OTORITAS JASA KEUANGAN

PANDUAN

STRATEGI ANTI FRAUD

PENYELENGGARA INOVASI TEKNOLOGI SEKTOR KEUANGAN (ITSK)

DEPARTEMEN PENGAWASAN ITSK, ASET KEUANGAN DIGITAL DAN ASET KRIPTO
OTORITAS JASA KEUANGAN

2024

DAFTAR ISI

DAFTAR ISI

I. PENDAHULUAN

"ITSK MEMILIKI PERAN KRUSIAL DALAM MENCIPTAKAN SOLUSI KEUANGAN YANG LEBIH INKLUSIF, MENINGKATKAN KEAMANAN TRANSAKSI, DAN MENDORONG PERTUMBUHAN EKONOMI SECARA KESELURUHAN."

Inovasi teknologi memiliki peran krusial dalam membentuk masa depan sektor keuangan, yang semakin digital, terhubung, dan responsif terhadap kebutuhan pelanggan dan pasar yang terus berkembang. Dalam membentuk masa depan sektor keuangan, ITSK dapat meningkatkan efisiensi, memperluas akses ke layanan keuangan, meningkatkan pengelolaan risiko, dan merespons perubahan pasar dengan lebih cepat. Jumlah Penyelenggara Inovasi Teknologi Sektor Keuangan terus berubah dari waktu ke waktu, per Januari 2024 terdapat 69 Penyelenggara Inovasi Teknologi Sektor Keuangan.

Penyedia ini dibagi menjadi 11 cluster dan model bisnis, yaitu aggregator, *financial planners*, *financing agents*, *funding agents*, *Insurance Hub*, *InsurTech*, *Online Distress Solution*, *RegTech* – PEP, *Tax & Accounting*, *Authentication*, dan *Wealth Tech*. Saat ini Penyelenggara Inovasi Teknologi Sektor Keuangan Indonesia sedang mengalami pertumbuhan yang sangat pesat. Hanya dalam beberapa tahun saja, jumlah Penyelenggara Inovasi Teknologi Sektor Keuangan di Indonesia semakin bertambah.

Sektor Inovasi Teknologi Sektor Keuangan di Indonesia merupakan salah satu industri yang menjanjikan. Indonesia merupakan rumah bagi 20% dari seluruh perusahaan Penyelenggara Inovasi Teknologi Sektor Keuangan di ASEAN dan diperkirakan akan menghasilkan pendapatan senilai USD 8,6 miliar pada tahun 2025. Inovasi Teknologi Sektor Keuangan telah mengalami lonjakan signifikan dalam tatanan normal baru akibat pandemi COVID-19. Potensi pengguna yang lebih tinggi dan peningkatan transaksi digital yang signifikan di masa depan telah menentukan laju kemajuan Inovasi Teknologi Sektor Keuangan. Salah satu pendorong utama kesuksesan Inovasi Teknologi Sektor Keuangan di Indonesia adalah pesatnya adopsi platform digital.

Platform ini telah menyederhanakan transaksi seperti e-wallet, internet banking, dan Quick Response Code Indonesian Standard (QRIS), yang memfasilitasi peralihan dari aktivitas keuangan tradisional offline ke online. Namun, dengan banyaknya dan mudahnya mendapatkan akses teknologi sektor keuangan, pada tahun 2022, Otoritas Jasa Keuangan (OJK) menerima 13.229 laporan pengaduan terkait fintech, dengan 3.294 di antaranya terkait dengan fraud. Dari Asosiasi Fintech Indonesia (AFTECH) pada 2021 mencatat 380 kasus fraud di industri fintech, dengan total kerugian mencapai Rp58,6 miliar. Selain kerugian secara finansial, fraud dapat menimbulkan kerugian secara non-finansial, seperti penurunan moral karyawan, penurunan reputasi perusahaan, memberikan pengaruh buruk terhadap loyalitas pelanggan, dan adanya sanksi dari regulator.

Hal ini dikhawatirkan berpotensi menurunkan rasa percaya masyarakat atas layanan jasa teknologi sektor keuangan yang diberikan oleh Penyelenggara Inovasi Teknologi Sektor Keuangan, dan pada akhirnya akan mempengaruhi kinerja para Penyelenggara Inovasi Teknologi Sektor Keuangan. Terdapatnya dampak atas kejadian *fraud* bagi Penyelenggara Inovasi Teknologi Sektor Keuangan, tentunya menjadi concern bagi OJK dan lembaga negara lainnya. Oleh karena itu, OJK terus berupaya antara lain melalui kebijakan yang tidak memberikan toleransi atas kejadian *fraud* (*zero tolerance fraud*).

OJK berkomitmen dengan sedang menyusun pengaturan khusus mengenai Penerapan Strategi Anti Fraud bagi Penyelenggara Inovasi Teknologi Sektor Keuangan. Selain OJK, Komisi Pemberantasan Korupsi (KPK) juga gencar menggalakkan upaya pencegahan kejadian *fraud*. Pada tahun 2021 misalnya, KPK telah menerbitkan Surat Edaran (SE) KPK Nomor 19 tahun 2021 tentang Pengendalian Gratifikasi bagi Industri Jasa Keuangan (IJK).

Upaya lain yang telah dilakukan OJK dalam rangka memperkuat industri Inovasi Teknologi Sektor Keuangan, terwujud melalui rencana jangka menengah yang tertuang dalam *Digital Finance Innovation Roadmap and Action Plan* bagi Inovasi Teknologi Sektor Keuangan tahun 2020-2024. Salah satu inisiatif dalam *Digital Finance Innovation Roadmap and Action Plan*, dengan menargetkan pengembangan yang suportif dan komprehensif ekosistem keuangan digital untuk menciptakan industri jasa keuangan yang kompetitif, tangguh terhadap perubahan dan cocok untuk masa depan. Kerangka peraturan yang menjadi inti rencana aksi bertujuan untuk mengimbangi perubahan teknologi, memitigasi risiko terkait teknologi, melindungi kepentingan konsumen, dan mendorong persaingan.

Riset dan penelitian akan menjadi tulang punggung pengembangan kerangka peraturan dan mendorong inovasi. Kolaborasi dengan berbagai pemangku kepentingan, seperti lembaga pemerintah, perusahaan teknologi, dan universitas, diperlukan untuk menghasilkan regulasi yang didorong oleh penelitian dan peningkatan kemampuan digital serta juga telah disusun action plan berupa penyusunan Panduan Strategi Anti Fraud (SAF) bagi Penyelenggara Inovasi Teknologi Sektor Keuangan.

Berdasarkan kondisi tersebut, maka OJK menilai dibutuhkannya sebuah kebijakan dalam rangka implementasi SAF khusus bagi Penyelenggara Inovasi Teknologi Sektor Keuangan. Dengan mempertimbangkan skala bisnis dan disparitas Penyelenggara Inovasi Teknologi Sektor Keuangan yang tinggi, maka dinilai diperlukan penyesuaian-penyesuaian, upaya bertahap serta berkelanjutan, serta melibatkan seluruh pihak yang berkepentingan dalam penerapan SAF bagi Penyelenggara Inovasi Teknologi Sektor Keuangan agar dapat menerapkan upaya pengendalian risiko *fraud*.

II. LITERATUR

APA SIH YANG DI MAKSUD DENGAN *FRAUD ?*

1. BLACK'S LAW DICTIONARY 8TH EDITION

"Tindakan **sengaja memberikan gambaran yang salah** tentang hal yang benar atau **menyembunyikan hal yang benar** untuk mempengaruhi orang lain agar bertindak **menguntungkan dirinya dan merugikan orang lain.**" Definisi lain dari *fraud* adalah aktivitas apa pun yang menggunakan penipuan untuk mencapai keuntungan. Fraud menjadi kejahatan jika hal tersebut merupakan "kesalahan penyajian yang disengaja atas kebenaran atau penyembunyian fakta material untuk mendorong orang lain melakukan tindakan yang merugikan dirinya.

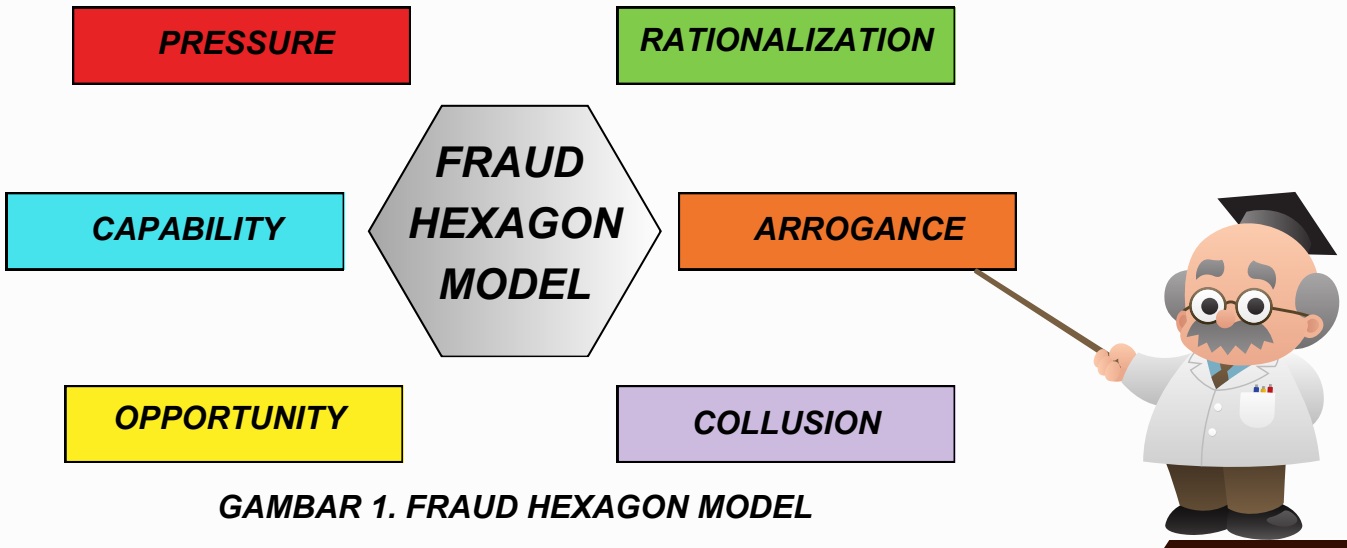
2. ASSOCIATION OF CERTIFIED FRAUD EXAMINATION (ACFE)

Perbuatan melawan hukum yang dilakukan dengan sengaja untuk tujuan tertentu manipulasi atau memberikan laporan keliru terhadap pihak lain) yang dilakukan oleh orang orang dari dalam atau luar organisasi untuk **mendapatkan keuntungan pribadi** ataupun **kelompok secara langsung** atau **tidak langsung merugikan pihak lain.**

3. INSTITUTE OF INTERNAL AUDITOR (IIA)

Suatu **perbuatan melawan hukum** yang dilakukan oleh individu di dalam maupun di luar organisasi atas dasar kesengajaan dengan tujuan untuk **menguntungkan individu organisasi** dan **mengakibatkan adanya kerugian.**

KENAPA BISA TERJADI *FRAUD?*



GAMBAR 1. FRAUD HEXAGON MODEL

1. STIMULUS (PRESSURE)

Pelaku pada saat ini melakukan kejahatan yang didorong oleh tekanan dimana hal ini dapat berasal dari tekanan akan kebutuhan keuangan, target keuangan yang menurun, perekonomian keluarga yang mendesak, dan lainnya, sehingga mendorong pelaku untuk berani melakukan pencurian kas perusahaan.

2. KAPABILITAS (CAPABILITY)

Hal ini menunjukan seberapa besar daya dan kapasitas dari suatu pihak untuk melakukan kecurangan di lingkungan perusahaan. Pada poin ini, salah satu contoh yang menggambarkan dengan jelas adalah saat terjadinya perubahan direksi yang merupakan terciptanya wujud conflict of interest (Sari & Nugroho, 2020).

3. OPPORTUNITY (PELUANG)

Bila terdapat kelemahan dalam pengendalian internal perusahaan, pengawasan yang melemah mendorong seseorang untuk bertindak dalam melakukan kecurangan. Celah ini dapat mengundang hal yang fatal bagi perusahaan dimana kelemahan dalam pengendalian internal yang berjalan dimanfaatkan oleh seseorang.

4. RATIONALIZATION

Pada poin tersebut, pelaku akan melakukan pembenaran atau merasa bahwa tindakannya benar saat mereka melakukan kecurangan. Perilaku tersebut muncul disaat seseorang merasa telah berbuat lebih bagi perusahaan, sehingga mereka terdorong untuk mengambil keuntungan yang didasari pemikiran bahwa hal tersebut sah-sah saja selama mereka bekerja dengan benar.

5. EGO (ARROGANCE)

Arogansi adalah sikap superioritas yang menyebabkan keserakahan dari orang yang percaya bahwa pengendalian internal tidak berlaku secara pribadi. Hal ini disebabkan saat seseorang merasa lebih tinggi kedudukannya ketimbang pihak lainnya (Desviana et al., 2020).

6. COLLUTION

Menurut Vousinas, (2019) kolusi merujuk kepada perjanjian yang menipu suatu pihak dimana pihak yang tertipu sebanyak dua orang atau lebih, untuk satu pihak yang bertujuan untuk mengambil tindakan lain untuk beberapa tujuan kurang baik, seperti menipu pihak ketiga dari hak yang dimilikinya.

APA SAJA KLASIFIKASI *FRAUD?*

Fraud sangat umum terjadi sehingga dapat dikategorikan dalam banyak cara. Namun, pada dasarnya setiap jenis *fraud* bersifat organisasional atau individual. Berikut karakteristik utama dari *fraud:*

1. INDIVIDU

Fraud terjadi ketika satu orang menjadi sasaran pelaku (termasuk pencurian identitas, phising, dan skema *"advance-fee"*). Salah satu *fraud* terhadap individu yang paling merugikan adalah skema *Ponzi.*

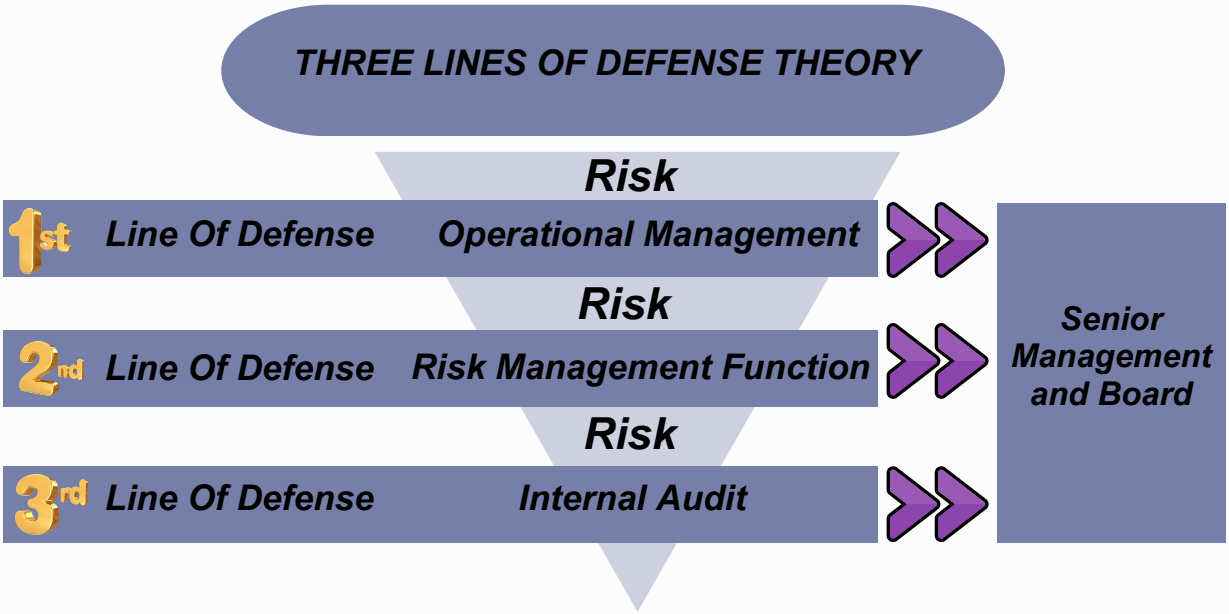
2. INTERNAL ORGANISASI

Sering disebut dengan *"occupational fraud,"* yaitu ketika seorang karyawan, manajer, atau eksekutif suatu organisasi melakukan *fraud* dalam organisasi sendiri, contohnya penggelapan, kecurangan pajak, dan melakukan penipuan kepada investor dan pemegang saham.

3. EKSTERNAL ORGANISASI

Hal ini mencakup *fraud* yang dilakukan terhadap organisasi dari pihak eksternal, seperti vendor yang melakukan penipuan tentang pekerjaan yang mereka lakukan, penyuapan dengan karyawan, dan kecurangan lainnya. Dengan berkembangnya teknologi, organisasi dapat terancam terkait pencurian kekayaan intelektual atau informasi pelanggan.

APA LAGI YANG BISA DIPELAJARI UNTUK MENGHADAPI *FRAUD?*



GAMBAR 2. THREE LINES OF DEFENSE THEORY

Teori tiga (3) lini pertahanan ini memberikan kemudahan untuk menyusun peran dan tanggung jawab yang jelas dalam upaya pengendalian dan pengelolaan risiko organisasi. Terdapat 3 lini dalam teori ini yaitu manajemen operasional lini pertama fungsi manajemen risiko lini kedua dan fungsi audit internal lini ketiga.

1. **Lini pertama,** merupakan lini bisnis atau manajemen operasional mencakup fungsi fungsi inti dari organisasi yang berperan sebagai pemilik risiko dan bertanggung jawab mengelola risiko (contoh: bagian operasional bank Teller CS, RM, IT), pengelola SDM).
2. **Lini kedua,** merupakan lini pertahanan yang menjalankan fungsi manajemen risiko dan pemantauan (contoh: fungsi manajemen risiko kepatuhan).
3. **Lini ketiga**, merupakan lini pengendalian internal yang bersifat independen dan memiliki objektivitas yang tinggi (contoh: internal audit).

ADAKAH REGULASI YANG MEMBANTU PENCEGAHAN *FRAUD?*

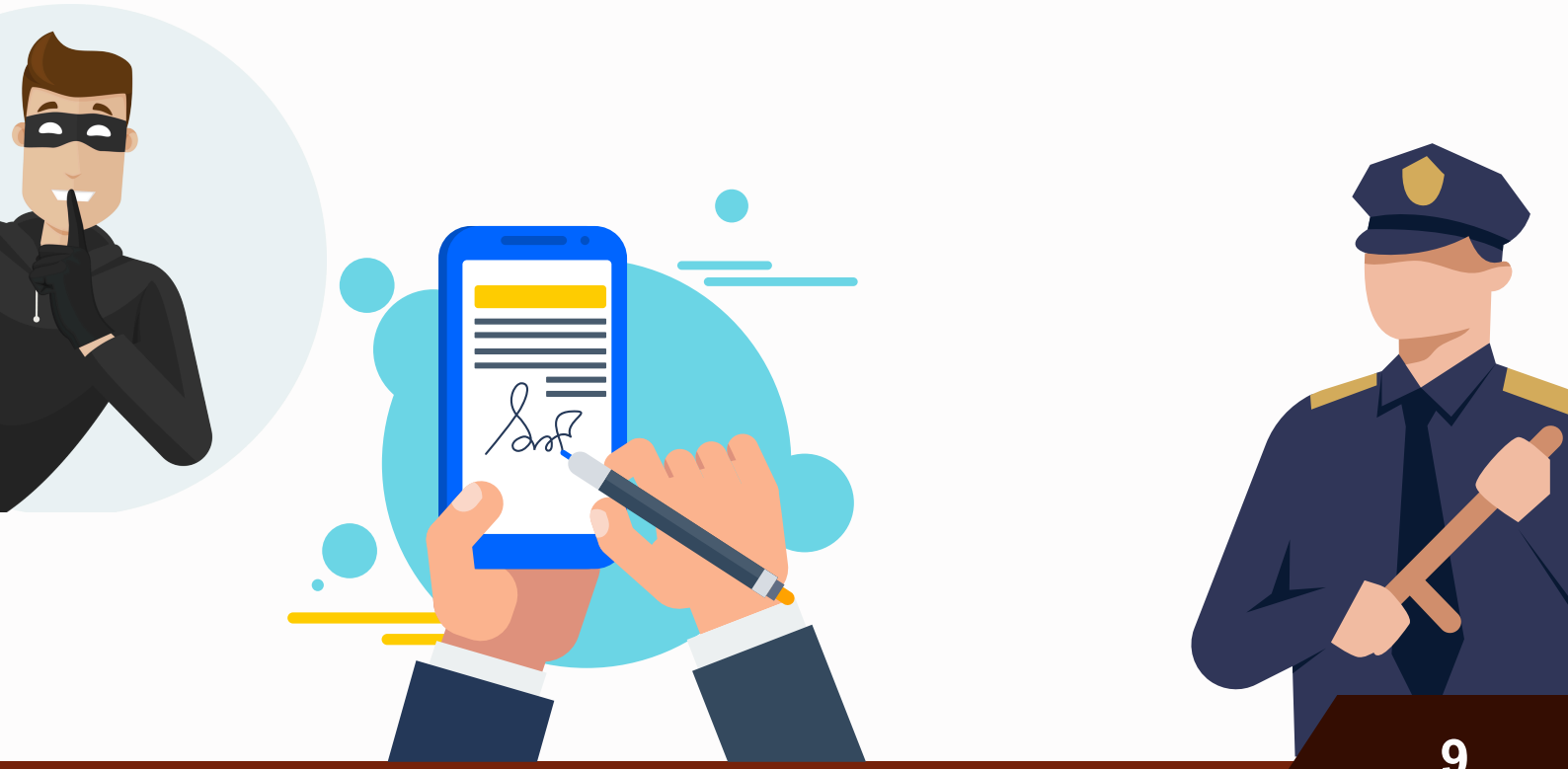
Regulasi yang membantu dalam pencegahan *fraud* tertuang dalam aturan pada daftar berikut :

III. RISIKO TRANSAKSI

KLASIFIKASI TRANSAKSI ELEKTRONIK RISIKO TINGGI

Transaksi elektronik yang berisiko tinggi adalah transaksi keuangan yang tidak dilakukan dengan tatap muka secara fisik, atau disebut transaksi keuangan digital. Dalam Perubahan UU ITE No 1 Tahun 2024 pasal 17 pasal (2a) “Transaksi Elektronik yang memiliki risiko tinggi bagi para pihak menggunakan Tanda Tangan Elektronik yang diamankan dengan Sertilikat Elektronik.” Dalam penerapannya, tanda tangan elektronik tersertifikasi akan melakukan verifikasi terhadap para pihak yang terlibat dalam dokumen elektronik sebelum mereka menandatangani dokumen. Proses verifikasi dilakukan dengan mencocokkan data mereka dengan data biometrik dan data kependudukan di Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri (Dukcapil Kemendagri).

Otoritas Jasa Keuangan (OJK) menilai penggunaan tanda tangan elektronik tersertifikasi sangat penting di sektor jasa keuangan yang memiliki risiko penipuan (fraud) tinggi. Atas hal tersebut, OJK telah menginisiasi komunikasi dengan Kominfo terkait interpretasi dari aturan Pasal 17 ayat 2a UU No. 1 Tahun 2024 dan bersepakat untuk memaknai bahwa TTE tersertifikasi wajib untuk digunakan dalam mengamankan transaksi keuangan yang dilakukan tanpa pertemuan tatap muka



IV. KEAMANAN DIGITAL

TINGKAT JAMINAN DALAM IDENTITAS DIGITAL

Tingkat Jaminan Identitas Digital adalah tingkat kepastian dalam proses autentikasi klaim terhadap identitas tertentu dapat dipercaya sebagai identitas "asli" pemohon. Tingkat jaminan yang lebih tinggi mengurangi risiko identitas palsu dan meningkatkan keamanan transaksi. Di sisi lain, tingkat jaminan juga membutuhkan biaya lebih dan proses yang lebih kompleks bagi pemegang identitas pemohon dan pihak yang memohon, yang perlu pertimbangan lebih bagi praktisi terkait berbagai persyaratan dari kasus penggunaan yang berbeda sehubungan dengan tingkat jaminan dalam identitas digital. Misalnya, autentikasi berbasis biometrik kemungkinan tidak sesuai untuk digunakan di semua kasus penggunaan karena beberapa transaksi yang memiliki risiko lebih rendah.

Tingkat jaminan bergantung pada kekuatan proses pembuktian identitas, jenis kredensial, serta mekanisme autentikasi yang digunakan selama transaksi. Untuk pembuktian identitas, tingkat jaminan bergantung pada metode identifikasi (misalnya, tatap muka atau jarak jauh), atribut/dokumen yang dikumpulkan, dan tingkat kepastian yang digunakan untuk memverifikasi atribut/dokumen tersebut (misalnya, melalui pemeriksaan silang dan deduplikasi). Untuk autentikasi, tingkat jaminan bergantung pada jenis kredensial, jumlah faktor autentikasi yang digunakan (yaitu satu factor atau banyak faktor), dan kekuatan kriptografi dari transaksi.

eIDAS (EU 2015) dan ISO/IEC 29115 telah mengembangkan standar untuk mengklasifikasikan tingkat jaminan berdasarkan proses dan teknologi ini. Selain itu, pedoman terbaru dari National Institute of Standards and Technology (NIST) Amerika Serikat (NIST 800-63-3) telah mengadaptasi kerangka kerja ini untuk memisahkan tingkat jaminan untuk pembuktian identitas ("tingkat jaminan identitas" atau IAL) dan untuk autentikasi ("tingkat jaminan autentikator" atau AAL). Selain itu, kerangka NIST membedakan tingkat jaminan untuk penegasan identitas dalam lingkungan federasi ("tingkat jaminan federasi" atau FAL). Meskipun banyak sistem akan memiliki level yang sama untuk masing-masing, praktisi juga dapat memilih IAL, AAL, dan FAL sebagai opsi berbeda, tergantung pada persyaratan sistem.

1. TINGKAT JAMINAN PEMBUKTIAN IDENTITAS:

Tingkat Jaminan Pembuktian Identitas:

- IAL1: Atribut, jika ada, merupakan pernyataan diri atau harus diperlakukan sebagai pernyataan diri; tidak ada proses pembuktian.
- IAL2: Diperlukan pembuktian identitas jarak jauh atau tatap muka minimal menggunakan prosedur yang diberikan dalam SP 800-63A.
- IAL3: Diperlukan pembuktian identitas tatap muka atau dengan pengawasan jarak jauh. Atribut pengenal harus diverifikasi melalui pemeriksaan dokumentasi fisik seperti yang dijelaskan dalam SP 800-63A.

2. TINGKAT JAMINAN AUTENTIKASI:

- AAL1: Membutuhkan tingkat kepercayaan tertentu tertentu terhadap proses autentikasi. AAL1 memerlukan autentikasi faktor tunggal menggunakan berbagai teknologi autentikasi yang tersedia. Autentikasi yang berhasil mengharuskan pemohon untuk membuktikan kepemilikan dan kontrol atas autentikator melalui protocol autentikasi yang aman.
- AAL2: Membutuhkan tingkat kepercayaan tinggi terhadap proses autentikasi. Untuk melakukan otentikasi di AAL2, pemohon harus membuktikan kepemilikan dan kontrol dari dua faktor autentikasi yang berbeda melalui protokol autentikasi yang aman. Teknik kriptografi diperlukan.
- AAL3: Membutuhkan tingkat kepercayaan sangat tinggi terhadap proses autentikasi. Autentikasi di AAL3 didasarkan pada bukti kepemilikan kunci melalui protokol kriptografi. AAL3 seperti AAL2 tetapi juga memerlukan autentikator kriptografi "kompleks" yang menyediakan keamanan terhadap peniruan pemverifikasi.

3. LOA FEDERASI:

- FAL1: Mengizinkan pihak yang memohon untuk menerima pernyataan pembawa dari penyedia identitas atau pemohon. Penyedia identitas harus menandatangani pernyataan tersebut menggunakan kriptografi.
- FAL2: Menambahkan persyaratan agar pernyataan dienkripsi menggunakan kriptografi sehingga pihak yang memohon adalah satu-satunya pihak yang dapat mendekripsikannya.
- FAL3: Memerlukan pengguna untuk menunjukkan bukti kepemilikan referensi kunci kriptografi yang dirujuk dalam pernyataan dan sumber pernyataan (assertion artifact). Pernyataan tersebut harus ditandatangani menggunakan kriptografi dan dienkripsikan ke pihak yang memohon menggunakan kriptografi.

Pemilihan Tingkat Jaminan tergantung pada kasus penggunaan; beberapa sektor dan jenis transaksi akan membutuhkan tingkat jaminan yang lebih tinggi daripada yang lainnya. Misalnya, mengubah alamat mungkin hanya memerlukan tingkat jaminan yang lebih rendah dibandingkan dengan mengubah kata sandi. Layanan keuangan biasanya membutuhkan tingkat jaminan yang lebih tinggi daripada yang lainnya karena sensitivitas data yang dikumpulkan dan disimpan dalam sistem tersebut. Idealnya, arsitektur autentikasi sistem identitans digital harus mampu menyediakan beberapa tingkat jaminan yang sesuai dengan kasus penggunaan yang berbeda.

BAGAIMANA DENGAN RUJUKAN STANDAR SAF DARI NEGARA LAIN?

1. GOVERNMENT:

- Financial Conduct Authority (FCA) - Inggris
- Securities and Exchange Commission (SEC) - Amerika Serikat
- European Banking Authority (EBA) - Uni Eropa
- Monetary Authority of Singapore (MAS) – Singapura
- Australian Securities and Investments Commission (ASIC) – Australia

2. ASSOCIATION:

- International Association of Certified Fraud Examiners (ACFE) - International
- Global Digital Finance (GDF) - International
- European Crowdfunding Network (ECN) – Uni Eropa.
- International RegTech Association (IRTA) - International
- Association of Certified Fraud Examiners (ACFE) Indonesia Chapter - Indonesia

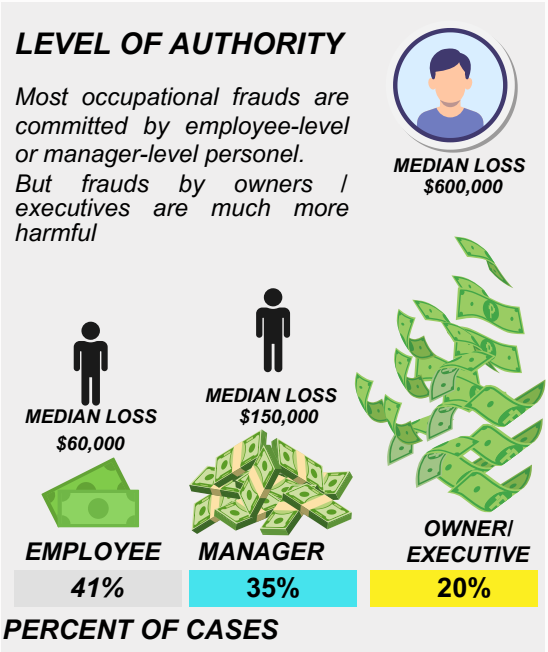
3. REVIEW BEST PRACTICE SAF DARI BERBAGAI NEGARA, STANDAR MINIMUM PILAR DAN CAKUPAN PILAR SAF SEBAGAI BERIKUT:

- International Association of Certified Fraud Examiners (ACFE) - International
- Global Digital Finance (GDF) - International
- European Crowdfunding Network (ECN) – Uni Eropa.
- International RegTech Association (IRTA) - International
- Association of Certified Fraud Examiners (ACFE) Indonesia Chapter - Indonesia

V. TIPOLOGI DAN MODUS FRAUD

GAMBAR 3. REPORT TO THE NATIONS ON OCCUPATIONAL FRAUD AND ABUSE – 2022 (ACFE)

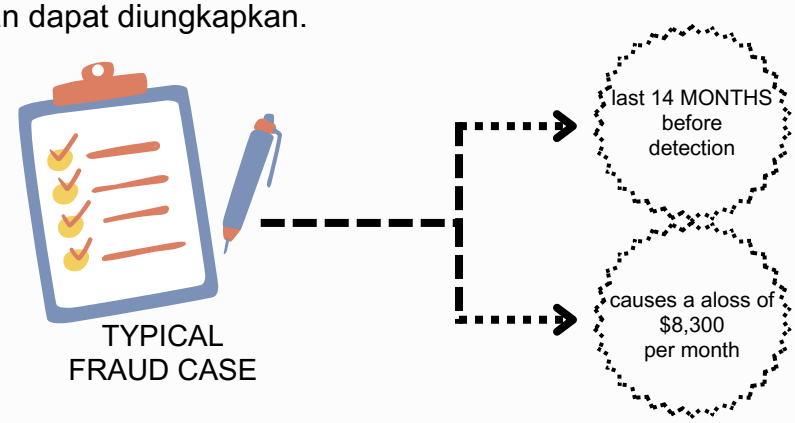
Berdasarkan data ACFE 2022, terdapat 2.088 kasus yang berasal dari 125 negara, di 8 region (USA Canada, Sub Saharan Africa, Asia Pacific, Western Europe, Middle East Nort Afica Southern Asia, Latin America Carribean and Eastern Europe Western/ Central Asia):



GAMBAR 4. LEVEL OF AUTHORITY

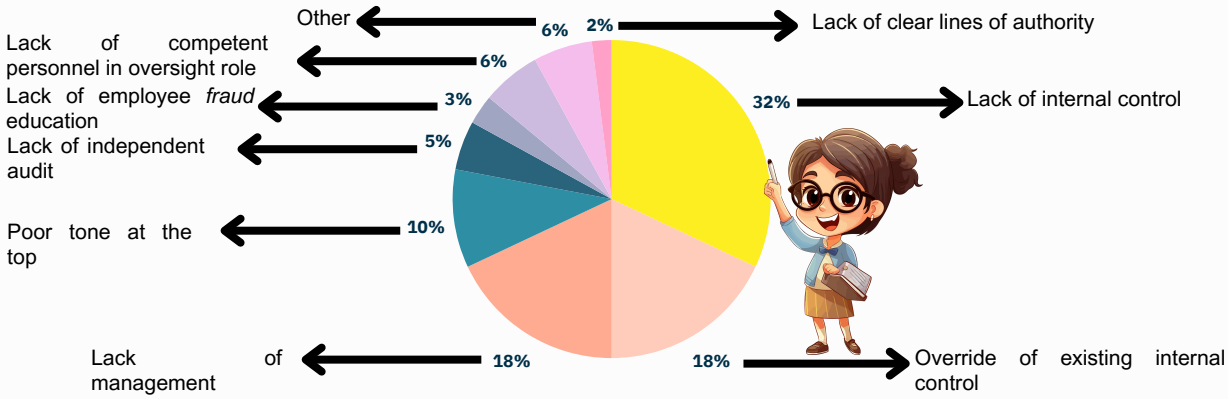
- Fraud yang dilaporkan diperkirakan menyebabkan kerugian total lebih dari 3,6 Triliun Dollar US. Responden memperkirakan secara khusus organisasi kerugian rata-rata 150.000 Dollar US.
- Pelaku *fraud* yang memiliki otoritas atau wewenang lebih tinggi cenderung menyebabkan kerugian yang jauh lebih besar. Pemilik/eksekutif hanya melakukan 20% dari total jumlah *fraud*, tetapi mereka menyebabkan kerugian terbesar.

Perbuatan *fraud* rata rata membutuhkan waktu paling cepat 14 bulan sebelum terdeteksi dan dapat diungkapkan.



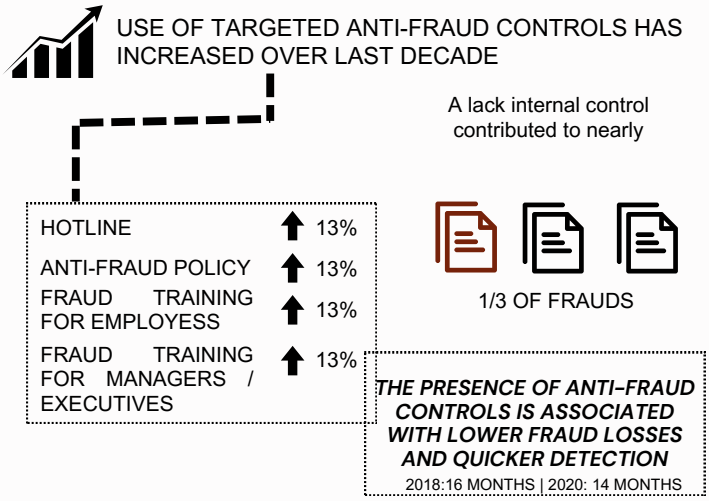
GAMBAR 5. TYPICAL FRAUD CASE

Kelemahan penyebab *fraud* terbesar didominasi oleh lemahnya Internal Control (32%), mengesampingkan peran Internal Control (18%), kurangnya review dari manajemen puncak (18%), lemahnya komitmen manajemen puncak dalam menjalankan anti *fraud* (10%), serta kurang optimalnya audit independen (5%).



GAMBAR 6. REPORT TO THE NATIONS ON OCCUPATIONAL FRAUD AND ABUSE – 2020 (ACFE)

Secara umum, sepertiga kasus *fraud* disebabkan oleh kurangnya peran Internal Control. Dengan adanya Internal Control yang tepat, mengurangi dampak kerugian yang diakibatkan oleh *fraud* dan dapat mendeteksi kejadian *fraud* lebih cepat.



Penggunaan beberapa instrumen anti *fraud* yang meningkat penggunaannya selama satu dasawarsa terakhir antara lain hotlines (Whistle Blowing System/WBS) (up 13%), kebijakan anti *fraud* (up 13%), pelatihan anti *fraud* bagi pegawai (up 11%), dan pelatihan anti *fraud* untuk level manajerial/executive (up 9%).

Berikut beberapa contoh kasus fraud di Amerika Serikat :

1. Kasus Enron : Kasus Enron, yang terjadi di Amerika Serikat pada awal tahun 2000-an, merupakan salah satu contoh kasus *fraud* paling terkenal dan berdampak besar dalam sejarah. Enron, sebuah perusahaan energi raksasa, melakukan manipulasi akuntansi selama bertahun-tahun untuk menyembunyikan kerugian dan melambungkan pendapatannya. Penipuan ini dilakukan dengan berbagai cara, termasuk mencatat aset fiktif, menggunakan skema off-balance-sheet, dan menekan akuntan untuk menyetujui laporan keuangan yang menyesatkan. Akibatnya, Enron bangkrut pada tahun 2001, menyebabkan kerugian finansial yang besar bagi investor, karyawan, dan pensiunan. Kasus ini juga memiliki dampak non-finansial yang signifikan, merusak kepercayaan publik terhadap pasar modal dan mendorong reformasi peraturan akuntansi. Manipulasi akuntansi adalah tindakan curang yang dilakukan dengan mengubah atau menyembunyikan informasi keuangan untuk menyesatkan investor, regulator, atau pihak lain.
2. Kasus WorldCom : Kasus WorldCom, yang terjadi di Amerika Serikat pada awal tahun 2000-an, merupakan salah satu contoh kasus *fraud* akuntansi terbesar dalam sejarah. WorldCom, sebuah perusahaan telekomunikasi raksasa, melakukan penipuan akuntansi selama bertahun-tahun untuk menyembunyikan kerugian dan melambungkan pendapatannya. Penipuan ini dilakukan dengan berbagai cara, termasuk mencatat biaya sebagai aset, menggelembungkan pendapatan, dan menggunakan skema *off balance sheet*. Akibatnya WorldCom bangkrut pada tahun 2002, menyebabkan kerugian finansial sebesar 11 miliar dolar bagi investor dan karyawan.

Kasus Enron dan kasus WorldCom berdampak signifikan terhadap kestabilan ekonomi negara Amerika Seikat, sehingga respon pemerintah atas kasus tersebut yaitu menerbitkan Undang- Undang Sarbanes-Oxley Act (SOX) yang diberlakukan di Amerika Serikat pada tahun 2002.

Tujuan utama SOX adalah untuk:

1. Melindungi investor: Meningkatkan akuntabilitas dan transparansi perusahaan publik, sehingga investor dapat membuat keputusan investasi yang lebih informed.
2. Mencegah *fraud*: Memperkuat kontrol internal dan menegakkan hukum terhadap *fraud* akuntansi dan keuangan.
3. Memperkuat tata kelola perusahaan: Meningkatkan standar tata kelola perusahaan dan mendorong dewan direksi untuk mengambil tanggung jawab lebih besar atas akuntansi dan keuangan perusahaan.

SOX terdiri dari 11 bab dan mencakup berbagai ketentuan, di antaranya:

1. Pembentukan Public Company Accounting Oversight Board (PCAOB): PCAOB adalah badan independen yang bertanggung jawab untuk mengawasi auditor perusahaan publik.
2. Meningkatkan standar pelaporan keuangan: Perusahaan publik diharuskan untuk mengikuti standar akuntansi yang lebih ketat dan memberikan pengungkapan yang lebih lengkap tentang informasi keuangan mereka.
3. Memperkuat pengendalian internal: Perusahaan publik diharuskan untuk memiliki pengendalian internal yang efektif atas pelaporan keuangan mereka.
4. Meningkatkan tanggung jawab dewan direksi: Dewan direksi perusahaan publik diharuskan untuk lebih terlibat dalam proses pelaporan keuangan dan bertanggung jawab atas keakuratan laporan keuangan perusahaan.
5. Melarang praktik akuntansi yang curang: SOX melarang berbagai praktik akuntansi yang curang, seperti manipulasi laba dan pengakuan pendapatan yang tidak semestinya.
6. Meningkatkan perlindungan whistleblower: SOX memberikan perlindungan bagi karyawan yang melaporkan *fraud* atau pelanggaran lainnya.
7. Meningkatkan penegakan hukum: SOX meningkatkan hukuman untuk *fraud* akuntansi dan keuangan.

SOX telah berdampak signifikan pada pasar modal AS dan global. SOX telah membantu meningkatkan kepercayaan investor terhadap pasar modal dan mendorong tata kelola perusahaan yang lebih baik. Namun, SOX juga telah dikritik karena biayanya yang tinggi dan kompleksitasnya.

CONTOH MODUS FRAUD DENGAN SIBER :

1. PENCURIAN DATA

- Modus : Pelaku melakukan peretasan untuk mencuri data sensitif, seperti data keuangan, data pribadi, atau rahasia dagang, dari sistem IT organisasi. Data ini kemudian dapat digunakan untuk melakukan *fraud*, seperti penipuan identitas, penggelapan dana, atau pemerasan.
- Contoh : Pada tahun 2021, Colonial Pipeline, perusahaan pipa bensin terbesar di Amerika Serikat, menjadi korban serangan ransomware yang mengakibatkan pencurian data dan gangguan operasional. Pelaku menuntut tebusan sebesar $4,4 juta dalam cryptocurrency untuk mengembalikan data yang dicuri.
- Pencegahan : Organisasi dapat mencegah pencurian data dengan menerapkan kontrol keamanan yang kuat, seperti enkripsi data, otentikasi dua faktor, dan edukasi karyawan tentang keamanan siber.

2. RANSOMWARE

- Modus: Pelaku menginfeksi sistem IT organisasi dengan malware ransomware, yang mengenkripsi data dan menuntut tebusan untuk mengembalikan akses ke data tersebut.
- Contoh: Pada tahun 2022, Kaseya, perusahaan manajemen perangkat lunak, menjadi korban serangan ransomware yang berdampak pada ribuan bisnis di seluruh dunia. Pelaku menuntut tebusan sebesar $4,5 juta dalam *cryptocurrency*.
- Pencegahan: Organisasi dapat mencegah serangan ransomware dengan menerapkan backup data reguler, patch sistem IT secara berkala, dan menggunakan solusi keamanan siber yang dapat mendeteksi dan mencegah malware.

3. SOCIAL NETWORK ENGINEERING

- Modus: Pelaku memanipulasi orang di media sosial untuk mengungkapkan informasi sensitif atau mengklik tautan berbahaya yang dapat menginfeksi perangkat mereka dengan malware.
- Contoh: Pada tahun 2023, scammers menggunakan media sosial untuk meniru identitas perwakilan perusahaan dan meminta pengguna untuk memberikan informasi pribadi atau keuangan.
- Pencegahan: Pengguna harus berhati-hati terhadap permintaan informasi sensitif di media sosial, memverifikasi identitas pengirim pesan, dan tidak mengklik tautan dari sumber yang tidak dikenal.

4. SERANGAN BERBASIS ARTIFICIAL INTELLIGENCE (AI):

- Modus: Pelaku menggunakan AI untuk membuat email phishing yang lebih meyakinkan, meniru suara manusia dalam panggilan telepon, atau menganalisis data keuangan untuk mengidentifikasi target *fraud*.
- Contoh: Pada tahun 2022, deepfake digunakan untuk membuat video yang meniru CEO perusahaan dan meminta karyawan untuk mentransfer uang ke rekening penipuan.
- Pencegahan: Organisasi harus menggunakan solusi keamanan siber yang dapat mendeteksi dan mencegah serangan AI, dan edukasi karyawan tentang bahaya deepfake dan serangan lainnya yang berbasis AI.

YUK, LAKUKAN TINDAKAN PENCEGAHAN!

1. Larangan nasabah menginformasikan PIN atau OTP pada petugas Penyelenggara Inovasi Teknologi Sektor Keuangan atau orang lain.
2. Meningkatkan pengawasan dan supervisi dari atasan, sehingga mengurangi perbuatan oknum yang tidak bertanggung jawab.
3. Manajemen Penyelenggara Inovasi Teknologi Sektor Keuangan harus menerapkan kontrol yang ketat terhadap setiap transaksi dan meningkatkan pengawasan internal.
4. Perhatikan gaya hidup pegawai Penyelenggara Inovasi Teknologi Sektor Keuangan yang ada.
5. Penyelenggara Inovasi Teknologi Sektor Keuangan melakukan sosialisasi secara berkesinambungan tentang anti *fraud* kepada pengurus dan semua pegawai. Antara lain terkait dengan aspek pidana penerimaan gratifikasi dan atau penggelapan.
6. Penetapan pemisahan fungsi (*segregation of duty*), tugas dan tanggung jawab dalam pelaksanaan pengelolaan aset Penyelenggara Inovasi Teknologi Sektor Keuangan. Misalnya rotasi dalam proses transaksi secara langsung, penggunaan mekanisme transaksi online, rotasi pegawai secara berkala, serta penerapan *four eyes principle* secara ketat.
7. Implementasi pengawasan secara menyeluruh oleh suatu fungsi, atau seorang karyawan yang memiliki tanggung jawab atas, audit internal pada Penyelenggara Inovasi Teknologi Sektor Keuangan. Implementasi pengawasan tersebut juga termasuk surprise audit.
8. Menyusun atau membentuk mekanisme pengaduan (*whistleblower*), termasuk mekanisme pelaporan kepada Dewan Komisaris dan Otoritas terkait.
9. Meningkatkan sistem pengendalian internal Penyelenggara Inovasi Teknologi Sektor Keuangan, antara lain dengan melakukan review secara periodik dan berkesinambungan.
10. Pengurus dan Pegawai Penyelenggara Inovasi Teknologi Sektor Keuangan memahami dampak dan risiko yang timbul terkait dengan pemberian dari pengguna atau calon pengguna dalam keterkaitan dengan pelaksanaan tugasnya.
11. Menyusun dan mengimplementasikan standar dan prosedur mekanisme pengelolaan aset Penyelenggara Inovasi Teknologi Sektor Keuangan, dan pengelolaan infrastruktur TI.
12. Pemeriksaan latar belakang pengurus dan pegawai Penyelenggara Inovasi Teknologi Sektor Keuangan.

VI. STRATEGI ANTI FRAUD

DEFINISI FRAUD

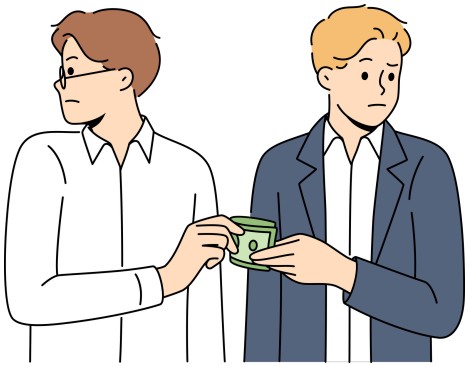
Fraud adalah tindakan penyimpangan atau pembiaran yang sengaja dilakukan untuk mengelabui menipu atau memanipulasi Penyelenggara Inovasi Teknologi Sektor Keuangan, konsumen atau pihak lain, yang terjadi di lingkungan Penyelenggara Inovasi Teknologi Sektor Keuangan dan/atau menggunakan sarana Penyelenggara Inovasi Teknologi Sektor Keuangan sehingga mengakibatkan Penyelenggara Inovasi Teknologi Sektor Keuangan, konsumen, atau pihak lain menderita kerugian dan/atau pelaku *fraud* memperoleh keuntungan keuangan baik secara langsung maupun tidak langsung.

JENIS PERBUATAN TERGOLONG FRAUD

Korupsi, penyuapan, penerimaan tidak sah, pemerasan, penyalahgunaan aset meliputi uang tunai, persediaan dan aset lainnya, penipuan, pembocoran informasi rahasia, dan tindakan lain yang dapat dipersamakan dengan Fraud.

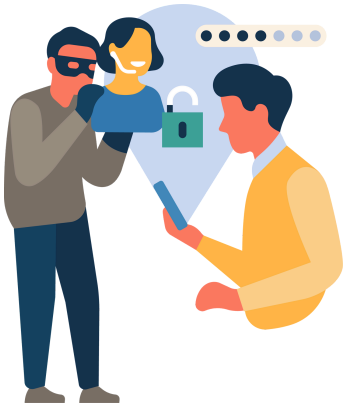
STRATEGI ANTI FRAUD BAGI INOVASI TEKNOLOGI SEKTOR KEUANGAN

1. Membuat prediksi proses kejadian *fraud* serta karakteristik dan jangkauan dari potensi *fraud*, diimplementasikan dalam bentuk sistem pengendalian *fraud*.
2. Merupakan bagian dari penerapan Manajemen Risiko, khususnya yang terkait dengan aspek sistem pengendalian intern.
3. Menggabungkan prinsip dasar dari Manajemen Risiko khususnya pengendalian internal dan tata kelola yang baik.
4. Membangun budaya sadar dan etika yang tahan terhadap kemungkinan *fraud* dalam organisasi perusahaan



KORUPSI

PEMBOCORAN DATA



IDENTITAS PALSU

VII. PENERAPAN MANAJEMEN RISIKO

PENGAWASAN AKTIF DIREKSI DAN DEWAN KOMISARIS

Pengawasan aktif Direksi dan Dewan Komisaris terhadap Fraud mencakup hal-hal yang menjadi kewenangan dan tanggung jawab Direksi dan Dewan Komisaris dalam penerapan Strategi Anti Fraud di Penyelenggara Inovasi Teknologi Sektor Keuangan. Kewenangan dan tanggung jawab tersebut paling sedikit sebagai berikut:

1. **Prinsip Dasar**
   - Menerapkan budaya dan kepedulian terhadap anti *fraud*
   - penandatanganan pakta integritas oleh seluruh jajaran organisasi
   - Meningkatkan awareness & pengawasan penerapan kode etik terkait pencegahan *fraud*
   - Menyusun & mengawasi penerapan strategi anti *fraud*
   - Melakukan pemantauan, menerapkan proses penindakan kasus dan evaluasi atas kejadian *fraud*, termasuk proses pengambilan keputusan, alur kerja dan kontrol
   - Mengembangkan saluran komunikasi yang efektif di eksternal Penyelenggara Inovasi Teknologi Sektor Keuangan dalam rangka pemahaman dan kepatuhan pada kebijakan dan prosedur.

2. Prinsip Lanjutan
- Prinsip dasar
- Menyusun dan mengawasi penerapan kode etik khusus terkait pencegahan *fraud*
- Mengembangkan kualitas sumber daya manusia (SDM)
- Memastikan Penyelenggara Inovasi Teknologi Sektor Keuangan memiliki Internal Control yang memadai.

KECUKUPAN KEBIJAKAN DAN PROSEDUR

Pembentukan unit atau fungsi yang menangani implementasi SAF atau yang membawahi audit internal dengan tugas pokok dan fungsi:

1. Merancang SAF bagi Penyelenggara Inovasi Teknologi Sektor Keuangan
2. Melaksanakan program kesadaran anti *fraud* (*fraud awareness*)
3. Menilai kepatuhan pelaksanaan SAF
4. Menetapan prosedur *wistleblowing* dalam organisasi
5. Menetapkan daftar red flag dalam jalur proses transaksi dalam organisasi

1. Prinsip Dasar

- Membentuk fungsi dalam struktur baik unit mandiri, atau dapat dirangkap oleh unit atau fungsi yang membawahi manajemen risiko.
- Menetapkan uraian tugas dan tanggung jawab yang jelas
- Pertanggungjawaban fungsi ada poin a di atas langsung kepada Direktur Utama, serta hubungan komunikasi dan pelaporan secara langsung kepada Dewan Komisaris
- Pelaksanaan tugas dilakukan oleh SDM yang memiliki integritas dan independensi.
- Membentuk dan menetapkan SOP untuk audit, pelaporan dan pertemuan secara rutin yang melibatkan pemangku kepentingan dalam organisasi

2. Prinsip Lanjutan

- Prinsip dasar
- Implementasi melalui fungsi dan/atau unit khusus dalam struktur organisasi
- Implementasi dilakukan oleh SDM yang memiliki kompetensi, integritas, dan independensi.

SISTEM PENGENDALIAN INTERNAL

Fokus Penyelenggara Inovasi Teknologi Sektor Keuangan dalam melakukan pengendalian dan pemantauan untuk meningkatkan efektifitas penerapan SAF.

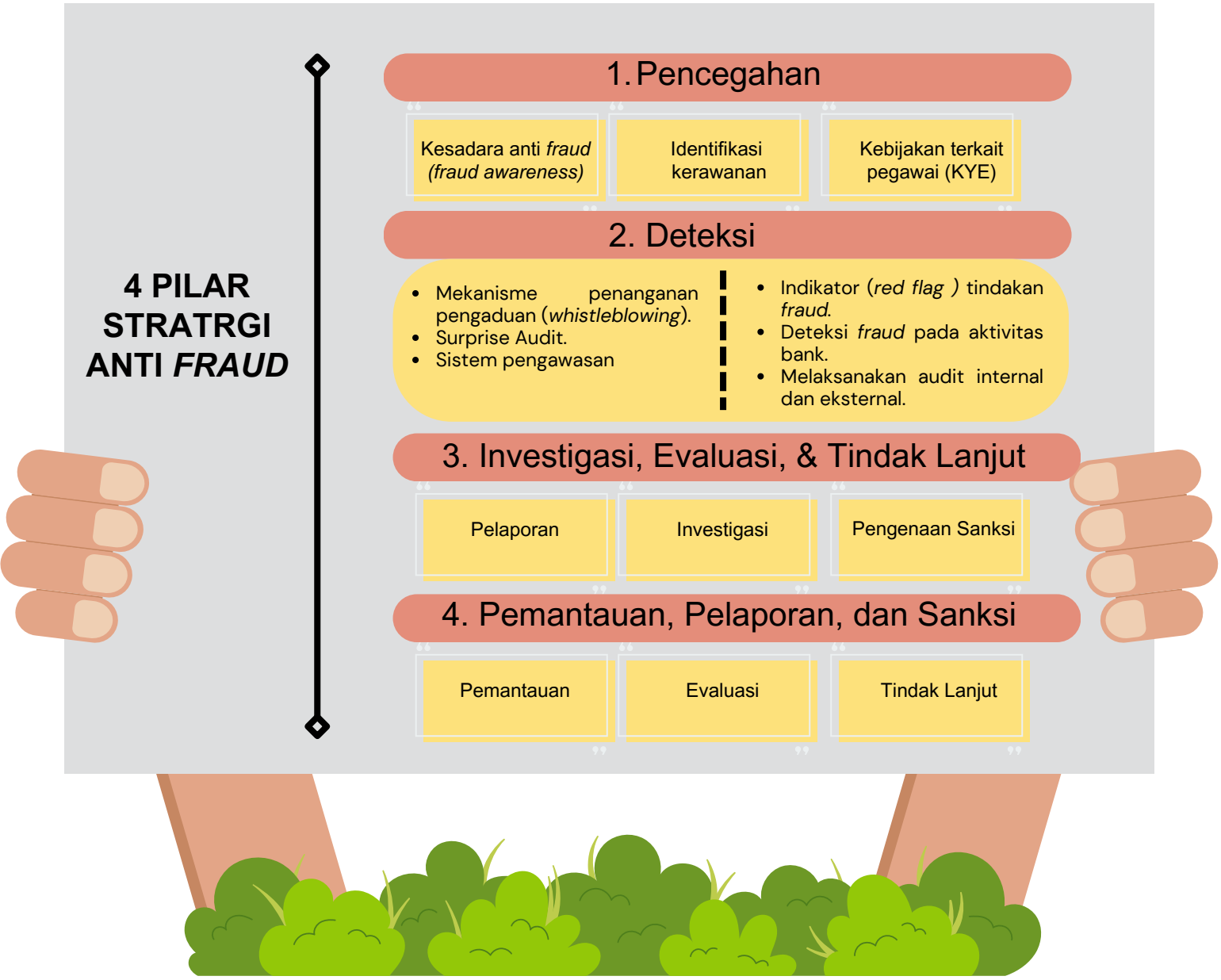
1. Prinsip Dasar

- Menyusun kebijakan dan prosedur pengendalian yang khusus ditujukan untuk pengendalian *fraud*
- Menyusun pengendalian melalui kaji ulang baik oleh manajemen (top level review) maupun oleh pejabat eksekutif yang membawahi pelaksanaan SAF
- Menyusun penetapan pemisahan fungsi dalam pelaksanaan aktivitas Penyelenggara Inovasi Teknologi Sektor Keuangan, misalnya penerapan four eyes principle dalam aktivitas perkreditan
- Melakukan pengendalian sistem informasi yang mendukung pengolahan, penyimpanan, dan pengamanan data secara elektronik untuk mencegah potensi terjadinya *fraud*
- Melakukan pengendalian lain dalam rangka pengendalian *fraud* seperti pengendalian aset fisik dan dokumentasi.

2. Prinsip Lanjutan

- Prinsip dasar
- Menyusun pengendalian dibidang SDM untuk efektivitas pengendalian *fraud*, misalnya kebijakan rotasi, kebijakan mutasi, cuti wajib, dan aktivitas sosial atau gathering
- Menyusun pengendalian sistem informasi, termasuk pengamanan data. Penyelenggara Inovasi Teknologi Sektor Keuangan wajib memiliki program kontinjensi yang memadai disertai dengan tersedianya sistem akuntansi untuk menjamin penggunaan data yang akurat dan konsisten dalam pencatatan dan pelaporan keuangan Penyelenggara Inovasi Teknologi Sektor Keuangan, antara lain melalui rekonsiliasi atau verifikasi data secara berkala.

EMPAT (4) PILAR STRATEGI ANTI FRAUD



1. PILAR I - PENCEGAHAN

1. Prinsip Dasar

a. Kesadaran anti *fraud*, antara lain diwujudkan melalui:

- Penyusunan dan sosialisasi deklarasi anti *fraud*,
- Program budaya anti *fraud* bagi pegawai,
- Program kepedulian dan kewaspadaan terhadap *fraud* bagi pengguna,
- Edukasi mengenai penalti atau akibat dari *fraud* kepada karyawan sebagai bagian dari onboarding process karyawan baru atau secara berkala
- Sosialisasi daftar red flag dan proses wistle-blowing dan memastikan budaya lapor yang terjamin untuk keamanan pelapor.

b. Kebijakan mengenal pegawai, sebagai wujud pencegahan *fraud* dari sisi SDM.

2. Prinsip Lanjutan

- Prinsip dasar
- Identifikasi kerawana, antara lain : dilakukan dengan mengidentifikasi risiko (dari internal atau eksternal) terjadinya *fraud* yang melekat pada setiap aktivitas Penyelenggara Inovasi Teknologi Sektor Keuangan. Hasil identifikasi dokumentasi dan diinformasikan kepada seluruh pihak dan dikinikan secara berkala khususnya dalam aktivitas yang berisiko tinggi.

2. PILAR II - DETEKSI

Pilar strategi anti *fraud* untuk identifikasi dan deteksi *fraud* dalam kegiatan usaha Penyelenggara Inovasi Teknologi Sektor Keuangan.

1. Prinsip Dasar

a. Kebijakan dan mekanisme penanganan pengaduan (whistleblowing), antara lain diwujudkan dalam pertimbangan:

- Perlindungan pelapor *fraud*,
- Regulasi terkait pengaduan *fraud*, mengacu pada ketentuan peraturan perundang-undangan,
- Sistem pelaporan *fraud* serta mekanisme tindak lanjutnya.

b. Sistem Pengawasan, tindakan pengujian pemeriksaan secara rahasia (oleh pihak independen dan/atau pihak internal Penyelenggara Inovasi Teknologi Sektor Keuangan secara berkala dan sewaktu-waktu jika diperlukan).

c. Melaksanakan audit internal dan eksternal.

2. Prinsip Lanjutan

- Prinsip dasar, antara lain dilakukan dengan pemeriksaan dadakan (surprise audit), perlu dilakukan khususnya pada unit bisnis dan aktivitas yang rawan terjadi *fraud*.
- Menentukan indikator (*Red Flag*) tindakan *fraud*, antara lain dilakukan dengan menetapkan metode deteksi *fraud* termasuk deteksi pemicu *fraud* pada masing-masing aktivitas Penyelenggara Inovasi Teknologi Sektor Keuangan.

3. PILAR III - INVESTIGASI, PELAPORAN, DAN SANKSI

1. Prinsip Dasar

- Investigasi (mengumpulkan bukti).
- Pelaporan, dengan mekanisme pelaporan yang efektif pada internal Penyelenggara Inovasi Teknologi Sektor Keuangan.
- Pengenaan Sanksi, dengan kebijakan dan mekanisme pengenaan sanksi yang efektif, adil, transparan, dan konsisten serta menimbulkan efek jera.
- Proses pemulihan akibat *fraud*.

2. Prinsip Lanjutan

- Prinsip dasar
- Investigasi (mengumpulkan bukti), standar investigasi paling sedikit mencakup antara lain: dilakukan dengan Penentuan pihak yang berwenang melaksanakan investigasi dengan mempertimbangkan independensi dan kompetensi yang dibutuhkan.
- Mekanisme investigasi (kebijakan Penyelenggara Inovasi Teknologi Sektor Keuangan untuk mendorong penyelidikan tepat waktu) untuk menindaklanjuti hasil deteksi dengan menjaga kerahasiaan informasi.

4. PILAR IV - PEMANTAUAN, EVALUASI, DAN TINDAK LANJUT

1. Prinsip Dasar

- Pemantauan, memantau tindak lanjut sesuai dengan ketentuan internal Penyelenggara Inovasi Teknologi Sektor Keuangan dan perundang-undangan.
- Evaluasi, memelihara data kejadian *fraud* yang bermanfaat untuk identifikasi dan evaluasi kelemahan dan penyebab terjadinya *fraud* serta perbaikan yang diperlukan.
- Tindak lanjut, menyusun tindak lanjut berdasarkan evaluasi memperbaiki dan menyempurnakan sistem pengendalian intern untuk mencegah terjadinya *fraud* yang serupa.

2. Prinsip Lanjutan

- Prinsip dasar
- Pelaksanaan evaluasi secara berkala terhadap sistem pengendalian *fraud* Penyelenggara Inovasi Teknologi Sektor Keuangan.

DAFTAR PUSTAKA

Anti-Phishing Working Group (2023). Phishing Activity Trend Report. https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf?_gl=1125rhw4_ga*MTU2Njc5MzY2Mi4xNzEzNTE4NTU2*_ga_55RF0RHXSR*MTcxMzUxODU1NS4xLjEuMTcxMzUxODY1Ny4wLjAuMA

Association of Certified Fraud Examiners (2020). Report to The Nations: *Global Study on Occupational Fraud and Abuse.* https://acfepublic.s3-us-west2.amazonaws.com/2020-Report-to-the-Nations.pdf

Association of Certified Fraud Examiner. (2020) Report to The Nations: Global Study on *Occupational Fraud and Abuse.* https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

Australian Financial Security Authority. (2020). AFSA Fraud Control Plan 2020 – 2022. https://www.afsa.gov.au/sites/default/files/afsa_fraud_control_plan_2020_-_2022.pdf

Association of Certified Fraud Examiners. Fraud 101: What Is Fraud?. https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

Badan Standarisasi Nasional. (2016). Sistem Manajemen Anti Penyuapan – Persyaratan d d*engan Panduan Penggunaan. Jakarta: Penulis*

Bank Syariah Indonesia. (2021). Kebijakan Anti Fraud PT Bank Syariah Indonesia Tbk. https://ir.bankbsi.co.id/misc/Kebijakan-Anti-Fraud-BSI.pdf

Bank of Ghana. (2021). Risk Management Guidelines. https://www.bog.gov.gh/wp-content/uploads/2021/05/BOG-Notice-No-BG-GOV-SEC-20 21-10-RISKMANAGEMENT-GUIDELINES-FOR-RCBs-Final.pdf

Cendrowski, Harry., et. al. (2007). The Handbook of Fraud Deterrence. Canada: John *Wiley & Sons, Inc.*

Center for The Protection of National Infrastructure. (2021). Employment Screening Quick *Guide.* https://www.cpni.gov.uk/employment-screening

Certified Information System Auditor. Ransomware 101. https://www.cisa.gov/stopransomware/ransomware-101

Chief Financial Officer. (2018). The Antifraud Playbook. https://www.cfo.gov/wp-content/uploads/2018/10/Interactive-Treasury-Playbook.pdf

Chartered Institute of Management Accountants. (2008). Fraud Risk Management: A Guide *to Good Practice. CIMA Global.* https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

Committee of Sponsoring Organizations of The Treadway Commission. (2016). Fraud Risk *Management Guide: Executive Summary.* https://www.coso.org/documents/coso-fraud-risk-management-guide-executive-summary. pdf

Departemen Pemeriksaan Khusus dan Investigasi Perbankan. (2018). Dugaan Tindak *Pidana Perbankan: Penyebab, Dampak dan Mitigasinya. Jakarta: Otoritas Jasa Keuangan.*

DiNapoli, Thomas P. Red Flags for Fraud. Office of The New York State Comptroller. https://www.osc.state.ny.us/files/local-government/publications/pdf/red_flags_fraud.pdf

European Banking Authority. (2015). Decision of The European Banking Authority Adopting *the Anti-Fraud Strategy 2015-2017.* https://www.eba.europa.eu/sites/default/documents/files/documents/10180/15718/3b6f4f06-643a-43a9-8c8d-189819479260/EBA%20DC%20120%20%28Decision%20on%20Anti%20Fraud%20Strategy_%29.pdf?retry=1

European Training Foundation. (2014). ETF Anti-fraud Strategy and Action Plan. https://www.etf.europa.eu/sites/default/files/2018-07/ETF%20Anti-Fraud%20Strategy.pdf_.pdf

Fraud Advisory Panel. (2011). An Indtroduction to Fraud Indicators. https://www.fraudadvisorypanel.org/wp-content/uploads/2015/04/Fraud-Facts-14B-FraudIndicators-Nov11.pdf

Government Accountability Office. (2015). A Framework for Managing Fraud Riskis in *Federal Programs.* https://www.gao.gov/products/gao-15-593sp

Groenewald, Liezl. (2020). Whistleblowing Management Handbook. The Ethic Institute. https://www.tei.org.za/wp-content/uploads/2020/09/Whistleblowing-Management-Handbo ok_Final-for-Web-.pdf

ID4D Practitioner's Guide (English). Identification for Development Washington, D.C. : *World Bank Group.* http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-G uide

Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905*

Iyer, Nigel dan Martin Samociuk. (2006). Fraud and Corruption: Prevention and Detection. *USA: Gower Publishing Company.*

Karyono. (2013). Forensic Fraud. Yogyakarta: Andi

Lembaga Pengembangan Fraud Auditing. (2013). Pelatihan Fraud Auditing: Tingkat Dasar *(FA.1) Modul 1, 2 & 3. Jakarta: Edisi Revisi.*

Luburic, Radoica. (2017). Strengthening the Three Lines of Defence in Terms of More *Efficient Operational Risk Management in Central Bank. Journal of Central Banking Theory and Practice, 1, 29-53.*

Luburic, Radoica, et.al. (2015). Quality Management in Terms of Strengthening The "Three *Lines of Defence" in Risk Management Process Approach. International Journal for Quality Research 9, 243-250*

National Bank for Agriculture and Rural Development. (2016). Frauds – Guidelines for *Classification, Reporting and Monitoring of Frauds.* https://www.nabard.org/demo/auth/writereaddata/tender/10011751042016-Cir-284-E.pdf

National Institute of Standards and Technology. (2024). The NIST Cybersecurity *Framework (CSF) 2.0.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Nurharyanto. (2013). Sistem Kendali Kecurangan (Fraud) Perbankan: Konsepsi, Asesmen *Risiko dan Penerapan Kebijakan Anti-Fraud. Jakarta: TINTA Creative Production.*

Nurhidayat, Ilmah dan Bevaola Kusumasari. (2017). Revisiting Understanding of The *Whistleblowing Concept in The Context of Indonesia. Policy and Governance Review, 1, 165-177.*

Office of the Comptroller of the Currency. (2019). Operational Risk: Fraud Risk *Management Principles.* https://www.occ.treas.gov/news-issuances/bulletins/2019/bulletin-201937.html

Otoritas Jasa Keuangan. (2020). Buku Memahami dan Menghindari Tindak Pidana *Perbankan. Jakarta: Penulis.*

Purba, Bona P., (2015). Fraud dan Korupsi: Pencegahan, Pendeteksian, dan *Pemberantasannya. Jakarta: PT Kawan Pustaka.*

PricewaterhouseCoopers. (2022). PwC's Global Economic Crime and Fraud Survey 2022. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Safii, Benny Imam. (2021). Strategi Anti Fraud BRI. Forum FGD OJK tentang Panduan *Penerapan SAF bagi BPR.*

Tunggal, Amin Widjaja. (2016). Pencegahan dan Pendeteksian Kecurangan. *Jakarta: Harvindo.*

Wikipedia contributors. (2024, January 18). Sarbanes–Oxley Act. *Wikipedia.* https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

Wikipedia contributors. (2024, April 17). Enron scandal. Wikipedia. https://en.wikipedia.org/wiki/Enron_scandal

Wikipedia contributors. (2024, April 18). Deepfake. *Wikipedia.* https://en.wikipedia.org/wiki/Deepfake

Wikipedia contributors. (2024b, March 15). WorldCom scandal. Wikipedia. https://en.wikipedia.org/wiki/WorldCom_scandal