PENILAIAN RISIKO SEKTORAL TINDAK PIDANA PENCUCIAN UANG PADA TINDAK PIDANA PENIPUAN SIBER TAHUN 2022

SECTORAL RISK ASSESMENT ON CYBER FRAUD

PENILAIAN RISIKO SEKTORAL TINDAK PIDANA PENCUCIAN UANG PADA TINDAK PIDANA PENIPUAN SIBER TAHUN 2022

SECTORAL RISK ASSESSMENT ON CYBER FRAUD 2022

TIM PENYUSUN

PENILAIAN RISIKO SEKTORAL
TINDAK PIDANA PENCUCIAN UANG
PADA TINDAK PIDANA PENIPUAN SIBER
TAHUN 2022

PENILAIAN RISIKO SEKTORAL TINDAK PIDANA PENCUCIAN UANG PADA TINDAK PIDANA PENIPUAN SIBER TAHUN 2022

Ukuran Buku : 297 x 210 mm

Jumlah Halaman : xv + 72 halaman

Naskah : Tim Penyusun Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang Pada Tindak Pidana Penipuan Siber Tahun 2022

Diterbitkan : Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), 2022

INFORMASI LEBIH LANJUT
Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK)
Indonesian Financial Transaction Reports and Analysis Center (INTRAC)
Jl. Ir. H Juanda No. 35 Jakarta 10120 Indonesia
Phone: (+6221) 3850455, 3853922
Fax: (+6221) 3856809 – 3856826
website: http://www.ppatk.go.id

TIM PENYUSUN
PENILAIAN RISIKO SEKTORAL TINDAK PIDANA PENCUCIAN UANG PADA TINDAK PIDANA PENIPUAN SIBER TAHUN 2022

A. PENGARAH

1. Direktur Tindak Pidana Penipuan Siber, Bareskrim POLRI
2. Direktur Tindak Pidana Ekonomi Khusus, Bareskrim POLRI
3. Direktur Tindak Pidana Ekonomi Umum, Bareskrim POLRI
4. Direktur Tindak Pidana Umum Lain, Kejaksaan Agung RI
5. Direktur Orang dan Harta Benda, Kejaksaan Agung RI
6. Direktur Otoritas Pusat Hukum Internasional, Kementerian Hukum dan HAM RI
7. Kepala Grup Penanganan APU-PPT, Otoritas Jasa Keuangan
8. Kepala Badan Pengawas Perdagangan Berjangka Komoditi
9. Satuan Tugas Waspada Investasi
10. Asisten Deputi Pengawasan Koperasi, Kementerian Koperasi dan UKM RI
11. Direktur Pengendalian Aplikasi Informatika, Kementerian Komunikasi dan Informasi Republik Indonesia
12. Direktur Analisis dan Pemeriksaan I dan II, PPATK
13. Perwakilan Kantor Staf Presiden RI

B. PELAKSANA

1. Direktorat Tindak Pidana Penipuan Siber, Bareskrim POLRI
   - Purnomo Hadi Suseno
   - Atang Setiawan
2. Direktorat Tindak Pidana Ekonomi Khusus, Bareskrim POLRI
   - Budy Hermawan
3. Direktorat Tindak Pidana Umum, Bareskrim POLRI
   - Hady Poerwanto
   - Nurhajiman
4. Direktorat Tindak Pidana Umum Lain, Kejaksaan Agung RI
   - Deddy Sunanda
5. Direktorat Orang dan Harta Benda, Kejaksaan Agung RI
   - Ade Nandar Silitonga
   - Lusiana

6. Direktorat Otoritas Pusat dan Hukum Internasional, Kementerian Hukum dan HAM RI
    - Romano Sitompul
7. Grup Penanganan APU-PPT, Otoritas Jasa Keuangan
    - Nasirullah
    - Adriane Widyaningdita Wiryawan
    - Rifki Arif Budianto
8. Kepala Badan Pengawas Perdagangan Berjangka Komoditi
    - Yovian Andri P
    - Asep Irvan N
9. Satuan Tugas Waspada Investasi
    - Irhamsah
    - Wahid Hakim Siregar
    - Tria Arga Putra Silalahi
    - Sidarta Putra Dharma
10. Asisten Deputi Pengawasan Koperasi, Kementerian Koperasi dan UKM RI
    - Meika Purnamasari
11. Direktur Pengendalian Aplikasi Informatika, Kementerian Komunikasi dan Informasi Republik Indonesia
    - Anthonius Malau
12. Direktur Analisis dan Pemeriksaan I, PPATK
    - Yudi Aditia
    - Ratih Putri Pertiwi
    - Ari Utami
    - Aulia Khoirunnisa
13. Direktur Analisis dan Pemeriksaan II, PPATK
    - Jessie Octavilisia
    - Ahdiani Febrianty
14. Direktorat Kerjasama dan Humas
    - Trinanda Ramadhan
15. Perwakilan Kantor Staf Presiden RI
    - I Nyoman Sastrawan
    - Hadi Prasojo
    - Devi Triasari

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Puji syukur kita panjatkan kepada Allah SWT karena berkat rahmat dan hidayah-Nya, PPATK selaku regulator anti pencucian uang dan pendanaan terorisme di Indonesia, telah selesai menyusun penilaian risiko tindak pidana asal penipuan siber. Pada pelaksanaan ini PPATK bekerja sama dengan berbagai pemangku kepentingan Kementerian/ Lembaga yang terlibat dalam penyusunan penilaian risiko ini. Saya ucapkan terima kasih kepada Pemangku Kepentingan yang telah bekerjasama dengan baik dalam penyusunan penilaian risiko ini, Pemangku Kepentingan dimaksud diantaranya adalah Mahkamah Agung, Kejaksaan Agung, Kepolisan Republik Indonesia, Kementerian Informasi dan Komunikasi, Otoristas Jasa Keuangan, Kementerian Koperasi dan UKM serta Badan Pengawas Perdagangan Berjangka Komoditi.

Tantangan – tantangan yang akan kita hadapi di masa depan akan semakin berat dan potensi kejahatan – kejahatan penipuan siber juga semakin meningkat dan memunculkan berbagai modus dan bentuk-bentuk baru kejahatan pencucian uang dan pendanaan terorisme, oleh karena itu pencegahan dan pemberantasan tindak pidana pencucian uang dan pendanaan terorisme tidak bisa dilakukan oleh PPATK sendiri. Perlu kerja keras bersama menjaga integritas, stabilitas sistem perekonomian, dan sistem keuangan negara. Saya berbangga hati bahwa Kerjasama yang baik ini dpat terwujud dalam penyusunan risiko penipuan siber ini.

Penyusunan risiko penipuan siber merupakan salah satu bukti bahwa, Pemerintah Indonesia memiliki komitmen yang sangat kuat dalam upaya mencegah dan memberantas tindak pidana pencucian uang. Berbagai langkah dalam rangka mengukuhkan komitmen Indonesia telah dilaksanakan secara terintegrasi melalui Startegi Kebijakan Nasional Dalam Upaya Pencegahan dan Pemberantasan TPPU di

Indonesia. Penilaian risiko penipuan siber merupakan bentuk konkret terhadap Implementasi *Financial Action Task Force Recommendations* (FATF Recommendation) No. 1 dalam rangka Indonesia menjadi anggota tetap FATF.

Saya menyambut baik penyusunan penilaian risiko penipuan siber ini karena merupakan hal yang sangat penting bagi seluruh *stakeholders* rezim APU-PPT, dalam rangka mengidentifikasi, menganalisis, dan mengevaluasi berbagai risiko penipuan siber secara domestik dan internasional (*in-ward* dan *out-ward*), meliputi karakteristik penipuan siber, profil, sektor industri, tipologi dan geografis wilayah. Secara khusus, penilaian risiko siber ini bertujuan untuk*:*

1. Untuk mengetahui analisis risiko pencucian uang pada tindak pidana penipuan berdasarkan wilayah terjadinya tindak pidana penipuan analisis tingkat risiko berdasarkan karakteristik tindak pidana, profil pelaku, peranan, modus pelaku, wilayah terjadinya tindak pidana, pemanfaatan sektor industri, pemanfaatan produk/jasa serta negara tempat aliran dana (tujuan, asal maupun transit).
2. Untuk mengetahui tipologi pencucian uang dan studi kasus untuk best pratice kasus – kasus pencucian uang dengan tindak pidana asal penipuan.
3. Untuk mengetahui strategi mitigasi risiko yang dilakukan baik untuk lembaga pengawas dan pengatur, lembaga penegak hukum ataupun pihak pelapor terhadap risiko yang telah terbentuk.

Akhirnya, saya mengucapkan terima kasih dan penghargaan kepada Tim SRA Penipuan Siber PPATK dan seluruh *stakeholders* rezim APUPPT yang tergabung dalam Tim penyusun SRA Penipuan Siber yang telah memberikan kontribusi atas penyusunan dokumen penilaian risiko penipuan siber terhadap tindak pidana pencucian uang tahun 2022. Semoga amal dan kebaikan kita diridhoi Allah SWT. *Amin Ya Rabbal 'Alamin.*

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Jakarta, 5 Juni 2022

Kepala PPATK

Dr. Ivan Yustiavandana

RINGKASAN EKSEKUTIF

Penyusunan penilaian risiko penipuan siber ini, merupakan langkah positif dan relevan untuk menindaklanjuti atas perkembangan dinamika teknologi informasi yang memberikan pengaruh besar dalam kehidupan masyarakat. Kemajuan teknologi informasi dan komunikasi yang terus berkembang pesat saat ini membuat masyarakat semakin mudah dalam memberikan dan menerima informasi. Hal tersebut membuat masyarakat dapat dengan mudah berkomunikasi tanpa ada batas jarak, ruang dan waktu. Seiring dengan perkembangan teknologi tersebut masyarakat juga dituntut untuk mampu mengikuti setiap perkembangan yang sedang terjadi. Perkembangan teknologi saat ini tidak hanya sekedar untuk kepentingan menjalin komunikasi dan bersosialisasi, namun selain itu juga mengarah pada jaringan bisnis dunia tanpa batas. Dari maraknya penggunaan teknologi informasi tersebut ternyata juga menimbulkan penipuan-penipuan yang merugikan para korban. Terlebih transaksi-transaksi penipuan tersebut dilakukan tanpa ada tatap muka antara para pihak dan mereka mendasarkan transaksi tersebut atas rasa kepercayaan satu sama lain. Kerugian akibat penipuan siber ini memiliki nilai yang cukup signifikan, penilaian risiko sektor tindak pidana asal penipuan siber perlu dilakukan dengan harapan bahwa kejahatan penipuan siber akan lebih mudah dicegah dan diberantas.

Penilaian risiko penipuan siber ini disusun berdasarkan kajian atau riset dengan pendekatan kuantitatif dan kualitatif. Pendekatan pertama banyak bersandar pada pengolahan data kuantitatif seperti jumlah frekuensi dan nominal laporan dan putusan. Sementara, pendekatan kedua mengacu pada pandangan dan persepsi pemangku kepentingan penipuan siber di Indonesia. Kajian tersebut dilakukan dengan menggunakan metode yang diadopsi dari panduan FATF dalam melakukan penilaian risiko terhadap tindak pidana pencucian uang dan pendanaan terorisme di berbagai negara–negara di dunia (FATF, 2019). Penilaian yang dilakukan mencakup variabel ancaman (*threat*) dan kerentanan (*vulnerability*) untuk menghasilkan kecenderungan (*likelihood*) kemudian dampak (*consequence*) pada 8 aspek atau disebut *point of concerns*.

Berdasarkan hasil penilaian yang telah dilakukan menggunakan metodologi tersebut diatas adalah :

1. Berdasarkan penilaian jenis/ karakteristik penipuan siber, diketahui bahwa BEC dan *Investment Fraud* merupakan jenis/ karakteristik penipuan siber yang berisiko tinggi.
2. Berdasarkan penilaian profil pelaku perseorangan penipuan siber, diketahui bahwa pegawai swasta dan pengusaha/ wiraswasta merupakan profil pelaku penipuan siber yang berisiko tinggi.
3. Berdasarkan penilaian profil pelaku non perseorangan penipuan siber, diketahui bahwa Perseroan Terbatas (PT) merupakan profil pelaku penipuan siber yang berisiko tinggi.
4. Berdasarkan penilaian peranan pelaku penipuan siber, diketahui bahwa *social engineer* merupakan peranan pelaku penipuan siber yang berisiko tinggi.
5. Berdasarkan penilaian tipologi penipuan siber, yang berisiko tingi adalah:
   - Penggunaan dokumen identitas palsu
   - Pembuatan rekening baru untuk menampung dana hasil kejahatan
   - Penggunaan rekening nominee: milik orang lain (baik yang dikenal/tidak kenal/fiktif)
   - Pola transaksi dengan menggunakan uang tunai (Cash Basis): tarik tunai, setor tunai; yang dilakukan untuk menyamarkan identitas
   - Penggunaan nama Perusahaan atau perorangan untuk menampung pengiriman uang sehingga seolah-olah nampak seperti transaksi bisnis
6. Berdasarkan penilaian wilayah penipuan siber, diketahui bahwa DKI Jakarta dan Jawa Barat merupakan wilayah penipuan siber yang berisiko tinggi.
7. Berdasarkan penilaian kelompok industri yang digunakan dalam penipuan siber, diketahui bahwa bank merupakan sektor industri penipuan siber yang berisiko tinggi.
8. Berdasarkan penilaian produk/jasa yang dimanfaatkan pelaku penipuan siber diketahui yang memiliki risiko tinggi adalah:
   - transfer dana dalam negeri (Online, SKN, RTGS)
   - tabungan
   - transfer dana dari dan ke luar negeri
   - virtual account
   - kartu debit
   - tarik/setor tunai

9. Berdasarkan aliran dana penipuan siber, diketahui bahwa kawasan Asia merupakan kawasan yang berisiko menjadi sumber, transit maupun tujuan akhir dari dana hasil kejahatan penipuan siber.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan Teknologi yang terus berkelanjutan telah menciptakan dunia tanpa batas (*borderless world*). Di satu sisi, perkembangan sistem politik dan ekonomi dunia tidak hanya menghadirkan dampak positif pembangunan ekonomi dan kesejahteraan sosial. Di sisi lain, perkembangan ini memfasilitasi hadirnya praktik-praktik kejahatan keuangan transnasional. Termasuk dalam kejahatan yang 'berkembang' adalah tindak pidana pencucian uang atau dikenal umumnya TPPU di Indonesia.

Indonesia adalah negara berkekuatan ekonomi besar dan potensial di kawasan Asia Pasifik yang berkepentingan besar untuk menjaga keamanan sektor keuangannya. Indonesia terus berkomitmen membangun rezim anti-pencucian uang atau APU. Hal ini terus diupayakan bukan hanya karena komitmennya sebagai anggota observer FATF *(Financial Action Task Force)* yang terus berupaya untuk menjadi anggota tetap, tetapi juga sebagai komitmen kolektif dunia untuk menjaga stabilitas keamanan global dan juga untuk mendorong pertumbuhan ekonomi dunia yang sehat dan berkelanjutan.

Perubahan *landscape* dan perkembangan modus operandi pidana pencucian uang di ini juga disinyalir mengalami perubahan signifikan di masa pandemi Covid-19 saat ini, di mana risiko TPPU juga terus berubah (FATF, 2020). Situasi pandemi yang memaksa masyarakat global untuk membatasi mobilitas manusia dan mengubah pola perilaku ekonomi publik dari yang semula offline menjadi online, terbukti telah mengubah peta risiko praktik pencucian uang di dunia, termasuk juga di Indonesia. Salah satu tindak pidana asal yang terjadi di Indonesia adalah tindak pidana penipuan siber.

Berdasarka data dari PPATK diketahui pula bahwa kejahatan penipuan siber yang merugikan korban cukup meningkat. Hal ini terlihat dari jumlah laporan transaksi keuangan mencurigakan (LTKM) selama kurun waktu 2018 s.d 2021 terdapat 472 LTKM yang dilaporkan oleh pihak pelapor di Indonesia dengan nilai Rp537M. Selain data LTKM tersebut diketahui pula bahwa putusan pengadilan terkait dengan penipuan siber selama periode 2018 hingga 2021 mencapai 29 putusan yang tersebar pada berbagai provinsi dengan nilai kerugian mencapai Rp455M. Hal-hal tersebut dapat mengindikasikan bahwa penipuan siber merupakan suatu tindak pidana yang cukup serius. Hal ini sejalan dengan penilai risiko nasional (NRA) TPPU tahun 2021 yang menyatakan bahwa analisis terhadap faktor ancaman menurut jenis tindak pidana asal diketahui bahwa Informasi

Transaksi Elektronik (ITE) Siber merupakan jenis tindak pidana asal TPPU yang berkategori tinggi di Indonesia. Beberapa contoh kasus penipuan siber yang terjadi di Indonesia yang merugikan para korban antara lain adalah:

a. *Business Email Compromise (BEC)*

Para pelaku mengirimkan email palsu pada tanggal 14 oktober 2020 mms b.v. (mms) menerima email dari c.s@sdbiosensor.co berisi berita informasi proforma infoice (faktur sementara) dan perubahan bank tujuan pembayaran ke rekening bank b nomor rek xxx an.cv.sd inc untuk pembayaran tahap kelima atas pembelian 50.860 paket alat tes rapid dan 70 paket instrument analisa hasil tes covid 19 dengan jumlah tagihan usd 3,065,375. Dimana domain asli email perusahaan adalah "@sdbiosensor.com dan @mediphos.com" bukan .co.

b. *Romance scam*

Pelaku (nama samaran “ba”) berkenalan dengan korban “key” melalui aplikasi skout (aplikasi mobile dating) dan melanjutkan komunikasi melalui aplikasi kakao talk (chatting) dan email. Pelaku “ba” meyakinkan korban “key” hendak mengirimkan uang sebesar usd25.000 dan beberapa hadiah untuk korban. Pelaku “ba” membuat beberapa website palsu, seperti website perusahaan logistik dan website kantor kepabeanan di bandara internasional jakarta, selanjutnya meminta korban “key” untuk membayar biaya kepabeanan. Korban “key” memenuhi permintaan pelaku “ba” dengan melakukan 3 kali transfer senilai total usd5.340 (~krw 6.068.572 atau rp70.771.650) ke rekening an. “ll” di bank sm di indonesia. Terkonfirmasi 3 kali transfer senilai total usd 5.340,00 (setara dengan krw 6.068.572,00 atau rp70.771.650,00) dari korban “key” ke rekening an. “ll” di bank sm di indonesia.

c. *Investment fraud*

Satgas waspada investasi mencatat bahwa total kerugian akibat investasi ilegal dari tahun 2018 hingga 2021 sebesar rp13,8 triliun. Penyebab utama maraknya investasi ilegal di era teknologi informasi saat ini dapat dilihat dari dua sisi, yakni dari sisi pelaku dan masyarakat yang menjadi sasaran para pelaku investasi ilegal.

Berdasarkan informasi – informasi tersebut diatas, maka diketahui bahwa kerugian akibat penipuan siber ini memiliki nilai yang cukup signifikan, sebagaimana diatur pada pasal 2 uu 8 tahun 2010, bahwa penipuan siber yang termasuk tindak pidana penipuan merupakan tindak pidana asal terjadinya

tppu. Ppatk sebagai regulator anti pencucian uang dan pendanaan terorisme, memiliki kewenangan untuk melakukan penilaian risiko sektor tindak pidana asal penipuan siber dengan harapan bahwa kejahatan penipuan siber akan lebih mudah dicegah dan diberantas.

1.2 TUJUAN

Secara umum tujuan dari penilaian risiko sektoral tindak pidana penipuan siber, adalah sebagai berikut:

a. Untuk mengetahui analisis risiko pencucian uang pada tindak pidana penipuan siber berdasarkan karakteristik tindak pidana, profil pelaku, peranan, modus pelaku, wilayah terjadinya tindak pidana, pemanfaatan sektor industri, produk dan/jasa yang digunakan serta negara tempat aliran dana (tujuan, asal maupun transit);
b. untuk mengetahui tipologi pencucian uang dan studi kasus untuk *best practice* kasus – kasus pencucian uang dengan tindak pidana asal penipuan; serta
c. untuk mengetahui strategi mitigasi risiko yang dilakukan baik untuk Lembaga Pengawas dan Pengatur, Lembaga Penegak Hukum ataupun pihak pelapor terhadap risiko yang telah terbentuk.

1.3 OUTPUT

Penilaian risiko sektor penipuan siber pada tahun 2022, diharapkan menghasilkan beberapa output penting bagi penguatan rezim anti pencucian uang di indonesia, diantaranya

a. Skala risiko pencucian uang pada tindak pidana penipuan siber berdasarkan karakteristik tindak pidana, profil pelaku, peranan, modus pelaku, wilayah terjadinya tindak pidana, pemanfaatan sektor industri, produk dan/jasa yang digunakan serta negara tempat aliran dana (tujuan, asal maupun transit);
b. tren tipologi pencucian uang dan studi kasus untuk *best pratice* kasus – kasus pencucian uang dengan tindak pidana asal penipuan siber; serta
c. arah kebijakan strategi mitigasi risiko yang dilakukan baik untuk Lembaga Pengawas dan Pengatur, Lembaga Penegak Hukum ataupun pihak pelapor terhadap risiko yang telah terbentuk.

1.4 RUANG LINGKUP

Data yang digunakan dalam penelitian ini mempunyai tempus waktu dari tahun 2018 – 2021.

BAB II
LANDASAN TEORI

2.1 TINDAK PIDANA PENIPUAN SIBER

Kemajuan teknologi informasi dan komunikasi yang terus berkembang pesat saat ini membuat masyarakat semakin mudah dalam memberikan dan menerima informasi. Hal tersebut membuat masyarakat dapat dengan mudah berkomunikasi tanpa ada batas jarak, ruang dan waktu. Seiring dengan perkembangan teknologi tersebut masyarakat juga dituntut untuk mampu mengikuti setiap perkembangan yang sedang terjadi. Perkembangan teknologi saat ini tidak hanya sekedar untuk kepentingan menjalin komunikasi dan bersosialisasi, namun selain itu juga mengarah pada jaringan bisnis dunia tanpa batas. Jaringan bisnis yang dimaksud adalah kegiatan perdagangan secara on-line melalui internet. Kegiatan perdagangan dengan memanfaatkan media internet ini dikenal dengan istilah *electronic commerce*, atau disingkat *e – commerce* (Ramli, 2004). Sementara *e – commerce* merupakan kegiatan – kegiatan bisnis yang menyangkut konsumen, manufaktur, *service providers*, dan pedagang perantara dengan menggunakan jaringan – jaringan komputer (Suhariyanto, 2012). *e – commerce* juga dapat dipahami sebagai suatu proses jual beli barang dan jasa yang dilakukan melalui jaringan komputer yaitu internet. Pada saat ini tidak dapat dipungkiri bahwa jual beli secara *online* dapat mengefektifkan dan mengefisiensikan waktu sehingga seseorang dapat melakukan transaksi jual beli dengan setiap orang dimanapun dan kapanpun. Terlebih transaksi tersebut dilakukan tanpa ada tatap muka antara para pihak dan mereka mendasarkan transaksi jual beli tersebut atas rasa kepercayaan satu sama lain sehingga jual beli yang terjadi diantara para pihak pun dilakukan secara elektronik (*online*) melalui jaringan internet.

Tindak pidana penipuan siber merupakan tindak pidana yang relatif baru, yang secara umum dilakukan oleh orang-orang yang ahli atau yang memiliki keahlian di bidang komputer dan teknologi informasi (Ersya, 2017) . Jika dilihat dari segi akibat kejahatan, maka kejahatan melalui dunia maya (internet) dapat berdampak di dalam maupun di luar dunia maya. Tidak terbatasnya ruang dan waktu dalam melakukan aktivitas dengan menggunakan internet sebagai media, menyebabkan sulitnya suatu aktivitas dalam dunia maya dideteksi secara konvensional. Sementara jika hal tersebut dilakukan dengan menggunakan sarana siber, maka kejahatan komputer dan siber dapat berbentuk sebagai berikut (Soepraptomo, 2000):

1. Penipuan berbasis aplikasi dengan penggunaaan komputer (*computer fraud*) yang mencakup:
   a. Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan menggunakan sarana komputer/siber dengan melawan hukum, yaitu dalam bentuk penipuan data dan penipuan program, yang terinci adalah:
      - Memasukkan instruksi yang tidak sah, ialah dilakukan oleh seseorang yang berwenang atau tidak, yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (misalnya transfer).
      - Mengubah data input, yang dilakukan seseorang dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum (misalnya memasukkan data gaji pegawai melebihi yang seharusnya).
      - Merusak data, ialah dilakukan seseorang untuk merusak print-out atau output dengan maksud untuk mengaburkan, menyembunyikan data atau informasi dengan itikad tidak baik.
      - Penggunaan komputer untuk sarana melakukan perbuatan pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnyadigunakan untuk melakukan kejahatan atau mengubah program.
   b. Perbuatan pidana penipuan, yang sesungguhnya dapat termasuk unsur perbuatan lain, yang pada pokoknya dimaksudkan menghindarkan diri dari kewajiban (misalnya wajib pajak) atau untuk memperoleh sesuatu yang bukan hak/miliknya melalui sarana komputer.
   c. Perbuatan curang untuk memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang yang dapat mengakses computer menstranfer rekening orang ke rekeningnya sendiri, sehingga merugikan orang lain.
   d. Konspirasi penipuan, ialah perbuatan pidana yang dilakukan beberapa orang secara bersama-sama untuk melakukan penipuan dengan sarana komputer.
   e. Pencurian ialah dengan sengaja mengambil dengan melawan hukum hak atau milik orang lain dengan maksud untuk dimilikinya sendiri.

2. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri.
3. Hacking, ialah melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan komputer yang dapat mengancam berbagai kepentingan.
4. Permutant pidana komunikasi, ialah hacking yang dapat membobol sistem online komputer menggunakan sistem komunikasi.
5. Perbuatan pidana perusakan sistem komputer, baik merusak data ataumenghapus kode-kode yang menimbulkan kerusakan dan kerugian.termasuk dalam perbuatan ini penambahan atau perubahan program, informasi, media, sehingga merusak sistem, demikian pula sengaja menyebarkan virus yang dapat merusak program dan sistem komputer, atau pemerasan dengan menggunakan sarana komputer/telekomunikasi.
6. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta, dan hak paten, ialah berupa pembajakan dengan memproduksi barang-barang tiruan untuk mendapatkan keuntungan melalui perdagangan.

Sementara itu Asril Sitompul (2001: 91-92) lebih memberikan penggolongan dengan bentuk yang lebih sederhana dalam bentuk-bentuk tindak pidana siber ini, menurutnya kejahatan komputer yang dilakukan lewat internet yang dapat diidentifikasi terdiri dari beberapa golongan, diantaranya:

1. Kejahatan yang berkaitan dengan data, seperti pemutusan transfer data.
2. Kejahatan yang berhubungan dengan jaringan (network), seperti penyadapan dan sabotase.
3. Kejahatan yang berkaitan dengan akses ke internet seperti hacking dan penyebaran virus.
4. Kejahatan yang berkaitan dengan komputer seperti membantu kejahatan di cyberspace, pemalsuan data lewat komputer untuk mencari keuntungan, dan pemalsuan data lewat komputer untuk digunakan sebagai data asli.
5. Kejahatan yang berhubungan dengan pasar modal.
6. Pornografi, penghinaan, pencemaran nama baik dan tindakan melawan hukum lainnya.

Selanjutnya dari pihak Interpol menyatakan bahwa penipuan siber dapat terdiri dari:

1. *Phishing, Vishing and SMShing*
   Email palsu/pesan teks/panggilan telepon yang mengaku berasal dari sumber yang sah seperti bank atau situs e-commerce digunakan untuk membujuk individu agar mengungkapkan informasi pribadi atau keuangan
2. *Telecom fraud*
   Korban acak dihubungi oleh penjahat yang mengaku sebagai teman, kerabat, atau seseorang yang berwenang dan ditipu untuk berpisah dengan pengiriman uang
3. *Business Email Compromise*
   Penjahat meretas sistem email untuk mendapatkan informasi tentang sistem pembayaran perusahaan, kemudian menipu karyawan perusahaan untuk mentransfer uang ke rekening bank mereka.
4. *Romance scams*
   Penjahat mengembangkan "hubungan" dengan korban melalui media sosial dengan tujuan akhir mendapatkan uang.
5. *Investment Fraud*
   Korban ditekan untuk berinvestasi dalam saham palsu atau tidak berharga, atau investasi lainnya yang sebenarnya tidak ada kegiatan investasi.

Penipuan siber sebagaimana disebutkan diatas, dilakukan secara elektronik merupakan tindak pidana sebagaimana diatur pada Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang – Undang Nomor 3 Tahun 2011 Tentang Transfer Dana. Tindak pidana dengan sanksi hukum terkait dengan penipuan siber adalah sebagai berikut:

Tabel 2.1 Tindak Pidana dengan Sanksi Hukum terkait Penipuan Siber

No	Delik Pidana	Perbuatan Kejahatan Transaksi Elektronik/ Siber
1	Pasal 30 Ayat (2) pada Undang – Undang Nomor 19 Tahun 2016	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi

No	Delik Pidana	Perbuatan Kejahatan Transaksi Elektronik/ Siber
	tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008	Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)
2	Pasal 32 Ayat (2) pada Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak
3	Pasal 35 pada Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008	Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)
4	Pasal 45 ayat (4) pada Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang –	Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan dan/ataupengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara

No	Delik Pidana	Perbuatan Kejahatan Transaksi Elektronik/ Siber
	Undang Nomor 11 Tahun 2008	paling lama 6 (enam) tahun dan/atau denda paling banyakRp1.000.000,00 (satu miliar rupiah).
5	Pasal 45A ayat (1) pada Undang – Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang – Undang Nomor 11 Tahun 2008	Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
6	Pasal 81 pada Undang – Undang RI Nomor 3 Tahun 2011	Setiap orang yang secara melawan hukum mengambil atau memindahkan sebagian atau seluruh Dana milik orang lain melalui Perintah Transfer Dana palsu dipidana dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)
7	Pasal 82 pada Undang – Undang RI Nomor 3 Tahun 2011	Penerima yang dengan sengaja menerima atau menampung, baik untuk diri sendiri maupun untuk orang lain, suatu Dana yang diketahui atau patut diduga berasal dari Perintah Transfer Dana yang dibuat secara melawan hukum dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)
8	Pasal 85 pada Undang – Undang RI Nomor 3 Tahun 2011	Setiap orang yang dengan sengaja menguasai dan mengakui sebagai miliknya Dana hasil transfer yang diketahui atau patut diketahui bukan haknya dipidana dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)

2.1 TINDAK PIDANA PENCUCIAN UANG PADA TINDAK PIDANA PENIPUAN SIBER

Tindak pidana penipuan siber merupakan pelanggaran terhadap hak-hak sosial dan hak-hak ekonomi masyarakat korban penipuan, sehingga tindak pidana penipuan siber tidak dapat lagi digolongkan sebagai kejahatan biasa melainkan telah menjadi kejahatan luar biasa. Selain mengambil hak-hak sosial dan ekonomi yang sudah pasti sangat merugikan korban penipuan, aparat penegak hukum juga sangat disulitkan dalam hal melacak hasil penipuan siber tersebut, sebab seringkali pencucian uang dilakukan dengan cara memasukkan hasil kejahatannya tersebut ke dalam sistem keuangan dan juga sudah ditransfer ke luar negeri yang sulit dilakukan pelacakan.

Kejahatan pencucian uang (*money laundering*) belakangan ini semakin mendapat perhatian khusus dari berbagai kalangan. Upaya penanganannya dilakukan secara nasional, regional, dan global melalui kerja sama antar-negara. Tindak pidana pencucian uang termasuk bentuk tindak pidana khusus yang memiliki hubungan dengan berbagai macam kejahatan. Tindak pidana pencucian uang diangap sebagai kejahatan lanjutan, yaitu sebagai upaya pelaku untuk menyamarkan hasil dari suatu kejahatan yang telah dilakukan sebelumnya agar dapat menikmati hasil tersebut tanpa terlacak, termasuk salah satunya yaitu dari hasil dari penipuan siber. Hal tersebut dapat dilihat dalam Pasal 2 ayat (1) Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Undang-Undang TPPU memberikan kewenangan bagi para penegak hukum, untuk melakukan penyidikan TPPU terhadap kasus-kasus penipuan siber yang didalamnya terdapat unsur-unsur TPPU yang dilakukan oleh para penipu sehingga upaya pencegahan dan pemberantasan TPPU dapat dilakukan dengan mengedepankan *asset recovery* atau pengembalian uang dan asset hasil dari tindak pidana penipuan siber. Berkenaan dengan penggunaan UU TPPU, terdapat empat keuntungan ketika penegak hukum menggabungkan pasal TPPU dengan tindak pidana penipuan siber, yaitu:

1. Penggabungan kedua pasal akan menjerat banyak aktor atau pelaku tindak pidana. Undang-Undang TPPU memungkinkan penegak hukum menjerat korporasi, pengendalinya, serta orang-orang yang turut mempengaruhi kebijakan korporasi.
2. Ancaman hukuman lebih maksimal, baik itu pidana penjara maupun denda.

3. Penggabungan ini juga efektif dalam pengembalian aset negara. Aset dalam bentuk apa pun, bisa disita oleh penegak hukum. Sistem pembuktian terbalik secara keperdataan yang telah dipraktikkan di beberapa negara, seperti Amerika, Inggris, dan beberapa negara Eropa lainnya dapat dijadikan rujukan pemberlakuan pembuktian terbalik dalam pengembalian aset kejahatan korupsi di Indonesia. Dalam hal pembuktian terbalik absolut, terdakwa diembani kewajiban untuk membuktikan bahwa harta yang dimiliki bukan berasal dari kejahatan dianut dalam UU TPPU.

BAB III
METODOLOGI PENELITIAN

Penilaian risiko penipuan siber ini disusun berdasarkan kajian atau riset dengan pendekatan kuantitatif dan kualitatif. Pendekatan pertama banyak bersandar pada pengolahan data kuantitatif seperti jumlah frekuensi dan nominal laporan dan putusan. Sementara, pendekatan kedua mengacu pada pandangan dan persepsi pemangku kepentingan penipuan siber di Indonesia. Kajian tersebut dilakukan dengan menggunakan metode yang diadopsi dari panduan FATF dalam melakukan penilaian risiko terhadap tindak pidana pencucian uang dan pendanaan terorisme di berbagai negara–negara di dunia (FATF, 2019). Penilaian yang dilakukan mencakup variabel ancaman (*threat*) dan kerentanan (*vulnerability*) untuk menghasilkan kecenderungan (*likelihood*) kemudian dampak (*consequence*) pada lima aspek atau disebut *point of concerns*. Pembahasan lebih detail dari metode tersebut adalah sebagai berikut.

3.1 DEFINISI VARIABEL

Penelitian guna penyusunan penipuan siber ini dilakukan untuk memotret pengetahuan dan pengalaman yang otentik dari berbagai elemen rezim Anti-Pencucian Uang (APU) seperti Pihak Pelapor (PP), Lembaga Pengawas dan Pengatur (LPP), Aparat Penegak Hukum (APH), di Indonesia. Penilaian risiko penipuan siber ini pada dasarnya dilakukan dengan berbasis metode analisis yang telah diadopsi dari praktik terbaik di dunia internasional. Metodologi yang digunakan dalam penyususnan risiko penipuan siber ini didasarkan pada panduan IMF (IMF, 2011), World Bank, dan FATF (FATF, 2013, 2019), yang menekankan pada proses untuk melakukan penilaian risiko di tingkat nasional. Beberapa variabel utama dari kajian dalam penyusunan penilaian risiko siber ini adalah sebagai berikut.

1. Ancaman

   Ancaman mengacu pada tindak pidana penipuan siber yang terkait dengan pencucian uang. Hal tersebut menunjukan suatu tindak pidana penipuan siber dilakukan dan hasil kejahatan yang dihasilkan relevan untuk memahami dalam beberapa kasus pada tindak pidana asal dengan dikaitkan metode pencucian uang jenis, profil pelaku kejahatan, wilayah terjadinya tindak kejahatan, dan metode penipuan siber.

2. Kerentanan

   Aspek kerentanan adalah faktor-faktor yang memfasilitasi atau menciptakan peluang untuk terjadinya penipuan siber. Kerentanan ini erat terkait dengan kelemahan sistem, regulasi, dan sumber daya manusia dari sektor industri, pengawasan dan pengaturan, serta penegakan pencegahan dan pemberantasan penipuan siber.

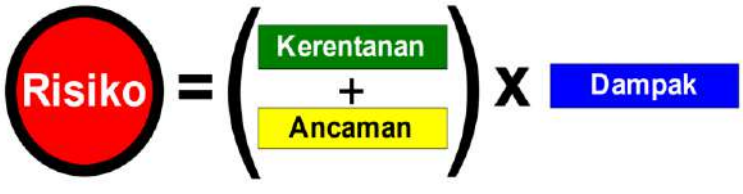
3. Dampak

   Aspek dampak adalah suatu akibat atau kerugian yang ditimbulkan dari tindak pidana pencucian uang terhadap lembaga, ekonomi dan sosial secara lebih luas termasuk juga kerugiab dari tindak kriminal itu sendiri.

4. Risiko

   Risiko dalam hal ini adalah fungsi dari ancaman, kerentanan, dan dampak. Pada tingkat nasional, risiko ini merupakan kecenderungan atau kemungkinan (ancaman dan kerentanan) kejadian penipuan siber yang memberikan dampak dan membahayakan integritas sistem keuangan nasional serta keselamatan dan keamanan nasional.

Dalam panduan dari International Monetary Fund (IMF), dijelaskan bahwa risiko merupakan formula yang dapat digambarkan dengan fungsi algoritma R= f[(T), (V)] x C. Dalam formula tersebut, R merepresentasikan risiko, T adalah ancaman, V ialah kerentanan, and C adalah dampak. Formulasi untuk melakukan penilaian risiko penipuan siber tersebut dapat dirumuskan sebagaimana gambar berikut:



Gambar 3.1 Formula Pemetaan Risiko berdasarkan IMF

3.2 TAHAPAN PENYUSUNAN SRA PENIPUAN SIBER

Jika dibedah, berikut adalah tiga tahapan utama dalam proses penyusunan SRA ini. Tahapan – tahapan ini telah dilakukan oleh berbagai negara dan juga telah berbasis pedoman yang telah dibuat oleh FATF. Tahap – tahap tersebut meliputi identifikasi, analisis dan evaluasi yang dijelaskan sebagai berikut.

3.2.1 Tahap pertama: Identifikasi

Tahapan identifikasi ini bertujuan untuk mendapatkan gambaran terkait sifat dan *volume* dari tiga variabel utama, yakni ancaman, kerentanan, dan dampak, yang mempengaruhi tingkat risiko penipuan siber di Indonesia. Dalam penyusuan SRA ini, disepakati bahwa perlu diidentifikasi 8 (delapan) aspek (PoC/ *point of concern*) dan yang perlu dinilai tingkat risikonya, yaitu bentuk/jenis tindak pidana penipuan siber, profil pelaku perseorangan, profil pelaku non perseorangan, peranan pelaku, tipologi, wilayah, kelompok industri dan Kawasan aliran dana.

Dalam rangka melakukan penilaian risiko terhadap penipuan siber berdasarkan tindak pidana asal, maka dirumuskan faktor-faktor pembentuk risikonya sebagaimana berikut.

Tabel 3.1 Faktor-Faktor Pembentuk Risiko TPA

Ancaman	Kerentanan	Dampak
• Jumlah frekuensi TKM • Jumlah frekuensi HA • Jumlah frekuensi HP • Jumlah frekuensi penyidikan TP • Jumlah frekuensi penyidikan TP – TPPU • Jumlah frekuensi penuntutan TP • Jumlah frekuensi penuntutan TP – TPPU • Jumlah frekuensi putusan TPPU • Jumlah pemblokiran situs/*website* investasi ilegal • Jumlah penindakan koperasi terkait dengan penipuan siber • Jumlah penipuan siber di bidang	• Kemampuan penanganan perkara oleh pemangku kebijakan • Kebijakan Penanganan Perkara Penipuan siber • Persepsi kerentanan	• Nominal frekuensi TKM • Nominal frekuensi HA • Nominal frekuensi HP • Nominal frekuensi penyidikan TP • Nominal frekuensi penyidikan TP – TPPU • Nominal frekuensi penuntutan TP • Nominal frekuensi penuntutan TP – TPPU • Nominal frekuensi putusan TPPU • Nominal pemblokiran situs/*website* investasi ilegal • Nominal penindakan koperasi terkait dengan penipuan siber

Ancaman	Kerentanan	Dampak
perdagangan berjangka komoditas • Data aduan dari Pihak Pelapor terkait Tindak Pidana Penipuan Siber • Data transaksi dari Pihak Pelapor terkait Tindak Pidana Penipuan Siber • Persepsi ancaman		• Nominal penipuan siber di bidang perdagangan berjangka komoditas • Nominal aduan dari Pihak Pelapor terkait Tindak Pidana Penipuan Siber • Nominal transaksi dari Pihak Pelapor terkait Tindak Pidana Penipuan Siber • Persepsi dampak

A. Jenis/ Karakteristik Penipuan Siber

Jenis/ karakteristik yang digunakan dalam penilaian risiko penipuan siber terdiri dari :

1. *Fraudulent Wire Transfer*

   Korban acak dihubungi oleh penjahat yang mengaku sebagai teman, kerabat, atau seseorang yang berwenang dan ditipu untuk berpisah dengan pengiriman uang
2. *Business Email Compromise*

   Penjahat meretas sistem email untuk mendapatkan informasi tentang sistem pembayaran perusahaan, kemudian menipu karyawan perusahaan untuk mentransfer uang ke rekening bank mereka.
3. *Romance scams*

   Penjahat mengembangkan “hubungan” dengan korban melalui media sosial dengan tujuan akhir mendapatkan uang.
4. *Investment Fraud*

   Korban ditekan untuk berinvestasi dalam saham palsu atau tidak berharga, atau investasi lainnya yang sebenarnya tidak ada kegiatan investasi.

B. Profil (non perseorangan)

Pada aspek ini, tingkat risiko penipuan siber dinilai berdasarkan profil pelaku. Berikut adalah daftar profil pelaku penipuan siber di Indonesia yang

didasarkan pada literatur (FATF, 2013, 2019; PPATK, 2019) dan khususnya UU no 8 tahun 2010 tentang TPPU.

1. Perseroan terbatas
2. Koperasi
3. CV
4. Perusahaan Daganga/ Usaha Dagang
5. Firma
6. Yayasan
7. Perkumpulan
8. Ormas Tidak berbadan hukum

C. Profil (perseorangan)

Pada aspek ini, tingkat risiko penipuan siber dinilai berdasarkan profil pelaku. Berikut adalah daftar profil pelaku penipuan siber di Indonesia yang didasarkan pada literatur (FATF, 2013, 2019; PPATK, 2019) dan khususnya UU no 8 tahun 2010 tentang TPPU.

1. Buruh, Pembantu Rumah Tangga dan Tenaga Keamanan
2. Ibu Rumah Tangga
3. Pedagang
4. Pegawai Bank
5. Pegawai BUMN/BUMD (termasuk pensiunan)
6. Pegawai Money Changer
7. Pegawai Swasta
8. Pejabat Lembaga Legislatif dan Pemerintah
9. Pelajar/Mahasiswa
10. Pengajar dan Dosen
11. Pengrajin
12. Pengurus dan pegawai yayasan/lembaga berbadan hukum lainnya
13. Pengurus Parpol
14. Pengurus/Pegawai LSM/organisasi tidak berbadan hukum lainnya
15. Pengusaha/Wiraswasta
16. Petani dan Nelayan
17. PNS (termasuk pensiunan)
18. Profesional dan Konsultan

19. TNI/Polri (termasuk pensiunan)
20. Ulama/Pendeta/Pimpinan organisasi dan kelompok keagamaan
21. Lain-Lain

D. Sektor Industri

Pada aspek sektor industri ini, tingkat risiko penipuan siber dinilai dengan mengacu pada daftar pihak pelapor TPPU di Indonesia yang didasarkan pada literatur (FATF, 2013, 2019; PPATK, 2019) dan khususnya UU no 8 tahun 2010 tentang TPPU. Berikut adalah daftarnya.

1. Bank
2. Perusahaan Pembiayaan
3. Perusahaan Asuransi dan Perusahaan Pialang Asuransi
4. Dana Pensiun Lembaga Keuangan
5. Perusahaan Efek
6. Manajer Investasi
7. Kustodian
8. Wali Amanat
9. Perposan sebagai Penyedia Jasa Giro
10. Pedagang Valuta Asing
11. Penyelenggara Alat Pembayaran Menggunakan Kartu
12. Penyelenggara E-Money dan / atau E-Wallet
13. Koperasi yang Melakukan Kegiatan Simpan Pinjam
14. Pegadaian
15. Pedagang Fisik Aset Kripto
16. Pialang Berjangka
17. Penyelenggara Kegiatan Usaha Pengiriman Uang
18. Perusahaan Modal Ventura
19. Perusahaan Pembiayaan Infrastruktur
20. Lembaga Keuangan Mikro
21. Lembaga Pembiayaan Ekspor
22. Penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi

23. Penyelenggara layanan urun dana melalui penawaran saham berbasis teknologi informasi
24. Penyelenggara layanan Transaksi Keuangan berbasis teknologi informasi
25. Perusahaan Properti/Agen Properti
26. Pegadang Kendaraan Bermotor
27. Pedagang Permata dan Perhiasan/Logam Mulia
28. Pegadang Barang Seni dan Antik
29. Balai Lelang

E. Wilayah (Region)

Pada aspek ini, tingkat risiko penipuan siber dinilai berdasarkan wilayah terjadinya penipuan siber sehingga dapat diketahui profil risiko dari provinsi sebagai tempat terjadinya penipuan. Seluruh propinsi di Indonesia menjadi obyek penilaian risiko penipuan siber. Dalam upaya melakukan penilaian risiko terhadap penipuan siber berdasarkan wilayah terjadinya penipuan siber.

F. Tipologi

Pada aspek tipologi, tingkat risiko TPPU dinilai dengan mengacu pada daftar pihak tipologi TPPU di Indonesia yang didasarkan pada literatur (FATF, 2013, 2019; PPATK, 2019) dan khususnya UU no 8 tahun 2010 tentang TPPU. Sedikit berbeda dengan POC lainnya, aspek tipologi ini dinilai secara penuh risiko oleh persepsi apgakum. Berikut adalah daftar tipologi TPPU yang dinilai risiko dalam SRA Penipuan Siber ini.

1. Penyembunyian harta hasil kejahatan ke dalam struktur bisnis
2. Penggunaan dokumen identitas palsu
3. Penggunaan kartu kredit, cek, note dalam pencucian uang hasil tindak kejahatan.
4. Pembuatan rekening baru untuk menampung dana hasil kejahatan
5. Penggunaan rekening *nominee:* milik orang lain (baik yang dikenal/tidak kenal/fiktif)
6. Pola transaksi dengan menggunakan uang tunai *(Cash Basis):* tarik tunai, setor tunai; yang dilakukan untuk menyamarkan identitas
7. Penggunaan pihak ketiga untuk pengiriman uang

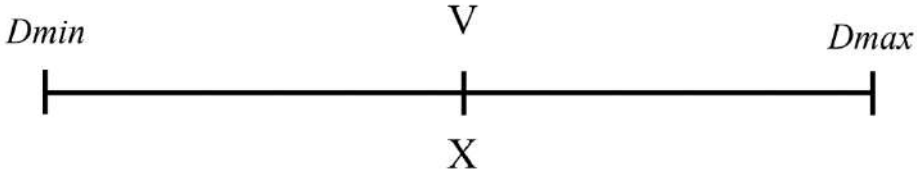
8. Penggunaan pihak lain/perantara dan pihak keluarga dalam upaya menyembunyikan atau menyamarkan asal usul harta kekayaan dari hasil tindak kejahatan
9. Transaksi yang dilakukan secara *Pass by* (dana masuk langsung ditransfer kembali atau tarik tunai)
10. Pembelian aset berupa tanah, bangunan, rumah dan mobil
11. Pembelian barang – barang mewah seperti (lukisan, barang – barang antik, berlian atau barang – barang *branded* dlll)
12. Penggunaan nama Perusahaan atau perorangan untuk menampung pengiriman uang sehingga seolah-olah nampak seperti transaksi bisnis
13. Penyalahgunaan bisnis yang sah dengan pemalsuan dokumen sehingga menyebabkan cacat administrasi
14. *Mingling:* Menggabungkan hasil kejahatan dengan bisnis yang sah untuk mengaburkan sumber dana. Penempatan uang tidak mengejar keuntungan
15. *Structuring:* Memecah-mecah transaksi dengan melibatkan berbagai pihak, volume tinggi dari transaksi yang kecil, penggunaan banyak akun/rekening guna menghindari deteksi kewajiban pelaporan oleh penyedia jasa keuangan/pihak pelapor
16. Penggunaan *"gatekeeper"* layanan profesional (Pengacara, Akuntan, Broker, Notaris, Konsultan Bisnis, Perencana Keuangan) bertujuan untuk mengaburkan identitas penerima manfaat *(Beneficiaries)* dan harta hasil kejahatan
17. Penggunaan *Virtual Currency* (Aset Kripto)
18. Pembelian saham dari uang hasil kejahatan
19. Pembelian polis asuransi
20. Penggunaan Perusahaan Multinasional, *Offshore Bank* dan *Offshore Trust*
21. Penggunaan skema pencucian uang dengan perdangan atau *Trade – Based Money Laundering (TBML)* dan Transfer Pricing (permainan harga)
22. Penggunaan Bank illegal atau alternative jasa pengiriman uang atau Hawala
23. Penggunaan *safe deposit box*

24. Pemanfaatan Alat Pembayaran Baru: Uang Elektronik, Dompet Elektronik
25. Pengoperasian perusahaan cangkang/*shell company* (perusahaan yang tercatat secara hukum namun tidak terdapat aktivitas, biasanya digunakan untuk menyembunyikan harta dari tindak kejahatan)
26. Penukaran mata uang asing dalam jumlah yang signifikan dengan cara mentransfer ke perusahaan *money changer*
27. Pemberian sumbangan pada lembaga keagamaan, sosial dan/ pendidikan

3.2.2 Tahap kedua: Analisis

Selanjutnya, tahapan analisis ini ditujukan untuk menganalisis risiko dengan berbasis dari fakta dan bukti yang telah teridentifikasi dalam aspek ancaman, kerentanan dan dampak, dan konsekuensi dari penipuan siber di Indonesia. Untuk melaksanakan analisis tersebut, dilakukan proses pembobotan atas setiap masing-masing PoC (*Point of Concern*) dari setiap variabel yang sudah diidentifikasi pada tahap sebelumnya. Berikut adalah pembobotan yang dilakukan.

Dalam melakukan kajian selanjutnya, kemudian dilakukan kuantifikasi terhadap setiap variabel dengan mentransformasikan volume ancaman, kerentanan, dan dampak ke dalam skala 3-9. Dalalm skala ini, data yang dengan nilai yang paling kecil otomatis menjadi skala 3, sementara data dengan nilai yang paling besar otomatis menjadi skala 9. Data dengan nilai diantara keduanya menjadi skala antara 3 hingga 9 tergantung besar kecilnya nilai data tersebut. Transformasi kuantitatif ini dilakukan dengan menggunakan metode sederhana sebagai berikut:



$$X = \frac{6(y - Dmin) + 3}{Dmax - Dmin}$$

Gambar 3.2 Transformasi Kuantitatif.
(Sumber: NRA Indonesia, 2015)

Untuk setiap PoC, masing – masing faktor pembentuk risikonya dari proses identifikasi dijumlahkan kemudian dirata – rata. Skala terkecil adalah 3 dan skala terbesar 9, baik untuk variabel ancaman, kerentanan dan dampaknya. Sesuai dengan formula penilaian risiko, setelah memperoleh nilai kuantitas ancaman dan kerentanan, keduanya kemudian dijumlahkan untuk memperoleh nilai kecenderungan (*likelihood*) (IMF, 2011). Nilai kecenderungan masing-masing PoC kemudian dirata-rata dan dikonversi lagi ke dalam skala 3 – 9.

Sesuai dengan formula risiko, setelah memperoleh nilai kecenderungan, kemudian dikalikan dengan skala dampak untuk mendapatkan nilai risiko. Karena skala kecenderungan dan dampak masing-masing bernilai 3-9, maka nilai risiko yang paling kecil adalah 9 (3X3) dan yang paling besar adalah 81 (9x9). Untuk mendapatkan skala yang konsisten yakni 3-9, nilai risiko yang diperoleh kemudian dikonversi dengan cara menghitung akar kuadrat masing-masing nilai risiko tersebut. Nilai risiko masing-masing PoC tersebut kemudian dibagi ke dalam tiga level, yaitu sebagai berikut:

Tabel 3.2 Rumusan Tingkat Risiko

Rentang nilai risiko	Level risiko
$3 \leq x < 5$	Rendah
$5 \leq x \leq 7$	Menegah
$x > 7$	Tinggi

Sumber: NRA Indonesia 2021

Berikut penjelasan alternatif terkait tingkat ancaman, kerentanan, dan dampak di atas:

1. Tinggi: terdapat jumlah dan nilai signifikan yang terlibat dalam transaksi mencurigakan dan kasus yang teridentifikasi secara faktual dan potensial
2. Menengah: terdapat jumlah dan nilai menengah (*moderate*) dalam transaksi mencurigakan dan kasus yang teridentifikasi secara faktual dan potensial
3. Rendah: terdapat jumlah dan nilai terbatas dalam transaksi mencurigakan dan kasus yang teridentifikasi secara faktual dan potensial

Gambaran risiko yang sudah dianalisis dapat ditampilkan ke dalam bentuk skala matrik dari risiko rendah, risiko sedang dan risiko tinggi sebagai berikut:

Gambar 3.3 Kecenderungan Tingkat Risiko
(Sumber: NRA Indonesia, 2021)

Dari matriks evaluasi risiko di atas, terlihat bahwa masing – masing level risiko memiliki strategi penanganan yang berbeda-beda. Tahapan evaluasi ini merupakan tahapan yang dilakukan dalam tingkatan pengambilan kebijakan untuk tujuan penentuan langkah strategis kedepannya.

3.2.3 Tahap ketiga: Evaluasi

Tahapan evaluasi merefleksikan prosesn pengambilan sikap dan keputusan atas hasil analisis di atas. Tujuannya adalah untuk menentukan prioritas dalam mengatasi risiko dengan melakukan revisitasi tujuan penilaian risiko pada awal proses penilaian. Di tahap evaluasi ini juga disusun strategi untuk mitigasi risiko. Pengambilan strategi mitigasi risiko ini dilakukan secara bersama dengan tim stake holder yang terlibat dalam penyusunan SRA penipuan siber ini. Dalam hasil evaluasi akhir ini, akan dirumuskan juga beberapa rekomendasi kebijakan maupun strategi sesuai tingkat risikonya.

Gambar 3.4 Arah Rekomendasi Berbasis Risiko
(Sumber: NRA Indonesia 2021)

Berdasarkan hasil penilaian risiko yang telah diperoleh melalui ketiga tahapan tersebut beserta rekomendasi yang telah dihasilkan, selanjutnya dilakukan monitoring, *review*, dan *update* secara berkala untuk memastikan risiko tersebut dapat dimitigasi dengan baik.

3.3 TEKNIK PENGUMPULAN DATA DAN ANALISIS

Penyusunan SRA penipuan siber ini melibatkan proses yang melewati berbagai tahapan dalam pengumpulan data dan informasi, terutama yang saat ini tidak tersedia dalam catatan maupun dokumen publik, serta membutuhkan kedalaman analisis untuk memahami perubahan tren ancaman, kerentanan dan dampak penipuan siber di Indonesia ini. Secara umum, dalam proses pencarian bukti-bukti terkait risiko penipuan siber, PPATK mengumpulkan data dan informasi dari berbagai *stakeholders* rezim Anti-Pencucian Uang melalui dua langkah awal. *Pertama*, penelitian dokumenter awal (*preliminary documentary research*) yang dilakukan untuk mengumpulkan informasi latar belakang guna mengartikulasikan dasar-dasar pemahaman dan perkembangan tren penipuan siber di tanah air.

Tinjauan kepustakaan ini diarahkan untuk menjaring data dan informasi dari artikel-artikel akademik, arsip materi berbasis internet, dan arsip lainnya berupa dokumen kebijakan dan laporan evaluasi dari pemerintah maupun lembaga non-pemerintah. Analisis dokumen tersebut dibutuhkan untuk memeriksa *track record*

kebijakan maupun dinamika ekonomi-politik dan keamanan nasional yang mengitarinya, sehingga bisa mencermati tren perkembangan penipuan siber saat ini. Tidak hanya itu, tahap awal ini juga ditujukan untuk memahami arah kebijakan rezim Anti-Pencucian Uang untuk menutup celah-celah terjadinya praktik penipuan siber.

Kedua, untuk melakukan validasi data dan informasi yang diperoleh dari hasil analisis dokumenter, tim peneliti juga menyelenggarakan diskusi awal jelang pelaksanaan penelitian (*pre-research discussion*). Fase diskusi awal ini melibatkan sejumlah *stakeholders* rezim Anti-Pencucian Uang yang dinilai memahami konteks persoalan penipuan siber di Indonesia. Setelah melakukan validasi data dan informasi yang memadai dari proses *pre-research discussion* ini, tim peneliti selanjutnya memetakan kompleksitas data dan informasi yang telah diperoleh untuk menemukan celah (*gap*) yang kemudian akan diperdalam dalam proses penelitian selanjutnya.

Hasil analisis dokumen dan diskusi itu kemudian dituangkan dalam instrumen pertanyaan *Focus Group Discussion* (FGD), guna memperkuat basis instrumen survei yang telah diadopsi dari FATF. Dengan menggabungkan temuan data kuantitatif dan kualitatif, diharapkan PPATK bisa mendapatkan analisa yang lebih solid dan memadai terkait aspek ancaman, kerentanan dan dampak penipuan siber di Indonesia saat ini. Selanjutnya adalah penjelasan mengenai teknik pengambilan data. Sementara itu, jika dilihat perspektif analisisnya, penyusunan SRA Penipuan Siber ini menggabungkan pendekatan kuantitatif dan kualitatif. Dari sisi pendekatan kuantitatif, terdapat dua sumber data yang menjadi acuan.

a. Data statistik: Statistik Pelaporan LTKM, Pertukaran Informasi, Penanganan Perkara, Putusan Pengadilan.
b. Kuesioner : Data Statistik dan *Self – Assessment* Apgakum, LPP, Pihak Pelapor.

Sementara, data kualitatif berasal dari studi kasus dan hasil diskusi dengan stakeholders pengampu penanganan Tindak Pidana Penipuan Siber.

3.3.1 Survei melalui kuesioner

Instrumen survei ini mengadopsi instrumen yang telah dikembangkan oleh FATF. Agar lebih mudah dipahami oleh responden, instrumen survei tersebut telah diterjemahkan dan disesuaikan dengan konteks keindonesiaan. Selanjutnya, populasi survei adalah para *stakeholders* dari rezim Anti-Pencucian Uang seperti Pihak Pelapor (PP), Lembaga Pengawas dan Pengatur (LPP), Aparat Penegak Hukum (APH), Lembaga Asosiasi, dan *stakeholders* lainnya yang dinilai memiliki

pemahaman yang memadai tentang perkembangan aspek ancaman, kerentanan dan dampak penipuan siber di Indonesia saat ini. Sehingga responden ditentukan secara *purposive non-probabilistic* berdasarkan kesesuaian dengan kriteria dan pemahaman mereka yang memadai terkait rezim anti-pencucian uang di Indonesia. Kurang lebih 18 responden telah terlibat dalam pengumpulan data survei analisa risiko penipuan siber ini. Proses pengumpulan data kuantatif ini dilakukan sejak April s,d Mei 2022. Terdapat tiga jenis kuesioner utama yang diarahkan kepada empat pemangku kepentingan utama dalam rezim APU di Di Indonesia. Tiga kuesioner utama tersebut adalah terhadap Aparat Penegak Hukum (APH), Pihak Pelapor (PP), Lembaga Pengawas dan Pengatur (LPP).

3.3.2 Focus Group Discussion (FGD)

Serangkaian tahap *Focus Group Discussion (FGD)* dilakukan dengan para *stakeholders* dari rezim Anti-Pencucian Uang seperti Pihak Pelapor (PP), Lembaga Pengawas dan Pengatur (LPP), Aparat Penegak Hukum (APH), Lembaga Asosiasi, dan *stakeholders* lainnya. Rangkaian FGD ini tidak hanya dilakukan untuk memperdalam dan memperkaya basis pemahaman yang lebih komprehensif tentang aspek ancaman, kerentanan, dampak penipuan siber yang diteliti, melainkan juga untuk memvalidasi informasi yang diperoleh dari hasil survei kuantitatif sebelumnya agar terhindar dari bias informasi dan kekeliruan persepsi.

Dalam tahap pelaksanaan FGD ini, peserta FGD telah diminta untuk memberikan penjelasan tentang pengalaman dan mengidentifikasi ancaman, kerentanan, dampak, dan langkah mitigasi serta rekomendasi aksi terkait perkembangan dinamika penipuan siber di Indonesia saat ini. Hasil perekaman gambar dan suara telah ditranskrip secara verbatim menjadi teks. Analisis tematik dilakukan dengan metode *grounded theory* melalui proses *coding* yakni *initial coding, focused coding*, dan *axial coding*, guna memungkinkan memahami struktur informasi yang diperoleh. Selanjutnya, hasil transcript dan hasil *coding* dianalisa setiap barisnya, untuk kemudian dipisahkan dan dikelompokkan berdasarkan isu dan informasi yang merefleksikan tujuan utama penelitian ini, yakni aspek – aspek risiko TPPU dan juga untuk merumuskan saran perbaikan sistem yang ada.

BAB IV
ANALISIS RISIKO

4.1 LANSKAP PENANGANAN TINDAK PIDANA PENIPUAN SIBER DI INDONESIA

Tindak pidana penipuan siber merupakan tindak pidana penipuan dengan basis media elektronik sebagai perantara pengunaannya. Dalam pembuktian dakwaan terhadap pelanggaran tindak pidana ini, para penegak hukum harus dapat menghadirkan bukti elektronik yang digunakan oleh para pelaku dan juga aktor utamanya. Sebab jika tidak, tindak pidana ini akan dianggap sebagai tindak pidana penipuan konvensional/tipu gelap.

Lembaga Penegak Hukum yang mempunyai wewenang dalam penanganan perkara tindak pidana penipuan siber ini diantaranya:

a. Bagian intelijen dan analisis transaksi dilakukan PPATK melalui penerimaaan LTKM (Laporan Transaksi Keuangan Mencurigakan) serta penyusunan Hasil Analisis (HA) dan Hasil Pemeriksaan (HP) yang selanjutnya dikirimkan kepada Lembaga Penegak Hukum ataupun Stakeholders terkait.
b. Bagian Penyidikan ditangani oleh Direktorat Tindak Pidana Penipuan Siber dan Direktorat Tindak Pidana Ekonomi Khusus dari Bareskrim POLRI.
c. Bagian Penuntutan ditangani oleh Direktorat Tindak Pidana Umum Lain serta Direktorat Orang dan Harta Benda, Kejaksaan Agung.
d. *Stakeholders* pendukung seperti Kominfo yang melakukan penutupan *website* investasi ilegal; Bappebti yang bertugas untuk mengawasi website investasi terutama untuk aset kripto ilegal dan juga memberikan rekomendasi kepada Kominfo untuk penutupan *website* investasi bodong/ilegal serta Kemenkop UKM RI yang bertugas untuk mengawasi dan mengatur adanya koperasi yang melakukan pengumpulan dana masyarakat.
e. Sementara itu, untuk pengejaran aset yang berada luar negeri ataupun usaha penangkapan pelaku yang berhasil kabur ke luar negeri dibantu oleh Direktorat Otoritas Pusat dan Hukum Internasional dari Kemenkumham RI yang mempunyai wewenang dalam melakukan kerjasama dengan negara terkait berdasarkan MLA (*Mutual Legal Assistance*).

Selain penegakan hukum untuk penanganan perkara tindak pidana penipuan siber, Indonesia memiliki Satuan Tugas Waspada Invetasi (SWI) dalam hal pencegahan

tindakan melawan hukum di bidang penghimpunan dana masyarakat dan pengelolaan investasi serta penanganan dugaan tindakan melawan hukum di bidang penghimpunan dana masyarakat dan pengelolaan investasi yang terkoordinasi sesuai dengan tugas dan wewenang masing-masing anggota Satgas. Satgas ini terdiri atas 12 Kementerian/Lembaga yang diantaranya Otoritas Jasa Keuangan, Kepolisian RI, Kejaksaan RI, Kementerian Perdagangan RI, Kementerian Koperasi dan UKM RI, Kementerian Komunikasi dan Informatika RI, Kementerian Agama RI, Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi RI, Kementerian Dalam Negeri RI, Bank Indonesia, Pusat Pelaporan dan Analisis Transaksi Keuangan dan Kementerian Investasi/Badan Koordinasi Penanaman Modal.

Selanjutnya, Tim Penipuan Siber telah melakukan penelusuran data intelijen terkait dengan penipuan siber pada *database* PPATK yang diperoleh dengan hasil berikut:

Tabel 4.1 Database PPATK terkait Penipuan Siber – TPPU

Tahun 2018 – 2021

Jenis Data	Jumlah	Nominal
LTKM	472	Rp537.376.796.132
Hasil Analisis	108	Rp1.123.613.917.516
Hasil Pemeriksaan	0	Rp0

PPATK sendiri telah menerapkan indikator khusus terkait Tindak Pidana Penipuan Siber pada sistem pelaporan goAML yang diluncurkan pada 1 Februari 2021, yaitu indikator *Business Email Compromise* (BEC). Hal ini ditujukan agar pihak pelapor mampu memberikan peringatan dini dan segera terhadap tindak pidana penipuan tersebut sebelum dana hasil tindak pidana tersebut dipindahalihkan.

Sementara itu, statistik penanganan perkara yang dilakukan oleh Lembaga Penegak Hukum dimulai dari penyidikan, penuntutan hingga persidangan digambarkan pada tabel berikut:

Tabel 4.2 Data Statistik Penanganan Perkara Tahun 2018 - 2021

Jenis Data	Jumlah	Nominal
Penyidikan TP	936	Rp27.779.064.843.099
Penyidikan TP dan TPPU	904	Rp255.064.843.099
Penuntutan TP	6	Rp6.134.814.589
Penuntutan TP dan TPPU	2	Rp2.615.688.815
Putusan TPPU	29	Rp455.715.617.231

Masih minimnya pembuktian perkara Tindak Pidana Pencucian Uang pada Penipuan Siber umumnya disebabkan para pelaku atau aktor utama dari rantai penipuan tersebut berasal dari luar negeri dan telah kembali ke negara asalnya serta uang hasil tindak pidana telah dipindahalihkan sehingga cukup sulit untuk melakukan penelusuran. Selain kendala tersebut, Tim juga berhasil merangkum tantangan yang dihadapi oleh para pemangku kebijakan dalam menangani perkara tindak pidana penipuan siber, yang diuraikan sebagai berikut:

a. Tantangan Penyidik
    1. Rumitnya aliran dana serta semakin maraknya penggunaan modus operandi seperti BEC dan investment fraud dari tindak pidana penipuan siber sehingga menyulitkan penyidik dalam untuk menelusuri aliran uang dari tindak pidana.
    2. Penggunaan aset kripto yang memutus mata rantai penyidikan sebab tidak bisa dilakukannya penelusuran transaksi pada aset kripto tersebut jika sudah wallet.
    3. Kesulitan pelacakan pelaku sebenarnya/ultimate Beneficial Owner (BO) karena tipologi yang digunakan dan melibatkan jaringan internasional.
    4. Masih maraknya modus tipologi yang menggunakan dokumen identitas palsu yang teregistrasi sehingga diperlukan kerjasama dengan berbagai stakeholders dan membutuhkan waktu yang cukup lama.
    5. Implementasi penyidikan TPPU untuk TP Penipuan Siber terutama penyidik Sektor Jasa Keuangan sebagai hasil uji materiil Mahkamah Konstitusi Nomor 15 Tahun 2021 (tertanggal 29 Juni 2021) untuk Penjelasan Pasal 74 UU Nomor 8 2010 masih dalam proses implementasi awal (penyiapan infrastuktur).

b. Tantangan Penuntut
    1. Penuntut terutama di daerah terpencil belum memiliki pemahaman yang seragam dalam penanganan TPA Penipuan Siber dan TPPU sehingga seringkali penuntutan hanya mengarah kepada penipuan konvensional.
    2. Jaksa Penuntut masih kesulitan dalam proses pengembalian kerugian terutama untuk kerugian yang melibatkan pihak ketiga sebab uang hasil tindak pidana telah habis digunakan oleh pelaku untuk keperluan konsumtif.
    3. Dalam penanganan kasus Penipuan Siber sering kali terjadi perbedaan persepsi antara hakim dan penuntut terkait pembuktian TPPU.

c. Tantangan *Stakeholders* dan Regulator
    1. Dalam kasus BEC, Invesment Fraud, Romance Scams dan Fraudulent Wire Transfer umumnya melibatkan banyak yurisdiksi namun waktu retensi penyelesaian kasus sangat singkat sementara proses MLA yang formal memerlukan waktu yang relatif panjang, terutama untuk pengejaran aset – aset dari pelaku tindak pidana yang tersimpan di luar negeri ataupun untuk pelaku utama yang telah kabur ke luar negeri.
    2. Kemudahan pembuatan domain situs *web* yang dimanfaatkan oleh pelaku Penipuan Siber.

Adapun Lembaga penegak hukum Indonesia telah menghasilkan beberapa capaian keberhasilan penanganan perkara pencucian uang dari tindak pidana penipuan siber, diantaranya:

1. Pengungkapan perkara pencucian uang kasus *Business Email Compromise* (BEC) yang melibatkan korban perusahaan Taiwan White Wood House Food Co. Ltd. *Aset Recovery* yang berhasil dilakukan berupa 1 unit mobil Honda Jazz dikembalikan kepada White Wood House Food Co. Ltd melalui perwakilan perusahaan.
2. Indonesia menerima penghargaan dari Duta Besar Kerajaan Belanda untuk Indonesia dan Duta Besar Italia untuk Indonesia atas keberhasilan Indonesia dalam pengembalian aset berupa uang milik perusahaan di Italia dan belanda terkait tindak pidana siber keuangan lintas negara dengan modus tindak pidana

pencucian uang, yakni sejumlah uang lebih dari Rp56,6 miliar kepada perusahaan Althea Italia S.P.A. di Italia dan sejumlah uang lebih dari Rp27,9 miliar dikembalikan kepada perusahaan Mediphos Medical Supplies B.V. di Belanda.

Keberhasilan tersebut diperoleh dengan kerjasama antara Lembaga Penegak Hukum di Indonesia dengan Penegak Hukum di Belanda dan Italia (Kejaksaan Agung RI, 2021) yang diuraikan sebagai berikut:

- **Kerjasama dengan Italia**

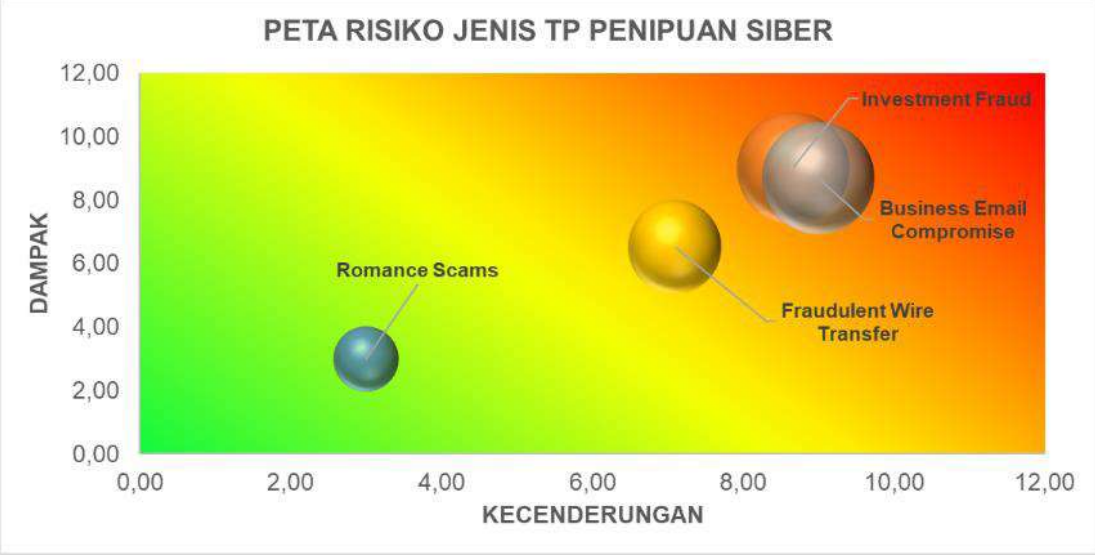
  Dalam perkara ini, Kedutaan Besar Italia sudah terlibat sejak tahap Kepolisian sampai tahap eksekusi dengan Kejaksaan. Dalam pengembalian aset Althea Group terdapat tantangan dan hambatan karena terdapat pihak ketiga yang mengaku sebagi pemilik yang sah atas uang tersebut, namun masalah tersebut dapat diatasi atas kerjasama yang terjalin antara Italia dengan Indonesia. Bentuk Kerjasama yang terjalin adalah kerjasama informal dan memberikan dampak yang sangat baik terhadap pemulihan aset korban. Kasus ini telah diputus oleh Pengadilan Negeri Serang pada tahun 2021.
- **Kerjasama dengan Belanda**

  Pengembalikan kerugian kepada korban dalam hal ini PT Medhipos sebesar USD1,9 Juta. PT Medhipos merupakan importer obat dan alat medis untuk menanggulangi covid-19 di Belanda. Namun PT Medhipos terkena kasus penipuan siber dengan menggunakan skema BEC dan melakukan pentransferan sejumlah uang ke rekening semua CV di Indonesia. Kasus ini telah Kasus ini telah diputus oleh Pengadilan Negeri Serang pada tahun 2021.

4.2 TINGKAT RISIKO TPPU BERDASARKAN JENIS TINDAK PIDANA PENIPUAN SIBER

Penilaian tingkat risiko TPPU berdasarkan jenis tindak pidana penipuan siber dilakukan untuk mengetahui jenis tindak pidana penipuan siber mana yang paling berisiko tinggi menjadi kasus TPPU-penipuan siber. Jenis-jenis tindak pidana penipuan siber yang perlu dinilai tingkat risikonya dalam kajian ini ditetapkan mencakup 4 (empat) jenis tindak pidana penipuan siber, yaitu: *Romance Scams, Investment Fraud, Business Email Compromise dan Fraudulent Wire Transfer*. Pengukuran tingkat risiko diperoleh dengan menghitung terlebih dahulu tingkat ancaman (*threat*), kerentanan (*vulnerability*)

dan dampak (*consequence*). Ketiga aspek tersebut diukur berdasarkan faktor – faktor pembentuk risiko yang telah ditetapkan sebelumnya.



Gambar 4.1 Peta Risiko menurut Jenis Tindak Pidana

Berdasarkan peta risiko di atas dapat disimpulkan bahwa ***Business Email Compromise*** dan ***Investment fraud*** merupakan jenis tindak pidana penipuan siber yang memiliki **risiko tinggi.** Hal ini didukung dengan adanya tingginya faktor ancaman dan dampak yang berasal dari data dan nominal penyidikan tindak pidana dan pencucian uang yang cukup besar. Dari data tahun 2018 – 2021, terhitung bahwa total nominal penyidikan tindak pidana terkait dengan *Investment Fraud* mencapai Rp27 Triliun atau mencapai dari 99,53% dari total penyidikan yang dilakukan oleh Lembaga Penegak Hukum pada rentang waktu tersebut. Di sisi lain, untuk kasus terkait penyidikan TPPU terkait *Business Email Compromise* pada rentang waktu tersebut juga mencapai Rp166 Miliar atau 65,17% dari total penyidikan pencucian uang pada waktu tersebut. Hal ini telah menunjukkan upaya serius dari Lembaga Penegak Hukum terkait dengan penanganan perkara penipuan siber pada kasus BEC dan *Investment Fraud*.

Kasus 1 – *Business Email Compromise*

Kasus Posisi	Tindak Pidana Asal
• Sdr. HWC pemilik email Eddie_Hsiao@pxmart.com.tw bekerja di WWH FOOD CO, Ltd yang beralamat di Jalan Jingye IV no 33 lantai 8 distrik Zhongshan, Taipei 104, sebagai staff procurement sejak Agustus 2018 melakukan penawaran kepada supplier melalui internet dan berkomunikasi menggunakan email Eddie_Hsiao@pxmart.com.tw diantaranya dengan supplier N FARMS beralamat di 1611 BUNKER HILL WAY, SUITE 200, SALINAS, CA. 93906, Amerika Serikat yang bergerak dalam bidang grosir buah dan sayur. Tugas pokok sdr. HWC sebagai staff procurement pada WWH FOOD CO, Ltd yaitu berkomunikasi dengan supplier untuk memesan buah buahan. perwakilan perusahaan Naturipe Farms menggunakan alamat email mmontufar@naturipefarms.com. • Pelaku kejahatan mengirimkan email palsu kepada korban penipuan, dengan alamat email mmontufar@naturipesfarms.com dan mengira bahwa email tersebut merupakan email asli dari N Farms yang telah menjalin kerjasama dengan perusahaan WWH Food CO, Ltd. Sedangkan email asli dari N farms adalah mmontufar@naturipefarms.com dimana hanya perbedaan huruf s yang	• Pada tanggal 5 Juni 2020 sdr. HWC mendapatkan email dari mmontufar@naturipesfarms.com (email penipuan), Isi dari email tersebut terkait perubahan no rekening bank. Lalu perusahaan sdr. HWC meminta mengirimkan surat keterangan yang menjelaskan tentang perubahan nomor rekening perusahaan Naturipe Farms dan pada tanggal 9 Juni 2020 sdr. HWC menerima email lagi dari mmontufar@naturipesfarms.com berisi surat pernyataan terkait perubahan no rekening dan ditandatangani oleh perwakilan dari Naturipe Farms yang diduga oleh sdr. HWC asli. Isi email dimaksud adalah perubahan rekening bank untuk melakukan transfer ke BANK MY dengan alamat Bank Jalan Panglima Polim Jakarta Selatan dengan Nomor Rekening 15030086xxxx, dan dengan adanya surat tersebut, maka dianggap tidak mencurigakan oleh korban. • Setelah dokumen tersebut diterima, sdr. HWC mengunggah dokumen tersebut ke sistem finace perusahaan untuk melakukan perubahan no rekening ke Bank MY No Rekening 15030086xxxx sesuai dengan surat keterangan yang

Kasus Posisi	Tindak Pidana Asal
tidak mudah ditemukan dengan membaca sekilas alamat email tersebut. Terdakwa CR merupakan orang yang dipekerjaan/ diperintah oleh Sdr DN dan Sdri Novita Febriyani alias Lisa alias Ivon alias Vita.	diterima dari PT N palsu tersebut. Setelah perubahan No Rekening tersebut berhasil, maka bagian finance akan memastikan jumlah pembayaran tersebut sesuai nominalnya dan dikirimkan sesuai dengan jadwal pembayarannya, agar tidak mencurigakan, pemilik email mmontufar@naturipesfarms menyebutkan rekening tersebut dimiliki oleh PT N LLC dengan alamat Jalan Jend Sudirman Kav 52-53 Jakarta 12190; • Pada tanggal 11 Juni 2020, CR (terdakwa) untuk membuka Rekening di Bank MY KCP Jalan Panglima Polim Jakarta Selatan, dokumen-dokumen untuk pembukaan rekening sudah dibawa oleh CR, diantaranya adalah akta pendirian tanggal 10 Juni 2020 yang beralamat di Gedung TT Lantai 7 Unit F, Distrik 8 Lot 28, Jl. Jenderal Sudirman Kav. 52-53 Jakarta Selatan. Rekening yang di buka oleh CR atas nama PT N LLC • Pada tanggal 12 Juni 2020 pihak WWH FOOD CO, Ltd melakukan transfer uang sejumlah 50,838.36 USD dari Nomor Rekening 03053116158 MIC Bank, Taipei ke Nomor Rekening 15030086xxxx an PT N LLC diterima sebesar USD 50.820,36 yang otomatis langsung

Kasus Posisi	Tindak Pidana Asal
	dikonversikan ke dalam bentuk rupiah oleh Bank dengan kurs Rp. 14.220 senilai Rp. 722.665.519,20, (tujuh ratus dua puluh dua juta enam ratus enam puluh lima ribu lima ratus sembilan belas rupiah koma dua puluh sen) dengan biaya materai Rp. 6000 (enam ribu rupiah); • Bahwa pada tanggal 19 Juni 2020 pihak WWH FOOD CO, Ltd melakukan 2 (dua) kali transaksi dari Nomor Rekening 03053116158 MIC Bank, Taipei masing-masing dengan jumlah USD 52,572 (lima puluh dua ribu lima ratus tujuh puluh dua dollar (amerika)) yang diterima oleh Bank MY tanggal 22 Juni 2020 secara otomatis langsung dikonversikan ke dalam mata uang rupiah oleh Bank MY dengan kurs Rp. 14.190 sebesar Rp. 745.741.260 (tujuh ratus empat puluh lima juta tujuh ratus empat puluh satu ribu dua ratus enam puluh rupiah) dan USD 98.436 (sembilan puluh delapan ribu empat ratus delapan belas dollar (amerika)) yang otomatis langsung dikonversikan ke dalam bentuk rupiah oleh Bank dengan kurs Rp. 14.190 senilai Rp. 1.396.551.420 (satu miliar tiga ratus sembilan puluh enam juta lima ratus lima

Kasus Posisi	Tindak Pidana Asal
	puluh satu ribu empat ratus dua puluh rupiah). Total keseluruhan yang ditransfer oleh pihak WWH Food Co, Ltd yaitu USD 201.846,36 dengan jumlah total lebih kurang Rp. 2.864.958.199,20 (dua miliar delapan ratus enam puluh empat juta sembilan ratus lima puluh delapan ribu seratus sembilan puluh sembilan rupiah koma duapuluh sen). • Pada tanggal 15 Juni 2020 bertempat di Bank MY terdakwa CR melakukan pengambilan / penarikan uang tunai rekening giro menggunakan cek No. MY2 259XXX sejumlah Rp. 320.000.000,00 (tiga ratus dua puluh juta rupiah) dari Rekening Nomor 15030086xxxx atas nama PT N LLC dan dilakukan RTGS (Real Time Gross Setlement) transaksi pemindahbukuan yang bersifat real time ke Nomor Rekening 070.3045.XXX Bank BC KCP Melawai Kebayoran Baru Jakarta Selatan atas nama PT. DIP yang beralamat di Kantor Ruko BSD PLAZA, BSD City, Kota Tangerang Selatan sejumlah Rp. 400.000.000,00 (empat ratus juta rupiah) dibebankan biaya RTGS sebesar Rp. 30.000 (tiga puluh ribu rupiah) setiap transaksi;

Kasus Posisi	Tindak Pidana Asal
	• Terhadap dana masuk sejumlah USD 52.554 dan sejumlah USD 98.418, selanjutnya pada tanggal 22 Juni 2020 bertempat di Bank MY Kantor Cabang Pembantu Jalan Panglima Polim Nomor 83 Jakarta Selatan, terdakwa CR melakukan RTGS (Real Time Gross Setlement) transaksi pemindahbukuan yang bersifat real time ke Rekening Bank BC KCP Mangga Besar Raya Jakarta Pusat dengan Nomor Rekening 1610054XXX atas nama PT. DIP yang beralamat di Ruko Matercella Jalan Bintaro, Tangerang Selatan sejumlah Rp. 714.250.000,00 (tujuh ratus empat belas juta dua ratus lima puluh ribu rupiah) dan terdakwa melakukan RTGS (Real Time Gross Setlement) transaksi pemindahbukuan yang bersifat real time ke Rekening Bank BC KCP Melawai Kebayoran Baru Jakarta Selatan dengan Nomor Rekening 070.3045.XXX atas nama PT DIP sebesar Rp. 185.705.000,00 (seratus delapan puluh lima juta tujuh ratus lima ribu rupiah). Dan tanggal yang sama terdakwa melakukan tarik tunai dengan Cek Nomor MY 2. 259XXX sejumlah Rp. 75.000.000,00 (tujuh puluh lima juta rupiah);

Kasus Posisi	Tindak Pidana Asal
	• Tanggal 23 Juni 2020, bertempat di Bank MY KCP Jalan Panglima Polim Nomor 83 Jakarta Selatan terdakwa CR melakukan tarik tunai cek Nomor MY 2. 259XXX sebesar Rp. 139.800.000,00 (seratus tiga puluh sembilan juta delapan ratus ribu rupiah) terdakwa melakukan RTGS (Real Time Gross Setlement) dan transaksi pemindahbukuan yang bersifat real time ke Rekening Nomor 161005XXX Bank BC KCP Mangga Besar Jakarta Pusat atas nama PT. DIP yang beralamat di Ruko Matercella Jalan Bintaro Utama Sektor 3A No E82, Pondok Karya, Pondok Aren, Tangerang Selatan sejumlah Rp. 1.027.061.199,00 (satu milyar dua puluh tujuh juta enam puluh satu ribu seratus sembilan puluh sembilan rupiah).

Tindak Pidana Pencucian Uang
• Terdakwa CR membuka rekening dengan identitas palsu berupa KTP palsu atas nama LUSY dan untuk melegalkan perbuatannya, terdakwa melalui Sdr.NF alias Lisa alias Ivon alias Vita membuat legalitas PT N LLC yang didirikan tanggal 10 Juni 2020. Dalam akte Pendirian Perusahaan terdakwa Sdri CR dicantumkan sebagai Direktur dengan identitas palsu. PT N LLC tidak memiliki karyawan dan hanya terdakwa yang bekerja di dalam perusahaan tersebut. Saat ini PT Naturipe Farms, LLC tidak berada di dalam kondisi aktif karena tidak memiliki klien. Kebijakan dari PT N LLC diatur oleh Sdri NF alias Lisa alias Ivon alias Vita dan masuknya terdakwa selaku Direktur di PT N LLC dikendalikan juga oleh Sdr DN.

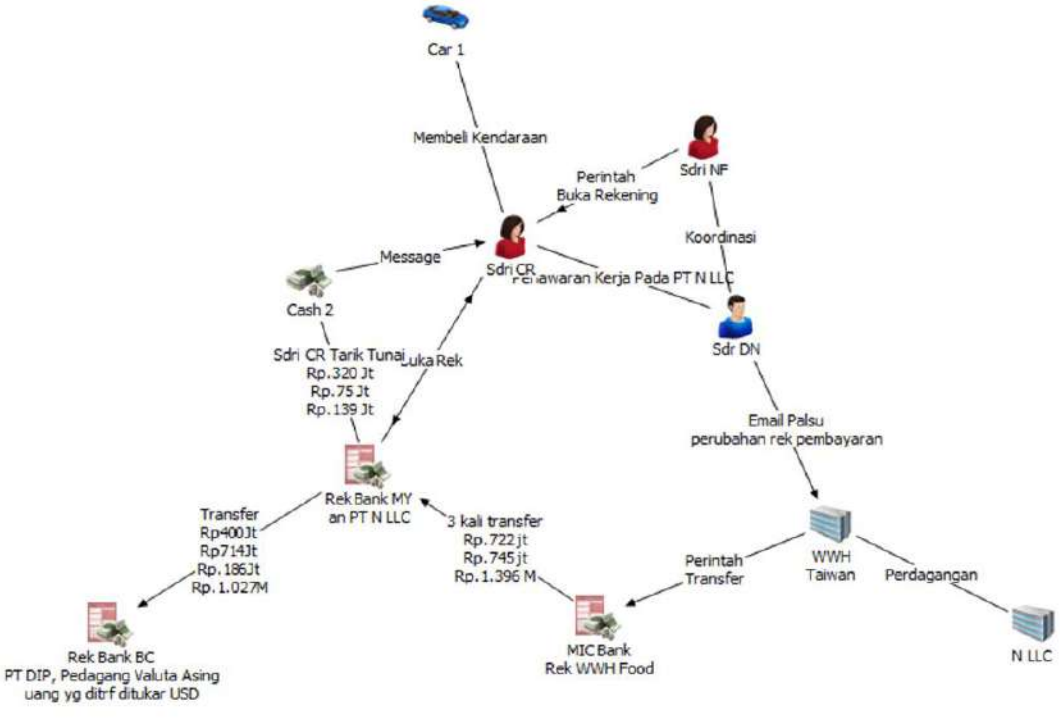
Rek ini sengaja dibuka untuk menampung uang hasil penipuan dari WWH Food Co, Ltd.

- Hasil transaksi penipuan dilakukan penarikan tunai oleh terdakwa dan dilakukan transfer RTGS ke Nomor Rekening atas nama PT DIP (pedagang valuta asing) kemudian ditukar dengan USD dan penarikan uang tunai dalam bentuk Rupiah. Hasilnya diserahkan terdakwa kepada Sdr NF alias Lisa alias Ivon alias Vita, sehingga terdakwa telah melakukan penerimaan pentransferan, melakukan pentransferan, melakukan transaksi mutasi antar rekening yang dimiliki dan atau dikuasai oleh terdakwa dan melakukan penarikan tunai selanjutnya digunakan terdakwa untuk menempatkan lagi, melakukan transfer, melakukan pengalihan, melakukan pembelanjaan, melakukan pembayaran, melakukan hibah, melakukan penitipan, melakukan pengubahan bentuk, melakukan penukaran dengan mata uang atau surat berharga atau berupa perbuatan lainnya atas harta kekayaan sebagaimana uraian diatas dilakukan terdakwa dengan tujuan untuk mengaburkan atau menyamarkan asal usul harta kekayaan diantarnya adanya Pembelian 1 (satu) unit honda jazz berwarna Putih seharga Rp. 185.000.000 (seratus delapan puluh lima juta rupiah) secara tunai dengan Nopol B 10XX UYD. Dalam putusan pengadilan telah diputuskan bahwa 1 (satu) unit mobil Honda Jazz Nopol B 10XX UYD, nomor mesin LI 5Z51014906, nomor rangka : MHRGK5860EJ408990 dan 1 (satu) lembar STNK mobil Honda Jazz Nopol B 10XX UYD a.n.LS; 1 (satu) BPKB nomor : L-09329207 a.n. LS; dikembalikan kepada WWH FOOD CO, Ltd di Taiwan melalui saksi CMK sebagai bentuk *asset recovery*.

Variabel Pembentuk	
Jenis Tindak Pidana	BEC
Peran Pelaku	Money Collector
Profil Pelaku	Wiraswasta
Kelompok Industri	Bank
Produk dan/Jasa	• Transfer dana dalam negeri (Online, SKN, RTGS) • Tarik/ setor tunai • Rekening Tabungan
Pola Transaksi	• Penggunaan nama perusahaan atau perorangan untuk menampung pengiriman uang sehingga seolah-olah nampak seperti transaksi bisnis • Pengoperasian perusahaan cangkang/shell company (perusahaan yang tercatat secara hukum namun tidak terdapat aktivitas, biasanya digunakan untuk menyembunyikan harta dari tindak kejahatan)
Redflag	• Menggunakan perusahaan baru yang namanya sangat mirip dengan nama perusahaan asing dan melakukan pembukaan rekening • Rekening baru dibuka dan memperoleh transfer dana masuk dari luar negeri dalam jumlah signifikan, dengan *underlying transaction* yang tidak jelas • Melakukan pass by setelah dana masuk, melakukan transfer

	kepada pihak lain dan melakukan penarikan tunai
Provinsi	DKI Jakarta
Kawasan Aliran Sumber Dana	Amerika Serikat
Kawasan Tujuan Sumber Dana	-

Skema Kasus

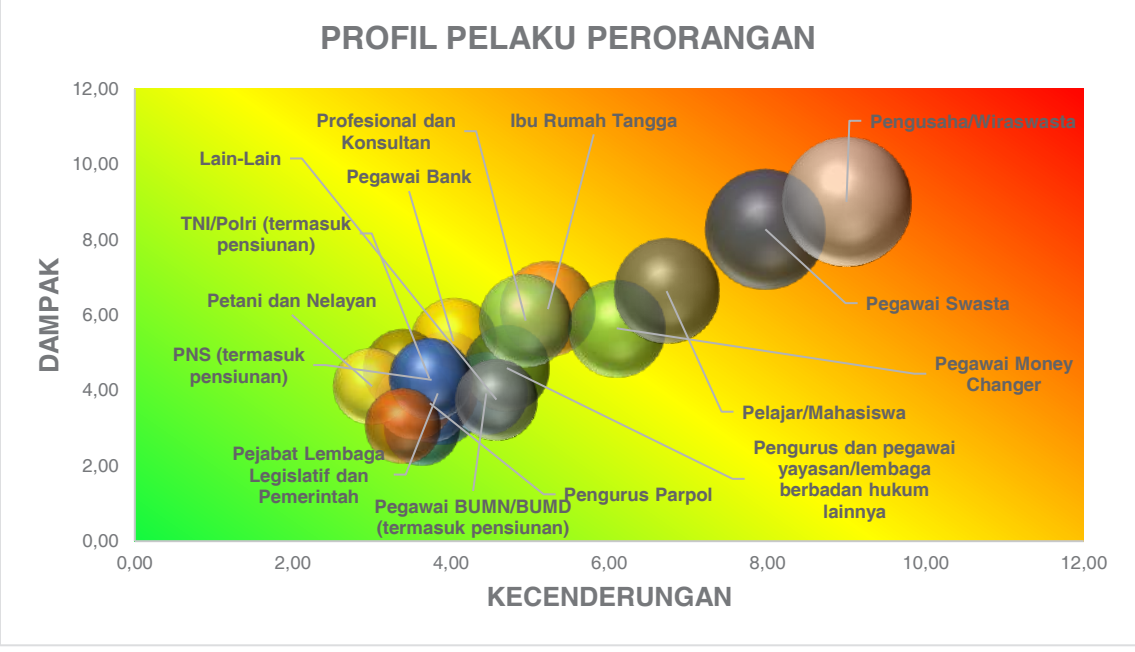


Gambar 4.2 Skema Studi Kasus 1 *(Business Email Compromise)*

Putusan Pengadilan					
No	Putusan Pengadilan	Tindak Pidana	Pasal	Pidana	
				Penjara	Denda
1	Pengadilan Tinggi Jakarta Nomor 351/Pid.Sus/2021/PT DKI	Transfer Dana dan Pencucian Uang	Pasal 85 Undang-Undang RI Nomor 3 Tahun 2011 Tentang Transfer Dana Jo Pasal 55 ayat 1 ke 1 KUHP Pasal pasal 3 Undang-Undang RI Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang jo Pasal 55 ayat 1 ke 1 KUHP	3 tahun	Rp50 Juta dengan subsider pidana kurungan 3 bulan

4.3 TINGKAT RISIKO TPPU BERDASARKAN PROFIL PERORANGAN PELAKU TINDAK PIDANA PENIPUAN SIBER

Hasil penilaian risiko pencucian uang terhadap profil pelaku perorangan diperoleh bahwa pelaku yang **berisiko tinggi** adalah **Pegawai Swasta** dan **Pengusaha/Wiraswasta**.



Gambar 4.3 Peta Risiko menurut Profil Pelaku Perorangan

Hal tersebut didukung dengan faktor ancaman yang cukup tinggi baik dari data penyidikan TP dan TPPU, penuntutan TP dan TPPU serta putusan TPPU, yang ketiga didominasi oleh profil Pengusaha/Wiraswata dan Pegawai Swasta.

Kasus 2 – *Fraudulent Wire Transfer*

Kasus Posisi	Tindak Pidana Asal
• Terdakwa UBN yang berprofesi sebagai wiraswasta mengajak terdakwa LT untuk bergabung melakukan tindak pidana penipuan menggunakan media elektronik melalui aplikasi *whatsapp* (WA). Terdakwa UBN mengajari terdakwa LT cara mengirimkan pesan kepada calon korban melalui WA dan cara penggunaan aplikasi *friend finder tool* yang berfungsi untuk mencari nomor pengguna WA yang berada di luar negeri (Taiwan dan Hong Kong), terdakwa UBN juga mengajari terdakwa LT melakukan pembicaraan terhadap para korban dengan mengaku sebagai petugas Bank X. Untuk dapat meyakinkan calon korban, terdakwa LT mengedit gambar/foto untuk dikirimkan kepada calon korban bahwa pesan yang mereka terima adalah benar. • Selain menggunakan aplikasi WA, terdakwa UBN juga sudah mempersiapkan rekening – rekening yang nantinya akan dipergunakan untuk	• Terdakwa LT mengirim *WhatsApp* ke nomor milik korban dengan isi berita berisi kalimat "selamat ... !!! Nomor SIMCARD ANDA TERPILIH MERAIH CEK SENILAI HKD $ 100.000 dari Bank XX • Terdakwa LT meminta korban untuk menghubungi bagian informasi Bank XX a.n. RDM yang diperankan oleh terdakwa UBN • RDM (terdakwa UBN) meminta korban melakukan transfer sebesar HK $ 1.500 (seribu lima ratus dollar Hong Kong) untuk biaya balik nama sertifikat dari Bank XX ke atas nama korban untuk mendapatkan undian berhadiah tersebut • RDM (terdakwa UBN) mengarahkan korban ke Sigit Purnomo (SP) yang diperankan oleh terdakwa LT dengan mengatakan bahwa korban akan dihubungi oleh SP selaku pegawai Bank XX cabang Hong Kong yang bertanggung jawab atas undian berhadiah yang korban terima • RDM (terdakwa UBN) melalui chat WA menghubungi korban agar menghubungi SP (terdakwa LT). Untuk meyakinkan korban, terdakwa LT mengirimkan gambar identitas palsu • SP (terdakwa LT) meminta korban mengirimkan uang sebesar HK $ 7.000 untuk surat pengantar tanda bukti dengan alasan agar uang undian bisa segera diproses • SP (terdakwa LT) meminta kembali kepada korban untuk mentransfer HK $ 20.000 untuk biaya peliputan dan jasa pengamanan dari

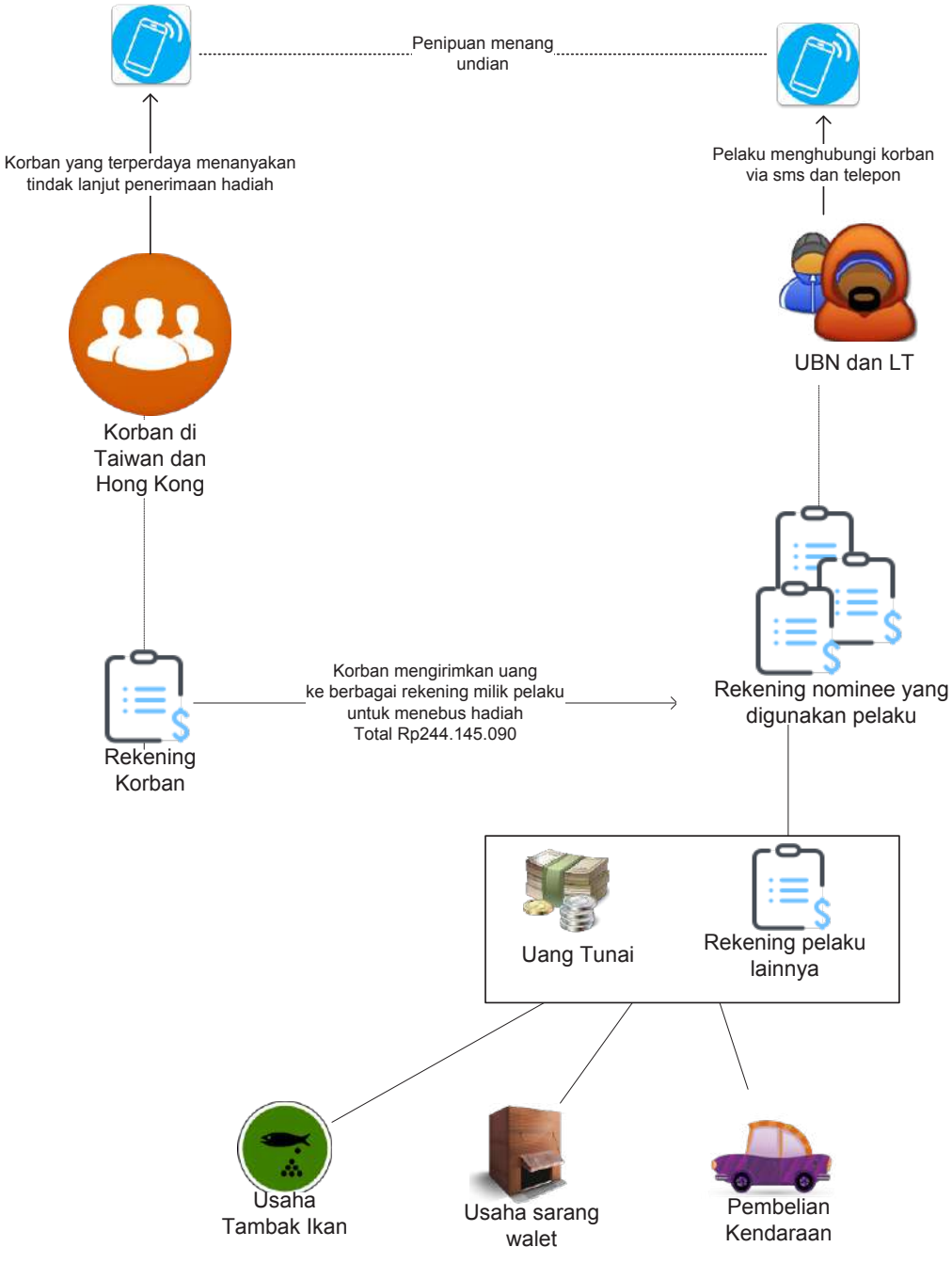
Kasus Posisi	Tindak Pidana Asal
menampung uang yang akan ditransfer oleh para korban dengan cara membeli rekening dari Andi Muklis (AM). Para terdakwa menggunakan modus undian berhadiah dari Bank XX untuk menipu para korban dan meminta korban melakukan transfer sejumlah uang untuk kebutuhan pencairan undian berhadiah, membuat surat perintah jalan, biaya perubahan sertifikat undian berhadiah, biaya dokumentasi, biaya pengawalan dari Kepolisian, dan seterusnya	Kepolisian Hong Kong, namun korban keberatan dan tidak tertarik lagi dengan undian berhadiah tersebut, kemudian korban meminta uangnya yang telah dikirimkan sebesar HK $ 8.500 untuk dikembalikan • RDM (terdakwa UBN) menghubungi korban dan menjelaskan bahwa Bank XX dari Jakarta mengurangi biaya peliputan dan jasa keamanan sebesar HK $ 15.000 dan korban memenuhi permintaan tersebut dengan cara membayar secara bertahap • Setelah korban mengirimkan uang sebesar HK $ 15.000, RDM (terdakwa UBN) dan SP (terdakwa LT) meminta korban untuk membayarkan biaya transportasi sebesar HK $ 1.500, mereka menjelaskan bahwa surat jalan telah kadaluarsa • Terdakwa menjanjikan korban bahwa terdakwa akan ke tempat korban bekerja dan akan memberikan uang hadiah yang korban terima dan akan memberikan uang pengganti surat pengantar tanda bukti undian berhadiah dan uang transport, namun sampai waktu yang ditentukan terdakwa tidak ada kabarnya • Selanjutnya terdakwa kembali menghubungi korban meminta nomor rekening korban untuk mengirimkan uang hadiah, beberapa saat kemudian terdakwa mengirimkan bukti setoran dan menjelaskan bahwa uang hadiah sudah dicairkan dan dikirimkan ke rekening korban. Namun setelah dicek oleh korban, tidak ada transfer sebagaimana bukti setoran tersebut. Kemudian terdakwa

Kasus Posisi	Tindak Pidana Asal
	menghubungi korban menjelaskan bahwa ada kesalahan tanda tangan terkait bukti setoran tersebut dan meminta korban untuk melakukan pembayaran sebesar HK $ 9.000 untuk biaya transfer • Terdakwa UBN dan terdakwa LT melakukan penipuan ke korban – korban lain dengan cara yang kurang lebih sama yakni berupa undian berhadiah dari Bank XX serta berpura – pura sebagai karyawan Bank XX melalui pesan WA • Total kerugian yang dialami para korban akibat perbuatan terdakwa sebesar Rp244.145.090

Tindak Pidana Pencucian Uang
Para terdakwa memiliki banyak rekening atas nama orang lain yang terdakwa beli melalui kenalannya yang digunakan untuk menampung uang yang ditransfer oleh para korban yang berhasil ditipu dengan modus pemenang undian Bank XXX melalui aplikasi WA yang secara fisik bisa digunakan oleh para terdakwa dengan tujuan untuk mengaburkan dari pihak – pihak lain yang ingin melacak perbuatan terdakwa, dimana jika korban telah melakukan pentransferan sejumlah uang ke nomor rekening yang ditentukan, selanjutnya uang yang masuk tersebut langsung ditransfer ke rekening lainnya ataupun ditarik secara tunai Dana dari hasil tindak pidana dipergunakan oleh para terdakwa untuk: • Membuat usaha burung wallet • Membayar cicilan mobil honda jazz warna putih • Membuat usaha tambak ikan • Membeli motor Yamaha mio • Dipergunakan untuk keperluan sehari – hari

Variabel Pembentuk	
Jenis Tindak Pidana	*Fraudulent Wire Transfer*
Peran Pelaku	*Social Engineer*
Profil Pelaku	Pengusaha/Wiraswasta
Kelompok Industri	Bank
Produk dan/Jasa	• Transfer dana dari dan ke luar negeri (Telegraphic Transfer) • Transfer dana dalam negeri (Online, SKN, RTGS) • Tarik/ setor tunai
Pola Transaksi	• Penggunaan rekening nominee: milik orang lain (baik yang dikenal/tidak kenal/fiktif) • Pola transaksi dengan menggunakan uang tunai (Cash Basis): tarik tunai, setor tunai; yang dilakukan untuk menyamarkan identitas • Pembelian aset berupa tanah, bangunan, rumah dan mobil
Redflag	• Rekening baru dibuka menerima sejumlah transfer dana yang berasal dari luar negeri dengan nominal yang signifikan tidak sesuai dengan profil pengguna jasa tanpa underlying yang jelas
Provinsi	Sulawesi Selatan
Kawasan Aliran Sumber Dana	Asia (Taiwan, Hong Kong)
Kawasan Tujuan Sumber Dana	Asia (Indonesia)

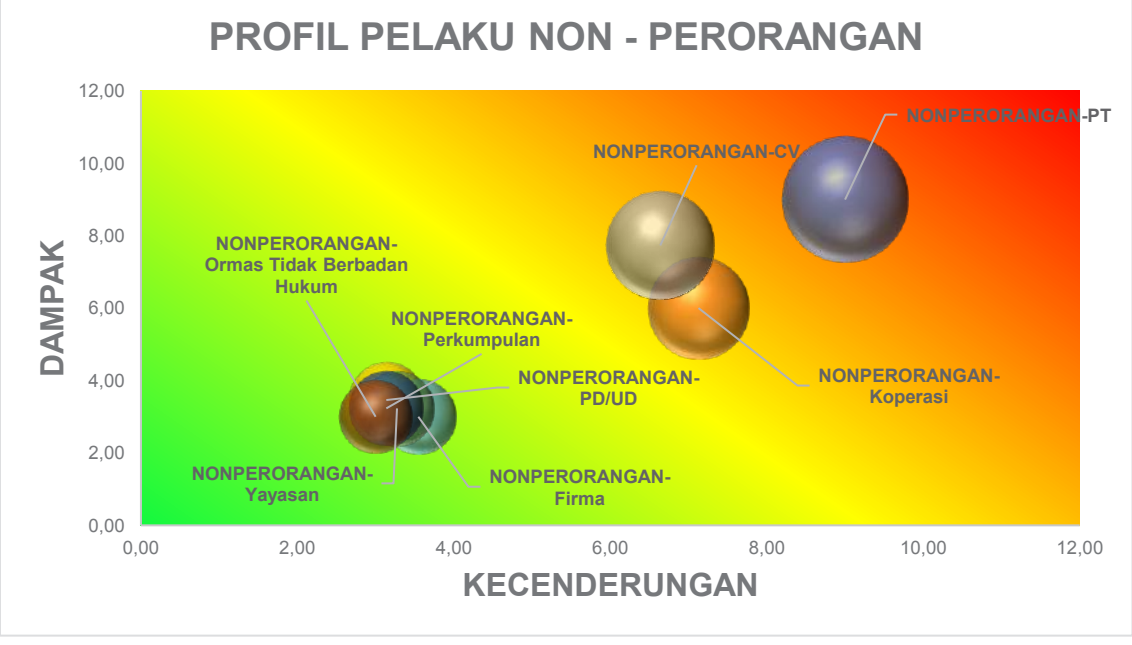
Skema Kasus



Gambar 4.4 Skema Studi Kasus Kasus 2 *(Fraudulent Wire Transfer)*

Putusan Pengadilan					
No	Putusan Pengadilan	Tindak Pidana	Pasal	Pidana	
				Penjara	Denda
1	Pengadilan Negeri Sidenreng Rappang Nomor 29/Pid.Sus/2021/PN Sdr	ITE dan Pencucian Uang	Pasal 45A ayat (1) jo. Pasal 28 ayat (1) UU Nomor 19 Tahun 2016 Pasal 3 jo. Pasal 10 UU Nomor 8 Tahun 2010	4 tahun 8 bulan	Rp1 Miliar dengan subsider pidana kurungan 1 bulan

4.4 TINGKAT RISIKO TPPU BERDASARKAN PROFIL NON-PERORANGAN PELAKU TINDAK PIDANA PENIPUAN SIBER

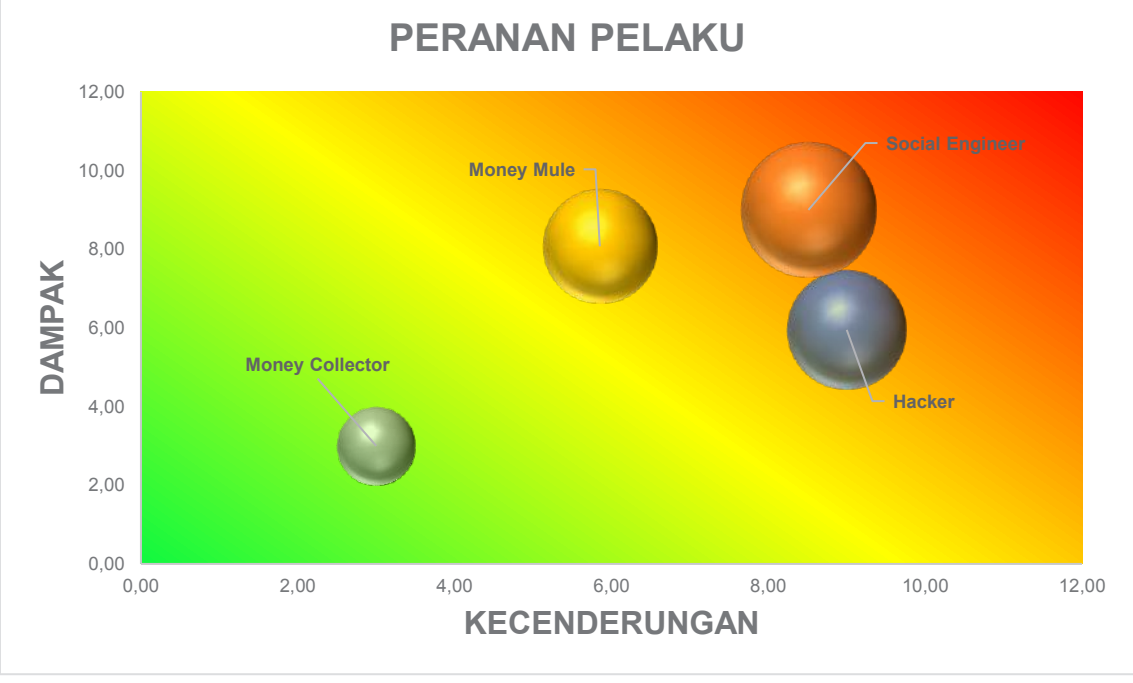


Gambar 4.5 Peta Risiko menurut Profil Pelaku Non - Perorangan

Berdasarkan peta risiko diatas dapat disimpulkan bahwa profil pelaku individu yang memiliki **risiko tinggi** antara lain **Nonperorangan-PT**. Adapun Nonperorangan-CV dan Nonperorangan-Koperasi memiliki risiko menengah.

4.5 TINGKAT RISIKO TPPU BERDASARKAN PERANAN PELAKU TINDAK PIDANA PENIPUAN SIBER

Penilaian tingkat risiko TPPU berdasarkan peranan pelaku tindak pidana penipuan siber dilakukan untuk mengetahui peranan pelaku tindak pidana penipuan siber mana yang paling berisiko tinggi. Penanan pelaku tindak pidana penipuan siber yang perlu dinilai tingkat risikonya dalam kajian ini ditetapkan mencakup 4 (empat) peranan pelaku tindak pidana penipuan siber, yaitu *Hacker, Social Engineer, Money Collector dan Money Mule.* Pengukuran tingkat risiko diperoleh dengan menghitung terlebih dahulu tingkat ancaman (*threat*), kerentanan (*vulnerability*) dan dampak (*consequence*). Ketiga aspek tersebut diukur berdasarkan faktor-faktor pembentuk risiko yang telah ditetapkan sebelumnya.



Gambar 4.6 Peta Risiko menurut Peranan Pelaku

Berdasarkan peta risiko di atas dapat disimpulkan bahwa peranan sebagai ***social engineer*** merupakan peranan pelaku tindak pidana penipuan siber yang memiliki **risiko tinggi**. Selanjutnya *Hacker dan Money Mule* merupakan peranan pelaku tindak pidana penipuan siber yang memiliki risiko menengah. Adapun *money collector* merupakan jenis tindak pidana penipuan siber dengan risiko rendah.

Kasus 3 – *Investment Fraud*

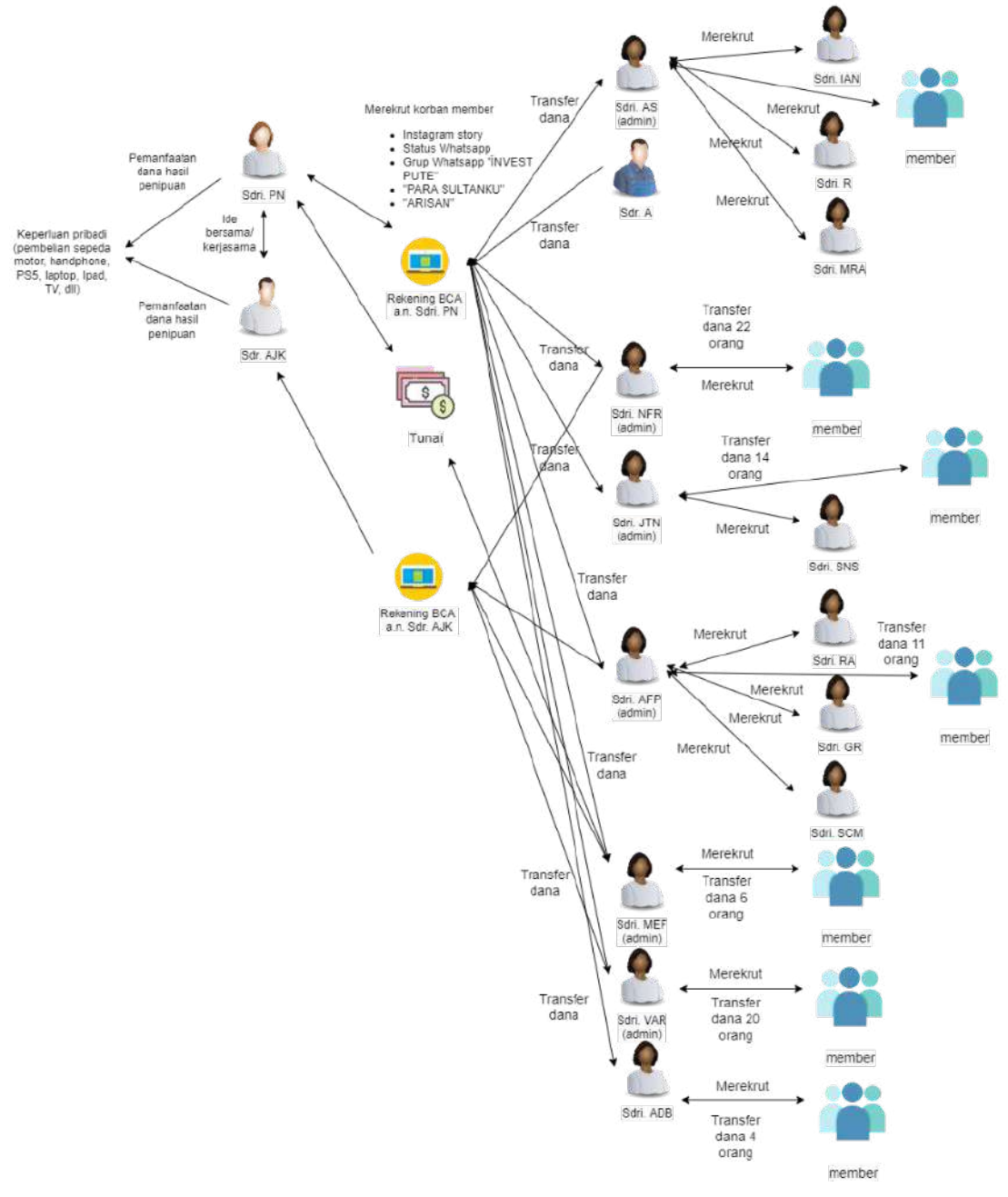
Kasus Posisi	Tindak Pidana Asal
Penawaran investasi dengan keuntungan 75% dengan jangka waktu 20 – 30 hari melalui media sosial hingga memperoleh anggota 300 orang. Kerugian yang ditaksir mencapai Rp845 Juta.	• Awalnya Terdakwa PN menyebarkan informasi elektronik di akun media sosial terdakwa dengan menawarkan investasi yang mempunyai klaim keuntungan 75% dari modal dalam jangka waktu 20 – 30 hari. Terdakwa pun berhasil mengumpulkan anggota hingga 300 orang yang dikumpulkan dalam satu grup media sosial. Di dalam grup tersebut, terdakwa selalu memberikan informasi terkait promo investasi keuntungan 75% dengan jangka waktu 10 sampai 15 hari. Selain itu, untuk meyakinkan para anggota tersebut, terdakwa juga mencantumkan testimoni atas keberhasilan anggota sebelumnya. • Selain menawarkan investasi dengan keuntungan pasti pada jangka waktu tertentu, Terdakwa PN juga memberikan penawaran menarik berupa bonus bonus Rp200 – 300 Ribu jika anggota tersebut dapat merekrut anggota baru yang menginvestasikan dananya senilai Rp2 Juta. • Uniknya untuk menutup kekurangan dana para anggota akibat skema Ponzi ini, beberapa anggota diminta melakukan transfer dana investasi ke rekening milik anggota lainnya atas perintaa. • Atas dasar perbuatan ini, total kerugian yang dialami oleh para korban mencapai Rp845.433.000.

Tindak Pidana Pencucian Uang
Pada putusan ini, kasus perkara pencucian uang belum diputuskan. Namun diketahui tipologi transaksi yang dilakukan dan umumnya dikenali dapat mengarah kepada pencucian uang, yang diantaranya: • Penggunaan rekening pihak ketiga *(nominee).* Terdakwa selain menggunakan rekening miliknya sendiri terdakwa juga menggunakan rekening milik pacar terdakwa. • Penggunaan pihak ketiga untuk pengiriman uang. Terdakwa sempat meminta beberapa anggota untuk melukan pengiriman uang kepada anggota yang lain, yang tujuannya untuk menutupi kekurangan dana. • Uang yang diperoleh terdakwa digunakan untuk pembelian barang – barang mewah dan keperluan pribadi.

Variabel Pembentuk	
Jenis Tindak Pidana	*Investment Fraud*
Peran Pelaku	*Social Engineer, Money Collector*
Profil Pelaku	Pelajar/Mahasiswa
Kelompok Industri	Bank
Produk dan/Jasa	• Transfer dana dalam negeri (Online, SKN, RTGS) • Tarik/ setor tunai
Pola Transaksi	• Penggunaan rekening pihak ketiga *(nominee)*. • Penggunaan pihak ketiga untuk pengiriman uang. • Pembelian barang – barang mewah seperti (lukisan, barang – barang antik, berlian atau barang – barang branded dll).
Redflag	• Transfer dana ditujukan ke rekening personal/pribadi, bukan rekening perusahaan yang terdaftar/ memiliki izin • Transfer dana dilakukan dari/ke lebih dari 1 rekening pengirim/penerima yang tidak memiliki hubungan usaha/ terkait dengan profil

	• Berita transaksi memuat kata-kata “invest”, ïnvestasi” • Pola transaksi yang tidak biasa dengan frekuensi tinggi
Provinsi	Kalimantan Timur
Kawasan Aliran Sumber Dana	Asia
Kawasan Tujuan Sumber Dana	Asia

Skema Kasus



Gambar 4.7 Skema Studi Kasus 3 *(Investment Fraud)*

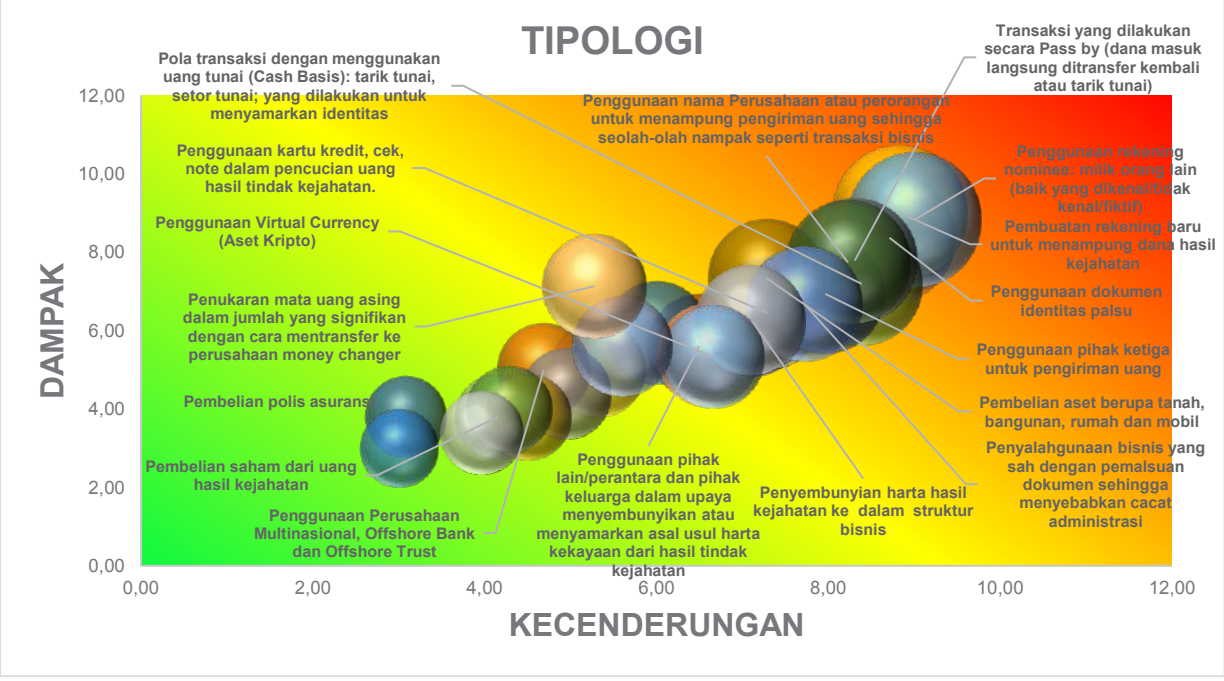
Putusan Pengadilan					
No	Putusan Pengadilan	Tindak Pidana	Pasal	Pidana	
				Penjara	Denda
1	Pengadilan Negeri Balikpapan Nomor 548/Pid.Sus/2021/PN Bpp	ITE dan Penipuan	Pasal 45 A ayat (1) UU Nomor 19 tahun 2016 tentang ITE jo. Pasal 55 ayat (1) ke 1 jo. Pasal 65 ayat (1) KUHPidana Pasal 378 KUHP jo. Pasal 55 ayat (1) ke 1 jo. Pasal 65 ayat (1) KUHPidana dan Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana	4 tahun	Rp250 Juta dengan subsider pidana kurungan 6 bulan

4.6 TINGKAT RISIKO TPPU BERDASARKAN TIPOLOGI PENCUCIAN UANG YANG DIGUNAKAN PELAKU TINDAK PIDANA PENIPUAN SIBER

Berdasarkan peta risiko terkait dengan tipologi pencucian uang dapat disimpulkan bahwa pelaku tindak pidana penipuan siber **berisiko tinggi** melakukan *placement*, *layering* maupun *integration* dengan pola sebagai berikut:

1. transaksi yang dilakukan secara ***Pass by*** (dana masuk langsung ditransfer kembali atau tarik tunai);
2. pola transaksi dengan menggunakan **uang tunai (Cash Basis)**: tarik tunai, setor tunai, yang dilakukan untuk menyamarkan identitas;
3. **pembuatan rekening baru** untuk menampung dana hasil kejahatan;
4. **penggunaan nama Perusahaan atau perorangan** untuk menampung pengiriman uang sehingga seolah-olah nampak seperti transaksi bisnis;
5. **penggunaan rekening *nominee:*** milik orang lain (baik yang dikenal/tidak kenal/fiktif); serta

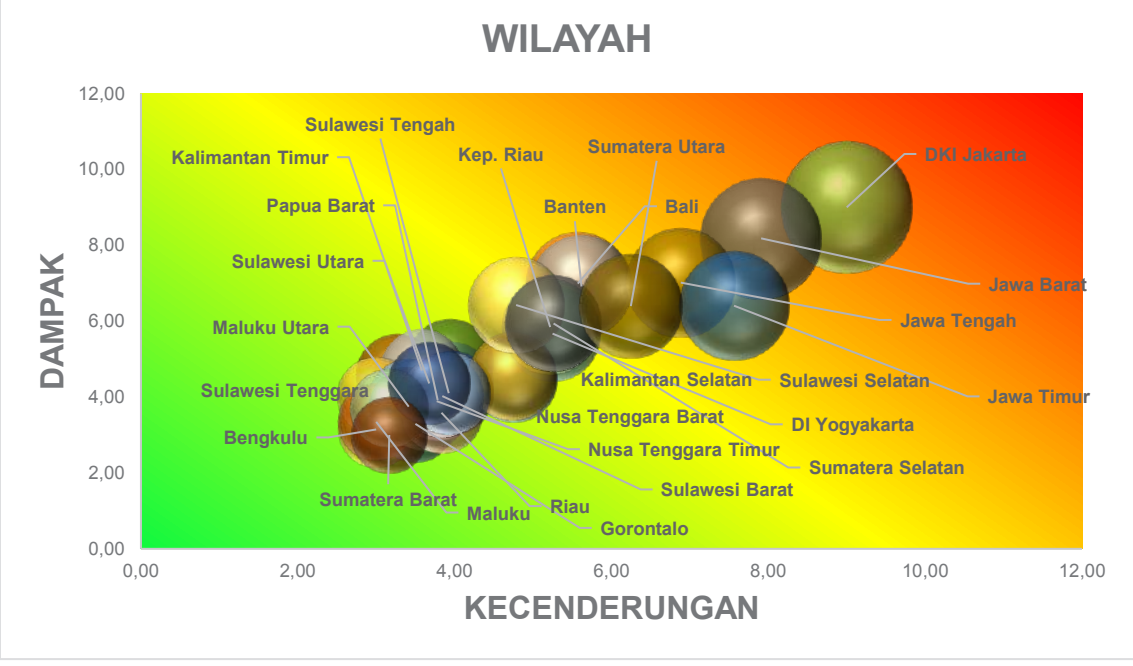
6. penggunaan dokumen **identitas palsu.**



Gambar 4.8 Peta Risiko menurut Tipologi Pencucian Uang

4.7 TINGKAT RISIKO TPPU BERDASARKAN WILAYAH TERJADINYA TINDAK PIDANA PENIPUAN SIBER

Penilaian tingkat risiko TPPU berdasarkan wilayah dilakukan untuk mengetahui di wilayah (provinsi) mana yang paling berisiko tinggi terjadinya kasus TPPU Tindak Pidana Penipuan Siber. Seluruh provinsi di Indonesia menjadi obyek penilaian pada pengkuran tingkat risiko ini.

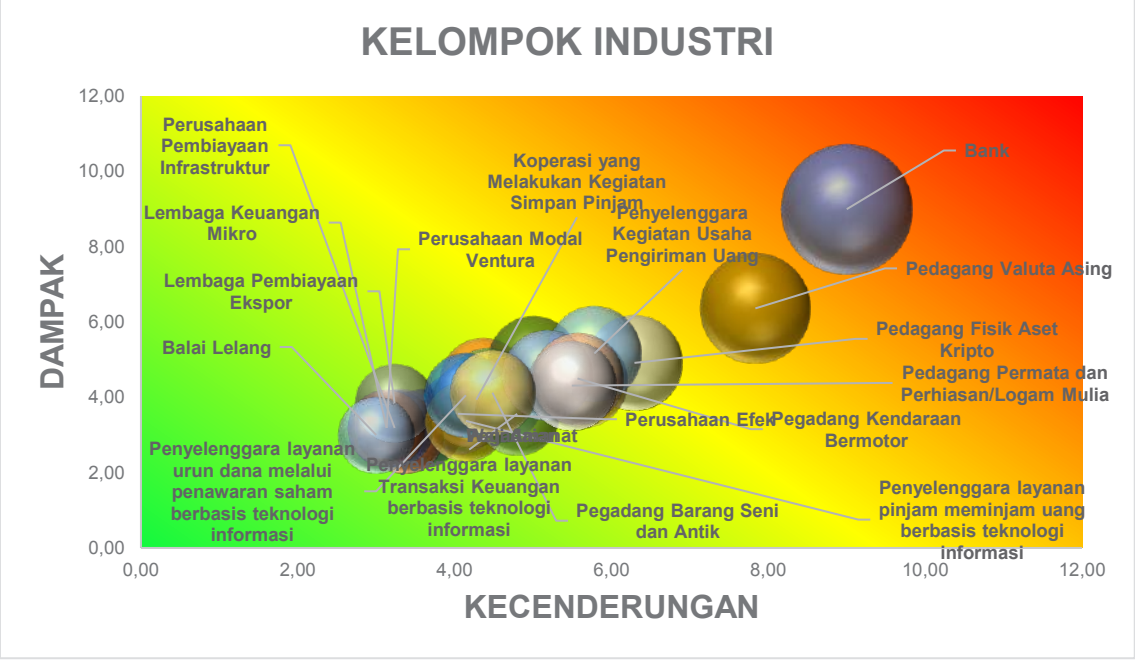


Gambar 4.9 Peta Risiko menurut Wilayah Terjadinya Tindak Pidana

Berdasarkan peta risiko di atas dapat disimpulkan bahwa **Provinsi DKI Jakarta dan Jawa Barat** merupakan wilayah geografis yang memiliki risiko tinggi terjadinya TPPU hasil Tindak Pidana Penipuan Siber. Selanjutnya *Provinsi Jawa Tengah dan Jawa Timur* merupakan wilayah geografis yang memiliki risiko menengah terjadinya TPPU hasil Tindak Pidana Penipuan Siber.

4.8 TINGKAT RISIKO TPPU BERDASARKAN KELOMPOK INDUSTRI YANG DIMANFAATKAN PELAKU TINDAK PIDANA PENIPUAN SIBER

Penilaian tingkat risiko TPPU menurut kelompok industri yang dimaksudkan dalam kajian ini yaitu kelompok industri sebagai sarana yang dimanfaatkan pelaku tindak pidana penipuan siber untuk melakukan pencucian uang.



Gambar 4.10 Peta Risiko berdasarkan Kelompok Industri yang Dimanfaatkan oleh Pelaku

Dari hasil penghitungan risiko diperoleh kelompok industri yang dimanfaatkan oleh pelaku yang **berisiko tinggi** digunakan untuk pencucian uang pada tindak pidana penipuan siber adalah **bank**. Hasil ini didapatkan dari tingginya faktor ancaman, kerentanan dan dampak yang mengakibatkan faktor *likehood* – nya tinggi. Adapun **pedagang valuta asing** memiliki skala **risiko menengah**.

Kasus 4 – *Business Email Compromise*

Kasus Posisi	Tindak Pidana Asal
• Kasus penipuan siber dengan modus BEC ini diinisiasi dari pelaporan Penyedia Jasa Keuangan (PJK) mengenai adanya transaksi mencurigakan yaitu pengambilan dana yang cukup besar dalam kurun waktu 1 hari. Selain itu, setelah dilakukan penelusuran lebih lanjut oleh PJK melalui proses EDD (*Enhance Due Diligence*), perusahaan yang	• Terdakwa LJ diajak dan dipengaruhi oleh oknum yang terdiri dari YS, AL, MS dan MR dengan dalih "pekerjaan pencairan dana". LJ diminta untuk menandatangani dan menyetujui dokumen akta pendirian perusahaan atas nama PT. GSG di kantor Notaris dan PPAT di daerah Bandung tanpa mengetahui isi dari dokumen tersebut. Terdakwa LJ ini kemudian diangkat menjadi Direktur perusahaan tersebut dan mempunyai

Kasus Posisi	Tindak Pidana Asal
didirikan oleh terdakwa adalah perusahaan fiktif. • LJ yang merupakan tukang pijat *online* terlibat kasus BEC (*Bussiness Email Compromise*) dengan WLS, Ltd yang berada di Inggris. Penipuan siber ini melibatkan transfer luar negeri melalui bank asing BOA sebagai bank korespondensi, dengan transfer dari WLS, Ltd kepada PT. GSG, perusahaan yang dibentuk oleh para oknum dengan LJ sebagai salah satu anggotanya. LJ sendiri berkedudukan sebagai Direktur Utama yang mempunyai wewenang penuh dalam menyetujui setiap transaksi keuangan di dalam PT. GSG. Penipuan siber ini merugikan WLS, Ltd sebesar Rp15.455.330.550 dengan *underlying* transaksi perdagangan konveksi atau tekstil fiktif.	kendali penuh atas transaksi yang terjadi di dalamnya. Selain mempunyai akta pendirian perusahaan, PT. GSG juga mempunyai dokumen kelengkapan administrasi seperti Surat Izin Usaha Perdagangan (SIUP), Izin Usaha Industri, Izin Lokasi, pengesahan pendirian dari sistem AHU *Online* Kemenkumham serta Surat Nomor Induk Berusaha (NIB). Namun perusahaan yang didalih bergerak di bidang konveksi dan transaksi tekstil ini, tidak dapat ditemukan eksistensinya dan hanya berbentuk bangunan kosong tanpa adanya identitas nama perusahaan. Selain itu ternyata kantor PT. GSG yang terdaftar pada AHU *Online* Kemenkumham adalah kantor virtual. • Berdasarkan putusan Pengadilan Negeri Bandung, diketahui bahwa PT. GSG ini menerima dana masuk melalui transaksi TT (*Telegraphic Transfer*) dari WLS, Ltd di Inggris melalui bank asing BOA sekitar Rp15 Miliar. Penerimaan dana dari WLS, Ltd ini ternyata diakomodir oleh warga negara Nigeria berinisial CK. Setelah dana masuk ke rekening PT. GSG di Bank MND sebesar kurang lebih Rp15 Miliar, para oknum yang terdiri dari YS, AL, MS dan MR dengan LJ sebagai Direktur pun datang ke Bank MND untuk melakukan penarikan seluruhnya. • Mengingat kantor cabang Bank MND yang didatangi oleh para oknum tersebut

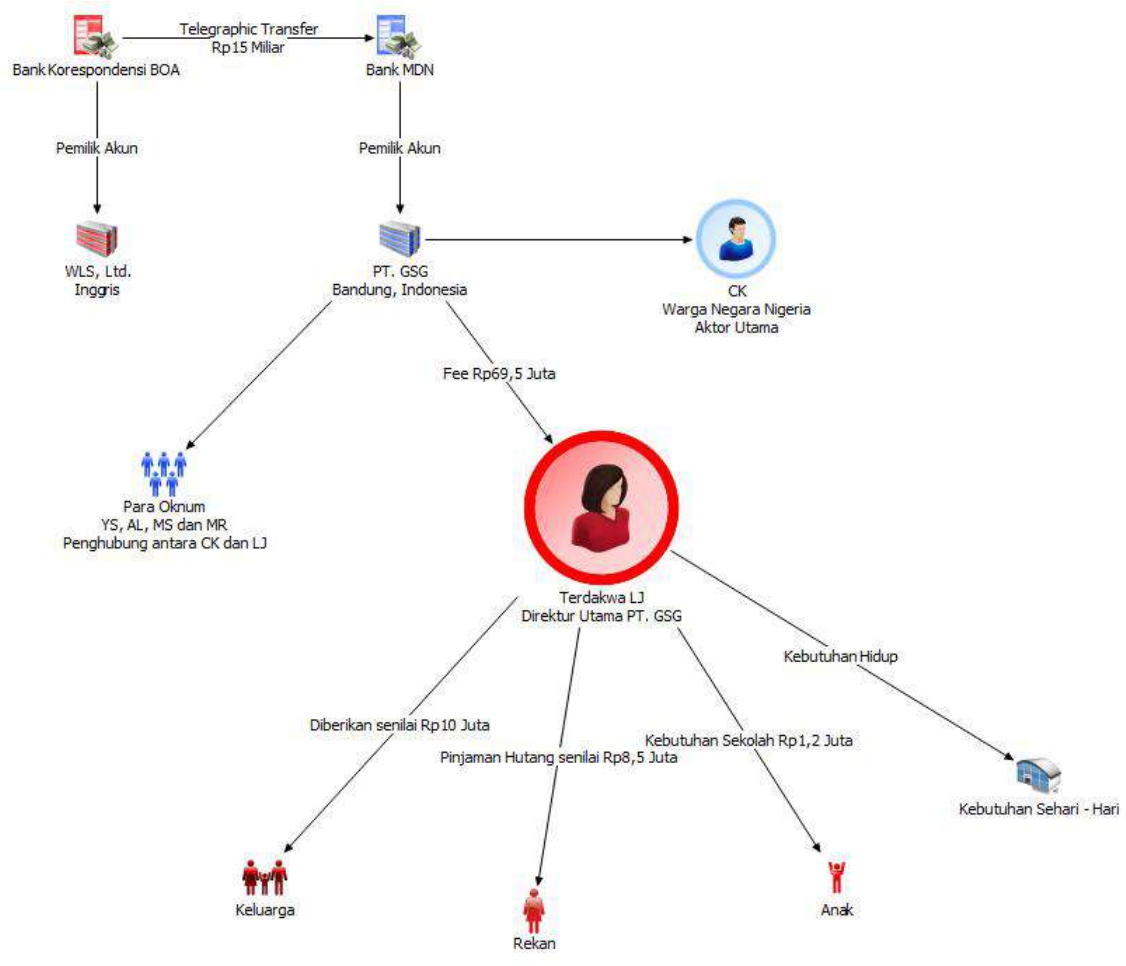
Kasus Posisi	Tindak Pidana Asal
	hanya mempunyai cadangan kas Rp8 Miliar di hari tersebut, maka diputuskan bahwa dana masing – masing Rp1 Miliar ditransfer ke rekening milik orang dan dana Rp6 Miliar dilakukan penarikan tunai. Di hari berikutnya, para oknum berencana untuk melakukan penarikan sisa dana namun tidak dapat dilakukan karena telah dilakukan penundaan transaksi selama 5 hari kerja oleh pihak bank. Hal ini mengingat Bank MND secara aktif melakukan pelaporan kepada Bareskrim POLRI dan PPATK terkait dengan adanya transaksi mencurigakan yaitu pengambilan dana dalam jumlah besar dan diputuskan untuk melakukan penundaan transaksi selama 5 hari kerja. Bank MND pun mengirimkan surat penundaan transaksi ini ke alamat yang tercantum pada identitas PT. GSG namun ternyata pada lokasi tersebut hanya terdapat bangunan kosong. • Pada tindak kejahatan ini, Terdakwa LJ bertugas sebagai Direktur perusahaan yang mempunyai andil dalam persetujuan pencairan dana di Bank MND sementara dalang utamanya termasuk pencarian dana dari luar negeri beserta ide pembentukan perusahaan berasal dari CK, warga negara Nigeria. Untuk para oknum YS, AL, MS dan MR bertugas sebagai penghubung antara perintah CK kepada LJ. Atas perannya

Kasus Posisi	Tindak Pidana Asal
	ini, Terdakwa LJ akan dijanjikan memperoleh komisi sebesar 2% dari total dana yang berhasil dicairkan namun imbalan yang baru diterima sebesar Rp69.500.000. Terdakwa LJ berdalih tidak mengetahui mengenai proses bisnis ataupun wewenang dan tanggungjawabnya di PT. GSG. • Meskipun belum terdapat pengaduan sebagai adanya tindak pidana penipuan dari WLS, Ltd mengenai transfer dana tersebut, Terdakwa LJ didakwa telah melanggar Pasal 85 Undang – Undang Transfer Dana dan Pasal 3 Undang – Undang Pencegahan dan Pemberantasan Pencucian Uang sebagaimana yang tercantum pada putusan Pengadilan Negeri Bandung.

Tindak Pidana Pencucian Uang
• Dari imbalan yang berhasil diterima oleh Terdakwa LJ sebesar Rp69.500.000 tersebut melalui transfer ke rekening terdakwa telah digunakan untuk keperluan sehari – hari yang diantara secara umum untuk: 1. Memberikan uang kepada keluarga dengan total sebesar Rp10.350.000; 2. memberikan kepada teman sebagai pinjaman hutang sebesar Rp8.500.000; 3. pembelian tas seharga Rp800.000; 4. kebutuhan sekolah anak terdakwa Rp1.200.000; serta 5. sisanya untuk kebutuhan keluarga dan biaya hidup. • Dapat dilihat bahwa upaya pencucian uang yang dilakukan oleh terdakwa masih bersifat sederhana. Namun Terdakwa LJ yang berkedudukan sebagai Direktur PT. GSG ini merupakan *materiele dader* dalam tindak pidana ini karena terdakwa telah memiliki niat dan pengetahuan akan adanya transaksi pencairan dana dari luar negeri. Terdakwa juga mengetahui bahwa dalam proses pendirian perusahaan di hadapan notaris diperlukan rekening perusahaan giro sebagai salah satu dasar

pendiriannya, yang selanjutnya digunakan sebagai tempat penampungan penerimaan dana dari WLS, Ltd sebesar Rp15 Miliar. Atas dasar pengetahuan tersebut, terdakwa dianggap memiliki pengetahuan yang cukup untuk mengetahui bahwa dana yang diperoleh adalah dana hasil tindak kejahatan.	
Variabel Pembentuk	
Jenis Tindak Pidana	*Business Email Compromise (BEC)*
Peran Pelaku	*Money Collector*
Profil Pelaku	Pengusaha/Wiraswasta
Kelompok Industri	Bank
Produk dan/Jasa	• Transfer dana dari dan ke luar negeri (Telegraphic Transfer) • Transfer dana dalam negeri (Online, SKN, RTGS) • Tarik/ setor tunai
Pola Transaksi	• Penggunaan nama Perusahaan atau perorangan untuk menampung pengiriman uang sehingga seolah – olah nampak seperti transaksi bisnis • Pengoperasian perusahaan cangkang/shell company (perusahaan yang tercatat secara hukum namun tidak terdapat aktivitas, biasanya digunakan untuk menyembunyikan harta dari tindak kejahatan)
Redflag	• Penarikan uang tunai dan transfer uang yang cukup masif dalam satu hari dari perusahaan yang baru didirikan • Rekening korporasi baru langsung menerima dana masuk yang cukup besar dari luar negeri
Provinsi	Jawa Barat
Kawasan Aliran Sumber Dana	Eropa
Kawasan Tujuan Sumber Dana	Asia

Skema Kasus



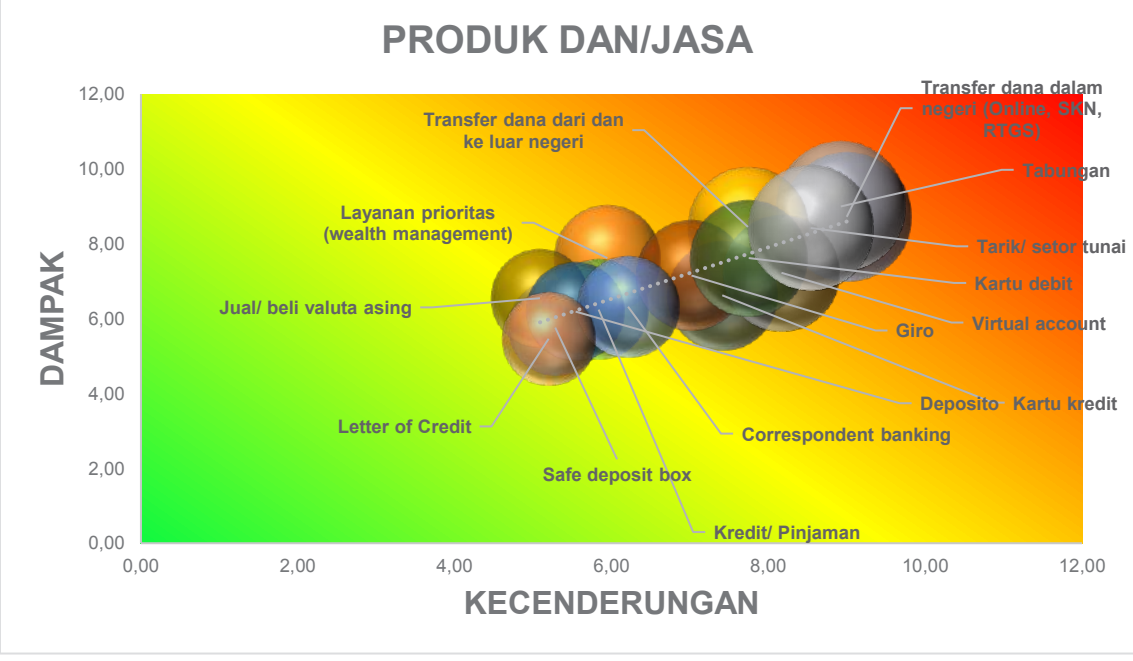
Gambar 4.11 Skema Studi Kasus 3 *(Business Email Compromise)*

Putusan Pengadilan

No	Putusan Pengadilan	Tindak Pidana	Pasal	Pidana	
				Penjara	Denda
1	Pengadilan Negeri Bandung Nomor 913/Pid.B/2021/PN. Bdg	Transfer Dana dan Pencucian Uang	Pasal 85 Undang – Undang Nomor 3 Tahun 2011 tentang Transfer Dana Jo. Pasal 55 Ayat (1) ke – 1 KUHPidana Pasal 3 Jo Pasal 10 Undang – Undang	3 tahun 6 bulan	Rp500 Juta dengan subsider pidana kurungan 3 bulan

No	Putusan Pengadilan	Tindak Pidana	Pasal	Pidana	
				Penjara	Denda
			Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Pencucian Uang		

4.9 TINGKAT RISIKO TPPU BERDASARKAN PRODUK DAN/ATAU JASA YANG DIGUNAKAN OLEH PELAKU



Gambar 4.12 Peta Risiko Berdasarkan Produk dan/atau Jasa yang Digunakan oleh Pelaku

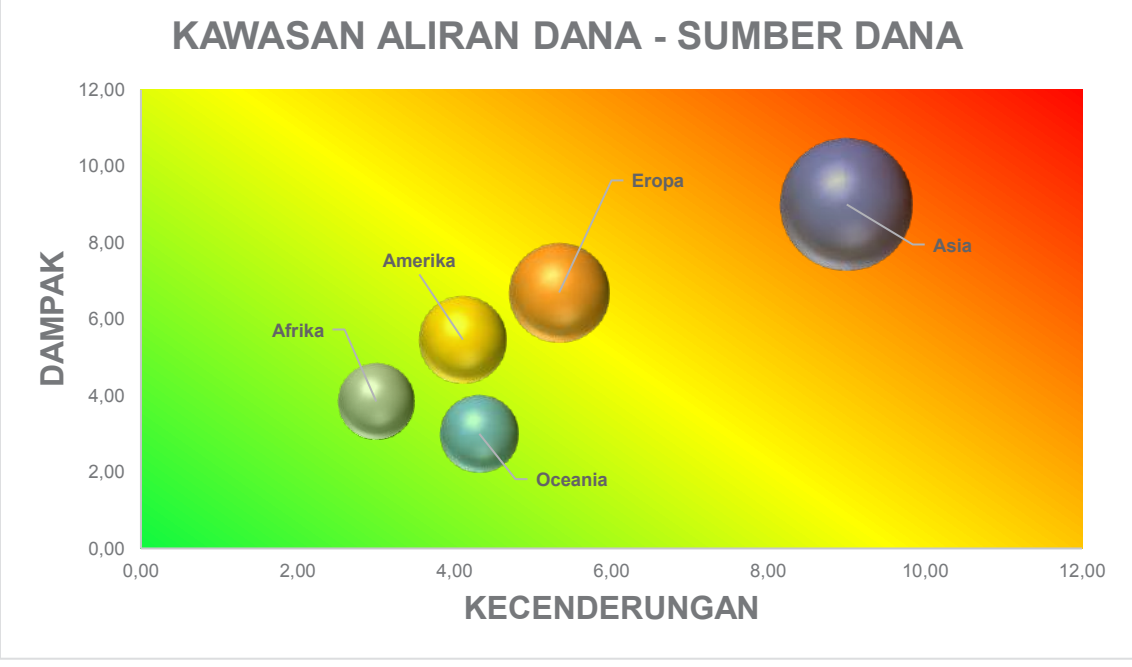
Dari hasil penghitungan risiko diperoleh bahwa produk dan/jasa yang ditawarkan oleh Pihak Pelapor yang rawan digunakan untuk pencucian uang pada tindak pidana penipuan siber adalah **transfer dana dalam negeri (Online, SKN, RTGS), tabungan, transfer dana dari dan ke luar negeri, *virtual account*, kartu debit serta tarik/setor tunai**. Hasil ini didukung dengan tingginya faktor ancaman, kerentanan dan dampak yang mengakibatkan faktor *likehood* – nya tinggi. Pada penilaian risiko ini, Tim melakukan penghimpunan juga data dari pihak pelapor yang terdiri dari data aduan masyarakat dan data transaksi (data yang pernah dilaporkan sebagai LTKM, data yang pernah diminta oleh Lembaga Penegak Hukum ataupun Analis) terkait tindak pidana

penipuan siber. Total nominal data aduan dan transaksi yang diberikan oleh pihak pelapor dari 2018 hingga 2021 pada 6 jenis produk dan/jasa tertinggi tersebut mencapai Ro5,5 Triliun dari total Rp6,7 Triliun atau mencapai 81,6% secara keseluruhan. Hal ini pun sejalan nominal Hasil Analisis yang dilakukan PPATK mencapai 99,2% dan hasil putusan Pengadilan mencapai 98,6% secara keseluruhan pada kurun waktu yang sama.

Jual beli valuta asing memiliki skala risiko menengah, hal ini sejalan dengann skala risiko Pedagang Valuta Asing yang memiliki skala risiko menengah dalam pemanfaatan sebagai sarana pencucian uang oleh pelaku tindak pidana penipuan siber.

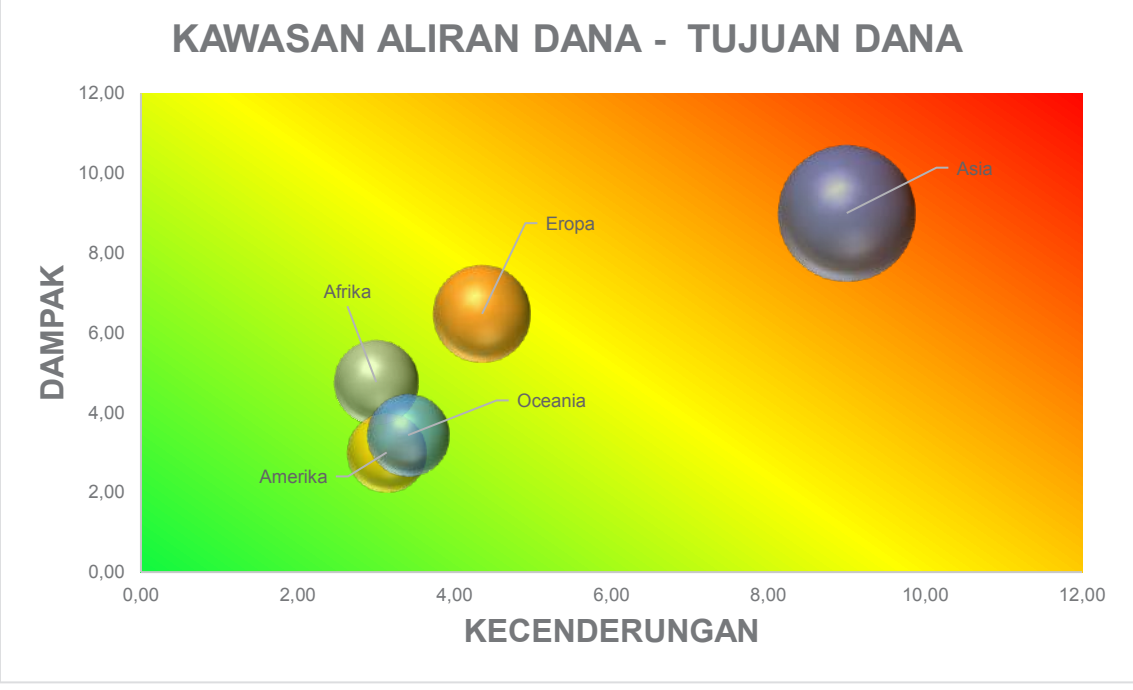
4.10 TINGKAT RISIKO TPPU BERDASARKAN ALIRAN DANA TINDAK PIDANA PENIPUAN SIBER

Penilaian tingkat risiko TPPU berdasarkan aliran dana dilakukan untuk mengetahui negara mana yang cenderung menjadi tujuan dana TPPU dari Indonesia, dan negara sumber dana Tindak Pidana Penipuan Siber. Pengukuran tingkat risiko berdasarkan aliran dana diperoleh dengan menghitung terlebih dahulu tingkat ancaman (*threat*), kerentanan (*vulnerability*) dan dampak (*consequence*). Ketiga aspek tersebut diukur berdasarkan faktor-faktor pembentuk risiko yang telah ditetapkan sebelumnya.



Gambar 4.13 Peta Risiko berdasarkan Kawasan Aliran Dana – Sumber Dana Tindak Pidana

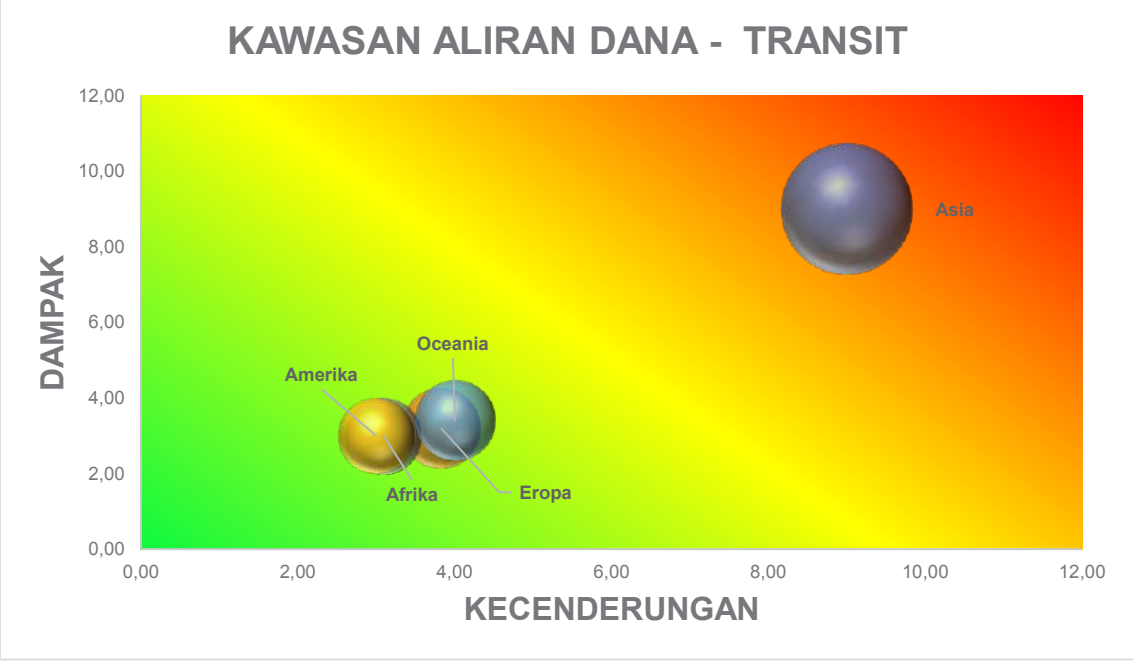
Berdasarkan peta risiko di atas dapat disimpulkan bahwa **Kawasan Asia** merupakan kawasan yang memiliki **risiko tinggi menjadi target** pelaku Tindak Pidana Penipuan Siber. Hal ini sejalan dengan jumlah penyidikan, jumlah penuntutan, jumlah putusan dan total nominal kerugian paling besar merupakan dari negara-negara di Kawasan Asia yang diantaranya adalah Korea Selatan, Singapura, Taiwan, Hongkong dan Indonesia. Adapun transaksi dengan nominal paling signifikan berasal dari Yunani dan Singapura.



Gambar 4.14 Peta Risiko berdasarkan Kawasan Aliran Dana – Tujuan Dana Tindak Pidana

Selanjutnya sebagai **kawasan tujuan pencucian uang** hasil tindak pidana penipuan siber **Kawasan Asia** juga memiliki **risiko tinggi,** hal ini terkait dengan uang hasil tindak pidana kejahatan siber dilakukan pencucian uang di Indonesia dan beberapa diantaranya dikirim ke luar negeri ke negara – negara di Kawasan Asia, yang diantaranya Indonesia, Tiongkok, Singapura, Hongkong, Uzbekistan dan Korea Selatan. Adapun negara tujuan dengan nominal transaksi paling signifikan adalah Nigeria dan Uzbekistan.

Sementara itu, untuk kawasan transit aliran tindak pidana tergambarkan pada peta risiko berikut:



Gambar 4.15 Peta Risiko berdasarkan Kawasan Aliran Dana – Transit Dana Hasil Tindak Pidana

Berdasarkan peta risiko di atas dapat disimpulkan bahwa **Kawasan Asia** merupakan kawasan yang memiliki **risiko tinggi** menjadi kawasan transit pelaku Tindak Pidana Penipuan Siber. Hal ini diperoleh berdasarkan tingginya hasil pengukuran faktor ancaman, kerentanan dan dampak yang telah dilakukan dari sumber data yang dimiliki.

BAB V
KESIMPULAN, REKOMENDASI DAN *REDFLAG*

5.1 KESIMPULAN

Berdasarkan hasil identifikasi dan analisis faktor ancaman, kerentanan dan dampak, serta risiko penipuan siber, maka dapat disimpulkan sebagai berikut:

1. Sebagai wujud pelaksanaan tindak lanjut atas hasil NRA 2021 serta dalam rangka peningkatan pencegahan dan pemberantasan tindak pidana pencucian uang melalui penilaian risiko secara sektoral khususnya terkait dengan penipuan siber
2. Penilaian risiko penipuan siber tahun 2022, merupakan langkah penting dan relevan untuk merespon perkembangan dan dinamika tingkat nasional mengenai upaya pencegahan dan pemberantasan tindak pidana pencucian uang. Pemahaman bersama tentang risiko penipuan siber oleh para pemangku kepentingan dalam rezim anti pencucian uang di Indonesia sangat penting dalam menentukan arah, kebijakan, dan strategi mitigasi yang efektif dan terus memperbaharui pemahaman nasional seiring dengan semakin kompleknya kejahatan penipuan siber.
3. Penyusunan penilaian risiko penipuan siber yang dilakukan untuk memetakan pengetahuaan dan pengalaman dari berbagai elemen rezim anti pencucian uang seperti pihak pelapor (PP), Lembaga Pengawas dan Pengatur (LPP), Lembaga Penegak Hukum dan stake holder lainnya di Indonesia. Pendekatan metodologi merujuk pada konsep utama yaitu ancaman, kerentanan, dan dampak dalam menghitung dan menganalisis tingkat risiko penipuan siber berdasarkan karakteristik, profil, wilayah, sektor industi, tipologi dan produk/ jasa.
4. Berdasarkan pemahaman dari para stakeholder yang terdiri dari Lembaga Pengawas dan Pengatur, Lembaga Penegak Hukum serta Stakeholder lainnya, maka tantangan yang dihadapi dalam pencegahan dan pemberantasan penipuan siber:
    a. Rumitnya aliran dana serta semakin maraknya penggunaan modus operandi seperti BEC dan investment fraud dari tindak pidana penipuan siber sehingga menyulitkan penyidik dalam untuk menelusuri aliran uang dari tindak pidana.
    b. Penggunaan aset kripto yang memutus mata rantai penyidikan sebab tidak bisa dilakukannya penelusuran transaksi pada aset kripto tersebut jika sudah wallet.
    c. Kesulitan pelacakan pelaku sebenarnya/ultimate Beneficial Owner (BO) karena tipologi yang digunakan dan melibatkan jaringan internasional.

d. Masih maraknya modus tipologi yang menggunakan dokumen identitas palsu yang teregistrasi sehingga diperlukan kerjasama dengan berbagai stakeholders dan membutuhkan waktu yang cukup lama.
e. Implementasi penyidikan TPPU untuk TP Penipuan Siber terutama penyidik Sektor Jasa Keuangan sebagai hasil uji materiil Mahkamah Konstitusi Nomor 15 Tahun 2021 (tertanggal 29 Juni 2021) untuk Penjelasan Pasal 74 UU Nomor 8 2010 masih dalam proses implementasi awal (penyiapan infrastuktur).
f. Penuntut terutama di daerah terpencil belum memiliki pemahaman yang seragam dalam penanganan TPA Penipuan Siber dan TPPU sehingga seringkali penuntutan hanya mengarah kepada penipuan konvensional.
g. Jaksa Penuntut masih kesulitan dalam proses pengembalian kerugian terutama untuk kerugian yang melibatkan pihak ketiga sebab uang hasil tindak pidana telah habis digunakan oleh pelaku untuk keperluan konsumtif.
h. Dalam penanganan kasus Penipuan Siber sering kali terjadi perbedaan persepsi antara hakim dan penuntut terkait pembuktian TPPU.
i. Dalam kasus BEC, Invesment Fraud, Romance Scams dan Fraudulent Wire Transfer umumnya melibatkan banyak yurisdik namun waktu retensi penyelesaian kasus sangat singkat sementara proses MLA yang formal memerlukan waktu yang relatif panjang, terutama untuk pengejaran aset – aset dari pelaku tindak pidana yang tersimpan di luar negeri ataupun untuk pelaku utama yang telah kabur ke luar negeri.
j. Kemudahan pembuatan domain situs web yang dimanfaatkan oleh pelaku Penipuan Siber.

5. Berdasarkan hasil analisis risiko penipuan siber dapat diketahui hal-hal sebagai berikut:
   a. Berdasarkan penilaian jenis/ karakteristik penipuan siber, diketahui bahwa BEC dan *Investment Fraud* merupakan jenis/ karakteristik penipuan siber yang berisiko tinggi.
   b. Berdasarkan penilaian profil pelaku perseorangan penipuan siber, diketahui bahwa pegawai swasta dan pengusaha/ wiraswasta merupakan profil penipuan siber yang berisiko tinggi.
   c. Berdasarkan penilaian profil pelaku non perseorangan penipuan siber, diketahui bahwa Perseroan Terbatas (PT) merupakan profil penipuan siber yang berisiko tinggi.

d. Berdasarkan penilaian pernanan pelaku penipuan siber, diketahui bahwa social enginer merupakan peranan pelaku penipuan siber yang berisiko tinggi.
e. Berdasarkan penilaian tipologi penipuan siber, yang berisiko tinggi adalah (1) penggunaan dokumen identitas palsu; (2) pembuatan rekening baru untuk menampung dana hasil kejahatan; (3) penggunaan rekening nominee: milik orang lain (baik yang dikenal/tidak kenal/fiktif); (4) pola transaksi dengan menggunakan uang tunai (Cash Basis): tarik tunai, setor tunai yang dilakukan untuk menyamarkan identitas; (5) transaksi yang dilakukan secara Pass by (dana masuk langsung ditransfer kembali atau tarik tunai) serta (6) penggunaan nama Perusahaan atau perorangan untuk menampung pengiriman uang sehingga seolah-olah nampak seperti transaksi bisnis
f. Berdasarkan penilaian wilayah penipuan siber, diketahui bahwa DKI Jakarta dan Jawa Barat merupakan wilayah penipuan siber yang berisiko tinggi.
g. Berdasarkan penilaian kelompok industri yang digunakan dalam penipuan siber, diketahui bahwa bank merupakan sektor industri penipuan siber yang berisiko tinggi.
h. Berdasarkan penilaian produk dan/atau jasa yang dimanfaatkan dalam penipuan siber diketahui bahwa (1) transfer dana dalam negeri (Online, SKN, RTGS); (2) tabungan; (3) transfer dana dari dan ke luar negeri; (4) virtual account; (5) kartu debit; (6) tarik/setor tunai
i. Berdasarkan penilaian aliran sumber dana yang digunakan dalam penipuan siber, diketahui bahwa kawasan Asia merupakan kawasan yang berisiko tinggi.
j. Berdasarkan penilaian aliran tujuan dana yang digunakan dalam penipuan siber, diketahui bahwa kawasan Asia merupakan kawasan yang berisiko tinggi.
k. Berdasarkan penilaian aliran dana transit yang digunakan dalam penipuan siber, diketahui bahwa kawasan Asia merupakan kawasan yang berisiko tinggi.

5.2 REKOMENDASI

Berdasarkan penilaian atas ancaman, kerentanan, dampak serta risiko penipuan siber, maka dapat direkomendasikan strategi mitigasi risiko yang telah dihasilkan:

Tabel 5.1 Strategi Mitigasi Risiko yang Direkomendasikan

No	Strategi Mitigasi	Jangka Waktu	Pihak Terkait
Strategi Pencegahan			
1	Pengetatan pendaftaran perusahaan dengan menggunakan nama dan kode legalitas perusahaan luar negeri (Ltd, BHD) sebab kasus BEC banyak memanfaatkan kemiripan nama perusahaan asing dalam transaksi keuangan.	Menengah	Kementerian Hukum dan Ham
2	Pembentukan watchlist jaringan pelaku tindak pidana siber terutama untuk individu yang melakukan registrasi perusahaan berulang kali.	Pendek	Kementerian Hukum dan HAM, Penegak Hukum
3	Diperlukan penyusunan pedoman teknis terkait identifikasi dan verifikasi identitas pengurus perusahaan yang tidak sesuai profil dan/atau palsu.	Pendek	LPP
4	Perlu adanya tindakan preventif salah satunya meningkatkan literasi kepada masyarakat terkait karakteristik jenis penipuan siber (BEC, Investment Fraud, Fraudulent Wire Transfer, Romance Scam), modus operandi (terutama bahaya jual beli rekening) dan cara penanggulangannya baik secara langsung maupun memanfaatkan program masing – masing regulator.	Pendek	LPP, Lembaga Penegak Hukum
5	Internalisasi *redflag* tindak pidana penipuan siber kepada pihak pelapor untuk meningkatkan jumlah pelaporan	Pendek	LPP

No	Strategi Mitigasi	Jangka Waktu	Pihak Terkait
	dan mitigasi aliran dana hasil kejahatan		
6	Sektor Jasa Keuangan melakukan peningkatan verifikasi terhadap profil dengan transaksi nasabah (incoming dan outgoing transfer) dan jual beli valuta asing dengan lebih seksama	Pendek	OJK, Bank Indonesia dan Penyedia Jasa Keuangan
7	Penerapan pengawasan tematik terhadap wire transfer dan bank koresponden oleh PJK khususnya perbankan sebagai internal control untuk mengantisipoasi transfer dana yang cukup cepat dan lintas batas.	Menengah	LPP
8	Peningkatan infrastuktur pendukung dalam penyidikan TP Penipuan Siber seperti pembentukan big data yang dapat diakses oleh stakeholders terkait (OJK, Bappebti, Kemenkumham dan Kominfo dll) dalam proses verifikasi dan identifikasi data perorangan maupun non perorangan.	Panjang	LPP, Stake Holder, Lembaga Penegak Hukum
9	Perlunya keterlibatan sektor industri selain bank seperti PBJ kendaraan dan barang mewah untuk pendeteksian dini indikasi penipuan terkait produk-produk investasi.	Pendek	LPP
10	Mendorong percepatan RUU Pembatasan Transaksi Uang Kartal	Pendek	Bank Indonesia dan PPATK
Strategi Pemberantasan			
11	Perlunya penyeragaman pemahaman Penuntut Umum dan Hakim dalam	Pendek	Lembaga Penegak Hukum

No	Strategi Mitigasi	Jangka Waktu	Pihak Terkait
	mempertajam analisis terhadap anatomi karakteristik Tindak Pidana Penipuan Siber dan pembuktian TPPU.		
12	Perlu adanya pedoman untuk pemulihan aset atas hasil kejahatan siber (*asset tracing* hingga perampasan dan pengembalian aset). Sebagai contoh, dalam kasus penipuan investasi, pelaporan ke penyidik bukan lagi dilakukan per individu, namun dalam naungan kelompok	Pendek	LPP, Lembaga Penegak Hukum dan *Stakeholders*
13	Memaksimalkan pemidanaan pelaku kejahatan penipuan siber termasuk pelaku TPPU yang tidak secara langsung terlibat ke tindak pidananya (seperti *social engineer* dan *money mules*) terkait 3 jenis pencucian uang (*stand-alone money laundering, self laundering*, *third party money laundering*) agar memberikan efek jera kepada para pelaku.	Pendek	Lembaga Penegak Hukum
Strategi Kerjasama			
14	Peningkatan sosialiasi kepada Lembaga Penegak Hukum terkait Peraturan PPATK Nomor 15 Tahun 2021 mengenai Permintaan Informasi kepada PPATK dalam rangka pencepatan proses penanganan perkara tindak pidana penipuan siber	Pendek	PPATK

No	Strategi Mitigasi	Jangka Waktu	Pihak Terkait
	yang sangat cepat perpindahan dananya.		
15	Penyusunan *first draft* formalisasi akses pertukaran data dan informasi kependudukan untuk deteksi dini identitas palsu melalui MoU dan PKS antara OJK – Dukcapil, BAPPEBTI – Dukcapil, dan KemenkopUKM – Dukcapil. PKS tersebut diantaranya adalah: • Akses data dukcapil diperluas ke Kartu Keluarga agar bisa mengetahui pihak terkait dalam hal asset tracing. • Akses data AHU berbayar per akses, supaya lebih efisien agar akses data tersebut menggunakan mekanisme *membership fee* yg tidak memberatkan pihak pelapor.	Pendek	LPP, Penegak Hukum, Pihak Pelapor dan *Stakeholders* lainnya
16	Penambahan kerjasama PPP (*Public Private Partnership*) terkait jenis penipuan siber *Investment Fraud* yang kemudian diimplementasikan ke dalam *redflag*.	Pendek	PPATK, LPP, Lembaga Penegak Hukum dan Pihak Pelapor
17	Perluasan kerjasama MLA dengan yurisdiksi berisiko tinggi hasil penilaian SRA Penipuan Siber Tahun 2022 untuk mengejar aset – aset yang terdapat di luar negeri ataupun tersangka yang telah kembali ke negara asal.	Panjang	Kementerian Hukum dan HAM

No	Strategi Mitigasi	Jangka Waktu	Pihak Terkait
18	Perlu adanya pembentukan wadah atau gugus tugas yang khusus menangani Tindak Pidana Penipuan Siber diantaranya 12 Kementerian/Lembaga (yang tergabung dalam SWI) serta Perusahaan Aplikasi Jasa Pembayaran, *market place* dalam rangka penanganan investment fraud serta peningkatan cyber patrol.	Panjang	Komite TPPU
19	Pelibatan Interpol dalam penanganan Tindak Pidana Penipuan Siber yang bersifat lintas yurisdiksi.	Pendek	Lembaga Penegak Hukum
20	Pembentukan membership untuk keringanan akses data berbayar (PNBP) atas data BO dan AHU yang melibatkan Kemenkumham, LPP, dan Dirjen Perbendaharaan.	Menengah	Kementerian Hukum dan HAM

Sementara itu, berikut adalah *redflag* yang terbentuk dari analisis transaksi keuangan yang berhasil disusun:

- Transaksi melibatkan perusahaan fiktif yang namanya mirip dengan perusahaan asing dengan indikasi menggunakan dokumen asli tapi palsu dengan alamat tempat usaha fiktif. Perusahaan tersebut adalah perusahaan cangkang (*shell company*) baru berdiri dan melakukan pembukaan rekening;
- transaksi Pengguna Jasa yang terkait dengan usaha menggunakan rekening perorangan (pemilik/pengurus/pegawai) sebagai *nominee*;
- rekening pengguna jasa digunakan untuk menampung dana dari banyak pihak lalu ditransfer ke rekening pihak yang terkait kasus investasi ilegal;
- pengguna Jasa tiba-tiba melakukan pengiriman dan penerimaan uang dalam jumlah besar melebihi kebiasaannya dari dan ke berbagai negara tanpa adanya *underlying* transaksi yang jelas;

- keterangan transaksi pada rekening individu dominan mencirikan penghimpunan dana masyarakat;
- pola transaksi pengguna jasa terutama nasabah non – perorangan (korporasi) tidak sesuai dengan profil usahanya;
- Pola transaksi berulang dimana pihak penerima dana juga dominan merupakan pihak pengirim dana
- Rekening yang baru dibuka menerima sejumlah transfer dana yang cukup besar nominalnya

DAFTAR PUSTAKA

Ersya, M. (2017). *Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia.*

Interpol. (n.d.). *Social engineering scams*. Retrieved April 10, 2022, from Interpol: https://www.interpol.int/Crimes/Financial-crime/Social-engineering-scams

Kejaksaan Agung RI. (2021, 11 16). *Berhasil Ungkap TP Siber Keuangan Lintas Negara, Jaksa Agung Diapresiasi Kedubes Italia dan Belanda.* Retrieved from kejaksaan.go.id: http://pji.kejaksaan.go.id/index.php/home/berita/1938

Media Indonesia. (2022, January 18). *OJK: Kerugian akibat investasi ilegal 2011-2021 capai Rp117,4 triliun*. Retrieved from MediaIndonesia.com: https://mediaindonesia.com/ekonomi/465173/ojk-kerugian-akibat-investasi-ilegal-2011-2021-capai-rp1174-triliun

Pusat Pelaporan dan Analisis Transaksi Keuangan. (2021). *Penilaian Risiko Indonesia terhadap Tindak Pidana Pencucian Uang Tahun 2021.* Jakarta: PPATK.

Pusat Pelaporan dan Analisis Transaksi Keuangan. (2021). *Riset Tipologi Tahun 2021 berdasarkan Putusan Pengadilan Pencucian Uang Tahun 2020.* Jakarta: PPATK.

Ramli, A. (2004). *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia.* Bandung: Refika Aditama.

Sitompul, A. (2001). *Hukum Internet (Pengenalan Mengenai Masalah Hukum Di Cyberspace).* Bandung: Citra Aditya Bakti.

Soepraptomo, H. (2000). Kejahatan Komputer dan Siber serta Antisipasi Pengaturan Pencegahannya di Indonesia. *Seminar Hukum Tentang E-Commerce dan Mekanisme Penyelesaian Masalahnya Melalui Arbitrase/Alternatif Penyelesaian Sengketa.* Jakarta: Law Offices of Remy &Darus.

Suhariyanto, B. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime), Urgensi Pengaturan dan Celah Hukumnya.* Jakarta: Rajawali Press.

LAMPIRAN

Lampiran 1 Tabel Kompilasi Hasil Penilaian Risiko Tindak Pidana Penipuan Siber

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
Jenis cyber fraud	Business Email Compromise	6,77	9,00	9,00	8,68	9,00	Tinggi
	Investment Fraud	6,22	9,00	8,66	9,00	8,99	Tinggi
	Fraudulent Wire Transfer	9,00	3,67	7,09	6,52	6,23	Menengah
	Romance Scams	3,00	3,00	3,00	3,00	3,00	Rendah
Pelaku - Profil Perorangan	Pengusaha/Wiraswasta	9,00	9,00	9,00	9,00	9,00	Tinggi
	Pegawai Swasta	8,39	7,62	7,97	8,27	7,72	Tinggi
	Pelajar/Mahasiswa	6,43	7,15	6,72	6,63	5,91	Menengah
	Pegawai Money Changer	4,74	7,62	6,09	5,65	5,04	Menengah
	Ibu Rumah Tangga	4,90	5,77	5,22	6,16	4,85	Rendah
	Profesional dan Konsultan	4,35	5,77	4,94	5,85	4,57	Rendah
	Pengurus dan pegawai yayasan/lembaga berbadan hukum lainnya	4,35	5,31	4,71	4,59	3,95	Rendah
	Pegawai Bank	3,97	4,38	4,03	5,30	3,93	Rendah
	Pedagang	4,70	3,46	3,93	4,50	3,62	Rendah
	Pegawai BUMN/BUMD (termasuk pensiunan)	3,39	5,77	4,44	3,92	3,60	Rendah
	Lain-Lain	4,10	5,31	4,57	3,76	3,57	Rendah
	PNS (termasuk pensiunan)	3,89	3,92	3,75	4,28	3,48	Rendah
	TNI/Polri (termasuk pensiunan)	3,38	4,38	3,73	4,31	3,48	Rendah
	Pengajar dan Dosen	3,18	3,92	3,39	4,57	3,43	Rendah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Pejabat Lembaga Legislatif dan Pemerintah	3,58	4,38	3,83	3,92	3,39	Rendah
	Buruh, Pembantu Rumah Tangga dan Tenaga Keamanan	4,14	3,92	3,88	3,61	3,31	Rendah
	Pengurus Parpol	3,39	4,38	3,73	3,66	3,28	Rendah
	Pengurus/Pegawai LSM/organisasi tidak berbadan hukum lainnya	3,00	4,38	3,53	3,73	3,23	Rendah
	Petani dan Nelayan	3,35	3,00	3,00	4,11	3,16	Rendah
	Pengrajin	3,19	4,38	3,63	3,00	3,04	Rendah
	Ulama/Pendeta/Pimpinan organisasi dan kelompok keagamaan	3,19	3,92	3,39	3,07	3,00	Rendah
Pelaku - Profil Non Perorangan	NONPERORANGAN-PT	9,00	9,00	9,00	9,00	9,00	Tinggi
	NONPERORANGAN-Koperasi	6,89	7,36	7,13	6,00	5,81	Menengah
	NONPERORANGAN-CV	6,46	6,82	6,64	7,73	6,53	Menengah
	NONPERORANGAN-PD/UD	3,27	3,00	3,14	3,46	3,15	Rendah
	NONPERORANGAN-Firma	3,55	3,55	3,55	3,00	3,14	Rendah
	NONPERORANGAN-Yayasan	3,55	3,00	3,27	3,23	3,13	Rendah
	NONPERORANGAN-Perkumpulan	3,27	3,00	3,14	3,23	3,09	Rendah
	NONPERORANGAN-Ormas Tidak Berbadan Hukum	3,00	3,00	3,00	3,00	3,00	Rendah
Peranan	Social Engineer	9,00	7,50	8,51	9,00	9,00	Tinggi
	Hacker	8,43	9,00	9,00	5,95	6,96	Menengah
	Money Mule	8,43	3,00	5,85	8,07	6,39	Menengah
	Money Collector	3,00	3,00	3,00	3,00	3,00	Rendah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
Tipologi Pencucian Uang	Pembuatan rekening baru untuk menampung dana hasil kejahatan	8,68	9,00	8,83	9,00	9,00	Tinggi
	Penggunaan rekening nominee: milik orang lain (baik yang dikenal/tidak kenal/fiktif)	9,00	9,00	9,00	8,82	8,99	Tinggi
	Penggunaan dokumen identitas palsu	8,45	9,00	8,71	8,37	8,44	Tinggi
	Transaksi yang dilakukan secara Pass by (dana masuk langsung ditransfer kembali atau tarik tunai)	7,67	9,00	8,31	7,79	7,74	Tinggi
	Penggunaan nama Perusahaan atau perorangan untuk menampung pengiriman uang sehingga seolah-olah nampak seperti transaksi bisnis	7,52	9,00	8,23	7,74	7,66	Tinggi
	Pola transaksi dengan menggunakan uang tunai (Cash Basis): tarik tunai, setor tunai; yang dilakukan untuk menyamarkan identitas	7,83	9,00	8,39	7,19	7,37	Tinggi
	Penggunaan pihak ketiga untuk pengiriman uang	7,02	9,00	7,97	6,94	6,94	Menengah
	Pembelian aset berupa tanah, bangunan, rumah dan mobil	7,20	7,50	7,28	7,34	6,78	Menengah
	Penyalahgunaan bisnis yang sah dengan pemalsuan dokumen sehingga menyebabkan cacat administrasi	7,04	8,50	7,72	6,69	6,63	Menengah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Penggunaan kartu kredit, cek, note dalam pencucian uang hasil tindak kejahatan.	7,22	7,50	7,29	6,45	6,24	Menengah
	Penyembunyian harta hasil kejahatan ke dalam struktur bisnis	6,88	7,50	7,11	6,25	6,02	Menengah
	Structuring: Memecah-mecah transaksi dengan melibatkan berbagai pihak, volume tinggi dari transaksi yang kecil, penggunaan banyak akun/rekening guna menghindari deteksi kewajiban pelaporan oleh penyedia jasa keuangan/pihak pelapor	6,85	7,50	7,10	6,26	6,01	Menengah
	Penukaran mata uang asing dalam jumlah yang signifikan dengan cara mentransfer ke perusahaan money changer	4,86	6,00	5,28	7,13	5,44	Menengah
	Penggunaan pihak lain/perantara dan pihak keluarga dalam upaya menyembunyikan atau menyamarkan asal usul harta kekayaan dari hasil tindak kejahatan	5,70	7,50	6,49	5,60	5,33	Menengah
	Pembelian barang – barang mewah seperti (lukisan, barang – barang antik, berlian atau barang – barang branded dlll)	6,25	6,00	6,00	5,94	5,27	Menengah
	Mingling: Menggabungkan hasil kejahatan dengan bisnis yang sah untuk mengaburkan sumber dana. Penempatan uang tidak mengejar keuntungan	5,40	8,00	6,60	5,39	5,26	Menengah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Penggunaan Virtual Currency (Aset Kripto)	5,52	8,00	6,66	5,33	5,26	Menengah
	Pengoperasian perusahaan cangkang/shell company (perusahaan yang tercatat secara hukum namun tidak terdapat aktivitas, biasanya digunakan untuk menyembunyikan harta dari tindak kejahatan)	4,99	6,50	5,60	5,60	4,90	Rendah
	Penggunaan “gatekeeper” layanan profesional (Pengacara, Akuntan, Broker, Notaris, Konsultan Bisnis, Perencana Keuangan) bertujuan untuk mengaburkan identitas penerima manfaat (Beneficiaries) dan harta hasil kejahatan	4,94	6,00	5,32	5,00	4,50	Rendah
	Penggunaan Perusahaan Multinasional, Offshore Bank dan Offshore Trust	4,24	5,50	4,69	5,00	4,23	Rendah
	Penggunaan skema pencucian uang dengan perdangan atau Trade – Based Money Laundering (TBML) dan Transfer Pricing (permainan harga).	4,24	6,00	4,95	4,40	4,09	Rendah
	Pemanfaatan Alat Pembayaran Baru: Uang Elektronik, Dompet Elektronik	4,46	4,50	4,28	4,00	3,69	Rendah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Penggunaan Bank illegal atau alternative jasa pengiriman uang atau Hawala	3,88	5,50	4,50	3,80	3,69	Rendah
	Pembelian saham dari uang hasil kejahatan	3,71	5,00	4,15	3,80	3,58	Rendah
	Pemberian sumbangan pada lembaga keagamaan, sosial dan/ pendidikan	3,85	4,50	3,96	3,40	3,38	Rendah
	Pembelian polis asuransi	3,65	3,00	3,08	3,80	3,23	Rendah
	Penggunaan safe deposit box	3,00	3,50	3,00	3,00	3,00	Rendah
Wilayah	DKI Jakarta	9,00	9,00	9,00	9,00	9,00	Tinggi
	Jawa Barat	8,48	7,33	7,91	8,18	7,63	Tinggi
	Jawa Timur	7,12	8,00	7,56	6,41	6,27	Menengah
	Jawa Tengah	7,77	6,00	6,88	7,02	6,26	Menengah
	Sumatera Utara	6,16	6,33	6,25	6,40	5,56	Menengah
	Bali	5,47	5,67	5,57	6,99	5,47	Menengah
	Banten	5,90	5,33	5,62	6,92	5,47	Menengah
	Sumatera Selatan	6,52	4,00	5,26	5,94	4,83	Rendah
	Sulawesi Selatan	5,90	3,67	4,78	6,43	4,79	Rendah
	Kep. Riau	5,44	5,00	5,22	5,84	4,77	Rendah
	DI Yogyakarta	5,16	5,33	5,25	5,67	4,70	Rendah
	Nusa Tenggara Barat	5,47	4,00	4,74	4,54	4,01	Rendah
	Kalimantan Selatan	4,85	4,67	4,76	4,48	3,99	Rendah
	Kalimantan Barat	4,55	3,33	3,94	4,91	3,83	Rendah
	Aceh	3,92	4,00	3,96	4,33	3,65	Rendah
	Kalimantan Timur	3,50	3,67	3,58	4,70	3,62	Rendah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Lampung	4,27	3,67	3,97	4,11	3,58	Rendah
	Kalimantan Tengah	3,93	3,67	3,80	4,24	3,56	Rendah
	Sulawesi Tengah	4,52	3,33	3,92	4,10	3,56	Rendah
	Sulawesi Utara	4,02	3,33	3,68	4,36	3,55	Rendah
	Sulawesi Barat	4,02	3,67	3,84	4,03	3,51	Rendah
	Jambi	3,53	3,00	3,26	4,58	3,46	Rendah
	Papua Barat	4,23	3,33	3,78	3,92	3,45	Rendah
	Nusa Tenggara Timur	4,21	3,33	3,77	3,89	3,44	Rendah
	Riau	3,66	4,00	3,83	3,59	3,36	Rendah
	Kep. Bangka Belitung	3,83	3,00	3,42	3,95	3,34	Rendah
	Papua	3,93	3,33	3,63	3,62	3,31	Rendah
	Maluku Utara	3,83	3,00	3,42	3,75	3,28	Rendah
	Kalimantan Utara	3,00	3,00	3,00	4,02	3,22	Rendah
	Sulawesi Tenggara	3,00	3,33	3,17	3,70	3,19	Rendah
	Gorontalo	3,33	3,67	3,50	3,29	3,17	Rendah
	Maluku	3,00	3,00	3,00	3,35	3,05	Rendah
	Sumatera Barat	3,00	3,33	3,17	3,00	3,01	Rendah
	Bengkulu	3,00	3,00	3,00	3,15	3,00	Rendah
Kelompok Industri	Bank	9,00	8,14	9,00	9,00	9,00	Tinggi
	Pedagang Valuta Asing	6,02	9,00	7,83	6,36	6,41	Menengah
	Pedagang Fisik Aset Kripto	5,34	6,86	6,29	4,92	4,83	Rendah
	Penyelenggara Kegiatan Usaha Pengiriman Uang	5,27	6,00	5,78	5,17	4,74	Rendah
	Pegadang Kendaraan Bermotor	4,87	6,00	5,57	4,50	4,34	Rendah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Penyelenggara E-Money dan / atau E-Wallet	4,27	5,57	5,00	4,97	4,32	Rendah
	Pialang Berjangka	4,13	6,86	5,63	4,41	4,32	Rendah
	Perusahaan Properti/Agen Properti	4,59	5,57	5,18	4,59	4,23	Rendah
	Pedagang Permata dan Perhiasan/Logam Mulia	4,31	6,43	5,49	4,31	4,22	Rendah
	Perusahaan Pembiayaan	4,40	4,29	4,37	4,45	3,87	Rendah
	Manajer Investasi	4,52	4,29	4,43	4,19	3,80	Rendah
	Pegadang Barang Seni dan Antik	3,75	5,14	4,48	4,13	3,79	Rendah
	Penyelenggara Alat Pembayaran Menggunakan Kartu	3,94	5,14	4,58	3,92	3,75	Rendah
	Penyelenggara layanan Transaksi Keuangan berbasis teknologi informasi	3,90	5,57	4,80	3,56	3,67	Rendah
	Koperasi yang Melakukan Kegiatan Simpan Pinjam	3,38	5,14	4,28	3,94	3,65	Rendah
	Penyelenggara layanan urun dana melalui penawaran saham berbasis teknologi informasi	3,56	4,71	4,14	4,06	3,65	Rendah
	Perposan sebagai Penyedia Jasa Giro	3,66	4,71	4,20	3,78	3,57	Rendah
	Perusahaan Efek	3,38	4,71	4,04	3,56	3,45	Rendah
	Penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi	3,56	4,71	4,14	3,38	3,42	Rendah
	Lembaga Pembiayaan Ekspor	3,19	3,43	3,23	3,84	3,29	Rendah
	Kustodian	3,00	4,29	3,60	3,19	3,21	Rendah
	Perusahaan Asuransi dan Perusahaan Pialang Asuransi	3,34	3,43	3,32	3,19	3,13	Rendah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Perusahaan Pembiayaan Infrastruktur	3,19	3,43	3,23	3,19	3,11	Rendah
	Wali Amanat	3,00	3,86	3,37	3,00	3,09	Rendah
	Pegadaian	3,00	3,86	3,37	3,00	3,09	Rendah
	Dana Pensiun Lembaga Keuangan	3,00	3,43	3,13	3,19	3,08	Rendah
	Perusahaan Modal Ventura	3,00	3,43	3,13	3,19	3,08	Rendah
	Lembaga Keuangan Mikro	3,00	3,43	3,13	3,19	3,08	Rendah
	Balai Lelang	3,19	3,00	3,00	3,00	3,00	Rendah
Profil Negara	**Sumber**						
	Asia	9,00	9,00	9,00	9,00	9,00	Tinggi
	Eropa	6,57	4,09	5,33	6,70	5,09	Menengah
	Amerika	5,21	3,00	4,11	5,46	3,94	Rendah
	Oceania	3,99	4,64	4,31	3,00	3,12	Rendah
	Afrika	3,00	3,00	3,00	3,85	3,00	Rendah
	Transit						
	Asia	9,00	9,00	9,00	9,00	9,00	Tinggi
	Oceania	3,38	4,64	4,01	3,40	3,38	Rendah
	Eropa	3,56	4,09	3,83	3,20	3,27	Rendah
	Afrika	3,19	3,00	3,09	3,00	3,02	Rendah
	Amerika	3,00	3,00	3,00	3,00	3,00	Rendah
	Tujuan						
	Asia	9,00	9,00	9,00	9,00	9,00	Tinggi
	Eropa	5,29	4,09	4,35	6,47	4,57	Rendah
	Afrika	3,89	3,00	3,00	4,76	3,41	Rendah
	Oceania	3,00	4,64	3,41	3,43	3,19	Rendah

RISIKO UTAMA	URAIAN	Ancaman	Kerentanan	Likehood	Dampak	Risiko	Kategori
	Amerika	4,13	3,00	3,13	3,00	3,00	Rendah
Produk dan/Jasa	Tabungan	9,00	7,71	8,92	9,00	9,00	Tinggi
	Transfer dana dalam negeri (Online, SKN, RTGS)	8,27	8,57	9,00	8,72	8,85	Tinggi
	Tarik/ setor tunai	7,93	8,14	8,54	8,42	8,30	Tinggi
	Transfer dana dari dan ke luar negeri	7,02	7,71	7,74	8,45	7,75	Tinggi
	Kartu debit	7,46	7,29	7,75	7,62	7,21	Tinggi
	Virtual account	6,45	9,00	8,17	7,23	7,21	Tinggi
	Giro	6,24	7,29	7,02	7,15	6,47	Menengah
	Kartu kredit	6,90	7,29	7,41	6,63	6,38	Menengah
	Layanan prioritas (wealth management)	4,87	6,86	5,95	7,62	6,06	Menengah
	Correspondent banking	4,88	7,29	6,21	6,32	5,55	Menengah
	Kredit/ Pinjaman	4,25	7,29	5,84	6,24	5,31	Menengah
	Deposito	4,19	6,86	5,54	6,19	5,13	Menengah
	Jual/ beli valuta asing	3,00	7,29	5,09	6,55	5,05	Menengah
	Safe deposit box	3,75	6,86	5,28	5,76	4,80	Rendah
	Letter of Credit	3,61	6,86	5,20	5,47	4,63	Rendah

PUSAT PELAPORAN DAN ANALISIS TRANSAKSI KEUANGAN (PPATK)
Jl. Ir. H Juanda No. 35 Jakarta 10120 Indonesia
Phone: (+6221) 3850455, 3853922
Fax: (+6221) 3856809, 3856826
website: http://www.ppatk.go.id