2017	Pedoman Penerapan Program APU/PPT pada Pialang Berjangka	
6.	Peraturan Kepala Bappebti Nomor 8 Tahun 2017	Penerapan Program APU/PPT pada Pialang Berjangka	

Sumber: Peneliti

3.4.2 Sumber Data Primer

Data primer merupakan data asli yang dikumpulkan oleh peneliti. Data primer harus bersifat apa adanya, tidak boleh diubah dan dipalsukan (Saunders *et al*., 2012). Pada penelitian ini, peneliti mengumpulkan data primer untuk

menjawab pertanyaan penelitian nomor 2 (dua) dan 3 (tiga) melalui wawancara semi-terstruktur dengan partisipan terpilih. Dalam wawancara semi-terstruktur, peneliti memiliki topik dan beberapa daftar pertanyaan yang akan dibahas dengan partisipan wawancara (Hamilton & Finley, 2020). Namun, urutan tersebut dapat bervariasi, bergantung dengan alur percakapan antara peneliti dengan partisipan wawancara. Wawancara penelitian bertujuan untuk mengumpulkan data yang valid, dapat diandalkan dan relevan dengan pertanyaan serta tujuan penelitian (Saunders *et al*., 2012).

Wawancara dilakukan secara *one-to-one* antara peneliti dengan satu partisipan wawancara secara bergantian (Saunders *et al.*, 2012). Secara tradisional, pengumpulan data dilakukan melalui pertemuan *in-person* untuk berdiskusi, berinteraksi dan melakukan wawancara. Namun, sejak diberlakukannya *lockdowns* karena Pandemi COVID-19 maka para peneliti memanfaatkan teknologi video untuk melakukan pertemuan, seperti: WhatsApp, Skype, Zoom, Google Meet dan teknologi lain yang sejenis (Molinari & de Villiers, 2021) yang kemudian rekaman hasil wawancara tersebut ditranskripsikan oleh peneliti ke dalam bentuk teks atau tulisan. Partisipan wawancara potensial akan dihubungi melalui *e-mail* atau media komunikasi lain oleh peneliti untuk dijelaskan mengenai latar belakang dan tujuan penelitian (Urumsah, 2012). Daftar partisipan wawancara pada penelitian ini disajikan melalui Tabel 3.2.

Tabel 3.2 Partisipan Wawancara

Inisial	Jenis Kelamin	Usia (Tahun)	Bidang Kompetensi dan Keahlian	Institusi
P1	Laki-Laki	31-35	*Anti-Money Laundering Operating System*	Flagright
P2	Laki-Laki	26-30	*Anti-Money Laundering Operating System*	Sistem Uji Tuntas (SIJITU)
P3	Perempuan	21-25	*Anti-Money Laundering Operating System*	Sistem Uji Tuntas (SIJITU)

Sumber: Peneliti

3.5 Teknik Analisis Data

3.5.1 *Qualitative Content Analysis*

Analisis data untuk rumusan masalah yang pertama dalam penelitian ini dilakukan dengan pendekatan *content analysis* (Holsti, 1969) karena tujuan dari penelitian ini lebih bersifat eksploratif (Berg, 2004). *Content analysis* dapat digunakan untuk semua jenis sumber dan pengumpulan data, baik untuk penelitian kualitatif maupun kuantitatif (Molinari & de Villiers, 2021). Pada penelitian kuantitatif, *content analysis* berasal dari *media research*, sedangkan *content analysis* pada penelitian kualitatif berakar pada *social research* (Bengtsson, 2016).

Qualitative content analysis bertujuan untuk mereduksi data-data—berupa teks atau kalimat—yang diperoleh menjadi beberapa tingkat interpretasi agar data-data tersebut dapat dideskripsikan secara sistematis (Silva, 2022) melalui proses kodifikasi atau *coding* ke dalam kategori yang sudah ditentukan (Molinari & de Villiers, 2021) atau dilambangkan dengan kalimat yang bermakna (Urumsah, 2012). Kodifikasi data yang berasal dari dokumen dalam penelitian ini

dilakukan dengan bantuan *software* analisis NVivo 12 dan terbagi atas tiga tahap, yaitu:

1. *Open Coding* (Corbin & Strauss, 2008), analisis data awal dengan pengkategorian fokus dan struktur data yang lebih rendah;
2. *Focused Coding* (Charmaz, 2006), mengkaji dan menganalisis kembali data pada *open codes* untuk dikategorikan ke dalam unit atau kategori yang lebih besar;
3. *Axial Coding* (Corbin & Strauss, 2008), proses mencari hubungan antar kategori data dari proses *coding* sebelumnya yang bertujuan untuk menunjukkan proses pengembangan teoritis.

Teknik analisis data dengan pendekatan *qualitative content analysis* yang digunakan oleh peneliti mengacu pada penelitian yang telah dilakukan oleh Shi *et al*., (2022) dan Silva (2022). Peneliti menggabungkan teknik analisis dari kedua penelitian tersebut dimana Shi *et al*., (2022) melakukan *qualitative content analysis* dengan bantuan *software* analisis NVivo, sedangkan Silva (2022) mengaplikasikan *open coding* dan *axial coding* dalam melakukan reduksi data pada pendekatan *qualitative content analysis*. Peneliti menambah satu jenis teknik pengkodifikasian, yaitu *focused coding* (Charmaz, 2006) agar hasil analisis dalam penelitian ini dapat memberikan informasi yang tersusun secara sistematis dan lebih komprehensif (Saunders *et al*., 2012).

3.5.2 *Qualitative Thematic Analysis*

Analisis data untuk rumusan masalah kedua dan ketiga dalam penelitian ini menggunakan pendekatan analisis tematik *(thematic analysis)* karena kedua

rumusan masalah tersebut bertujuan untuk mengeksplorasi alasan dari terjadinya suatu peristiwa (Ayres, 2007). *Thematic analysis* merupakan bagian dari fenomenologi (Vaismoradi *et al*., 2013) yang berfokus pada pencarian dan pembuatan tema dari kumpulan data (Social Change UK, 2018). Dalam mereduksi data, pendekatan *thematic analysis* mirip dengan pendekatan *content analysis* karena menggunakan teknik pengkodean (Social Change UK, 2018). Perbedaannya terletak pada tahapan proses yang dilakukan ketika melakukan analisis data. Dalam penelitian ini, tahapan yang dilakukan mengacu pada Social Change UK (2018) dan mengikuti pendekatan serupa yang dilakukan oleh Sampat *et al*. (2023), yaitu sebagai berikut:

1. Membaca dan memahami seluruh kumpulan data tanpa melakukan pengkodean *(coding)*;
2. Mengidentifikasi tema-tema utama dengan pengaplikasian *open coding*;
3. Meninjau, menyusun, dan mengelompokkan kembali tema-tema serupa dengan pengaplikasian *focused coding*;
4. Merevisi pelabelan atau penamaan tema pada hasil *coding*;
5. Mengidentifikasi hubungan dari tema-tema yang signifikan dengan mengapalikasikan *axial coding*;
6. Memeriksa konsistensi dari hasil analisis data.

Dalam melakukan pendekatan *thematic analysis*, peneliti dibantu dengan *software* analisis NVivo. Penggunaan *software* ini didasarkan pada penelitian Sampat *et al*. (2023) yang melakukan pendekatan *thematic analysis* dengan bantuan *software* analisis NVivo.

3.6 Teknik Pengujian Keabsahan Data

Reliabilitas dan validitas dapat diterapkan pada semua jenis penelitian karena hal penting dari suatu penelitian adalah dapat memberikan penjelasan yang masuk akal *(plausible)* dan dapat dipercaya *(credible)* (Morse, 2002). Pada penelitian kualitatif, reliabilitas dan validitas bergantung dengan kemampuan peneliti. Peneliti harus memiliki sikap yang responsif dan mudah beradaptasi, memiliki sensitivitas serta kemampuan untuk memverifikasi hasil penelitian (Morse, 2002).

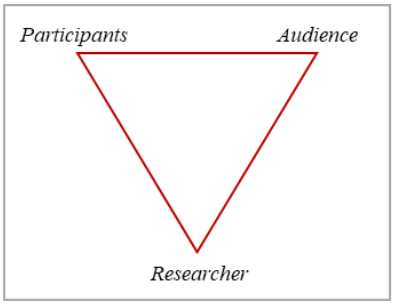
3.6.1 Uji Reliabilitas

Uji reliabilitas mengacu pada hasil yang konsisten atau kompatibel dalam suatu percobaan dan atau uji statistik (Hancock & Algozzine, 2006). Uji reliabilitas pada penelitian kualitatif dipekenalkan oleh Morse (2002) melalui strategi verifikasi *(verification strategies)* yang merujuk pada mekanisme yang digunakan oleh peneliti selama proses penelitian dengan melakukan identifikasi dan koreksi kesalahan dari setiap proses yang dilakukan. Peneliti memastikan kesesuaian dan keselarasan antara pertanyaan penelitian, kajian pustaka, pengumpulan dan analisis data dengan hasil pengembangan teoritis serta interpretasi dari temuan dan hasil penelitian.

3.6.2 Uji Validitas

Uji validitas bertujuan untuk memastikan bahwa hasil penelitian merepresentasikan peristiwa yang sebenarnya (Saunders *et al*., 2012). Pada penelitian kualitatif, uji validitas menurut Hancock dan Algozzine (2006) dilakukan dengan teknik triangulasi yang merujuk pada verifikasi terhadap

berbagai sumber. Uji validitas dalam penelitian ini dilakukan melalui dua tahap. Pada tahap pertama, uji validitas dilakukan melalui *cluster analysis* berdasarkan kesamaan kata *(word similarity)* pada setiap sumber data yang digunakan. Hasil uhi validitas dalam penelitian ini dilampirkan pada Lampiran 14 dan 15. Sedangkan pada tahap kedua, peneliti mengungkapkan hasil penelitiannya kepada partisipan wawancara untuk memastikan kebenaran atas hasil temuan dan interpretasi peneliti. Selanjutnya, peneliti juga mendiskusikan hasil temuan dan interpretasinya kepada para ahli di bidang yang ditelitinya untuk mendapatkan *expert review* dan gambaran kemungkinan dari perspektif *audience*.



Gambar 3.2 *Triangulated Inquiry*
Sumber: Hancock dan Algozzine (2006)

3.7 Penyajian Data

Hasil analisis data melalui reduksi data pada proses *coding* divisualisasikan ke dalam *report maps* dan *framework matrices* agar hasil analisis data dapat tersusun secara sistematis.

3.7.1 *Report Maps*

Report maps menggambarkan hasil penelitian dengan menjawab pertanyaan penelitian yang sudah disusun melalui konsep pola yang saling berhubungan.

Pola-pola tersebut tersusun atas kategori-kategori atau kodifikasi dari data penelitian.

3.7.2 *Matrix Coding Query*

Matrix coding query terdiri atas *row* dan *column* yang merupakan susunan *nodes* atau ketegori dan sumber data. Perpotongan antara *row* dan *column* berisi jumlah *coding* dari masing-masing *nodes* terhadap sumber data. *Matrix coding query* dalam penelitian ini dapat dilihat pada Lampiran 4 sampai dengan Lampiran 8.

3.7.3 *Framework Matrices*

Hasil dari proses *coding* lainnya adalah *framework matrix* yang menyajikan hasil analisis data dalam bentuk tabel. Tabel ini berisi sumber data primer dan sekunder yang sudah dilakukan *coding* oleh peneliti berdasarkan kategori atau kodifikasi yang sudah ditentukan. *Framework matrices* dalam penelitian ini dapat dilihat pada Lampiran 9 sampai dengan Lampiran 13.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Mekanisme Anti-Pencucian Uang untuk Aset Kripto di Indonesia

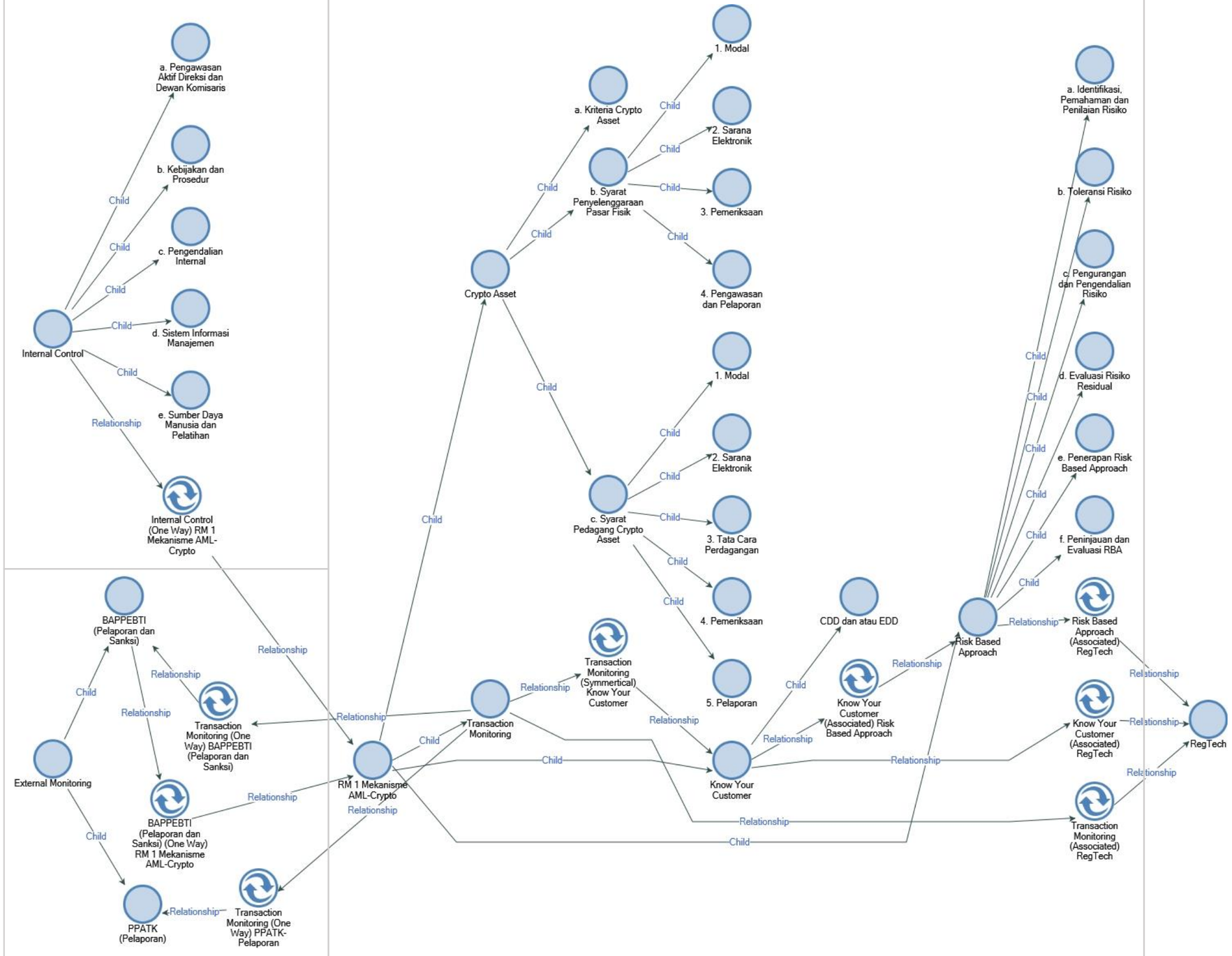
Anti-Pencucian Uang atau disingkat APU adalah upaya pencegahan dan pemberantasan terhadap tindak pidana pencucian uang. Mekanisme ini memaparkan serangkaian tindakan dalam mencegah pencucian uang dengan melibatkan aset kripto yang perlu dilakukan oleh institusi terkait. Pada dasarnya, aset kripto yang telah berkembang di Indonesia tidak dapat diklasifikasikan sebagai mata uang karena mata uang yang sah di Indonesia menurut Undang-Undang Republik Indonesia Nomor 7 Tahun 2011 adalah mata uang rupiah yang disimbolkan dengan "Rp" sehingga aset kripto ditetapkan dan dibatasi penggunaannya hanya sebagai komoditi yang dapat dijadikan subjek kontrak berjangka serta diperdagangkan di bursa berjangka (Peraturan Menteri Perdagangan Nomor 99: Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto (Crypto Asset), 2018).

Aset kripto bersifat tidak berwujud dan berbentuk digital—berupa koin dan token—dengan menggunakan kriptografi, jaringan informasi teknologi, dan buku besar yang terdistribusi *(blockchain)* untuk mengatur penciptaan unit baru, memverifikasi transaksi serta mengamankan transaksi tanpa campur tangan pihak lain. Di Indonesia, pedagang dan pelanggan yang melakukan kegiatan transaksi dan atau perdagangan pada pasar fisik aset kripto harus terlebih dahulu memperoleh persetujuan dari Kepada Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) yang memiliki tugas pokok untuk melakukan pembinaan, pengaturan,

pengembangan, dan pengawasan terhadap perdagangan berjangka (Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka, 2021).

Dalam penerapannya, serangkaian tindakan dalam mencegah pencucian uang melalui aset kripto dipantau oleh Bappebti dan PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan) sebagai pihak eksternal serta dikendalikan oleh manajemen pialang berjangka sebagai pihak internal melalui pengendalian internal yang telah ditetapkan. Mekanisme APU dengan melibatkan aset kripto yang ditunjukkan melalui *report maps* pada Gambar 4.1 merupakan hasil analisis data yang berasal dari data sekunder berupa undang-undang dan peraturan terkait yang kemudian peneliti klasifikasikan ke dalam tiga kategori besar, yaitu penerapan, mekanisme, dan pemanfaatan teknologi. Pada kategori mekanisme yang menjadi pemaparan utama pada sub-bab ini, peneliti membagi kembali ke dalam empat sub-kategori yang saling berhubungan berdasarkan referensi dan jumlah *coding* yang terdapat pada Lampiran 6, yaitu *crypto asset*, *risk-based approach*, *know your customer*, dan *transaction monitoring*.

Penerapan	Mekanisme	Pemanfaatan Teknologi



Gambar 4.1 *Report Map* Mekanisme Anti-Pencucian Uang untuk Aset Kripto di Indonesia

Sumber: NVivo 12

4.1.1 *Crypto Asset*

Crypto asset atau aset kripto—sebagaimana yang telah dipaparkan sebelumnya—merupakan bagian dari komoditi yang dapat dijadikan sebagai subjek kontrak berjangka yang berbentuk aset digital dan atau tidak berwujud. Dalam penelitian ini, aset kripto menjadi komoditi pada proses *concealment* (penyembunyian) dan *conversion* (konversi) dalam proses pencucian uang—yang berasal dari tindak pidana asal—melalui transaksi pada pasar fisik aset kripto di bursa berjangka. Di Indonesia, Bappebti telah menetapkan syarat dan ketentuan yang berlaku dalam menentukan komoditi yang dapat disebut sebagai aset kripto beserta syarat dan ketentuan yang harus dipenuhi bagi penyelenggara perdagangan pasar fisik aset kripto dan pedagang aset kripto.

4.2.1.1 Kriteria Aset Kripto

Aset kripto yang dapat diperdagangkan di Indonesia harus memenuhi kriteria dan ketentuan paling sedikit sebagaimana yang disajikan pada Tabel 4.1.

Tabel 4.1 Kriteria dan Ketentuan Jenis Aset Kripto

No.	Kriteria	Ketentuan
1.	Berbasis *distributed ledger technology*	Contoh: *Blockchain*
2.	Aset kripto utilitas *(utility crypto)* atau aset kripto beragun aset *(crypto backed asset)*	Khusus untuk *utility crypto* maka *coin market cap* harus masuk ke dalam peringkat 500 besar bursa aset kripto dunia.
3.	Memiliki hasil penilaian dengan metode *Analytical Hierarchy Process* (AHP) berdasarkan ketetapan Bappebti	- Memiliki *coin maret cap*; - Masuk dalam transaksi bursa aset kripto dunia; - Memiliki manfaat ekonomi (seperti: perpajakan, ekonomi digital, industri informatika); - Telah melakukan penilaian risiko TPPU.

Sumber: Peneliti, Diolah

4.2.1.2 Syarat Penyelenggara Perdagangan Aset Kripto

Penyelenggaraan perdagangan Pasar Fisik Aset Kripto hanya dapat dilakukan dengan menggunakan sarana elektronik yang dimiliki oleh pedagang fisik aset kripto dan diawasi oleh bursa berjangka yang telah memperoleh persetujuan dari Kepala Bappebti dengan syarat bahwa bursa berjangka tersebut tidak diperbolehkan untuk menyelenggarakan subjek komoditi lain (Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka, 2021). Pembentukan Pasar Fisik Aset Kripto dibawah pengawasan Bappebti bertujuan untuk memberikan sarana pembentukan harga yang transparan sehingga dapat digunakan sebagai referensi harga di bursa berjangka, memberikan kepastian hukum dan perlindungan kepada pelanggan aset kripto serta memfasilitasi inovasi, pertumbuhan, dan perkembangan kegiatan usaha perdagangan aset kripto di Indonesia (Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 5: Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka, 2019). Untuk memperoleh persetujuan dari Bappebti dalam melakukan perdagangan aset kripto di bursa berjangka maka bursa berjangka wajib memenuhi persayaratan dan ketentuan sebagaimana yang disajikan pada Tabel 4.2.

Tabel 4.2 Syarat dan Ketentuan Penyelenggara Perdagangan Aset Kripto

No.	Syarat	Ketentuan
1.	Modal	- Modal Disetor: Paling sedikit Rp 500,000,000,000 - Modal SDM: Memiliki pegawai atau bekerjasama dengan tenaga ahli yang memiliki sertifikasi CISA *(Certified Information Systems Auditor)* dan CISSP *(Certified Information Systems Security Professional)*
2.	Sarana Elektronik	- Ditujukan sebagai sistem pendukung dalam fungsi pengawasan dan pelaporan; - Bersifat akurat, aktual, aman, terpercaya, *online*, *realtime*, dan *compatible*; - Dapat melindungi akses data profil, keuangan, dan transaksi setiap pelanggan; - Memiliki BCP *(Business Continuity Plan)*, DRC *(Disaster Recovery Center)*, dan konfigurasi dengan spesifikasi yang tertera dalam *framework matrices* pada Lampiran 9.
3.	Pemeriksaan	Pemeriksaan dan audit terhadap sistem elektronik dilakukan oleh lembaga independen dan atau auditor dengan kompetensi di bidang sistem informasi, seperti: CISA dan memiliki keahlian di bidang teknologi aset kripto dan *blockchain*.
4.	Pengawasan dan Pelaporan	- Dilaksanakan secara teratur, transparan, wajar, dan dapat diakses secara *real time*; - Melakukan pengawasan terhadap seluruh transaksi dan audit terhadap anggota yang berkaitan; - Melakukan evaluasi dan kajian atas usulan penambahan atau pengurangan terhadap aset kripto.

Sumber: Peneliti, Diolah

4.2.1.3 Syarat Pedagang Aset Kripto

Pedagang aset kripto bertindak dalam memfasilitasi transaksi perdagangan aset kripto yang meliputi kegiatan jual beli antara aset kripto dengan mata uang rupiah, pertukaran antar jenis aset kripto, dan pemindahan aset kripto antar *wallet*. Dalam melaksanakan aktivitasnya, pedagang aset kripto wajib melakukan pengkajian dan penilaian risiko terhadap aktivitas bisnisnya, termasuk risiko pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal. Untuk dapat melakukan aktivitas sebagai pedagang aset kripto di bursa berjangka maka

pedagang aset kripto wajib memenuhi syarat dan ketentuan sebagaimana yang disajikan pada Tabel 4.3.

Tabel 4.3 Syarat dan Ketentuan Pedagang Aset Kripto

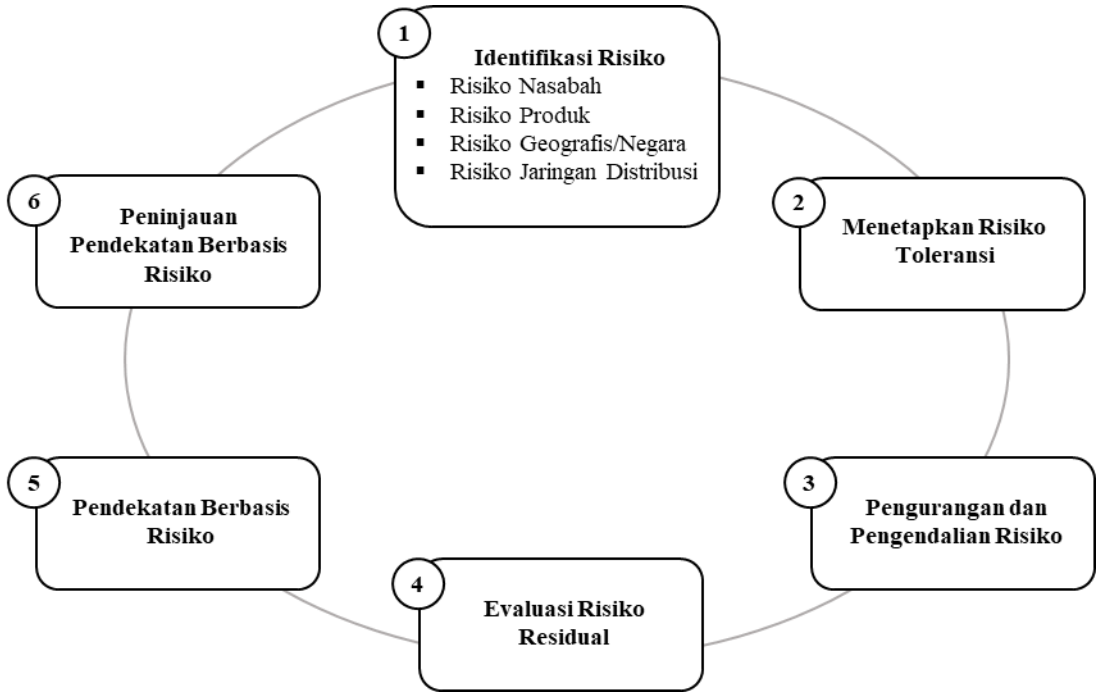
No.	Syarat	Ketentuan
1.	Modal	- Modal Disetor: Paling sedikit Rp 80,000,000,000 - Modal SDM: Terbagi ke dalam Divisi Teknologi Informasi, Audit, Legal, Pengaduan Pelanggan, *Client Support* serta Divisi *Accounting* dan *Finance*.
2.	Sarana Elektronik	- Bersifat akurat, aktual, aman, terpercaya, *online*, *realtime*, dan *compatible*; - Dapat melindungi akses data keuangan dan transaksi setiap pelanggan; - Memiliki BCP *(Business Continuity Plan)*, DRC *(Disaster Recovery Center)*, konfigurasi, *database* transaksi aset kripto serta memiliki *server* dan atau *cloud server*. - Memiliki sertifikasi ISO 27001 *(Information Security Management System)*.
3.	Tata Cara Perdagangan *(Trading Rules)*	- Paling sedikit memuat: (1) Definisi dan istilah; (2) Proses pendaftaran pelanggan; (3) Pernyataan dan jaminan; (4) Kewajiban dan tanggung jawab; (5) Pengkinian data; (6) Tata cara transaksi; (7) Penetapan biaya transaksi dan penarikan; (8) Keamanan transaksi; (9) Layanan pengaduan pelanggan; (10) Penyelesaian perselisihan pelanggan; (11) *Force majeur*; (12) Penerapan program APU PPT. - Ketentuan lebih rinci tertera dalam *framework matrices* pada Lampiran 9.
4.	Pemeriksaan	- Pemeriksaan dan audit terhadap sistem elektronik dilakukan oleh lembaga independen dan atau auditor dengan kompetensi di bidang sistem informasi, seperti: CISA dan memiliki keahlian di bidang teknologi aset kripto dan *blockchain*. - Jika hasil pemeriksaan dan audit terbukti tidak *compatible*, maka pedagang aset kripto wajib menyesuaikan dan atau mengganti sistem.
5.	Pelaporan	Dilaporkan secara berkala kepada Kepala Bappebti yang terdiri atas: - Laporan transaksi harian dan bulanan; - Laporan keuangan harian dan bulanan; - Laporan kegiatan perusahaan secara triwulan dan tahunan.

Sumber: Peneliti, Diolah

4.1.2 *Risk-Based Approach*

Sebagaimana rekomendasi dari FATF nomor 1, maka Pemerintah Indonesia melalui Bappebti memberikan pedoman bagi bursa berjangka maupun pedagang aset kripto dalam rangka menerapkan program APU yang didasarkan pada pendekatan berbasis risiko *(risk-based approach)* yang sejalan dengan penilaian risiko nasional (*nastional risk assessment*/NRA) dan penilaian risiko sektoral (*sectoral risk assessment*/SRA). Namun, penilaian risiko yang tercantum dalam NRA dan SRA dapat berkembang dan mengalami perubahan beriringan dengan dinamika perkembangan teknologi sehingga bursa berjangka dan pedagang aset kripto harus responsif terhadap berbagai jenis perubahan risiko. Pedoman ini menjadi dasar yang harus diterapkan dalam setiap jenis aktivitas bisnis dalam perdagangan aset kripto—seperti: *know your customer* dan *transaction monitoring*—serta bertujuan untuk mengatur kegiatan perdagangan aset kripto yang wajar, efisien, efektif, transparan, dan dapat terlindung dari praktek TPPU (Peraturan Kepala Badan Pengawas Perdagangan Bejangka Komoditi Nomor 11: Pedoman Penerapam Program Anti Pencucian Uang Dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka (2017); Peraturan Kepala Badan Pengawas Perdagangan Bejangka Komoditi Nomor 11 Lampiran: Pedoman Penerapam Program Anti Pencucian Uang Dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka (2017); (Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) Di Bursa Berjangka, 2021)).

Siklus pendekatan berbasis risiko yang perlu diterapkan meliputi enam langkah seperti yang disajikan pada Gambar 4.2.



Gambar 4.2 Siklus Pendekatan Berbasis Risiko
Sumber: Peneliti, Diolah

Enam langkah dalam siklus pendekatan berbasis risiko harus dilaksanakan secara bertahap dan berkesinambungan untuk memperoleh hasil yang optimal. Berikut ini pemaparan dari masing-masing langkah:

1. **Identifikasi, Pemahaman dan Penilaian Risiko**

   Melakukan pengidentifikasian risiko, memahami, dan menilai risiko TPPU yang berkaitan dengan nasabah, negara atau geografis, produk, jasa, dan transaksi atau jaringan distribusi wajib dilakukan oleh penyelenggara perdagangan aset kripto sebelum meluncurkan produk dan teknologi serta melaksanakan aktivitas usaha. Tindakan-tindakan tersebut harus dilakukan secara proporsional dan memadai agar dapat mengelola dan memitigasi risiko-

risiko yang muncul (Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Penerapan Program Anti Pencucian Uang Dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka, 2017). Adapun rincian dari masing-masing risiko yang perlu diidentifikasi, dipahami, dan dinilai disajikan melalui Tabel 4.4.

Tabel 4.4 Jenis dan Kategori Berisiko Tinggi

No.	Jenis Risiko	Ketegori Berisiko Tinggi
1.	Nasabah	a. Nasabah yang melakukan hubungan usaha atau transaksi secara tidak wajar dan tidak sesuai dengan profil nasabah; b. Nasabah korporasi dengan struktur kepemilikan yang kompleks sehingga pemilik manfaat *(beneficial owner)*, pemilik akhir *(ultimate owner)*, dan pengendali akhir *(ultimate controller)* sulit diidentifikasi; c. Nasabah yang pemilik manfaatnya tidak diketahui; d. Nasabah yang tidak bersedia memberikan data dan informasi dalam proses identifikasi atau memberikan informasi yang tidak signifikan serta berpotensi sebagai informasi fiktif.
2.	Negara/Geografis	a. Dana yang diterima dari dan atau dikirim ke negara/yurisdiksi berisiko tinggi; b. Nasabah memiliki hubungan yang signifikan dengan negara/yurisdiksi berisiko tinggi.
3.	Produk/Jasa/ Transaksi	Diidentifikasi dan dinilai secara keseluruhan atas berbagai potensi risiko yang muncul dari setiap produk/jasa/transaksi.
4.	Jaringan Distribusi	Jaringan distribusi dengan adanya transaksi tanpa pertemuan langsung *(non-face to face)*.
5.	Lainnya yang Relevan	a. Tren tipologi, metode, teknik, dan skeman TPPU terbaru; b. Model bisnis terbaru yang melibatkan teknologi terkini.

Sumber: Peneliti, Diolah

Selanjutnya, dilakukan penilaian dengan teknik penskoran *(scoring)* terhadap berbagai jenis risiko tersebut yang disusun berdasarkan skala dan jenis atau kegiatan usaha yang dilakukan dengan pengkategorian risiko pada Tabel 4.5.

Tabel 4.5 Penskoran Risiko *(Scoring)* berdasarkan Skala Usaha

No.	Skala Usaha	Kategori Risiko			
		Rendah *(Low)*	**Menengah *(Medium)***	**Menengah-Tinggi *(Medium-High)***	**Tinggi *(High)***
1.	Kecil	V	-	-	V
2.	Menengah	V	V	V	V
3.	Besar	V	V	V	V

Sumber: Peneliti, Diolah

2. Toleransi Risiko

Toleransi risiko menetapkan dan menentukan batasan risiko yang dapat diterima dan ditoleransi oleh penyelenggara perdagangan aset kripto dan merupakan penjabaran atas tingkat risiko yang akan diambil *(risk appetite)* serta menjadi komponen penting dalam mencapai efektivitas manajemen risiko. Dalam menetapkan dan menentukan toleransi risiko, penyelenggara perdagangan aset kripto perlu mempertimbangkan beberapa risiko, yaitu:

a. Risiko regulator *(regulatory risk)*;

b. Risiko reputasi *(reputational risk)*;

c. Risiko hukum *(legal risk)*;

d. Risiko keuangan *(financial risk)*.

3. Pengurangan dan Pengendalian Risiko

Pengurangan dan pengendalian risiko dalam aktivitas perdagangan aset kripto dilakukan melalui pengendalian internal dan mitigasi risiko berdasarkan

toleransi, penerimaan, penilaian, dan identifikasi risiko yang sudah dilakukan. Langkah tersebut dapat membantu penyelenggara perdagangan aset kripto untuk tetap berada dalam batas toleransi risiko yang sudah ditetapkan, responsif dalam melakukan pengkinian informasi nasabah dan penerima manfaat, melakukan pemantauan berkelanjutan terhadap hubungan usaha yang terjadi dalam proses perdagangan aset kripto, serta menetapkan dan melaksanakan mitigasi dan pengendalian internal secara konsisten.

4. **Evaluasi Risiko Residual**

   Risiko residual merupakan risiko yang tersisa setelah dilakukan mitigasi dan pengendalian risiko. Evaluasi ini bertujuan untuk memastikan bahwa tingkat risiko residual tidak lebih tinggi dari toleransi risiko yang sudah ditetapkan. Jika risiko residual lebih tinggi dari batas toleransi risiko maka penyelenggara perdagangan aset kripto wajib melakukan kembali mitigasi dan pengendalian risiko serta melakukan penyesuaian tingkat risiko yang dimiliki dengan risiko yang dapat ditoleransi atau diterima.

5. **Penerapan Pendekatan Berbasis Risiko *(Risk-Based Approach)***

   Dalam menerapkan pendekatan berbasis risiko, penyelenggaara perdagangan aset kripto harus mendokumentasikan siklus pendekatan berbasis risiko dalam bentuk kebijakan dan prosedur dengan syarat minimum sebagaimana yang disajikan pada Tabel 4.6.

Tabel 4.6 Syarat Minimum Pendekatan Berbasis Risiko

No.	Syarat Penerapan	Tujuan
1.	Identifikasi nasabah	Melakukan pengkinian data dan informasi terhadap nasabah dan penerima manfaat.
2.	Penilaian risiko	a. Melakukan pemantauan terhadap seluruh hubungan usaha yang dimiliki; b. Memastikan bahwa mitigasi dan pengendalian risiko telah dilakukan berdasarkan proses pendekatan berbasis risiko.
3.	Tindakan khusus	a. Melakukan pemantauan yang lebih sering terhadap seluruh hubungan usaha yang berisiko tinggi; b. Melakukan langkah tertentu terhadap nasabah berisiko tinggi.
4.	Pelaporan	Melaporkan temuan-temuan kepada otoritas terkait, terutama pelaporan atas transaksi mencurigakan.

Sumber: Peneliti, Diolah

6. Peninjauan dan Evaluasi Pendekatan Berbasis Risiko

Langkah ini dilakukan secara berkala dan bertujuan untuk mengetahui efektivitas atas kepatuhan penerapan program APU melalui peninjauan kebijakan dan prosedur terhadap penilaian risiko, mitigasi risiko, dan pemantauan berkelanjutan yang intensif. Peninjauan pada pendekatan berbasis risiko membantu penyelenggara perdagangan aset kripto untuk melakukan pengaturan terhadap hasil peninjauan dan menetapkan langkah korektif untuk ditindaklanjuti dalam menyempurnakan kebijakan dan prosedur berdasarkan kebutuhan dalam aktivitas bisnis yang dijalankan.

4.1.3 *Know Your Customer*

Proses penerimaan calon pelanggan dengan menerapkan prinsip mengenal calon pelanggan (*know your customer*/KYC) menjadi langkah awal dan atau pendeteksian dini atas berbagai potensi yang mungkin terjadi dari aktivitas selanjutnya. Proses ini dilakukan oleh setiap pedagang aset kripto dan tidak terbatas

pada saat proses penerimaan pelanggan saja, namun juga selama menjadi pelanggan aset kripto melalui pengkinian profil pelanggan. Seluruh penerapan KYC dilakukan berdasarkan pendekatan berbasis risiko.

Pada KYC tahap awal, dilaksanakan proses identifikasi dan verifikasi data yang terhubung dengan data administrasi kependudukan yang dimiliki oleh Kementerian Dalam Negeri dan dilakukan melalui sistem elektronik daring *(online)* yang sah menurut ketentuan peraturan perundang-undangan serta dapat menjamin kerahasiaan setiap data dan informasi. Selanjutnya, jika calon pelanggan dan atau pelanggan termasuk ke dalam pelanggan berisiko tinggi *(high risk customers)* maka harus dilaksanakan proses identifikasi dan verifikasi lebih lanjut melalui uji tuntas nasabah (*customer due diligence*/CDD) dan atau uji tuntas lanjutan (*enhanced due diligence*/EDD) untuk memastikan kebenaran data isian dengan profil atau latar belakang calon pelanggan. Calon pelanggan dan atau pelanggan yang termasuk ke dalam kategori *high risk customer* adalah sebagai berikut:

1. Latar belakang atau profil calon pelanggan termasuk berisiko tinggi;
2. Produk yang digunakan termasuk ke dalam produk berisiko tinggi yang digunakan sebagai sarana TPPU;
3. Transaksi dengan pihak yang berasal dari negara berisiko tinggi atas tindak TPPU;
4. Transaksi yang dilakukan tidak sesuai dengan latar belakang atau profil pelanggan;
5. Negara atau domisili calon pelanggan serta tempat dilakukannya transaksi termasuk ke dalam negara berisiko tinggi;

6. Calon pelanggan dan atau pelanggan termasuk ke dalam daftar terduga pelaku terorisme atau organisasi terorisme dan atau termasuk ke dalam daftar hitam nasional (DHN);
7. Transaksi yang dilakukan diduga terkait TPPU.

Adapun CDD yang dilaksanakan terhadap *high risk customer* meliputi proses identifikasi, verifikasi, dan pemantauan terhadap pelanggan aset kripto untuk memastikan kesesuaian antara profil pelanggan dengan pola transaksi yang dilakukan. Sedangkan proses EDD merupakan tindakan CDD yang lebih mendalam dan dilakukan pada calon pelanggan yang juga termasuk ke dalam orang yang populer secara politis (*politically exposed person*/PEP) yang meliputi: (1) PEP asing, sebagai orang yang diberi kewenangan untuk melakukan fungsi penting *(prominent function)* oleh negara asing; (2) PEP domestik, sebagai orang yang diberi kewenangan untuk melakukan fungsi penting *(prominent function)* oleh negara; dan (3) Orang yang diberi kewenangan untuk melakukan fungsi penting *(prominent function)* oleh organisasi internasional. Proses EDD juga dilakukan pada calon pelanggan, pelanggan, dan atau pemilik manfaat *(beneficial owner)* yang memiliki hubungan terkait *(closes associates)* dengan PEP, seperti: perusahaan yang dimiliki oleh PEP, pihak yang secara umum diketahui publik memiliki hubungan yang dekat dengan PEP serta keluarga inti, kandung, tiri dan atau keluarga angkat PEP.

Rincian dari masing-masing tahapan yang harus dilaksanakan pada proses CDD dan atau EDD disajikan dalam Tabel 4.7.

Tabel 4.7 Proses *Customer Due Dilligence* dan *Enhanced Due Dilligence*

No.	Tahapan	*Customer Due Dilligence*	*Enhanced Due Dilligence*
1.	Identifikasi	a. *High risk customer*; b. Terdapat transaksi yang setara dengan Rp 100,000,000; c. Terdapat keraguan atas kebenaran data, informasi, dan atau dokumen pendukung; d. Terdapat indikasi transaksi mencurigakan.	a. *High risk customer*; b. PEP; c. *Closes associates* dengan PEP;
2.	Verifikasi	Melakukan wawancara secara *face-to-face* untuk meyakini identitas calon pelanggan.	a. Mencari informasi tambahan tentang: - Tujuan dari pembukaan rekening aset kripto; - Sumber dana atau kekayaan calon pelanggan; - Alasan dari transaksi yang dilakukan. b. Meminta persetujuan dari pejabat senior untuk menerima atau menolak calon pelanggan.
3.	Pemantauan	a. Memastikan kesesuaian antara latar belakang calon pelanggan atau pelanggan dengan pola transaksi; b. Melakukan klasifikasi transaksi dan pemantauan rekening; c. Dilakukan secara berkesinambungan dan didokumentasikan secara tertulis.	a. Memastikan kesesuaian antara latar belakang calon pelanggan atau pelanggan dengan pola transaksi dengan penambahan intensitas waktu dan SDM; b. Melakukan klasifikasi transaksi dan pemantauan rekening; c. Dilakukan secara berkesinambungan dan didokumentasikan secara tertulis.

Sumber: Peneliti, Diolah

Seluruh rangkaian proses KYC ini—terutama proses identifikasi dan verifikasi--diselenggarakan dengan berbasis *regulatory technology* (RegTech) yang mana

kualifikasi kriterianya menggunakan *face recognition* dengan karakteristik *liveness* yang terintegrasi dengan data *biometric*. Proses KYC tidak terlepas dan menjadi dasar atas aktivitas pemantauan transaksi *(transaction monitoring)* karena kedua proses tersebut dilakukan secara berkesinambungan.

4.1.4 *Transaction Monitoring*

Dalam upaya mencegah pencucian uang yang melibatkan aset kripto maka penyelenggara perdagangan aset kripto harus melaksanakan aktivitas pemantauan transaksi atau *transaction monitoring* dengan menerapkan prinsip *know your transaction* (KYT) dalam setiap prosesnya, yang mana proses ini dilakukan secara berkesinambungan dengan prinsip KYC untuk memastikan bahwa pola transaksi yang dilakukan berkesesuaian dengan latar belakang pelanggan atau nasabah aset kripto.

Prinsip KYT yang diterapkan dalam aktivitas transaksi penarikan dan atau perpindahan aset kripto di Pasar Fisik Aset Kripto dilakukan melalui proses verifikasi yang dilaksanakan oleh Lembaga Kliring Berjangka untuk kepentingan penjaminan dan penyelesaian transaksi dengan dua metode verifikasi, yaitu *travel rules* dan DvP *(Delivery versus Payment)*. Proses verifikasi ini dibedakan dan didasarkan pada jenis transaksi yang dilakukan. Untuk transaksi penarikan aset kripto maka hanya diterapkan metode DvP, sedangkan untuk transaksi perpindahan aset kripto diterapkan metode *travel rules* dan DvP dengan rincian yang disajikan pada Tabel 4.8.

Tabel 4.8 Proses Verifikasi berdasarkan Jenis Transaksi

<table>
<tr><th rowspan="3">Metode Verifikasi</th><th colspan="3">Jenis Transaksi</th></tr>
<tr><th rowspan="2">Penarikan Aset Kripto</th><th colspan="2">Perpindahan Aset Kripto</th></tr>
<tr><th>Setara atau Lebih dari USD 1,000</th><th>Kurang dari USD 1,000</th></tr>
<tr><td>Travel Rules</td><td>-</td><td>a. Memastikan informasi pengirim yang meliputi:
- Nama dan alamat pengirim;
- Alamat wallet pengirim;
- KTP bagi WNI atau passport dan KITAP[2] atau KITAS[3] bagi WNA;
- Tempat dan tanggal lahir pengirim.
b. Mendapatkan informasi penerima yang meliputi:
- Nama dan alamat penerima;
- Alamat wallet penerima;</td><td>Memastikan informasi yang meliputi:
- Nama pengirim;
- Alamat wallet pengirim;
- Nama penerima;
- Alamat wallet penerima.</td></tr>
<tr><td>DvP (Delivery versus Payment)</td><td colspan="3">a. Memastikan kesesuaian dana yang ada pada rekening yang terpisah dengan saldo atau catatan kepemilikan aset kripto;
b. Menolak permintaan penarikan dan atau pemindahan aset kripto jika tidak terdapat kesesuaian antara permintaan dengan saldo atau catatan kepemilikan aset kripto;
c. Melakukan pencatatan perpindahan dana dan saldo atau catatan kepemilikan aset kripto;
d. Meminta kepada penyelenggara perdagangan dan atau pedagang aset kripto untuk mengubah saldo atau catatan atas kepemilikan aset kripto yag disimpan di tempat penyimpanan sebagaimana kondisi yang sebenarnya;
e. Melakukan pendebetan dan pengkreditan rekening keuangan pelanggan aset kripto dan atau pedagang fisik aset kripto untuk kepentingan penjaminan dan penyelesaian transaksi.</td></tr>
</table>

Sumber: Peneliti, Diolah

[2] Kartu Izin Tinggal Tetap
[3] Kartu Izin Tinggal Terbatas

Selanjutnya, penerapan prinsip KYT juga dilaksanakan dalam proses pendeteksian dan pemantauan transaksi aset kripto yang dilakukan secara berkesinambungan dengan:

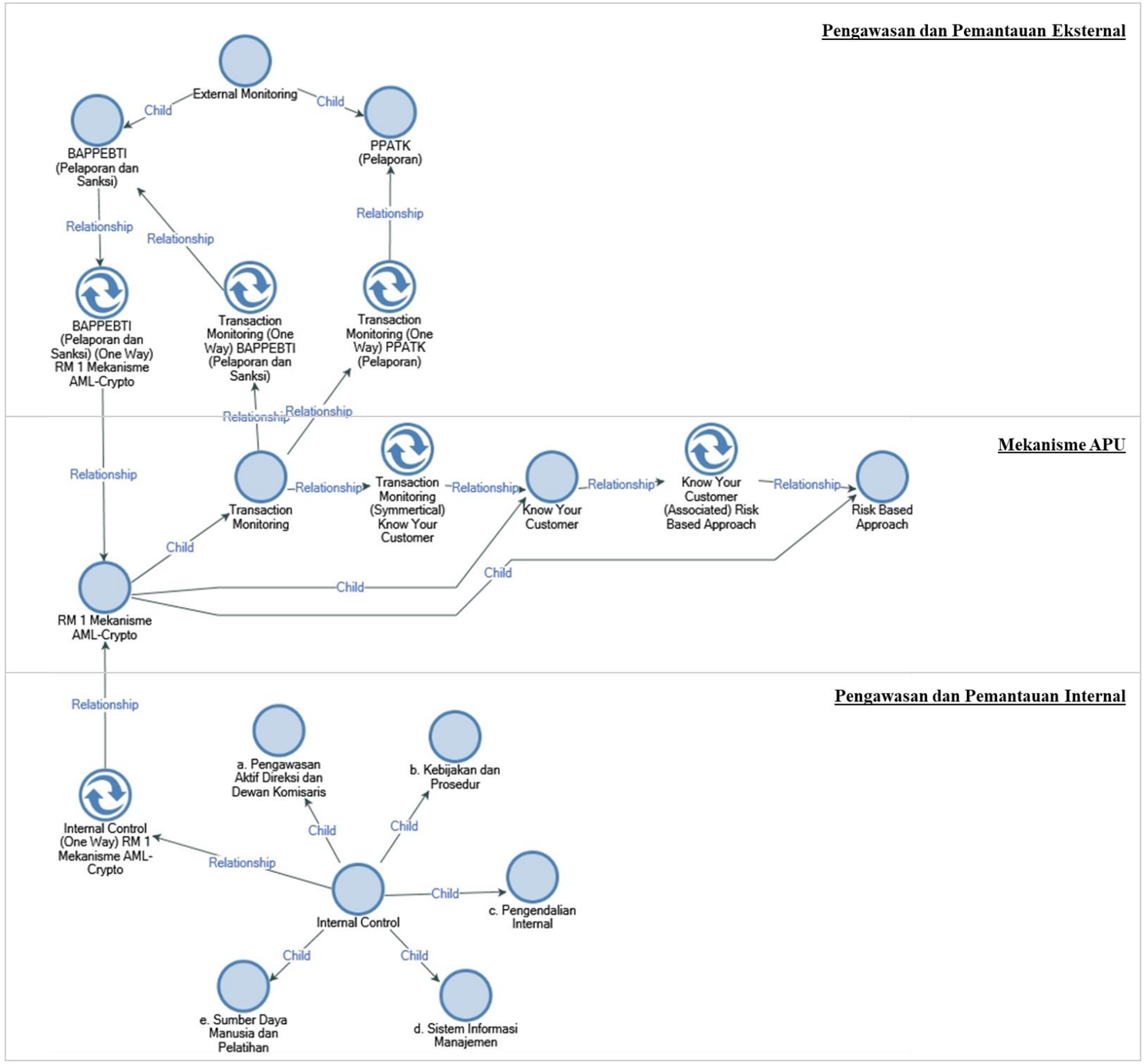
1. Meneliti kategori risiko nasabah, apakah termasuk ke dalam *high risk customer* atau daftar hitam negara (DHN);
2. Meneliti sumber dana nasabah, apakah sumber dana dapat dideteksi dan diketahui;
3. Meneliti transaksi nasabah untuk memastikan bahwa transaksi yang dilakukan sejalan dengan latar belakang risiko nasabah;
4. Menganalisis seluruh transaksi yang tidak sesuai dengan latar belakang nasabah;
5. Meminta informasi mengenai latar belakang dan tujuan transaksi yang dilakukan oleh nasabah jika transaksi tersebut tidak sesuai dengan latar belakang nasabah.

Seluruh rangkaian proses dalam *transaction monitoring* berdasarkan prinsip KYT ini harus diselenggarakan dengan memanfaatkan *regulatory technology* (RegTech) melalui aplikasi *blockchain analytic tools* untuk mengidentifikasi, menganalisis, memantau, dan meninjau transaksi aset kripto saat ini beserta dengan rekam jejaknya di masa lampau untuk mengetahui dan menelusuri setiap transaksi yang dilakukan oleh nasabah. Apabila dari rangkaian proses tersebut terdapat indikasi transaksi mencurigakan yang ditandai dengan tidak sesuainya transaksi tersebut dengan kriteria dan ketentuan yang telah ditetapkan dalam proses verifikasi, pendeteksian, dan pemantauan transaksi maka penyelenggara perdagangan aset kripto harus melaporkan kepada Bappebti dan PPATK sebagai

Laporan Transaksi Mencurigakan berdasarkan ketentuan dalam pencegahan dan pemberantasan TPPU.

4.1.5 Pengawasan dan Pemantauan terhadap Penerapan Anti-Pencucian Uang untuk Aset Kripto di Indonesia

Pengawasan dan pemantauan terhadap penerapan dari mekanisme APU dilakukan sebagai upaya dalam mencegah dan memberantas tindak pidana pencucian uang yang melibatkan penggunaan aset kripto di Indonesia. Pengawasan dan pemantauan ini dilakukan oleh pihak eksternal dan internal dari penyelenggara perdagangan aset kripto untuk menciptakan sinergi pembinaan, pengaturan, pengembangan, pengawasan, dan pemantauan secara menyeluruh. Pengawasan dan pemantauan yang dilakukan oleh pihak eksternal menjadi tanggungjawab dan kewajiban Bappebti serta PPATK, sedangkan tanggungjawab dan kewajiban dari pihak internal dilaksanakan oleh manajemen pialang berjangka. Sinergisitas dan peran dari masing-masing pihak terhadap penerapan APU untuk aset kripto dipaparkan melalui *report maps* pada Gambar 4.3. Masing-masing *node* yang menjadi *'child node'* dalam *report maps* tersebut didasarkan pada referensi dan jumlah *coding* yang terdapat pada Lampiran 7.



Gambar 4.3 *Report Map* Pengawasan dan Pemantauan terhadap Penerapan Anti-Pencucian Uang untuk Aset Kripto di Indonesia

Sumber: NVivo 12

4.1.5.1 Pengawasan dan Pemantauan Internal

Pengawasan dan pemantauan internal terhadap penerapan program APU untuk aset kripto dilakukan oleh manajemen penyelenggara perdagangan aset kripto. Hal ini bertujuan untuk mengelola dan memitigasi risiko secara lebih mendalam serta meningkatkan penerapan program APU di dalam ekosistem perdagangan aset kripto. Pengawasan dan pemantauan internal ini paling sedikit meliputi: (1) Pengawasan aktif direksi dan dewan komisaris; (2) Kebijakan dan prosedur; (3) Pengendalian internal; (4) Sistem informasi manajemen; dan (5) Sumber daya manusia dan pelatihan. Pemaparan dari masing-masing komponen tersebut adalah sebagai berikut:

1. **Pengawasan Aktif Direksi dan Dewan Komisaris**

   Direksi dan dewan komisaris penyelenggara perdagangan aset kripto memiliki peranan masing-masing dalam pengawasan penerapan program APU sehingga terdapat perbedaan tugas dan tanggungjawab antara direksi dan dewan komisaris yang disajikan pada Tabel 4.9.

Tabel 4.9 Perbedaan Tugas dan Tanggungjawab Pengawasan antara Direksi dan Dewan Komisaris

No.	Tugas dan Tanggungjawab Pengawasan	Direksi	Dewan Komisaris
1.	Pengawasan, pengelolaan, dan mitigasi risiko TPPU	Memberikan persetujuan yang bersifat teknis pelaksanaan.	Memberikan persetujuan yang bersifat strategis pelaksanaan.
2.	Kebijakan dan prosedur tertulis mengenai penerapan program APU	Memastikan program APU dapat diterapkan dalam berbagai keadaan, responsif terhadap perkembangan produk dan teknologi, serta dapat mendeteksi modus pencucian uang.	a. Memberikan persetujuan atas penerapan program APU yang diajukan oleh direksi; b. Melakukan pengawasan atas pelaksanaan tugas direksi dalam penerapan program APU; c. Memastikan struktur organisasi memadai untuk penerapan program APU; d. Mengagendakan pembahasan program penerapan APU dengan direksi.

Sumber: Peneliti, Diolah

Secara umum, dapat dikatakan bahwa direksi penyelenggara perdagangan aset kripto bertanggungjawab atas ruang lingkup teknis pelaksanaan, sedangkan dewan komisaris penyelenggara perdagangan aset kripto bertanggungjawab atas ruang lingkup strategis pelaksanaan. Pemisahan dan perbedaan tugas ini bertujuan untuk meningkatkan efektifitas penerapan program APU dalam ekosistem perdagangan aset kripto.

2. Kebijakan dan Prosedur

Adanya kebijakan dan prosedur sebagai salah satu bentuk pengawasan dan pemantauan internal terhadap penerapan program APU untuk aset kripto bertujuan untuk memastikan bahwa penyelenggara perdagangan aset kripto memiliki kebijakan dan prosedur yang telah disetujui oleh direksi dan dewan komisaris. Kebijakan dan prosedur tersebut harus berkaitan dengan penerapan *risk based approach*, *know your customer*, dan *transaction monitoring* serta kebijakan dan prosedur yang berkaitan dengan pelaporan atas transaksi mencurigakan. Tabel 4.10 menunjukkan rincian kebijakan dan prosedur yang harus dimiliki oleh penyelenggara perdagangan aset kripto.

Tabel 4.10 Kebijakan dan Prosedur Penerapan Program Anti-Pencucian Uang untuk Aset Kripto

No.	Aktivitas Penerapan Anti-Pencucian Uang	Kebijakan dan Prosedur
1.	*Risk Based Approach*	Pengelolaan risiko pencucian uang yang berkelanjutan.
2.	*Know your Customer*	a. Identifikasi dan verifikasi nasabah; b. Identifikasi dan verifikasi *beneficial ownership*; c. Penutupan hubungan usaha atau penolakan transaksi; d. Pentatausahaan proses CDD.
3.	*Transaction Monitoring*	a. Pemeliharaan data secara akurat yang terkait dengan transaksi nasabah; b. Pengkinian dan pemantauan transaksi.
4.	Pelaporan	a. Pelaporan kepada pejabat senior, direksi, dan dewan komisaris; b. Pelaporan kepada PPATK.

Sumber: Peneliti, Diolah

3. Pengendalian Internal

Pengendalian internal ini bertujuan untuk mendeteksi kelemahan dan penyimpangan dari penerapan program APU yang dilakukan secara independen

dan berkala untuk memastikan efektivitas penerapan program APU dalam ekosistem perdagangan aset kripto. Pengendalian internal ini harus meliputi:

a. Penunjukkan pejabat yang bertanggungjawab dalam penerapan program APU;
b. Pemantauan khusus terhadap kegiatan operasional yang berpotensi tinggi, baik dari nasabah, produk, wilayah geografis, dan atau hal lain yang dinilai rentan dan berpotensi berkaitan dengan transaksi mencurigakan;
c. Penyampaian informasi yang cepat dan tepat jika terdapat indikasi atau dugaan terkait TPPU, inisiatif kepatuhan, kekurangan terkait kepatuhan, tindakan korektif diambil, dan laporan atas aktivitas mencurigakan;
d. Penerapan kebijakan, prosedur, dan kontrol atau uji tuntas nasbah atau CDD;
e. Penyediaan kontrol yang memadai bagi pelanggan atau nasabah, transaksi, dan produk berisiko tinggi; dan
f. Pengujian terhadap efektivitas pelaksanaan program APU dengan mengambil sampel secara acak *(random sampling)* dan melakukan pendokumentasian atas pengujian yang dilakukan.

4. Sistem Informasi Manajemen

Sistem informasi manajemen sebagai salah satu bagian dalam pengawasan dan pemantauan internal terhadap penerapan program APU untuk aset kripto ditujukan untuk mengidentifikasi, menganalisa, memantau, dan menyediakan laporan secara efektif mengenai karakteristik pelanggan atau nasabah serta transaksi yang dilakukannya sehingga sistem informasi manajemen harus dapat menyimpan data dan informasi nasabah secara akurat, lengkap, dan terkini,

termasuk bidang usaha serta negara dimana nasabah bertempat dan atau melakukan transaksi.

5. Sumber Daya Manusia dan Pelatihan

Dalam rangka meningkatkan efekktivitas penerapan program APU maka diperlukan sumber daya manusia (SDM) yang memiliki kompetensi di bidang pencucian uang, khususnya pencucian uang yang melibatkan aset kripto. Untuk dapat mencapai hal tersebut maka penyelenggara perdagangan aset kripto harus melakukan penyaringan SDM serta melakukan pengembangan SDM melalui pelatihan yang dilakukan secara berkesinambungan. Proses penyaringan SDM dilakukan melalui *pre-empolyee screening* dengan menerapkan prinsip *know your employee* (KYE) yang berpedoman pada ketentuan penerapan strategi *anti-fraud*. Prinsip KYE mencakup pengenalan dan pemantauan profil, perilaku, dan gaya hidup calon karyawan dan atau karyawan. Sedangkan untuk pengembangan SDM, penyelenggara perdagangan aset kripto harus menyelenggarakan pelatihan bagi para pegawai mengenai:

a. Penerapan dan ketentuan peraturan perundang-undangan yang terkait dengan program APU;
b. Teknik, metode, dan tipologi pencucian uang;
c. Kebijakan dan prosedur penerapan program APU untuk aset kripto serta tanggungjawab pegawai dalam mencegah dan memberantas pencucian uang yang melibatkan penggunaan aset kripto.

4.1.5.2 Pengawasan dan Pemantauan Eksternal

Pengawasan dan pemantauan eksternal terhadap perdagangan aset kripto beserta penerapan program APU dilakukan oleh Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) dan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). Keduanya memiliki peranan masing-masing dalam mengawasi dan memantau penerapan APU dalam perdagangan aset kripto di Indonesia.

1. **Badan Pengawas Perdagangan Berjangka Komoditi**

   Badan Pengawas Perdagangan Berjangka Komoditi atau Bappebti adalah lembaga pemerintah yang memiliki tugas pokok untuk melakukan pembinaan, pengaturan, pengembangan, dan pengawasan terhadap perdagangan berjangka, salah satunya adalah perdagangan aset kripto. Dalam hal perdagangan aset kripto beserta penerapan program APU dalam ekosistem perdagangan aset kripto, maka Bappebti memiliki peran sebagai berikut:

   a. **Penerima Laporan**

      Untuk mengawasi dan memastikan bahwa penerapan program APU dilaksanakan dalam ekosistem perdagangan aset kripto maka Bappebti mewajibkan penyelenggara perdagangan aset kripto dan atau pedagang aset kripto untuk melaporakan setiap transaksi yang mencurigakan kepada Bappebti. Laporan transaksi mencurigakan ini dilaksanakan berdasarkan aktivitas *transaction monitoring*, *know your customer*, dan *risk based approach* yang dilakukan secara berkesinambungan.

b. Pemberi Sanksi

Bappebti memiliki hak untuk memberi sanksi kepada penyelenggara perdagangan aset kripto dan atau pedagang aset kripto jika tidak mengikuti ketentuan program APU yang telah ditetapkan oleh Bappebti. Pemberian sanksi diberikan berdasarkan jenis dan tingkat pelanggaran yang dilakukan oleh penyelenggara perdagangan aset kripto dan atau pedagang aset kripto. Sanksi yang diberikan berupa:

1) Peringatan tertulis;
2) Denda dengan membayar sejumlah uang tertentu;
3) Pembekuan atau pencabutan kegiatan usaha;
4) Pembekuan atau pencabuatan izin;
5) Pembatalan persetujuan.

2. Pusat Pelaporan dan Analisis Transaksi Keuangan

Pusat Pelaporan dan Analisis Transaksi Keuangan atau PPATK adalah lembaga independen yang berperan sebagai *financial intelligence unit* yang dibentuk dalam rangka mencegah TPPU. Untuk itu, PPATK berhak mendapatkan laporan dari penyelenggara perdagangan aset kripto dan atau pedagang aset kripto mengenai transaksi mencurigakan berdasarkan aktivitas *transaction monitoring*, *know your customer*, dan *risk based approach* yang telah dilakukan. Selanjutnya, laporan tersebut menjadi tanggungjawab dan akan ditindaklanjuti oleh PPATK sebagaimana peraturan perundang-undangan mengenai pemberantasan tindak pidana pencucian uang dan pendanaan terorisme.

4.1.6 Diskusi Umum

Saat ini, pertumbuhan mata uang kripto *(cryptocurrency)* bersifat global, negara-negara besar, seperti: Amerika Serikat, Inggris, Jerman, Australia, dan Jepang menjadi pusat utama untuk pertukaran aset virtual (Kirkpatrick *et al.*, 2021). Di Indonesia, pertumbuhan pelanggan atau investor aset virtual (kripto) dalam kurun waktu tiga tahun terakhir terus meningkat. Tercatat per Oktober 2023, jumlah pelanggan aset kripto sebanyak 18,06 Juta dengan nilai transaksi selama tahun 2023 sebesar Rp 104,9 Triliun (Tempo, 2023). Regulasi aset virtual menjadi hal penting bagi regulator karena aset virtual termasuk ke dalam klasifikasi instrumen investasi paling berisiko (Kirkpatrick *et al.*, 2021), baik risiko kerugian yang mengancam investor maupun risiko pencucian uang yang mengancam hukum.

Penelitian ini mengungkapkan proses pencegahan pencucian uang yang melibatkan aset virtual *(crypto laundering)* berdasarkan regulasi yang berlaku di Indonesia. Berdasarkan analisis isi *(content analysis)* ditemukan pengaturan dalam penggunaan aset virtual (kripto) dan proses pencegahan *crypto laundering.*

Di Indonesia, penggunaan aset virtual (kripto) hanya terbatas pada perdagangan di bursa berjangka *(trading)* dan bukan sebagai alat tukar. Pembatasan penggunaan ini sejalan dengan regulasi yang berlaku di Jerman. Di Jerman, penggunaan aset kripto hanya diizinkan untuk diperdagangkan *(trading)* dan tidak berlaku sebagai alat tukar (Kirkpatrick *et al.*, 2021). Pengaturan perdagangan aset kripto di Jerman menjadi tugas dan tanggungjawab Otoritas Pengawas Keuangan Federal (BaFin/*Bundesanstalt für Finanzdienstleistungsaufsicht)* sebagai regulator terpusat *(centralized regulator)*. Demikian juga di Inggris dan Jepang, pengaturan

perdagangan aset virtual menjadi tugas dan tanggungjawab Otoritas Perilaku Keuangan (FCA/*Financial Conduct Authority*) dan Badan Jasa Keuangan Jepang (JFSA/*Japan's Financial Service Authority*). Sementara di Indonesia—sampai pada saat penelitian ini ditulis—ditemukan bahwa pengaturan perdagangan aset virtual masih menjadi tugas dan tanggungjawab Bappebti (Badan Pengawas Perdagangan Berjangka Komoditi). Jika berkaca pada Jerman, Inggris, dan Jepang maka seharusnya pengaturan perdagangan aset virtual di Indonesia menjadi tugas dan tanggungjawab Otoritas Jasa Keuangan (OJK). OJK memiliki fungsi untuk menyelenggarakan sistem pengaturan dan pengawasan terintegrasi terhadap seluruh kegiatan di sektor jasa keuangan, sehingga seluruh kegiatan yang berkaitan dengan perdagangan aset virtual (kripto) seharusnya berada di bawah pengaturan dan pengawasan OJK.

Adapun dalam hal yang berkaitan dengan pencegahan pencucian uang yang melibatkan aset virtual, temuan penelitian mengungkapkan bahwa proses pencegahan di Indonesia dilakukan dengan melaksanakan KYC *(know your customer)* dan pemantauan transaksi *(transaction monitoring)*. Keduanya diterapkan dengan mengacu pada kebijakan pendekatan berbasis risiko *(risk-based approach)*, sehingga organisasi (FinTech *crypto*) harus melakukan penilaian risiko *(risk assessment)*. Temuan ini sejalan dengan temuan proses pencegahan *crypto laundering* di beberapa negara lain, seperti Inggris dan Bermuda (Kirkpatrick *et al*., 2021). Secara umum, regulasi yang berlaku di Indonesia, Inggris, dan Bermuda mengatur pencegahan *crypto laundering* yang harus dilaksanakan melalui proses

risk assessment, KYC, dan *transaction monitoring*. Namun, jika dibandingkan secara khusus maka terdapat perbedaan regulasi dari ketiga negara tersebut.

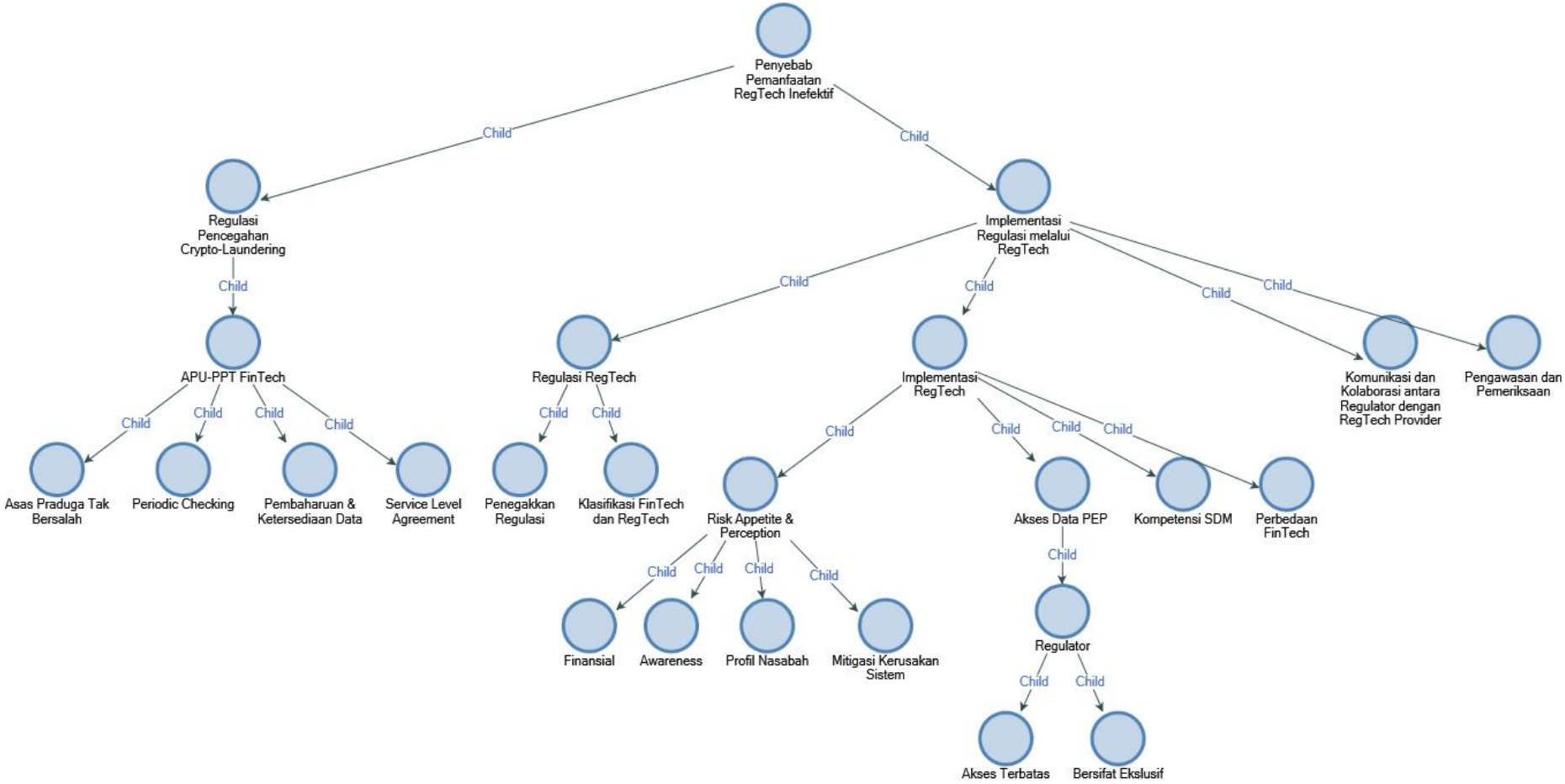
Di Inggris, edukasi dan pelatihan terhadap SDM yang berkaitan langsung dengan pencegahan *crypto laundering* menjadi bagian dari regulasi mekanisme pencegahan *crypto laundering* (Kirkpatrick *et al*., 2021). Sementara di Indonesia, hal tersebut belum menjadi bagian dari regulasi. Saat ini, regulasi pencegahan *crypto laundering* masih mengatur sistem secara teknis dan belum mengatur mengenai SDM yang terlibat. Regulasi hanya mengatur mengenai syarat dalam pemilihan SDM melalui proses KYE *(know your employee)* yang dilaksanakan sebelum SDM melakukan perikatan kerja dengan organisasi (FinTech *crypto*). Perbedaan regulasi terkait dengan edukasi dan pelatihan SDM tersebut didukung oleh data primer yang diperoleh melalui wawancara, bahwa tidak adanya peran regulasi dan regulator dalam pengelolaan SDM berimplikasi pada rendahnya tingkat kesadaran *(awareness)* terhadap risiko *crypto laundering*.

Sedangkan di Bermuda, regulasi mengharuskan organisasi untuk melakukan pengujian berkala terhadap prosedur pencegahan *crypto laundering* yang dimilikinya, apakah prosedur tersebut masih relevan dan memadai dalam menghadapi setiap permasalahan yang ditemukan (Kirkpatrick *et al*., 2021). Di Indonesia, hal tersebut belum terdapat dalam regulasi. Hal ini didukung dengan temuan dari data primer, bahwa tidak adanya ketentuan mengenai peninjauan atau pemeriksaan berkala menjadi kekurangan yang melemahkan regulasi pencegahan *crypto laundering*.

Penerapan regulasi yang berlaku di Inggris dan Bermuda dapat memberikan wawasan kepada regulator dan para pihak yang terlibat, bahwa regulasi yang saat ini berlaku di Indonesia masih perlu dikaji dan dioptimalkan kembali karena regulasi yang aman seharusnya dapat mencakup seluruh elemen yang berkaitan dengan pencegahan *crypto laundering* serta dapat memperkirakan peristiwa yang mungkin terjadi di masa mendatang (McCarthy, 2022).

4.2 Penyebab Pemanfaatan RegTech di Indonesia Inefektif

Berdasarkan hasil analisis data dengan menerapkan *open coding*, diketahui bahwa penyebab tidak efektifnya pemanfaatan RegTech dalam mencegah *crypto laundering* di Indonesia terbagi atas dua kategori yang saling berkaitan, yaitu adanya celah pada regulasi pencegahan *crypto laundering* serta dalam proses implementasi regulasi tersebut melalui RegTech. Implementasi regulasi melalui RegTech terbagi ke dalam empat tema utama, yaitu: (1) Regulasi Pemanfaatan RegTech; (2) Implementasi RegTech; (3) Komunikasi dan Kolaborasi antara Regulator dengan RegTech *Provider*; dan (4) Pengawasan dan Pemeriksaan dari Regulator. Dalam hal ini juga ditemukan beberapa subjek yang berperan serta berkaitan dengan pencegahan *crypto-laundering* dan pemanfaatan RegTech, yaitu regulator sebagai penyusun regulasi, FinTech *crypto* sebagai *crypto exchanger*, dan RegTech *provider* yang berperan dalam implementasi RegTech pada FinTech *crypto*. Gambar 4.4 menunjukkan hasil analisis berupa *report map* mengenai penyebab tidak efektifnya pemanfaatan RegTech yang diolah melalui *software* NVivo 12. Penyusunan tema dalam *report map* tersebut juga didasarkan pada referensi dan jumlah coding yang disajikan melalui Lampiran 8.



Gambar 4.4 *Report Map* Penyebab Pemanfaatan RegTech di Indonesia Inefektif

Sumber: NVivo 12

4.2.1 Regulasi Pencegahan *Crypto Laundering*

Regulasi pencegahan *crypto-laundering* mengatur dan menetapkan kerangka kerja yang harus diterapkan oleh FinTech *crypto* dalam mencegah pencucian uang yang melibatkan nasabah melalui FinTech yang dikelolanya. Menurut P2 yang memiliki kompetensi dan keahlian dalam bidang AML *Operating System*, FinTech *crypto* di Indonesia sangat memungkinkan untuk dijadikan sebagai sarana pencucian uang oleh para pelaku. Namun, sebagian besar FinTech *crypto* tidak memiliki prosedur anti-pencucian uang (APU) sehingga penerapan mekanisme pencegahan pencucian uang untuk aset kripto menjadi tidak efektif.

Mendukung pernyataan tersebut, P1—yang juga memiliki kompetensi dan keahlian dalam bidang AML *Operating System*—menyebutkan bahwa kurangnya kesadaran FinTech *crypto* mengenai berbagai risiko pencucian uang yang melibatkan aset kripto menjadi hal yang dapat memperburuk penerapan mekanisme APU untuk aset kripto di Indonesia. Berdasarkan hasil analisis data dengan pengaplikasian *focused coding*, diketahui bahwa celah atau kekurangan dalam regulasi pencegahan *crypto laundering* terdapat pada asas praduga tak bersalah, *periodic checking*, pembaharuan dan ketersediaan data, dan SLA *(service level agreement).*

4.2.1.1 Asas Praduga Tak Bersalah

Menurut P1, asas praduga tak bersalah menjadi kedilemaan yang dihadapi oleh para FinTech *crypto* dalam menghadapi nasabah dan atau calon nasabah yang memiliki latar belakang berisiko tinggi *(high risk profile)*. Hal ini disampaikan dalam wawancara:

> "… karena kita kalau misalnya melakukan itu, melanggar hukum juga karena kita langsung *judges* gitu dan dia bisa *sue* perusahaan itu juga karena belum ada kekuatan hukum tetap tapi sudah di-*treat* ini, serba salah jadinya."

Asas praduga tak bersalah sebagai salah satu asas hukum yang menetapkan bahwa seseorang dianggap tidak bersalah sampai terdapat bukti yang dapat membuktikan kesalahannya. Ketika putusan pengadilan belum ditetapkan atau belum memiliki kekuatan hukum maka nasabah FinTech *crypto* yang terdeteksi sebagai nasabah berisiko tinggi tetap tidak dapat dipisahkan *(off boarding)* dari aktivitasnya di FinTech tersebut. Sejalan dengan Wronka (2022c), perlakuan kepada nasabah berisiko tinggi jika disamakan dengan perlakuan terhadap nasabah daftar hitam maka dapat melanggar independensi dan atau *self-determination* dari nasabah tersebut. Namun demikian, nasabah dan atau calon nasabah dengan latar belakang profil berisiko tinggi memiliki potensi yang lebih besar untuk melakukan *crypto laundering*. Implikasi dari hal ini, maka penting bagi regulator untuk meninjau dan mengkritisi kembali regulasi anti-pencucian uang dalam ekosistem aset virtual. Regulator perlu memperkirakan serta mensimulasikan berbagai skenario dalam kasus *crypto laundering* sehingga dapat memperkirakan regulasi yang tepat dan mengakomodir kebutuhan pencegahan *crypto laundering* di Indonesia. Sebagai bagian dari aktivitas pencegahan, regulasi yang berlaku harus dapat mengantisipasi dan memperkirakan peristiwa yang berpotensi terjadi di masa yang akan datang (McCarthy, 2022).

4.2.1.2 *Periodic Checking*

Periodic checking tidak diatur dalam regulasi pencegahan *crypto laundering*. Hal ini disampaikan oleh P1 dalam wawancara:

> "Jadi periode ini sebenarnya tidak ada Undang-Undang-nya kalau di Indonesia secara spesifik berapa lama kamu harus *periodic checking*."

Periodic checking merupakan bagian dari proses penilaian risiko *(risk assessment)* yang bertujuan untuk memeriksa dan memperbaharui profil risiko dari masing-masing nasabah FinTech *crypto* karena profil risiko dari masing-masing nasabah dapat berubah seiring dengan aktivitas keuangan yang dilakukannya. Di Indonesia, mayoritas perusahaan FinTech *crypto* melakukan *periodic checking* sebanyak satu kali dalam periode waktu 3 bulan atau 6 bulan. Periode waktu ini relatif lama karena mengingat bahwa dalam mekanisme pencegahan *crypto laundering*, hasil pemetaan risiko nasabah menjadi dasar yang digunakan dalam aktivitas KYC *(know your customer)* dan *transaction monitoring.* Meiryani (2023) menyebutkan bahwa kebijakan mengenai penilaian risiko *(risk assessment)* sangat berpengaruh dalam penguatan regulasi pencegahan *crypto laundering.* Dalam hal ini, maka regulator perlu merinci kembali berbagai kebijakan dalam penilaian risiko yang berpotensi melemahkan dan menghambat proses penilaian risiko. Hambatan dan kelemahan dalam proses penilaian risiko berimplikasi pada rendahnya keakuratan hasil dari proses KYC dan *transaction monitoring*.

4.2.1.3 Pembaharuan dan Ketersediaan Data

Menurut P2, FinTech *crypto* dan atau RegTech *Provider* tidak dapat memastikan kapan dilakukannya pembaharuan data mengenai status risiko nasabah pada RegTech yang digunakan oleh FinTech. Hal ini disebabkan karena pembaharuan data profil risiko tersebut bergantung dengan ketersediaan data mengenai profil keuangan nasabah yang dikeluarkan oleh regulator. Disebutkan oleh P2 melalui wawancara yang sudah dilakukan:

> "Jadi bisa saja minggu depan ada, bisa saja minggu depan tidak ada, bulan depan tidak ada, tapi besok langsung ada."

> "… tergantung ketersediaan data mereka (regulator), tergantung *update* yang tersedia dari mereka (regulator)."

Selain ketersediaan dan pembaharuan data yang dikeluarkan oleh regulator tidak dapat dipastikan, menurut P3—yang memiliki kompetensi dan keahlian di bidang AML *Operating System*—data profil keuangan nasabah yang dikeluarkan oleh regulator tersebut juga belum memenuhi kebutuhan data yang diperlukan dalam implementasi pemanfaatan RegTech untuk mencegah *crypto laundering*. Hal ini disebabkan karena data yang dikeluarkan oleh regulator hanya terbatas pada daftar nasabah yang berisiko tinggi saja serta tidak memasukkan data anggota keluarga dan kerabat dari nasabah berisiko tinggi tersebut (*relative close associate*/RCA).

Update atau pembaharuan dan ketersediaan data mengenai profil keuangan nasabah menjadi tanggung jawab regulator, dalam hal ini adalah Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). Tidak terstrukturnya pembaharuan data profil keuangan tersebut diduga karena tidak ada regulasi atau kebijakan yang mengharuskan PPATK untuk melakukan pembaharuan data dalam kurun waktu tertentu. Demikian juga dengan ketersediaan data RCA dari calon nasabah dan atau nasabah, menurut Ryan dan Stahl (2021) pemberian data tersebut berpotensi melanggar pedoman etika penggunaan teknologi yang sangat mengutamakan privasi.

Tentunya, hal ini berimplikasi pada kebijakan pencegahan *crypto laundering*. Perlu adanya sinergisitas peran antar-regulator, maka dari itu dibutuhkan peran Bappebti sebagai pembuat kebijakan yang dilengkapi dengan peran dari PPATK.

Dalam hal kebijakan, Bappebti perlu mengatur pengelolaan data nasabah dengan memperhatikan periode waktu pembaharuan data tanpa melanggar aspek etika dan privasi dalam penggunaan teknologi. Bappebti juga perlu mengkoordinasikan kebijakan tersebut kepada PPATK sebagai penyedia data nasabah bagi RegTech *provider*.

4.2.1.4 *Service Level Agreement*

Di Indonesia, *Sevice Level Agreement* atau SLA belum diatur, hal ini disampaikan oleh P1:

> "Iya, makannya kalau di luar kan ada regulasi SLA-nya *(Service Level Aggrement)* untuk FinTech-nya karena kalau misalnya FinTech, kan dia menggunakan uang masyarakat yang masuk ke sistemnya dia, pasti ada perlindungan dong dari pemerintahnya. Nah, seberapa perlindungannya kalau misalnya untuk FinTech dengan ukuran tertentu, maksimal *disrupt*-nya segini."

Sevice Level Agreement atau SLA merupakan kesepakatan para pihak yang berkepentingan untuk menjalankan kewajibannya masing-masing berdasarkan regulasi yang berlaku. Di beberapa negara Asia Tenggara, khususnya Singapura, pengaturan SLA pada FinTech sudah masif dilakukan. Sedangkan di Indonesia, belum masifnya pengaturan SLA dalam ekosistem FinTech *crypto* atau ekosistem perdagangan aset kripto diduga karena regulator masih berfokus pada perbankan digital. Di sisi lain, FinTech *crypto* di Indonesia relatif baru bertumbuh, sehingga ekosistem yang terbentuk belum komprehensif. Namun, dalam hal pengaturan SLA, seharusnya regulator dapat responsif dan adaptif dalam penyusunan kebijakan. Tidak berbeda dengan perbankan digital, FinTech *crypto* pun menggunakan dana masyarakat sehingga pengaturan SLA seharusnya dapat dijadikan sebagai prioritas.

4.2.2 Implementasi Regulasi Pencegahan *Crypto Laundering* melalui RegTech

RegTech merupakan sistem yang membantu organisasi dalam mengimplementasikan mekanisme atau prosedur dari regulator yang bersifat wajib *(mandatory)*. Pemanfaatan RegTech bertujuan untuk menciptakan efisiensi dan efektivitas organisasi dalam menjalankan kewajiban dan atau kepatuhannya terhadap regulator. RegTech memastikan bahwa setiap aktivitas yang dilakukan oleh nasabah di dalam FinTech *crypto* dapat dipertanggungjawabkan dan telah memenuhi kepatuhan terhadap regulasi yang berlaku.

Dalam mekanisme pencegahan *crypto-laundering*, RegTech berperan besar untuk meminimalisir adanya kelalaian manusia *(human error)* dalam proses pencegahan *crypto-laundering*. Pemanfaatan RegTech ini sudah dianjurkan oleh Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) melalui regulasi yang ditetapkannya sebagaimana pemaparan pada sub-bab 4.2 mengenai mekanisme pencegahan *crypto-laundering*. Namun, dalam penerapannya terdapat beberapa kendala yang menyebabkan pemanfaatan RegTech menjadi tidak efektif. Berdasarkan hasil analisis data dengan pengaplikasian *focused coding* diketahui bahwa penyebab tersebut diklasifikasikan ke dalam empat tema utama, yaitu: (1) Regulasi Pemanfaatan RegTech; (2) Implementasi RegTech; (3) Komunikasi dan Kolaborasi antara Regulator dengan RegTech *Provider*; dan (4) Pengawasan dan Pemeriksaan dari Regulator.

4.2.2.1 Regulasi Pemanfaatan RegTech

4.2.2.1.1 Penegakkan Regulasi

Pemanfaatan RegTech sebagai teknologi yang digunakan dalam membantu pencegahan *crypto laundering* sudah dianjurkan oleh Bappebti selaku regulator. Namun, ketegasan dan urgensi dalam penegakkan regulasi tersebut masih belum terlihat. Hal ini disampaikan oleh P2:

> "Itu setelah mengeluarkan Undang-Undang tapi tindak tegasnya, *penalty*-nya itu belum ada."
>
> "Memang disebutkan, tapi prakteknya tidak ada sanksi, tidak ada urgensi di sana."
>
> "… karena yang sangat mempengaruhi implementasi adalah kurang tegasnya *penalty* atau sanksi dari regulator terhadap FinTech *player*."

Hal tersebut juga didukung dengan pernyataan dari P3:

> "*Sense of urgency*-nya balik lagi ke regulator, Mbak. Mereka nge-*push* atau tidak? Kalau tidak nge-*push*, ya *"Mending saya screening-nya lewat Google aja"*, gitukan."

Sebelum mengimplementasikan RegTech, FinTech *crypto* harus terlebih dahulu memiliki mekanisme pencegahan *crypto-laundering*. Namun, P2 menyatakan bahwa tidak terdapatnya sanksi dan atau tindak tegas dari regulator terhadap pemanfaatan RegTech mempengaruhi kesadaran dan perspektif para FinTech *crypto* terhadap urgensi dalam memiliki mekanisme pencegahan *crypto-laundering* berbasis sistem.

Di sisi lain, P1 menyampaikan bahwa:

> "… karena untuk mereka untuk pakai RegTech ada satu investasi dan investasi ini biasanya tidak kecil, kan. Nah, kalau misalnya kita lihat FinTech yang kecil ya fokusnya *growth*."

FinTech *crypto* menghadapi tantangan tersendiri dalam mengimplementasikan RegTech. Bagi FinTech *crypto* yang baru berkembang, tujuan utamanya adalah meningkatkan pertumbuhan usaha *(growth)* sehingga aspek lain yang tidak berhubungan langsung dengan *growth* perusahaan dan membutuhkan biaya—seperti: aspek kepatuhan melalui pemanfaatan RegTech—relatif tidak menjadi bagian dari prioritas atau tujuan utama.

Melengkapi pemaparan tersebut, P2 dan P3 menyampaikan dalam wawancara:

> "… bagi mereka yang merasa ini belum jadi prioritas mereka, mereka itu tidak adain *budget compliance*-nya di situ gitu, *budget compliance*-nya terlalu kecil biasanya karena tidak ada urgensi di sana." *(P2)*

> "… andaikan ada urgensi di sana, kita yakin *compliance budget* masing-masing mereka akan ditambahkan. Balik lagi ke *budgeting*-nya mereka, karena tidak ada urgensinya itu." *(P2)*

> "Mereka akan menalar lagi, *"Urgent gak, sih? Kayaknya kalau tidak dipakai, tidak diapa-apain, deh."* " *(P2)*

> "… tidak ditegur juga oleh regulatornya." *(P3)*

> "… tidak ada denda atau sanksi." *(P3)*

Meskipun mayoritas FinTech *crypto* saat ini masih berada pada tahap bertumbuh *(growth)*, pemanfaatan RegTech tetap bergantung dengan urgensi dan tindak tegas regulator terhadap regulasi yang sudah ditetapkannya. Jika terdapat urgensi dan penegasan dari regulator terhadap regulasi yang sudah ditetapkan maka para FinTech *player* berpotensi untuk menaikkan anggaran kepatuhannya, salah satunya anggaran untuk pemanfaatan RegTech. Menurut P2, kurangnya tindak tegas dari regulator terhadap regulasi yang sudah ditetapkannya dibuktikan dengan belum dilaksanakannya *random audit compliance program* terhadap FinTech *crypto*

secara periodik yang berimplikasi pada tingkat kesadaran para FinTech crypto terhadap kebijakan pemanfaatan RegTech.

Keberhasilan dari implementasi RegTech pada FinTech *crypto* di Indonesia bergantung dengan penetapan dan ketegasan atas penegakkan regulasi yang mengaturnya. Penetapan regulasi dan pedoman yang komprehensif dapat mendukung implementasi RegTech yang lebih baik (Sarabdeen, 2023). Jika merujuk pada penelitian yang dilakukan oleh Kurum (2020) maka diketahui bahwa dalam mempengaruhi institusi keuangan untuk mengimplementasikan RegTech diperlukan peran penting regulator melalui regulasi yang ditetapkannya. Implikasinya, maka diperlukan peran regulator dalam penegakkan kebijakan secara tegas dan nyata untuk mendorong pemanfaatan RegTech pada FinTech *crypto*. Dapat dikatakan bahwa peran regulator terhadap FinTech *crypto* secara *'top-down'* diperlukan untuk mencapai konsistensi dalam penegakkan regulasi (McCarthy, 2022).

4.2.2.1.2 Klasifikasi FinTech dan RegTech

Hal lain yang berkaitan dengan regulasi sebagai penyebab tidak efektifnya pemanfaatan RegTech di Indonesia menurut P1, yaitu belum adanya regulasi serta sinergisitas dalam regulasi yang mengklasifikasikan FinTech dan regulasi yang mengklasifikasikan RegTech. Kedua hal tersebut perlu diklasifikasikan kembali berdasarkan ukuran perusahaan dan volume transaksi sehingga pemanfaatan RegTech dapat diintegrasikan dan diselaraskan berdasarkan ukuran dan volume transaksi pada FinTech *crypto*.

P1 juga menyebutkan dalam wawancara:

> "… belum secara terperinci sih karena ini *regulation* yang dibuat kan untuk mencakup semua, baik yang kecil maupun yang besar. Nah, kecil besarnya FinTech ini kalau di internasional sudah dibedakan secara regulasinya karena kita tidak bisa menggunakan satu regulasi untuk ketok rata semua …"

> "… karena pelaporan untuk perusahaan yang besar ya, sama FinTech yang sekarang nih yang masih bertumbuh atau masih *just introduce* nih di Indonesia, *totally* berbeda karena ya yang sudah besar kan mereka sudah punya satu standar sendiri kan ya, dan kalau yang bertumbuh, ya mereka banyak yang bingung harus gimana."

Pengklasifikasian FinTech dan RegTech dapat didasarkan pada regulasi internasional. Regulasi internasional sudah mengklasifikasikan RegTech dan FinTech berdasarkan ukuran dan volume transaksinya karena satu regulasi saja tidak dapat digunakan secara merata untuk semua ukuran FinTech dan RegTech. Tentunya, dalam implementasi RegTech terdapat perbedaan antara implementasi pada FinTech yang berukuran besar dengan FinTech yang masih bertumbuh, terutama dalam hal pelaporan hasil dari setiap proses pencegahan *crypto laundering*.

Dalam kaitannya dengan regulasi dan prosedur di Indonesia, P1 menyebutkan dalam wawancara:

> "Kan kalau misalnya saya sebagai *user* yang *on boarder*, saya akan dicek *against database* ini, seberapa valid data ini. Kalau misal data ini tidak valid dan menyebabkan saya *off board*, siapa yang bertanggungjawab? Nah ini yang jadi masalah karena tidak ada *framework*-nya. Jadi belum tahu nih kalau misalnya ada apa yang terjadi, siapa yang bertanggung jawab, siapa yang akan memberikan pertanggung jawaban."

Belum terdapatnya regulasi yang mengklasifikasikan RegTech dan FinTech serta kerangka kerja *(framework)* yang dapat dijadikan acuan oleh RegTech *provider* menyebabkan adanya kerancuan di antara RegTech *provider* ketika melakukan implementasi RegTech pada FinTech *crypto*. Perbedaan utama terdapat pada

cakupan data yang perlu diproses oleh RegTech. Jika cakupan data yang diakomodasi oleh RegTech tidak mencukupi kebutuhan FinTech *crypto* maka berpotensi menghasilkan informasi yang bias (Sarabdeen, 2023). Hal ini menyebabkan implementasi RegTech menjadi terhambat dan tidak komprehensif karena tidak adanya *check and balance*. Maka dari itu, implikasinya berfokus pada kebijakan pemanfaatan RegTech. Regulator perlu menyusun kebijakan yang mengklasifikasikan RegTech berdasarkan klasifikasi pada FinTech *crypto* untuk menghindari bias dalam cakupan data yang berpotensi pada akurasi informasi yang dihasilkan.

4.2.2.2 Implementasi RegTech

Penyebab kedua dari tidak efektifnya pemanfaatan RegTech dalam mencegah *crypto laundering* di Indonesia, yaitu adanya kendala ketika RegTech *provider* melakukan implementasi RegTech pada FinTech *crypto*. Berdasarkan temuan penelitian, terdapat empat kendala utama dalam implementasi RegTech pada FinTech *crypto*, yaitu: (1) Perbedaan jenis FinTech yang menyebabkan perbedaan pada RegTech yang diimplementasikan; (2) *Risk appetite and perception* dari FinTech *crypto*; (3) Terbatasnya akses data PEP *(politically exposed person)* yang dihadapi oleh RegTech *provider*; dan (4) Kompetensi SDM pada FinTech *crypto*.

4.2.2.2.1 Perbedaan Jenis FinTech *Crypto*

Menurut P3, perbedaan mendasar dalam implementasi RegTech terletak pada perbedaan volume kebutuhan untuk *screening* calon nasabah. Jumlah calon nasabah dan atau nasabah pada *big size* FinTech lebih luas dan besar jika dibandingkan dengan FinTech yang masih bertumbuh *(small to medium size)*.

Dalam hal ini, P2 juga menyebutkan:

> "… kalau yang sudah *big*, mereka ambil semuanya, mereka implementasikan semuanya."

Implementasi RegTech pada FinTech berukuran besar *(big size)* mencakup semua modul, mulai dari modul *risk profiling*, *know your customer*, sampai pada modul *transaction monitoring*.

Sedangkan pada FinTech yang masih bertumbuh *(small to medium size)*, P2 menyampaikan dalam wawancara:

> "… kalau yang kecil mereka *priority based*, mana yang diprioritaskan terlebih dahulu? Karena ya namanya masih kecil, anggarannya pasti ada yang lebih diprioritaskan dibandingkan *compliance cost*. Jadi mereka pilih, maksudnya seperti "Oh, yang ini dulu nih, yang krusial dulu", mungkin yang *risk profiling* mereka lakukan manual dulu tidak apa-apa, tidak pakai RegTech misalnya. Terus juga misal yang tadi *transaction monitoring* mereka lakukan manual, tapi *watch list name screening*-nya untuk deteksi *high risk profile*-nya mereka langsung implementasi di awal."

Implementasi RegTech pada FinTech yang masih bertumbuh *(small to medium size)* didasarkan pada prioritas kebutuhan karena anggaran untuk biaya kepatuhan *(compliance cost)* relatif masih terbatas. Biasanya, FinTech jenis ini hanya mengimplementasikan satu jenis modul dalam RegTech dan atau hanya menggunakan *database* untuk *watch list name screening* sebagai tahapan awal dalam *risk profiling* saja dan tidak mengimplementasikan RegTech secara komprehensif.

Sebagaimana yang sudah dipaparkan sebelumnya, bahwa tidak efektifnya pemanfaatan RegTech di Indonesia—beberapan di antaranya—disebabkan karena belum adanya regulasi yang mengklasifikasikan RegTech dan FinTech, belum adanya kerangka kerja yang dapat dijadikan acuan ketika melakukan implementasi RegTech, serta belum adanya tindak tegas dari regulator sehingga *compliance cost*

dari FinTech relatif kecil. Hal tersebut berimplikasi pada implementasi RegTech, dimana pemilihan modul pada saat implementasi RegTech yang dilakukan oleh FinTech *crypto* didasarkan pada pertimbangan subjektif FinTech *crypto* dan bukan didasarkan pada pertimbangan regulasi yang berlaku serta pemenuhan kriteria dalam kerangka kerja untuk mencapai hasil yang optimal. Maka penting bagi regulator untuk segera menegakkan regulasi dan atau kerangka kerja yang berkaitan dengan pengklasifikasian RegTech berdasarkan kebutuhan FinTech *crypto*, sehingga RegTech yang diimplementasikan oleh RegTech *provider* tidak didasarkan pada pertimbangan subjektif FinTech *crypto* ataupun RegTech *provider*.

4.2.2.2.2 *Risk Appetite and Perception*

Setiap perusahaan FinTech *crypto* memiliki batasan atau toleransi dan persepsinya masing-masing terhadap risiko sehingga manajemen risiko antara satu FinTech *crypto* dengan FinTech *crypto* lainnya dapat berbeda. Berdasarkan temuan penelitian, perbedaan toleransi dan persepsi FinTech *crypto* terhadap risiko menjadi salah satu kendala dalam implementasi pemanfaatan RegTech. Toleransi dan persepsi terhadap risiko tersebut mempengaruhi beberapa hal yang berkaitan dengan implementasi RegTech, yaitu kesadaran *(awareness)* terhadap risiko, manajemen keuangan FinTech *crypto*, persepsi terhadap profil nasabah, dan mitigasi kerusakan sistem dari FinTech *crypto*.

A. Kesadaran *(Awareness)* terhadap Risiko dan Biaya Kepatuhan

Dalam pencegahan *crypto laundering*, menurut P3, kesadaran FinTech *crypto* terhadap risiko sangat mempengaruhi keputusan dalam pengimplementasian RegTech karena untuk saat ini—sebagaimana yang sudah dipaparkan

sebelumnya—belum terdapat kerangka kerja yang dapat dijadikan acuan dalam pemanfaatan RegTech. Implementasi RegTech bergantung dengan toleransi dan tingkat risiko yang ditetapkan oleh FinTech *crypto* bagi perusahaannya.

Dalam hal ini, P1 dan P2 menyampaikan dalam wawancara:

> "… tapi ya itu *risk appetite*-nya perusahaan juga sih …" *(P1)*

> "… misal kripto, dari sekian banyak mungkin yang pakai hanya satu atau dua, gitu. Yang sadar hanya satu atau dua dari sekian banyak, rasionya terlalu jomplang." *(P2)*

Mayoritas FinTech *crypto* tidak memiliki prosedur anti-pencucian uang yang berbasis sistem. Hal ini dibuktikan dengan rendahnya permintaan dari FinTech *crypto* kepada RegTech *provider* untuk mengimplementasikan RegTech di perusahaannya. Sedangkan beberapa FinTech *crypto* yang sudah mengimplementasikan RegTech, menurut P2, sebagian besar hanya bersifat administratif saja dan bukan didasarkan pada kesadarannya terhadap pencegahan *crypto laundering,* sehingga RegTech tersebut tidak dimanfaatkan sebagaimana tujuannya. Beberapa FinTech *crypto* hanya memiliki lisensinya saja, namun tidak memiliki bukti bahwa RegTech tersebut digunakan.

Terkait dengan kesadaran dari FinTech *crypto*, P2 juga menyampaikan:

> "… bagi mereka yang merasa ini belum jadi prioritas mereka, mereka itu tidak adain *budget compliance*-nya di situ gitu, *budget compliance*-nya terlalu kecil biasanya."

> "… "Kenapa tidak saya *marketing* aja? Saya kan masih *growing*. Kenapa saya tidak *endorse*? Kenapa saya tidak kolaborasi?" …"

Kesadaran FinTech *crypto* akan mempengaruhi persepsi terhadap pengelolaan anggaran kepatuhan melalui implementasi RegTech. FinTech *crypto* relatif lebih mempertimbangkan pengalokasian anggarannya untuk pengembangan usaha

dibandingkan untuk biaya kepatuhan melalui implementasi RegTech. Hal ini juga disampaikan oleh P1:

> "Karena untuk mereka untuk pakai RegTech ada satu investasi dan investasi ini biasanya tidak kecil kan. Nah, kalau misalnya kita lihat FinTech yang kecil ya fokusnya *growth*."
>
> "… karena belum untung."
>
> "… bandingkan dengan *hiring* orang, 10 orang atau 20 orang buat *eye bowling*-in semua."
>
> "Saya ambil contoh implementasi RegTech 200 Juta, terus saya *hiring* 10 orang misalnya, 1 orang 10 Juta per bulan misalnya, nah itu 100 Juta. Sisa 100 Juta-nya bisa pakai untuk *growth*."

Bagi FinTech *crypto*, implementasi RegTech menjadi sebuah investasi sehingga FinTech—terutama FinTech yang baru bertumbuh—mengukur antara biaya yang dikeluarkan *(cost)* dengan manfaat yang didapatkan *(benefit)* dari implementasi RegTech. Perbandingan antara *cost* dan *benefit* tersebut jika menurut perhitungan FinTech *crypto* belum menguntungkan maka FinTech *crypto* cenderung tidak mengimplementasikan RegTech dan lebih berfokus pada pertumbuhan *(growth)* perusahaan. Adapun untuk proses pencegahan pencucian uang, FinTech *crypto* bergantung dengan kemampuan para pegawainya dan tanpa bantuan sistem.

Berdasarkan beberapa penelitian yang sudah dilakukan, para peneliti menemukan bahwa implementasi RegTech berimplikasi pada efisiensi biaya jangka panjang (Sarabdeen, 2023; Meiryani *et al.*, 2022; Kurum, 2020). Implikasi tersebut menimbulkan paradoks, meskipun RegTech meningkatkan efisiensi biaya jangka panjang, namun biaya yang perlu dikeluarkan oleh FinTech *crypto* ketika pertama kali mengimplementasikan RegTech tergolong mahal (Sarabdeen, 2023), sehingga FinTech *crypto*—terutama yang baru bertumbuh—cenderung berfokus untuk

mengembangkan usaha dan mengabaikan fungsi kepatuhan. Diduga, hal tersebut menjadi faktor pendorong—selain kesadaran—bagi FinTech *crypto* dalam pengambilan keputusan untuk mengimplementasikan RegTech.

Sangat dimungkinkan bahwa sebagian besar FinTech *crypto* sudah memiliki kesadaran untuk mengimplementasikan program pencegahan *crypto laundering* melalui RegTech, hanya saja kesadaran tersebut masih dihadapkan pada pertimbangan dalam pengalokasian biaya yang terbatas. Maka penting bagi regulator sebagai *'key player'* untuk memanfaatkan *regulatory sandbox* dalam mengembangkan RegTech yang dapat mempertemukan titik tengah antara kebutuhan regulator dengan sumber daya yang dimiliki oleh FinTech *crypto*. Melalui *regulatory sandbox*, RegTech *provider* dapat memenuhi kebutuhan produk atau layanan RegTech dengan melakukan pengembangan dan pengujian terhadap sistem sebelum sistem tersebut diimplementasikan secara masif (Sarabdeen, 2023). Kemudian, regulator juga perlu melakukan pendekatan yang holistik kepada FinTech *crypto* untuk membangun dan memperkuat kesadaran terhadap risiko *crypto laundering* serta penguatan program pencegahan *crypto laundering* berbasis sistem.

B. Persepsi terhadap Profil Nasabah

Sebelum nasabah melakukan aktivitas keuangannya pada FinTech *crypto (on boarding)* maka FinTech *crypto* melakukan *screening* terlebih dahulu kepada setiap calon nasabah. Tujuannya untuk memeriksa dan memetakan risiko nasabah serta memastikan bahwa nasabah tersebut tidak termasuk ke dalam Daftar Hitam

Nasional (DHN). Terkait dengan penggunaan basis data, P1 menyampaikan dalam wawancara:

> "… kebanyakan perusahaan pada berfikir *sanction list* lah, sudah berfikir satu kiblat yang besarnya, *sanction*. Tapi kan di Indonesia, lokal kan ada *maintain* DTTOT."

Dalam proses *screening* calon nasabah, mayoritas perusahaan FinTech *crypto* hanya menggunakan *sanction list* yang berskala internasional saja sebagai basis data dan relatif tidak menggunakan Daftar Hitam Nasional (DHN) atau Daftar Terduga Terorisme dan Organisasi Terorisme (DTTOT) yang berskala nasional. Menurut P1, hal tersebut dapat meningkatkan potensi FinTech *crypto* untuk menerima calon nasabah berisiko tinggi karena terdapat kemungkinan bahwa calon nasabah sudah terdaftar di DHN, namun belum dilaporkan di *sanction list*.

P1 juga menyampaikan dalam wawancara:

> "… balik lagi, *risk appetite*-nya perusahaan itu. Jadi perusahaan kan sebenarnya dari Tim APU-PPT-nya itu kan biasanya ada satu daftar, kayak satu dokumen, ini loh *risk appetite*-nya saya."

Penggunaan basis data ini bergantung kembali dengan pertimbangan dan *risk appetite* dari FinTech *crypto* karena tidak adanya kerangka kerja yang dapat dijadikan sebagai acuan mengenai batasan risiko yang harus diterapkan oleh FinTech *crypto*. Selanjutnya, P1 menyampaikan:

> "Mungkin ada perusahaan yang langsung sudah lihat dia masuk pengadilan, sudah *off board* "Saya tidak mau *deal* dengan nasabah seperti ini". Mungkin ada perusahaan yang lain tetap *keep*. Balik lagi mereka ada pertimbangannya masing-masing, sih."

Perbedaan *risk appetite* mempengaruhi persepsi FinTech *crypto* terhadap profil nasabah. Hal ini tercermin dari perbedaan tindakan dan perlakuan terhadap nasabah antara satu FinTech *crypto* dengan FinTech *crypto* lainnya. Tentunya, menurut P1,

dampak dari perbedaan penggunaan basis data dan persepsi dari masing-masing FinTech *crypto* tersebut menjadi celah yang mendukung tidak efektifnya pemanfataan RegTech di Indonesia.

Dalam implementasi RegTech, FinTech *crypto* dan RegTech *provider* saling bersinergi sehingga persepsi dan kendala yang dihadapi oleh keduanya saling mempengaruhi. Diduga, perbedaan persepsi di antara FinTech *crypto* ini dipengaruhi oleh kurangnya kerangka kerja *(framework)* yang dapat dijadikan acuan dalam pengelolaan risiko, terutama risiko dan implikasi dari basis data yang digunakan. Dugaan lainnya karena adanya keterbatasan akses data yang diberikan oleh regulator sehingga RegTech *provider* bekerjasama dengan pihak privat di luar Indonesia untuk memperoleh data berskala internasional. Tidak diketahui apakah proses perolehan data tersebut sudah mematuhi prinsip keamanan dan privasi data. Jika tidak mematuhi prinsip keamanan dan privasi data maka perlunya regulator untuk mengatasi hal tersebut. Pentingnya kerangka kerja sebagai acuan yang dapat menyelaraskan persepsi antar-FinTech *crypto* ataupun antara FinTech *crypto* dengan RegTech *provider*. Kerangka kerja tersebut juga harus dapat memberikan batasan yang jelas mengenai perolehan dan penggunaan data agar terhindar dari permasalahan privasi dan penyalahgunaan data.

C. Mitigasi Kerusakan Sistem

Implementasi RegTech tidak terlepas dari adanya risiko gangguan atau kerusakan sistem. Menurut P1, mitigasi risiko gangguan atau kerusakan sistem dari masing-masing perusahaan FinTech *crypto* dapat berbeda karena dipengaruhi oleh

perbedaan *risk appetite* dari masing-masing perusahaan. Selanjutnya, P1 juga menyampaikan:

> "Iya, makannya kalau di luar kan ada regulasi SLA-nya."
>
> "… seberapa perlindungannya kalau misalnya untuk FinTech dengan ukuran tertentu, maksimal *disrupt*-nya segini."

Meskipun *risk appetite* setiap perusahaan berbeda-beda dan berpotensi menurunkan tingkat efektivitas dari pemanfaatan RegTech, namun karena di Indonesia belum terdapat SLA *(Service Level Agreement)* maka acuan dalam mitigasi gangguan dan kerusakan sistem ketika implementasi RegTech masih tetap bergantung dengan *risk appetite* perusahaan.

Diduga, temuan ini terjadi karena regulator belum berfokus pada FinTech *crypto* sehingga cenderung mengabaikan risiko yang mungkin terjadi pada FinTech *crypto*, termasuk risiko kerusakan sistem yang ditimbulkan ketika implementasi RegTech. Perkembangan FinTech dengan berbagai teknologi baru menimbulkan risiko siber *(cyber risk)* yang tidak dapat diantisipasi (Sangwan *et al.*, 2020), mulai dari risiko kelalaian penggunaan data sampai pada risiko kerusakan sistem. Maka penting bagi regulator untuk menyusun regulasi yang dapat melindungi FinTech dari berbagai risiko kerusakan (Ahern, 2018). Penggunaan teknologi baru pada FinTech—seperti: *blockchain*—memiliki beberapa keuntungan, namun meningkatnya berbagai kejahatan keuangan yang melibatkan *crypto asset* memberikan bukti bahwa seharusnya regulator tidak mengabaikan bidang ini (Sangwan *et al*., 2020).

4.2.2.2.3 Akses Data PEP *(Politically Exposed Person)*

Menurut P2, terbatasnya jumlah data PEP yang diimplementasikan dalam RegTech disebabkan karena terbatasnya akses yang diberikan oleh regulator kepada RegTech *provider* sebagai mitra dari FinTech *crypto*. P3 juga menyampaikan dalam wawancara yang mendukung pernyataan P2:

> "… kalau untuk akses kesana, itu hanya bisa PJK (Penyedia Jasa Keuangan), jadi di luar itu kita tidak bisa akses datanya …"

Menurut P1, mayoritas akses terhadap data PEP ini bersifat ekslusif sehingga hanya perusahaan-perusahaan tertentu saja yang mendapatkan akses terhadap data PEP tersebut. Hal ini didukung kembali dengan pernyataan dari P3:

> "… malah perusahaan-perusahaan yang bukan RegTech, jadi penyedia jasa IT, justru mereka mendapatkan akses. Harusnya kan RegTech yang justru diutamakan."

> "… jadi kita agak bingung aja, kenapa mereka di-*approve* aksesnya sedangkan kita tidak dikasih."

Pemberian akses oleh regulator terhadap data PEP cenderung diberikan kepada perusahaan-perusahaan IT *provider* dan bukan perusahaan RegTech *provider* yang sudah terstandarisasi. Menurut P3, keterbatasan akses terhadap data PEP juga berpengaruh terhadap akses terhadap data RCA *(relative close assocaiate)* dari nasabah dan atau calon nasabah. Data PEP dan RCA digunakan dalam proses *screening* sebagai titik kritis dalam proses penilaian risiko para calon nasabah karena proses KYC *(know your customer)* dan *transaction monitoring*—yang merupakan proses selanjutnya—bergantung dengan hasil dari proses tersebut.

Dalam penelitian yang dilakukan oleh Wronka (2022c) disebutkan bahwa proses *screening* berbasis daftar pemblokiran atau daftar hitam *(blacklist)* menjadi

bagian penting dalam pencegahan *crypto laundering*. Melalui proses ini, RegTech dapat mengidentifikasi dan memetakan calon nasabah dan atau nasabah FinTech *crypto* yang memiliki latar belakang berisiko tinggi *(high risk profile)*. Namun demikian, penelitian ini menemukan bahwa proses *screening* yang dilakukan melalui pemanfaatan RegTech menjadi tidak efektif karena keterbatasan akses terhadap data PEP *(politically exposed person)* dan RCA *(relative close associate)* yang dihadapi oleh RegTech *provider*. Regulator seharusnya dapat memberikan akses prioritas dan lebih terbuka kepada RegTech *provider* untuk menunjang dan menguatkan efektivitas dari implementasi pemanfaatan RegTech di Indonesia. Di saat yang bersamaan, hal ini menimbulkan kontradiksi karena jika regulator memberikan akses penuh terhadap data pribadi *(personal data)* beserta data RCA kepada RegTech *provider*—yang kemudian digunakan dalam implementasi RegTech—maka dapat melanggar pedoman etika penggunaan teknologi yang sangat mengutamakan privasi (Ryan & Stahl, 2021). Dalam mekanisme tata kelola data, selain mematuhi pedoman privasi dan perlindungan data, RegTech *provider* juga harus memastikan bahwa akses dan perolehan data pribadi yang digunakan bersifat sah (Ibiricu & van der Made, 2020).

Untuk memastikan bahwa data pribadi yang diperoleh dan digunakan dalam RegTech bersifat sah dan terverifikasi sehingga hasil dari pemanfaatan RegTech dapat optimal maka RegTech *provider* harus berupaya menerapkan strategi dalam memperoleh data selain data yang disediakan oleh regulator. Sangat penting untuk memahami sifat kepribadian individu dan budaya nasional yang berkembang karena persepsi terhadap privasi dan keterbukaan informasi dari masing-masing

individu bergantung dengan kedua hal tersebut (Liyanaarachchi *et al*., 2021). Berdasarkan penelitian yang dilakukan terhadap pengguna teknologi di Asia, ditemukan bahwa meningkatnya kasus pelanggaran privasi terhadap data pribadi sangat berpengaruh terhadap menurunnya tingkat kepercayaan masyarakat kepada institusi keuangan di negaranya (Liyanaarachchi *et al*., 2021). Hal tersebut berimplikasi pada strategi yang diterapkan oleh RegTech *provider* untuk memperoleh informasi data pribadi secara sah dan terverifikasi. RegTech *provider* harus menerapkan pendekatan yang fleksibel dan mengalihkan fokus yang berorientasi pada nasabah FinTech *crypto*. Penerapan *interface* yang interaktif ketika calon nasabah melakukan pendaftaran pada FinTech *crypto* dapat memperkuat hubungan antara calon nasabah dengan FinTech *crypto* serta dapat dimanfaatkan oleh RegTech *provider* untuk memperoleh informasi pribadi yang akurat secara sah dan terverifikasi (Steinhoff *et al*., 2019) melalui beberapa pertanyaan relevan yang berkaitan dengan informasi yang dibutuhkan. Dengan mempertimbangkan teori pertukaran sosial *(social exchange theory)* (Homans, 1958), sebagai timbal balik yang diberikan kepada nasabah maka FinTech *crypto* dan RegTech *provider* harus dapat memberikan jaminan *(assurance)* bahwa teknologi yang digunakan sudah mematuhi pedoman privasi dan perlindungan data nasabah.

4.2.2.2.4 Kompetensi Sumber Daya Manusia

Selain kendala dalam proses pengimplementasian sistem, kendala selanjutnya berasal dari sumber daya manusia (SDM) yang terlibat dalam penggunaan dan pemanfaatan RegTech. Hal ini disampaikan oleh P2 dan P3:

> "… mereka akan bingung "Ini tuh *tools* sebenarnya fungsinya buat apa, sih?", *then* nanya berulang-ulang …" *(P2)*

> "… mereka bingung "Ini tujuannya buat apa, sih?", mereka sampai bingung fitur ini tuh buat apa tujuannya." *(P2)*

> "… kalau dari kami sih melihatnya masih lumayan bingung cara penerapan di perusahaan mereka …" *(P3)*

Kendala SDM ini mendukung tidak efektifnya pemanfaatan RegTech karena mayoritas SDM yang terlibat dalam penggunaan RegTech belum memahami apa yang harus dilakukan terhadap prosedur dalam penerapan atau penggunaan RegTech. Mayoritas SDM belum memiliki latar belakang kompetensi dan pengalaman di bidang AML sehingga tidak memahami fungsi dari *tools* yang terdapat pada RegTech. Meskipun demikian, masih terdapat beberapa SDM pada perusahaan FinTech *crypto* yang memiliki kompetensi dan pengalaman di bidang AML. Menurut P2, hal ini membantu keberhasilan dari pemanfaatan RegTech yang diimplementasikan karena SDM ini relatif lebih proaktif dalam memanfaatkan berbagai *tools* yang terdapat dalam RegTech.

Dalam implementasi RegTech, selain pengaturan pada RegTech maka penting untuk lebih menekankan pada tata kelola SDM yang bertanggungjawab terhadap pemanfaatan teknologi. Menurut McCarthy (2022) dalam sistem manajemen risiko pemanfaatan teknologi diperlukan keterlibatan dan peran dari SDM, bukan hanya acuan teknis dalam pengaturan teknologi saja. Pengawasan terhadap SDM penting dilakukan karena bertujuan untuk memastikan bahwa pendelegasian dalam penggunaan dan atau pengoperasian RegTech dilakukan oleh SDM yang bertanggungjawab (McCarthy, 2022). Maka penting bagi regulator untuk dapat membentuk dan memberikan pelatihan kepada SDM FinTech *crypto*, terutama bagi

SDM yang dinilai memiliki potensi untuk mengembangkan RegTech di masa depan.

4.2.2.3 Komunikasi dan Kolaborasi antara Regulator dengan RegTech *Provider*

Penyebab utama yang ketiga dari tidak efektifnya implementasi regulasi melalui pemanfaatan RegTech di Indonesia, yaitu karena kurangnya komunikasi dan kolaborasi antara regulator dengan RegTech *provider*. Hal ini disampaikan oleh P2:

> "Pemanfaatan kolaborasi dan komunikasi yang kurang dengan RegTech seperti kita …"
>
> "OJK, BI, Bappebti, itu ke kita mungkin komunikasinya masih kurang, ya. Contoh, kita pernah ajak PPATK, contoh, untuk kolaborasi minta data PEP *list* nasional, itu masih ditolak."
>
> "… goAML PPATK, itu juga masih ditolak …"

Menurut P3, sampai saat ini komunikasi masih dilakukan secara tidak langsung. Komunikasi dilakukan dari regulator kepada FinTech *crypto*, kemudian FinTech *crypto* menyampaikan kepada RegTech *provider*, termasuk dalam hal ini adalah komunikasi mengenai perubahan regulasi yang berpengaruh terhadap alur kerja sistem dalam RegTech. Sedangkan dalam hal kolaborasi, hal ini disampaikan oleh P2:

> "… kenapa begitu ada RegTech, kurang gitu pemanfaatannya."

Kurangnya komunikasi dan kolaborasi ini terjadi pada mayoritas RegTech *provider*, termasuk pada RegTech *provider* yang menjadi *regulatory sandbox* dan sudah terdaftar di OJK. P1 juga menyebutkan bahwa belum terdapat keuntungan yang diperoleh secara jelas oleh para RegTech *provider* tersebut, termasuk

keuntungan dalam hal kolaborasi pemanfaatan RegTech untuk mendukung implementasi regulasi.

Temuan ini diduga karena ekosistem FinTech *crypto* dan RegTech di Indonesia belum komprehensif sehingga masih terdapat kesenjangan komunikasi, baik antar-regulator maupun antara regulator dengan RegTech *provider*. Dalam mendorong pemanfaatan RegTech maka penting bagi regulator untuk menguatkan kembali kolaborasinya dengan RegTech *provider* yang berstatus sebagai *regulatory sandbox.* Seharusnya regulator memfasilitasi dan memberikan kesempatan prioritas bagi *regulatory sandbox* untuk mengembangkan sistem sebagai bagian dari inovasi RegTech, terutama pada RegTech *provider* asal Indonesia. *Regulatory sandbox* memungkinkan RegTech *provider* untuk melakukan pengembangan dan pengujian terhadap inovasi solusi dalam kurun waktu tertentu sebelum produk atau layanan RegTech diperkenalkan dan diimplementasikan pada FinTech (Sarabdeen, 2023). Termasuk dalam hal ini, institusi yang menaungi regulator dapat bertindak sebagai *'petri-dishes'* dalam adopsi RegTech yang dikembangkan dalam *regulatory sandbox* sebelum RegTech diimplementasikan secara masif (McCarthy, 2022).

4.2.2.4 Pengawasan dan Pemeriksaan

Penyebab utama yang keempat dari tidak efektifnya implementasi regulasi melalui pemanfaatan RegTech di Indonesia, yaitu karena kurangnya pengawasan dan pemeriksaan dari regulator kepada perusahaan FinTech *crypto*. Hal ini disampaikan oleh P1:

> "… mereka banyak fokus yang terkenal saja, yang kecil-kecil masih belum bisa terangkul lah …"

> "Karena kan kalau misalnya adopsi, siapa yang bertanggung jawab? Siapa yang menilai? Tidak ada yang menilai, kan? Kalau misalnya tidak ada yang menilai, buat apa harus implementasi?"

Mayoritas pengawasan dan pemeriksaan dilakukan pada FinTech yang relatif sudah banyak diketahui oleh masyarakat dan berukuran besar saja, namun pada FinTech yang masih bertumbuh tidak dilakukan pengawasan dan pemeriksaan. Terkait dengan pengawasan dan pemeriksaan yang sudah dilakukan oleh regulator, P2 menyampaikan dalam wawancara:

> "… awal-awal 2022 ya kalau saya tidak salah. Memang klien kita pernah kena tegur tuh, kena audit random berkala, audit random itu kena dia dan baru tahu urgensinya."

> "… di saat awal tahun itu saja kita mendengar ada audit random. *Then* sampai sekarang ini kita belum dengar lagi ada kegiatan audit random."

Pengawasan dan pemeriksaan dari regulator terhadap FinTech *crypto* hanya dilakukan satu kali, yaitu hanya pada kuartal I di tahun 2022. Adapun sampai pada saat wawancara ini dilakukan—yaitu, pada kuartal III tahun 2023—belum terdapat adanya pengawasan dan pemeriksaan kembali dari regulator.

Kurangnya pengawasan dan pemeriksaan ini berimplikasi pada tindakan dan sikap para FinTech *crypto*—terutama FinTech yang baru bertumbuh—terhadap implementasi RegTech karena regulator hanya berfokus pada FinTech yang berukuran besar saja. Temuan ini sejalan dengan temuan penelitian di Afrika Selatan yang dilakukan oleh Gaviyau dan Sibindi (2023), bahwa regulator hanya melakukan pemeriksaan terhadap institusi keuangan yang berukuran besar. Pada kenyataannya, semua ukuran institusi keuangan atau FinTech *crypto* berpotensi digunakan sebagai sarana pencucian uang. Para pelaku yang terlibat akan menggunakan berbagai cara dan *platform* untuk 'menghalalkan' hasil dari

perbuatan kriminalnya (Dupuis & Gleason, 2020). Gaviyau dan Sibindi (2023) juga menemukan bahwa regulator memiliki keterbatasan waktu dalam melakukan pengawasan dan pemeriksaan. Secara rata-rata, regulator hanya dapat melakukan pemeriksaan terhadap tujuh institusi keuangan dalam kurun waktu satu tahun dan hanya dilakukan kepada institusi keuangan yang berukuran besar saja.

Tidak menutup kemungkinan bahwa keterbatasan regulator yang ditemui di Afrika Selatan juga dihadapi oleh regulator di Indonesia. Maka penting bagi regulator untuk mengembangkan dan mengaktifkan kembali FinTech *supervisory sandbox* yang dapat membantu regulator dalam melakukan pengawasan terhadap FinTech *crypto* terkait aspek kepatuhan dalam pemanfaatan RegTech. *Sandbox* menggabungkan antara ketentuan dalam regulasi dengan inisiasi langkah-langkah praktis yang berorientasi pada industri (McCarthy, 2022). Inisiasi tersebut akan memberikan pengaturan pengawasan *(supervisory arrangement)* dengan fleksibilitas yang lebih luas (Ng & Kwok, 2017), sehingga pengawasan dan pemeriksaan terhadap FinTech *crypto* dapat dilaksanakan secara efisien dan efektif.

4.3 Rekomendasi Perbaikan dalam Pemanfaatan RegTech di Indonesia

Berdasarkan hasil analisis data menggunakan analisis tema *(thematic analysis)* serta pengaplikasian *open* dan *focused coding* sehingga menghasilkan referensi dan *coding* dengan jumlah tertentu yang disajikan pada Lampiran 9, ditemukan beberapa rekomendasi perbaikan yang dapat digunakan dalam meningkatkan efektivitas pemanfaatan RegTech di Indonesia. Tabel 4.11 menujukkan hasil analisis yang terdiri atas dua tema utama dan enam sub-tema.

Tabel 4.11 Rekomendasi Perbaikan

Tema Utama	Sub-Tema
Pencegahan *Crypto Laundering*	Prosedur APU-PPT FinTech di semua Size
	Akses Data PEP oleh RegTech *Provider*
Pemanfaatan RegTech	Kolaborasi Regulator dengan RegTech Provider Lokal
	Klasifikasi RegTech
	Penetapan dan Pemberian Sanksi/*Penalty*
	Edukasi Regulator kepada FinTech *Crypto*

Sumber: Peneliti, Diolah

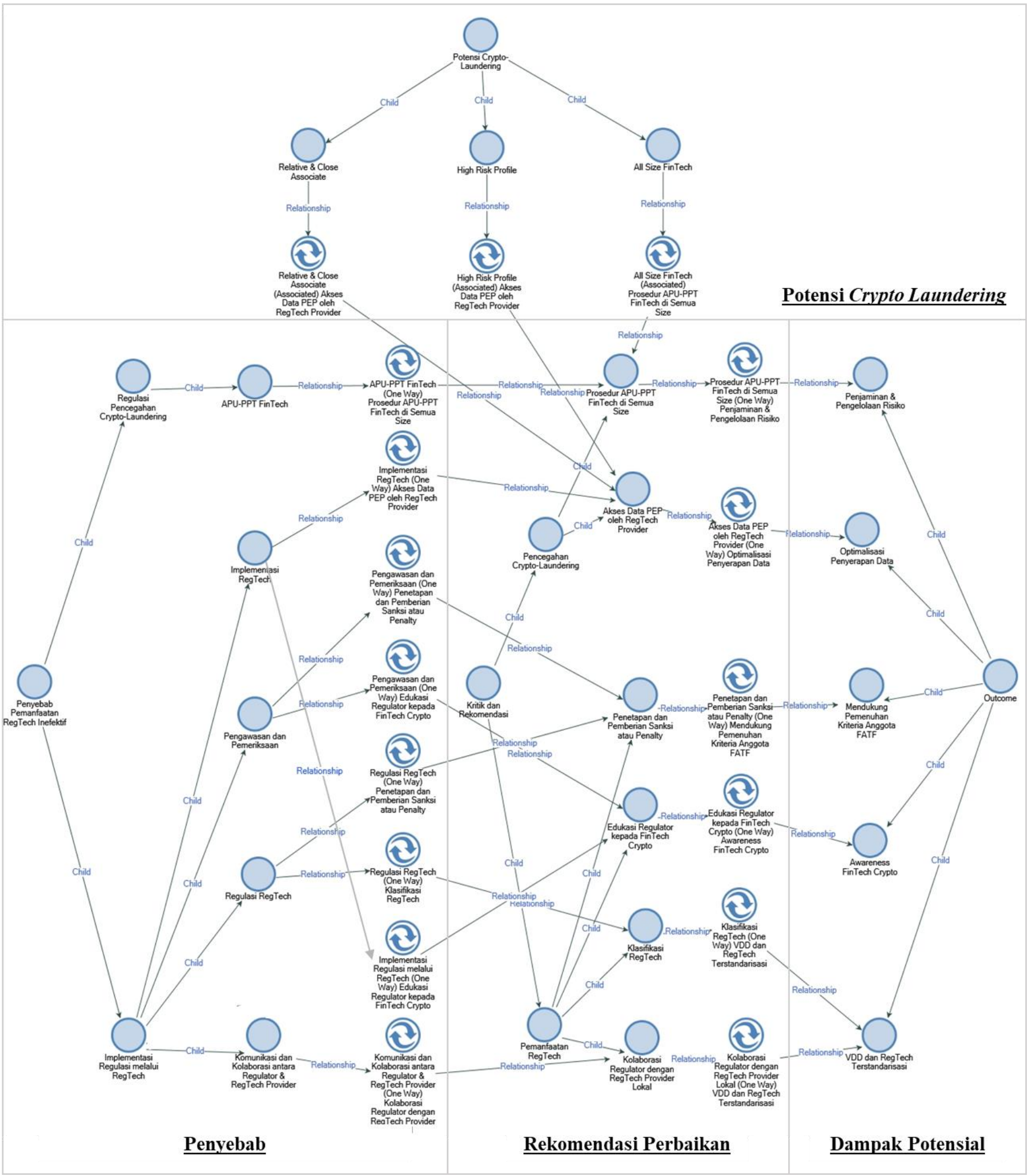
Masing-masing rekomendasi perbaikan tersebut didasarkan pada temuan penelitian mengenai penyebab tidak efektifnya pemanfaatan RegTech di Indonesia dengan mengaplikasikan *axial coding*. Kemudian, rekomendasi tersebut dihubungkan kembali dengan hasil dari analisis tema *(thematic analysis)* mengenai dampak potensial melalui pengaplikasian *focused coding* dan *axial coding* sehingga menghasilkan *coding* dengan jumlah tertentu yang disajikan pada Lampiran 10. Hasil analisis tersebut ditunjukkan melalui Tabel 4.12.

Tabel 4.12 Penyebab, Rekomendasi Perbaikan, dan Dampak Potensial

Penyebab	Rekomendasi Perbaikan	Dampak Potensial
Komunikasi dan Kolaborasi	Kolaborasi Regulator dengan RegTech *Provider* Lokal	VDD dan RegTech Terstandarisasi
Regulasi RegTech	Klasifikasi RegTech	
Pengawasan dan Pemeriksaan	Penetapan dan Pemberian Sanksi/*Penalty*	Mendukung Pemenuhan Kriteria Anggota FATF
Implementasi RegTech	Edukasi Regulator kepada FinTech *Crypto*	*Awareness* FinTech *Crypto*
APU-PPT FinTech	Akses Data PEP oleh RegTech *Provider*	Optimalisasi Penyerapan Data
	Prosedur APU-PPT FinTech di semua *Size*	Penjaminan dan Pengelolaan Risiko

Sumber: Peneliti, Diolah

Adapun visualisasi dari hasil analisis yang menggabungkan dan menghubungkan antara penyebab tidak efektifnya pemanfaataan RegTech dalam mencegah *crypto laundering*, potensi *crypto laundering*, rekomendasi perbaikan, dan dampak potensial ditunjukkan melalui Gambar 4.5. Hasil analisis ini berupa *report map* yang diolah melalui *software* NVivo 12.



Gambar 4.5 *Report Map* Penyebab, Rekomendasi Perbaikan, dan Dampak Potensial

Sumber: NVivo 12

4.3.1 Pencegahan *Crypto Laundering*

4.3.1.1 Prosedur APU-PPT FinTech *Crypto* di Semua Ukuran

Rekomendasi perbaikan ini didasarkan pada penyebab yang mempengaruhi tidak efektifnya pemanfaatan RegTech, yaitu terdapat beberapa kekurangan dalam mekanisme dan penerapan mekanisme pencegahan *crypto laundering* sehingga menyebabkan prosedur pencegahan *crypto laundering* belum dapat diterapkan secara menyeluruh oleh semua jenis dan ukuran FinTech *crypto* sebagaimana yang sudah dipaparkan pada sub-bab 4.2.1.

Menurut P2, setiap jenis dan ukuran FinTech *crypto* wajib memiliki prosedur APU dan atau APU-PPT karena risiko *crypto laundering* terdapat pada semua jenis dan ukuran FinTech, tidak terkecuali pada FinTech *crypto* yang masih bertumbuh atau berukuran kecil. P2 juga menyebutkan dalam wawancara:

> "Iya, prosedurnya itu punya, *screening*-nya punya. Ketika diaudit oleh salah satu regulator "Mana proses *screening*-nya?" itu ada, dilakukan proses KYC, dilakukan *screening watch list* SIJITU, contoh, *screening* lewat SIJITU, oke, *pass* gitu, atau misal "Coba dilihat mana pemantauan transaksinya?", ada juga di *history*-nya bahwa memang dilakukan pemantauan transaksi. Lalu juga "Penilaian risiko berjangkanya coba saya mau lihat *history*-nya", contoh misalnya regulator ngomong seperti itu, mereka punya *evidence*-nya bahwa mereka melakukan prosedur itu."

> "… biasanya investor, apalagi investor asing, itu punya *concern* lebih loh di ranah APU-PPT-nya. Jadi, selain untuk menjaga sisi si LJK dari risiko sanksi, ada risiko reputasi juga di situ."

Prosedur APU yang dimaksud dalam rekomendasi perbaikan ini mencakup semua proses, mulai dari proses *screening* sampai dengan pemantauan transaksi berbasis sistem. Dengan diterapkannya rekomendasi perbaikan ini, diharapkan dapat berdampak terhadap peningkatan pengelolaan risiko yang diterapkan oleh FinTech

crypto serta dapat memberikan penjaminan risiko kepada regulator dan investor pengembang FinTech *crypto*, khususnya risiko sanksi dan risiko reputasi.

Pengelolaan dan penjaminan risiko perlu ditekankan untuk meminimalisir risiko *crypto laundering* yang dilakukan melalui interaksi antara sistem virtual dengan sistem pada sektor riil yang saat ini digunakan oleh mayoritas pelaku (Meiryani, 2023). Maka tepat jika regulator menyusun kebijakan APU berbasis sistem (RegTech) untuk masing-masing ukuran FinTech *crypto* karena RegTech yang tepat dapat mendeteksi risiko atau memperkirakan masalah yang berpotensi mengancam berbagai jenis dan ukuran FinTech *crypto* (Sarabdeen, 2023).

4.3.1.2 Akses Data PEP oleh RegTech *Provider*

Salah satu penyebab tidak efektifnya pemanfaatan RegTech di Indonesia, yaitu karena adanya berbagai kendala dalam implementasi RegTech yang berpengaruh terhadap pencegahan *crypto laundering*. Kendala utama tersebut berkaitan erat dengan akses data *politically exposed person* (PEP) oleh RegTech *provider*. Sebagaimana pemaparan pada sub-bab 4.2.2, bahwa RegTech *provider* mengalami kesulitan dalam memeroleh data PEP karena akses data PEP tersebut bersifat terbatas, ekslusif, dan relatif diberikan oleh regulator hanya kepada IT *provider*, bukan kepada RegTech *provider*.

Dikarenakan data PEP berkaitan erat dengan data RCA *(relative close associate)* maka P3 menyampaikan dalam wawancara:

> "Oh kebanyakan sih dari RCA-nya *(relative close associate)* ya, jadi anggota keluarga dari si *profile*-nya ditemukan."

Akses data PEP menjadi sangat penting dan dibutuhkan oleh RegTech *provider* karena potensi *crypto laundering* dapat berasal dari nasabah dengan latar belakang

profil risiko yang tinggi *(high risk profile)* serta kerabat dekat dari para pelaku tindak pidana atau profil yang sudah tercatat dalam DHN dan atau *sanction list*. Maka dari itu, menurut P2, diperlukan akses terbuka terhadap data PEP yang diperoleh RegTeh *provider* untuk meningkatkan efektivitas dari pemanfaatan RegTech dalam pencegahan *crypto laundering*. P2 juga menyebutkan bahwa secara ideal, seharusnya akses data PEP lebih diutamakan untuk diberikan kepada RegTech *provider* jika dibandingkan dengan FinTech *crypto* dan atau IT *provider*. Hal ini disebabkan karena mayoritas FinTech *crypto* dan atau IT *provider* belum memiliki infrastruktur yang memadai untuk menyerap, menyambungkan, dan mengintegrasikan data-data tersebut ke dalam sistem RegTech.

Secara teknis, pemberian akses oleh regulator kepada RegTech *provider* dapat mengoptimalkan distribusi serta penyerapan data PEP dan RCA yang digunakan dalam RegTech. Namun, sebagaimana yang sudah didiskusikan pada sub-bab 4.2.2 bahwa pemberian akses tersebut berpotensi melanggar pedoman etika dalam penggunaan teknologi yang sangat mengutamakan privasi (Ryan & Stahl, 2021), sehingga diharapkan RegTech *provider* dapat menerapkan pendekatan yang fleksibel dalam memperoleh informasi data pribadi secara sah dan terverifikasi. Hal ini berimplikasi pada peran regulator selaku pembuat kebijakan. Regulator harus memiliki pedoman pengumpulan data bagi RegTech *provider* yang memastikan bahwa pengumpulan data dilakukan berdasarkan persetujuan calon nasabah serta menjamin keamanan dan privasi data nasabah atau calon nasabah. Regulasi atau kebijakan pengumpulan data disusun untuk menghindari pengumpulan data yang berlebihan, tidak sesuai tujuan, tidak akurat, dan tidak relevan (Sarabdeen, 2023).

Maka dari itu, regulasi yang disusun oleh regulator harus memadai dalam mencegah dan mengantisipasi berbagai tantangan yang berkaitan dengan penyalahgunaan data.

4.3.2 Pemanfaatan RegTech

4.3.2.1 Klasifikasi RegTech

Rekomendasi perbaikan ini didasarkan karena ditemukannya beberapa celah pada regulasi pemanfaatan RegTech. Menurut P1, untuk memperbaiki hal tersebut sehingga dapat meningkatkan pemanfaatan RegTech di Indonesia maka diperlukan regulasi yang mengklasifikasikan RegTech. Klasifikasi RegTech tersebut dapat dilakukan berdasarkan ukuran dan cakupan RegTech dalam melakukan implementasi prosedur anti-pencucian uang berbasis sistem. Melalui regulasi tersebut maka RegTech *provider* dapat memiliki suatu kerangka kerja *(framework)* yang dapat dijadikan acuan ketika mengimplementasikan RegTech. Terkait dengan hal ini, P1 menyampaikan dalam wawancara:

> "Makannya di klasifikasi katalog ini bisa melakukan VDD, kan? Kalau sekarang, kalau misalnya itu, siapa yang benar dan siapa yang benar, siapa yang tidak benar, kan tidak jelas."

Dengan adanya kerangka kerja maka regulator dapat melakukan uji tuntas vendor atau *vendor due diligence* (VDD) terhadap RegTech *provider*. VDD yang dilakukan oleh regulator bertujuan untuk mengidentifikasi dan memastikan bahwa RegTech *provider* tersebut telah menerapkan prosedur anti-pencucian uang berbasis sistem berdasarkan regulasi dan atau kerangka kerja *(framework)* yang sudah disusun. Dengan demikian, setiap RegTech yang akan diimplementasikan pada FinTech

crypto telah terstandarisasi secara integral berdasarkan kebutuhan FinTech *crypto* dan regulator.

Temuan ini sejalan dengan European Banking Authority (2021) yang menganalisis pemanfaatan RegTech, disebutkan bahwa berdasarkan perspektif RegTech *provider* kurangnya keselarasan regulasi menjadi hambatan dalam pemanfaatan RegTech, sehingga perlu dilakukan konvergensi standar regulasi. Dalam opsi jangka panjang, konvergensi standar regulasi dapat mendorong pelaksanaan sertifikasi pada RegTech (European Banking Authority, 2021). Dengan demikian, penting bagi regulator untuk menelaah dan menyelaraskan antara satu regulasi dengan regulasi lainnya, seperti menyelaraskan antara klasifikasi FinTech *crypto* dengan ukuran dan cakupan RegTech. Jika regulasi tersebut sudah selaras dan dapat diimplementasikan secara komprehensif maka regulator dapat memulai untuk melakukan VDD atau sertifikasi terhadap RegTech *provider*.

4.3.2.2 Kolaborasi antara Regulator dengan RegTech *Provider*

Rekomendasi perbaikan ini didasarkan pada kendala dalam pemanfaatan RegTech, dimana komunikasi dan kolaborasi antara regulator dengan RegTech *provider* relatif belum efektif. Komunikasi yang dilakukan oleh regulator tidak dilakukan secara langsung dengan RegTech *provider*, melainkan hanya kepada FinTech *crypto* saja. Sedangkan dalam hal kolaborasi, P2 menyampaikan dalam wawancara:

> "Nah, kenapa gak manfaatin produk 100% lokal dari anak bangsa? Itu tuh dimaksimalin kerjasama, diajak kolaborasi, gitu. Pemanfaatannya dimaksimalin."

Saat ini, regulator belum mengoptimalkan peran RegTech *provider* dalam membantu implementasi regulasi pencegahan *crypto laundering* melalui pemanfaatan RegTech, termasuk pada RegTech *provider* yang sudah menjadi *regulatory sandbox*. Menurut P3, diperlukan dukungan dari regulator untuk mengoptimalkan pemanfaatan RegTech dalam mencegah *crypto laundering*. Sejalan dengan hal tersebut, P2 menyebutkan bahwa dukungan dari regulator kepada RegTech *provider* dapat berupa pendampingan bagi RegTech *provider* agar dapat menyelaraskan dengan tujuan jangka panjang dari regulator, mediasi antara RegTech *provider* dengan FinTech *crypto*, serta mempermudah perizinan kolaborasi antara RegTech *provider* dengan instansi-instansi terkait yang dibutuhkan oleh RegTech *provider*.

Hadirnya RegTech di Indonesia berperan dalam mengimplementasikan Industri 4.0 dan berkontribusi terhadap penguatan ekosistem digital. Anshari dan Almunawar (2022) menemukan bahwa ekosistem digital dapat mendorong pengembangan industri teknologi informasi dan komunikasi. Maka penting bagi regulator untuk dapat mendorong pengembangan ekosistem digital dan kolaborasi antara pihak yang berkepentingan dalam ekosistem digital (pertukaran aset virtual), baik pihak dari sektor publik maupun sektor privat karena adopsi Industri 4.0 di Indonesia mayoritas dilakukan oleh sektor privat (Anshari, 2020). Kolaborasi menjadi elemen penting dalam keberhasilan pengembangan teknologi-teknologi yang terkait dengan keuangan (Utami & Ekaputra, 2021). Komunikasi dan kolaborasi yang terintegrasi ini diharapkan dapat memperkuat dan memudahkan regulator dalam menerapkan *vendor due diligence* (VDD) kepada RegTech

provider sehingga RegTech yang diimplementasikan sudah terstandarisasi serta memenuhi kebutuhan regulator dan FinTech *crypto*.

4.3.2.3 Edukasi Regulator kepada FinTech *Crypto*

Rekomendasi ini didasarkan pada penyebab tidak efektifnya pemanfaatan RegTech, dimana terdapat beberapa kendala dalam implementasi RegTech yang dihadapi oleh RegTech *provider* serta dalam pengawasan dan pemeriksan yang seharusnya dilakukan oleh regulator. Dalam implementasi RegTech—selain terdapatnya keterbatasan dalam mengakses data PEP—tidak efektifnya pengimplementasian RegTech juga disebabkan karena bergantung dengan *risk appetite and perception* serta kompetensi SDM dari FinTech *crypto*. Sedangkan dalam pengawasan dan pemeriksaan, regulator relatif hanya berfokus pada FinTech berukuran besar saja. Namun, pada kenyataannya, semua jenis dan ukuran FinTech *crypto* berpotensi sebagai sarana *crypto laundering*. Untuk memperbaiki hal tersebut, P3 menyampaikan dalam wawancara:

> "… edukasi dari regulatornya juga karena kalau untuk *small to medium size* FinTech biasanya yang kami temui sih, dari *case* kami, mereka biasanya kurang paham tentang AML."

Peran aktif dari regulator sangat diperlukan. Edukasi kepada SDM FinTech *crypto*, terutama kepada FinTech yang berukuran *small to medium* menjadi bagian dari tanggungjawab regulator untuk mendukung keberhasilan implementasi pemanfaatan RegTech sebagai teknologi yang mendukung fungsi kepatuhan.

Saran perbaikan ini sejalan dengan termuan Anshari dan Almunawar (2022) yang menyebutkan bahwa dalam adopsi Indusrti 4.0, pengetahuan SDM dan kemampuan manajemen yang memadai berperan penting dalam mendukung

kesiapan ekosistem digital di Indonesia. Ketika memasuki Industri 4.0, para organisasi memiliki ketakutan dalam pengelolaan sumber daya, termasuk sumber daya manusia (Anshari & Almunawar, 2022). Maka dalam pemanfaatan RegTech, regulator perlu memberikan wadah edukasi kepada para SDM FinTech *crypto* untuk membentuk SDM yang memahami dampak dari *crypto laundering* dan dapat mengoptimalkan pemanfaatan RegTech dalam mencegah *crypto laundering*. Fokus utama dari edukasi dapat berkaitan dengan prosedur pencegahan *crypto laundering* berbasis sistem, mulai dari potensi dan dampak *crypto laundering*, urgensi pemanfaatan RegTech, sampai pada kompetensi yang harus dimiliki oleh SDM FinTech *crypto*. Melalui edukasi ini, diharapkan dapat meningkatkan kesadaran *(awareness)* FinTech *crypto* terhadap potensi dan dampak dari *crypto laundering* serta pencegahan *crypto laundering* berbasis sistem atau dengan pemafaatan RegTech.

4.3.2.4 Penetapan dan Pemberian Sanksi

Rekomendasi perbaikan ini didasarkan pada kekurangan yang terdapat dalam regulasi RegTech serta kekurangan dalam pengawasan dan pemeriksaan terhadap FinTech *crypto*. Sebagaimana yang sudah dipaparkan sebelumnya, bahwa kekurangan-kekurangan tersebut mempengaruhi efektivitas pemanfaatan RegTech dalam mencegah *crypto laundering* di Indonesia.

Menurut P2, untuk menegaskan bahwa regulasi yang sudah ditetapkan harus dipatuhi dan dijalankan, serta pengawasan dan pemeriksaan yang dilakukan oleh regulator sejalan dengan tujuan maka regulator perlu menetapkan dan memberikan sanksi kepada FinTech *crypto* jika tidak memenuhi fungsi kepatuhan terhadap

regulasi pencegahan *crypto laundering* yang sudah ditetapkan. P2 juga menyebutkan dalam wawancara:

> "Cukup kasih sanksi yang jelas, sanksi administratif, sanksi yang bahkan sampai tegas gitu, kasih yang jelas dan mulai dijalankan sanksi itu supaya dari hal kecil implikasinya …"

> "… harus dipertegas ya sanksinya, lalu juga disebutkan industri-industri yang memang diwajibkan, diperluas lagi …"

Penetapan dan pemberian sanksi ini juga mempertegas bahwa regulasi yang berlaku tersebut merupakan sebuah keharusan dan berifat mendesak. Pemberian sanksi kepada FinTech *crypto* dapat berjenjang, mulai dari sanksi administratif sampai pada sanksi yang bersifat lebih mengikat.

Menurut Teichmann dan Wittmann (2023) mekanisme anti-pencucian uang yang aman seharusnya dapat mendorong kelancaran dan ketegasan dalam penerapan sanksi terkait fungsi kepatuhan. Hal ini menjadi refleksi bagi regulator, sangat dimungkinkan bahwa mekanisme anti-pencucian uang dalam perdagangan aset virtual (kripto) di Indonesia memang belum memadai dan optimal. Maka penting bagi regulator untuk menguji dan menelaah kembali ketahanan dan kecukupan mekanisme anti-pencucian uang berbasis sistem dalam mengatasi masalah yang mungkin muncul dalam pemanfaatan RegTech, termasuk kepatuhan para FinTech *crypto* dalam memanfaatkan RegTech. Dengan adanya penetapan dan pemberian sanksi yang tegas kepada FinTech *crypto* diharapkan dapat mendorong kesiapan para LJK (Lembaga Jasa Keuangan) dalam mengimplementasikan regulasi pencegahan pencucian uang berbasis sistem, sehingga dapat mendukung penguatan Indonesia sebagai negara anggota FATF *(Financial Action Task Force)* dengan status *full membership.*

BAB V

PENUTUP

5.1 Kesimpulan Penelitian

Berdasarkan hasil analisis data dan pembahasan yang sudah dipaparkan maka dapat ditarik kesimpulan sebagai barikut:

1. Mekanisme pencegahan *crypto laundering* di Indonesia mengacu pada regulasi yang dikeluarkan dan ditetapkan oleh Bappebti (Badan Pengawas Perdagangan Berjangka Komoditi). Proses pencegahan dilakukan melalui KYC *(know your customer)* dan pemantauan transaksi *(transaction monitoring)* dengan pendekatan berbasis risiko *(risk-based approach)*. Saat ini, pengawasan terhadap penerapan proses pencegahan tersebut masih dilakukan oleh Bappebti.
2. Ditemukan bahwa tidak efektifnya pemanfaatan RegTech dalam pencegahan *crypto laundering* disebabkan karena kekurangan pada regulasi pencegahan *crypto laundering* dan kendala ketika mengimplementasikan regulasi melalui RegTech. Kekurangan pada regulasi pencegahan *crypto laundering* terdapat pada asas praduga tak bersalah, *periodic checking*, pembaharuan dan ketersediaan data, dan SLA *(service level agreement)*. Sedangkan kendala ketika mengimplementasikan regulasi melalui RegTech ditemukan pada regulasi pemanfaatan RegTech, implementasi RegTech, komunikasi dan kolaborasi antara regulator dengan RegTech *provider*, serta pengawasan dan pemeriksaan dari regulator.

3. Rekomendasi perbaikan didasarkan pada temuan penyebab. Dalam pencegahan *crypto laundering* rekomendasi kepada regulator yang dapat dilakukan, yaitu dengan meninjau atau menyusun kembali prosedur APU-PPT untuk semua ukuran FinTech *crypto* dan memberikan akses data PEP *(politically exposed person)* kepada RegTech *provider*. Sedangkan dalam pemanfaatan RegTech, rekomendasi perbaikan yang dapat dilakukan, yaitu dengan mengklasifikasikan jenis RegTech, melakukan kolaborasi antara regulator dengan RegTech *provider* lokal, edukasi regulator kepada FinTech *crypto*, serta penetapan dan pemberian sanksi kepada FinTech *crypto* jika tidak menjalankan fungsi kepatuhan.

5.2 Kontribusi dan Implikasi Penelitian

Kontribusi akademik dalam penelitian ini, yaitu memberikan dan memperkaya wawasan terhadap hasil penelitian sebelumnya. Temuan penelitian ini melengkapi temuan penelitian mengenai tingkat efektivitas pemanfataan RegTech. Beberapa penelitian tersebut dilakukan dengan pendekatan kuantitatif sehingga belum menjelaskan penyebab tidak efektifnya pemanfaatan RegTech di Indonesia. Penelitian ini melengkapi kesenjangan tersebut dengan mengeksplorasi penyebab tidak efektifnya pemanfaatan RegTech.

Selanjutnya, penelitian ini berimplikasi pada beberapa pemangku kepentingan *(stakeholder)* yang terlibat, yaitu:

1. Regulator

   Berdasarkan temuan-temuan dalam penelitian ini maka sangat dimungkinkan bahwa mekanisme anti-pencucian uang dalam perdagangan aset virtual (kripto)

di Indonesia memang belum memadai dan optimal. Maka penting bagi regulator untuk menguji dan menelaah kembali ketahanan dan kecukupan mekanisme anti-pencucian uang berbasis sistem dalam mengatasi masalah yang mungkin muncul dalam pemanfaatan RegTech, termasuk kepatuhan para FinTech *crypto* dalam memanfaatkan RegTech.

2. RegTech *Provider*

   Terdapat beberapa temuan dalam penelitian ini yang berkaitan langsung dengan RegTech *provider*, terutama dalam proses perolehan data yang digunakan pada tahap KYC *(know your customer)*. Temuan tersebut berkaitan erat dengan isu privasi dan keamanan data. Dalam hal ini, selain RegTech *provider* berfokus pada pengembangan RegTech, maka penting untuk memperhatikan berbagai isu yang berkaitan dengan penggunaan, penjaminan privasi, dan keamanan data pribadi nasabah dalam implementasi dan penggunaan teknologi.

3. FinTech *Crypto*

   Penelitian ini mengungkapkan beberapa hal yang berkaitan dengan FinTech *crypto*, terutama mengenai kesadaran untuk memanfaatkan RegTech. Penting bagi FinTech *crypto* untuk menyadari bahwa potensi *cypto laundering* dengan berbagai teknologi yang digunakannya dapat terjadi pada semua jenis dan ukuran FinTech sehingga pencegahan berbasis sistem perlu dilakukan. FinTech *crypto* perlu berkomunikasi dan bekerjasama dengan RegTech *provider* untuk mengimplementasikan RegTech berdasarkan kebutuhan dan kemampuan keuangan yang dimilikinya.

5.3 Keterbatasan dan Saran Penelitian

Peneliti mengakui bahwa penelitian kualitatif ini dapat bersifat subjektif karena pengumpulan data primer untuk mengeksplorasi penyebab tidak efektifnya pemanfaatan RegTech hanya dilakukan berdasarkan perspektif RegTech *provider*. Peneliti mengalami keterbatasan dalam pengumpulan data sehingga tidak memperoleh data yang mewakili perspektif FinTech *crypto* sebagai pengguna RegTech.

Penelitian selanjutnya dapat memperluas penelitian ini dengan menyertakan perspektif FinTech *crypto* dan mengintegrasikan antara aspek ekonomi, aspek legal, dan aspek politik. Sedangkan bagi regulator, diharapkan temuan pada penelitian ini dapat digunakan sebagai pertimbangan dalam memperbaiki regulasi yang berkaitan dengan pencegahan *crypto laundering* berbasis sistem (RegTech).

DAFTAR PUSTAKA

Adachi, D., & Aoyagi, J. (2020). Blockchain and Economic Transactions. *Cryptocurrency and Blockchain Technology*. https://doi.org/10.1515/9783110660807-002

Ahern, D. M. (2018). *Regulatory arbitrage in a FinTech world: devising an optimal EU regulatory response to crowdlending*.

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, *179*(November 2021), 1–30. https://doi.org/10.1016/j.techfore.2022.121632

Al-Tawil, T. N. (2022). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-07-2022-0109

Albrecht, Duffin, K. M. K., Hawkins, S., & Morales Rocha, V. M. (2019). The Use of Cryptocurrencies in the Money Laundering Process. *Journal of Money Laundering Control*, *22*(2), 210–216. https://doi.org/10.1108/JMLC-12-2017-0074

Albrecht, W., Albrecht, C., Albrecht, C., & Zimbelman, M. (2012). *Fraud Examination* (4th ed.). Cengange Learning South-Western.

Alexander, K. (2001). The International Anti-Money-Laundering Regime: The Role of the Financial Action Task Force. *Journal of Money Laundering Control*, *4*(3), 231–248. https://doi.org/10.1108/eb027276

Aluko, A., & Bagheri, M. (2012). The impact of money laundering on economic and financial stability and on political development in developing countries. *Journal of Money Laundering Control*, *15*(4), 1–5. https://doi.org/DOI 10.1108/13685201211266024

Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business*, *100*, 7–25. https://doi.org/10.1016/j.jeconbus.2018.07.003

Anshari, M. (2020). Workforce Mapping of Fourth Industrial Revolution: Optimization to Identity. *Journal of Physics: Conference Series*, *1477*(7). https://doi.org/10.1088/1742-6596/1477/7/072023

Anshari, M., & Almunawar, M. N. (2022). Adopting open innovation for SMEs and industrial revolution 4.0. *Journal of Science and Technology Policy Management*, *13*(2), 405–427. https://doi.org/10.1108/JSTPM-03-2020-0061

APGML. (2018). *Anti-money Laundering and counter-teorrorist financing measures Indonesia Mutual Evaluation Report*. *September*.

Ayres. (2007). Qualitative research proposals – Part II: Conceptual Models and Methodological Options. *Wound Ostomy Continence Nurs*, *34*, 131–133.

Azevedo Araujo, R. (2010). An evolutionary game theory approach to combat money laundering. *Journal of Money Laundering Control*, *13*(1), 70–78. https://doi.org/10.1108/13685201011010236

Basel Institue of Governance. (2021). Basel AML Index 2021 : 10th Public Edition Ranking money laundering and terrorist financing risks around the world. *Annual Report*.

Basel Institute on Governance. (2013). Basel AML Index 2012 and 2013 Report. *Annual Report*.

Basel Institute on Governance. (2014). Basel AML Index 2014 Report. *Annual Report*.

Basel Institute on Governance. (2015). Basel AML Index 2015 Report. *Annual Report*, *August*.

Basel Institute on Governance. (2016). Basel AML Index 2016 Report. *Annual Report*, *July*.

Basel Institute on Governance. (2017). Basel AML Index 2017 Report. *Annual Report*, *August*.

Basel Institute on Governance. (2018). Basel AML Index 2018 Report. *Annual Report*, *October*.

Basel Institute on Governance. (2019). Basel AML Index 2019 Report. *Annual Report*, *August*.

Basel Institute on Governance. (2020). Basel AML Index : 9th Public Edition Ranking money laundering and terrorist financing risks around the world. *Annual Report*.

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Berg, B. L. (2004). *Qualitative Research Methods for the Social Sciences* (5th ed.). Pearson.

Bin Belaisha, B., & Brooks, G. (2014). Money laundering in Dubai: strategies and future directions. *Journal of Money Laundering Control*, *17*(3), 343–354. https://doi.org/10.1108/JMLC-10-2013-0038

Bolam, B., Gleeson, K., & Murphy, S. (2003). "Lay person" or "health expert"? Exploring theoretical and practical aspects of reflexivity in qualitative health research. *Forum Qualitative Sozialforschung*, *4*(2).

Bulmer, M., Sturgis, P. J., & Allum, N. (2009). *Secondary Analysis of Survey Data*.

SAGE.

Bylund, A. (2023). *What Is Blockchain?* The Motley Fool. https://www.fool.com/terms/b/blockchain/

CAMS. (2012). *Certification Examination Certification Examination*. Association of Certified Anti-Money Laundering Specialists.

Chainalysis. (2022). *The 2022 Crypto Crime Report* (Issue February). https://go.chainalysis.com/2022-crypto-crime-report.html

Charmaz, K. (2006). Constructing Grounded Theory. In *British Library*. SAGE.

Corbin, J., & Strauss, A. (2008). *Basics of Qualitative Research* (3rd ed.). SAGE.

de Villiers, C., Dumay, J., & Maroun, W. (2019). Qualitative accounting research: dispelling myths and developing a new research agenda. *Accounting and Finance*, *59*(3), 1459–1487. https://doi.org/10.1111/acfi.12487

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, *28*(1), 60–74. https://doi.org/10.1108/JFC-06-2020-0113

Dyntu, V., & Dykyi, O. (2019). Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies*, *4*(5), 75–81. https://doi.org/10.30525/2256-0742/2018-4-5-75-81

European Banking Authority. (2021). *Analysis of RegTech in the EU Financial Sector* (Issue June). https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015484/EBA analysis of RegTech in the EU financial sector.pdf

Fabre, G. (2003). Criminal Prosperity: Drug Trafficking, Money Laundering, and Financial Crises after the Cold War. *Psychology Press*.

FATF. (2003). *The Forty Recommendations*.

FATF. (2022). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. *FATF, Paris, France, March*, 1–142. www.fatf-gafi.org/recommendations.html

Finder. (2022). *Finder Cryptocurrency Adoption Index*. https://www.finder.com/id/finder-cryptocurrency-adoption-index

FINOS. (2020). *Open RegTech Strategic Initiative*. https://www.finos.org/open-regtech

Freij, Å. (2020). Using technology to support financial services regulatory compliance: current applications and future prospects of regtech. *Journal of Investment Compliance*, *21*(2/3), 181–190. https://doi.org/10.1108/joic-10-2020-0033

Gaviyau, W., & Sibindi, A. B. (2023). Anti-money laundering and customer due diligence : empirical evidence from South Africa. *Journal of Money Laundering Control*, *26*(7), 224–238. https://doi.org/10.1108/JMLC-06-2023-0103

Gilmour. (2014). Understanding Money Laundering – A Crime Script Approach. *The European Review of Organised Crime*, *1*(2), 35–56.

Gilmour. (2016). Preventing money laundering: a test of situational crime prevention theory. *Journal of Money Laundering Control*, *19*(4), 376–396. https://doi.org/10.1108/JMLC-10-2015-0045

Gilmour, P. M. (2022). Reexamining the anti-money-laundering framework: a legal critique and new approach to combating money laundering. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-02-2022-0041

Go, L., & Benarkah, N. (2019). Quo Vadis legal profession participation in anti-money laundering. *Journal of Money Laundering Control*, *22*(4), 764–769. https://doi.org/10.1108/JMLC-12-2018-0072

Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, *17*(4), 441–458. https://doi.org/10.1108/13590791011082797

Hamilton, A. B., & Finley, E. P. (2020). Reprint of: Qualitative methods in implementation research: An introduction. *Psychiatry Research*, *283*(August 2019), 112629. https://doi.org/10.1016/j.psychres.2019.112629

Hancock, D., & Algozzine, B. (2006). *A Practical Guide for Doing Case Study Research*.

Haryono, & Sofwan. (2020). Implementasi Peraturan Bank Indonesia No.14/27/PBI/2012 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, *7*(1), 1–20.

Hassan, S. S. U., Hussain, M. A., & Sajid, S. (2022). The effectiveness of anti-money laundering legislation in Islamic banking of Pakistan: experts' opinion. *Journal of Money Laundering Control*, *25*(1), 135–149. https://doi.org/10.1108/JMLC-02-2021-0014

Holsti, O. (1969). *Content Analysis for the Social Sciences*. Addison-Wesley.

Homans, G. C. (1958). Social Behavior as Exchange. *American Journal of Sociology*, *63*(6), 597–606.

Ibiricu, B., & van der Made, M. L. (2020). Ethics by design: a code of ethics for the digital age. *Records Management Journal*, *30*(3), 395–414. https://doi.org/10.1108/RMJ-08-2019-0044

Jakfar, B. N. (2022). Perbandingan Hukum tentang Mata Uang Virtual sebagai Aset Terpidana Tindak Pidana Korupsi di Indonesia. *Jurnal Ilmiah Indonesia*, *7*(7), 9898–9911. https://www.who.int/news-room/fact-sheets/detail/autism-

spectrum-disorders

Juntunen, J., & Teittinen, H. (2022). Accountability in anti-money laundering – findings from the banking sector in Finland. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-12-2021-0140

Kementerian Keuangan RI. (2022). *Menuju Era Uang Rupiah Digital*. https://djpb.kemenkeu.go.id/portal/id/berita/lainnya/opini/3950-menuju-era-uang-rupiah-digital.html

Khalid, S. N. A. (2009). Reflexivity in Qualitative Accounting Research. *Journal of Financial Reporting and Accounting*, *7*(2), 81–95. https://doi.org/10.1108/19852510980000005

Kirkpatrick, K., Stephens, A., Gerber, J., Nettesheim, M., & Bellm, S. (2021). Understanding regulatory trends: digital assets & anti-money laundering. *Journal of Investment Compliance*, *22*(4), 345–353. https://doi.org/10.1108/joic-07-2021-0033

KPMG. (2018). *There's a Revolution Coming: Embracing the Challenge of RegTech 3.0*. https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/09/regtech-revolution-coming.pdf

Kurum, E. (2020). RegTech solutions and AML compliance: what future for financial crime? *Journal of Financial Crime*. https://doi.org/10.1108/JFC-04-2020-0051

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-07-2022-0161

Litchfield, H. (2015). A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology. *Australian Computer Society*.

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Online banking and privacy: redesigning sales strategy through social exchange. *International Journal of Bank Marketing*, *39*(6), 955–983. https://doi.org/10.1108/IJBM-05-2020-0278

Lukito, A. S. (2016). Financial intelligent investigations in combating money laundering crime: An Indonesian legal perspective. *Journal of Money Laundering Control*, *19*(1), 92–102. https://doi.org/10.1108/JMLC-09-2014-0029

Mardiansyah. (2021). *Penilaian Risiko Indonesia Pencucian Uang*. Pusat Pelaporan dan Analisis Transaksi Keuangan.

Mason, J. (2002). *Qualitative Researching* (2nd ed.). SAGE.

McCarthy, J. (2022). The regulation of RegTech and SupTech in finance: ensuring consistency in principle and in practice. *Journal of Financial Regulation and*

Compliance, *31*(2), 186–199. https://doi.org/10.1108/JFRC-01-2022-0004

Meiryani. (2023). Exploration of potential money laundering crimes with virtual currency facilities in Indonesia. *Journal of Money Laundering Control*, *2022*(Wcp 2022). https://doi.org/10.1108/JMLC-01-2023-0010

Meiryani, M., Soepriyanto, G., & Audrelia, J. (2022). Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-04-2022-0059

Meiryani, & Warganegara, D. L. (2022). Juridical review of law enforcement on money launderers: case study from Indonesia. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-05-2022-0062

Molinari, M., & de Villiers, C. (2021). Qualitative accounting research in the time of COVID-19 – changes, challenges and opportunities. *Pacific Accounting Review*, *33*(5), 568–577. https://doi.org/10.1108/PAR-09-2020-0176

Moore, M. (2018). *Everything You Need to Know About Blockchain*. Albawaba. https://www.albawaba.net/business/everything-you-need-know-about-blockchain-1158228

Morse, J. K. (2002). Verfication Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, *1*(2). https://doi.org/10.5862/MCE.55.7

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28. https://doi.org/10.1108/JMLC-11-2019-0092

Naheem, M. A. (2018). TBML suspicious activity reports – a financial intelligence unit perspective. *Journal of Financial Crime*, *25*(3), 721–733. https://doi.org/10.1108/JFC-10-2016-0064

Naheem, M. A. (2020). The State of Kuwait's anti-money laundering & combatting terrorist financing infrastructure and performance evaluation. *Journal of Money Laundering Control*, *23*(2), 441–456. https://doi.org/10.1108/JMLC-04-2018-0034

Ng, A. W., & Kwok, B. K. B. (2017). Emergence of FinTech and Cybersecurity in a Global Financial Centre: Strategic Approach by a Regulator. *Journal of Financial Regulation and Compliance*, *16*(2). https://doi.org/https://doi.org/10.1108/JFRC-01-2017-0013

Nguyen Le, C. (2013). The growing threat of money laundering to Vietnam: The necessary of intensive countermeasures. *Journal of Money Laundering Control*, *16*(4), 321–332. https://doi.org/10.1108/JMLC-05-2013-0014

Patton, M. Q. (2003). Qualitative Research and Evaluation Methods (3rd ed.). In *Evaluation Journal of Australasia* (Vol. 3, Issue 2, pp. 60–61).

https://doi.org/10.1177/1035719X0300300213

Pavlidis, G. (2020). International regulation of virtual assets under FATF's new standards. *Journal of Investment Compliance*, *21*(1), 1–8. https://doi.org/10.1108/joic-08-2019-0051

Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 5: Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka, (2019).

Peraturan Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka, (2021).

Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 11: Pedoman Penerapam Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, 1 (2017).

Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 11 Lampiran: Pedoman Penerapam Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, (2017).

Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8: Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, (2017).

Peraturan Menteri Perdagangan Nomor 99: Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto (Crypto Asset), (2018).

Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in Cryptocurrencies and Blockchain Technologies: a Monetary Theory and Regulation Perspective. *The Journal of Financial Perspectives: FinTech*, *3*(3).

Pickett, K. H. S., & Pickett, J. (2002). *Financial Crime Investigation and Control*. Wiley.

Pontes, R., Lewis, N., McFarlane, P., & Craig, P. (2022). Anti-money laundering in the United Kingdom: new directions for a more effective regime. *Journal of Money Laundering Control*, *25*(2), 401–413. https://doi.org/10.1108/JMLC-04-2021-0041

Pramod, V., Li, J., & Gao, P. (2012). A framework for preventing money laundering in banks. *Information Management & Computer Security*, *20*(2), 88–106.

Undang-Undang Republik Indonesia Nomor 7: Mata Uang, (2011).

Reznik, O., Utkina, M., & Bondarenko, O. (2021). Financial intelligence (monitoring) as an effective way in the field of combating money laundering. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-09-2021-0102

Ruiz, E. P., & Angelis, J. (2021). Combating money laundering with machine

learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering Control*, *25*(4), 766–778. https://doi.org/10.1108/JMLC-09-2021-0106

Ryan, M., & Stahl, B. C. (2021). Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. *Journal of Information, Communication and Ethics in Society*, *19*(1), 61–86. https://doi.org/10.1108/JICES-12-2019-0138

Salehi, M., & Imeny, V. M. (2019). Anti-money laundering developments in Iran: Do Iranian banks have an integrated framework for money laundering deterrence? *Qualitative Research in Financial Markets*, *11*(4), 387–410. https://doi.org/10.1108/QRFM-05-2018-0063

Sampat, B., Mogaji, E., & Nguyen, N. P. (2023). The dark side of FinTech in financial services: a qualitative enquiry into FinTech developers' perspective. *International Journal of Bank Marketing*. https://doi.org/10.1108/IJBM-07-2022-0328

Sangwan, V., Harshita, Prakash, P., & Singh, S. (2020). Financial technology: a review of extant literature. *Studies in Economics and Finance*, *37*(1), 71–88. https://doi.org/10.1108/SEF-07-2019-0270

Sarabdeen, J. (2023). Laws on regulatory technology (RegTech) in Saudi Arabia: are they adequate? *International Journal of Law and Management*. https://doi.org/10.1108/IJLMA-03-2023-0042

Saunders, M., Lewis, P., & Thornhill, A. (2012). Research methods for business students. In *International Journal of the History of Sport* (Vol. 30, Issue 1). www.pearson.com/uk

Schneider, F., & Windischbauer, U. (2008). Money laundering: Some facts. *European Journal of Law and Economics*, *26*(3), 387–404. https://doi.org/10.1007/s10657-008-9070-x

Seebacher, S., & Schüritz, R. (2017). Blockchain technology as an enabler of service systems: a structured literature review. *8th International Conference on Exploring Services Science*, 12–23.

Shi, X., Yao, X., Liang, J., Gan, S., & Li, Z. (2022). China's cultivation of master nursing specialist: A qualitative content analysis of the stakeholders. *Nurse Education in Practice*, *63*(May), 1–7. https://doi.org/10.1016/j.nepr.2022.103359

Silva, D. (2022). Pre-service teachers' understanding of culture in multicultural education: A qualitative content analysis. *Teaching and Teacher Education*, *110*, 1–11. https://doi.org/10.1016/j.tate.2021.103580

Social Change UK. (2018). *An Introductory Guide to Qualitative Research Analysis*. https://social-change.co.uk/files/Knowledge_Hub_-_qualitative_research_analysis.pdf%0Ahttps://social-change.co.uk/blog/a-

brief-guide-to-qualitative-research-analysis

Steinhoff, L., Arli, D., Weaven, S., & Kozlenkova, I. V. (2019). Online Relationship Marketing. *Journal of the Academy of Marketing Science*, *47*(3), 369–393.

Sultana, S. (2020). Role of financial intelligence unit (FIU) in anti-money laundering quest: Comparison between FIUs of Bangladesh and India. *Journal of Money Laundering Control*, *23*(4), 931–947. https://doi.org/10.1108/JMLC-01-2020-0003

Teichmann, F., Boticiu, S., & Sergi, B. S. (2022). RegTech - Potential Benefits and Challenges of Businesses. *Technology in Society*. https://doi.org/10.1016/j.techsoc.2022.102150

Teichmann, & Wittmann, C. (2023). Practical considerations regarding the implementation of economic sanctions by Swiss financial service providers. *Journal of Money Laundering Control*. https://doi.org/https://doi.org/10.1108/JMLC-12-2022-0167

Tempo. (2023). *Tren Investor Aset Kripto Meningkat Sepanjang 2023, tapi Nilai Transaksi Menurun*. https://bisnis.tempo.co/read/1805369/tren-investor-aset-kripto-meningkat-sepanjang-2023-tapi-nilai-transaksi-menurun

Thompson, R. (2018). AML/CFT in Myanmar: a review of recent developments. *Journal of Money Laundering Control*, *21*(3), 358–369. https://doi.org/10.1108/JMLC-08-2017-0036

Truby, J. (2016). Qatar's progress towards preventing terror finance through the abuse of charitable status and the financial sector. *Journal of Money Laundering Control*, *19*(4), 500–516. https://doi.org/10.1108/JMLC-08-2015-0031

Turner, J. E. (2011). *Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud*. Wiley.

Umalkar, M. (2021). RegTech: An Untapped Opportunity. *Journal of Digital Banking*, *6*(1), 72–82.

Urumsah, D. (2012). Factors Influencing Indonesian Consumers to Use e-Services in Indonesian Airline Companies. *Doctoral Dissertation*, *July*.

Utami, A. M., & Septivani, M. D. (2022a). Regulatory Technology (RegTech): The Solution to Prevent Money Laundering in Indonesia. *Telaah Bisnis*, *23*(1), 86. https://doi.org/10.35917/tb.v23i1.288

Utami, A. M., & Septivani, M. D. (2022b). Solutions to money laundering prevention through Regulatory Technology (RegTech): Evidence from Islamic and conventional banks. *Jurnal Ekonomi & Keuangan Islam*, *8*(1), 17–31. https://doi.org/10.20885/jeki.vol8.iss1.art2

Utami, & Ekaputra. (2021). A paradigm shift in financial landscape: encouraging

collaboration and innovation among Indonesian FinTech lending players. *Journal of Science and Technology Policy Management*, *12*(2), 309–330. https://doi.org/https://doi.org/10.1108/JSTPM-03-2020-0064

Utami, S. (2021). Tindak Pidana Pencucian Terhadap Uang Virtual Money Laundering on Virtual Money. *Al-Adl : Jurnal Hukum*, *13*(1), 1–27. https://ojs.uniska-bjm.ac.id/index.php/aldli/article/view/4224

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content Analysis and Thematic Analysis: Implications for Conducting a Qualitative Descriptive Study. *Nursing and Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048

van Wegberg, R., Oerlemans, J. J., & van Deventer, O. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, *25*(2), 419–435. https://doi.org/10.1108/JFC-11-2016-0067

Viritha, B., Mariappan, V., & Venkatachalapathy, V. (2015). Combating money laundering by the banks in India: compliance and challenges. *Journal of Investment Compliance*, *16*(4), 78–95. https://doi.org/10.1108/joic-07-2015-0044

Williams, C. (2014). Artificial harmony: Why cooperative efforts to create a global financial intelligence unit have faltered. *Journal of Money Laundering Control*, *17*(4), 428–439. https://doi.org/10.1108/JMLC-08-2013-0030

Wronka, C. (2022a). Anti-money laundering regimes: a comparison between Germany, Switzerland and the UK with a focus on the crypto business. *Journal of Money Laundering Control*, *25*(3), 656–670. https://doi.org/10.1108/JMLC-06-2021-0060

Wronka, C. (2022b). "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*(2), 330–344. https://doi.org/10.1108/JMLC-04-2021-0035

Wronka, C. (2022c). Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, *25*(1), 79–94. https://doi.org/10.1108/JMLC-02-2021-0017

Zabelina, Vasiliev, & Galushkin. (2018). Regulatory Technologies in the AML/CFT. *KnE Social Sciences*, *3*(2), 394. https://doi.org/10.18502/kss.v3i2.1569

Zaman, A., Tlemsani, I., Matthews, R., & Hashim, M. A. M. (2023). Assessing the potential of blockchain technology for Islamic crypto assets. *Competitiveness Review*. https://doi.org/10.1108/CR-05-2023-0100

Zolkaflil, S., Omar, N., & Nazri, S. N. F. S. M. (2019). Implementation evaluation: a future direction in money laundering investigation. *Journal of Money*

Laundering Control, *22*(2), 318–326. https://doi.org/10.1108/JMLC-03-2018-0024

LAMPIRAN

LAMPIRAN 1 Surat Izin Penelitian 1

UNIVERSITAS ISLAM INDONESIA

FAKULTAS
BISNIS DAN EKONOMIKA

Gedung Prof. Dr. Ace Partadiredja
Universitas Islam Indonesia
Condong Catur Depok Yogyakarta 55283
T. (0274) 881546, 885376
F. (0274) 882589
E. fbe@uii.ac.id
W. fbe.uii.ac.id

Nomor : ____/DEK/10/Div.SDM/___/_____
Hal **: Permohonan Ijin Penelitian**

Kepada Yth:
Tn. TH
Flagright, APAC Representative

Assalamu'alaikum Wr.Wb.

Diberitahukan dengan hormat, bahwa mahasiswa sebelum mengakhiri pendidikan di Fakultas Bisnis dan Ekonomika UII Yogyakarta diwajibkan membuat karya ilmiah berupa riset/penelitian. Sehubungan dengan hal itu mahasiswa kami:

Nama : KHARISMA FATMALINA FAJRI
NIM : 20919050
Jurusan : Akuntansi
Alamat : Sukaluyu, Telukjambe Timur, Karawang, Jawa Barat 41361

Bermaksud mohon keterangan/data pada instansi/perusahaan yang Bapak/Ibu pimpin untuk keperluan menyusun skripsi dengan judul:

Evaluasi Pemanfaatan Regulatory Technology dalam Sistem Anti-Pencucian Uang untuk Aset Virtual di Indonesia

Dosen Pembimbing : Dekar Urumsah, SE., S.Si., M.Com(IS)., Ph.D., CFra.

Hasil karya ilmiah tersebut semata-mata bersifat dan bertujuan keilmuan dan tidak disajikan kepada pihak luar. Oleh karena itu kami mohon perkenan Bapak/Ibu untuk dapat memberikan data/keterangan yang diperlukan oleh mahasiswa tersebut.

Atas perhatian dan bantuan Bapak/Ibu, kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 05 April 2023

Dekan,

Johan Arifin, S.E., M.Si., Ph.D., CFrA, CertIPSAS.
NIK.

LAMPIRAN 2 Surat Izin Penelitian 2

UNIVERSITAS ISLAM INDONESIA

FAKULTAS
BISNIS DAN EKONOMIKA

Gedung Prof. Dr. Ace Partadiredja
Universitas Islam Indonesia
Condong Catur Depok Yogyakarta 55283
T. (0274) 881546, 885376
F. (0274) 882589
E. fbe@uii.ac.id
W. fbe.uii.ac.id

Nomor : ____/DEK/10/Div.SDM/___/_____
Hal **: Permohonan Ijin Penelitian**

Kepada Yth:
Tn. CRA dan Nn. TMB
SIJITU, AML Operating System

Assalamu'alaikum Wr.Wb.

Diberitahukan dengan hormat, bahwa mahasiswa sebelum mengakhiri pendidikan di Fakultas Bisnis dan Ekonomika UII Yogyakarta diwajibkan membuat karya ilmiah berupa riset/penelitian. Sehubungan dengan hal itu mahasiswa kami:

Nama : KHARISMA FATMALINA FAJRI
NIM : 20919050
Jurusan : Akuntansi
Alamat : Sukaluyu, Telukjambe Timur, Karawang, Jawa Barat 41361

Bermaksud mohon keterangan/data pada instansi/perusahaan yang Bapak/Ibu pimpin untuk keperluan menyusun skripsi dengan judul:

Evaluasi Pemanfaatan Regulatory Technology dalam Sistem Anti-Pencucian Uang untuk Aset Virtual di Indonesia

Dosen Pembimbing : Dekar Urumsah, SE., S.Si., M.Com(IS)., Ph.D., CFra.

Hasil karya ilmiah tersebut semata-mata bersifat dan bertujuan keilmuan dan tidak disajikan kepada pihak luar. Oleh karena itu kami mohon perkenan Bapak/Ibu untuk dapat memberikan data/keterangan yang diperlukan oleh mahasiswa tersebut.

Atas perhatian dan bantuan Bapak/Ibu, kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 05 April 2023

Dekan,

Johan Arifin, S.E., M.Si., Ph.D., CFrA, CertIPSAS.
NIK.

LAMPIRAN 3 Protokol Pengumpulan Data

No.	Dokumen/Pertanyaan	Sumber Data (Jenis)	Topik (Rumusan Masalah)
1	Undang-Undang Nomor 7 Tahun 2011 tentang Penggunaan Mata Uang	Sekunder (Dokumen Regulasi)	Mekanisme Anti-Pencucian Uang untuk Aset Kripto di Indonesia (RM 1)
2	Peraturan Menteri Perdagangan Nomor 99 Tahun 2018 tentang Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto		
3	Peraturan Bappebti Nomor 8 Tahun 2021 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto		
4	Peraturan Bappebti Nomor 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto di Bursa Berjangka		
5	Peraturan Bappebti Nomor 11 Tahun 2017 tentang Pedoman Penerapan Program APU/PPT pada Pialang Berjangka		
6	Peraturan Bappebti Nomor 8 Tahun 2017 tentang Penerapan Program APU/PPT pada Pialang Berjangka		
8	Bagaimana tanggapan Bapak/Ibu mengenai tren kasus pencucian uang melalui aset kripto di Indonesia?	Primer (Wawancara)	Penyebab Pemanfaatan RegTech Tidak Efektif (RM 2)
9	Apakah Bapak/Ibu dapat memberikan gambaran mengenai pemanfaatan RegTech di Indonesia?		
10	Bagaimana pemanfaatan RegTech pada proses jual-beli aset kripto di Indonesia?		
11	Mengapa pemanfaatan RegTech pada proses jual-beli aset kripto belum menunjukkan hasil yang signifikan?		
12	Apa kritik Bapak/Ibu terhadap pemanfaatan RegTech untuk proses jual-beli aset kripto di Indonesia?		Rekomendasi Perbaikan terhadap Pemanfaatan RegTech (RM 3)
13	Bagaimana saran dan rekomendasi Bapak/Ibu untuk meningkatkan pemanfaatan RegTech sehingga hasilnya memiliki pengaruh yang siginifikan terhadap pencegahan pencucian uang melalui aset kripto di Indonesia?		

LAMPIRAN 4 Transkrip Wawancara 1

Narasumber : P1

Jabatan / Instansi : Asia-Pacific Representative / Flagright

Kompetensi : Anti-Money Laundering Operating System

Tempat, Tanggal : Zoom Meeting, 25 Juli 2023

P : Pewawancara

N : Narasumber

P : Halo, Pak Tommy. Selamat Pagi, izin mempekenalkan diri kembali. Saya Kharisma dari Universitas Islam Indonesia. Sebelum memasuki sesi wawancara, silahkan Bapak memperkenalkan diri terlebih dahulu.

N : Oke, saya Tommy. Saya representative-nya Flagright di Asia Pasifik. Jadi saya handle dari growth sampai requirement. Jadi mengerti lah tentang requiremetnt-requirement yang ada di jurisdiction berbeda-beda, di Filiphina, di Indonesia. Dan covers-nya dari Flagright sebenarnya lebih banyak transaksi yang fiat, jadi transaksi yang uang currency, bukan yang crypto. Makannya saya pengen coba meeting untuk mengerti sih dari pertanyaan-pertanyaan itu akan fokus semuanya di crypto atau emang ada fiat-nya.

P : Oke, Pak. Jadi kalau di Indonesia setelah saya mencari tahu dari beberapa referensi itu tidak semuanya crypto, tapi ada perpindahan ke fiat. Jadi saya rasa masih ada nyambungnya begitu ya, Pak.

N : Hmm, iya. Karena di Indonesia kan untuk yang crypto agak berbeda dengan yang di luar. Kalau di luar kan bisa jadi alat pembayaran, kalau di Indonesia hanya bisa jadi komoditas. Jadi antara dia beli dan jual, dan nanti ada margin-nya gitu lah. Nah tentang kemungkinan pencucian uang di Indonesia sebenarnya lebih sedikit di Indonesia karena tidak ada pembayaran, kecuali yang illegal ya. Kalau yang illegal itu bisa jadi alat pembayaran. Karena kalau misalnya jadi komoditas itu sama seperti kita membeli saham, jadi nanti kita hold terus abis itu dalam jangka waktu tertentu naik kita jual. Nah, di situ kita dapat keuntungan. Kedua, yang tentang, kan pertanyaan-pertanyaannya apa yang terjadi dalam aktivitas pencucian uang di crypto ya?

P : Iya, lebih ke penggunaan RegTech-nya itu Pak. Kenapa dari penelitian sebelumnya itu kan hasilnya tidak signifikan. Nah, di penelitian ini mau meng-

explore kenapa tidak signifikannya itu, apakah ada faktor dari SDM-nya, atau dari …

N : Kalau boleh tau, boleh di-elaborasi gak tidak signifikannya seperti apa? Mungkin dari penelitiannya atau dari observasinya, apa yang dilihat sehingga jadi konklusi bahwa ini tidak signifikan?

P : Dari adaptasi dari penggunaan RegTech-nya itu Pak. Jadi masih belum masif gitu penggunaan RegTech-nya itu.

N : Oh jadi penggunaanya ya.

P : Iya penggunaannya, terutama untuk di FinTech.

N : Oke oke, kalau boleh tau, ini juga coba mengerti lebih jauh ya. Seberapa jauh pengetian dari RegTech yang sekarang, so far, yang dimengerti oleh Kharisma sekarang ini.

P : Kalau yang saya pahami, RegTech itu Regulatory Technology ya Pak, yang digunakan oleh lembaga-lembaga keuangan atau kalau sekarang digunakan juga oleh FinTech-FinTech, yang dimana di situ tujuannya untuk memudahkan dalam pemenuhana regulasi-regulasi yang diminta atau yang harus dipenuhi di Indonesia kalau di Indonesia.

N : Iya, dan kalau saya bisa elaborasi lebih dalam lagi. Ambil contoh dari sebuah journey lah ya, misal saya pengguna crypto, ada sebuah perusahaan crypto, saya mau daftar di satu perusahaan crypto untuk jual beli crypto. Nah, journey-nya itu kan dimulai dari kita masuk, daftar di aplikasi kita masukin e-mail, terus nanti ada OTP, nanti ada kayak KYC, ada foto, liveness checking, sampai nanti dia on boarding di dalam, dia transaksi jual-beli, dan terjadi satu aktivitas relationship antara saya sebagai pengguan crypto dengan perusahaan crypto. Nah, tujuan utama dari RegTech itu adalah memastikan setiap perjalanan user dari pertama kali masuk, masukin e-mail, nomor HP, dapat OTP, sampai dia udah mulai jual-beli crypto, semua journey-nya accountable. Maksudnya accountable itu adalah, pas dia masuk, dia daftar, nomor yang dia daftarkan itu sesuai yang dia punya, dia gak pakai nomor orang lain lah, atau kayak sekarang kan ada SMS OTP yang dia scam call kan ya. Nah, itu satu, accountable. Kedua, dia daftar, apakah nomor yang dipakai sesuai dengan siapa yang memakai, yaitu kan ada upload KTP, pengecekan foto liveness checking, apakah ini orangnya sesuai dengan orang yang ada di KTP. Nah, accountable, memastikan saya menggunakan dokumen milik saya untuk mendaftar, itu yang kedua. Yang ketiga, oke saya sudah memastikan bahwa saya adalah siapa yang saya daftar di aplikasi crypto, baik crypto atau non crypto sama sih. Jadi, saya sudah memastikan bahwa saya adalah siapa yang saya bilang saya. Nah, tugasnya perusahaan itu adalah memastikan apakah saya ini masuk ke dalam daftar hitam,

baik dari daftar hitam DTTOT (Daftar Terduga Teroris dan Organisasi Teroris) yang kepolisian di Indonesia ataupun yang internasional, sanction listing atau OFAC list, OFAC list yang informasi terbuka yang tentang siapa aja yang masuk ke sanction list atau blacklist. Nah itu memastikan bahwa perusahaan crypto ini mau membentuk satu relationship dengan calon nasabah, itu nasabah ini clean, tidak ada daftar hitam karena kan balik lagi perusahaan ini kan risk appetite, deal dengan orang-orang yang risk-nya segini level lah, saya bisa toleransi risikonya segini lah misalnya contohnya. Yang paling penting tidak ada di daftar hitam di sanction list. Mungkin DTTOT di Indonesia akses DTTOT belum banyak yang bisa dapat, nah itu juga satu aksesabilitas perusahaan, gak semua orang dapat akses DTTOT daftar hitam kepolisian.

P : Nah itu sebabnya apa Pak?

N : Kebanyakan akses ini sifatnya ekslusif, lebih ke edukasi ke perusahaan A, kan kebanyakan perusahaan pada berfikir sanction list lah, udah berfikir satu kiblat yang yang besarnya sanction. Tapi kan di Indonesia, lokal, kan ada maintain DTTOT. Nah bisa aja DTTOT ini belum dilaporkan di sanction. Jadi bisa aja saya perusahaan crypto atau non crypto ini on boarding seseorang yang di sanction bersih nih, tapi di DTTOT hitam. Nah itu kan risiko juga kan. Tapi balik lagi, perjalanan RegTech itu memastikan setiap lini perjalanan itu accountable. Jangan sampai ada satu bagian itu yang tidak accountable, itu akan bermasalah. Nah, tadi kita baru sampai, kita memastikan saya itu siapa, sudah mengecek saya itu tidak ada di daftar hitam sanction list atau OFAC list. Masuk sebagai, kalau di perusahaan itu user ID-nya lah, jadi sudah dapat user ID-nya. Biasanya kalau sebagai RegTech dia akan di-tag, misalnya saya Tommy risikonya medium karena baru awal, belum ada catatan transaksi, belum ada catatan aktivitas, masih medium. Nanti berjalannya waktu, misalnya contoh buat crypto, saya jual-beli crypto, kalau misalnya e-wallet, kalau pakai ovo ya misalnya saya transfer atau saya bayar, itu aktivitas ini akan memberikan dampak ke risiko, risk assessment-nya nasabah. Nah itu juga harus accountable, bagaimana nanto, misalnya contoh, pas saya daftar aplikasi itu saya tidak ada di daftar hitam, tapi kan daftar hitam itu kan berubah terus nih, update terus, internasional maupun lokal. Nah itu ada ngecek terus, apakah saya ada di daftar hitam, periodik. Kadang-kadang perusahaan ada yang 3 bulan, 6 bulan, ada yang 1 tahun. Jadi periode ini sebenarnya tidak ada Undang-Undang nya kalau di Indonesia secara spesifik berapa lama kamu harus periodic checking. Karena periodic checking ini biaya untuk perusahaan, per checking ini ada cost, berapa ribu sampai berapa puluh ribu rupiah. Kalau USD-nya berapa puluh cents lah.

P : Oke Pak, saya mau balik lagi nanya kalau misal di Internasional dia masuk daftar hitam, tapi di nasional belum masuk daftar. Nah itu yang dilakukan

perusahaan bagaimana? Kan tadi dijelaskan Bapak, yang terpenting accountable. Nah apakah perbedaan itu tidak menjadi masalah?

N : Balik lagi, risk appetite-nya perusahaan itu. Jadi perusahaan kan sebenarnya dari Tim APU-PPT nya itu kan biasanya ada satu daftar, kayak satu dokumen, ini loh risk appetite-nya saya, yang kalau internasional, kalau sudah masuk daftar hitam kebanyakan tidak mungkin di on board sih. Jadi risk appetite-nya misalnya ada toleransi apa yang bisa, misalnya dia masuk daftar hitam, oke itu udah out of question, itu udah gak boleh masuk. Mungkin kalau yang di Indonesia, pengadilan contohnya. Kalau pengadilan belum ada catatan putusan, tetap bisa on boarding karena belum ada kekuatan hukum tetap kan ya, kecuali kalau nanti udah ada kekuatan hukum tetap, baru nanti bisa di off board.

P : Nah dari situ Pak, dari pengadilan belum ada penetapan, itu bukannya ada risiko juga ya Pak untuk dia melakukan kejahatan keuangan?

N : Iya, betul betul. Makannya kalau misalnya yang kayak begitu, berarti dia tetap bisa on board. Kadang ada beberapa financial institution yang dia bisa on board tapi ada notice, jadi ini user-nya high risk. Kalau user-nya high risk maka akan dipantau lebih sering, kayak gitu. Nah, dari situ misal putusan sudah keluar atau memang bahkan putusan belum keluar tapi ada aktivitas yang mencurigakan maka bisa di-freeze atau di off board.

P : Berarti selama perjalanan dia on board itu terus menerus begitu ya, Pak?

N : Iya, betul. Yang paling penting adalah accountable-nya. Jadi kalau misalnya dibilang ada risiko pasti ada risiko, setiap perusahaan punya toleransi risiko yang berbeda-beda. Mungkin ada perusahaan yang langsung sudah lihat dia masuk pengadilan, sudah off board "saya tidak mau deal dengan nasabah seperti ini". Mungkin ada perusahaan yang lain tetap keep. Balik lagi mereka ada pertimbangannya masing-masing sih.

P : Untuk pertimbangan itu, apa dari regulator ada batas minimalnya tidak, Pak? Atau itu bergantung dengan perusahaannya masing-masing?

N : Kalau dari pemerintah kan yang sudah pasti kalau sudah berkekuatan hukum tetap, sudah gak boleh. Tapi selama yang belum, kan kita apa ya dibilangnya? Kan kalau untuk Undang-Undang nya saya kurang ngerti ya, tapi ada satu bagian yang dibilangnya kita harus, apa namanya, prasangkanya tidak boleh langsung salah gitu.

P : Ohh, asas praduga tak bersalah.

N : Iya, iya, kayak gitu. Karena kita kalau misalnya melakukan itu, melanggar hukum juga karena kita langsung judges gitu dan dia bisa sue perusahaan itu juga

karena belum ada kekuatan hukum tetap tapi sudah di-treat ini, serba salah jadinya, gitu.

P : Kalau untuk penilaian risiko, Pak. Kan sebelum KYC itu ada penilaian risiko ya Pak. Nah, kalau di Indonesia itu sebenarnya penilaian risiko ini sudah menggunakan RegTech atau belum Pak? Karena kalau yang saya baca di Undang-Undang nya, di peraturan yang dari Bappebti itu, Bappebti ini tidak secara lugas memerintahkan bahwa penilaian risiko itu harus menggunakan RegTech. Jadi dari realisasinya sendiri apakah RegTech sudah digunakan atau belum?

N : Kalau sekarang saya lihat dari market, ada yang menggunakan, ada yang tidak. Kalau misalnya perusahaan FinTech yang masih kecil, mungkin tidak. Bahkan the worst yang saya pernah lihat ya, ya mereka pakai google sheet aja. Jadi ini list customer-nya, ini paling ada warna, ini "low risk", "medium risk", "high risk". Jadi kayak cuma di google sheet edit-edit doang untuk penilaian risikonya. Dan so far masih ada yang berjalan gitu. Bagi perusahaan kan selama solusinya masih berjalan, ya pakai saja, kecuali ini sudah tidak berjalan. Karena untuk meraka untuk pakai RegTech ada satu investasi dan investasi ini biasanya tidak kecil kan. Nah, kalau misalnya kita lihat FinTech yang kecil ya fokusnya growth, jangan sampai mereka itu terganggu lah. Mereka fokusnya tetap di growth dulu sih.

P : Tapi itu memengaruhi kerja dari sistem AML-nya sendiri gak Pak?

N : Sangat, sangat memengaruhi. Sama aja kayak kalau pakai RegTech kan dia otomatis tuh, jadi ada informasi ini masuk, kriteria apa, anda masuk risiko kecil atau risiko menengah atau risiko besar. Kalau manual seperti itu pasti ada satu, yang paling inti saja, human error, ya kan? Kalau kita manual kadang kita ketik aja salah. Human error misalnya dia nge-judge satu risiko bahwa ini risiko kecil atau risiko besar, human error tuh lumayan gede. Apalagi ketika kita mengecek KYC-nya manual. Jadi ada beberapa kayak misalnya perusahaan remittance atau perusanaan business account yang disini, ketika daftar itu harus menunggu satu minggu untuk apakah bisa on board atau gak. Satu minggu ini biasanya untuk dikirim ke Tim APU-PPT nya untuk kayak dibacain semuanya satu-satu, terus apakah ini masuk kriteria, pelan-pelan kayak gitu kan. Tapi kalau misalnya 1 investigator, 10 aja satu hari kan, ya bisa saja 1 salah. Ya namanya manusia kan, pasti ada salah melihatnya. Itu risikonya. Tapi ya itu risk appetite-nya perusahaan juga sih.

P : Berarti kalau misal saya highlight ya Pak. Sebenarnya mau perusahaan kecil atau besar, juga membutuhkan RegTech, tapi dari size-nya saja mungkin yang membedakan?

N : Iya, kebanyakan volume dari transaksi, volume user, itu salah satu konsiderasinya juga sih. Kadang-kadang ada yang user-nya banyak pun mereka belum mau masuk ke RegTech.

P : Alasannya kenapa Pak biasanya?

N : Karena belum untung.

P : Oh, jadi tetap dinilai investasinya juga ya Pak antara cost and benefit-nya.

N : Iya. Kadang-kadang gini pemikirannya, saya employed RegTech 200 Juta, bandingkan dengan hiring orang, 10 orang atau 20 orang buat eye bowling-in semua. Ada pertimbangannya masing-masing sih.

P : Tapi semisal dari pandangan Bapak, untuk perusahaan FinTech sekecil apapun, ada baiknya sudah menggunakan RegTech ya Pak? Baik itu menggunakan vendor atau build sendiri.

N : Iya, iya, betul. Tapi gak semua perusahaan kan punya tim development yang memadai kan ya.

P : Iya, iya.

N : Nah itu pertimbangan lagi sih. Memang secara natural-nya memang perlu untuk ada sistem karena balik lagi, human eye bowl itu paling tinggi error-nya, begitu.

P : Nah oke, kalau dari SDM-nya sendiri Pak. Kalau dari Flagright yang saya lihat kan lebih ke memasang RegTech. Nah dari Flagright sendiri, itu apakah hanya memasang sistem saja atau berjalan berkesinambungan sampai dengan pelatihan SDM-nya itu sendiri dan pengawasan dari sistemnya?

N : Kalau dari kita, kita ada pemasangan sistemnya dan ada juga buat consulting-nya juga. Jadi consulting-nya misalnya dia pasang sistemnya kita, kita consult nih, oke kamu pasang sistem ini sesuai dengan regulasi di jurisdiction yang ada kan. Nah itu nanti kita ada consultation-nya. Nah, tentang bagian SDM-nya, ini sebenarnya masih baru banget ya karena kita masih diskusi. Sempat ada pemikiran bahwa “Well, mereka yang punya bisnis, mereka gak ngerti kan tentang APU-PPT. Kenapa gak kita offering aja?”, maksudnya “Kamu cari orang APU-PPT lah yang memang punya pengalaman”, ya kita bisa solved untuk itu. Tapi ini baru pertimbangan. Kita belum masuk ke dalam sana, tapi ada petimbangan kesana karena banyak FinTech-FinTech yang gak ngerti gitu maksudnya ya “Oh ini saya perlu ya?” karena ada salah satu juga yang saya ngomong, perusahaan payment juga di Philippine, hmm “Saya sudah dapat license nih, tapi apa yang harus saya lakukan?” itu untuk di bagian APU-PPT nya, karena “Saya gak ngerti nih, yang saya tahu, saya sudah dapat license, saya bisa jualan”, dan sudah, jualan, dapetin

user, selama user ada transaksi banyak, saya untung. Tapi ada satu akuntabilitas yang harus dijaga, yaitu di dalam bahwa user yang di-on board, transkasi yang dieksekusi adalah yang bersih, gitu. Karena informasi ini kan nanti akan di-judge di pengadilan. Contoh misalnya ada kasus ya, "Apakah anda sudah melakukan planning atau perencanaan di perusahaan kamu?", kalau belum ada habis lah itu. Kalau ada pun, seberapa extend anda sudah melakukan, "Apakah anda sudah melakukan otomatisasi? Machine learning kah? AI kah? Seberapa dalam anda implementasi itu?", itu akan menjadi pembeda juga.

P : Oke, kalau dari regulasinya sendiri Pak, apakah sudah meng-cover semua hal yang Bapak sebutkan tadi?

N : Kalau regulasi, ada sih. Ada secara tertulis bahwa ada keperluan untuk melaporkan STR (Suspicious Transaction Reports), kan melalui goAML ya kalau di Indonesia.

P : Iya, iya.

N : Nah, tapi menurut saya masih belum secara terperinci sih karena ini regulation yang dibuat kan untuk mencakup semua, baik yang kecil maupun yang besar. Nah, kecil besarnya FinTech ini kalau di internasional sudah dibedakan secara regulasinya karena kita gak bisa menggunakan satu regulasi untuk ketok rata semua. Tapi ya harus dimaklumi juga karena Indonesia kan masih on progress ya, apalagi masih mencoba untuk menjadi member-nya FATF nih, belum ada result-nya. Ya harapannya dengan jadi member FATF, kita ada diedukasi juga. Jadi Indonesia diedukasi oleh beberapa negara lain yang sudah mature di sistem APU-PPT. Harapannya bisa lebih di apa ya, di-encourage lah ya institusi finansial di Indonesia.

P : Berarti kalau secara regulasi itu masih abu-abu gitu ya Pak? Antara ini apakah untuk FinTech yang besar saja atau sudah mencakup semua.

N ; Iya, iya. Karena pelaporan untuk perusahaan yang besar ya, sama FinTech yang sekarang nih yang masih bertumbuh atau masih just introduce nih di Indonesia, totally berbeda karena ya yang sudah besar kan mereka sudah punya satu standar sendiri kan ya. Dan kalau yang bertumbuh, ya mereka banyak yang bingung harus gimana. Untungnya di Indonesia pakai goAML, goAML ini mereka ada satu template yang sangat membantu lah, Cuma adopsinya yang masih kurang baik karena belum ada satu apa ya, kayak petugas check-nya itu gak begitu banyak. Karena petugasnya OJK kan gak begitu banyak dan mereka banyak fokus yang terkenal saja, yang kecil-kecil masih belum bisa terangkul lah, kayak gitu.

P : Berarti memang dari regulasinya sendiri belum terlalu memdai begitu ya Pak untuk dirangkul "Oke FinTech ini harus menggunakan RegTech".

N : Iya, apalagi sebelumnya kita tahu crypto kan dipegang sama Bappebti ya.

P : Iya, sekarang baru mau switch ke OJK dan BI.

N : Sebenarnya gak switch sih, kalau kemarin saya baru lihat beritanya adalah kerjasama. Jadi Bappebti tetap ada, ada involved OJK sama BI. Jadi OJK dan BI itu yang akhirnya memberikan 'expert advice' lah ini harus begini harus begini. Makannya Bappebti kemarin bikin exchange house juga kemarin kan, bahwa ini regulasi kalau untuk exchange house begini, kalau buat wallet-nya harus begini. Ya jadi kayak expert advice lah.

P : Jadi kayak kolaborasi lah ya Pak?

N : Iya, kemarin sempat saya pikir juga bakal dipindah tangan kan, tapi kayaknya enggak deh kalau saya lihat.

P : Iya, saya kira juga bakal dipindah tangan gitu Pak.

N : Iya, hehe.

P : Oke Pak. Nah katakanlah kita membicarakan FinTech yang besar gitu ya Pak ketika dia menggunakan RegTech dari vendor, misal dari Flagright arau yang lain. Nah itu sebenarnya dari pemerintah sendiri, dari regulator, itu ada VDD (Vendor Due Dilligence)-nya gak Pak? Untuk sistem ini, RegTech ini gak apa-apa digunakan.

N : Katanya akan, untuk sekarang belum sih. Untuk sekarang mereka masih lihat ya vendor ini kalau misalkan goAML punya template, ya sesuai atau tidak sesuai, gitu saja sih.

P : Berarti selama ini untuk acuan vendor RegTech-nya sendiri kemana Pak?

N : Internasional, jadi untuk jurisdiction lain yang pakai goAML, ini contohnya, ini best practice-nya, kita share ke Indonesia.

P : Oke, tapi kalau di Indonesia sendiri, sebenarnya kan ada perbedaan ya Pak? Maksudnya, ada perbedaan yang signifikan gak Pak dari penerapannya?

N : Kalau goAML gak ada perbedaan.

P : Gak ada perbedaan, berarti kalau dari goAML yang digunakan oleh negara lain, itu bisa diadaptasi secara langsung atau dia masih ada adjustment lagi?

N : Kalau yang pelaporan goAML-nya, formatnya itu enggak, gak perlu adjustment lagi karena memang sama semua di negara-negara yang adopt goAML. Yang paling

perbedaannya adalah skenario-skenarionya karena setiap negara kan punya skenario yang berbeda-beda. Misal contoh, aktivitas APU-PPT yang di luar negeri berbeda dengan yang di Indonesia karena cara pencucian uang di Indonesia sama di luar negeri kadang-kadang ada yang beda.

P : Biasanya perbedaan yang mencolok itu di bagian mana Pak? Maksudnya kalau secara keseluruhan kan tahapannya dari penilaian risiko, KYC, transaction monitoring, dan pelaporan, itu kan sama dengan negara lain. Jadi yang lebih membedakannya itu bagian spesifik yang seperti apa ya, Pak?

N : Jadi, contoh bagian transaction monitoring, ada skenarionya. Contoh kalau di Singapore ada money muling, ketika orang menggunakan akun-akun murid-murid sekolah untuk mencuci uang. Nah kalau di Indonesia kan kebanyakan ini dipakai untuk, contoh yang paling banyaknya pencucian uang dari hasil tindak pidana korupsi. Nah itu kan dia menggunakan transaksi dengan PT-PT shell company, nah kalau di Indonesia lebih banyaknya dengan shell company. Kalau di luar negeri lebih banyaknya pencucian uang dengan humans, students. Malaysia juga, Malaysia kan banyaknya universitas, students, itu banyak dipakai juga. Makannya kemarin saya banyak diskusi juga dengan satu universitas di Malaysia, UCSI, mereka kan juga ada satu e-wallet license juga, namanya UCSI Pay, itu tujuannya untuk membayar uang kuliah lah contohnya. Nah itu saja, walaupun dipakai internal juga ada yang main juga. Nah, memang penggunaan teknologi bagus lah, memang kan mempermudah untuk orang membayar uang kuliah lah. Tapi ada risiko-risiko yang harus di-apa ya namanya, harus dicek juga dan mereka aware bahwa ini ada satu masalah serius juga yang harus ditangani.

P : Kalau dari RegTech-nya sendiri Pak. Itu sejauh mana RegTech ini bisa mendeteksi adanya transaksi mencurigakan? Khususnya di crypto ini Pak, karena kalau di crypto itu kan transaksinya menggunakan blockchain yang nantinya terenkripsi, jadi gak tau nih transaksinya punya siapa.

N : Kalau misalnya gak tau punya siapa, sekarang kalau di US ada bikin namanya, kayak credit bureau, biro kredit gitu, sekarang buat crypto juga. Jadi ini address-address yang high risk, dia ada database-nya. Itu kalau yang di luar negeri kayak gitu. Kalau di Indonesia, yang non crypto ya biro kredit lah, KBIJ (Kredit Biro Indonesia Jaya), Pefindo (Pemeringkat Efek Indonesia). Itu mereka ngecek, saya misalnya kredit, apa ya kalau di Indonesia, SLIK?

P : Oh iya, SLIK, SLIK OJK.

N : Nah itu sama sistemnya, tapi buat crypto. Jadi kalau misalnya SLIK itu untuk manusianya, nah kalau yang di US itu untuk address-nya, alamat crypto-nya.

P : Kalau di Indonesia belum kesana ya Pak?

N : Mungkin ada yang coba tapi belum aku lihat sih.

P : Oke, berarti Pak kalau yang saya Tarik dari tidak signifikannya pemanfataan RegTech itu, pertama bisa dari regulasinya sendiri, yang dia belum merangkul semua size dari FinTech ini?

N : Iya, iya, karena masih belum memadai lah dari regulatornya.

P : Dan yang kedua tadi dari SDM-nya juga belum mengetahui "Apa yang harus saya lakukan?" begitu.

N : Iya, masih banyak yang "Oh saya dapat lisensi, kira-kira butuh apa?", memang secara regulasi tertulis tapi kan tidak semua orang bisa membaca dan translate apa yang 'saya' lakukan kan? Kecuali ada lawyer atau konsultan yang membaca ini dan "Oke gua baca ini, gua perlu ini", nah ini translation yang masih agak susah.

P : Oke Pak, ini seperti yang tadi Bapak bilang, dari Flagright sendiri ada rencana untuk memberikan pelatihan dan pendampingan kepada FinTech-FinTech. Nah ini kan Flagright dari pihak swasta, kalau dari negara sendiri atau pemerintahan sendiri, itu ada tidak Pak? Kayak memastikan atau memberikan pelatihan gitu, Pak.

N : Lewat itu, lewat AFTECH (Asosiasi FinTech Indonesia). Nah itu sekarang kan perusahaan-perusahaan yang mau daftar lisensi PJP (Penyedia Jasa Pembayaran) 1, 2, 3, itu minimal requirement-nya sekarang ya, member-nya AFTECH. Jadi untuk jadi member-nya AFTECH mereka harus daftar dan ajak tim-nya pelatihan. Jadi ada pelatihan-pelatihan lah untuk requirement-nya.

P : Nah itu kan untuk FinTech-FinTech yang sudah legal ya, Pak?

N : Iya.

P : Kalau untuk FinTech-FinTech yang illegal itu, bagaimana Pak menanggulanginya?

N : Nah itu, itu, dari awal secara legal standing kan udah gak benar ya. Jadi untuk bagian itu kita gak lihat sih.

P : Ada pengawasannya tidak Pak dari regulator?

N : Ada kan, biasa kalau OJK ada setiap bulan ya kadang-kadang ini yang illegal-illegal akan di-block di Kominfo, kayak gitu. Kalau illegal, ya pasti ada. Kita kan living di internet ya, setiap orang bisa beli domain dan langsung bikin-bikin sesuatu kan, dan ya tugasnya regulator, pemerintah, ya untuk mengecek dan memastikan bahwa mereka itu tidak bisa diakses di Indonesia. Tapi balik lagi karena ada bisnis, ada uangnya, ya pasti mereka cari jalur puternya seperti apa. Nah, kayak gitu.

P : Iya ya, Pak.

N : Risiko tetap ada, kita gak bisa bilang risiko itu 0. Bahkan di negara maju pun masih tetap ada dan hal yang illegal itu masih banyak. Nah, tentang yang jadi masalahnya "Apakah pemerintah ini bisa untuk mendeteksi itu atau membuat program untuk mendeteksi itu?", kalau sekarang kan misalnya ada LaporKu ya, untuk kalau misalnya ada scam, ada fraud. Nah, satu kebijakan-kebijakan yang bisa untuk membantu ngecek yang illegal-illegal ini. Karena balik lagi, kalau misal yang illegal-illegal ini bisa bekerja dan mereka bisa dapat uang, yang legal ini yang pusing "Lah, user-user saya banyakan milih yang illegal dong?". Pertama, cost-nya mereka kan gak banyak, cost dari illegal, karena cost untuk licensing ini gak kecil. PJP 3 aja minimal 500 Juta, PJP 1 itu sampai 15M, itu untuk biaya lisensi saja. Nah pertanyaan balik lagi "Ini saya sudah keluar segini, bagaimana cara saya invest biar bisa dapat uang?", kan sebagai bisnis kan. Nah itu yang menjadi, apa ya, satu dorongan lah yang menjadi kenapa harus illegal? Ya karena illegal gak perlu lisensi dan gak perlu modal besar.

P : Oke, Pak. Berarti dari implementasi RegTech ini menurut perusahaan harus berbanding lurus sama cost and benefit-nya perusahaan ya, Pak? Walaupun sebenarnya RegTech itu, salah satu kelebihannya kan ada cost and time efficiency ya Pak yang saya tahu.

N : Iya.

P : Nah tapi untuk mendorong perusahaan menggunakan RegTech, itu tetap kembali kepada penilaian perusahaan antara cost and benefit yang mereka dapat gitu ya Pak?

N : Betul. Saya ambil contoh implementasi RegTech 200 Juta, terus saya hiring 10 orang misalnya, 1 orang 10 Juta per bulan misalnya, nah itu 100 Juta. Sisa 100 Juta-nya saya bisa pakai untuk growth-nya FinTech, perbandingan lagi kan? Kebijakan perusahaan masing-masing, kayak gitu.

P : Kalau penilaian secara relatifnya, implementasi RegTech itu tergolongnya mahal atau murah?

N : Kalau misal kayak kita contoh ya sanksi-sanksi nya atau risikonya lah kalau misal terjadi money laundering kan besar sekali. Ya bisa aja misal kayak contoh pas kemarin sempat ada masalah di satu aktivitas money laundering lah, itu masuk ke pengadilan. Itu FinTech-nya sudah gak boleh beroperasi, karena mereka harus diam dan ngecek semua transaksinya, apakah ada uangnya itu kemana aja. Balik lagi kan, bisnis kalau tutup, kalau gak beroperasi, pengadilan kalau bilang "Oke, anda gak boleh beroperasi 6 bulan", nah itu, apakah risiko ini sepadan dengan implementasi RegTech kan itu berbeda-beda kan ya. Ada orang yang mungkin oke

dengan 6 bulan gak berjalan gak apa-apa, kayak contoh yang kita lihat, mungkin pernah aware dengan crypto juga, namanya Luno. Luno 8 bulan tidak beroperasi karena sempat ada kendala di bagian transaksi dan ya begitu, sampai akhirnya harus di-freeze dan sampai akhirnya terjadi lay off. Karena yah, namanya bisnis kalau misalnya gak berjalan, tetap ada expenses bulanan, ya pasti yang sebagai investor juga mereka mau tutup kerannya, ya gak boleh lagi dong karena kita tida ada income, expense terus, ya gak bisa juga kan, kayak gitu.

P : Berarti masih tergantung sama preferensi dari perusahaannya itu sendiri ya Pak?

N : Iya, tapi tetap dari kita, kita sebagai pihak swasta akan edukasi dan pemerintah juga edukasi bahwa dengan adanya RegTech, paling besar itu kita meminimalisir human error untuk itu. Yang kedua untuk compliance, ya kadang-kadang untuk transaksi ketika kita eye bowl, itu gak terdekteksi apa yang terjadi gitu. Misalnya saya ada A transfer B, B transfer C, C transfer A, kalau misalnya kita Cuma lihat daftar transaksi ini gak keliatan pattern-nya. Tapi kalau misalnya pakai machine learning yang digunakan RegTech, bisa tahu "Ini uang yang saya transfer 100 Juta balik lagi ke saya lagi", nah ini apa yang terjadi, apa duitnya diputar di sini gitu. Nah itu juga jadi pertanyaan dan bisa dijaring gitu intinya. Kalau pakai eye bowl, itu kemungkinan untuk dijaringnya agak kecil sih.

P : Nah dari pihak swasta dan pemerintah sendiri, bagaimana gitu Pak untuk mengajak dan memberi tahu bahwa "RegTech ini penting loh"?

N : Pertama, kalau misalnya sebagai yang dari RegTech, ya yang paling penting dari pemerintah kan ada Undang-Undang nya, sudah ada Undang-Undang nya, ya mereka yang gak ngerti yang mereka udah ada license, ya mereka kita kasih tahu "Ini kamu sudah ada license, kamu butuh ini loh. Sesuai dengan Undang-Undang ini, kamu butuh transaction monitoring kah, atau customer risk assessment", nah dari situ baru kita edukasi. Kadang-kadang mereka gak ngerti kan "Saya butuh apa sih?", nah kita yang datang, kita yang ngomong bahwa "Ini kamu PJP 1, PJP 2, PJP 3, requirement kamu ini ini, dan apakah kamu sudah implementasi? Kalau belum, ya ini solusinya", nah balik lagi ke perusahaan apakah mereka mau solusinya atau mau build in house atau manual, ada beberapa opsi lah mereka.

P : Itu permintaan dari perusahaannya atau secara proaktif dari vendor RegTech-nya?

N : Dua-dua nya, kadang-kadang kita yang out list atau mereka yang in bound meminta.

P : Kalau dari swasta sendiri ada kerjasama dengan pemerintah gak Pak yang sudah terealisasi?

N : Ya paling lewat AFTECH, kegiatan-kegiatan AFTECH.

P : Oh berarti pemerintah mengajak swasta untuk memberikan edukasi gitu Pak.

N : Iya, iya. Jadi AFTECH kan sering banget tuh ada event-event, pelatihan-pelatihan dan mereka ajak swasta "Hei ini dari RegTech ini, ajarin buat bagian ini", ini ada di bagian lembaga edukasinya lah.

P : Tapi kalau dari pemerintah sendiri, pernah gak Pak mengajak swasta untuk kayak "Oke kita duduk bareng untuk memformulasikan penggunaan RegTech ini harus bagaimana dan seperti apa?"

N : Kadang-kadang ada diskusi dengan internal team-nya pemerintah ya. Cuma gak banyak sih, ada invitation based juga sih.

P : Hasil diskusi-diskusi itu diserap oleh pemerintah gak Pak? Maksudnya, output dan outcome-nya apa ada secara nyata atau hanya formalitas saja?

N : Untuk sekarang kalau saya lihat karena Indonesia mau FATF ya lumayan banyak aktivitasnya sekarang, dibanding dulu ya. Sekarang sudah mulai ada, kalau ngomongin OJK, peraturan-peraturannya itu sudah mulai di-refresh terus, lebih aktif dibandingkan dulu kan? Dulu paling 2 tahun sekali di-update, refresh, sekarang OJK 1 tahun saja ada 1 POJK POJK baru. Bahkan untuk bagian IKD (Inovasi Keuangan Digital) sendiri saja sudah dipecah lagi, lebih detail di bawah. Jadi ya lumayan aktif lah sekarang OJK.

P : Baik, Pak. Kalau untuk sarana dan prasarana, karena sejujurnya juga saya kurang memahami ya Pak untuk implementasi RegTech ke FinTech. Nah itu untuk keamanan sistem sendiri, yang memastikan dari vendornya sendiri berarti Pak?

N : Iya, jadi ada 2 opsi. Kadang adan FinTech yang dia sudah punya cloud sendiri atau gak on premis yang dia misalnya taro server di kantornya dia. Nah kalau misalnya di kantornya dia, ya security punya institusi finansial itu, dia yang ngecek, dia yang jaga. Kalau misalnya cloud, kadang-kadang contoh kayak misalnya AWS ada PCI DSS (Payment Card Industry Data Security Standard) yang buat ngecek SOC 2 (Smart Cloud System and Organization Controls). Nah itu ada terlatih yang ngecek juga. Nah kadang juga ada FinTech yang "Oke, aku gak mau maintain infrastruktur, aku juga gak mau taro server di kantor, aku mau pakai layanan kamu lewat API", jadi cloud-nya akan swasta yang pegang, sudah dijaga, ada sertifikasi SOC 2 sama PCI DSS. Dari situ, yang swasta akan nembak, misalnya pas lagi on boarding ngecek "Eh ini user ini ada di-blacklist gak?", kita feedback hit atau non-

hit, kayak gitu. Transaksi juga dikirim nanti diliat pattern-nya hit or non-hit, kayak gitu. Nah itu dari FinTech tuh sudah tidak banyak maintain infrasturktur lagi.

P : Ya, jadi security-nya ini tergantung sama dia maunya seperti apa ya Pak?

N : Iya, jadi ada beberapa opsi lah. On premis, private cloud, atau public cloud, kayak gitu.

P : Oke, berarti kalau untuk keamanannya itu bergantung lagi dengan perusahaannya? Maksudnya, bisa bergantung dengan perusahaannya, bisa bergantung dengan vendornya?

N : Ya sebenarnya bukan vendor sih karena data ini kan masuk di cloud. Cloud ini yang manage ya AWS kah, Google kah, kayak gitu. Nah yang membedakan kalau on premis ya institusi sendiri yang jaga.

P : Berarti seperti tadi ya Pak, bergantung dengan perusahannya?

N : Yah.

P : Tapi kalau secara risiko, itu lebih besar risiko yang on premis atau yang tadi menggunakan public cloud?

N : Semua punya risiko masing-masing. Taro server di kantornya, konslet, data hilang, risiko kan? Terus yang di public cloud, yah ngomongin tentang risiko kita gak bisa bilang itu 0% risiko. Bisa contoh misal public cloud-nya down, atau mungkin yang jalurnya misalnya ke US atau Singapore, kan kadang-kadang kan public cloud ada yang di US kan ya. Banyak banget cerita yang kabel lautnya putus atau apa, starfish disruption. Jadi ada satu planning disaster recovery lah kalau misalnya ada apa-apa, baik di itu on premis, atau di cloud, tetap sebagai institusi finansial tetap harus ada disaster recovery-nya.

P : Kalau di perusahaan yang besar kan mungkin memang ada ya Pak disaster recovery-nya, dari Bappebti juga yang saya tahu memang sudah ada regulasinya. Tapi kalau untuk perusahaan-perusahaan yang kecil itu bagaimana ya Pak?

N : Disaster recovery-nya itu gak harus semuanya komprehensif, kadang-kadang disaster recovery-nya FinTech itu hanya 1 page saja, yaitu setiap hari saya back up ini server, kalau server-nya mati at least saya ada back up-an last 24 hour. Jadi balik lagi seberapa risk appetite-nya saya "Apakah saya bisa bertahan last 24 hour punya data atau last hour, 1 jam lalu punya data". Nah, tentang bagaimana cara penggunaan back up ini kan pasti planning ya "Oke, saya ada back up, ini server mati, nanti ini bisa ada di cloud, di cloud dulu sementara, jadi aplikasi gak kena disrupt, atau mungkin aplikasi kena disrupt 1 jam atau 2 jam. Kalau FinTech-

FinTech kecil kan ya pasti gak apa-apa, karena kan mereka ada risiko-risikonya sendiri lah, risk appetite-nya sendiri, gitu.

P : Risk appetite-nya sendiri itu Pak, kan berarti setiap perusahaan berbeda ya Pak? Bergantung dengan perusahaannya. Berarti dari regulator juga gak bisa menyamaratakan ya Pak?

N : Iya, makannya kalau di luar kan ada regulasi SLA-nya (Service Level Aggrement) untuk FinTech-nya karena kalau misalnya FinTech, kan dia menggunakan uang masyarakat yang masuk ke sistemnya dia, pasti ada perlindungan dong dari pemerintahnya. Nah, seberapa perlindungannya kalau misalnya untuk FinTech dengan ukuran tertentu, maksimal disrupt-nya segini. Kayak contoh DBS kemarin di Singapura disrupt kan, risiko, bahkan kena sanksi begitu besar. Jadi setiap framework FinTech terntentu kalau di luar negeri mereka ada kayak maksimum down time-nya berapa. Apalagi kalau perusahaan besar karena yang udah dipakai setiap hari, ya mati 1 menit pun sudah loss besar bagi negara itu. Kayak Singapore contohnya, kemarin cuma 5 menit mati DBS, kena sanksi 1 Miliar Dollar. Karena kenapa? Karena bagi Singapore ini 1 Miliar Dollar ini kecil, karena dia 5 menit-nya ini dia kehilangan puluhan miliar dollar dari transaksi luar negeri yang masuk dan kapitalisasinya karena balik lagi, misalnya contoh saya sebagai investor di Singapura dan saya mengirim uang ke Singapura ternyata ada disruption selama 5 menit, trust saya berkurang dong? Kepercayaan saya berkurang. Kalau biasa setiap tahunnya nanti ada framework nih, negara-negara tertentu tingkat trust-nya seberapa tinggi. Nah, perbankan kalau sampai sesignifikan itu, 5 menit aja gak bisa, gitu.

P : Kalau dari Bapak sendiri, kan kalau di Indonesia masih bertumbuh dari penggunaan RegTech-nya. Kira-kira negara mana yang bisa dijadikan contoh atau kiblat yang mulai dari regulasi sampai dengan implementasi RegTech dan pengawasannya sudah ideal?

N : Singapore, paling gampang.

P : Kalau untuk sekarang, apa bedanya jauh sekali Pak dengan Indonesia?

N : Jauh sekali sih, karena yah kebanyakan negara-negara di Asia Tenggara studi bandingnya dengan Singapore. Karena mereka memang negara yang bergantung dengan finansial, ya negara yang gak ada sumber daya alam, gak ada apa kan, ya mereka solly bergantung dengan financial institution. Nah karena dia solly bergantung dengan financial institution, mereka harus regulated itu, make sure ini berkesinambungan, maksudnya bisa berterus-terus jalan gitu, karena kalau misalnya sekali bermasalah, kan pasti antisipasinya, pemikiran orang-orang adalah di Singapore orang masuk duit ke situ yaudah gitu, aman kan? Tapi yang paling

penting di Singapore adalah trust, makannya yang dijual Singapura ke negara-negara manapun adalah trust-nya karena negara mana pun ketika dia invest, dia tahu duit ini aman dan duit ini aman adalah bersih dari korupsi itu satu. Acountable, bahwa duit ini masuk, siapa yang masukin duit ini, sudah jelas siapa itu. Makannya kalau misalnya kita buka akun perbankan di Singapura, dicek semua, namanya, ini kamu ada blacklist lah, apa, semua, sangatlah ketat banget sih. Makannya kalau misalnya kita lihat beberapa institusi finansial kalau di Singapura kena crime itu fantastis banget. Kenapa? Karena mereka sudah begitu ketatnya sampai masih tetap ada masalah, ya pasti ada masalah besar, gitu.

P : Kalau perbedaan yang paling mencolok antara Indonesia dengan Singapore, dari apanya Pak?

N : Dari regulasinya sendiri. Banyak kan Indonesia kalau misalnya OJK itu regulasinya berkaca dari Singapura. Ya kita gak bisa bilang copy paste ya, ada dia ambil kemudian diadptasi lagi.

P : Kalau boleh tahu, regulasi spesifiknya yang bagian mana Pak?

N : Major Payment Institution, kalau di Indonesia kan jadi PJP.

P : Kalau dari proses AML-nya sendiri Pak, ada perbedaan yang mencolok gak?

N : Ya, perbedaan karena Major Payment Institution kan dipecah lagi beberapa. Kalau di Indonesia PJP dibagi 3. Nah AML dari setiap ini juga berbeda-beda. Contoh misal saya payment gateway, payment gateway kalau di Singapore gimana? Karena kalau si Singapore kan facilitate a lot international transaction. Kalau kita ngomongin payment gateway di Indonesia, kan gak ada international transaction. Kayak contoh kalau di lokal ada NextPay, ini kan payment gateway juga, tapi dia gak fasilitas remittance contohnya. Nah itu secara APU-PPT kan berbeda, kalau misalnya yang ada internasional, ada sanction list, satu, yang paling penting. Kalau yang local transaction, DTTOT, gak perlu sanction.

P : Baik, kalau dari Bapak sendiri ada rekomendasi tidak Pak untuk ke depannya di Indonesia sendiri untuk supaya penggunaan RegTech ini lebih masif?

N : Ya, kalau misalnya ini yang saya lihat kan pemerintah sudah bagus ya tentang regulasi-regulasinya dan menjelaskan. Kadang ada regulasi yang dibuat ada di situ saja dan tidak accessable bagi institusi finansial. Nah sekarang pemerintah sudah lebih accessable, mereka terbuka untuk “Hey, ini aku taro regulasi sini, kamu gak ngeti atau kamu mau object this regulation”, pemerintah sekarang sudah buka untuk itu akses. Nah, harapannya dengan adanya keterbukaan ini, lebih banyak financial

institution yang apa ya, dengan kemudahan ini mereka lebih gampang lah untuk adopsi RegTech. Dan memang kalau dibilang jujur secara regulasi untuk RegTech-nya sendiri masih belum sih, belum ada, katanya akan tahun depan. Cuma, karena itu akan turunan kalau di AFTECH namanya infrastructure enabler, jadi enabler lah sebagai RegTech, ada satu turunannya. Baru 1 perusahaan di Indonesia yang terdaftar di situ.

P : Perusahaan apa itu Pak?

N : SIJITU, dan akhirnya perusahaan di situ hanya untuk daftar saja. Dan pertanyaanya masih banyak RegTech lainnya yang tidak terdaftar, kenapa? Ya, pertama karena belum ada edukasi lagi dan masuk di situ juga tidak ada benefit yang jelas ih, nah itu mungkin yang tahun depan yang akan lebih diperjelas "Apakah saya sebagai RegTech mendaftar di situ hanya untuk mendaftar atau ada benefit lain?", kalau di Singapore kan misal ada namanya cosmic project, yaitu information sharing antara RegTech. Nah kita belum sampai ke situ, tapi akan.

P : Berarti karena implementasinya juga belum signifikan, jadi untuk mencapai ke information sharing pun saat ini masih belum?

N : Klasifikasinya baru dimulai tahun depan. Di IKD-nya sendiri ya, di pemerintah OJK-nya sendiri, ada klasifikasi khusus buat RegTech-nya, namanya infrastructure enabler.

P : Kalau untuk RegTech yang sekarang, kalau yang saya ketahui itu kan sekarang memasuki era RegTech 3.0 ya?

N : Wah, saya malah kurang paham kalau itu. Gimana nih maksudnya?

P : Jadi Pak kalau yang saya tahu, RegTech 2.0 itu kan yang lebih ke KYC dan transaction monitoring. Nah kalau yang 3.0 ini yang lebih kepada KYD (Know your Data), kalau yang saya tangkap tadi seperti information sharing tadi. Bisa dikatakan seperti itu tidak Pak sekarang arah perkembangan RegTech-nya ini?

N : Belum ada standar lah ya kalau untuk information sharing, bahkan di Singapore pun belum, baru mulai kan cosmic project-nya. Permasalahannya dulu kalau di Singapura, saya orang daftar hitam nih, saya daftar di UOB terus dia block saya kan? Nah saya tinggal ke DBS aja, ke OCBC, karena belum ada information sharing kan. Nah kalau di Indonesia kan jelas masalahnya, saya misalnya di-blacklist di Flip, saya tinggal daftar di Xendit, saya tinggal daftar dimana, karena kan Flip sama Xendit mereka gak ada information sharing. Dan misalnya saya sebagai orang jahat, saya kedeteksi di satu perusahaan FinTech, saya masih mudah lah untuk daftar kemana-mana. Karena kalau misalnya dengan ada information sharing, ruang

geraknya criminal itu lebih susah karena sudah ada information sharing kan. Harapannya ya kita ke depannya ke situ. Cuma ya kita beresin dulu lah klasifikasi RegTech, karena kita RegTech tuh belum dapat klasifikasi khususnya di OJK-nya.

P : Harusnya klasifikasinya seperti apa Pak?

N : Kayak tadi yang saya mention, infrastructure enabler. Kalau misalnya sudah ada klasifikasinya, baru jelas nih kita masuk ke sini, peraturan regulasi gini, yang kita sebagai Grup RegTech bisa menyuarakan suaranya lewat mana, regulasinya seperti apa, pemanfaatannya seperti apa, nanti kan lebih jelas gitu ada framework-nya. Nah sekarang kan gak ada framework, everyone is ngerjain sendiri-sendiri. Misalnya saya RegTech dari Flagright, ya ada RegTech darimana-mana ya mereka sesuai dengan standar mereka sendiri-sendiri, gak ada kayak satu framework dari pemerintah. Memang secara teknologi kita menggunakan yang sama, transaction monitoring, customer scoring. Tapi kan dengan adanya standar itu, pemerintah jadi lebih bisa nge-manage "Kira-kira kalau saya keluarin regulasi ini, berdampak ke RegTech-nya seperti apa, pemanfaatan berdampak ke FinTech-nya seperti apa?", baru jelas kan kalau misal ada framework-nya.

P : Berarti VDD juga masuk ya Pak semisal klasifikasi dan framework-nya sudah jelas?

N : Iya bisa masuk. Makannya di klasifikasi katalog itu bisa melakukan VDD kan? Kalau sekarang, kalau misalnya itu, siapa yang benar dan siapa yang gak benar kan gak jelas.

P : Bergantung dengan preferensi masing-masing ya jadinya?

N : Iya, makannya kalau misalnya mau sekarang kita bikin VDD, tambah klasifikasi, susah juga, subjektif kan jadinya "Oh kamu dekat sama pemerintah ya? Kamu jadi VDD yang bagus" gitu kan misalnya. Kan gak jelas jadinya, gitu.

P : Baik, berarti tadi selain dari FinTech-nya diklasifikasikan, dari RegTech-nya juga perlu diklasifikasikan juga ya Pak?

N : Iya, iya.

P : Pengklasifikasian RegTech ini apakah tujuannya nanti untuk menyesuaikan dengan size dari FinTech-nya?

N: Bisa, bisa. Contoh dari AML sendiri kita beda-beda. Kayak, contoh AML sendiri ada yang pegang biro kredit contoh, itu AML juga kan. Terus sanction screening, ada AML yang gak pegang sanction screening, itu regulasinya berbeda. Nah, kalau misalnya pakai sanction screening, data ini yang kamu pegang oleh RegTech ini, dipegang oleh siapa dan siapa yang memvalidasi ini data. Kan kalau misalnya saya

sebagai user yang on boarder, saya akan dicek against database ini, seberapa valid data ini. Kalau misal data ini tidak valid dan menyebabkan saya off board, siapa yang bertanggung jawab? Nah ini yang jadi masalah karena tidak ada framework-nya. Jadi belum tahu nih kalau misalnya ada apa yang terjadi, siapa yang bertanggung jawab, siapa yang akan memberikan pertanggung jawaban.

P : Berarti seperti PIC-nya belum tahu begitu ya Pak?

N : Iya, iya. Makannya karena tidak ada jelas begini jadinya adopsinya kurang. Karena kan kalau misalnya adopsi, siapa yang bertanggung jawab? Siapa yang menilai? Gak ada yang menilai kan? Kalau misalnya perusahaan gak ada yang menilai, buat apa kita harus implementasi? Jadinya kayak ayam dan telor kan jadinya.

P : Iya, iya.

LAMPIRAN 5 Transkrip Wawancara 2

Narasumber 1 : P2

Jabatan / Instansi : AML-CDD Product Manager / SIJITU

Kompetensi : Anti-Money Laundering Operating System

Tempat, Tanggal : SIJITU, 15 Agustus 2023

Narasumber 2 : P3

Jabatan / Instansi : Product Development & Consultant / SIJITU

Kompetensi : Anti-Money Laundering Operating System

Tempat, Tanggal : SIJITU, 15 Agustus 2023

P : Pewawancara

N1 : Nararumber 1

N2 : Narasumber 2

P : Saya izin memperkenalkan diri kembali ya Pak, dan Mba. Saya Kharisma dari UII, saat ini keperluan saya untuk mewawancarai guna meng-explore penyebab dari belum signifikannya penggunaan RegTech di Indonesia karena sebelumnya kan sudah dilakukan penelitian mengenai pemanfaatan RegTech ini, tapi hasilnya belum signifikan. Jadi masih banyak yang belum menggunakan RegTech, terutama untuk di FinTech-FinTech yang salah satu produknya adalah kripto. Nah, saya disini mencoba meng-explore penyebab tidak signifikannya, apakah dari sisi regulasinya, atau SDM-nya, atau ada hal-hal yang lainnya.

N1 : Ya, ini kartu nama saya.

P : Oh iya, Pak. Ini kita wawancaranya langsung 2 saja kali ya? Atau bagaimana, Pak, Mba?

N1 : Boleh-boleh, silahkan.

P : Oke, yang pertama, bisa dijelaskan terlebih dahulu atau tidak, RegTech itu apa dan apa saya yang di-cover oleh RegTech?

N1 : Silahkan Tiffani, saya juga mau dengar apa.

N2 : Kalau Regulatory Technology itu biasanya menyangkut dengan teknologi untuk mengatur hal-hal yang diperlukan oleh regulator, contohnya seperti CDD. Kalau untuk CDD sendiri, di RegTech itu di dalamnya ada beberapa hal atau poin yang diatur, seperti eKYC, kemudian ada background check atau PEP (Politically Exposed Person) check kita biasa sebutnya. Jadi untuk mengecek background atau latar belakang dari calon customer-nya, jadi customer ini apakah memiliki background high risk atau tidak, dan ya biasanya kalau RegTech sih umumnya yang saya tahu fokusnya ke CDD, customer due diligence.

P : Kalau untuk transaction monitoring-nya bagaimana?

N2 : Kalau dari transaction monitoring yang saya tahu itu masuknya ke ranah anti-fraud. Masih masuk ke RegTech juga, tapi kalau transaction monitoring itu di luar dari ranah CDD. Jadi berfokusnya hanya untuk monitoring suatu transaksi, apakah suatu transaksi bisa dikategorikan sebagai high risk transaction atau tidak.

P : Tapi masih di-cover RegTech berarti ya, Mba?

N2 : Masih di-cover, masih di dalam RegTech.

P : Baik. Nah, kalau sebelum eKYC itu kan biasanya penilaian risiko ya Mba? Untuk itu, apakah di-cover juga tidak Mba dengan RegTech?

N2 : Oh ya, kalau di kami disebutnya risk profiling. Jadi kalau untuk risk profiling sendiri kita bisa check risk level dari calon customer-nya. Jadi kita bisa mengukur, apakah level calon customer ini ada di high risk, medium risk, atau low risk.

N1 : Kalau dari saya, RegTech itu sistem yang membantu segala prosedur yang mandatory dari regulator, apa saja itu, eKYC. Kebetulan, kita RegTech-nya yang AML. Emang di luar sih yang terkenal itu RegTech AML, anti-money laundering. Ya kalau sekarang jadi satu lah, AML-CFT ya kan? Nah kalau di kita itu transaction monitoring, terus itu tadi juga risk profiling, itu kan semua ada tuh di POJK 8, sebelumnya POJK 23, sebelumnya lagi POJK 12 ya, diperbaharui terus. Itu tuh semua disebut, mulai dari deteksi high risk profil, sampai transaction monitoring mereka, sampai ke penilaian risiko mereka, itu tuh semua disebutkan dan wajib dilakukan oleh penyelenggara jasa keuangan. Nah oleh karena itu, RegTech hadir sebagai wadah yang mampu membantu untuk menjalankan kewajiban itu menggunakan sistem. Supaya lebih efisien dan efektif, gitu sih.

P : Baik baik. Oke, mungkin pernah ada klien dari FinTech ya Mba, Pak?

N1 : Oh ya banyak, banyak.

P : Nah kalau khusus yang FinTech kripto pernah menangani tidak?

N2 : Oh ya, pernah.

P : Dari FinTech-FinTech itu, kalau yang saya tahu kan dari regulasi tidak ada pembagian AML untuk FinTech berdasarkan size atau volume-nya. Nah itu mempengaruhi tidak dari implementasi RegTech-nya?

N1 : Oke, jadi sebenarnya yang baru dimasukkan ke rezim APU-PPT itu kalau saya tidak salah itu peer to peer lending (P2P). FinTech-FinTech lain seperti, contoh e-money, apalagi kripto. Itu kan sudah beda regulator ya, BAPPEBTI.

P : Iya BAPPEBTI.

N1: Tapi kemarin ada SK dari Kepala BAPPEBTI untuk menyarankan atau menghimbau penyelenggara crypto exchanger untuk kerjasama dengan RegTech. Tapi saya tidak tahu di situ ada atau tidak penalty karena yang sangat mempengaruhi implementasi adalah kurang tegasnya penalty atau sanksi dari regulator terhadap FinTech-FinTech player ini. Jadi sebenarnya RegTech ini dibutuhkan, tentu dibutuhkan, karena kan selain memberantas atau menghindari pencucian uang, itu juga kita menghindari pendanaan terorisme. Yang sulit itu pendanaan terorisme, uangnya itu tidak harus besar, uang kecil pun, 10 Juta pun bisa jadi bom, kasarnya ngomongnya gitu kan, dan tidak harus dari sumber tindak pidana, sumber dari yang halal pun bisa. Jadi itu pendanaan terorisme, kamu jual kelapa di pinggir jalan, than duitnya dipakai buat pendanaan terorisme juga bisa kan? Itu yang harus kita deteksi, siapa sih jaringan-jaringan individu yang terhubung dengan jaringan-jaringan terorisme ini. Itu yang harus kita deteksi di FinTech layer. Terkadang kendalanya, FinTech itu merasa dananya tidak cukup besar untuk dijadikan sarana pencucian uang. Tapi mereka lupa, kalau disitu ada bahaya pendanaan terorisme juga, gitu.

P : Oke, berarti itu di transaction monitoring ya untuk dicek-nya?

N1: Nah, kita justru saranin untuk di deteksi high risk profile.

P : Oh di awal?

N1: Betul, di awal, ‘Apakah mereka ini kerabat dari orang memang yang merupakan anggota dari organisasi terorisme kah? Atau dia kerabat dari politically exposed person (PEP) bukan?’, seperti itu. Itu kita harus deteksi di awal karena yang perlu kita garis bawahi, pencucian uang ataupun pendanaan terorisme, itu jarang pakai akun atas nama pribadi. Prakteknya pasti pakai akun nama kerabat-kerabatnya, dipecah, entah ke istrinya, pegawainya, ke kerabatnya yang lain, ke anaknya, biasa pakai akun mereka.

P : Baik, berarti akses pertamanya itu kan ke datanya ya, Pak, Mba? Data dari orang-orang yang ter-expose ini maksudnya. Nah, itu ada kesulitan tidak dalam mendapatkan akses data-data tersebut?

N2: Kalau saat ini sih kita partnership dengan data provider dari Singapore, sebenarnya head quarter-nya di London. Kita kerjasama dengan mereka untuk menggunakan watch list mereka, watch list itu database yang isinya profil-profil high risk. Jadi, mereka sudah punya sendiri, kita partnership dengan mereka, kita subscribe ke mereka untuk dipakai di sistem.

P : Berarti ruang lingkupnya internasional ya?

N2: Iya internasional.

P : Kalau yang untuk di dalam negeri, akses datanya ada atau tidak?

N2: Kalau dalam negeri ada dari PPATK, itu data dari SIGAP (Sistem Informasi Anti-Pencuain Uang dan Pendanaan Terorisme) dan dia ada PEP data juga. Tapi kalau untuk akses kesana, itu hanya bisa PJK (Penyedia Jasa Keuangan), jadi diluar itu kita tidak bisa akses datanya.

P : Jadi kalau untuk data itu yang bertanggung jawab itu perusahaan RegTech-nya ya? Bukan dari FinTech-nya?

N2: Iya betul, jadi yang punya aksesnya itu hanya beberapa PJK aja.

N1: Data apa dulu nih?

P : Data PEP dan keluarga atau kerabatnya.

N1: Ada 2 versi, berbayar sama gratis. Kalau gratis tuh data pemerintah. Nah, kalau berbayar tadi data dari swasta, perusahaan swasta yang tadi sudah disebut oleh Tiffani, itu dia crawling data sendiri, nah itu kita harus bayar ke mereka, kalau data pemerintah tadi gratis, tapi mereka pilih nih siapa yang akan di-supply data itu. Nah, kita bukan Penyedia Jasa Keuangan, kita bukan LJK, Lembaga Jasa Keuangan. Kita adalah RegTech, so kita gak dapat, yang dapat adalah LJK.

P : Tapi sebenarnya, menurut Mba dan Bapak sendiri, harusnya perusahaan RegTech itu dapat gak sih fasilitas seperti itu?

N1: Harusnya dapat, kenapa? Karena itu akan membantu sekali PJK untuk menerapkan lebih mudah. Karena gini, rata-rata contoh FinTech, FinTech itu belum punya infrasturktur atau sistem yang memadai untuk absorpt data itu misalnya atau belum ada on boarding yang cukup gitu, karena Tim IT-nya biasanya kecil skalanya kalau memang mereka belum sebesar, kalau mereka bukan big players di FinTech, gitu. Ya let’s see, peer to peer yang baru berkembang gitu kan, itu kan small banget

ya organisasinya. So, untuk menyediakan sistem yang bisa menampung data itu atau mengkoneksikan, mengintegrasikan data itu, itu butuh human resource lagi. Kenapa gak pakai SIJITU aja, gitu? Yang memang sudah bisa kita bantu dan kita sudah tercatat di OJK, gitu sih. Jadi menurut kita kalau kita dikasih aksesnya akan lebih membantu dan distribusi data itu bisa lebih maksimal.

P : Baik, dan akan lebih aman juga ya Pak kalau dari sisi FinTech-nya ketika screening data awal tadi?

N1: Iya tentu, karena pasti akan lebih maksimal ya penyerapan datanya. Selain itu ada juga data DTTOT, proliferasi, itu memang free dan bisa diakses lewat website-nya PPATK tapi tetap kita masukkan juga ke sistem kita dan siapapun bisa akses itu sih sebenarnya. PJK pun dapat didistribusikan lewat regulator mereka masing-masing.

P : Tapi kalau untuk DTTOT, update-nya secara berkala Pak?

N1: Dinamis ya, tergantung ketersediaan data mereka, tergantung update yang tersedia dari mereka. Jadi bisa saja minggu depan ada, bisa saja minggu depan gak ada, bulan depan gak ada, tapi besok langsung ada.

P : Oke, berarti tergantung ketersediaan data mereka ya. Tapi apa cukup meng-cover kebutuhan selama ini atau tidak? Terutama ketika proses KYC-nya.

N2: Kalau meng-cover keseluruhannya sih kami bilang gak cukup kalau hanya pakai DTTOT dan WMD (Weapon of Mass Destruction/Senjata Pemusnah Massal) aja, karena satu, mereka gak ada data anggota keluarga dan kerabat dari high risk profile-nya. Jadi sangat kurang sih kalau hanya dari DTTOT dan WMD.

P : Jadi tadi ya, tetap harus digabungkan dengan data dari swasta itu ya?

N2: Yes, betul.

P : Baik, kalau untuk regulasinya sendiri, tadi kan disampaikan oleh Pak Cornellius tidak ada penalty untuk FinTech yang tidak menggunakan RegTech. Nah itu implikasi ke FinTech-nya sendiri gimana? Apakah mempengaruhi FinTech-FinTech yang sudah menggunakan RegTech sehingga jadi ke-trigger karena yang tidak menggunakan RegTech juga selama ini tidak ada sanksi dari regulator.

N1: Nah sebenarnya gini, bukan memakai atau tidak memakai RegTech yang bisa menyebabkan penalty atau sanksi dari regulator masing-masing. Nah, yang menyebabkan adalah mereka tidak mempunyai prosedur APU-PPT. So, one day, mereka pasti punya risiko dong untuk dijadikan sarana pencucian uang atau

pendanaan terorisme, dan itu sudah pernah terjadi di FinTech, saya tidak bisa disclose namanya, salah satu brand. Itu pernah terjadi dan ternyata kejadian itu membenarkan bahwa FinTech ini bisa jadi sarana untuk melakukan pencucian uang dan pendanaan terorisme, TPPU dan TPPT. Nah, oleh karena itu implikasinya kalau tidak ada penalty, sebenarnya ya betul yang tadi kamu bilang, mereka jadi gak aware untuk memiliki prosedur APU-PPT yang komprehensif, yang layak, yang punya standar, gitu. Then, sebenarnya, di sisi lain, selain dari sisi regulator, biasanya investor, apalagi investor asing, itu punya concern lebih loh di ranah APU-PPT-nya. Jadi, selain untuk menjaga sisi si Lembaga Jasa Keuangan dari risiko sanksi, ada risiko reputasi juga di situ. Ada salah satu Lembaga Jasa Keuangan, waktu itu mau bikin fest, ada requirement salah satunya adalah harus punya prosedur APU-PPT yang memang memadai, seperti itu. Itu sebagai reputasi mereka di sisi investor, ya stakeholder dan shareholder lah, gitu.

P : Jadi kalau dari sisi regulasi, tadi kan berarti tidak ada pembagian FinTech berdasarkan volume atau size-nya, dan yang saya baca dari Peraturan BAPPEBTI juga tidak ada pembagiannya. Kalau untuk itu, perlu tidak Pak untuk ada pembagian seperti itu dari BAPPEBTI?

N1: Hmm, kalau menurut saya sih, jadi BAPPEBTI ini bersama OJK dan BI kan 3 regulator yang berbeda, ya. Sebenarnya BI punya regulasinya sendiri terhadap APU-PPT. OJK juga punya, walaupun kalau saya baca sih, jujur isinya sama saja, tapi kan judulnya beda, PBI 19, POJK sekarang kalau yang baru itu POJK 3 ya, tahun 2023 kan. Nah kalau BAPPEBTI, jujur saya belum tahu ada regulasinya atau tidak, tapi pasti ada. Nah, sebenarnya kalau dipisah-pisah gak perlu, sih. Secara garis besar sama sih semuanya, nanti implikasinya sebenarnya nanti. Karena di situ disebutkan ‘Setiap Lembaga Jasa Keuangan punya risk appetite-nya masing-masing’, ya kan? So, menurut kita gak harus prosedurnya kompleks banget. Tapi setidaknya punya di garis besarnya saja.

P : Jadi yang penting FinTech-FinTech itu atas regulasi tersebut juga punya APU-PPT-nya sendiri, begitu ya?

N1: Iya, prosedurnya itu punya, screening-nya punya. Ketika di-audit oleh salah satu regulator ‘Mana proses screening-nya?’ itu ada, dilakukan proses KYC, dilakukan screening watch list SIJITU, contoh, screening lewat SIJITU, oke, pass gitu, atau misal ‘Coba dilihat mana pemantauan transaksinya?’, ada juga di history-nya bahwa memang dilakukan pemantauan transaksi. Lalu juga ‘Penilaian risiko berjangkanya coba saya mau lihat history-nya’, contoh misalnya regulator ngomong seperti itu, mereka punya evidence-nya bahwa mereka melakukan prosedur itu.

P : Jadi accountable ya semuanya.

N1: Yes.

P : Oke, FinTech kan approve jadi sarana TPPU. Nah, seberapa besar dampaknya terhadap FinTech itu sendiri atau bagaimana dari temuan dari praktek yang sudah-sudah?

N2: Oh kebanyakan sih dari RCA-nya (Relative and Close Associate) ya, jadi anggota keluarga dari si profile-nya itu yang ditemukan. Jadi mereka mau registrasi di FinTech, ada temuannya gitu dari namanya.

P : Itu FinTech-nya yang sudah besar atau yang masih kecil-kecil, Mbak?

N2: Medium size, P2P.

P : Jadi mereka itu menggunakannya FinTech yang kecil-kecil juga ya.

N1: Itu dari pengalaman kita ya. Kalau dari temuan regulator yang menghebohkan jagat FinTech, jagat AFTECH lah ya, itu cukup besar sih, salah satu big player menurut kita. Mungkin bisa kita simpulkan, gak peduli size-nya, selama ada celah, penjahat pasti masuk.

P : Makannya tadi ya, perlunya prosedur APU-PPT di semua size FinTech ya?

N1: Betul.

P : Kalau dari RegTech-nya sendiri, perlu diterapkan di semua size FinTech tidak?

N1: Kalau menurut kita penting. Karena sesuai yang tadi sudah kita diskusikan, selain ada risiko pencucian uang, ada pendanaan terorisme juga yang itu gak mandang size-nya, amount of money-nya, yang cukup sulit itu sih.

P : Karena tadi ya? Gak mesti ada predicate crime-nya.

N1: Yes.

P : Kalau dari SIJITU sendiri, ada perbedaan implementasi RegTech-nya tidak untuk masing-masing FinTech yang berbeda size dan volume-nya?

N2: Kalau misalnya dia big size, itu kebutuhannya juga besar dan lebih luas lagi, contohnya salah satu klien kita itu P2P big player, itu dia pasti volume kebutuhan untuk screening-nya juga jauh lebih besar dibanding small to medium size player.

P : Yang lebih membedakannya apa?

N2: Yang membedakan lebih di volume-nya, sih. Tapi kebutuhan mereka untuk di screening dan profiling-nya itu sama seperti small to medium size.

P : Oh jadi prosesnya tetap sama? Background check-nya sama gitu, ya?

N1: Mungkin saya bantu. Biasa kalau yang kecil mereka priority based, mana yang diprioritaskan terlebih dahulu? Karena ya namanya masih kecil, anggarannya pasti ada yang lebih diprioritaskan dibandingkan compliance cost. Jadi mereka pilih, maksudnya seperti 'Oh, yang ini dulu nih, yang krusial dulu', mungkin yang risk profiling mereka lakukan manual dulu tidak apa-apa, tidak pakai RegTech misalnya. Terus juga misal yang tadi transaction monitoring mereka lakukan manual, tapi watch list name screening-nya untuk deteksi high risk profile-nya mereka langsung implementasi di awal. Tapi kalau yang sudah big, mereka ambil semuanya, mereka implementasikan semuanya. Bahkan sampai transaction monitoring mereka butuh, mereka akan implementasi.

P : Jadi kalau secara prosesnya tetap sama. Tapi yang membedakan itu, yang mau diadopsi yang bagian mana dulu nih, gitu ya?

N1: Iya, prioritasnya mana dulu. Karena kan tadi, yang tertulis di POJK dan PBI memang mereka harus melakukan semuanya, gitu.

P : Kalau untuk transaction monitoring, ditelusurinya sampai mana? Apakah sampai ke predicate crime-nya?

N1: Enggak, kita tidak menelusuri predicate crime-nya. Kita cuma bantu sampai ke pelaporan, ke STR (Suspicious Transaction Reporting), mengisi STR dan submit ke PPATK, gitu. Jadi yang menelusuri nanti PPATK-nya.

P : Berarti untuk mendeteksi suspicious transaction-nya saja ya?

N1: Iya.

N2: Kita ngasih alert-nya aja.

N1: Iya, ngasih alert-nya.

P : Kalau untuk pengawasnya sendiri, dari regulator. Kan kalau yang saya tau dari peraturannya itu, Perusahaan FinTech disarankan untuk menggunakan RegTech. Tapi dari regulator pengawasannya bagaimana? Kan sudah ada peraturannya nih, nah dari regulator action selanjutnya seperti apa?

N1: Nah kalau itu, jujur ya, mungkin dari opini pribadi SIJITU. Itu setelah mengeluarkan Undang-Undang tapi tindak tegasnya, penalty-nya itu belum ada karena terakhir yang diinfokan kan diadakan audit, random audit terhadap implementasi prosedur APU-PPT. Nah, yang kita lihat, yang kita rasakan, belum ada audit random-nya dan belum ada sanksi yang jelas bagi yang belum punya prosedur APU-PPT sehingga implikasinya lagi, mereka kurang aware terhadap kebijakan ini, terhadap kewajiban ini, gitu.

P : Jadi karena pengawasannya belum ada, FinTech juga jadi seperti "Yaudah saya gak pakai RegTech juga gak masalah", seperti itu ya?

N1: Yes, betul.

P : Tapi sebaiknya pakai ya? Kalau dari sisi perusahaan penyedia jasa RegTech, sebaiknya bagaimana?

N1: Coba mulai dari saya. Indonesia kan mau mulai join jadi anggota FATF, nah kenapa gak dimulai dari hal kecil? Lembaga Jasa Keuangannya ini punya prosedur APU-PPT semuanya. Dengan cara gimana? Cukup kasih sanksi yang jelas, sanksi administratif, sanksi yang bahkan sampai yang tegas gitu, kasih yang jelas dan mulai dijalankan sanksi itu supaya dari hal kecil implikasinya, siapa tahu, kita bisa benar-benar jadi anggota FATF, gitu loh. Pasti kan yang di-assess juga kesiapan LJK-LJK-nya, seperti apa prosedurnya, regulasinya seperti apa sih? Mungkin dari assessment FATF-nya gitu kan. Seperti itu sih, jadi penting banget segala lini karena ya mengutip kata-kata dari Pak Imran dari OJK "Namanya penjahat, namanya kriminal, kalau buat cuci duit, segala cara, segala teknologi pasti dipakai", gitu.

N2: Kalau menurut aku juga penting, sih. Tapi kan biasanya nih, perusahaan-perusahaan, terutama pas masa pandemi dan setelah pandemi tuh mengeluhkan revenue-nya kurang, gak ada dana untuk beli packages produk AML. Tapi sebenarnya dengan adanya produk kita, itu gak bisa jadi excuse lagi karena menurut kami pun dengan pakai SIGAP dan PEP Check-nya yang PPATK itu sudah cukup meng-cover dan kalau pakai produk kami juga harganya cukup terjangkau untuk small to medium. Jadi menurut kami, bukan penting lagi sih, tapi wajib untuk diterapkan.

P : Karena dari penyedia RegTech juga bisa menyesuaikan ya dengan size dan volume-nya FinTech itu?

N2: Iya.

P : Baik. Selanjutnya, kalau untuk transaction monitoring, sebenarnya ini lebih ke transaksi kripto ya, kan mereka menggunakan blockchain dan saya juga lihat di website-nya SIJITU kalau pernah menangani klien yang bergerak di kripto. Nah untuk transaction monitoring tadi, sejauh mana RegTech ini bisa meng-cover?

N1: Kalau dari kita, jujur saat meng-handle klien yang kripto itu mereka tidak menggunakan transaction monitoring. Nah yang biasa menggunakan itu klien-klien dari perbankan. Di kripto, mereka lebih ke proses on boarding-nya sih.

P : Berarti di awal-nya saja ya? Untuk di risk profiling-nya.

N1: Yes.

P : Tapi kalau dari RegTech-nya sendiri, memungkinkan tidak untuk meng-cover proses transaction monitoring yang menggunakan blockchain itu?

N1: Sebenernya itu mampu-mampun saja ya karena itu stick dengan core system-nya mereka, karena gak direct ya, gak direct ketika transaksi berlangsung mereka di-hit. Jadi at the end of the day, kayak selesai operational day, itu data-data transaksi dikumpulin, terus di-screening. Jadi biar dilihat nih, yang mana yang alert. Nanti kalau sudah dikasih alert ya masuk ke akun-akun-nya si Staff AML-nya mereka. Jadi memungkinkan banget karena di sana tidak akan interacting proses transaksinya sama sekali. Tidak ada transaksi yang di-stop. Contoh lagi mengirim sekian koin ke kamu, then tiba-tiba sistemnya SIJITU stop karena sudah melebihi limit coin per day-nya, nah tidak seperti itu cara kerjanya. Jadi tidak ada intervensi terhadap transaksi, seperti itu.

P : Tapi kalau secara infrastrukturnya memungkinkan saja ya, Pak?

N1: Memungkinkan saja sih sebenarnya.

P : Tergantung perusahaan RegTech-nya juga berarti ya, Pak?

N1: Tergantung perusahaan kriptonya.

P : Gimana tuh Pak maksudnya?

N1: Maksudnya, ada tidak core system-nya, contoh, terus mau atau tidak menyediakan server infrastruktur terbaru untuk stick bareng itu, karena kan enggak di kita yang nyediain, mereka yang menyediakan untuk absorpsi software kita, seperti itu.

P : Kalau yang selama ini klien menggunakannya yang bagaimana? Kalau setahu saya kan ada yang on premis, terus ada apa lagi, ya? Saya agak lupa.

N2: Kalau crypto trader yang klien kami sih sekarang dia pakainya web platform dashboard-nya kami, jadi gak on premis, tapi di web portal kami.

P : Kalau seperti itu, yang bertanggungjawab untuk maintenance dari siapa?

N2: Dari kami.

P : Jadi mereka seperti subscribe saja begitu ya?

N2: Iya.

P : Baik, kalau dari sisi keamanan data, lebih aman yang mana? Apakah yang server-nya di klien atau yang di SIJITU-nya?

N2: Sebenarnya kalau di kami juga terhitungnya masih aman karena kami tidak simpan data, kami hanya simpan log penggunaannya saja. Jadi di kami, keamanan data juga terjamin karena kami simpan data screening-nya si crypto trader. Tapi kalau misalnya record-nya crypto trader-nya, di core banking-nya mereka juga aman karena datanya tidak keluar.

P : Baik, baik. Oh ya, saya mau balik lagi ke transaction monitoring yang kripto tadi. Tadi kan sebenarnya dari sisi infrastruktur itu memungkinkan saja, ya? Nah, kalau blockchain ini kan pakai data-data yang terenkripsi, ya? Itu apakah ada perbedaan dalam proses transaction monitoring-nya dengan yang dilakukan di perbankan yang menggunakan fiat currency?

N1: Kalau kita jujur karena belum ada pengalaman, belum ada memang demand dari kriptonya sejujurnya ya. Jadi kita belum bisa jawab pertanyaan itu karena memang belum dilakukan. Jadi seperti itu.

P : Jadi kalau dari pengalaman SIJITU sejauh ini, FinTech kripto masih jarang adopsi RegTech yang untuk transaction monitoring?

N1: Iya, karena belum ada demand-nya dari mereka. Belum ada kebutuhannya dari mereka. Kalau perbankan, mereka memang membutuhkan.

P : Dan dari regulasi juga kalau di kripto belum ada pengawasannya juga ya? Balik lagi ke regulasi tadi.

N1: Betul, balik lagi ke situ. Kalau perbankan kan sudah jelas, harus punya untuk end-to-end. Kalau kripto, we don’t know.

P : Baik. Kalau untuk SDM-nya sendiri, dari SIJITU menyediakan jasa consulting atau tidak ketika implementasi sistemnya? Apakah ketika sudah implementasi sudah selesai, atau SDM dari klien diedukasi juga dalam mengoperasikan RegTech-nya?

N2: Kalau kita, kita menyediakan sistemnya. Tapi kalau misalnya klien kami untuk consult juga, cara pakai sistemnya untuk di-implement ke perusahaan mereka juga kita sebisa mungkin kasih edukasinya ke mereka.

P : Oke, berarti ada ya. Kalau kerjasama dengan regulator sendiri ada atau tidak? Karena RegTech ini kan salah satu sistem yang disarankan oleh regulator, nah dari regulatornya sendiri ada peran dalam memberikan edukasi juga atau tidak?

N2: Kalau edukasi sih, biasanya kalau FinTech yang sudah bergabung dengan asosiasi, biasanya suka ada seminar-seminar tentang money laundering, tentang CDD.

P : Kalau di luar pelatihan atau seminar dari regulator melalui AFTECH, kompetensi atau skill dan pengetahuan dari SDM itu memadai atau tidak dalam memahami dan mengoperasikan RegTech ini?

N2: Beda-beda sih, Mbak. Kalau misalnya, biasanya company yang medium to big, mereka mengerti apa yang harus dilakukan dengan prosedurnya mereka masing-masing. Tapi kalau misalnya yang small, kalau dari kami sih melihatnya masih lumayan bingung cara penerapan di perusahaan mereka.

P : Jadi meskipun semisal mereka punya sertifikasi, tidak menjamin ya?

N1: Mungkin itu kembali ke perusahaannya masing-masing. Mungkin yang tadi Tiffani sebutkan adalah pengalaman kita dan tidak bisa dijadikan data yang mewakilkan secara keseluruhan, ya. Kita tidak tahu apakah si small size company ini menggunakan officer yang sudah CAMS gitu atau punya sertifikasi AML gitu. Nah, kita tidak tahu, balik lagi ke human resources masing-masing. Tapi biasanya, secara garis besar mereka paham sih karena kan ini hanya sistem, dimana memang kita rancangnya sesuai dengan POJK, kewajiban-kewajiban POJK kita terjemahkan ke dalam sistem. So, biasanya mereka paham. Yang lebih gak paham mungkin secara teknis "Ini bagaimana ya, Bu?", secara teknis saja. Tapi kalau prosedur "Oh ternyata ini, oh ini buat ini", then mereka sudah bisa sih biasanya.

P : Kalau saya simpulkan, RegTech ini mentranslasikan peraturan-peraturan tersebut, yang kemudian diimplementasikan dalam bentuk sistem supaya lebih mudah dioperasikan oleh FinTech-FinTech tadi ya?

N1: Betul, betul.

P : Baik, kembali lagi tadi ke sebelumnya. Kan tadi sempat disebutkan, di masa setelah pandemi ini banyak perusahaan yang revenue-nya turun, dan tidak mau implement RegTech karena tidak ada budget-nya. Berarti apakah implementasi RegTech ini selain bergantung dengan awareness-nya FinTech, ini bergantung juga sama budget yang mereka sediakan ya?

N2: Iya, betul.

P : Saat ini FinTech-FinTech, apakah masih berada di sisi menghitung antara cost dan benefit dari RegTech ini?

N1: Hmm gini, sebenarnya banyak juga kok yang tidak ada penalty, tidak ada sanksi dari regulator, tapi mereka aware dengan ini. Memang ada risiko dijadikan tindak pidana pencucian uang dan pendanaan terorisme, mereka tahu dampaknya itu cukup besar. Nah, tapi bagi yang mereka merasa ini belum jadi prioritas mereka, mereka itu tidak adain budget compliance-nya di situ gitu, budget compliance-nya itu terlalu kecil biasanya karena tidak ada urgensi disana. Andaikan diadakan urgensi

disana, kita yakin compliance budget masing-masing mereka akan ditambahkan. Balik lagi ke budgeting-nya mereka karena tidak ada urgensi-nya itu. Kalo ke benefit, kita yakin 100%, selama ini kita presentasi ke perusahaan-perusahaan, sekalipun yang baru, yang mereka belum punya license pun mereka "Ini bagus", "Ini dibutuhkan", tapi urgent gak sih? Mereka akan menakar lagi, "Urgent gak sih? Kayaknya kalau gak dipakai gak diapa-apain deh"

N2: Sense of urgency-nya balik lagi regulator, Mbak. Mereka nge-push atau enggak? Kalau gak nge-push ya "Mending saya screening-nya lewat google aja", gitu kan.

N1: Betul, betul.

P : Iya, iya. Berarti kembali lagi ke regulasi dan framework-nya tadi ya, karena tidak ada pengawasan juga dari regulatornya. Walaupun secara eksplisit kan memang disebutkan memakai RegTech dengan fitur apa saja.

N1: Memang disebutkan, tapi prakteknya gak ada sanksi, gak ada urgensi disana.

P : Jadi FinTech juga sebenarnya bukan tidak mau menambah cost, mereka juga mau kok sebenarnya, tapi kembali lagi ke urgensinya tadi "Kalau tidak ada urgensinya, ya buat apa?"

N1: Betul, "Kenapa gak saya marketing aja? Saya kan masih growing. Kenapa saya gak endorse? Kenapa saya gak kolaborasi?", gitu contohnya.

N2: Dan gak ditegur juga sama regulatornya.

P : Sama sekali tidak ada peringatan berarti, Mbak?

N2: Sebenarnya kalau peringatan ada, tapi gak ada denda atau sanksi.

N1: Gak ada sanksi administratif yang benar-benar, gitu.

P : Biasanya kalau peringatan itu, setelah berapa lama FinTech berjalan? Atau ada peringatan secara berkala juga?

N1: Selama yang kita tahu itu belum ada yang benar-benar gitu. Waktu di awal, awal-awal 2022 ya kalau saya tidak salah. Memang klien kita pernah kena tegur tuh, kena audit random berkala, audit random itu kena dia dan baru tahu urgensinya. Sampai hari ini, dari detik itu sampai hari ini mereka rajin jadinya pakai. Tapi dari sebelum mereka kena audit random berkala itu, mereka gak pakai sama sekali, mereka hanya kerjasama saja dengan kita, mereka bayar saja tapi pakainya enggak.

P : Jadi tujuannya apa kalau begitu?

N1: Mungkin supaya punya lisensinya saja “Oh iya kita pakai SIJITU”, tapi ketika ditanya mana buktinya tidak ada. Nah di saat awal tahun itu saja kita mendengar ada audit random. Then sampai sekarang ini kita belum dengar lagi ada kegiatan audit random itu.

P : Ini jadi harusnya tanggungjawan siapa?

N1: OJK, BI, kalau PPATK sih engga ya.

P : Oh ya karena PPATK hanya untuk STR saja ya.

N1: Iya, dia untuk memproses dan memeriksa transaksi keuangan mencurigakan. Laporan-laporan yang di-submit oleh LJK, itu tugasnya mereka. Tapi kalau misalnya seperti ‘parents-nya’ itu harusnya OJK, BI, BAPPEBTI.

P : Kalau yang khusus kripto berarti ke BAPPEBTI, ya?

N1: Yes.

P : Oke, jadi kalau untuk awareness FinTech menggunakan RegTech juga balik lagi ke regulasi ya?

N1: Iya, paling besar perannya regulasi. Nomor 2 mungkin sort of investor dan stakeholder ya. Tapi paling besar pasti regulasi, gak ada urgensi disana. Balik lagi kesana, gak ada urgensi jadi budget yang ada pasti dialihkan ke yang lain.

P : Jadi kalau dari kesadaran FinTech-nya sendiri, apa mereka “Oke walaupun gak ada pengawasan dari regulator tapi kami mau tetap pakai”?

N1: Iya, iya, klien kami kayak gitu. Tapi kan klien SIJITU dibandingkan LJK yang ada di Indonesia, contoh industri, kita ambil salah satu saja ya, misal kripto. Dari sekian banyak, mungkin yang pakai hanya satu atau dua, gitu. Yang sadar hanya satu atau dua dari sekian banyak, rasionya terlalu jomplang.

P : Iya, jadi banyakan yang tidak pakai ya?

N1: Banyakan yang tidak pakai. Bahkan industri-industri sekuritas saja, saya dengar dari bursa efek-nya langsung, itu hampir 90% gak punya prosedur APU-PPT based on system, gitu. Yang punya standar kayak SIJITU itu mereka gak punya, jadi sedikit saja.

P : Kalau dari SIJITU, untuk prosedurnya mengacunya ke regulasi dalam negeri ya berarti?

N1: Iya, tapi untuk datanya kami mengacunya ke internasional, data global. Acuan yang di Indonesia juga rekomendasi FATF kok, sama saja sebenarnya kurang lebih.

P : Beda di prosedurnya saja kali ya? Di skenario kasus-kasusnya karena masing-masing negara berbeda.

N1: Iya, betul.

P : Kalau untuk pelatihan, kembali lagi ke SDM-nya tadi. Dari SIJITU kan tadi kalau memang mereka meminta untuk diberi edukasi terlebih dahulu, nanti bisa difasilitasi oleh SIJITU. Nah ini apakah secara berkala diberi semacam pelatihan itu atau bagaimana?

N2: Kalau kita sih sesuai kebutuhannya mereka saja.

N1: Edukasinya edukasi apa dulu nih? Terkait upadate regulasi atau penggunaan sistem?

P : Dua-duanya.

N1: Kalau penggunaan sistem mah kita pasti kasih kapanpun mereka butuh. Kalau edukasi terkait update, itu kita biasanya ngadain event kerjasama asosiasi karena jarang sih mereka minta edukasi langsung ke kita terkait regulasi karena biasanya regulasi itu mintanya kalau gak ke asosiasi sebagai jembatan antara regulator dan penyelenggara, ya langsung ke regulatornya.

P : Berarti dari sistem RegTech-nya juga ketika ada regulasi baru, akan update terus ya sistemnya?

N1: Iya, kita update terus sistemnya nih. Supaya, ya itu karena kan kita punya misi adalah salah satunya membantu penyenglenggara jasa keuangan untuk comply dengan regulasi yang berlaku. Kalau regulasi lama, ya gak sesuai dengan misi kita dong? Jadi kita update terus. Ini seperti baru keluar POJK baru, kita juga sudah harus enhanced sistem lagi nih. Kita pelajari, kita enhanced dan kita edukasi market-nya. Lewat mana? Lewat asosiasi, kita adain event, forum group discussion, dan lain-lain.

P : Oh, saya kira itu dari perusahaan RegTech-nya ke klien.

N1: Enggak, enggak.

P : Jadi melalui AFTECH tadi ya?

N1: Iya, melalui AFTECH tadi biasanya. Rata-rata kalau sudah ada update, compliance officer-nya itu juga update sih, gak harus lewat kita, jadi mereka pelajari sendiri. Bahkan dari regulatornya harusnya ada penyuluhannya langsung, ada sosialisasinya juga pasti dari regulator karena itu tanggungjawab regulator, bukan RegTech.

P : Tapi ada kerjasama atau tidak ketika sosialiasasi antara perusahaan RegTech dengan regulator?

N2: Enggak ada, sih. Malah biasanya itu dari regulator, mereka audiensi dulu ke klien-klien kami, baru nanti klien-klien kami contact kami, mereka bilang "Oh, kami baru audiensi nih sama regulator, kami ada tambahan rules seperti ini. Ini bisa gak di-implement di SIJITU?", biasanya seperti itu.

P : Berarti nanti dari SIJITU, build sistemnya lagi, lalu implement ke klien?

N2: Kita sesuaikan sama sistemnya kita sih, apakah bisa memenuhi kebutuhannya regulator ini atau tidak.

P : Contohnya apa Mbak kalau boleh tahu untuk yang baru-baru ini? Sebelumnya seperti apa, lalu setelah ada peraturan baru kemudian sistemnya jadi bagaimana?

N2: Kalau yang terbaru sih, dari OJK itu mereka ada kebutuhan maksimal 3 hari setelah DTTOT itu update, PJK sudah harus screening semua nama calon customer dan customer-nya. Jadi, ya mereka klien-klien kami contact kami "Kami sudah audiensi dengan OJK. OJK ada arahan DTTOT harus di-screening maksimal 3 hari setelah update, apakah SIJITU bisa menyediakan list DTTOT-nya 3 hari setelah di-update oleh PPATK?"

P : Berarti dari sisi regulasi ini bisa dikatakan cukup meng-cover kebutuhan prosedur APU-PPT-nya ya?

N2: Dari CDD-nya?

P : Iya, dari CDD dan transaction monitoring sampai pelaporan juga.

N1: Iya, justru dia jadi acuannya, jadi pedoman utamanya, gitu. Jadi kita juga bikin sistem based on POJK itu, kewajibannya apa aja sih? Contoh misal kayak screening, terus penilaian risiko, monitoring transaksi, pelaporan, itu kan kita ambil dari situ, kita serap dari situ, baru kita jadiin sistem "Oh kayak gini, ya. Workflow-nya kita jadiin begini, begini, begini", seperti itu. Jadi itu acuannya, biasanya kalau mereka update itu, contoh yang baru tuh mereka update menguatkan posisi DTTOT dan proliferasinya ini karena kemarin kan hanya PEP, ya ada lah teroris tapi kurang di-highlight, yang saat ini di-highlight sekaligus juga si proliferasi. Mungkin mereka sadar kali ya soal perang yang terjadi antara Ukraina dengan Rusia. Nah, nama-nama itu juga harus di-screening kan, takutnya masuk nih kriminal-kriminal orang yang bikin nuklir dan lain-lain, gitu.

P : Baik. Nah, untuk regulasi ini kan dari regulator, sedangkan yang implementasi di lapangan ini adalah perusahaan-perusahaan RegTech. Nah

itu pernah tidak menemui semacam "Ini sebenarnya ada potensi bahaya tapi secara regulasi belum diatur", ada yang seperti itu tidak?

N1: Kita sih, jujur, untuk itu enggak karena assessment itu, letaknya assessement risiko, ya yang menyusun pedomannya pasti dari sisi regulator dan kita tidak memberikan rekomendasi selama ini, ya. Biasanya, harusnya ya, yang bisa memberikan itu adalah si penyelenggara jasa keuangan. Tapi, menurut kita regulasi kita sudah cover seluruhnya sih, cukup meng-cover apalagi itu acuannya rekomendasi FATF. So, menurut kita gak ada rekomendasi yang bersifat personal dari kita ke regulator, belum ada sampai saat ini. Tapi tidak menutup kemungkinan akan ada, gitu. Yang selalu kita highlight adalah tadi, urgensinya, kurang tegasnya karena mungkin kita acuannya Singapore kali ya? Let's see, benchmark-nya adalah perusahaan-perusahaan Singapore. Perusahaan-perusahaan Singapore itu yang kecil-kecil aja itu pakai, screening nama, dan lain-lain karena jelas di sana sanksinya apa. Nah kita berharap Indonesia bisa seperti Singapore, gitu, sebagai benchmark kita.

P : Karena kalau tadi di Singapore ada regulasinya, ada penalty-nya, ada pengawasannya…

N1: Iya, ada urgensinya.

P : Kalau dari Mbak dan Bapak, sebagai yang mewakili perusahaan RegTech, ada kritik atau rekomendasi tidak untuk implementasi pemanfaatan RegTech ini? Dari sisi ketika melakukan implementasinya, kah? Atau dari sisi lain yang bertujuan untuk memaksimalkan pemanfaatan RegTech di FinTech ini.

N1: Kalau dari saya sih, balik lagi ke urgensinya, karena gini, salah satu RegTech yang tercatat di OJK itu kan SIJITU. Nah, kenapa gak manfaatin produk 100% lokal dari anak bangsa? Itu tuh dimaksimalkan, diajak kerjasama, diajak kolaborasi, gitu. Pemanfaatannya dimaksimalkan, daripada player-palyer dari luar negeri, seperti Singapura, US, dan lain-lain, masuk kesini mungkin standarnya standar internasional padahal yang kita butuh standar nasional sebenarnya, gitu lho, yang dekat dengan regulatornya. Kita adalah regulatory sandbox-nya OJK lho, kenapa mereka tidak memanfaatkan yang ada? Yang ada di dalam ranahnya mereka, gitu. So, (1) Urgensi, (2) Pemanfaatan kolaborasi dan komunikasi yang kurang dengan RegTech seperti kita, menurut kita.

P : Komunikasi antara regulator dengan RegTech?

N1: Iya, antara regulator dengan kita. Seperti OJK, BI, BAPPEBTI, itu ke kita mungkin komunikasinya masih kurang, ya. Contoh, kita mau, pernah ajak PPATK, contoh, untuk kolaborasi minta data PEP list nasional, itu masih ditolak, untuk

kerjasama pelaporannya dibantu, pelaporan STR, kamu tahu LTKM, LTKT, LTKL, kan?

P : Iya.

N1: Itu disalurinnya lewat kita ke goAML PPATK, itu juga masih ditolak. Jadi, menurut kita, pemanfaatan RegTech yang memang sudah tercatat di salah satu regulator ini masih kurang.

P : Padahal regulator juga yang merekomendasikan pakai RegTech, gitu ya?

N1: Iya, betul. Tapi kenapa begitu ada RegTech, kurang gitu pemanfaatannya.

P : Dari regulator ngasih tau gak alasannya kenapa?

N1: Kalau dari PPATK, mereka minta rekomendasi dari OJK. Jadi masih dilempar-lempar aja sih. Jadi menurut kita, urgensinya lagi sih yang masih kurang. Mereka belum sadar bahwa ada RegTech yang memang bisa dimanfaatkan untuk membantu LJK supaya POJK yang mereka buat ini bisa dibuat ada penalty-nya. Mungkin, mereka menilai belum bisa ada penalty-nya karena belum ada wadah, di saat sebenarnya sudah ada wadahnya untuk memenuhi itu, gitu.

P : Kalau dari Mbak Tiffani?

N2: Tapi menariknya tuh, malah perusahaan-perusahaan yang bukan RegTech, jadi penyedia jasa IT, justru mereka yang mendapatkan akses. Harusnya kan RegTech yang justru diutamakan.

P : Mereka ini semacam yang build sendiri? Yang kayak misal klien mau build sendiri untuk prosedur tertentu, lalu kerjasama dengan penyedia layanan IT tersebut?

N2: Iya, justru perusahaan-perusahaan IT ini yang mereka mendapatkan aksesnya ke portal SIGAP, ke PEP Check-nya PPATK gitu. Jadi kita agak bingung aja, kenapa mereka di-approve aksesnya sedangkan kita gak dikasih.

P : Jadi mereka implementasi sistem-sistem dalam RegTech, tapi sebenarnya mereka bukan perusahaan RegTech? Dan tidak tercatat di OJK juga ya?

N1: Iya, kalau tercatat itu salah satu syaratnya mass use, ada standarisasinya di sana. Kalau yang tadi IT Provider itu, ya kamu disuruh bikin A, B, C, D, ya ikut aja. Kalau di kita ada standarisasinya, ada workflow-nya. Kalau di sana, workflow-nya dari klien, mereka tinggal bikinin aja, mereka tinggal susunin aja.

N2: Kalau mass use kan siapa aja bisa pakai nih, bisa register langsung. Tapi kalau misalnya si IT Provider ini mereka ya hanya untuk klien-nya aja.

P : Jadi berdasarkan kebutuhan gitu ya?

N2: Iya.

P : Oh kalau di akuntansi tuh contoh kayak ada SAP, gitu ya? Sama ada juga sistem yang di-build sendiri gitu kan.

N2: Iya, iya.

N1: Iya, betul.

P : Baik, baik. Nah, mungkin yang terakhir nih, saran dari Mbak Tiffani dan Pak Cornellius, saran untuk bagaimana ya supaya memaksimalkan pemanfaatan RegTech, terutama memanfaatkan SIJITU ini lah sebagai RegTech anak bangsa yang juga sudah tercatat di OJK dan terstandarisasi? Terutama pemanfaatan di FinTech kripto yang tadi disebutkan bahwa belum banyak yang menggunakan.

N1: Kalau dari saya memang harus dipertegas ya, sanksinya, lalu juga disebutkan industri-industri yang memang diwajibkan, diperluas lagi, jangan Cuma FinTech aja, mungkin juga e-money, crypto exchanger, dan lain-lain, disebutkan semuanya dan dipertegas sanski administrasinya, serta juga dipermudah nih kolaborasi dengan regulator-regulator dan instansi terkait supaya pemanfaatannya maksimal karena kalau dulu sebelum ada SIJITU, PJK bisa bilang compliance cost itu terlalu mahal, mereka gak punya budget. Tapi kalau SIJITU, yang dia start dari 5 Juta aja, itu sudah tidak ada lagi kata mahal, semua bisa, semua dimungkinkan punya prosedur APU-PPT yang berstandar, gitu. Jadi menurut kita, jangan sampai inovasi ini mati gitu, justru harus dipelihara, harus di-maintenance, harus dikembangkan bersama-sama supaya kita punya standar prosedur APU-PPT yang jelas seperti di Singapura. Di Singapura, semacam SIJITU ini banyaknya banyak banget gitu, menjamur, mulai dari fiturnya lengkap sampai dengan yang satu-satuan aja, gitu. Nah, apalagi SIJITU ini sudah berusaha kerjanya, berkaryanya, dekat dengan regulator, dengan mendaftarkan diri dengan menjadi RegTech yang tercatat di OJK, gitu sih menurut Saya.

P : Baik, kalau dari Mba Tiffani?

N2: Mungkin selain penggalakkan di sisi regulatornya terhadap penggunaan RegTech-nya, di sisi lain mungkin edukasinya ya, edukasi dari regulatornya juga karena kalau untuk small to medium size FinTech biasanya yang kami temui sih, dari case kami, mereka biasanya kurang paham tentang AML. Jadi mungkin kalau edukasinya sudah strong, mereka juga pasti jadi merasa urgent, ada urgensinya untuk pakai AML System seperti SIJITU, dan terakhir sih, dukungan dari regulator. Biasanya kan di sini sih banyaknya pemainnya dari luar, jadi provider system itu

dari luar dan biasanya FinTech-FinTech besar pakainya dari luar, sudah pasti, karena ya selain ada connection antar petingginya, ya produk luar lebih prestige.

P : Menurut mereka?

N2: Iya menurut mereka.

P : Tapi kan sebenarnya sama saja, ya.

N1: Lebih bergengsi, "Kita pakai dari US, nih", gitu lho, biasanya.

P : Oh ya, maaf ada satu lagi, kita balik lagi. Kalau dari sisi SDM, kan kalau yang saya cari tahu dari beberapa perusahaan FinTech, khususnya kripto sih, jadi mereka officer sistem AML-nya dan sampai pelaporan melalui goAML-nya itu rata-rata tidak ada background AML. Jadi mereka diedukasi sendiri oleh FinTech-nya, nah ini bagaimana menyikapinya? Perbedaannya bagaimana antara yang memiliki background dengan yang tidak memiliki background AML? Karena beberapa yang saya coba tanya melalui LinkedIn, tadinya kan saya mau coba wawancara officer-nya juga, terus mereka jawab "Duh, maaf ya Saya juga baru belajar AML jadi gak tahu banyak tentang AML", sedangkan mereka adalah officer AML System.

N2: Karena mostly legal person ya yang di bagian compliance.

P : Kalau yang saya lihat, ada yang legal, ada juga yang tidak.

N2: Sebenarnya dari background-nya gak ada yang spesifik sih untuk menjadi officer AML System, tapi kalau menurut kami, yang paling baik sih yang sudah punya background AML, ya sertifikasi AML, yang sudah specialized di bidang AML-nya sih.

P : Tapi ada perbedaan gak dari sisi output-nya, antara yang punya background sama yang gak punya? Semisal keduanya sama-sama diedukasi di saat yang bersamaan, nah output pengetahuan dan skill-nya sama tidak?

N1: Kalau dari pengalaman Saya pribadi, kalau mereka yang memang gak punya background, mereka akan bingung "Ini tuh tools sebenarnya fungsinya buat apa, sih?", then nanya berulang-ulang, ya based on pengalaman SIJITU ya, gak luas cakupannya, mereka bingung "Ini tuh tujuannya buat apa sih?", mereka sampai bingung fitur ini tuh buat apa tujuannya. So, gak maksimal mungkin ya pemanfaatannya. Tapi kalau mereka yang punya background, mereka akan bilang "Kalau ini…", misal contoh PEP List, kita bisa deteksi PEP. Nah mereka akan tanya "Kerabatnya akan di-expose gak? Berapa derajat bisa ter-expose kerabat-kerabat dari si PEP?". Jadi, disana mereka punya urgensi untuk ngambil lebih banyak fitur

daripada mereka yang gak mengerti sama sekali. Mereka yang gak mengerti sama sekali ya “Kayaknya ini cukup deh”.

P : Ngikut aja berarti ya?

N1: Iya, manut aja, manut aja. Tapi kalau yang ini, gak pernah merasa puas, contoh misalnya “Kayaknya Saya butuh yang lebih dari ini deh. Kayaknya saya butuh ini juga deh. Kayaknya saya butuh ini.”, gitu.

N2: Tapi menurutku, misal mereka yang background-nya gak ada specialized di AML tapi punya experience banyak di AML, itu lebih baik juga sih daripada yang hanya punya sertifikasi tapi gak ada experience-nya.

P : Jadi lebih ke experience-nya ya.

N1: Hmm iya experience.

P : Oke, oke. Nah, ini kan SIJITU adalah perusahaan RegTech yang satu-satunya tercatat di OJK. Nah ini ada benefit-nya gak buat SIJITU?

N2: Kalau benefit-nya sih, selain dekat dengan regulator, kita bisa, ada trust point-nya lah dibanding dengan RegTech-RegTech yang belum ada status tercatatnya karena kan kalau misalnya tercatat kita ada di regulatory sandbox-nya OJK ya, berarti semua pengembangan produk, ya fitur-fitur kita pasti diawasin lah, gitu. Jadi kita ada trust point-nya sih, lebih ke tingkat kepercayaan klien bisa bertambah karena kita dekat dengan regulator dan kita patuh dengan regulator.

P : Tapi kalau untuk keuntungan-keuntungan yang lain, kayak misal akses data itu masih belum dapat ya?

N2: Iya.

P : Jadi keuntungannya secara administratif saja ya?

N1: Iya, kalau keuntungan akses untuk komunikasi ke regulator A, B, C, itu belum kita rasakan di tahap ini. Kita gak tahu kalau mungkin nanti naik jadi terdaftar, berizin, dan lain-lain, kita belum tahu. Tapi kalau untuk di titik ini kita jujur belum merasakan, komunikasinya hanya ke OJK, itu saja. Tapi kalau komunikasi ke, seperti PPATK yang lintas regulator itu belum merasakan.

P : Harusnya ada ya?

N1: Harusnya ada, harusnya mereka malah menemani, memediasi, gitu contohnya. Kita harapkan seperti itu.

P : Dan sudah teruji dan tercatat juga kan ya.

N1: Iya, sudah tercatat juga kan.

N2: Justru yang lebih banyak ngasih benefit itu kalau kita join asosiasi, dengan kita di-connect-in sama FinTech-FinTech yang gabung juga sama asosiasinya. Terus, saat si asosiasi bikin event yang tentang AML, tentang CDD, tentang RegTech, kita bisa ikut, jadi kita bisa ethic educate juga.

P : Maaf Saya kurang paham, kalau asosiasi tuh yang menginisiasi dari regulator atau para pelaku?

N1: Pasti pelaku, mereka yang pemain-pemain FinTech bikin asosiasi, ya AFTECH itu kan yang mendirikan Pak Niki Luhur ya, yang punya VIDA. Jadi memang didirikan, tujuan utamanya ya, jembatan antara regulator dengan player FinTech, ya untuk saling update apa yang ada di market. Walaupun ya bisa dibilang, mereka juga ada yang kompetitor, ya ada juga yang partner. Tapi FinTech, selama di dalam situ masih punya tujuan yang sama sih.

P : Jadi cukup sering juga dapat klien melalui AFTECH?

N1: Secara gak langsung ya, karena kan kita juga cukup aktif kayak adain event, atau kalau ada event pun kita datang, sekedar untuk peserta pun itu cukup membantu karena kita kan B2B banget ya. So, networking penting.

LAMPIRAN 6 *Matrix Coding Query* Mekanisme Anti-Pencucian Uang untuk Aset Kripto di Indonesia[4]

	A : 1. UU 7 - 2011_Mata Uang	B : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	C : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	D : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	E : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	F : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	G : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka
1 : Crypto Asset	0	0	1	5	0	0	0
2 : a. Kriteria Crypto Asset	0	0	3	1	0	0	0
3 : b. Syarat Penyelenggaraan Pasar Fisik	0	0	2	1	0	0	0
4 : 1. Modal	0	0	2	0	0	0	0
5 : 2. Sarana Elektronik	0	0	7	0	0	0	0
6 : 3. Pemeriksaan	0	0	1	0	0	0	0
7 : 4. Pengawasan dan Pelaporan	0	0	2	0	0	0	0
8 : c. Syarat Pedagang Crypto Asset	0	0	3	2	0	0	0
9 : 1. Modal	0	0	2	0	0	0	0
10 : 2. Sarana Elektronik	0	0	6	0	0	0	0
11 : 3. Tata Cara Perdagangan	0	0	5	0	0	0	0
12 : 4. Pemeriksaan	0	0	2	0	0	0	0
13 : 5. Pelaporan	0	0	1	1	0	0	0
14 : Know Your Customer	0	0	2	0	1	0	7
15 : CDD dan atau EDD	0	0	8	0	2	21	13

[4] Berdasarkan Jumlah *Coding*

16 : Transaction Monitoring	0	0	13	0	2	0	11
17 : Risk Based Approach	0	0	1	0	2	6	0
18 : a. Identifikasi, Pemahaman dan Penilaian Risiko	0	0	0	0	0	13	2
19 : b. Toleransi Risiko	0	0	0	0	0	3	0
20 : c. Pengurangan dan Pengendalian Risiko	0	0	0	0	0	5	0
21 : d. Evaluasi Risiko Residual	0	0	0	0	0	4	0
22 : e. Penerapan Risk Based Approach	0	0	0	0	0	5	0
23 : f. Peninjauan dan Evaluasi RBA	0	0	0	0	0	4	0

LAMPIRAN 7 *Matrix Coding Query* Pengawasan dan Pemantauan terhadap Penerapan Anti-Pencucian Uang untuk Aset Kripto di Indonesia[5]

	A : 1. UU 7 - 2011_Mata Uang	B : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	C : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	D : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	E : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	F : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	G : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka
1 : Internal Control	0	0	0	0	0	1	4
2 : a. Pengawasan Aktif Direksi dan Dewan Komisaris	0	0	0	0	0	4	0
3 : b. Kebijakan dan Prosedur	0	0	0	0	0	2	3
4 : c. Pengendalian Internal	0	0	0	0	0	8	1
5 : d. Sistem Informasi Manajemen	0	0	0	0	0	6	1
6 : e. Sumber Daya Manusia dan Pelatihan	0	0	0	0	0	5	2
7 : External Monitoring	0	0	0	0	2	0	0
8 : BAPPEBTI (Pelaporan dan Sanksi)	0	0	0	1	1	0	1
9 : PPATK (Pelaporan)	0	0	0	1	1	1	1

[5] Berdasarkan Jumlah *Coding*

LAMPIRAN 8 *Matrix Coding Query* Penyebab Pemanfaatan RegTech di Indonesia Inefektif[6]

	A : P1	B : P2	C : P3
1 : Implementasi RegTech	0	0	0
2 : Akses Data PEP	0	0	0
3 : Regulator	0	1	1
4 : Akses Terbatas	0	0	1
5 : Bersifat Ekslusif	2	0	2
6 : Kompetensi SDM	4	3	2
7 : Perbedaan FinTech	0	0	0
8 : Small to Medium Size	0	2	2
9 : Big Size	0	1	2
10 : Risk Appetite & Perception	0	0	0
11 : Awareness	2	10	1
12 : Finansial	5	1	2
13 : Mitigasi Kerusakan Sistem	2	0	0
14 : Profil Nasabah	5	0	0
15 : Komunikasi dan Kolaborasi antara Regulator dengan RegTech Provider	1	5	1
16 : Pengawasan dan Pemeriksaan	5	2	0
17 : Regulasi RegTech	0	0	0
18 : Klasifikasi FinTech dan RegTech	7	0	0
19 : Penegakkan Regulasi	2	15	3
20 : Regulasi Pencegahan Crypto-Laundering	0	0	0
21 : APU-PPT FinTech	1	2	0
22 : Asas Praduga Tak Bersalah	3	0	0
23 : Pembaharuan & Ketersediaan Data	0	1	1
24 : Periodic Checking	1	0	0
25 : Service Level Agreement	1	0	0

[6] Berdasarkan Jumlah *Coding*

LAMPIRAN 9 *Matrix Coding Query* Rekomendasi Perbaikan[7]

	A : P1	B : P2	C : P3
1 : Pencegahan Crypto-Laundering	0	0	0
2 : Prosedur APU-PPT FinTech di Semua Size	0	4	0
3 : Pemanfaatan RegTech	0	0	0
4 : Akses Data PEP oleh RegTech Provider	0	1	0
5 : Edukasi Regulator kepada FinTech Crypto	0	0	1
6 : Klasifikasi RegTech	1	0	0
7 : Kolaborasi Regulator dengan RegTech Provider Lokal	0	3	1
8 : Penetapan dan Pemberian Sanksi atau Penalty	0	4	0

[7] Berdasarkan Jumlah *Coding*

LAMPIRAN 10 *Matrix Coding Query* Dampak Potensial[8]

	A : P1	B : P2	C : P3
1 : Awareness FinTech Crypto	0	0	1
2 : Mendukung Pemenuhan Kriteria Anggota FATF	0	1	0
3 : Optimalisasi Penyerapan Data	0	4	0
4 : Penjaminan & Pengelolaan Risiko	0	1	0
5 : VDD dan RegTech Terstandarisasi	3	4	0

[8] Berdasarkan Jumlah *Coding*

LAMPIRAN 11 *Framework Matrix* Mekanisme Anti-Pencucian Uang untuk Aset Kripto di Indonesia

	A : RM 1 Mekanisme AML-Crypto	B : Crypto Asset	C : a. Kriteria Crypto Asset	D : b. Syarat Penyelenggaraan Pasar Fisik	E : 1. Modal	F : 2. Sarana Elektronik
1 : 1. UU 7 -2011_Mata Uang	UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 7 TAHUN 2011 TENTANG MATA UANG DENGAN RAHMAT TUHAN YANG MAHA ESA PRESIDEN REPUBLIK INDONESIA, Menimbang : a. bahwa Negara Kesatuan Republik Indonesia sebagai suatu negara yang merdeka dan berdaulat memiliki Mata Uang sebagai salah satu simbol kedaulatan negara yang harus dihormati dan dibanggakan oleh seluruh warga Negara Indonesia; Mata Uang adalah uang yang dikeluarkan oleh Negara Kesatuan Republik Indonesia yang selanjutnya disebut Rupiah. Ciri Rupiah adalah tanda tertentu pada setiap Rupiah yang ditetapkan dengan tujuan untuk menunjukkan identitas, membedakan harga atau nilai nominal, dan mengamankan Rupiah tersebut dari upaya pemalsuan. Kertas Uang adalah bahan baku yang digunakan untuk membuat Rupiah kertas yang mengandung unsur pengaman dan yang tahan lama. Logam Uang adalah bahan baku yang digunakan untuk membuat Rupiah logam yang mengandung unsur pengaman dan yang tahan lama. Pengelolaan Rupiah adalah suatu kegiatan yang mencakup Perencanaan, Pencetakan, Pengeluaran, Pengedaran, Pencabutan dan Penarikan, serta Pemusnahan Rupiah yang dilakukan secara efektif, efisien, transparan, dan akuntabel. Pasal 2 (1) Mata Uang Negara Kesatuan Republik Indonesia adalah Rupiah. (2) Macam Rupiah terdiri atas Rupiah kertas dan Rupiah logam. (3) Rupiah sebagaimana dimaksud pada ayat (1) disimbolkan dengan Rp. Mata Uang adalah uang yang dikeluarkan oleh Negara Kesatuan Republik Indonesia yang selanjutnya disebut Rupiah. Ciri Rupiah adalah tanda tertentu pada setiap Rupiah yang ditetapkan dengan tujuan untuk menunjukkan identitas, membedakan harga atau nilai nominal, dan mengamankan Rupiah tersebut dari upaya pemalsuan. Kertas Uang adalah bahan baku yang digunakan untuk membuat Rupiah kertas yang mengandung unsur pengaman dan yang tahan lama.					

	Logam Uang adalah bahan baku yang digunakan untuk membuat Rupiah logam yang mengandung unsur pengaman dan yang tahan lama. Pengelolaan Rupiah adalah suatu kegiatan yang mencakup Perencanaan, Pencetakan, Pengeluaran, Pengedaran, Pencabutan dan Penarikan, serta Pemusnahan Rupiah yang dilakukan secara efektif, efisien, transparan, dan akuntabel. Pasal 2 (1) Mata Uang Negara Kesatuan Republik Indonesia adalah Rupiah. (2) Macam Rupiah terdiri atas Rupiah kertas dan Rupiah logam. (3) Rupiah sebagaimana dimaksud pada ayat (1) disimbolkan dengan Rp.					
2 : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	bahwa aset kripto (crypto asset) telah berkembang luas di masyarakat dan merupakan komoditi yang layak dijadikan sebagai subjek Kontrak Berjangka yang diperdagangkan di Bursa Berjangka; Aset Kripto (Crypto Asset) ditetapkan sebagai Komoditi yang dapat dijadikan Subjek Kontrak Berjangka yang diperdagangkan di Bursa Berjangka. bahwa aset kripto (crypto asset) telah berkembang luas di masyarakat dan merupakan komoditi yang layak dijadikan sebagai subjek Kontrak Berjangka yang diperdagangkan di Bursa Berjangka; Aset Kripto (Crypto Asset) ditetapkan sebagai Komoditi yang dapat dijadikan Subjek Kontrak Berjangka yang diperdagangkan di Bursa Berjangka.					

3 : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	Badan Pengawas Perdagangan Berjangka Komoditi yang selanjutnya disebut Bappebti adalah lembaga pemerintah yang tugas pokoknya melakukan pembinaan, pengaturan, pengembangan, dan pengawasan Perdagangan Berjangka. Aset Kripto (Crypto Asset) yang selanjutnya disebut Aset Kripto adalah Komoditi tidak berwujud yang berbentuk digital, menggunakan kriptografi, jaringan informasi teknologi, dan buku besar yang terdistribusi, untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain. Pedagang Fisik Aset Kripto adalah pihak yang telah memperoleh persetujuan dari Kepala Bappebti untuk melakukan kegiatan transaksi yang berkaitan dengan Aset Kripto baik atas nama diri sendiri dan/atau memfasilitasi Pelanggan Aset Kripto. Pelanggan Aset Kripto adalah pihak yang menggunakan jasa Pedagang Fisik Aset Kripto untuk membeli atau menjual Aset Kripto diperdagangkan di Pasar Fisik Aset Kripto. Koin adalah salah satu bentuk Aset Kripto yang memiliki konfigurasi blockchain tersendiri dan memiliki karakteristik seperti Aset Kripto yang muncul pertama kali yaitu bitcoin. Token adalah salah satu bentuk Aset Kripto yang dibuat sebagai produk turunan dari Koin. Badan Pengawas Perdagangan Berjangka Komoditi yang selanjutnya disebut Bappebti adalah lembaga pemerintah yang tugas pokoknya melakukan pembinaan, pengaturan, pengembangan, dan pengawasan Perdagangan Berjangka. Aset Kripto (Crypto Asset) yang selanjutnya disebut Aset Kripto adalah Komoditi tidak berwujud yang berbentuk digital, menggunakan kriptografi, jaringan informasi teknologi, dan buku besar yang terdistribusi, untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain. Pedagang Fisik Aset Kripto adalah pihak yang telah memperoleh persetujuan dari Kepala Bappebti untuk melakukan kegiatan transaksi yang berkaitan dengan Aset Kripto baik atas nama diri sendiri dan/atau memfasilitasi Pelanggan Aset Kripto. Pelanggan Aset Kripto adalah pihak yang menggunakan jasa Pedagang Fisik Aset Kripto untuk membeli atau menjual Aset Kripto	Aset Kripto (Crypto Asset) yang selanjutnya disebut Aset Kripto adalah Komoditi tidak berwujud yang berbentuk digital, menggunakan kriptografi, jaringan informasi teknologi, dan buku besar yang terdistribusi, untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain. Aset Kripto (Crypto Asset) yang selanjutnya disebut Aset Kripto adalah Komoditi tidak berwujud yang berbentuk digital, menggunakan kriptografi, jaringan informasi teknologi, dan buku besar yang terdistribusi, untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain.	Jenis Aset Kripto yang dapat diperdagangkan apabila telah memenuhi kriteria paling sedikit sebagai berikut: a. berbasis distributed ledger technology; b. berupa Aset Kripto utilitas (utilty crypto) atau Aset Kripto beragun aset (Crypto Backed Asset); dan c. telah memiliki hasil penilaian dengan metode Analytical Hierarchy Process (AHP) yang ditetapkan oleh Bappebti. Hasil penilaian dengan metode Analytical Hierarchy Process (AHP) sebagaimana dimaksud pada ayat (2) huruf c wajib mempertimbangkan ketentuan sebagai berikut: a. nilai kapitalisasi pasar (market cap) Aset Kripto (coin market cap); b. masuk dalam transaksi bursa Aset Kripto besar di dunia; c. memiliki manfaat ekonomi, seperti perpajakan, menumbuhkan ekonomi digital, industri informatika dan kompetensi tenaga ahli dibidang informatika (digital talent); dan d. telah dilakukan penilaian risikonya, termasuk risiko pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal. Jenis Aset Kripto yang dapat diperdagangkan apabila telah memenuhi kriteria paling sedikit sebagai berikut: a. berbasis distributed ledger technology; b. berupa Aset Kripto utilitas (utilty crypto) atau Aset Kripto beragun aset (Crypto Backed Asset); dan c. telah memiliki hasil penilaian dengan metode Analytical Hierarchy Process (AHP) yang ditetapkan oleh Bappebti. Hasil penilaian dengan metode Analytical Hierarchy Process (AHP) sebagaimana dimaksud pada ayat (2) huruf c wajib mempertimbangkan ketentuan sebagai berikut: a. nilai kapitalisasi pasar (market cap) Aset Kripto (coin market cap); b. masuk dalam transaksi bursa Aset Kripto besar di dunia; c. memiliki manfaat ekonomi, seperti perpajakan, menumbuhkan ekonomi digital, industri informatika dan kompetensi tenaga ahli dibidang informatika (digital talent); dan d. telah dilakukan penilaian risikonya, termasuk risiko pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal.	Perdagangan Pasar Fisik Aset Kripto hanya dapat diselenggarakan menggunakan sarana elektronik yang dimiliki oleh Pedagang Fisik Aset Kripto yang difasilitasi dan pengawasan pasarnya dilakukan oleh Bursa Berjangka yang telah memperoleh persetujuan dari Kepala Bappebti. Bursa Berjangka yang telah mendapatkan persetujuan untuk menyelenggarakan perdagangan Aset Kripto tidak dapat menyelenggarakan transaksi untuk subyek Komoditi lainnya. Perdagangan Pasar Fisik Aset Kripto hanya dapat diselenggarakan menggunakan sarana elektronik yang dimiliki oleh Pedagang Fisik Aset Kripto yang difasilitasi dan pengawasan pasarnya dilakukan oleh Bursa Berjangka yang telah memperoleh persetujuan dari Kepala Bappebti. Bursa Berjangka yang telah mendapatkan persetujuan untuk menyelenggarakan perdagangan Aset Kripto tidak dapat menyelenggarakan transaksi untuk subyek Komoditi lainnya.	Untuk dapat memperoleh persetujuan dalam melakukan perdagangan Pasar Fisik Aset Kripto sebagaimana dimaksud pada ayat (1), selain memenuhi persyaratan sebagaimana diatur dalam Peraturan Bappebti yang mengatur penyelenggaraan perdagangan pasar fisik Komoditi di Bursa Berjangka, Bursa Berjangka wajib memenuhi persyaratan: a. pada saat awal pengajuan permohonan memiliki modal disetor paling sedikit Rp500.000.000.000,00 (lima ratus miliar rupiah) paling lambat 2 (dua) bulan sejak memperoleh izin usaha sebagai Bursa Berjangka yang khusus memfasilitasi perdagangan Aset Kripto; b. mempertahankan ekuitas paling sedikit sebesar 80% (delapan puluh perseratus) dari modal yang disetor sebagaimana dimaksud pada ayat (2) huruf a; c. memiliki paling sedikit 1 (satu) pegawai yang bersertifikasi Certified Information Systems Auditor (CISA) dan 1 (satu) pegawai yang bersertifikasi Certified Information Systems Security Professional (CISSP), atau memiliki kerjasama dengan lembaga tempat yang memiliki tenaga ahli atau langsung bekerjasama dengan tenaga ahli yang bersertifikasi Certified Information Systems Auditor (CISA) dan Certified Information Systems Security Professional (CISSP) dalam rangka pengawasan dan - 9 - pengamanan transaksi Aset Kripto pada Pedagang Fisik Aset Kripto; d. memiliki sistem pengawasan dan pelaporan untuk penyelenggaraan perdagangan Pasar Fisik Aset Kripto yang terjadi pada Pedagang Fisik Aset Kripto. e. memiliki peraturan dan tata tertib Pasar Fisik Aset Kripto; dan f. memiliki komite Pasar Fisik Aset Kripto. Untuk dapat memperoleh persetujuan dalam melakukan perdagangan Pasar Fisik Aset Kripto sebagaimana dimaksud pada ayat (1), selain memenuhi persyaratan sebagaimana diatur dalam Peraturan Bappebti yang mengatur penyelenggaraan perdagangan pasar fisik Komoditi di Bursa Berjangka, Bursa Berjangka wajib memenuhi persyaratan: a. pada saat awal pengajuan permohonan memiliki modal disetor paling sedikit Rp500.000.000.000,00 (lima ratus miliar rupiah) paling lambat 2 (dua) bulan sejak memperoleh izin usaha sebagai Bursa Berjangka yang khusus	(1) Sistem pengawasan dan pelaporan sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf d wajib memenuhi persyaratan paling sedikit sebagai berikut: a. akurat, aktual, aman, terpercaya, online dan realtime serta compatible secara sistem maupun - aplikasi dengan sistem Lembaga Kliring Berjangka dan Pedagang Fisik Aset Kripto; b. memenuhi standar spesifikasi dan fungsi sesuai dengan standar fungsionalitas seb c. fitur dan fungsi yang tersedia memenuhi seluruh ketentuan yang berlaku dal d. memiliki fungsi yang dapat melindungi akses data profil, keuangan, dan transaksi setiap Pelanggan Aset Kripto; e. memiliki Business Continuity Plan (BCP) yang selalu mutakhir (up to date); f. memiliki Disaster Recovery Centre (DRC): 1. ditempatkan di dalam negeri dengan lokasi paling dekat 20 km (dua puluh kilometer) dengan lokasi server utama; 2. menggunakan server atau cloud server yang memadai dan memiliki standar ISO 27001; dan 3. memiliki kantor perwakilan resmi di Indonesia. g. memiliki konfigurasi dengan spesifikasi: 1. dapat menjamin terpeliharanya komunikasi dengan sistem di Lembaga Kliring Berjangka dan Pedagang Fisik Aset Kripto secara realtime sesuai dengan protokol yang telah ditentukan ole 2. memiliki tingkat keamanan sistem yang baik untuk mengatasi gangguan dari dalam dan luar sistem. h. memenuhi persyaratan database yang berfungsi untuk mengelola dan menyimpan data transaksi, dan data pengawasan serta pelaporan Aset Kripto seb i. server atau cloud server yang digunakan memiliki spesifikasi teknis yang baik untuk memfasilitasi penggunaan sistem dan/atau sarana pengawasan dan pelaporan online yaitu: 1. server atau cloud server termasuk cadangan (mirroring) harus ditempatkan di dalam negeri; 2. server atau cloud server harus memiliki cadangan (mirroring) server; dan 3. server atau cloud server didukung oleh prasarana dan sarana yang memadai sehingga dapat menjamin kesinambungan operasional. j. memiliki sertifikasi ISO 27001

	diperdagangkan di Pasar Fisik Aset Kripto. Koin adalah salah satu bentuk Aset Kripto yang memiliki konfigurasi blockchain tersendiri dan memiliki karakteristik seperti Aset Kripto yang muncul pertama kali yaitu bitcoin. Token adalah salah satu bentuk Aset Kripto yang dibuat sebagai produk turunan dari Koin.				memfasilitasi perdagangan Aset Kripto; b. mempertahankan ekuitas paling sedikit sebesar 80% (delapan puluh perseratus) dari modal yang disetor sebagaimana dimaksud pada ayat (2) huruf a; c. memiliki paling sedikit 1 (satu) pegawai yang bersertifikasi Certified Information Systems Auditor (CISA) dan 1 (satu) pegawai yang bersertifikasi Certified Information Systems Security Professional (CISSP), atau memiliki kerjasama dengan lembaga tempat yang memiliki tenaga ahli atau langsung bekerjasama dengan tenaga ahli yang bersertifikasi Certified Information Systems Auditor (CISA) dan Certified Information Systems Security Professional (CISSP) dalam rangka pengawasan dan - 9 - pengamanan transaksi Aset Kripto pada Pedagang Fisik Aset Kripto; d. memiliki sistem pengawasan dan pelaporan untuk penyelenggaraan perdagangan Pasar Fisik Aset Kripto yang terjadi pada Pedagang Fisik Aset Kripto. e. memiliki peraturan dan tata tertib Pasar Fisik Aset Kripto; dan f. memiliki komite Pasar Fisik Aset Kripto.	(Information Security Management System) yang di dalamnya terdapat Statement of Applicability (SOA) untuk ISO 27017 (cloud security) dan ISO 27018 (cloud privacy) apabila menggunakan cloud services maka kewajiban atas ISO 27017 (cloud security) dan ISO 27018 (cloud privacy)tersebut harus dipenuhi oleh perusahaan penyedia cloud service; k. sertifikasi ISO sebagaimana dimaksud pada huruf j hanya dapat diterbitkan oleh lembaga sertifikasi yang telah diakui oleh lembaga pemerintah yang - 13 menyelenggarakan urusan keamanan informasi; dan l. memiliki pengamanan open Application Programming Interface (API) yang sudah ditentukan prosedurnya, seperti proses enkripsi-dekripsi, whitelist Internet Protocol (IP), tunnel dan certificate. (2) Sistem pengawasan dan pelaporan sebagaimana dimaksud pada ayat (1) wajib diperiksa atau diaudit oleh lembaga independen yang memiliki kompetensi di bidang sistem informasi. (1) Sistem pengawasan dan pelaporan sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf d wajib memenuhi persyaratan paling sedikit sebagai berikut: a. akurat, aktual, aman, terpercaya, online dan realtime serta compatible secara sistem maupun - aplikasi dengan sistem Lembaga Kliring Berjangka dan Pedagang Fisik Aset Kripto; b. memenuhi standar spesifikasi dan fungsi sesuai dengan standar fungsionalitas seb c. fitur dan fungsi yang tersedia memenuhi seluruh ketentuan yang berlaku dal d. memiliki fungsi yang dapat melindungi akses data profil, keuangan, dan transaksi setiap Pelanggan Aset Kripto; e. memiliki Business Continuity Plan (BCP) yang selalu mutakhir (up to date); f. memiliki Disaster Recovery Centre (DRC): 1. ditempatkan di dalam negeri dengan lokasi paling dekat 20 km (dua puluh kilometer) dengan lokasi server utama; 2. menggunakan server atau cloud server yang memadai dan memiliki standar ISO 27001; dan 3. memiliki kantor perwakilan resmi di Indonesia.

						g. memiliki konfigurasi dengan spesifikasi: 1. dapat menjamin terpeliharanya komunikasi dengan sistem di Lembaga Kliring Berjangka dan Pedagang Fisik Aset Kripto secara realtime sesuai dengan protokol yang telah ditentukan ole 2. memiliki tingkat keamanan sistem yang baik untuk mengatasi gangguan dari dalam dan luar sistem. h. memenuhi persyaratan database yang berfungsi untuk mengelola dan menyimpan data transaksi, dan data pengawasan serta pelaporan Aset Kripto seb i. server atau cloud server yang digunakan memiliki spesifikasi teknis yang baik untuk memfasilitasi penggunaan sistem dan/atau sarana pengawasan dan pelaporan online yaitu: 1. server atau cloud server termasuk cadangan (mirroring) harus ditempatkan di dalam negeri; 2. server atau cloud server harus memiliki cadangan (mirroring) server; dan 3. server atau cloud server didukung oleh prasarana dan sarana yang memadai sehingga dapat menjamin kesinambungan operasional. j. memiliki sertifikasi ISO 27001 (Information Security Management System) yang di dalamnya terdapat Statement of Applicability (SOA) untuk ISO 27017 (cloud security) dan ISO 27018 (cloud privacy) apabila menggunakan cloud services maka kewajiban atas ISO 27017 (cloud security) dan ISO 27018 (cloud privacy)tersebut harus dipenuhi oleh perusahaan penyedia cloud service; k. sertifikasi ISO sebagaimana dimaksud pada huruf j hanya dapat diterbitkan oleh lembaga sertifikasi yang telah diakui oleh lembaga pemerintah yang - 13 menyelenggarakan urusan keamanan informasi; dan l. memiliki pengamanan open Application Programming Interface (API) yang sudah ditentukan prosedurnya, seperti proses enkripsi-dekripsi, whitelist Internet Protocol (IP), tunnel dan certificate. (2) Sistem pengawasan dan pelaporan sebagaimana dimaksud pada ayat (1) wajib diperiksa atau diaudit oleh lembaga independen yang memiliki kompetensi di bidang sistem informasi.

4 : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto		Aset Kripto (Crypto Asset) yang selanjutnya disebut Aset Kripto adalah Komoditi tidak berwujud yang berbentuk digital aset, menggunakan kriptografi, jaringan peer-to-peer, dan buku besar yang terdistribusi, untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain. Bukti Simpan Aset Kripto adalah dokumen yang diterbitkan oleh Pengelola Tempat Penyimpanan sebagai tanda bukti kepemilikan atas Aset Kripto yang disimpan. Wallet adalah media yang dipergunakan untuk menyimpan aset kripto baik berupa koin atau token. Token adalah salah satu bentuk Aset Kripto yang dibuat sebagai produk turunan dari koin. Koin adalah salah satu bentuk Aset Kripto yang memiliki konfigurasi blockchain tersendiri dan memiliki karakteristik seperti Aset Kripto yang muncul pertama kali yaitu bitcoin. Aset Kripto (Crypto Asset) yang selanjutnya disebut Aset Kripto adalah Komoditi tidak berwujud yang berbentuk digital aset, menggunakan kriptografi, jaringan peer-to-peer, dan buku besar yang terdistribusi, untuk mengatur penciptaan unit baru, memverifikasi transaksi, dan mengamankan transaksi tanpa campur tangan pihak lain. Bukti Simpan Aset Kripto adalah dokumen yang diterbitkan oleh Pengelola Tempat Penyimpanan sebagai tanda bukti kepemilikan atas Aset Kripto yang disimpan. Wallet adalah media yang dipergunakan untuk menyimpan aset kripto baik berupa koin atau token. Token adalah salah satu bentuk Aset Kripto yang dibuat sebagai produk turunan dari koin. Koin adalah salah satu bentuk Aset Kripto yang memiliki konfigurasi blockchain tersendiri dan memiliki karakteristik seperti Aset Kripto yang muncul pertama kali yaitu bitcoin.	(2) Aset Kripto dapat diperdagangkan apabila memenuhi persyaratan paling sedikit sebagai berikut: a. berbasis distributed ledger technology; b. berupa Aset Kripto utilitas (utilty crypto) atau Aset Kripto beragun aset (Crypto Backed Asset); c. nilai kapitalisasi pasar (market cap) masuk ke dalam peringkat 500 (lima ratus) besar kapitalisasi pasar Aset Kripto (coinmarketcap) untuk Kripto Aset utilitas; d. masuk dalam transaksi bursa Aset Kripto terbesar di dunia; e. memiliki manfaat eknomi, seperti perpajakan, menumbuhkan industri informatika dan kompetensi tenaga ahli dibidang informatika (digital talent); dan f. telah dilakukan penilaian risikonya, termasuk risiko pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal. (3) Aset Kripto hanya dapat diperdagangkan apabila telah ditetapkan oleh Kepala Bappebti dalam daftar Aset Kripto yang diperdagangkan di Pasar Fisik Aset Kripto. (2) Aset Kripto dapat diperdagangkan apabila memenuhi persyaratan paling sedikit sebagai berikut: a. berbasis distributed ledger technology; b. berupa Aset Kripto utilitas (utilty crypto) atau Aset Kripto beragun aset (Crypto Backed Asset); c. nilai kapitalisasi pasar (market cap) masuk ke dalam peringkat 500 (lima ratus) besar kapitalisasi pasar Aset Kripto (coinmarketcap) untuk Kripto Aset utilitas; d. masuk dalam transaksi bursa Aset Kripto terbesar di dunia; e. memiliki manfaat eknomi, seperti perpajakan, menumbuhkan industri informatika dan kompetensi tenaga ahli dibidang informatika (digital talent); dan f. telah dilakukan penilaian risikonya, termasuk risiko pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal. (3) Aset Kripto hanya dapat diperdagangkan apabila telah ditetapkan oleh Kepala Bappebti dalam daftar Aset Kripto yang diperdagangkan di Pasar Fisik Aset Kripto.	b. tujuan pembentukan Pasar Fisik Aset Kripto sebagai sarana pembentukan harga yang transparan dan penyediaan sarana serah terima fisik, serta dipergunakan sebagai referensi harga di Bursa Berjangka; c. kepastian hukum; d. perlindungan Pelanggan Aset Kripto; dan e. memfasilitasi inovasi, pertumbuhan, dan perkembangan kegiatan usaha perdagangan fisik Aset Kripto. b. tujuan pembentukan Pasar Fisik Aset Kripto sebagai sarana pembentukan harga yang transparan dan penyediaan sarana serah terima fisik, serta dipergunakan sebagai referensi harga di Bursa Berjangka; c. kepastian hukum; d. perlindungan Pelanggan Aset Kripto; dan e. memfasilitasi inovasi, pertumbuhan, dan perkembangan kegiatan usaha perdagangan fisik Aset Kripto.		
5 : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme yang selanjutnya disingkat APU dan PPT adalah upaya pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Pendanaan Terorisme. Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme yang selanjutnya disingkat APU dan PPT adalah upaya pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Pendanaan Terorisme.					

6 : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka						
7 : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka						

	G : 3. Pemeriksaan	H : 4. Pengawasan dan Pelaporan	I : c. Syarat Pedagang Crypto Asset	J : 1. Modal	K : 2. Sarana Elektronik	L : 3. Tata Cara Perdagangan
1 : 1. UU 7 -2011_Mata Uang						
2 : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto						
3 : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	(1) Sertifikat ISO 27001 sebagaimana yang diwajibkan dalam Peraturan Badan ini hanya dapat diterbitkan oleh lembaga sertifikasi yang telah diakui oleh lembaga pemerintah yang menyelenggarakan urusan keamanan informasi. (2) Pelaksanaan audit sistem dan pemeriksaan terhadap sistem elektronik yang digunakan oleh Bursa Berjangka, Lembaga Kliring Berjangka, Pedagang Fisik Aset Kripto dan Pengelola Tempat Penyimpanan Aset Kripto wajib dilakukan oleh lembaga independen yang memiliki auditor dengan kompetensi di bidang sistem informasi. (3) Lembaga independen yang melakukan audit sistem atau pemeriksaan dalam peraturan badan ini wajib memiliki kriteria paling sedikit: a. 1 (satu) orang pegawai tetap yang bersertifikasi Certified Information System Auditor (CISA); b. 1 (satu) orang tenaga ahli yang memiliki keahlian di bidang teknologi Aset Kripto dan blockchain; c. memiliki perizinan dari kementerian/lembaga atau otoritas, apabila diwajibkan; dan d. sudah menjalankan aktivitas usahanya paling singkat 2 (dua) tahun dan memiliki pengalaman audit di bidang keuangan non perbankan. (1) Sertifikat ISO 27001 sebagaimana yang diwajibkan dalam Peraturan Badan ini hanya dapat diterbitkan oleh lembaga sertifikasi yang telah diakui oleh lembaga pemerintah yang menyelenggarakan urusan keamanan informasi. (2) Pelaksanaan audit sistem dan pemeriksaan terhadap sistem elektronik yang digunakan oleh Bursa Berjangka, Lembaga Kliring Berjangka, Pedagang Fisik Aset Kripto dan Pengelola Tempat Penyimpanan Aset Kripto wajib dilakukan oleh lembaga independen yang memiliki auditor dengan kompetensi di bidang sistem informasi. (3) Lembaga independen yang melakukan audit sistem atau pemeriksaan dalam peraturan badan ini	Bursa Berjangka melaksanakan kewajiban: wajib - a. menyediakan fasilitas sistem yang handal untuk terselenggaranya pelaksanaan pelaporan dan pengawasan Pasar Fisik Aset Kripto yang teratur, transparan dan wajar; b. melakukan pengawasan pasar terhadap seluruh transaksi perdagangan Pasar Fisik Aset Kripto, termasuk melakukan audit terhadap para anggotanya; c. menyediakan akses terhadap sistem pengawasan dan pelaporan yang handal dan real time kepada Bappebti dalam rangka pengawasan; d. mengambil langkah-langkah untuk menjamin terlaksananya mekanisme perdagangan Pasar Fisik Aset Kripto dengan baik dan melaporkan kepada Bappebti; e. melakukan evaluasi terhadap Aset Kripto yang telah diperdagangkan di Pasar Fisik Aset Kripto; dan f. melakukan kajian atas usulan penambahan atau pengurangan jenis Aset Kripto dan menyampaikan rekomendasi hasil kajiannya kepada Bappebti. Bursa Berjangka melaksanakan kewajiban: wajib - a. menyediakan fasilitas sistem yang handal untuk terselenggaranya pelaksanaan pelaporan dan pengawasan Pasar Fisik Aset Kripto yang teratur, transparan dan wajar; b. melakukan pengawasan pasar terhadap seluruh transaksi perdagangan Pasar Fisik Aset Kripto, termasuk melakukan audit terhadap para anggotanya; c. menyediakan akses terhadap sistem pengawasan dan pelaporan yang handal dan real time kepada Bappebti dalam rangka pengawasan; d. mengambil langkah-langkah untuk menjamin terlaksananya mekanisme perdagangan Pasar Fisik Aset Kripto	(1) Pedagang Fisik Aset Kripto untuk dapat melakukan kegiatannya dalam memfasilitasi transaksi perdagangan Pasar Fisik Aset Kripto wajib memperoleh persetujuan dari Kepala Bappebti. (2) Ruang lingkup kegiatan sebagaimana dimaksud pada ayat (1) meliputi: a. jual dan/atau beli antara Aset Kripto dan mata uang Rupiah; b. pertukaran antar satu atau lebih antar jenis Aset Kripto; c. penyimpanan Aset Kripto milik Pelanggan Aset Kripto; dan d. transfer atau pemindahan Aset Kripto antar Wallet. (6) Kegiatan sebagaimana dimaksud pada ayat (3) termasuk perubahan dan perkembangannya wajib dilakukan pengkajian dan dilakukan penilaian risikonya, termasuk risiko pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal. (2) Pedagang Fisik Aset Kripto dilarang menjalankan kegiatan usaha lain selain sebagai Pedagang Fisik Komoditi. (1) Pedagang Fisik Aset Kripto untuk dapat melakukan kegiatannya dalam memfasilitasi transaksi perdagangan Pasar Fisik Aset Kripto wajib memperoleh persetujuan dari Kepala Bappebti. (2) Ruang lingkup kegiatan sebagaimana dimaksud pada ayat (1) meliputi: a. jual dan/atau beli antara Aset Kripto dan mata uang Rupiah; b. pertukaran antar satu atau lebih antar jenis Aset Kripto; c. penyimpanan Aset Kripto milik Pelanggan Aset Kripto; dan d. transfer atau pemindahan Aset Kripto antar Wallet. (6) Kegiatan sebagaimana dimaksud pada ayat (3) termasuk perubahan dan perkembangannya wajib dilakukan pengkajian dan dilakukan penilaian risikonya, termasuk risiko pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal.	Pedagang Fisik Aset Kripto wajib memenuhi persyaratan: a. memiliki modal disetor paling sedikit Rp80.000.000.000,00 (delapan puluh miliar rupiah); b. mempertahankan ekuitas paling sedikit sebesar 80% (delapan puluh perseratus) dari modal yang disetor sebagaimana dimaksud pada ayat (1) huruf a; c. memiliki struktur organisasi minimal Divisi Informasi Teknologi, Divisi Audit, Divisi Legal, Divisi Pengaduan Pelanggan Aset Kripto, Divisi Client Support, Divisi Accounting dan Finance; d. memiliki sistem dan/atau sarana perdagangan online yang dipergunakan untuk memfasilitasi penyelenggaraan perdagangan Pasar Fisik Aset Kripto yang terhubung dengan Bursa Berjangka dan Lembaga Kliring Berjangka; (2) Pedagang Fisik Aset Kripto wajib mempertahankan modal bersih disesuaikan yang menunjukkan perhitungan modal kerja Pedagang Fisik Aset Kripto yang merupakan selisih antara aset lancar dengan total liabilitas. Pedagang Fisik Aset Kripto wajib memenuhi persyaratan: a. memiliki modal disetor paling sedikit Rp80.000.000.000,00 (delapan puluh miliar rupiah); b. mempertahankan ekuitas paling sedikit sebesar 80% (delapan puluh perseratus) dari modal yang disetor sebagaimana dimaksud pada ayat (1) huruf a; c. memiliki struktur organisasi minimal Divisi Informasi Teknologi, Divisi Audit, Divisi Legal, Divisi Pengaduan Pelanggan Aset Kripto, Divisi Client Support, Divisi Accounting dan Finance; d. memiliki sistem dan/atau sarana perdagangan online yang dipergunakan untuk memfasilitasi penyelenggaraan perdagangan Pasar Fisik Aset Kripto yang terhubung dengan Bursa Berjangka dan Lembaga Kliring Berjangka; (2) Pedagang Fisik Aset Kripto wajib mempertahankan modal bersih	(3) Sistem dan/atau sarana perdagangan online sebagaimana dimaksud pada ayat (1) huruf d wajib memenuhi persyaratan paling sedikit sebagai berikut: - a. akurat, aktual, aman, terpercaya, online dan realtime serta compatible secara sistem maupun aplikasi dengan sistem Bursa Berjangka dan Lembaga Kliring Berjangka; b. memenuhi standar spesifikasi dan fungsi sesuai dengan standar fungsionalitas sebagaimana diatur dalam Peraturan Badan ini, peraturan dan tata tertib Bursa Berjangka dan Lembaga Kliring Berjangka; c. fitur dan fungsi yang tersedia memenuhi seluruh ketentuan yang berlaku dalam Peraturan Badan ini, peraturan dan tata tertib Bursa Berjangka dan Lembaga Kliring Berjangka; d. memiliki fungsi yang dapat memproteksi akses data keuangan dan data transaksi setiap Pelanggan Aset Kripto; e. memiliki Business Continuity Plan (BCP) yang selalu mutakhir (up to date); f. memiliki Disaster Recovery Centre (DRC): g. memiliki konfigurasi h. memenuhi persyaratan database yang berfungsi untuk mengelola dan menyimpan data transaksi Aset Kripto seb i. server atau cloud server yang digunakan memiliki spesifikasi teknis yang baik untuk memfasilitasi penggunaan sistem dan/atau sarana perdagangan online yai j. memiliki sertifikasi ISO 27001 (Information Security Management System) yang di dalamnya sudah terdapat Statement of Applicability (SOA) untuk ISO 27017 (cloud security) dan ISO 27018 (cloud privacy) apabila menggunakan cloud services maka kewajiban atas ISO 27017 (cloud security) dan ISO 27018 (cloud privacy)	e. memiliki tata cara perdagangan (trading rules) paling sedikit memuat: 1. definisi dan istilah; 2. proses pendaftaran Pelanggan Aset Kripto; - 3. pernyataan dan jaminan; 4. kewajiban dan tanggung jawab; 5. pengkinian data; 6. tata cara kegiatan transaksi, meliputi transaksi jual/beli, deposit, withdrawal, pengiriman Aset Kripto ke Wallet lain, kegiatan lain yang telah mendapat persetujuan dari Bappebti; 7. biaya transaksi dan batas penarikan dana; 8. keamanan transaksi; 9. layanan pengaduan Pelanggan Aset Kripto; 10. penyelesaian perselisihan Pelanggan Aset Kripto; 11. force majeur; 12. penerapan program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme serta Proliferasi Senjata Pemusnah Massal (APUPPT); dan 13. penyampaian syarat dan ketentuan dalam hal calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto mengambil posisi untuk diri sendiri; f. memiliki Standar Operasional Prosedur (SOP) paling sedikit mengatur tentang: 1. pemasaran dan penerimaan Pelanggan Aset Kripto; 2. pelaksanaan transaksi; 3. pengendalian dan pengawasan internal; 4. penyelesaian perselisihan Pelanggan Aset Kripto; dan 5. penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal. g. memiliki paling sedikit 1 (satu) pegawai yang bersertifikasi Certified Information Systems Security Professional (CISSP) atau memiliki kerja sama - 27 - dengan lembaga yang memiliki tenaga ahli atau langsung memiliki perjanjian kerja sama dengan tenaga ahli yang bersertifikasi Certified Information Systems Security Professional (CISSP); dan h. memiliki calon anggota direksi, anggota dewan komisaris, pemegang

	wajib memiliki kriteria paling sedikit: a. 1 (satu) orang pegawai tetap yang bersertifikasi Certified Information System Auditor (CISA); b. 1 (satu) orang tenaga ahli yang memiliki keahlian di bidang teknologi Aset Kripto dan blockchain; c. memiliki perizinan dari kementerian/lembaga atau otoritas, apabila diwajibkan; dan d. sudah menjalankan aktivitas usahanya paling singkat 2 (dua) tahun dan memiliki pengalaman audit di bidang keuangan non perbankan.	dengan baik dan melaporkan kepada Bappebti; e. melakukan evaluasi terhadap Aset Kripto yang telah diperdagangkan di Pasar Fisik Aset Kripto; dan f. melakukan kajian atas usulan penambahan atau pengurangan jenis Aset Kripto dan menyampaikan rekomendasi hasil kajiannya kepada Bappebti.	(2) Pedagang Fisik Aset Kripto dilarang menjalankan kegiatan usaha lain selain sebagai Pedagang Fisik Komoditi.	disesuaikan yang menunjukkan perhitungan modal kerja Pedagang Fisik Aset Kripto yang merupakan selisih antara aset lancar dengan total liabilitas.	tersebut harus dipenuhi oleh perusahaan penyedia cloud service; (3) Sistem dan/atau sarana perdagangan online sebagaimana dimaksud pada ayat (1) huruf d wajib memenuhi persyaratan paling sedikit sebagai berikut: - a. akurat, aktual, aman, terpercaya, online dan realtime serta compatible secara sistem maupun aplikasi dengan sistem Bursa Berjangka dan Lembaga Kliring Berjangka; b. memenuhi standar spesifikasi dan fungsi sesuai dengan standar fungsionalitas sebagaimana diatur dalam Peraturan Badan ini, peraturan dan tata tertib Bursa Berjangka dan Lembaga Kliring Berjangka; c. fitur dan fungsi yang tersedia memenuhi seluruh ketentuan yang berlaku dalam Peraturan Badan ini, peraturan dan tata tertib Bursa Berjangka dan Lembaga Kliring Berjangka; d. memiliki fungsi yang dapat memproteksi akses data keuangan dan data transaksi setiap Pelanggan Aset Kripto; e. memiliki Business Continuity Plan (BCP) yang selalu mutakhir (up to date); f. memiliki Disaster Recovery Centre (DRC): g. memiliki konfigurasi h. memenuhi persyaratan database yang berfungsi untuk mengelola dan menyimpan data transaksi Aset Kripto seb i. server atau cloud server yang digunakan memiliki spesifikasi teknis yang baik untuk memfasilitasi penggunaan sistem dan/atau sarana perdagangan online yai j. memiliki sertifikasi ISO 27001 (Information Security Management System) yang di dalamnya sudah terdapat Statement of Applicability (SOA) untuk ISO 27017 (cloud security) dan ISO 27018 (cloud privacy) apabila menggunakan cloud services maka kewajiban atas ISO 27017 (cloud security) dan ISO 27018 (cloud privacy) tersebut harus dipenuhi oleh perusahaan penyedia cloud service;	saham, Pengendali dan/atau Pemilik Manfaat (Beneficial Owner) yang wajib lulus uji kepatutan dan kelayakan (fit and proper test) yang diselenggarakan oleh Bappebti. (2 Pedagang Fisik Aset Kripto harus memperhatikan ketentuan sebagai berikut: a. berperan menjadi market maker atau liquidity provider dalam transaksi; b. memberikan prioritas kepada Pelanggan Aset Kripto dalam pengambilan posisi jual atau beli; c. menggunakan dana atau Aset Kripto milik Pedagang Fisik Aset Kripto sendiri dan dana wajib ditempatkan pada rekening terpisah Lembaga Kliring Berjangka sedangkan Aset Kripto ditempatkan di Pengelola Tempat Penyimpanan Aset Kripto; d. dilarang menggunakan dana atau Aset Kripto milik Pelanggan Aset Kripto; e. menyampaikan mekanisme pengambilan posisi kepada Bappebti, Bursa Berjangka, Lembaga Kliring Berjangka dan Pelanggan Aset Kripto; dan f. melakukan pencatatan tersendiri mengenai pelaksanaannya. Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto dalam penyelenggaraan transaksi perdagangan Pasar Fisik Aset Kripto memiliki hak untuk: a. menerima atau menolak calon Pelanggan Aset Kripto berdasarkan hasil penerapan prinsip Know Your Customer (KYC) dan Customer Due Diligence (CDD) yang diatur dalam peraturan perundangundangan; dan b. menetapkan dan memungut biaya atau fee transaksi terhadap setiap transaksi yang dilakukan oleh Pelanggan Aset Kripto yang besarannya memperhatikan prinsip efisiensi dan kewajaran. e. memiliki tata cara perdagangan (trading rules) paling sedikit memuat: 1. definisi dan istilah; 2. proses pendaftaran Pelanggan Aset Kripto; - 3. pernyataan dan jaminan; 4. kewajiban dan tanggung jawab; 5. pengkinian data; 6. tata cara kegiatan transaksi, meliputi transaksi jual/beli, deposit, withdrawal, pengiriman Aset Kripto ke Wallet lain, kegiatan lain yang telah mendapat persetujuan dari Bappebti; 7. biaya transaksi dan batas penarikan dana; 8. keamanan transaksi; 9. layanan pengaduan Pelanggan Aset Kripto; 10. penyelesaian perselisihan Pelanggan Aset Kripto; 11. force majeur; 12. penerapan program Anti Pencucian Uang dan Pencegahan

						Pendanaan Terorisme serta Proliferasi Senjata Pemusnah Massal (APUPPT); dan 13. penyampaian syarat dan ketentuan dalam hal calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto mengambil posisi untuk diri sendiri; f. memiliki Standar Operasional Prosedur (SOP) paling sedikit mengatur tentang: 1. pemasaran dan penerimaan Pelanggan Aset Kripto; 2. pelaksanaan transaksi; 3. pengendalian dan pengawasan internal; 4. penyelesaian perselisihan Pelanggan Aset Kripto; dan 5. penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal. g. memiliki paling sedikit 1 (satu) pegawai yang bersertifikasi Certified Information Systems Security Professional (CISSP) atau memiliki kerja sama - 27 - dengan lembaga yang memiliki tenaga ahli atau langsung memiliki perjanjian kerja sama dengan tenaga ahli yang bersertifikasi Certified Information Systems Security Professional (CISSP); dan h. memiliki calon anggota direksi, anggota dewan komisaris, pemegang saham, Pengendali dan/atau Pemilik Manfaat (Beneficial Owner) yang wajib lulus uji kepatutan dan kelayakan (fit and proper test) yang diselenggarakan oleh Bappebti. (2 Pedagang Fisik Aset Kripto harus memperhatikan ketentuan sebagai berikut: a. berperan menjadi market maker atau liquidity provider dalam transaksi; b. memberikan prioritas kepada Pelanggan Aset Kripto dalam pengambilan posisi jual atau beli; c. menggunakan dana atau Aset Kripto milik Pedagang Fisik Aset Kripto sendiri dan dana wajib ditempatkan pada rekening terpisah Lembaga Kliring Berjangka sedangkan Aset Kripto ditempatkan di Pengelola Tempat Penyimpanan Aset Kripto; d. dilarang menggunakan dana atau Aset Kripto milik Pelanggan Aset Kripto; e. menyampaikan mekanisme pengambilan posisi kepada Bappebti, Bursa Berjangka, Lembaga Kliring Berjangka dan Pelanggan Aset Kripto; dan f. melakukan pencatatan tersendiri mengenai pelaksanaannya. Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto dalam penyelenggaraan transaksi perdagangan

						Pasar Fisik Aset Kripto memiliki hak untuk: a. menerima atau menolak calon Pelanggan Aset Kripto berdasarkan hasil penerapan prinsip Know Your Customer (KYC) dan Customer Due Diligence (CDD) yang diatur dalam peraturan perundangundangan; dan b. menetapkan dan memungut biaya atau fee transaksi terhadap setiap transaksi yang dilakukan oleh Pelanggan Aset Kripto yang besarannya memperhatikan prinsip efisiensi dan kewajaran.

4 : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto			Pedagang Fisik Aset Kripto wajib memenuhi ketentuan sebagai berikut: a. memberitahukan setiap perubahan sistem, bisnis proses, dan peraturan dan tata tertib yang dimiliki; b. menyediakan dan/atau membuka akses terhadap seluruh sistem yang dipergunakan kepada Bappebti dalam rangka pengawasan dengan hak akses untuk membaca (read only); c. mengikuti edukasi dan konseling yang diperlukan untuk pengembangan perdagangan Aset Kripto; e. mengikuti setiap pelaksanaan koordinasi dan kerja sama dengan Bappebti, kementerian/lembaga lain. Pedagang Fisik Aset Kripto wajib memenuhi ketentuan sebagai berikut: a. memberitahukan setiap perubahan sistem, bisnis proses, dan peraturan dan tata tertib yang dimiliki; b. menyediakan dan/atau membuka akses terhadap seluruh sistem yang dipergunakan kepada Bappebti dalam rangka pengawasan dengan hak akses untuk membaca (read only); c. mengikuti edukasi dan konseling yang diperlukan untuk pengembangan perdagangan Aset Kripto; e. mengikuti setiap pelaksanaan koordinasi dan kerja sama dengan Bappebti, kementerian/lembaga lain.			
5 : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka						
6 : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka						
7 : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka						

	M : 4. Pemeriksaan	N : 5. Pelaporan	O : Know Your Customer	P : CDD dan atau EDD	Q : Risk Based Approach	R : a. Identifikasi, Pemahaman dan Penilaian Risiko
1 : 1. UU 7 -2011_Mata Uang						
2 : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto						
3 : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	(4) Sistem dan/atau sarana perdagangan online sebagaimana dimaksud pada ayat (1) huruf d wajib diperiksa atau diaudit oleh lembaga independen yang memiliki kompetensi di bidang sistem informasi. (5) Dalam hal hasil audit sistem dan/atau sarana perdagangan online sebagaimana dimaksud pada ayat (4) terbukti tidak compatible baik secara sistem maupun aplikasi dengan sistem Bursa Berjangka, Lembaga Kliring Berjangka, dan Pengelola Tempat Penyimpanan Aset Kripto dan/atau tidak memenuhi standar spesifikasi dan fungsi minimum sebagaimana diatur dalam Peraturan Badan ini, peraturan tata tertib Bursa Berjangka dan Lembaga Kliring Berjangka, maka Pedagang Fisik Aset Kripto wajib menyesuaikan atau mengganti dengan sistem dan/atau sarana perdagangan online lainnya yang compatible. (1) Sertifikat ISO 27001 sebagaimana yang diwajibkan dalam Peraturan Badan ini hanya dapat diterbitkan oleh lembaga sertifikasi yang telah diakui oleh lembaga pemerintah yang menyelenggarakan urusan keamanan informasi. (2) Pelaksanaan audit sistem dan pemeriksaan terhadap sistem elektronik yang digunakan oleh Bursa Berjangka, Lembaga Kliring Berjangka, Pedagang Fisik Aset Kripto dan Pengelola Tempat Penyimpanan Aset Kripto wajib dilakukan oleh lembaga independen yang memiliki auditor dengan kompetensi di bidang sistem informasi. (3) Lembaga independen yang melakukan audit sistem atau pemeriksaan dalam peraturan badan ini wajib memiliki kriteria paling sedikit: a. 1 (satu) orang pegawai tetap yang bersertifikasi Certified Information System Auditor (CISA); b. 1 (satu) orang tenaga ahli yang memiliki keahlian di bidang teknologi Aset Kripto dan blockchain; c. memiliki perizinan dari kementerian/lembaga atau otoritas, apabila diwajibkan; dan d. sudah menjalankan aktivitas usahanya paling singkat 2 (dua) tahun dan memiliki pengalaman audit di bidang keuangan non perbankan. (4) Sistem dan/atau sarana perdagangan	(1) Pedagang Fisik Aset Kripto wajib menyampaikan kepada Kepala Bappebti: a. laporan transaksi secara harian dan bulanan; b. laporan keuangan secara harian, bulanan, dan tahunan; dan c. laporan kegiatan perusahaan secara triwulanan dan tahunan. (1) Pedagang Fisik Aset Kripto wajib menyampaikan kepada Kepala Bappebti: a. laporan transaksi secara harian dan bulanan; b. laporan keuangan secara harian, bulanan, dan tahunan; dan c. laporan kegiatan perusahaan secara triwulanan dan tahunan.	proses penerimaan calon Pelanggan Aset Kripto wajib menerapkan prinsip mengenal calon Pelanggan Aset Kripto atau Know Your Customer (KYC) Pedagang Fisik Aset Kripto wajib melakukan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal yang ditetapkan oleh Kepala Bappebti terhadap seluruh Pelanggan Aset Kripto baik pada saat proses penerimaan Pelanggan Aset Kripto, selama menjadi Pelanggan Aset Kripto, pemantauan transaksi, dan melakukan proses pengkinian penilaian risiko Pelanggan Aset Kripto secara berkala. proses penerimaan calon Pelanggan Aset Kripto wajib menerapkan prinsip mengenal calon Pelanggan Aset Kripto atau Know Your Customer (KYC) Pedagang Fisik Aset Kripto wajib melakukan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal yang ditetapkan oleh Kepala Bappebti terhadap seluruh Pelanggan Aset Kripto baik pada saat proses penerimaan Pelanggan Aset Kripto, selama menjadi Pelanggan Aset Kripto, pemantauan transaksi, dan melakukan proses pengkinian penilaian risiko Pelanggan Aset Kripto secara berkala.	melakukan Customer Due Diligence (CDD) atau Enhanced Due Diligence (EDD) untuk memastikan kebenaran dan kelengkapan data isian Pelanggan Aset Kripto dan latar belakang atau profil Pelanggan Aset Kripto Pelaksanaan Customer Due Diligence (CDD) atau Enhanced Due Diligence (EDD) sebagaimana dimaksud pada ayat (1) wajib dilakukan sesuai dengan peraturan Bappebti dan peraturan perundang-undangan yang mengatur tentang penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal. Akun Pelanggan Aset Kripto sebagaimana dimaksud dalam Pasal 25 ayat (4) hanya dapat dipergunakan apabila Pelanggan Aset Kripto telah lulus proses identifikasi dan verifikasi sesuai dengan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal sebagaimana dimaksud pada ayat (2). Penerapan prinsip mengenal calon Pelanggan Aset Kripto atau Know Your Customer (KYC), Customer Due Diligence (CDD) dan/atau Enhanced Due Diligence (EDD), calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto wajib terkoneksi dengan data administrasi kependudukan yang dimiliki oleh Kementerian Dalam Negeri. Data isian yang tercantum dalam sistem penerimaan sebagaimana dimaksud pada ayat (1) harus dapat digunakan oleh calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto sebagai pedoman untuk melakukan Customer Due Diligence (CDD) atau Enhanced Due Diligence (EDD) bagi Pelanggan Aset Kripto yang berisiko tinggi. Calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto sebelum menerima penempatan sejumlah Aset Kripto dari Pelanggan Aset Kripto sebagaimana dimaksud pada ayat (2), wajib terlebih dahulu melakukan	Pedagang Fisik Aset Kripto wajib melakukan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal yang ditetapkan oleh Kepala Bappebti terhadap seluruh Pelanggan Aset Kripto baik pada saat proses penerimaan Pelanggan Aset Kripto, selama menjadi Pelanggan Aset Kripto, pemantauan transaksi, dan melakukan proses pengkinian penilaian risiko Pelanggan Aset Kripto secara berkala. Pedagang Fisik Aset Kripto wajib melakukan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal yang ditetapkan oleh Kepala Bappebti terhadap seluruh Pelanggan Aset Kripto baik pada saat proses penerimaan Pelanggan Aset Kripto, selama menjadi Pelanggan Aset Kripto, pemantauan transaksi, dan melakukan proses pengkinian penilaian risiko Pelanggan Aset Kripto secara berkala.	

	online sebagaimana dimaksud pada ayat (1) huruf d wajib diperiksa atau diaudit oleh lembaga independen yang memiliki kompetensi di bidang sistem informasi. (5) Dalam hal hasil audit sistem dan/atau sarana perdagangan online sebagaimana dimaksud pada ayat (4) terbukti tidak compatible baik secara sistem maupun aplikasi dengan sistem Bursa Berjangka, Lembaga Kliring Berjangka, dan Pengelola Tempat Penyimpanan Aset Kripto dan/atau tidak memenuhi standar spesifikasi dan fungsi minimum sebagaimana diatur dalam Peraturan Badan ini, peraturan tata tertib Bursa Berjangka dan Lembaga Kliring Berjangka, maka Pedagang Fisik Aset Kripto wajib menyesuaikan atau mengganti dengan sistem dan/atau sarana perdagangan online lainnya yang compatible. (1) Sertifikat ISO 27001 sebagaimana yang diwajibkan dalam Peraturan Badan ini hanya dapat diterbitkan oleh lembaga sertifikasi yang telah diakui oleh lembaga pemerintah yang menyelenggarakan urusan keamanan informasi. (2) Pelaksanaan audit sistem dan pemeriksaan terhadap sistem elektronik yang digunakan oleh Bursa Berjangka, Lembaga Kliring Berjangka, Pedagang Fisik Aset Kripto dan Pengelola Tempat Penyimpanan Aset Kripto wajib dilakukan oleh lembaga independen yang memiliki auditor dengan kompetensi di bidang sistem informasi. (3) Lembaga independen yang melakukan audit sistem atau pemeriksaan dalam peraturan badan ini wajib memiliki kriteria paling sedikit: a. 1 (satu) orang pegawai tetap yang bersertifikasi Certified Information System Auditor (CISA); b. 1 (satu) orang tenaga ahli yang memiliki keahlian di bidang teknologi Aset Kripto dan blockchain; c. memiliki perizinan dari kementerian/lembaga atau otoritas, apabila diwajibkan; dan d. sudah menjalankan aktivitas usahanya paling singkat 2 (dua) tahun dan memiliki pengalaman audit di bidang keuangan non perbankan.			Customer Due Diligence (CDD) terhadap Wallet milik Pelanggan Aset Kripto atau Wallet bukan milik Pelanggan Aset Kripto untuk memastikan identitas Wallet dan tidak bersumber atau berasal dari tindak pidana, pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal. melakukan Customer Due Diligence (CDD) atau Enhanced Due Diligence (EDD) untuk memastikan kebenaran dan kelengkapan data isian Pelanggan Aset Kripto dan latar belakang atau profil Pelanggan Aset Kripto Pelaksanaan Customer Due Diligence (CDD) atau Enhanced Due Diligence (EDD) sebagaimana dimaksud pada ayat (1) wajib dilakukan sesuai dengan peraturan Bappebti dan peraturan perundang-undangan yang mengatur tentang penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal. Akun Pelanggan Aset Kripto sebagaimana dimaksud dalam Pasal 25 ayat (4) hanya dapat dipergunakan apabila Pelanggan Aset Kripto telah lulus proses identifikasi dan verifikasi sesuai dengan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal sebagaimana dimaksud pada ayat (2). Penerapan prinsip mengenal calon Pelanggan Aset Kripto atau Know Your Customer (KYC), Customer Due Diligence (CDD) dan/atau Enhanced Due Diligence (EDD), calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto wajib terkoneksi dengan data administrasi kependudukan yang dimiliki oleh Kementerian Dalam Negeri. Data isian yang tercantum dalam sistem penerimaan sebagaimana dimaksud pada ayat (1) harus dapat digunakan oleh calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto sebagai pedoman untuk melakukan Customer Due Diligence (CDD) atau Enhanced Due Diligence (EDD) bagi Pelanggan Aset Kripto yang berisiko tinggi. Calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto sebelum		

				menerima penempatan sejumlah Aset Kripto dari Pelanggan Aset Kripto sebagaimana dimaksud pada ayat (2), wajib terlebih dahulu melakukan Customer Due Diligence (CDD) terhadap Wallet milik Pelanggan Aset Kripto atau Wallet bukan milik Pelanggan Aset Kripto untuk memastikan identitas Wallet dan tidak bersumber atau berasal dari tindak pidana, pencucian uang dan pendanaan terorisme serta proliferasi senjata pemusnah massal.		
4 : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto		menyampaikan laporan berkala dan sewaktu-waktu atas pelaksanaan perdagangan Aset Kripto yang bentuk dan isinya ditentukan lebih lanjut dalam Surat Edaran Kepala Bappebti menyampaikan laporan berkala dan sewaktu-waktu atas pelaksanaan perdagangan Aset Kripto yang bentuk dan isinya ditentukan lebih lanjut dalam Surat Edaran Kepala Bappebti				
5 : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka			Nasabah yang Berisiko Tinggi (High Risk Customers) adalah Nasabah yang berdasarkan latar belakang identitas dan riwayatnya dianggap memiliki risiko tinggi melakukan kegiatan terkait dengan tindak pidana pencucian uang dan/atau Pendanaan Kegiatan Terorisme. Nasabah yang Berisiko Tinggi (High Risk Customers) adalah Nasabah yang berdasarkan latar belakang identitas dan riwayatnya dianggap memiliki risiko tinggi melakukan kegiatan terkait dengan tindak pidana pencucian uang dan/atau Pendanaan Kegiatan Terorisme.	Uji Tuntas Nasabah (Customer Due Diligence) yang selanjutnya disingkat CDD adalah kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Pialang Berjangka untuk memastikan transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi Calon Nasabah atau Nasabah. Uji Tuntas Lanjut (Enhanced Due Diligence) yang selanjutnya disingkat EDD adalah tindakan CDD lebih mendalam yang dilakukan Pialang Berjangka terhadap Calon Nasabah atau Nasabah, yang berisiko tinggi termasuk Politically Exposed Person (PEP) dan/atau dalam area berisiko tinggi. Uji Tuntas Nasabah (Customer Due Diligence) yang selanjutnya disingkat CDD adalah kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Pialang Berjangka untuk memastikan transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi Calon Nasabah atau Nasabah. Uji Tuntas Lanjut (Enhanced Due Diligence) yang selanjutnya disingkat EDD adalah tindakan CDD lebih mendalam yang dilakukan Pialang Berjangka terhadap Calon Nasabah atau Nasabah, yang berisiko tinggi termasuk Politically Exposed Person (PEP) dan/atau dalam area berisiko tinggi.	untuk mewujudkan kegiatan Perdagangan Berjangka yang teratur, wajar, efisien, efektif, dan transparan serta dalam suasana persaingan yang sehat terutama menciptakan industri Perdagangan Berjangka yang sehat dan terlindung dari praktik tindak pidana pencucian uang dan dijadikan sarana pendanaan kegiatan terorisme diperlukan adanya suatu pedoman dalam rangka menerapkan program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme, yang didasarkan pada pendekatan berbasis risiko (risk based approach) sesuai dengan prinsip umum yang berlaku secara internasional; untuk mewujudkan kegiatan Perdagangan Berjangka yang teratur, wajar, efisien, efektif, dan transparan serta dalam suasana persaingan yang sehat terutama menciptakan industri Perdagangan Berjangka yang sehat dan terlindung dari praktik tindak pidana pencucian uang dan dijadikan sarana pendanaan kegiatan terorisme diperlukan adanya suatu pedoman dalam rangka menerapkan program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme, yang didasarkan pada pendekatan berbasis risiko (risk based approach) sesuai dengan prinsip umum yang berlaku secara internasional;	

6 : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka				Uji tuntas Nasabah (Customer Due Dilligence/CDD) merupakan kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan Pialang Berjangka untuk memastikan bahwa transaksi tersebut sesuai dengan profil calon Nasabah atau Nasabah. Pialang Berjangka harus melakukan prosedur CDD pada saat: 1) melakukan hubungan usaha dengan calon Nasabah, misalnya pada saat pembukaan rekening efek. 2) 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). 3) terdapat indikasi transaksi keuangan mencurigakan yang terkait dengan Pencucian Uang dan/atau Pendanaan Terorisme 4) Pialang Berjangka meragukan kebenaran informasi yang diberikan oleh Nasabah, penerima kuasa, dan/atau pemilik manfaat (beneficial owner). e. apabila diperlukan dapat dilakukan wawancara dengan calon Nasabah untuk memperoleh keyakinan atas kebenaran informasi, bukti identitas, dan dokumen pendukung calon Nasabah; g. pertemuan langsung (face to face) dengan calon Nasabah pada awal melakukan hubungan usaha dalam rangka meyakini kebenaran identitas calon Nasabah; h. kewaspadaan terhadap transaksi atau hubungan usaha dengan calon Nasabah yang berasal atau terkait dengan negara yang belum memadai dalam melaksanakan rekomendasi Financial Action Task Force (FATF) i. penyelesaian proses verifikasi identitas calon Nasabah dan pemilik manfaat (beneficial owner) dilakukan sebelum membina hubungan usaha dengan calon Nasabah. b. Dalam hal pemilik manfaat (beneficial owner) tergolong sebagai PEP maka prosedur yang diterapkan adalah prosedur CDD yang lebih ketat atau uji tuntas lanjut (enhanced due dilligence/EDD). 8) memastikan bahwa calon Nasabah, Nasabah, dan pemilik manfaat tidak memiliki rekam jejak negatif dengan melakukan verifikasi identitas calon Nasabah, Nasabah dan pemilik manfaat menggunakan sumber independen lainnya antara lain sebagai berikut: a.	perlu adanya peningkatan kualitas penerapan program APU dan PPT yang didasarkan pada pendekatan berbasis risiko (risk based approach) 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). Pialang Berjangka harus merujuk dan mempertimbangkan risiko sebagaimana yang tercantum dalam NRA dan SRA. Adapun risiko yang tercantum dalam NRA dan SRA tersebut dapat berkembang dan mengalami perubahan. Oleh karena itu, penerapan program APU dan PPT yang dimiliki Pialang Berjangka harus responsif terhadap perubahan risiko tersebut. Dalam menilai risiko Pialang Berjangka juga mempertimbangkan dampak risiko tersebut, dimana dampak suatu risiko dilihat dari tingkat kerusakan dan kerugian yang serius yang timbul jika terdapat TPPU dan TPPT yang material. Dalam menerapkan manajemen risiko atas risiko Pencucian Uang dan Pendanaan Terorisme, Pialang Berjangka dapat mengembangkan metode manajemen risiko sesuai dengan karakteristik Pialang Berjangka dengan tetap mengacu pada ketentuan peraturan perundang-undangan yang mengatur mengenai APU dan PPT. Dalam melakukan pendekatan berbasis risiko (risk based approach), Pialang Berjangka harus melakukan 6 (enam) langkah kegiatan sebagai berikut: a. melakukan identifikasi, pemahaman, dan penilaian terhadap risiko bawaan; b. menetapkan toleransi risiko; c. menyusun langkah pengurangan dan pengendalian risiko; d. melakukan evaluasi atas risiko residual; e. menerapkan pendekatan berbasis risiko; dan f. melakukan peninjauan dan evaluasi atas pendekatan berbasis risiko yang telah dimiliki. perlu adanya peningkatan kualitas penerapan program APU dan PPT yang didasarkan pada pendekatan berbasis risiko (risk based approach) sesuai dengan prinsip-prinsip umum yang berlaku secara internasional, serta sejalan dengan penilaian risiko nasional (national risk assessment/NRA) dan	Pialang Berjangka harus mempertimbangkan unsur yang memicu timbulnya risiko baik dari sisi Nasabah, geografis/negara/yurisdiksi, produk, jasa, atau transaksi, dan jaringan distribusi (delivery channels). Jumlah aktual atas risiko yang diinventarisasi oleh Pialang Berjangka akan bervariasi bergantung pada kegiatan usaha, dan produk atau jasa yang ditawarkan. c. Risiko Nasabah Beberapa kategori Nasabah yang aktivitasnya dapat diindikasikan memiliki risiko tinggi antara lain: 1) Nasabah yang melakukan hubungan usaha atau transaksi yang tidak wajar atau tidak sesuai dengan profil Nasabah, 2) Nasabah korporasi yang struktur kepemilikannya kompleks dan menimbulkan kesulitan untuk diidentifikasi siapa yang menjadi pemilik manfaat (beneficial owner), pemilik akhir (ultimate owner) atau pengendali akhir (ultimate controller) dari korporasi 3) Nasabah yang termasuk dalam kategori orang yang Populer Secara Politis (politically exposed person) yang selanjutnya disingkat PEP, termasuk anggota keluarga atau pihak yang terkait (close associates) dari PEP 4) Nasabah yang pemilik manfaatnya (beneficial owner) tidak diketahui 5) Nasabah yang tidak bersedia memberikan data dan informasi dalam proses identifikasi atau Nasabah yang memberikan informasi yang sangat minim atau informasi yang patut diduga sebagai informasi fiktif. d. Risiko Negara atau Area Geografis Pialang Berjangka harus mengidentifikasi unsur risiko tinggi terkait dengan lokasi geografis, baik lokasi geografis Pialang Berjangka maupun lokasi geografis Nasabah atau lokasi tempat terjadinya hubungan usaha, dan dampaknya pada keseluruhan risiko. Risiko Pencucian Uang dan Pendanaan Terorisme pada Pialang Berjangka meningkat apabila: - 19 - 1) dana diterima dari atau dikirim ke negara/yurisdiksi yang berisiko tinggi; atau 2) Nasabah memiliki hubungan yang signifikan dengan negara/yurisdiksi berisiko tinggi. e. Risiko Produk/Jasa/Transaksi Penilaian risiko secara keseluruhan juga harus mengikutsertakan penentuan

				daftar teroris dan/atau daftar terduga teroris dan organisasi teroris yang diterbitkan oleh Kepolisian Negara Republik Indonesia; b. daftar hitam nasional (DHN); atau c. data lainnya yang dimiliki Pialang Berjangka, identitas pemberi kerja dari calon Nasabah, Nasabah, dan pemilik manfaat, rekening telepon, dan rekening listrik; dan/atau Uji Tuntas Lanjut (Enhanced Due Diligence/EDD) a. Dalam hal Pialang Berjangka menilai Nasabah berisiko tinggi maka Pialang Berjangka menerapkan kadar CDD yang lebih tinggi berupa EDD terhadap Nasabah yang bersangkutan. Verifikasi informasi dalam pelaksanaan EDD dapat dilakukan antara lain dengan cara: 1. mencari informasi tambahan tentang Nasabah bersangkutan dan melakukan pengkinian atas data identitas Nasabah atau pemilik manfaat (beneficial owner); 2. mencari informasi tambahan tentang sifat peruntukan dari hubungan bisnis tersebut; 3. mencari informasi tambahan mengenai sumber dana atau sumber kekayaan Nasabah tersebut; 4. mencari infromasi tambahan mengenai alasan dari transaksi yang dimaksud atau yang dilakukan; 5. meminta persetujuan dari pejabat senior untuk memulai atau meneruskan hubungan bisnis tersebut; dan/atau 6. melakukan pemantauan yang semakin diperketat terhadap hubungan bisnis tersebut, yaitu dengan menambah jumlah dan waktu pengawas yang dipakai, dan memiliki pola transaksi yang memerlukan pemeriksaan lebih lanjut. Pialang Berjangka harus melakukan kegiatan pemantauan yang paling sedikit: 1) dilakukan secara berkesinambungan untuk mengidentifikasi kesesuaian antara transaksi Nasabah dengan profil Nasabah dan menatausahakan dokumen tersebut, terutama terhadap hubungan usaha atau transaksi dengan Nasabah dan/atau Pialang Berjangka dari negara dengan program APU dan PPT kurang memadai; 2) melakukan analisis terhadap seluruh transaksi yang tidak sesuai dengan profil Nasabah; dan 3) apabila diperlukan, meminta informasi tentang latar belakang dan tujuan transaksi terhadap transaksi yang tidak sesuai dengan profil Nasabah, dengan memperhatikan ketentuan anti tipping off sebagaimana dimaksud dalam UndangUndang mengenai	penilaian risiko sektoral (sectoral risk assessment/SRA). Pialang Berjangka harus merujuk dan mempertimbangkan risiko sebagaimana yang tercantum dalam NRA dan SRA. Adapun risiko yang tercantum dalam NRA dan SRA tersebut dapat berkembang dan mengalami perubahan. Oleh karena itu, penerapan program APU dan PPT yang dimiliki Pialang Berjangka harus responsif terhadap perubahan risiko tersebut. Dalam menilai risiko Pialang Berjangka juga mempertimbangkan dampak risiko tersebut, dimana dampak suatu risiko dilihat dari tingkat kerusakan dan kerugian yang serius yang timbul jika terdapat TPPU dan TPPT yang material. Dalam menerapkan manajemen risiko atas risiko Pencucian Uang dan Pendanaan Terorisme, Pialang Berjangka dapat mengembangkan metode manajemen risiko sesuai dengan karakteristik Pialang Berjangka dengan tetap mengacu pada ketentuan peraturan perundang-undangan yang mengatur mengenai APU dan PPT. Dalam melakukan pendekatan berbasis risiko (risk based approach), Pialang Berjangka harus melakukan 6 (enam) langkah kegiatan sebagai berikut: a. melakukan identifikasi, pemahaman, dan penilaian terhadap risiko bawaan; b. menetapkan toleransi risiko; c. menyusun langkah pengurangan dan pengendalian risiko; d. melakukan evaluasi atas risiko residual; e. menerapkan pendekatan berbasis risiko; dan f. melakukan peninjauan dan evaluasi atas pendekatan berbasis risiko yang telah dimiliki.	risiko potensial yang muncul dari berbagai produk Pialang Berjangka f. Risiko Jaringan Distribusi (delivery channels) Jaringan distribusi merupakan media yang digunakan untuk memperoleh suatu produk atau jasa, atau media - 21 - yang digunakan untuk melakukan suatu transaksi. Jaringan distribusi harus dipertimbangkan sebagai risiko transaksi. Jaringan distribusi, yang memungkinkan adanya transaksi tanpa pertemuan langsung (non face to face), memiliki risiko bawaan yang lebih tinggi. g. Risiko Relevan lainnya Faktor lain yang relevan yang dapat memberikan dampak pada risiko Pencucian Uang dan Pendanaan Terorisme, seperti: 1) tren tipologi, metode, teknik, dan skema Pencucian Uang dan Pendanaan Terorisme; dan 2) model bisnis Pialang Berjangka. Penskoran (scoring) Penilaian Risiko 1) Setelah melakukan identifikasi dan dokumentasi risiko bawaan, Pialang Berjangka perlu memberikan - 22 - level pada setiap risiko. 2) Skala risiko perlu disusun, disesuaikan dengan skala bisnis dan jenis usaha Pialang Berjangka. 3) Usaha dengan skala bisnis kecil yang melakukan transaksi sederhana dapat mengategorikan risiko dalam 2 (dua) kategori rendah dan tinggi. 4) Untuk kegiatan usaha bisnis dengan skala bisnis lebih besar diharapkan dapat mengategorikan risiko dalam beberapa level, misalnya menengah, menengah-tinggi (medium-high), atau tinggi (high). Pialang Berjangka harus mempertimbangkan unsur yang memicu timbulnya risiko baik dari sisi Nasabah, geografis/negara/yurisdiksi, produk, jasa, atau transaksi, dan jaringan distribusi (delivery channels). Jumlah aktual atas risiko yang diinventarisasi oleh Pialang Berjangka akan bervariasi bergantung pada kegiatan usaha, dan produk atau jasa yang ditawarkan. c. Risiko Nasabah Beberapa kategori Nasabah yang aktivitasnya dapat diindikasikan memiliki risiko tinggi antara lain: 1) Nasabah yang melakukan hubungan usaha atau transaksi yang tidak wajar atau tidak sesuai dengan profil Nasabah, 2) Nasabah korporasi yang struktur kepemilikannya kompleks dan

				pencegahan dan pemberantasan TPPU. e. Pialang Berjangka harus melakukan klasifikasi terkait transaksi dan Nasabah yang membutuhkan pemantauan khusus. Pemantauan terhadap rekening Nasabah harus dipantau lebih ketat apabila terdapat Nasabah berisiko tinggi. f. Seluruh kegiatan pemantauan didokumentasikan dengan baik dalam bentuk tertulis baik melalui dokumen formal seperti memo, nota, atau catatan maupun melalui dokumen informal seperti korespondensi melalui surat elektronik (email). c. Pialang Berjangka harus memastikan bahwa dokumen, data, atau informasi yang dihimpun dalam proses CDD selalu diperbarui dan relevan dengan melakukan pemeriksaan kembali terhadap data yang ada, khususnya yang terkait dengan Nasabah berisiko tinggi Dalam hal proses CDD menunjukkan adanya calon Nasabah atau Nasabah yang dikategorikan berisiko tinggi maka pegawai Pialang Berjangka yang melaksanakan CDD melaporkan kepada direktur utama. Direktur utama bertanggung jawab terhadap penerimaan dan/atau penolakan hubungan usaha dengan calon Nasabah dan Nasabah yang berisiko tinggi. Direktur Utama sebagai penanggungjawab penerapan program APU dan PPT, wajib mendokumentasikan terkait jumlah calon Nasabah atau Nasabah yang berisiko tinggi termasuk jumlah Nasabah berisiko tinggi yang ditolak, diterima, atau dilakukan penutupan hubungan usaha. d. Direktur utama harus memberikan arahan atas laporan yang disampaikan dan menetapkan langkah mitigasi risiko. Uji tuntas Nasabah (Customer Due Dilligence/CDD) merupakan kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan Pialang Berjangka untuk memastikan bahwa transaksi tersebut sesuai dengan profil calon Nasabah atau Nasabah. Pialang Berjangka harus melakukan prosedur CDD pada saat: 1) melakukan hubungan usaha dengan calon Nasabah, misalnya pada saat pembukaan rekening	menimbulkan kesulitan untuk diidentifikasi siapa yang menjadi pemilik manfaat (beneficial owner), pemilik akhir (ultimate owner) atau pengendali akhir (ultimate controller) dari korporasi 3) Nasabah yang termasuk dalam kategori orang yang Populer Secara Politis (politically exposed person) yang selanjutnya disingkat PEP, termasuk anggota keluarga atau pihak yang terkait (close associates) dari PEP 4) Nasabah yang pemilik manfaatnya (beneficial owner) tidak diketahui 5) Nasabah yang tidak bersedia memberikan data dan informasi dalam proses identifikasi atau Nasabah yang memberikan informasi yang sangat minim atau informasi yang patut diduga sebagai informasi fiktif. d. Risiko Negara atau Area Geografis Pialang Berjangka harus mengidentifikasi unsur risiko tinggi terkait dengan lokasi geografis, baik lokasi geografis Pialang Berjangka maupun lokasi geografis Nasabah atau lokasi tempat terjadinya hubungan usaha, dan dampaknya pada keseluruhan risiko. Risiko Pencucian Uang dan Pendanaan Terorisme pada Pialang Berjangka meningkat apabila: - 19 - 1) dana diterima dari atau dikirim ke negara/yurisdiksi yang berisiko tinggi; atau 2) Nasabah memiliki hubungan yang signifikan dengan negara/yurisdiksi berisiko tinggi. e. Risiko Produk/Jasa/Transaksi Penilaian risiko secara keseluruhan juga harus mengikutsertakan penentuan risiko potensial yang muncul dari berbagai produk Pialang Berjangka f. Risiko Jaringan Distribusi (delivery channels) Jaringan distribusi merupakan media yang digunakan untuk memperoleh suatu produk atau jasa, atau media - 21 - yang digunakan untuk melakukan suatu transaksi. Jaringan distribusi harus dipertimbangkan sebagai risiko transaksi. Jaringan distribusi, yang memungkinkan adanya transaksi tanpa pertemuan langsung (non face to face), memiliki risiko bawaan yang lebih tinggi. g. Risiko Relevan lainnya Faktor lain yang relevan yang dapat memberikan dampak pada risiko Pencucian Uang dan

				efek. 2) 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). 3) terdapat indikasi transaksi keuangan mencurigakan yang terkait dengan Pencucian Uang dan/atau Pendanaan Terorisme 4) Pialang Berjangka meragukan kebenaran informasi yang diberikan oleh Nasabah, penerima kuasa, dan/atau pemilik manfaat (beneficial owner). e. apabila diperlukan dapat dilakukan wawancara dengan calon Nasabah untuk memperoleh keyakinan atas kebenaran informasi, bukti identitas, dan dokumen pendukung calon Nasabah; g. pertemuan langsung (face to face) dengan calon Nasabah pada awal melakukan hubungan usaha dalam rangka meyakini kebenaran identitas calon Nasabah; h. kewaspadaan terhadap transaksi atau hubungan usaha dengan calon Nasabah yang berasal atau terkait dengan negara yang belum memadai dalam melaksanakan rekomendasi Financial Action Task Force (FATF) i. penyelesaian proses verifikasi identitas calon Nasabah dan pemilik manfaat (beneficial owner) dilakukan sebelum membina hubungan usaha dengan calon Nasabah. b. Dalam hal pemilik manfaat (beneficial owner) tergolong sebagai PEP maka prosedur yang diterapkan adalah prosedur CDD yang lebih ketat atau uji tuntas lanjut (enhanced due dilligence/EDD). 8) memastikan bahwa calon Nasabah, Nasabah, dan pemilik manfaat tidak memiliki rekam jejak negatif dengan melakukan verifikasi identitas calon Nasabah, Nasabah dan pemilik manfaat menggunakan sumber independen lainnya antara lain sebagai berikut: a. daftar teroris dan/atau daftar terduga teroris dan organisasi teroris yang diterbitkan oleh Kepolisian Negara Republik Indonesia; b. daftar hitam nasional (DHN); atau c. data lainnya yang dimiliki Pialang Berjangka, identitas pemberi kerja dari calon Nasabah, Nasabah, dan pemilik manfaat, rekening telepon, dan rekening listrik; dan/atau Uji Tuntas Lanjut (Enhanced Due	Pendanaan Terorisme, seperti: 1) tren tipologi, metode, teknik, dan skema Pencucian Uang dan Pendanaan Terorisme; dan 2) model bisnis Pialang Berjangka. Penskoran (scoring) Penilaian Risiko 1) Setelah melakukan identifikasi dan dokumentasi risiko bawaan, Pialang Berjangka perlu memberikan - 22 - level pada setiap risiko. 2) Skala risiko perlu disusun, disesuaikan dengan skala bisnis dan jenis usaha Pialang Berjangka. 3) Usaha dengan skala bisnis kecil yang melakukan transaksi sederhana dapat mengategorikan risiko dalam 2 (dua) kategori rendah dan tinggi. 4) Untuk kegiatan usaha bisnis dengan skala bisnis lebih besar diharapkan dapat mengategorikan risiko dalam beberapa level, misalnya menengah, menengah-tinggi (medium-high), atau tinggi (high).	

				Diligence/EDD) a. Dalam hal Pialang Berjangka menilai Nasabah berisiko tinggi maka Pialang Berjangka menerapkan kadar CDD yang lebih tinggi be		
7 : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka			Nasabah yang Berisiko Tinggi (High Risk Customers) adalah Nasabah yang berdasarkan latar belakang identitas dan riwayatnya dianggap memiliki risiko tinggi melakukan kegiatan terkait dengan tindak pidana Pencucian Uang dan/atau Pendanaan kegiatan Terorisme. Kriteria berisiko tinggi dari calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) sebagaimana dimaksud pada ayat (1) dapat dilihat dari: a. latar belakang atau profil calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner), termasuk Nasabah Berisiko Tinggi (High Risk Customers); b. produk Perdagangan Berjangka yang berisiko tinggi untuk digunakan sebagai sarana Pencucian Uang dan/atau Pendanaan Terorisme; c. transaksi dengan pihak yang berasal dari Negara Berisiko Tinggi (High Risk Countries); d. transaksi tidak sesuai dengan profil; e. termasuk dalam kategori PEP; f. bidang usaha calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) termasuk usaha yang berisiko tinggi (High Risk Business); g. negara atau teritori asal, domisili, atau dilakukannya transaksi calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) termasuk Negara Berisiko Tinggi (High Risk Countries); h. tercantumnya calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) dalam daftar terduga teroris dan organisasi teroris; atau i. transaksi yang dilakukan calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) diduga terkait dengan tindak pidana di sektor jasa keuangan, tindak pidana Pencucian Uang, dan/atau tindak pidana Pendanaan Terorisme. Dalam hal calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) adalah anggota keluarga atau pihak yang terkait (close associates) dari PEP maka seluruh ketentuan yang terkait dengan PEP dalam Peraturan Kepala Badan ini berlaku juga terhadap anggota keluarga atau pihak yang terkait (close associates) dari PEP dimaksud. meliputi: a. orang tua kandung/tiri/angkat; b. saudara kandung/tiri/angkat; c. anak	Uji Tuntas Nasabah (Customer Due Diligence) yang selanjutnya disingkat CDD adalah kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Pialang Berjangka untuk memastikan transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi calon Nasabah atau Nasabah. Uji Tuntas Lanjut (Enhanced Due Diligence) yang selanjutnya disingkat EDD adalah tindakan CDD lebih mendalam yang dilakukan Pialang Berjangka terhadap calon Nasabah atau Nasabah, yang berisiko tinggi termasuk Politically Exposed Person (PEP) dan/atau dalam area berisiko tinggi. 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 efek yang ditempatkan pada Pialang Berjangka (ultimately own account), mengendalikan transaksi Nasabah, memberikan kuasa untuk melakukan transaksi, mengendalikan korporasi dan/atau merupakan pengendali akhir dari transaksi yang dilakukan melalui badan hukum. Orang yang Populer Secara Politis (Politically Exposed Person) yang selanjutnya disingkat PEP meliputi: a. PEP Asing yaitu orang yang diberi kewenangan untuk melakukan fungsi penting (prominent function) oleh negara lain (asing) b. PEP Domestik yaitu orang yang diberi kewenangan untuk melakukan fungsi penting (prominent function) oleh negara c. Orang yang diberi kewenangan untuk melakukan fungsi penting (prominent function) oleh organisasi internasional Pialang Berjangka wajib melakukan prosedur CDD pada saat: a. proses penerimaan calon Nasabah menjadi Nasabah Pialang Berjangka; 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 keraguan kebenaran data, informasi, dan/atau dokumen pendukung		Pialang Berjangka wajib mengidentifikasi, menilai, dan memahami risiko tindak pidana Pencucian Uang dan/atau tindak pidana Pendanaan Terorisme terkait dengan Nasabah, negara atau area geografis, produk, jasa, transaksi atau jaringan distribusi (delivery channels) (2) Pialang Berjangka wajib melakukan penilaian risiko sebagaimana dimaksud pada ayat (1) sebelum produk, praktik usaha dan teknologi diluncurkan atau digunakan. (3) Pialang Berjangka wajib melakukan tindakan yang memadai untuk mengelola dan memitigasi risiko sebagaimana dimaksud pada ayat (1). Pialang Berjangka wajib mengidentifikasi, menilai, dan memahami risiko tindak pidana Pencucian Uang dan/atau tindak pidana Pendanaan Terorisme terkait dengan Nasabah, negara atau area geografis, produk, jasa, transaksi atau jaringan distribusi (delivery channels) (2) Pialang Berjangka wajib melakukan penilaian risiko sebagaimana dimaksud pada ayat (1) sebelum produk, praktik usaha dan teknologi diluncurkan atau digunakan. (3) Pialang Berjangka wajib melakukan tindakan yang memadai untuk mengelola dan memitigasi risiko sebagaimana dimaksud pada ayat (1).

			kandung/tiri/angkat; d. kakek atau nenek kandung/tiri/angkat; e. cucu kandung/tiri/angkat; f. saudara kandung/tiri/angkat dari orang tua; g. suami atau istri; h. mertua atau besan; i. suami atau istri dari anak kandung/tiri/angkat; j. kakek atau nenek dari suami atau istri; k. suami atau istri dari cucu kandung/tiri /angkat; l. saudara kandung/tiri/angkat dari suami; atau m. istri beserta suami atau istrinya dari saudara, yang bersangkutan. Pihak yang terkait dengan PEP sebagaimana dimaksud pada ayat (1) meliputi: 1. perusahaan yang dimiliki atau dikelola oleh PEP; atau 2. pihak yang secara umum dan diketahui publik mempunyai hubungan dekat dengan PEP. Seperti supir, asisten pribadi, sekretaris pribadi. Nasabah yang Berisiko Tinggi (High Risk Customers) adalah Nasabah yang berdasarkan latar belakang identitas dan riwayatnya dianggap memiliki risiko tinggi melakukan kegiatan terkait dengan tindak pidana Pencucian Uang dan/atau Pendanaan kegiatan Terorisme. Kriteria berisiko tinggi dari calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) sebagaimana dimaksud pada ayat (1) dapat dilihat dari: a. latar belakang atau profil calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner), termasuk Nasabah Berisiko Tinggi (High Risk Customers); b. produk Perdagangan Berjangka yang berisiko tinggi untuk digunakan sebagai sarana Pencucian Uang dan/atau Pendanaan Terorisme; c. transaksi dengan pihak yang berasal dari Negara Berisiko Tinggi (High Risk Countries); d. transaksi tidak sesuai dengan profil; e. termasuk dalam kategori PEP; f. bidang usaha calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) termasuk usaha yang berisiko tinggi (High Risk Business); g. negara atau teritori asal, domisili, atau dilakukannya transaksi calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) termasuk Negara Berisiko Tinggi (High Risk Countries); h. tercantumnya calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) dalam daftar terduga teroris dan organisasi teroris; atau i.	yang diberikan oleh calon Nasabah, Nasabah, penerima kuasa, dan/atau Pemilik Manfaat (Beneficial Owner); d. terdapat indikasi Transaksi Keuangan Mencurigakan yang terkait dengan Pencucian Uang dan/atau Pendanaan Terorisme. (2) Pialang Berjangka wajib memastikan bahwa calon Nasabah orang perseorangan bertindak untuk diri sendiri dan bukan untuk kepentingan pihak ketiga atau Pemilik Manfaat (Beneficial Owner). (3) Dalam hal Pialang Berjangka mengetahui calon Nasabah perseorangan bertindak untuk kepentingan pihak ketiga atau Pemilik Manfaat (Beneficial Owner) maka Pialang Berjangka wajib menolak untuk melakukan penerimaan sebagai Nasabah. (3) Dalam hal calon Nasabah Non Orang Perseorangan bertindak untuk kepentingan Pemilik Manfaat (Beneficial Owner) Pialang Berjangka wajib melakukan verifikasi bahwa pihak yang bertindak untuk dan atas nama Pemilik Manfaat (Beneficial Owner) telah mendapatkan otorisasi dari Pemilik Manfaat (Beneficial Owner). Pialang Berjangka wajib melakukan CDD terhadap Pemilik Manfaat (Beneficial Owner). Dalam hal Pemilik Manfaat (Beneficial Owner) sebagaimana dimaksud pada ayat (2) tergolong sebagai PEP maka prosedur yang diterapkan adalah prosedur EDD. Uji Tuntas Nasabah (Customer Due Diligence) yang selanjutnya disingkat CDD adalah kegiatan berupa identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Pialang Berjangka untuk memastikan transaksi sesuai dengan profil, karakteristik, dan/atau pola transaksi calon Nasabah atau Nasabah. Uji Tuntas Lanjut (Enhanced Due Diligence) yang selanjutnya disingkat EDD adalah tindakan CDD lebih mendalam yang dilakukan Pialang Berjangka terhadap calon Nasabah atau Nasabah, yang berisiko tinggi termasuk Politically Exposed Person (PEP) dan/atau dalam area berisiko tinggi. 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 efek yang		

			transaksi yang dilakukan calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) diduga terkait dengan tindak pidana di sektor jasa keuangan, tindak pidana Pencucian Uang, dan/atau tindak pidana Pendanaan Terorisme. Dalam hal calon Nasabah, Nasabah, atau Pemilik Manfaat (Beneficial Owner) adalah anggota keluarga atau pihak yang terkait (close associates) dari PEP maka seluruh ketentuan yang terkait dengan PEP dalam Peraturan Kepala Badan ini berlaku juga terhadap anggota keluarga atau pihak yang terkait (close associates) dari PEP dimaksud. meliputi: a. orang tua kandung/tiri/angkat; b. saudara kandung/tiri/angkat; c. anak kandung/tiri/angkat; d. kakek atau nenek kandung/tiri/angkat; e. cucu kandung/tiri/angkat; f. saudara kandung/tiri/angkat dari orang tua; g. suami atau istri; h. mertua atau besan; i. suami atau istri dari anak kandung/tiri/angkat; j. kakek atau nenek dari suami atau istri; k. suami atau istri dari cucu kandung/tiri/angkat; l. saudara kandung/tiri/angkat dari suami; atau m. istri beserta suami atau istrinya dari saudara, yang bersangkutan. Pihak yang terkait dengan PEP sebagaimana dimaksud pada ayat (1) meliputi: 1. perusahaan yang dimiliki atau dikelola oleh PEP; atau 2. pihak yang secara umum dan diketahui publik mempunyai hubungan dekat dengan PEP. Seperti supir, asisten pribadi, sekretaris pribadi.	ditempatkan pada Pialang Berjangka (ultimately own account), mengendalikan transaksi Nasabah, memberikan kuasa untuk melakukan transaksi, mengendalikan korporasi dan/atau merupakan pengendali akhir dari transaksi yang dilakukan melalui badan hukum. Orang yang Populer Secara Politis (Politically Exposed Person) yang selanjutnya disingkat PEP meliputi: a. PEP Asing yaitu orang yang diberi kewenangan untuk melakukan fungsi penting (prominent function) oleh negara lain (asing) b. PEP Domestik yaitu orang yang diberi kewenangan untuk melakukan fungsi penting (prominent function) oleh negara c. Orang yang diberi kewenangan untuk melakukan fungsi penting (prominent function) oleh organisasi internasional Pialang Berjangka wajib melakukan prosedur CDD pada saat: a. proses penerimaan calon Nasabah menjadi Nasabah Pialang Berjangka; 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 keraguan kebenaran data, informasi, dan/atau dokumen pendukung yang diberikan oleh calon Nasabah, Nasabah, penerima kuasa, dan/atau Pemilik Manfaat (Beneficial Owner); d. terdapat indikasi Transaksi Keuangan Mencurigakan yang terkait dengan Pencucian Uang dan/atau Pendanaan Terorisme. (2) Pialang Berjangka wajib memastikan bahwa calon Nasabah orang perseorangan bertindak untuk diri sendiri dan bukan untuk kepentingan pihak ketiga atau Pemilik Manfaat (Beneficial Owner). (3) Dalam hal Pialang Berjangka mengetahui calon Nasabah perseorangan bertindak untuk kepentingan pihak ketiga atau Pemilik Manfaat (Beneficial Owner) maka Pialang Berjangka wajib menolak untuk melakukan penerimaan sebagai Nasabah. (3) Dalam hal calon Nasabah Non Orang Perseorangan bertindak untuk kepentingan Pemilik Manfaat (Beneficial Owner) Pialang Berjangka wajib melakukan verifikasi bahwa pihak yang bertindak untuk dan atas nama Pemilik Manfaat (Beneficial Owner) telah mendapatkan otorisasi dari Pemilik		

				Manfaat (Beneficial Owner). Pialang Berjangka wajib melakukan CDD terhadap Pemilik Manfaat (Beneficial Owner). Dalam hal Pemilik Manfaat (Beneficial Owner) sebagaimana dimaksud pada ayat (2) tergolong sebagai PEP maka prosedur yang diterapkan adalah prosedur EDD.		

	S : b. Toleransi Risiko	T : c. Pengurangan dan Pengendalian Risiko	U : d. Evaluasi Risiko Residual	V : e. Penerapan Risk Based Approach	W : f. Peninjauan dan Evaluasi RBA	X : Transaction Monitoring
1 : 1. UU 7 -2011_Mata Uang						
2 : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto						
3 : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka						Pedagang Fisik Aset Kripto wajib melakukan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal yang ditetapkan oleh Kepala Bappebti terhadap seluruh Pelanggan Aset Kripto baik pada saat proses penerimaan Pelanggan Aset Kripto, selama menjadi Pelanggan Aset Kripto, pemantauan transaksi, dan melakukan proses pengkinian penilaian risiko Pelanggan Aset Kripto secara berkala. Calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto dilarang memfasilitasi transaksi apabila Pelanggan Aset Kripto tidak memiliki kecukupan dana dan/atau saldo Aset Kripto, termasuk memberikan fasilitas pembiayaan dengan menyediakan dana dan/atau Aset Kripto bagi pelanggannya untuk melakukan transaksi Aset Kripto. Setiap transaksi yang dilakukan oleh Pelanggan Aset Kripto yang difasilitasi oleh Pedagang Fisik Aset Kripto wajib dilakukan verifikasi Verifikasi sebagaimana dimaksud pada ayat (3) dilakukan oleh Lembaga Kliring Berjangka untuk kepentingan penjaminan dan penyelesaian transaksi serta melakukan fungsi DvP (Delivery versus Payment) dengan: a. memastikan kesesuaian dana yang ada pada rekening yang terpisah dengan saldo atau catatan kepemilikan Aset Kripto; b. melakukan pencatatan perpindahan dana dan saldo atau catatan kepemilikan Aset Kripto c. meminta kepada Pedagang Fisik Aset Kripto dan/atau Pengelola Tempat Penyimpanan Aset Kripto untuk mengubah saldo atau catatan atas kepemilikan Aset Kripto yang disimpan di tempat penyimpanan sesuai dengan kondisi yang sebenarnya d. melakukan pendebetan dan pengkreditan rekening keuangan Pelanggan Aset Kripto dan/atau Pedagang Fisik Aset Kripto untuk kepentingan penjaminan dan penyelesaian transaksi

						Penarikan Aset Kripto oleh Pelanggan Aset Kripto dari Pedagang Fisik Aset Kripto hanya dapat dilakukan apabila berdasarkan hasil verifikasi sebagaimana dimaksud dalam Pasal 36 ayat (3) terdapat kesesuaian antara permintaan penarikan Aset Kripto dengan saldo atau catatan kepemilikan Aset Kripto. Dalam memberikan jasa perpindahan atau transfer Aset Kripto, Pedagang Fisik Aset Kripto wajib menerapkan prinsip travel rules sebagai berikut: a. dalam perpindahan atau transfer Aset Kripto lebih dari atau sama dengan nilai dalam Rupiah yang setara dengan USD1.000,00 (seribu dollar amerika), keterangan dan/atau informasi yang diperoleh: 1. pengirim meliputi: a) nama pengirim; b) alamat Wallet pengirim; c) Kartu Tanda Penduduk bagi warga negara Indonesia, atau passport dan kartu identitas yang diterbitkan oleh Negara asal Pelanggan Aset Kripto (KITAP) atau Kartu Izin Tinggal Terbatas (KITAS) bagi warga negara asing; d) alamat pengirim; dan e) tempat dan tanggal lahir pengirim. 2. penerima, dalam hal penerima atau alamat Wallet termasuk cold Wallet atau Wallet diluar Pedagang Fisik Aset Kripto, meliputi: a) nama penerima; b) alamat Wallet penerima; dan c) alamat penerima. b. Dalam perpindahan atau transfer Aset Kripto kurang dari nilai dalam Rupiah yang setara dengan USD1.000,00 (seribu dollar amerika), keterangan dan/atau informasi yang diperoleh: 1. nama pengirim; 2. alamat Wallet pengirim; 3. nama penerima; dan 4. alamat Wallet penerima. Calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto menerapkan prinsip Know Your Transaction (KYT) atas Asset Kripto yang masuk atau yang keluar. Pedagang Fisik Aset Kripto wajib melakukan ketentuan penerapan program anti pencucian uang dan pencegahan pendanaan terorisme serta proliferasi senjata pemusnah massal yang ditetapkan oleh Kepala Bappebti terhadap seluruh Pelanggan Aset Kripto baik pada saat proses penerimaan Pelanggan Aset Kripto, selama menjadi Pelanggan Aset Kripto, pemantauan transaksi, dan melakukan proses pengkinian penilaian risiko Pelanggan Aset Kripto secara berkala.

						Calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto dilarang memfasilitasi transaksi apabila Pelanggan Aset Kripto tidak memiliki kecukupan dana dan/atau saldo Aset Kripto, termasuk memberikan fasilitas pembiayaan dengan menyediakan dana dan/atau Aset Kripto bagi pelanggannya untuk melakukan transaksi Aset Kripto. Setiap transaksi yang dilakukan oleh Pelanggan Aset Kripto yang difasilitasi oleh Pedagang Fisik Aset Kripto wajib dilakukan verifikasi Verifikasi sebagaimana dimaksud pada ayat (3) dilakukan oleh Lembaga Kliring Berjangka untuk kepentingan penjaminan dan penyelesaian transaksi serta melakukan fungsi DvP (Delivery versus Payment) dengan: a. memastikan kesesuaian dana yang ada pada rekening yang terpisah dengan saldo atau catatan kepemilikan Aset Kripto; b. melakukan pencatatan perpindahan dana dan saldo atau catatan kepemilikan Aset Kripto c. meminta kepada Pedagang Fisik Aset Kripto dan/atau Pengelola Tempat Penyimpanan Aset Kripto untuk mengubah saldo atau catatan atas kepemilikan Aset Kripto yang disimpan di tempat penyimpanan sesuai dengan kondisi yang sebenarnya d. melakukan pendebetan dan pengkreditan rekening keuangan Pelanggan Aset Kripto dan/atau Pedagang Fisik Aset Kripto untuk kepentingan penjaminan dan penyelesaian transaksi Penarikan Aset Kripto oleh Pelanggan Aset Kripto dari Pedagang Fisik Aset Kripto hanya dapat dilakukan apabila berdasarkan hasil verifikasi sebagaimana dimaksud dalam Pasal 36 ayat (3) terdapat kesesuaian antara permintaan penarikan Aset Kripto dengan saldo atau catatan kepemilikan Aset Kripto. Dalam memberikan jasa perpindahan atau transfer Aset Kripto, Pedagang Fisik Aset Kripto wajib menerapkan prinsip travel rules sebagai berikut: a. dalam perpindahan atau transfer Aset Kripto lebih dari atau sama dengan nilai dalam Rupiah yang setara dengan USD1.000,00 (seribu dollar amerika), keterangan dan/atau informasi yang diperoleh: 1. pengirim meliputi: a) nama pengirim; b) alamat Wallet pengirim; c) Kartu Tanda Penduduk bagi warga negara Indonesia, atau passport dan

						kartu identitas yang diterbitkan oleh Negara asal Pelanggan Aset Kripto (KITAP) atau Kartu Izin Tinggal Terbatas (KITAS) bagi warga negara asing; d) alamat pengirim; dan e) tempat dan tanggal lahir pengirim. 2. penerima, dalam hal penerima atau alamat Wallet termasuk cold Wallet atau Wallet diluar Pedagang Fisik Aset Kripto, meliputi: a) nama penerima; b) alamat Wallet penerima; dan c) alamat penerima. b. Dalam perpindahan atau transfer Aset Kripto kurang dari nilai dalam Rupiah yang setara dengan USD1.000,00 (seribu dollar amerika), keterangan dan/atau informasi yang diperoleh: 1. nama pengirim; 2. alamat Wallet pengirim; 3. nama penerima; dan 4. alamat Wallet penerima. Calon Pedagang Fisik Aset Kripto atau Pedagang Fisik Aset Kripto menerapkan prinsip Know Your Transaction (KYT) atas Asset Kripto yang masuk atau yang keluar.
4 : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto						
5 : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka						Transaksi Keuangan Mencurigakan adalah transaksi keuangan mencurigakan sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme. Transaksi Keuangan Mencurigakan adalah transaksi keuangan mencurigakan sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme.

6 : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Toleransi risiko merupakan penjabaran dari tingkat risiko yang akan diambil (risk appetite). Toleransi risiko adalah komponen penting dari manajemen risiko yang efektif. konsep toleransi risiko akan membuat Pialang Berjangka mampu untuk menentukan tingkat ancaman terpapar risiko yang dapat ditoleransi oleh Pialang Berjangka Dalam menetapkan toleransi risiko, Pialang Berjangka perlu mempertimbangkan kategori risiko di bawah ini, yaitu: 1) risiko regulator (regulatory risk); 2) risiko reputasi (reputational risk); 3) risiko hukum (legal risk); dan 4) risiko keuangan (financial risk). Toleransi risiko merupakan penjabaran dari tingkat risiko yang akan diambil (risk appetite). Toleransi risiko adalah komponen penting dari manajemen risiko yang efektif. konsep toleransi risiko akan membuat Pialang Berjangka mampu untuk menentukan tingkat ancaman terpapar risiko yang dapat ditoleransi oleh Pialang Berjangka Dalam menetapkan toleransi risiko, Pialang Berjangka perlu mempertimbangkan kategori risiko di bawah ini, yaitu: 1) risiko regulator (regulatory risk); 2) risiko reputasi (reputational risk); 3) risiko hukum (legal risk); dan 4) risiko keuangan (financial risk).	Mitigasi risiko akan membantu kegiatan usaha Pialang Berjangka tetap berada dalam batas toleransi risiko yang telah ditetapkan. Pengendalian internal dan mitigasi risiko yang tinggi didasarkan pada toleransi risiko dan penerimaan risiko (risk appetite). Diharapkan pengendalian internal dan mitigasi risiko akan sepadan dengan risiko yang telah diidentifikasi oleh Pialang Berjangka. Dalam penilaian risiko, semua area berisiko tinggi yang telah diidentifikasi harus dimitigasi dengan pengendalian internal atau langkah lain, serta didokumentasikan dengan baik. Dengan adanya kegiatan mitigasi risiko, diharapkan Pialang Berjangka dapat: 1) melakukan pengkinian dan penatausahaan terhadap informasi Nasabah dan penerima manfaat (beneficial owner); 2) menetapkan dan melaksanakan kegiatan pemantauan berkelanjutan pada setiap tingkatan hubungan usaha Pialang Berjangka (bagi Nasabah berisiko rendah dilakukan secara periodik dan bagi Nasabah berisiko tinggi dilakukan lebih sering); 3) melaksanakan mitigasi terhadap area berisiko tinggi. Strategi mitigasi risiko ini harus tercantum dalam kebijakan dan prosedur; dan 4) menerapkan prosedur pengendalian internal secara konsisten. Pialang Berjangka juga harus dapat menunjukkan kepada Bappebti bahwa langkah mitigasi tersebut telah dilaksanakan secara efektif, misalnya ditunjukkan melalui audit internal. Mitigasi risiko akan membantu kegiatan usaha Pialang Berjangka tetap berada dalam batas toleransi risiko yang telah ditetapkan. Pengendalian internal dan mitigasi risiko yang tinggi didasarkan pada toleransi risiko dan penerimaan risiko (risk appetite). Diharapkan pengendalian internal dan mitigasi risiko akan sepadan dengan risiko yang telah diidentifikasi oleh Pialang Berjangka. Dalam penilaian risiko, semua area berisiko tinggi yang telah diidentifikasi harus dimitigasi dengan pengendalian internal atau langkah lain, serta didokumentasikan dengan baik. Dengan adanya kegiatan mitigasi risiko, diharapkan Pialang Berjangka dapat: 1) melakukan pengkinian dan penatausahaan terhadap informasi	Pialang Berjangka perlu memperhatikan bahwa seketat apapun mitigasi risiko dan manajemen risiko yang dimiliki oleh Pialang Berjangka, Pialang Berjangka tetap memiliki risiko residual yang harus dikelola secara baik. Pialang Berjangka harus memastikan bahwa tingkat risiko residual tidak lebih besar dari tingkat toleransi risiko yang telah ditetapkan Pialang Berjangka. Dalam hal risiko residual masih lebih besar daripada toleransi risiko, atau dalam hal pengendalian internal dan mitigasi terhadap area berisiko tinggi tidak memadai, Pialang Berjangka wajib kembali melakukan langkah pengurangan dan pengendalian risiko sebagaimana dimaksud dalam huruf c dan meningkatkan level atau kuantitas dari langkah mitigasi yang telah ditetapkan. Dengan adanya kegiatan evaluasi terhadap risiko residual, diharapkan Pialang Berjangka: 1) melakukan evaluasi terhadap risiko residual yang dimiliki; dan 2) Pialang Berjangka perlu menyesuaikan tingkat risiko yang dimiliki dengan risiko yang ditoleransi/diterima. Pialang Berjangka perlu memperhatikan bahwa seketat apapun mitigasi risiko dan manajemen risiko yang dimiliki oleh Pialang Berjangka, Pialang Berjangka tetap memiliki risiko residual yang harus dikelola secara baik. Pialang Berjangka harus memastikan bahwa tingkat risiko residual tidak lebih besar dari tingkat toleransi risiko yang telah ditetapkan Pialang Berjangka. Dalam hal risiko residual masih lebih besar daripada toleransi risiko, atau dalam hal pengendalian internal dan mitigasi terhadap area berisiko tinggi tidak memadai, Pialang Berjangka wajib kembali melakukan langkah pengurangan dan pengendalian risiko sebagaimana dimaksud dalam huruf c dan meningkatkan level atau kuantitas dari langkah mitigasi yang telah ditetapkan. Dengan adanya kegiatan evaluasi terhadap risiko residual, diharapkan Pialang Berjangka: 1) melakukan evaluasi terhadap risiko residual yang dimiliki; dan 2) Pialang Berjangka perlu menyesuaikan tingkat risiko yang dimiliki dengan risiko yang ditoleransi/diterima.	Pendekatan berbasis risiko yang dimiliki Pialang Berjangka perlu didokumentasikan dalam bentuk kebijakan dan prosedur untuk menunjukkan tingkat kepatuhan Pialang Berjangka. Kebijakan dan prosedur terkait pendekatan berbasis risiko harus dikomunikasikan, dipahami, dan dipatuhi oleh semua pegawai, khususnya pegawai yang melakukan identifikasi dan penatausahaan data dan informasi Nasabah serta pelaporan transaksi kepada otoritas terkait. Kebijakan dan prosedur terkait pendekatan berbasis risiko harus memenuhi persyaratan minimal sebagai berikut: 1) identifikasi Nasabah; 2) penilaian resiko; 3) tindakan khusus terhadap area berisiko tinggi; 4) penatausahaan; dan 5) pelaporan. Dengan adanya pendekatan berbasis risiko, diharapkan Pialang Berjangka dapat: 1) memastikan bahwa penilaian risiko yang telah dilakukan menggambarkan proses pendekatan berbasis risiko, frekuensi pemantauan Nasabah yang berisiko rendah dan berisiko tinggi, dan juga menggambarkan langkah pengendalian internal yang diberlakukan untuk mengurangi risiko tinggi yang telah diidentifikasi; 2) menerapkan pendekatan berbasis risiko; 3) melakukan pengkinian data dan informasi terhadap Nasabah dan penerima manfaat (beneficial owner); 4) melakukan pemantauan terhadap seluruh hubungan usaha yang dimiliki; 5) melakukan pemantauan yang lebih sering terhadap hubungan usaha yang berisiko tinggi terkait Pencucian Uang dan Pendanaan Terorisme; 6) melakukan langkah tertentu terhadap Nasabah berisiko tinggi; dan/atau 7) melibatkan pejabat senior dalam menghadapi situasi atau area berisiko tinggi (misalnya untuk PEP, pemberian persetujuan melakukan hubungan usaha diberikan oleh pejabat senior). Pendekatan berbasis risiko yang dimiliki Pialang Berjangka perlu didokumentasikan dalam bentuk kebijakan dan prosedur untuk menunjukkan tingkat kepatuhan Pialang Berjangka. Kebijakan dan prosedur terkait pendekatan berbasis risiko harus dikomunikasikan, dipahami, dan dipatuhi oleh semua pegawai, khususnya pegawai yang melakukan identifikasi	Penilaian risiko yang dimiliki oleh Pialang Berjangka harus ditinjau berdasarkan kebutuhan untuk menguji efektivitas dari kepatuhan penerapan program anti Pencucian Uang dan pencegahan Pendanaan Terorisme, yang meliputi: 1) kebijakan dan prosedur; 2) penilaian risiko terkait Pencucian Uang dan Pendanaan Terorisme; dan 3) program pelatihan sumber daya manusia (bagi karyawan dan pejabat senior). Peninjauan atas penilaian risiko terkait Pencucian Uang dan Pendanaan Terorisme harus mencakup seluruh unsur termasuk kebijakan dan prosedur terhadap penilaian risiko, mitigasi risiko dan pemantauan berkelanjutan yang lebih intensif. peninjauan dapat membantu dalam mengevaluasi kebutuhan untuk menyempurnakan kebijakan dan prosedur yang ada, atau untuk pembentukan kebijakan dan prosedur yang baru. Dengan adanya peninjauan pada pendekatan berbasis risiko, diharapkan Pialang Berjangka dapat: 1) melakukan peninjauan sesuai dengan kebutuhan Pialang Berjangka atau dalam hal terdapat perubahan model bisnis, akuisisi portofolio baru dan sebagainya; 2) menghasilkan tinjauan yang mencakup kepatuhan kebijakan dan prosedur, penilaian risiko terhadap Pencucian Uang dan Pendanaan Terorisme, dan program pelatihan untuk menguji efektivitas pendekatan berbasis risiko; 3) melakukan penatausahaan terhadap proses peninjauan dan melaporkan kepada pejabat senior; dan 4) melakukan penatausahaan hasil peninjauan bersama dengan penetapan langkah yang bersifat korektif untuk ditindaklanjuti. Penilaian risiko yang dimiliki oleh Pialang Berjangka harus ditinjau berdasarkan kebutuhan untuk menguji efektivitas dari kepatuhan penerapan program anti Pencucian Uang dan pencegahan Pendanaan Terorisme, yang meliputi: 1) kebijakan dan prosedur; 2) penilaian risiko terkait Pencucian Uang dan Pendanaan Terorisme; dan 3) program pelatihan sumber daya manusia (bagi karyawan dan pejabat senior). Peninjauan atas penilaian risiko terkait Pencucian Uang dan Pendanaan Terorisme harus mencakup seluruh unsur termasuk kebijakan dan prosedur terhadap penilaian risiko, mitigasi risiko	

		Nasabah dan penerima manfaat (beneficial owner); 2) menetapkan dan melaksanakan kegiatan pemantauan berkelanjutan pada setiap tingkatan hubungan usaha Pialang Berjangka (bagi Nasabah berisiko rendah dilakukan secara periodik dan bagi Nasabah berisiko tinggi dilakukan lebih sering); 3) melaksanakan mitigasi terhadap area berisiko tinggi. Strategi mitigasi risiko ini harus tercantum dalam kebijakan dan prosedur; dan 4) menerapkan prosedur pengendalian internal secara konsisten. Pialang Berjangka juga harus dapat menunjukkan kepada Bappebti bahwa langkah mitigasi tersebut telah dilaksanakan secara efektif, misalnya ditunjukkan melalui audit internal.		dan penatausahaan data dan informasi Nasabah serta pelaporan transaksi kepada otoritas terkait. Kebijakan dan prosedur terkait pendekatan berbasis risiko harus memenuhi persyaratan minimal sebagai berikut: 1) identifikasi Nasabah; 2) penilaian resiko; 3) tindakan khusus terhadap area berisiko tinggi; 4) penatausahaan; dan 5) pelaporan. Dengan adanya pendekatan berbasis risiko, diharapkan Pialang Berjangka dapat: 1) memastikan bahwa penilaian risiko yang telah dilakukan menggambarkan proses pendekatan berbasis risiko, frekuensi pemantauan Nasabah yang berisiko rendah dan berisiko tinggi, dan juga menggambarkan langkah pengendalian internal yang diberlakukan untuk mengurangi risiko tinggi yang telah diidentifikasi; 2) menerapkan pendekatan berbasis risiko; 3) melakukan pengkinian data dan informasi terhadap Nasabah dan penerima manfaat (beneficial owner); 4) melakukan pemantauan terhadap seluruh hubungan usaha yang dimiliki; 5) melakukan pemantauan yang lebih sering terhadap hubungan usaha yang berisiko tinggi terkait Pencucian Uang dan Pendanaan Terorisme; 6) melakukan langkah tertentu terhadap Nasabah berisiko tinggi; dan/atau 7) melibatkan pejabat senior dalam menghadapi situasi atau area berisiko tinggi (misalnya untuk PEP, pemberian persetujuan melakukan hubungan usaha diberikan oleh pejabat senior).	dan pemantauan berkelanjutan yang lebih intensif. peninjauan dapat membantu dalam mengevaluasi kebutuhan untuk menyempurnakan kebijakan dan prosedur yang ada, atau untuk pembentukan kebijakan dan prosedur yang baru. Dengan adanya peninjauan pada pendekatan berbasis risiko, diharapkan Pialang Berjangka dapat: 1) melakukan peninjauan sesuai dengan kebutuhan Pialang Berjangka atau dalam hal terdapat perubahan model bisnis, akuisisi portofolio baru dan sebagainya; 2) menghasilkan tinjauan yang mencakup kepatuhan kebijakan dan prosedur, penilaian risiko terhadap Pencucian Uang dan Pendanaan Terorisme, dan program pelatihan untuk menguji efektivitas pendekatan berbasis risiko; 3) melakukan penatausahaan terhadap proses peninjauan dan melaporkan kepada pejabat senior; dan 4) melakukan penatausahaan hasil peninjauan bersama dengan penetapan langkah yang bersifat korektif untuk ditindaklanjuti.	
7 : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka						Transaksi Keuangan Mencurigakan adalah transaksi keuangan mencurigakan sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme Pialang Berjangka wajib menolak transaksi dan/atau menutup hubungan usaha dengan Nasabah dalam hal: b. memiliki sumber dana transaksi yang diketahui dan/atau patut diduga berasal dari hasil tindak pidana; dan/atau c. Nasabah terdapat dalam daftar terduga teroris dan organisasi teroris.

						Dalam hal Pialang Berjangka menduga adanya transaksi keuangan terkait dengan tindak pidana Pencucian Uang dan Pendanaan Terorisme, dan Pialang Berjangka meyakini bahwa proses CDD akan melanggar ketentuan anti tipping-off, Pialang Berjangka wajib tidak melanjutkan prosedur CDD dan wajib melaporkan Transaksi Keuangan Mencurigakan tersebut kepada PPATK. (1) Pialang Berjangka wajib melakukan pemantauan terhadap Nasabah dengan cara meneliti transaksi Nasabah untuk memastikan bahwa transaksi yang dilakukan sejalan dengan pemahaman Pialang Berjangka atas Nasabah, kegiatan usaha dan profil risiko Nasabah, termasuk sumber dananya. (2) Pialang Berjangka wajib melakukan upaya pengkinian data, informasi, dan/atau dokumen pendukung sebagaimana dimaksud dalam Pasal 18, Pasal 21, dan Pasal 26 melalui reviu terhadap profil dan transaksi nasabah yang termasuk dalam tingkat risiko tinggi. (1) Pialang Berjangka wajib melakukan analisis terhadap seluruh transaksi yang tidak sesuai dengan profil Nasabah. (2) Pialang Berjangka dapat meminta informasi tentang latar belakang dan tujuan transaksi terhadap transaksi yang tidak sesuai dengan profil Nasabah Pialang Berjangka wajib melakukan pemantauan yang berkesinambungan terhadap hubungan usaha atau transaksi dengan Nasabah yang berasal dari Negara Berisiko Tinggi (High Risk Countries). Transaksi Keuangan Mencurigakan adalah transaksi keuangan mencurigakan sebagaimana dimaksud dalam Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang dan Undang-Undang yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme Pialang Berjangka wajib menolak transaksi dan/atau menutup hubungan usaha dengan Nasabah dalam hal: b. memiliki sumber dana transaksi yang diketahui dan/atau patut diduga berasal dari hasil

						tindak pidana; dan/atau c. Nasabah terdapat dalam daftar terduga teroris dan organisasi teroris. Dalam hal Pialang Berjangka menduga adanya transaksi keuangan terkait dengan tindak pidana Pencucian Uang dan Pendanaan Terorisme, dan Pialang Berjangka meyakini bahwa proses CDD akan melanggar ketentuan anti tipping-off, Pialang Berjangka wajib tidak melanjutkan prosedur CDD dan wajib melaporkan Transaksi Keuangan Mencurigakan tersebut kepada PPATK. (1) Pialang Berjangka wajib melakukan pemantauan terhadap Nasabah dengan cara meneliti transaksi Nasabah untuk memastikan bahwa transaksi yang dilakukan sejalan dengan pemahaman Pialang Berjangka atas Nasabah, kegiatan usaha dan profil risiko Nasabah, termasuk sumber dananya. (2) Pialang Berjangka wajib melakukan upaya pengkinian data, informasi, dan/atau dokumen pendukung sebagaimana dimaksud dalam Pasal 18, Pasal 21, dan Pasal 26 melalui reviu terhadap profil dan transaksi nasabah yang termasuk dalam tingkat risiko tinggi. (1) Pialang Berjangka wajib melakukan analisis terhadap seluruh transaksi yang tidak sesuai dengan profil Nasabah. (2) Pialang Berjangka dapat meminta informasi tentang latar belakang dan tujuan transaksi terhadap transaksi yang tidak sesuai dengan profil Nasabah Pialang Berjangka wajib melakukan pemantauan yang berkesinambungan terhadap hubungan usaha atau transaksi dengan Nasabah yang berasal dari Negara Berisiko Tinggi (High Risk Countries).

LAMPIRAN 12 *Framework Matrix* Pengawasan dan Pemantauan terhadap Penerapan Anti-Pencucian Uang untuk Aset Kripto di Indonesia

	A : External Monitoring	B : BAPPEBTI (Pelaporan dan Sanksi)	C : PPATK (Pelaporan)
1 : 1. UU 7 -2011_Mata Uang			
2 : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto			
3 : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka			
4 : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto		Pedagang Fisik Aset Kripto wajib melaporkan setiap transaksi Aset Kripto yang mencurigakan kepada Kepala Bappebti dan melaporkan setiap transaksi keuangan yang mencurigakan kepada Kepala Pusat Pelaporan Analisis dan Transaksi Keuangan. Pedagang Fisik Aset Kripto wajib melaporkan setiap transaksi Aset Kripto yang mencurigakan kepada Kepala Bappebti dan melaporkan setiap transaksi keuangan yang mencurigakan kepada Kepala Pusat Pelaporan Analisis dan Transaksi Keuangan.	Pedagang Fisik Aset Kripto wajib melaporkan setiap transaksi Aset Kripto yang mencurigakan kepada Kepala Bappebti dan melaporkan setiap transaksi keuangan yang mencurigakan kepada Kepala Pusat Pelaporan Analisis dan Transaksi Keuangan. Pedagang Fisik Aset Kripto wajib melaporkan setiap transaksi Aset Kripto yang mencurigakan kepada Kepala Bappebti dan melaporkan setiap transaksi keuangan yang mencurigakan kepada Kepala Pusat Pelaporan Analisis dan Transaksi Keuangan.
5 : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Badan Pengawas Perdagangan Berjangka Komoditi yang selanjutnya disebut Bappebti adalah lembaga pemerintah yang tugas pokoknya melakukan pembinaan, pengaturan, pengembangan, dan pengawasan perdagangan berjangka. Pusat Pelaporan dan Analisis Transaksi Keuangan yang selanjutnya disingkat PPATK adalah lembaga independen yang dibentuk dalam rangka mencegah dan memberantas tindak pidana Pencucian Uang sebagaimana dimaksud dalam peraturan perundangudangan yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang. Badan Pengawas Perdagangan Berjangka Komoditi yang selanjutnya disebut Bappebti adalah lembaga pemerintah yang tugas pokoknya melakukan pembinaan, pengaturan, pengembangan, dan pengawasan perdagangan berjangka. Pusat Pelaporan dan Analisis Transaksi Keuangan yang selanjutnya disingkat PPATK adalah lembaga independen yang dibentuk dalam rangka mencegah dan memberantas tindak pidana Pencucian Uang sebagaimana dimaksud dalam peraturan perundangudangan yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang.	Badan Pengawas Perdagangan Berjangka Komoditi yang selanjutnya disebut Bappebti adalah lembaga pemerintah yang tugas pokoknya melakukan pembinaan, pengaturan, pengembangan, dan pengawasan perdagangan berjangka. Badan Pengawas Perdagangan Berjangka Komoditi yang selanjutnya disebut Bappebti adalah lembaga pemerintah yang tugas pokoknya melakukan pembinaan, pengaturan, pengembangan, dan pengawasan perdagangan berjangka.	Pusat Pelaporan dan Analisis Transaksi Keuangan yang selanjutnya disingkat PPATK adalah lembaga independen yang dibentuk dalam rangka mencegah dan memberantas tindak pidana Pencucian Uang sebagaimana dimaksud dalam peraturan perundangudangan yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang. Pusat Pelaporan dan Analisis Transaksi Keuangan yang selanjutnya disingkat PPATK adalah lembaga independen yang dibentuk dalam rangka mencegah dan memberantas tindak pidana Pencucian Uang sebagaimana dimaksud dalam peraturan perundangudangan yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang.
6 : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka			penyusunan pelaporan kepada PPATK dan Bappebti penyusunan pelaporan kepada PPATK dan Bappebti

7 : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka		Setiap pihak yang melakukan pelanggaran ketentuan dalam Peraturan Kepala Badan ini, termasuk pihak yang menyebabkan terjadinya pelanggaran tersebut dikenakan sanksi administratif berupa: a. peringatan tertulis; b. denda yaitu kewajiban untuk membayar sejumlah uang tertentu; c. pembekuan atau pencabutan kegiatan usaha; d. pembekuan atau pencabutan izin; dan/atau e. pembatalan persetujuan. Setiap pihak yang melakukan pelanggaran ketentuan dalam Peraturan Kepala Badan ini, termasuk pihak yang menyebabkan terjadinya pelanggaran tersebut dikenakan sanksi administratif berupa: a. peringatan tertulis; b. denda yaitu kewajiban untuk membayar sejumlah uang tertentu; c. pembekuan atau pencabutan kegiatan usaha; d. pembekuan atau pencabutan izin; dan/atau e. pembatalan persetujuan.	Kewajiban Pelaporan adalah kewajiban pelaporan kepada PPATK sebagaimana diatur dalam peraturan perundang-udangan yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang, dan pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme. Kewajiban Pelaporan adalah kewajiban pelaporan kepada PPATK sebagaimana diatur dalam peraturan perundang-udangan yang mengatur mengenai pencegahan dan pemberantasan tindak pidana Pencucian Uang, dan pencegahan dan pemberantasan tindak pidana Pendanaan Terorisme.

	D : Internal Control	E : a. Pengawasan Aktif Direksi dan Dewan Komisaris	F : b. Kebijakan dan Prosedur	G : c. Pengendalian Internal	H : d. Sistem Informasi Manajemen	I : e. Sumber Daya Manusia dan Pelatihan
1 : 1. UU 7 -2011_Mata Uang						
2 : 2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto						
3 : 3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka						
4 : 4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto						
5 : 5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka						
6 : 5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Penerapan program APU dan PPT berbasis risiko paling sedikit meliputi: a. pengawasan aktif direksi dan dewan komisaris; b. kebijakan dan prosedur; c. pengendalian internal; d. sistem manajemen informasi; dan e. sumber daya manusia dan pelatihan. Penerapan program APU dan PPT berbasis risiko paling sedikit meliputi: a. pengawasan aktif direksi dan dewan komisaris; b. kebijakan dan prosedur; c. pengendalian internal; d. sistem manajemen informasi; dan e. sumber daya manusia dan pelatihan.	A. Pengawasan Aktif Direksi 1. Direksi bertanggung jawab atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme. 2. Direksi memberikan persetujuan yang bersifat teknis atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme yang berkaitan dengan teknis pelaksanaan tugas Direksi. memastikan bahwa kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT dapat diterapkan dalam berbagai situasi terutama responsif terhadap perubahan dan pengembangan produk, jasa dan teknologi di sektor jasa keuangan serta mampu untuk mendeteksi modus Pencucian Uang dan Pendanaan Terorisme. B. Pengawasan Aktif Dewan Komisaris 1. Dewan komisaris bertanggung jawab atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme. 2. Dewan komisaris memberikan	A. Identifikasi dan Verifikasi Calon Nasabah, Nasabah, dan Pemilik Manfaat (beneficial owner) B. Penolakan dan Penutupan Hubungan Usaha A. Identifikasi dan Verifikasi Calon Nasabah, Nasabah, dan Pemilik Manfaat (beneficial owner) B. Penolakan dan Penutupan Hubungan Usaha	Sistem pengendalian internal yang efektif sebagaimana dimaksud dalam Pasal 42 ayat (1) Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8 tahun 2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, harus mampu mendeteksi kelemahan dan penyimpangan dari penerapan program APU dan PPT. Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka harus memiliki kerangka pengendalian internal yang meliputi: a. penunjukan UKK dan/atau pejabat yang bertanggung jawab dalam mengelola penerapan program APU dan PPT; b. pemantauan khusus terhadap kegiatan operasional yang berpotensi berisiko tinggi baik dari Nasabah, produk ataupun wilayah geografis termasuk terhadap hal yang dinilai rentan, dan berpotensi berkaitan dengan transaksi yang mencurigakan	Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka, paling sedikit memiliki kriteria sebagai berikut: a. dapat menyimpan data dan informasi Nasabah yang akurat, lengkap, dan terkini. data dan informasi dimaksud wajib digunakan sebagai salah satu parameter dalam melakukan pemantauan transaksi Nasabah b. dapat menyediakan informasi rincian orang, bidang usaha, dan negara yang memenuhi kriteria area berisiko tinggi dan wajib dilakukan pengkinian secara reguler c. dapat mengidentifikasi transaksi keuangan yang mencurigakan dengan menggunakan parameter yang disesuaikan secara berkala dan memperhatikan kompleksitas usaha, volume transaksi, dan risiko yang dimiliki Pialang Berjangka d. dapat menyediakan laporan secara efektif mengenai karakteristik transaksi yang dilakukan oleh Nasabah	Dalam rangka pencegahan penggunaan Pialang Berjangka sebagai media atau tujuan Pencucian Uang dan Pendanaan Terorisme, Pialang Berjangka harus melakukan: 1. prosedur penyaringan (pre-employee screening) pada saat penerimaan calon karyawan baru sebagai bagian dari penerapan know your employee (KYE) 2. pengenalan dan pemantauan profil karyawan antara lain mencakup perilaku dan gaya hidup karyawan 3. prosedur penyaringan (pre-employee screening), pengenalan dan pemantauan terhadap profil karyawan dituangkan dalam kebijakan know your employee yang berpedoman pada ketentuan yang mengatur mengenai penerapan strategi anti fraud. B. Pelatihan Pialang Berjangka wajib menyelenggarakan pelatihan terkait penerapan program APU dan PPT yang dilakukan secara berkesinambungan sesuai kebutuhan, kompleksitas usaha, dan penilaian risiko Pialang Berjangka

		persetujuan yang bersifat strategis atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme yang berkaitan dengan kebijakan, pengawasan, dan prosedur yang sifatnya signifikan dan mendasar dalam penerapan program APU dan PPT. b. memberikan persetujuan atas kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT yang diusulkan oleh direksi; c. melakukan pengawasan atas pelaksanaan tugas Direksi dalam penerapan program APU dan PPT; d. memastikan struktur organisasi memadai untuk penerapan program APU dan PPT; dan e. mengagendakan pembahasan program penerapan APU dan PPT dalam rapat dewan komisaris dengan direksi. A. Pengawasan Aktif Direksi 1. Direksi bertanggung jawab atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme. 2. Direksi memberikan persetujuan yang bersifat teknis atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme yang berkaitan dengan teknis pelaksanaan tugas Direksi. memastikan bahwa kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT dapat diterapkan dalam berbagai situasi terutama responsif terhadap perubahan dan pengembangan produk, jasa dan teknologi di sektor jasa keuangan serta mampu untuk mendeteksi modus Pencucian Uang dan Pendanaan Terorisme. B. Pengawasan Aktif Dewan Komisaris 1. Dewan komisaris		c. penyampaian informasi yang cepat dan tepat dalam hal terdapat indikasi dan/atau dugaan terkait TPPU dan TPPT, inisiatif kepatuhan, kekurangan terkait kepatuhan, tindakan korektif diambil, dan laporan aktivitas yang mencurigakan d. penerapan kebijakan, prosedur dan kontrol atas uji tuntas Nasabah (CDD e. penyediaan kontrol yang memadai bagi Nasabah, transaksi dan produk yang berisiko tinggi, seperti batasan transaksi atau persetujuan manajemen f. pengujian terhadap keefektifan dari pelaksanaan program APU dan PPT dengan mengambil contoh secara acak (random sampling) dan melakukan pendokumentasian atas pengujian yang dilakukan. Sistem pengendalian internal yang efektif sebagaimana dimaksud dalam Pasal 42 ayat (1) Peraturan Kepala Badan Pengawas Perdagangan Berjangka Komoditi Nomor 8 tahun 2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme pada Pialang Berjangka, harus mampu mendeteksi kelemahan dan penyimpangan dari penerapan program APU dan PPT. Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka harus memiliki kerangka pengendalian internal yang meliputi: a. penunjukan UKK dan/atau pejabat yang bertanggung jawab dalam mengelola penerapan program APU dan PPT; b. pemantauan khusus terhadap kegiatan operasional yang berpotensi berisiko tinggi baik dari	e. dapat memungkinkan Pialang Berjangka untuk menelusuri setiap transaksi (individual transaction), baik untuk keperluan internal dan/atau Bappebti, maupun dalam kaitannya dengan kasus peradilan Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme Pada Pialang Berjangka, paling sedikit memiliki kriteria sebagai berikut: a. dapat menyimpan data dan informasi Nasabah yang akurat, lengkap, dan terkini. data dan informasi dimaksud wajib digunakan sebagai salah satu parameter dalam melakukan pemantauan transaksi Nasabah b. dapat menyediakan informasi rincian orang, bidang usaha, dan negara yang memenuhi kriteria area berisiko tinggi dan wajib dilakukan pengkinian secara reguler c. dapat mengidentifikasi transaksi keuangan yang mencurigakan dengan menggunakan parameter yang disesuaikan secara berkala dan memperhatikan kompleksitas usaha, volume transaksi, dan risiko yang dimiliki Pialang Berjangka d. dapat menyediakan laporan secara efektif mengenai karakteristik transaksi yang dilakukan oleh Nasabah e. dapat memungkinkan Pialang Berjangka untuk menelusuri setiap transaksi (individual transaction), baik untuk keperluan internal dan/atau Bappebti, maupun dalam kaitannya dengan kasus peradilan	Topik pelatihan paling sedikit mengenai: a. implementasi peraturan perundang-undangan yang terkait dengan program APU dan PPT; b. teknik, metode, dan tipologi Pencucian Uang atau Pendanaan Terorisme termasuk tren dan perkembangan profil risiko produk Pialang Berjangka; dan c. kebijakan dan prosedur penerapan program APU dan PPT serta peran dan tanggung jawab pegawai dalam mencegah dan memberantas Pencucian Uang atau Pendanaan Terorisme, termasuk konsekuensi apabila karyawan melakukan tipping off Kedalaman topik pelatihan disesuaikan dengan kebutuhan Pialang Berjangka dan kesesuaian dengan tugas dan tanggung jawab karyawan Dalam rangka pencegahan penggunaan Pialang Berjangka sebagai media atau tujuan Pencucian Uang dan Pendanaan Terorisme, Pialang Berjangka harus melakukan: 1. prosedur penyaringan (pre-employee screening) pada saat penerimaan calon karyawan baru sebagai bagian dari penerapan know your employee (KYE) 2. pengenalan dan pemantauan profil karyawan antara lain mencakup perilaku dan gaya hidup karyawan 3. prosedur penyaringan (pre-employee screening), pengenalan dan pemantauan terhadap profil karyawan dituangkan dalam kebijakan know your employee yang berpedoman pada ketentuan yang mengatur mengenai penerapan strategi anti fraud. B. Pelatihan Pialang Berjangka wajib menyelenggarakan pelatihan terkait penerapan program APU dan PPT yang dilakukan secara berkesinambungan sesuai

		bertanggung jawab atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme. 2. Dewan komisaris memberikan persetujuan yang bersifat strategis atas kebijakan, pengawasan, serta prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme yang berkaitan dengan kebijakan, pengawasan, dan prosedur yang sifatnya signifikan dan mendasar dalam penerapan program APU dan PPT. b. memberikan persetujuan atas kebijakan dan prosedur tertulis mengenai penerapan program APU dan PPT yang diusulkan oleh direksi; c. melakukan pengawasan atas pelaksanaan tugas Direksi dalam penerapan program APU dan PPT; d. memastikan struktur organisasi memadai untuk penerapan program APU dan PPT; dan e. mengagendakan pembahasan program penerapan APU dan PPT dalam rapat dewan komisaris dengan direksi.		Nasabah, produk ataupun wilayah geografis termasuk terhadap hal yang dinilai rentan, dan berpotensi berkaitan dengan transaksi yang mencurigakan c. penyampaian informasi yang cepat dan tepat dalam hal terdapat indikasi dan/atau dugaan terkait TPPU dan TPPT, inisiatif kepatuhan, kekurangan terkait kepatuhan, tindakan korektif diambil, dan laporan aktivitas yang mencurigakan d. penerapan kebijakan, prosedur dan kontrol atas uji tuntas Nasabah (CDD e. penyediaan kontrol yang memadai bagi Nasabah, transaksi dan produk yang berisiko tinggi, seperti batasan transaksi atau persetujuan manajemen f. pengujian terhadap keefektifan dari pelaksanaan program APU dan PPT dengan mengambil contoh secara acak (random sampling) dan melakukan pendokumentasian atas pengujian yang dilakukan.		kebutuhan, kompleksitas usaha, dan penilaian risiko Pialang Berjangka Topik pelatihan paling sedikit mengenai: a. implementasi peraturan perundang-undangan yang terkait dengan program APU dan PPT; b. teknik, metode, dan tipologi Pencucian Uang atau Pendanaan Terorisme termasuk tren dan perkembangan profil risiko produk Pialang Berjangka; dan c. kebijakan dan prosedur penerapan program APU dan PPT serta peran dan tanggung jawab pegawai dalam mencegah dan memberantas Pencucian Uang atau Pendanaan Terorisme, termasuk konsekuensi apabila karyawan melakukan tipping off Kedalaman topik pelatihan disesuaikan dengan kebutuhan Pialang Berjangka dan kesesuaian dengan tugas dan tanggung jawab karyawan
7 : 6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	(1) Pialang Berjangka wajib memiliki kebijakan, pengawasan, dan prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme, yang diusulkan oleh direksi dan disetujui oleh dewan komisaris, agar Pialang Berjangka mampu mengelola dan memitigasi risiko yang telah diidentifikasi. (2) Pialang Berjangka wajib memantau penerapan kebijakan, pengawasan dan prosedur sebagaimana dimaksud pada ayat (1) dan meningkatkan penerapannya jika diperlukan. (3)		Kebijakan dan prosedur penerapan program APU dan PPT sebagaimana dimaksud pada ayat (1) meliputi paling sedikit: a. identifikasi dan verifikasi Nasabah; b. identifikasi dan verifikasi Beneficial Owner; c. penutupan hubungan usaha atau penolakan transaksi; d. pengelolaan risiko Pencucian Uang dan/atau Pendanaan Terorisme yang berkelanjutan terkait dengan Nasabah, negara, produk dan jasa serta jaringan distribusi (delivery channels); e. pemeliharaan data yang akurat terkait dengan transaksi, penatausahaan proses CDD, dan penatausahaan kebijakan dan prosedur;	dilakukannya pemeriksaan secara independen dan berkala untuk memastikan efektivitas penerapan program APU dan PPT. dilakukannya pemeriksaan secara independen dan berkala untuk memastikan efektivitas penerapan program APU dan PPT.	(1) Pialang Berjangka wajib memiliki sistem informasi yang dapat mengidentifikasi, menganalisa, memantau dan menyediakan laporan secara efektif mengenai karakteristik transaksi yang dilakukan oleh Nasabah. (2) Pialang Berjangka wajib memiliki dan memelihara profil Nasabah secara terpadu (single customer identification file) (1) Pialang Berjangka wajib memiliki sistem informasi yang dapat mengidentifikasi, menganalisa, memantau dan menyediakan laporan secara efektif mengenai karakteristik transaksi yang dilakukan oleh Nasabah. (2) Pialang Berjangka wajib	Untuk mencegah digunakannya Pialang Berjangka sebagai media atau tujuan Pencucian Uang dan/atau Pendanaan Terorisme yang melibatkan pihak internal Pialang Berjangka, Pialang Berjangka wajib melakukan: a. prosedur penyaringan untuk penerimaan karyawan baru (pre employee screening); dan b. pengenalan dan pemantauan terhadap profil karyawan. Pialang Berjangka wajib menyelenggarakan pelatihan yang berkesinambungan tentang: a. penerapan ketentuan peraturan perundang-undangan yang terkait dengan program APU dan PPT; b. teknik, metode, dan tipologi Pencucian Uang dan/atau Pendanaan Terorisme; dan

	Pialang Berjangka wajib menetapkan tindakan yang lebih mendalam untuk mengelola dan memitigasi risiko dalam hal risiko yang lebih tinggi teridentifikasi. Penerapan program APU dan PPT sebagaimana dimaksud pada ayat (1) paling sedikit meliputi: a. pengawasan aktif direksi dan dewan komisaris; b. kebijakan dan prosedur; b. pengendalian intern; c. sistem informasi manajemen; dan d. sumber daya manusia dan pelatihan. (1) Pialang Berjangka wajib memiliki kebijakan, pengawasan, dan prosedur pengelolaan dan mitigasi risiko Pencucian Uang dan Pendanaan Terorisme, yang diusulkan oleh direksi dan disetujui oleh dewan komisaris, agar Pialang Berjangka mampu mengelola dan memitigasi risiko yang telah diidentifikasi. (2) Pialang Berjangka wajib memantau penerapan kebijakan, pengawasan dan prosedur sebagaimana dimaksud pada ayat (1) dan meningkatkan penerapannya jika diperlukan. (3) Pialang Berjangka wajib menetapkan tindakan yang lebih mendalam untuk mengelola dan memitigasi risiko dalam hal risiko yang lebih tinggi teridentifikasi. Penerapan program APU dan PPT sebagaimana dimaksud pada ayat (1) paling sedikit meliputi: a. pengawasan aktif direksi dan dewan komisaris; b. kebijakan dan prosedur; b. pengendalian intern; c. sistem informasi manajemen; dan d. sumber daya manusia dan pelatihan.		f. pengkinian dan pemantauan; g. pelaporan kepada pejabat senior, direksi dan dewan komisaris terkait pelaksanaan kebijakan dan prosedur penerapan program APU dan PPT; dan h. pelaporan kepada PPATK. Pialang Berjangka wajib menerapkan kebijakan dan prosedur penerapan program APU dan PPT sebagaimana dimaksud dalam Pasal 12 secara konsisten dan berkesinambungan Kebijakan dan prosedur penerapan program APU dan PPT sebagaimana dimaksud pada ayat (1) meliputi paling sedikit: a. identifikasi dan verifikasi Nasabah; b. identifikasi dan verifikasi Beneficial Owner; c. penutupan hubungan usaha atau penolakan transaksi; d. pengelolaan risiko Pencucian Uang dan/atau Pendanaan Terorisme yang berkelanjutan terkait dengan Nasabah, negara, produk dan jasa serta 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 terkait pelaksanaan kebijakan dan prosedur penerapan program APU dan PPT; dan h. pelaporan kepada PPATK. Pialang Berjangka wajib menerapkan kebijakan dan prosedur penerapan program APU dan PPT sebagaimana dimaksud dalam Pasal 12 secara konsisten dan berkesinambungan		memiliki dan memelihara profil Nasabah secara terpadu (single customer identification file)	c. kebijakan dan prosedur penerapan program APU dan PPT serta peran dan tanggung jawab pegawai dalam mencegah dan memberantas Pencucian Uang dan/atau Pendanaan Terorisme. Untuk mencegah digunakannya Pialang Berjangka sebagai media atau tujuan Pencucian Uang dan/atau Pendanaan Terorisme yang melibatkan pihak internal Pialang Berjangka, Pialang Berjangka wajib melakukan: a. prosedur penyaringan untuk penerimaan karyawan baru (pre employee screening); dan b. pengenalan dan pemantauan terhadap profil karyawan. Pialang Berjangka wajib menyelenggarakan pelatihan yang berkesinambungan tentang: a. penerapan ketentuan peraturan perundang-undangan yang terkait dengan program APU dan PPT; b. teknik, metode, dan tipologi Pencucian Uang dan/atau Pendanaan Terorisme; dan c. kebijakan dan prosedur penerapan program APU dan PPT serta peran dan tanggung jawab pegawai dalam mencegah dan memberantas Pencucian Uang dan/atau Pendanaan Terorisme.

LAMPIRAN 13 *Framework Matrix* Penyebab Pemanfaatan RegTech di Indonesia Inefektif

	A : Penyebab Pemanfaatan RegTech Inefektif	B : Implementasi Regulasi melalui RegTech	C : Implementasi RegTech	D : Akses Data PEP	E : Regulator	F : Akses Terbatas	G : Bersifat Ekslusif	H : Kompetensi SDM
1 : P1							DTTOT di Indonesia akses DTTOT belum banyak yang bisa dapat, nah itu juga satu aksesabilitas perusahaan, gak semua orang dapat akses DTTOT daftar hitam kepolisian Kebanyakan akses ini sifatnya ekslusif	karena banyak FinTech-FinTech yang gak ngerti gitu maksudnya ya "Oh ini saya perlu ya?" "Saya gak ngerti nih, yang saya tahu, saya sudah dapat license, saya bisa jualan" Iya, masih banyak yang "Oh saya dapat lisensi, kira-kira butuh apa?", memang secara regulasi tertulis tapi kan tidak semua orang bisa membaca dan translate apa yang 'saya' lakukan kan? Kecuali ada lawyer atau konsultan yang membaca ini dan "Oke gua baca ini, gua perlu ini", nah ini translation yang masih agak susah. Kadang-kadang mereka gak ngerti kan "Saya butuh apa sih?"
2 : P2					gratis, tapi mereka pilih nih siapa yang akan di-supply data itu			secara garis besar mereka paham sih karena kan ini hanya sistem, dimana memang kita rancangnya sesuai dengan POJK, kewajiban-kewajiban POJK kita terjemahkan ke dalam sistem Yang lebih gak paham mungkin secara teknis "Ini bagaimana ya, Bu?", secara teknis saja. Tapi kalau prosedur "Oh ternyata ini, oh ini buat ini", then mereka sudah bisa sih biasanya. mereka yang memang gak punya background, mereka akan bingung "Ini tuh tools sebenarnya fungsinya buat apa, sih?", then

								nanya berulang-ulang, ya based on pengalaman SIJITU ya, gak luas cakupannya, mereka bingung "Ini tuh tujuannya buat apa sih?", mereka sampai bingung fitur ini tuh buat apa tujuannya. So, gak maksimal mungkin ya pemanfaatannya. Tapi kalau mereka yang punya background, mereka akan bilang "Kalau ini…", misal contoh PEP List, kita bisa deteksi PEP. Nah mereka akan tanya "Kerabatnya akan di-expose gak? Berapa derajat bisa ter-expose kerabat-kerabat dari si PEP?" secara garis besar mereka paham sih karena kan ini hanya sistem, dimana memang kita rancangnya sesuai dengan POJK, kewajiban-kewajiban POJK kita terjemahkan ke dalam sistem Yang lebih gak paham mungkin secara teknis "Ini bagaimana ya, Bu?", secara teknis saja. Tapi kalau prosedur "Oh ternyata ini, oh ini buat ini", then mereka sudah bisa sih biasanya. mereka yang memang gak punya background, mereka akan bingung "Ini tuh tools sebenarnya fungsinya buat apa, sih?", then nanya berulang-ulang, ya based on pengalaman SIJITU ya, gak luas cakupannya, mereka bingung "Ini tuh tujuannya buat apa sih?", mereka sampai bingung fitur ini tuh buat apa tujuannya. So, gak maksimal mungkin ya pemanfaatannya. Tapi kalau mereka yang punya background, mereka akan bilang "Kalau ini…", misal contoh PEP List, kita bisa deteksi PEP. Nah mereka akan tanya "Kerabatnya akan di-expose gak? Berapa derajat bisa ter-expose kerabat-kerabat dari si PEP?"
3 : P3					dari PPATK, itu data dari SIGAP (Sistem Informasi Anti-Pencuain Uang dan Pendanaan Terorisme) dan dia ada PEP data	kalau untuk akses kesana, itu hanya bisa PJK (Penyedia Jasa Keuangan), jadi diluar itu kita tidak bisa akses datanya	malah perusahaan-perusahaan yang bukan RegTech, jadi penyedia jasa IT, justru mereka yang mendapatkan akses. Harusnya kan RegTech yang justru diutamakan justru perusahaan-perusahaan IT ini yang mereka mendapatkan aksesnya ke portal SIGAP, ke PEP Check-nya PPATK gitu. Jadi kita agak bingung aja, kenapa mereka di-approve aksesnya sedangkan kita gak dikasih	biasanya company yang medium to big, mereka mengerti apa yang harus dilakukan dengan prosedurnya mereka masing-masing. Tapi kalau misalnya yang small, kalau dari kami sih melihatnya masih lumayan bingung cara penerapan di perusahaan mereka mereka yang background-nya gak ada specialized di AML tapi punya experience banyak di AML, itu lebih baik juga sih daripada yang hanya punya sertifikasi tapi gak ada experience-nya

								biasanya company yang medium to big, mereka mengerti apa yang harus dilakukan dengan prosedurnya mereka masing-masing. Tapi kalau misalnya yang small, kalau dari kami sih melihatnya masih lumayan bingung cara penerapan di perusahaan mereka mereka yang background-nya gak ada specialized di AML tapi punya experience banyak di AML, itu lebih baik juga sih daripada yang hanya punya sertifikasi tapi gak ada experience-nya

	I : Perbedaan FinTech	J : Big Size	K : Small to Medium Size	L : Risk Appetite & Perception	M : Awareness	N : Finansial	O : Mitigasi Kerusakan Sistem
1 : P1					Tapi ya itu risk appetite-nya perusahaan juga sih balik lagi ke perusahaan apakah mereka mau solusinya atau mau build in house atau manual Tapi ya itu risk appetite-nya perusahaan juga sih balik lagi ke perusahaan apakah mereka mau solusinya atau mau build in house atau manual	Karena untuk meraka untuk pakai RegTech ada satu investasi dan investasi ini biasanya tidak kecil kan. Nah, kalau misalnya kita lihat FinTech yang kecil ya fokusnya growth Karena belum untung. Kadang-kadang gini pemikirannya, saya employed RegTech 200 Juta, bandingkan dengan hiring orang, 10 orang atau 20 orang buat eye bowling-in semua. Ada pertimbangannya masing-masing sih. Saya ambil contoh implementasi RegTech 200 Juta, terus saya hiring 10 orang misalnya, 1 orang 10 Juta per bulan misalnya, nah itu 100 Juta. Sisa 100 Juta-nya saya bisa pakai untuk growth-nya FinTech, perbandingan lagi kan? Ya bisa aja misal kayak contoh pas kemarin sempat ada masalah di satu aktivitas money laundering lah, itu masuk ke pengadilan. Itu FinTech-nya sudah gak boleh beroperasi, karena mereka harus diam dan ngecek semua transaksinya, apakah ada uangnya itu kemana aja. Balik lagi kan, bisnis kalau tutup, kalau gak beroperasi, pengadilan kalau bilang “Oke, anda gak boleh beroperasi 6 bulan”, nah itu, apakah risiko ini sepadan dengan implementasi RegTech kan itu berbeda-beda kan ya. Ada orang yang mungkin oke dengan 6 bulan gak berjalan gak apa-apa Karena untuk meraka untuk pakai RegTech ada satu investasi dan investasi ini biasanya tidak kecil kan. Nah, kalau misalnya kita lihat FinTech yang kecil ya fokusnya growth Karena belum untung. Kadang-kadang gini pemikirannya, saya employed RegTech 200 Juta, bandingkan dengan hiring orang, 10 orang atau 20 orang buat eye bowling-in semua. Ada pertimbangannya masing-masing sih. Saya ambil contoh implementasi RegTech 200 Juta, terus saya hiring 10 orang misalnya, 1 orang 10 Juta per bulan misalnya, nah itu 100 Juta. Sisa 100 Juta-nya saya bisa pakai untuk growth-nya FinTech, perbandingan lagi kan? Ya bisa aja misal kayak contoh pas kemarin sempat ada masalah di satu aktivitas money laundering lah, itu	Jadi balik lagi seberapa risk appetite-nya saya “Apakah saya bisa bertahan last 24 hour punya data atau last hour, 1 jam lalu punya data”. Nah, tentang bagaimana cara penggunaan back up ini kan pasti planning ya “Oke, saya ada back up, ini server mati, nanti ini bisa ada di cloud, di cloud dulu sementara, jadi aplikasi gak kena disrupt, atau mungkin aplikasi kena disrupt 1 jam atau 2 jam. Kalau FinTech-FinTech kecil kan ya pasti gak apa-apa, karena kan mereka ada risiko-risikonya sendiri lah, risk appetite-nya sendiri, gitu. Iya, makannya kalau di luar kan ada regulasi SLA-nya (Service Level Aggrement) untuk FinTech-nya karena kalau misalnya FinTech, kan dia menggunakan uang masyarakat yang masuk ke sistemnya dia, pasti ada perlindungan dong dari pemerintahnya. Nah, seberapa perlindungannya kalau misalnya untuk FinTech dengan ukuran tertentu, maksimal disrupt-nya segini. Jadi balik lagi seberapa risk appetite-nya saya “Apakah saya bisa bertahan last 24 hour punya data atau last hour, 1 jam lalu punya data”. Nah, tentang bagaimana cara penggunaan back up ini kan pasti planning ya “Oke, saya ada back up, ini server mati, nanti ini bisa ada di cloud, di cloud dulu sementara, jadi aplikasi gak kena disrupt, atau mungkin aplikasi kena disrupt 1 jam atau 2 jam. Kalau FinTech-FinTech kecil kan ya pasti gak apa-apa, karena kan mereka ada risiko-risikonya sendiri lah, risk appetite-nya sendiri, gitu. Iya, makannya kalau di luar kan ada regulasi SLA-nya (Service Level Aggrement) untuk FinTech-nya karena kalau misalnya FinTech, kan dia menggunakan uang masyarakat yang masuk ke sistemnya dia, pasti ada perlindungan dong dari pemerintahnya. Nah, seberapa perlindungannya kalau misalnya untuk FinTech dengan ukuran tertentu, maksimal disrupt-nya segini.

							masuk ke pengadilan. Itu FinTech-nya sudah gak boleh beroperasi, karena mereka harus diam dan ngecek semua transaksinya, apakah ada uangnya itu kemana aja. Balik lagi kan, bisnis kalau tutup, kalau gak beroperasi, pengadilan kalau bilang “Oke, anda gak boleh beroperasi 6 bulan”, nah itu, apakah risiko ini sepadan dengan implementasi RegTech kan itu berbeda-beda kan ya. Ada orang yang mungkin oke dengan 6 bulan gak berjalan gak apa-apa	

2 : P2		kalau yang sudah big, mereka ambil semuanya, mereka implementasikan semuanya. Bahkan sampai transaction monitoring mereka butuh, mereka akan implementasi	kalau yang kecil mereka priority based, mana yang diprioritaskan terlebih dahulu? Karena ya namanya masih kecil, anggarannya pasti ada yang lebih diprioritaskan dibandingkan compliance cost. Jadi mereka pilih, maksudnya seperti 'Oh, yang ini dulu nih, yang krusial dulu', mungkin yang risk profiling mereka lakukan manual dulu tidak apa-apa, tidak pakai RegTech misalnya. Terus juga misal yang tadi transaction monitoring mereka lakukan manual, tapi watch list name screening-nya untuk deteksi high risk profile-nya mereka langsung implementasi di awal. Iya, prioritasnya mana dulu		mau atau tidak menyediakan server infrastruktur terbaru untuk stick bareng itu, karena kan enggak di kita yang nyediain, mereka yang menyediakan untuk absorpsi software kita belum ada memang demand dari kriptonya Iya, karena belum ada demand-nya dari mereka. Belum ada kebutuhannya dari mereka. bagi yang mereka merasa ini belum jadi prioritas mereka, mereka itu tidak adain budget compliance-nya di situ gitu, budget compliance-nya itu terlalu kecil biasanya Betul, "Kenapa gak saya marketing aja? Saya kan masih growing. Kenapa saya gak endorse? Kenapa saya gak kolaborasi?" sebelum mereka kena audit random berkala itu, mereka gak pakai sama sekali, mereka hanya kerjasama saja dengan kita, mereka bayar saja tapi pakainya enggak supaya punya lisensinya saja "Oh iya kita pakai SIJITU", tapi ketika ditanya mana buktinya tidak ada gak ada urgensi jadi budget yang ada pasti dialihkan ke yang lain contoh industri, kita ambil salah satu saja ya, misal kripto. Dari sekian banyak, mungkin yang pakai hanya satu atau dua, gitu. Yang sadar hanya satu atau dua dari sekian banyak, rasionya terlalu jomplang hampir 90% gak punya prosedur APU-PPT based on system	Terkadang kendalanya, FinTech itu merasa dananya tidak cukup besar untuk dijadikan sarana pencucian uang. Terkadang kendalanya, FinTech itu merasa dananya tidak cukup besar untuk dijadikan sarana pencucian uang.	
					mau atau tidak menyediakan server infrastruktur terbaru untuk stick bareng itu, karena kan enggak di kita yang nyediain, mereka yang menyediakan untuk absorpsi software kita belum ada memang demand dari kriptonya Iya, karena belum ada demand-nya dari mereka. Belum ada kebutuhannya dari mereka. bagi yang mereka merasa ini belum jadi prioritas mereka, mereka itu tidak adain budget compliance-nya di situ gitu, budget compliance-nya itu terlalu kecil biasanya Betul, "Kenapa gak saya marketing aja? Saya kan masih growing. Kenapa		

					saya gak endorse? Kenapa saya gak kolaborasi?” sebelum mereka kena audit random berkala itu, mereka gak pakai sama sekali, mereka hanya kerjasama saja dengan kita, mereka bayar saja tapi pakainya enggak supaya punya lisensinya saja “Oh iya kita pakai SIJITU”, tapi ketika ditanya mana buktinya tidak ada gak ada urgensi jadi budget yang ada pasti dialihkan ke yang lain contoh industri, kita ambil salah satu saja ya, misal kripto. Dari sekian banyak, mungkin yang pakai hanya satu atau dua, gitu. Yang sadar hanya satu atau dua dari sekian banyak, rasionya terlalu jomplang hampir 90% gak punya prosedur APU-PPT based on system		

3 : P3		big size, itu kebutuhannya juga besar dan lebih luas lagi, contohnya salah satu klien kita itu P2P big player, itu dia pasti volume kebutuhan untuk screening-nya juga jauh lebih besar dibanding small to medium size player. Yang membedakan lebih di volume-nya, sih. Tapi kebutuhan mereka untuk di screening dan profiling-nya itu sama seperti small to medium size.	big size, itu kebutuhannya juga besar dan lebih luas lagi, contohnya salah satu klien kita itu P2P big player, itu dia pasti volume kebutuhan untuk screening-nya juga jauh lebih besar dibanding small to medium size player. Yang membedakan lebih di volume-nya, sih. Tapi kebutuhan mereka untuk di screening dan profiling-nya itu sama seperti small to medium size.		P : Baik, kembali lagi tadi ke sebelumnya. Kan tadi sempat disebutkan, di masa setelah pandemi ini banyak perusahaan yang revenue-nya turun, dan tidak mau implement RegTech karena tidak ada budget-nya. Berarti apakah implementasi RegTech ini selain bergantung dengan awareness-nya FinTech, ini bergantung juga sama budget yang mereka sediakan ya? N2: Iya, betul P : Baik, kembali lagi tadi ke sebelumnya. Kan tadi sempat disebutkan, di masa setelah pandemi ini banyak perusahaan yang revenue-nya turun, dan tidak mau implement RegTech karena tidak ada budget-nya. Berarti apakah implementasi RegTech ini selain bergantung dengan awareness-nya FinTech, ini bergantung juga sama budget yang mereka sediakan ya? N2: Iya, betul	mengeluhkan revenue-nya kurang, gak ada dana untuk beli packages produk AML P : Baik, kembali lagi tadi ke sebelumnya. Kan tadi sempat disebutkan, di masa setelah pandemi ini banyak perusahaan yang revenue-nya turun, dan tidak mau implement RegTech karena tidak ada budget-nya. Berarti apakah implementasi RegTech ini selain bergantung dengan awareness-nya FinTech, ini bergantung juga sama budget yang mereka sediakan ya? N2: Iya, betul mengeluhkan revenue-nya kurang, gak ada dana untuk beli packages produk AML P : Baik, kembali lagi tadi ke sebelumnya. Kan tadi sempat disebutkan, di masa setelah pandemi ini banyak perusahaan yang revenue-nya turun, dan tidak mau implement RegTech karena tidak ada budget-nya. Berarti apakah implementasi RegTech ini selain bergantung dengan awareness-nya FinTech, ini bergantung juga sama budget yang mereka sediakan ya? N2: Iya, betul	

	P : Profil Nasabah	Q : Komunikasi dan Kolaborasi antara Regulator dengan RegTech Provider	R : Pengawasan dan Pemeriksaan	S : Regulasi RegTech	T : Klasifikasi FinTech dan RegTech	U : Penegakkan Regulasi
1 : P1	kebanyakan perusahaan pada berfikir sanction list lah, udah berfikir satu kiblat yang yang besarnya sanction. Tapi kan di Indonesia, lokal, kan ada maintain DTTOT. Nah bisa aja DTTOT ini belum dilaporkan di sanction. Jadi bisa aja saya perusahaan crypto atau non crypto ini on boarding seseorang yang di sanction bersih nih, tapi di DTTOT hitam Balik lagi, risk appetite-nya perusahaan itu. Jadi perusahaan kan sebenarnya dari Tim APU-PPT nya itu kan biasanya ada satu daftar, kayak satu dokumen, ini loh risk appetite-nya saya kalau yang di Indonesia, pengadilan contohnya. Kalau pengadilan belum ada catatan putusan, tetap bisa on boarding karena belum ada kekuatan hukum tetap kan ya, kecuali kalau nanti udah ada kekuatan hukum tetap, baru nanti bisa di off board Mungkin ada perusahaan yang langsung sudah lihat dia masuk pengadilan, sudah off board “saya tidak mau deal dengan nasabah seperti ini”. Mungkin ada perusahaan yang lain tetap keep. Balik lagi mereka ada pertimbangannya masing-masing sih Makannya kalau misalnya kita buka akun perbankan di Singapura, dicek semua, namanya, ini kamu ada blacklist lah, apa, semua, sangatlah ketat banget sih. kebanyakan perusahaan pada berfikir sanction list lah, udah berfikir satu kiblat yang yang besarnya sanction. Tapi kan di Indonesia, lokal, kan ada maintain DTTOT. Nah bisa aja DTTOT ini belum dilaporkan di sanction. Jadi bisa aja saya perusahaan crypto atau non crypto ini on boarding seseorang yang di sanction bersih nih, tapi di DTTOT hitam Balik lagi, risk appetite-nya perusahaan itu. Jadi perusahaan kan sebenarnya dari Tim APU-PPT nya itu kan biasanya ada satu daftar, kayak satu dokumen, ini loh risk appetite-nya saya kalau yang di Indonesia, pengadilan contohnya. Kalau pengadilan belum ada catatan putusan, tetap bisa on boarding karena belum ada kekuatan hukum tetap kan ya, kecuali kalau nanti udah ada kekuatan hukum tetap, baru nanti bisa di off board Mungkin ada perusahaan yang langsung sudah lihat dia masuk pengadilan, sudah off board “saya tidak mau deal dengan nasabah seperti ini”. Mungkin ada perusahaan yang lain tetap keep. Balik lagi mereka ada pertimbangannya masing-masing sih Makannya kalau misalnya kita buka akun perbankan di Singapura, dicek semua,	masih banyak RegTech lainnya yang tidak terdaftar, kenapa? Ya, pertama karena belum ada edukasi lagi dan masuk di situ juga tidak ada benefit yang jelas masih banyak RegTech lainnya yang tidak terdaftar, kenapa? Ya, pertama karena belum ada edukasi lagi dan masuk di situ juga tidak ada benefit yang jelas	mereka banyak fokus yang terkenal saja, yang kecil-kecil masih belum bisa terangkul lah “Apakah pemerintah ini bisa untuk mendeteksi itu atau membuat program untuk mendeteksi itu?” Karena balik lagi, kalau misal yang illegal-illegal ini bisa bekerja dan mereka bisa dapat uang, yang legal ini yang pusing “Lah, user-user saya banyakan milih yang illegal dong?” Kan kalau misalnya saya sebagai user yang on boarder, saya akan dicek against database ini, seberapa valid data ini. Kalau misal data ini tidak valid dan menyebabkan saya off board, siapa yang bertanggung jawab? Nah ini yang jadi masalah karena tidak ada framework-nya. Jadi belum tahu nih kalau misalnya ada apa yang terjadi, siapa yang bertanggung jawab, siapa yang akan memberikan pertanggung jawaban. Karena kan kalau misalnya adopsi, siapa yang bertanggung jawab? Siapa yang menilai? Gak ada yang menilai kan? Kalau misalnya perusahaan gak ada yang menilai, buat apa kita harus implementasi? mereka banyak fokus yang terkenal saja, yang kecil-kecil masih belum bisa terangkul lah “Apakah pemerintah ini bisa untuk mendeteksi itu atau membuat program untuk mendeteksi itu?” Karena balik lagi, kalau misal yang illegal-illegal ini bisa bekerja dan mereka bisa dapat uang, yang legal ini yang pusing “Lah, user-user saya banyakan milih yang illegal dong?” Kan kalau misalnya saya sebagai user yang on boarder, saya akan dicek against database ini, seberapa valid data ini. Kalau misal data ini tidak valid dan menyebabkan saya off board, siapa yang bertanggung jawab? Nah ini yang jadi masalah karena tidak ada framework-nya. Jadi belum tahu nih kalau misalnya ada apa yang terjadi, siapa yang bertanggung jawab, siapa yang akan memberikan pertanggung jawaban. Karena kan kalau misalnya adopsi, siapa yang bertanggung jawab? Siapa yang menilai? Gak ada yang menilai kan? Kalau misalnya perusahaan gak ada yang menilai, buat apa kita harus implementasi?		belum secara terperinci sih karena ini regulation yang dibuat kan untuk mencakup semua, baik yang kecil maupun yang besar. Nah, kecil besarnya FinTech ini kalau di internasional sudah dibedakan secara regulasinya karena kita gak bisa menggunakan satu regulasi untuk ketok rata semua Karena pelaporan untuk perusahaan yang besar ya, sama FinTech yang sekarang nih yang masih bertumbuh atau masih just introduce nih di Indonesia, totally berbeda karena ya yang sudah besar kan mereka sudah punya satu standar sendiri kan ya. Dan kalau yang bertumbuh, ya mereka banyak yang bingung harus gimana. Iya, iya, karena masih belum memadai lah dari regulatornya. secara regulasi untuk RegTech-nya sendiri masih belum Klasifikasinya baru dimulai tahun depan. Di IKD-nya sendiri ya, di pemerintah OJK-nya sendiri, ada klasifikasi khusus buat RegTech-nya, namanya infrastructure enabler. kita beresin dulu lah klasifikasi RegTech, karena kita RegTech tuh belum dapat klasifikasi khususnya di OJK-nya Kan kalau misalnya saya sebagai user yang on boarder, saya akan dicek against database ini, seberapa valid data ini. Kalau misal data ini tidak valid dan menyebabkan saya off board, siapa yang bertanggung jawab? Nah ini yang jadi masalah karena tidak ada framework-nya. Jadi belum tahu nih kalau misalnya ada apa yang terjadi, siapa yang bertanggung jawab, siapa yang akan memberikan pertanggung jawaban. belum secara terperinci sih karena ini regulation yang dibuat kan untuk mencakup semua, baik yang kecil maupun yang besar. Nah, kecil besarnya FinTech ini kalau di internasional sudah dibedakan secara regulasinya karena kita gak bisa menggunakan satu regulasi untuk ketok rata semua Karena pelaporan untuk perusahaan yang besar ya, sama FinTech yang sekarang nih yang masih bertumbuh atau masih just introduce nih di Indonesia, totally berbeda karena ya yang sudah besar kan mereka sudah punya satu standar sendiri kan ya. Dan kalau yang bertumbuh, ya mereka banyak yang bingung harus gimana. Iya, iya, karena masih belum memadai lah dari regulatornya. secara regulasi untuk RegTech-nya sendiri masih belum	Karena untuk meraka untuk pakai RegTech ada satu investasi dan investasi ini biasanya tidak kecil kan. Nah, kalau misalnya kita lihat FinTech yang kecil ya fokusnya growth Karena kan kalau misalnya adopsi, siapa yang bertanggung jawab? Siapa yang menilai? Gak ada yang menilai kan? Kalau misalnya perusahaan gak ada yang menilai, buat apa kita harus implementasi? Karena untuk meraka untuk pakai RegTech ada satu investasi dan investasi ini biasanya tidak kecil kan. Nah, kalau misalnya kita lihat FinTech yang kecil ya fokusnya growth Karena kan kalau misalnya adopsi, siapa yang bertanggung jawab? Siapa yang menilai? Gak ada yang menilai kan? Kalau misalnya perusahaan gak ada yang menilai, buat apa kita harus implementasi?

	namanya, ini kamu ada blacklist lah, apa, semua, sangatlah ketat banget sih.				Klasifikasinya baru dimulai tahun depan. Di IKD-nya sendiri ya, di pemerintah OJK-nya sendiri, ada klasifikasi khusus buat RegTech-nya, namanya infrastructure enabler. kita beresin dulu lah klasifikasi RegTech, karena kita RegTech tuh belum dapat klasifikasi khususnya di OJK-nya Kan kalau misalnya saya sebagai user yang on boarder, saya akan dicek against database ini, seberapa valid data ini. Kalau misal data ini tidak valid dan menyebabkan saya off board, siapa yang bertanggung jawab? Nah ini yang jadi masalah karena tidak ada framework-nya. Jadi belum tahu nih kalau misalnya ada apa yang terjadi, siapa yang bertanggung jawab, siapa yang akan memberikan pertanggung jawaban.		

2 : P2		Pemanfaatan kolaborasi dan komunikasi yang kurang dengan RegTech seperti kita OJK, BI, BAPPEBTI, itu ke kita mungkin komunikasinya masih kurang, ya. Contoh, kita mau, pernah ajak PPATK, contoh, untuk kolaborasi minta data PEP list nasional, itu masih ditolak goAML PPATK, itu juga masih ditolak Iya, betul. Tapi kenapa begitu ada RegTech, kurang gitu pemanfaatannya. kalau keuntungan akses untuk komunikasi ke regulator A, B, C, itu belum kita rasakan di tahap ini Pemanfaatan kolaborasi dan komunikasi yang kurang dengan RegTech seperti kita OJK, BI, BAPPEBTI, itu ke kita mungkin komunikasinya masih kurang, ya. Contoh, kita mau, pernah ajak PPATK, contoh, untuk kolaborasi minta data PEP list nasional, itu masih ditolak goAML PPATK, itu juga masih ditolak Iya, betul. Tapi kenapa begitu ada RegTech, kurang gitu pemanfaatannya. kalau keuntungan akses untuk komunikasi ke regulator A, B, C, itu belum kita rasakan di tahap ini	Selama yang kita tahu itu belum ada yang benar-benar gitu. Waktu di awal, awal-awal 2022 ya kalau saya tidak salah. Memang klien kita pernah kena tegur tuh, kena audit random berkala, audit random itu kena dia dan baru tahu urgensinya. di saat awal tahun itu saja kita mendengar ada audit random. Then sampai sekarang ini kita belum dengar lagi ada kegiatan audit random Selama yang kita tahu itu belum ada yang benar-benar gitu. Waktu di awal, awal-awal 2022 ya kalau saya tidak salah. Memang klien kita pernah kena tegur tuh, kena audit random berkala, audit random itu kena dia dan baru tahu urgensinya. di saat awal tahun itu saja kita mendengar ada audit random. Then sampai sekarang ini kita belum dengar lagi ada kegiatan audit random			tidak tahu di situ ada atau tidak penalty karena yang sangat mempengaruhi implementasi adalah kurang tegasnya penalty atau sanksi dari regulator terhadap FinTech-FinTech player kalau tidak ada penalty, sebenarnya ya betul yang tadi kamu bilang, mereka jadi gak aware untuk memiliki prosedur APU-PPT yang komprehensif, yang layak, yang punya standar Itu setelah mengeluarkan Undang-Undang tapi tindak tegasnya, penalty-nya itu belum ada belum ada audit random-nya dan belum ada sanksi yang jelas bagi yang belum punya prosedur APU-PPT sehingga implikasinya lagi, mereka kurang aware terhadap kebijakan ini, terhadap kewajiban ini Betul, balik lagi ke situ. Kalau perbankan kan sudah jelas, harus punya untuk end-to-end. Kalau kripto, we don't know. bagi yang mereka merasa ini belum jadi prioritas mereka, mereka itu tidak adain budget compliance-nya di situ gitu, budget compliance-nya itu terlalu kecil biasanya karena tidak ada urgensi disana Andaikan diadakan urgensi disana, kita yakin compliance budget masing-masing mereka akan ditambahkan. Balik lagi ke budgeting-nya mereka karena tidak ada urgensi-nya itu Mereka akan menakar lagi, "Urgent gak sih? Kayaknya kalau gak dipakai gak diapa-apain deh" Memang disebutkan, tapi prakteknya gak ada sanksi, gak ada urgensi disana. Gak ada sanksi administratif yang benar-benar paling besar perannya regulasi paling besar pasti regulasi, gak ada urgensi disana Yang selalu kita highlight adalah tadi, urgensinya, kurang tegasnya karena mungkin kita acuannya Singapore kali ya? Let's see, benchmark-nya adalah perusahaan-perusahaan Singapore. Perusahaan-perusahaan Singapore itu yang kecil-kecil aja itu pakai, screening nama, dan lain-lain karena jelas di sana sanksinya apa. Iya, ada urgensinya. urgensinya lagi sih yang masih kurang. Mereka belum sadar bahwa ada RegTech yang memang bisa dimanfaatkan untuk membantu LJK supaya POJK yang mereka buat ini bisa dibuat ada penalty-nya. Mungkin, mereka menilai belum bisa ada penalty-nya karena belum ada wadah, di saat sebenarnya sudah ada wadahnya untuk memenuhi itu

						tidak tahu di situ ada atau tidak penalty karena yang sangat mempengaruhi implementasi adalah kurang tegasnya penalty atau sanksi dari regulator terhadap FinTech-FinTech player kalau tidak ada penalty, sebenarnya ya betul yang tadi kamu bilang, mereka jadi gak aware untuk memiliki prosedur APU-PPT yang komprehensif, yang layak, yang punya standar Itu setelah mengeluarkan Undang-Undang tapi tindak tegasnya, penalty-nya itu belum ada belum ada audit random-nya dan belum ada sanksi yang jelas bagi yang belum punya prosedur APU-PPT sehingga implikasinya lagi, mereka kurang aware terhadap kebijakan ini, terhadap kewajiban ini Betul, balik lagi ke situ. Kalau perbankan kan sudah jelas, harus punya untuk end-to-end. Kalau kripto, we don't know. bagi yang mereka merasa ini belum jadi prioritas mereka, mereka itu tidak adain budget compliance-nya di situ gitu, budget compliance-nya itu terlalu kecil biasanya karena tidak ada urgensi disana Andaikan diadakan urgensi disana, kita yakin compliance budget masing-masing mereka akan ditambahkan. Balik lagi ke budgeting-nya mereka karena tidak ada urgensi-nya itu Mereka akan menakar lagi, "Urgent gak sih? Kayaknya kalau gak dipakai gak diapa-apain deh" Memang disebutkan, tapi prakteknya gak ada sanksi, gak ada urgensi disana. Gak ada sanksi administratif yang benar-benar paling besar perannya regulasi paling besar pasti regulasi, gak ada urgensi disana Yang selalu kita highlight adalah tadi, urgensinya, kurang tegasnya karena mungkin kita acuannya Singapore kali ya? Let's see, benchmark-nya adalah perusahaan-perusahaan Singapore. Perusahaan-perusahaan Singapore itu yang kecil-kecil aja itu pakai, screening nama, dan lain-lain karena jelas di sana sanksinya apa. Iya, ada urgensinya. urgensinya lagi sih yang masih kurang. Mereka belum sadar bahwa ada RegTech yang memang bisa dimanfaatkan untuk membantu LJK supaya POJK yang mereka buat ini bisa dibuat ada penalty-nya. Mungkin, mereka menilai belum bisa ada penalty-nya karena belum ada wadah, di saat sebenarnya sudah ada wadahnya untuk memenuhi itu

3 : P3		Enggak ada, sih. Malah biasanya itu dari regulator, mereka audiensi dulu ke klien-klien kami, baru nanti klien-klien kami contact kami Enggak ada, sih. Malah biasanya itu dari regulator, mereka audiensi dulu ke klien-klien kami, baru nanti klien-klien kami contact kami				Sense of urgency-nya balik lagi regulator, Mbak. Mereka nge-push atau enggak? Kalau gak nge-push ya “Mending saya screening-nya lewat google aja”, gitu kan. gak ditegur juga sama regulatornya kalau peringatan ada, tapi gak ada denda atau sanksi Sense of urgency-nya balik lagi regulator, Mbak. Mereka nge-push atau enggak? Kalau gak nge-push ya “Mending saya screening-nya lewat google aja”, gitu kan. gak ditegur juga sama regulatornya kalau peringatan ada, tapi gak ada denda atau sanksi

	V : Regulasi Pencegahan Crypto-Laundering	W : APU-PPT FinTech	X : Asas Praduga Tak Bersalah	Y : Pembaharuan & Ketersediaan Data	Z : Periodic Checking	AA : Service Level Agreement
1 : P1		Tapi ada risiko-risiko yang harus di-apa ya namanya, harus dicek juga dan mereka aware bahwa ini ada satu masalah serius juga yang harus ditangani. Tapi ada risiko-risiko yang harus di-apa ya namanya, harus dicek juga dan mereka aware bahwa ini ada satu masalah serius juga yang harus ditangani.	Kalau user-nya high risk maka akan dipantau lebih sering, kayak gitu. Nah, dari situ misal putusan sudah keluar atau memang bahkan putusan belum keluar tapi ada aktivitas yang mencurigakan maka bisa di-freeze atau di off board. Kalau dari pemerintah kan yang sudah pasti kalau sudah berkekuatan hukum tetap, sudah gak boleh. Karena kita kalau misalnya melakukan itu, melanggar hukum juga karena kita langsung judges gitu dan dia bisa sue perusahaan itu juga karena belum ada kekuatan hukum tetap tapi sudah di-treat ini, serba salah jadinya Kalau user-nya high risk maka akan dipantau lebih sering, kayak gitu. Nah, dari situ misal putusan sudah keluar atau memang bahkan putusan belum keluar tapi ada aktivitas yang mencurigakan maka bisa di-freeze atau di off board. Kalau dari pemerintah kan yang sudah pasti kalau sudah berkekuatan hukum tetap, sudah gak boleh. Karena kita kalau misalnya melakukan itu, melanggar hukum juga karena kita langsung judges gitu dan dia bisa sue perusahaan itu juga karena belum ada kekuatan hukum tetap tapi sudah di-treat ini, serba salah jadinya		Kadang-kadang perusahaan ada yang 3 bulan, 6 bulan, ada yang 1 tahun. Jadi periode ini sebenarnya tidak ada Undang-Undang nya kalau di Indonesia secara spesifik berapa lama kamu harus periodic checking. Kadang-kadang perusahaan ada yang 3 bulan, 6 bulan, ada yang 1 tahun. Jadi periode ini sebenarnya tidak ada Undang-Undang nya kalau di Indonesia secara spesifik berapa lama kamu harus periodic checking.	Iya, makannya kalau di luar kan ada regulasi SLA-nya (Service Level Aggrement) untuk FinTech-nya karena kalau misalnya FinTech, kan dia menggunakan uang masyarakat yang masuk ke sistemnya dia, pasti ada perlindungan dong dari pemerintahnya. Nah, seberapa perlindungannya kalau misalnya untuk FinTech dengan ukuran tertentu, maksimal disrupt-nya segini. Iya, makannya kalau di luar kan ada regulasi SLA-nya (Service Level Aggrement) untuk FinTech-nya karena kalau misalnya FinTech, kan dia menggunakan uang masyarakat yang masuk ke sistemnya dia, pasti ada perlindungan dong dari pemerintahnya. Nah, seberapa perlindungannya kalau misalnya untuk FinTech dengan ukuran tertentu, maksimal disrupt-nya segini.

2 : P2		yang menyebabkan adalah mereka tidak mempunyai prosedur APU-PPT FinTech ini bisa jadi sarana untuk melakukan pencucian uang dan pendanaan terorisme, TPPU dan TPPT yang menyebabkan adalah mereka tidak mempunyai prosedur APU-PPT FinTech ini bisa jadi sarana untuk melakukan pencucian uang dan pendanaan terorisme, TPPU dan TPPT		Dinamis ya, tergantung ketersediaan data mereka, tergantung update yang tersedia dari mereka. Jadi bisa saja minggu depan ada, bisa saja minggu depan gak ada, bulan depan gak ada, tapi besok langsung ada. Dinamis ya, tergantung ketersediaan data mereka, tergantung update yang tersedia dari mereka. Jadi bisa saja minggu depan ada, bisa saja minggu depan gak ada, bulan depan gak ada, tapi besok langsung ada.		
3 : P3				Kalau meng-cover keseluruhannya sih kami bilang gak cukup kalau hanya pakai DTTOT dan WMD (Weapon of Mass Destruction/Senjata Pemusnah Massal) aja, karena satu, mereka gak ada data anggota keluarga dan kerabat dari high risk profile-nya. Jadi sangat kurang sih kalau hanya dari DTTOT dan WMD. Kalau meng-cover keseluruhannya sih kami bilang gak cukup kalau hanya pakai DTTOT dan WMD (Weapon of Mass Destruction/Senjata Pemusnah Massal) aja, karena satu, mereka gak ada data anggota keluarga dan kerabat dari high risk profile-nya. Jadi sangat kurang sih kalau hanya dari DTTOT dan WMD.		

LAMPIRAN 14 *Framework Matrix* Rekomendasi Perbaikan

	A : Kritik dan Rekomendasi	B : Pemanfaatan RegTech	C : Akses Data PEP oleh RegTech Provider	D : Edukasi Regulator kepada FinTech Crypto	E : Klasifikasi RegTech	F : Kolaborasi Regulator dengan RegTech Provider Lokal
1 : P1					kita beresin dulu lah klasifikasi RegTech, karena kita RegTech tuh belum dapat klasifikasi khususnya di OJK-nya	
2 : P2			Harusnya dapat, kenapa? Karena itu akan membantu sekali PJK untuk menerapkan lebih mudah.			Nah, kenapa gak manfaatin produk 100% lokal dari anak bangsa? Itu tuh dimaksimalkan, diajak kerjasama, diajak kolaborasi, gitu. Pemanfaatannya dimaksimalkan dipermudah nih kolaborasi dengan regulator-regulator dan instansi terkait supaya pemanfaatannya maksimal Harusnya ada, harusnya mereka malah menemani, memediasi
3 : P3				edukasi dari regulatornya juga karena kalau untuk small to medium size FinTech biasanya yang kami temui sih, dari case kami, mereka biasanya kurang paham tentang AML		dukungan dari regulator

	G : Penetapan dan Pemberian Sanksi atau Penalty	H : Pencegahan Crypto-Laundering	I : Prosedur APU-PPT FinTech di Semua Size
1 : P1			
2 : P2	Cukup kasih sanksi yang jelas, sanksi administratif, sanksi yang bahkan sampai yang tegas gitu, kasih yang jelas dan mulai dijalankan sanksi itu supaya dari hal kecil implikasinya ‘parents-nya’ itu harusnya OJK, BI, BAPPEBTI balik lagi ke urgensinya, karena gini, salah satu RegTech yang tercatat di OJK itu kan SIJITU. Nah, kenapa gak manfaatin produk 100% lokal dari anak bangsa? Itu tuh dimaksimalkan, diajak kerjasama, diajak kolaborasi, gitu. Pemanfaatannya dimaksimalkan harus dipertegas ya, sanksinya, lalu juga disebutkan industri-industri yang memang diwajibkan, diperluas lagi, jangan Cuma FinTech aja, mungkin juga e-money, crypto exchanger, dan lain-lain, disebutkan semuanya dan dipertegas sanski administrasinya		menurut kita gak harus prosedurnya kompleks banget. Tapi setidaknya punya di garis besarnya saja Iya, prosedurnya itu punya, screening-nya punya. Ketika di-audit oleh salah satu regulator ‘Mana proses screening-nya?’ itu ada, dilakukan proses KYC, dilakukan screening watch list SIJITU, contoh, screening lewat SIJITU, oke, pass gitu, atau misal ‘Coba dilihat mana pemantauan transaksinya?’, ada juga di history-nya bahwa memang dilakukan pemantauan transaksi. Lalu juga ‘Penilaian risiko berjangkanya coba saya mau lihat history-nya’, contoh misalnya regulator ngomong seperti itu, mereka punya evidence-nya bahwa mereka melakukan prosedur itu. P : Makannya tadi ya, perlunya prosedur APU-PPT di semua size FinTech ya? N1: Betul. selain ada risiko pencucian uang, ada pendanaan terorisme juga yang itu gak mandang size-nya, amount of money-nya
3 : P3			

LAMPIRAN 15 *Framework Matrix* Dampak Potensial

	A : Outcome	B : Awareness FinTech Crypto	C : Mendukung Pemenuhan Kriteria Anggota FATF	D : Optimalisasi Penyerapan Data	E : Penjaminan & Pengelolaan Risiko	F : VDD dan RegTech Terstandarisasi
1 : P1						itu mungkin yang tahun depan yang akan lebih diperjelas "Apakah saya sebagai RegTech mendaftar di situ hanya untuk mendaftar atau ada benefit lain?" Kalau misalnya sudah ada klasifikasinya, baru jelas nih kita masuk ke sini, peraturan regulasi gini, yang kita sebagai Grup RegTech bisa menyuarakan suaranya lewat mana, regulasinya seperti apa, pemanfaatannya seperti apa, nanti kan lebih jelas gitu ada framework-nya. Nah sekarang kan gak ada framework, everyone is ngerjain sendiri-sendiri. Misalnya saya RegTech dari Flagright, ya ada RegTech darimana-mana ya mereka sesuai dengan standar mereka sendiri-sendiri, gak ada kayak satu framework dari pemerintah. Memang secara teknologi kita menggunakan yang sama, transaction monitoring, customer scoring. Tapi kan dengan adanya standar itu, pemerintah jadi lebih bisa nge-manage "Kira-kira kalau saya keluarin regulasi ini, berdampak ke RegTech-nya seperti apa, pemanfaatan berdampak ke FinTech-nya seperti apa?" Makannya di klasifikasi katalog itu bisa melakukan VDD kan? Kalau sekarang, kalau misalnya itu, siapa yang benar dan siapa yang gak benar kan gak jelas.
2 : P2			siapa tahu, kita bisa benar-benar jadi anggota FATF, gitu loh. Pasti kan yang di-assess juga kesiapan LJK-LJK-nya, seperti apa prosedurnya, regulasinya seperti apa	FinTech itu belum punya infrasturktur atau sistem yang memadai untuk absorpt data itu misalnya atau belum ada on boarding yang cukup untuk menyediakan sistem yang bisa menampung data itu atau mengkoneksikan, mengintegrasikan data itu, itu butuh human resource lagi kalau kita dikasih aksesnya akan lebih membantu dan distribusi data itu bisa lebih maksimal karena pasti akan lebih maksimal ya penyerapan datanya	biasanya investor, apalagi investor asing, itu punya concern lebih loh di ranah APU-PPT-nya. Jadi, selain untuk menjaga sisi si Lembaga Jasa Keuangan dari risiko sanksi, ada risiko reputasi juga di situ.	player-palyer dari luar negeri, seperti Singapura, US, dan lain-lain, masuk kesini mungkin standarnya standar internasional padahal yang kita butuh standar nasional Kalau di kita ada standarisasinya, ada workflow-nya. dulu sebelum ada SIJITU, PJK bisa bilang compliance cost itu terlalu mahal, mereka gak punya budget. Tapi kalau SIJITU, yang dia start dari 5 Juta aja, itu sudah tidak ada lagi kata mahal, semua bisa, semua dimungkinkan punya prosedur APU-PPT yang berstandar supaya kita punya standar prosedur APU-PPT yang jelas seperti di Singapura
3 : P3		kalau edukasinya sudah strong, mereka juga pasti jadi merasa urgent, ada urgensinya untuk pakai AML System				

LAMPIRAN 16 Uji Validitas Data Sekunder

File A	File B	Pearson correlation coefficient
Files\\4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	Files\\3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	0,980425
Files\\6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	Files\\5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	0,885940
Files\\6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	Files\\5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	0,686701
Files\\5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	0,657797
Files\\5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	0,634457
Files\\6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	Files\\1. UU 7 -2011_Mata Uang	0,610866
Files\\6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	Files\\3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	0,593354
Files\\5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	0,553226
Files\\6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	Files\\4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	0,550306
Files\\5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\1. UU 7 -2011_Mata Uang	0,526542
Files\\5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\1. UU 7 -2011_Mata Uang	0,509723
Files\\5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	0,497994
Files\\3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	Files\\1. UU 7 -2011_Mata Uang	0,463756
Files\\4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	Files\\1. UU 7 -2011_Mata Uang	0,454321
Files\\5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	0,431412
Files\\5. BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	0,424229
Files\\4. BAPPEBTI 5-2019_Teknis Penyelenggaraan Pasar Fisik Aset Kripto	Files\\2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	0,363303
Files\\2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	Files\\1. UU 7 -2011_Mata Uang	0,353405
Files\\3. BAPPEBTI 8-2021_Pedoman Penyelenggaraan Perdagangan Aset Kripto di Bursa Berjangka	Files\\2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	0,329928
Files\\6. BAPPEBTI 8-2017_Penerapan Program APU PPT pada Pialang Berjangka	Files\\2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	0,272171
Files\\5. Lampiran_BAPPEBTI 11-2017_Program APU PPT pada Pialang Berjangka	Files\\2. PERMENDAG 99-2018_Kebijakan Umum Penyelenggaraan Perdagangan Berjangka Aset Kripto	0,214159

LAMPIRAN 17 Uji Validitas Data Primer

File A	File B	Pearson correlation coefficient
Files\\Interview 2 – P2 & P3_Transcript	Files\\Interview 1 – P1_Transcript	0,864756