GLOBAL PERSPECTIVES & INSIGHTS

FRAUD

BAGIAN 1: Kecurangan dalam *Cryptosphere*

BAGIAN 2: Auditor Internal and Investigator Kecurangan: Sebuah Kemitraan yang Bernilai

BAGIAN 3: Efek Setelah Kejadian: Kecurangan pada Era Setelah COVID

The Institute of Internal Auditors

Daftar Isi

Diterjemahkan dan diselaraskan oleh IIA Indonesia Volunteer:

1. Dyan Garneta P. Sari, CIA, CRMA, CGAP
2. Fauzan Wahyuabdi Pratama, CIA, CGAP
3. Indra Permana, CIA, CRMA
4. Diana Laurencia Sidauruk, CIA
5. Riani Nurainah Lisnasari, CIA
6. I Gde Wiyadnya
7. Agnes Maria Widiyanti

Bagian 1

Kecurangan dalam *Cryptosphere*

Tentang para Ahli

Dana Lawrence, CIA, CRMA, CFSA, CAMS, CRVPM

Dana Lawrence adalah Kepala Staf Kepatuhan pada Fideseo. Ia seorang ahli yang diakui dan pemimpin pada penyusunan, pengukuran, serta remediasi program kepatuhan, manajemen risiko organisasi (ERM), audit internal, dan tata kelola yang kompleks. Karir Lawrence dalam bidang teknologi dan jasa keuangan meliputi hipotek, perbankan komunitas, bank besar di AS dan global, kemitraan perbankan terbuka, teknologi keuangan, dan *crypto*. Dia memegang peran kepemimpinan senior, bekerja langsung dengan regulator perbankan dan auditor internal/eksternal. Lawrence adalah pembicara publik dan pembawa acara yang popular, berbicara pada acara lokal, nasional, dan global dengan jumlah partisipan mencapai 40.000 orang. Dia adalah seorang relawan dan pemuka pemikiran yang memiliki komitmen pada berbagai kelompok antara lain The IIA.

Lourdes Miranda, CAMS, CCE, CCFI, CEIC, CFE, CRC, FIS, MS

Lourdes Miranda adalah Kepala Staf Kepatuhan pada SendCrypto, sebuah perusahaan teknologi *blockchain*. Dia merupakan mantan petugas CIA dan analis FBI dengan lebih dari 20 tahun pengalaman pada pemerintahan dan korporasi, dengan spesialisasi pada bidang investigasi kejahatan keuangan dan pengumpulan serta analisis intelijen secara global. Dia memiliki pengalaman lapangan yang luas dengan target pada pencuci uang dan pemodal teroris. Sejak 2017, Miranda bekerja untuk FinTechs sebagai seorang investigator kripto senior, petugas kepatuhan senior dan manajer risiko, pembangun kepatuhan, investigasi, kripto, dan tim intelijen dan program pelatihan. Dia juga seorang penulis, instruktur, dan kontributor pada berbagai kursus daring sebagai ahli materi pokok. Sebagai tambahan, Miranda juga seorang Anggota Dewan Penasehat untuk Toronto Compliance & AML Enterprise (TCAE) yang berbasis di Kanada.

Pendahuluan

Crypto dan kecurangan pada percakapan global

Sam Bankman-Fried, pendiri karismatik pertukaran *crypto* FTX, pernah memiliki kekayaan $26,5 miliar. Sebagai seorang pemimpin yang pada suatu titik merupakan pertukaran terbesar ketiga di pasar *crypto*, Bankman-Fried dan FTX merupakan kesayangan dari berbagai investor terkenal seperti BlackRock dan pemain NFL Tom Brady. Namun, dia kehilangan semua kekayaannya hampir dalam semalam di salah satu keruntuhan perusahaan paling dramatis dalam sejarah modern.

Bankman-Fried ditahan pada 13 Desember 2022 di Bahama. Menurut laporan yang diterbitkan, dia menghadapi berbagai tuntutan seperti *wire fraud* (kecurangan yang melibatkan penggunaan suatu bentuk telekomunikasi/internet), konspirasi *wire fraud*, kecurangan sekuritas, konspirasi kecurangan sekuritas, dan pencucian uang.

Sementara ada hal yang membuat manusia tertarik dalam pertunjukan kehancuran yang luar biasa tersebut, kejadian itu juga memunculkan pertanyaan yang lebih besar tentang aset digital. Sejajar dengan skandal seperti Tornado Cash dan Bitzlazo, keruntuhan FTX dan dampak lanjutannya pada industri telah memicu banyak pertanyaan tentang kelangsungan jangka panjang aset *crypto* – setidaknya dalam kondisi sekarang, dimana Kepala U.S. Securities and Exchange Commission menyebutnya sebagai "Wild West".

Walaupun dibangun pada teknologi *blockchain*, yang merupakan salah satu cara paling aman untuk memelihara aset dan informasi *crypto*, jika pimpinan yang sangat menonjol pada salah satu pertukaran mata uang *crypto* paling terkemuka dunia diduga dapat melakukan tindakan kecurangan skala besar, kerentanan lain apa lagi yang dapat terjadi pada perusahaan yang beroperasi di industri pada berbagai kapasitas? Bagaimana lanskap risiko berubah dengan meroketnya aset *crypto*, dan bagaimana beberapa organisasi dan fungsi internal audit mereka berhasil merespon perubahan ini?

Bagian 1 dari seri yang terdiri atas tiga bagian tentang kecurangan ini akan menjawab pertanyaan-pertanyaan tersebut dengan menjelaskan skema kecurangan umum yang terlihat pada tahap awal dunia aset *crypto*. Untuk infomasi lebih tentang topik ini, IIA akan menyelenggarakan pemutaran ulang dari seminar daring terkini "*Fraud perspectives: Blockchain, Crypto, and KYC*", dengan tanya jawab langsung dengan ahli yang menguasai materi pokok yang dikutip dalam dokumen ringkasan ini.

Ketidakpastian pada *Cryptosphere*

Masa depan yang menarik, namun berisiko

Sekarang organisasi memberikan perhatian

Walaupun implikasinya sangat luas dan tidak kurang revolusioner, teknologi *blockchain* relatif mudah untuk dipahami secara konseptual sebagai suatu hal yang tidak lebih dari catatan log yang selalu bertumbuh terus menerus atas suatu transaksi aset digital yang dapat dibagikan dan disimpan secara virtual pada struktur jaringan apapun. Yang membedakannya adalah ia menggunakan metodologi verifikasi yang terus menerus mengenkripsi blok dengan setiap transaksi baru sehingga membuatnya lebih aman.

"Teknologi itu sendiri sangat rumit dan perlu bertahun-tahun pelatihan dan pendidikan untuk menganalisisnya, tetapi saya menganggap *blockchain* itu sendiri sebagai laporan keuangan," kata Lourdes Miranda, Kepala Staf Kepatuhan SendCrypto, sebuah perusahaan teknologi *blockchain*. "*Blockchain* memiliki informasi berkaitan dengan siapa yang mengirim aset, di mana aset tersebut didepositokan, jika ada penarikan, dan saldo yang dihasilkan."

Mata uang *crypto* dapat dikatakan sebagai aset yang paling terkenal yang menggunakan teknologi ini, yang menciptakan sistem moneter *open-source* terdesentralisasi atau sistem yang terpisah dari pengaruh entitas, seperti bank sentral – tapi contoh lain dari aset *crypto* berdasarkan teknologi *blockchain* termasuk *non-fungible tokens* (NFTs), *distributed ledger technologies* (DLTs), token *game*, dan lain-lain.

Namun demikian, seiring dengan kecepatan belajar industri, hanya karena asset kripto dibangun di atas teknologi yang aman hampir tidak mungkin untuk dimanipulasi dengan metode tradisional, bukan berarti bahwa pengadopsinya bebas kebal dari risiko. Runtuhnya FTX mengilustrasikan hal ini lebih dalam dari satu cara. Misalnya, hal ini menunjukkan betapa buruknya tata kelola perusahaan dan pengendalian internal yang tidak tepat dapat merusak, tidak hanya untuk organisasi, tetapi juga untuk investor di seluruh lanskap industri.

Hal ini merupakan salah satu inti surat terbaru dari Presiden dan CEO IIA Anthony Pugliese kepada Kongres AS yang meminta mereka agar membentuk persyaratan baru untuk mendorong tata kelola korporasi dalam pertukaran mata uang *crypto*, perusahaan teknologi *blockchain*, pasar NFT, dan platform Web3 yang beroperasi di AS. "Tidak terhitung investor yang sekarang membayar harga kegagalan FTX," kata Pugliese. "Jelas bahwa kita tidak dapat mengandalkan pertukaran *crypto* tanpa regulasi untuk melakukan hal yang benar oleh mereka sendiri – kita perlu untuk mengamanatkan standar tata kelola korporasi yang lebih kuat dan memastikan akuntabilitas disaat pertukaran ini tidak melindungi pelanggan mereka. Ketika *bad actor* korporasi gagal, tidak seharusnya investor yang menanggung dampaknya".

Pugliese menekankan keruntuhan FTX dan konsekuensi pasarnya dapat dimitigasi melalui aksi fungsi audit internal yang baik. "Keruntuhan FTX merupakan pengingat terakhir bahwa organisasi tanpa audit internal yang kuat adalah, sebaik-baiknya bermain dengan api, dan seburuk-buruknya menyiapkan mereka sendiri dan pemangku kepentingannya kepada bencana – dan suatu hal yang secara keseluruhan dapat dicegah – kehancuran," katanya.

Perhatian Pugliese dan lain-lainnya tidak diabaikan. Pada 3 Januari 2023, *Federal Reserve, Federal Deposit Insurance Corp* (FDIC) dan *Office of the Comptroller of the Currency* (OCC) merilis pernyataan bersama untuk pertama kalinya tentang mata uang *crypto*. Di dalamnya, mereka menyoroti berbagai jenis risiko yang dapat terjadi pada organisasi perbankan yang beroperasi pada mata uang *crypto* dalam berbagai bentuk, misalnya:

- Risiko kecurangan dan penipuan antar sesama partisipan aset *crypto*.
- Ketidakpastian hukum yang berkaitan dengan praktik kustodian, penebusan, dan hak kepemilikan.
- Representasi dan pengungkapan yang tidak akurat atau menyesatkan dari perusahaan aset *crypto.*
- Volatilitas yang signifikan pada pasar aset *crypto,* yang efeknya termasuk dampak potensial pada aliran deposit yang terkait dengan perusahaan aset *crypto.*
- Risiko penularan dalam sektor aset *crypto* sebagai hasil dari saling keterkaitan antarpartisipan aset *crypto* tertentu, termasuk melalui pinjaman, investasi, pendanaan, jasa, dan kesepakatan operasinal yang tidak jelas.
- Manajemen risiko dan praktik tata kelola di dalam sektor aset *crypto* menunjukkan kurangnya kematangan dan kekuatan.
- Meningkatnya risiko berkaitan dengan jaringan terbuka, publik, dan/atau terdesentralisasi, atau sistem serupa.

Sementara seluruh risiko tersebut layak untuk didiskusikan (dan banyak kasus dapat diterapkan pada organisasi di luar bank yang berkecimpung dalam *crypto*), ringkasan ini akan membatasi fokus pada tindakan kecurangan yang dilakukan pada peserta *crypto* dan bentuk menonjol yang mereka lakukan pada lingkungan saat ini.

Sebuah Lanskap yang Matang untuk Kecurangan

Sebuah lanskap risiko yang terus berkembang

Sebuah alat baru di dalam kotak peralatan *bad actor*

Sementara aset *crypto* memiliki serangkaian karakteristik yang menguntungkan seperti transparansi dan enkripsi yang sangat canggih terhadap manipulasi, karakteristik yang sama ini telah membuat aset tersebut (dan teknologi *blockchain* di belakangnya) sebagai alat yang ampuh bagi mereka yang ingin melakukan kecurangan.

Memang, imbauan kepada *bad actor* inilah yang menarik perhatian regulator dan penegak hukum. "Satu-satunya alasan mengapa pelanggan peduli dengan aset *crypto* adalah karena *bad actor* menggunakannya untuk mendanai operasional dan pencucian uang", kata Miranda, yang meneliti kejahatan keuangan untuk CIA dan FBI selama hampir 30 tahun. "*Blockchain* sangat sulit untuk dimanipulasi, namun dapat digunakan melalui suatu cara yang mendorong aktivitas jahat."

Salah satu metodenya, misalnya, adalah penggunaan identitas palsu dalam *blockchain*. "Hal ini sangat besar di *cryptosphere*", kata Miranda. "*Bad actor* akan menggunakan legitimasi, identitas sah yang dibeli pada pasar gelap untuk melewati proses *know your customer* (KYC) saat mereka membuka *wallet*. Identitas ini tidak memiliki latar belakang kriminal dan tidak ada di daftar hitam manapun – mereka sepenuhnya bersih. Kemudian, dengan nama bersih ini mereka dapat memindahkan uang yang sebagian besar tidak terdeteksi sampai investigator dapat melihat tren kecurangan dengan mata mereka sendiri."

Industri aset *crypto* juga telah memperkenalkan berbagai alat yang, meski dirancang untuk kenyamanank pelanggan, memiliki berbagai celah yang dapat dieksploitasi. Inisiator kecurangan, misalnya, dapat membuat sentral transaksi *crypto* seperti ATM bitcoin, bbersama dengan telepon sekali pakai untuk menghindari pelacakan dari penegak hukum.

"Katakan misalnya saya di New York, dan saya ingin memindahkan uang dan saya harus membayar para *bad actor* yang bekerja untuk saya di Miami. Mereka ingin dibayar dan dibayar dengan cepat. Saya tidak akan menggunakan cek dan saya tidak dapat menggunakan komputer atau laptop karena pelacakan alamat IP, sehingga yang saya lakukan adalah menuju ke ATM Bitcoin di New York dan menggunakaan uang uang kas dan telepon sekali pakai. Dengan cara ini, saya dapat membayar orang-orang sambal menghindari protokol anti pencucian uang. Itulah kecurangan," kata Miranda.

Pig butchering

Taktik kecurangan umum lainnya yang dapat digunakan oleh *bad actor* dikenal dengan istilah grafis "*pig butchering*". Hal ini pada pada dasarnya merupakan konsep pelaku kecurangan secara metafora "menggemukkan" korban mereka dengan menginvestasikan banyak waktu dengan mereka untuk membangun kepercayaan," kata Dana Lawrence, Kepala Staf Kepatuhan pada perusahaan konsultan bisnis dan teknologi Fideseo. Waktu yang diinvestasikan oleh pelaku kecurangan dapat terjadi di mana saja, menurut Lawrence, namun yang paling menonjol dilakukan adalah bisa di media sosial maupun melalui teks selama berminggu-minggu atau berbulan-bulan. Lawrence mengutip LinkedIn secara spesifik sebagai sebuah platform yang disukai, serta situs sosial seperti Twitter.

Pada kasus-kasus ini, *bad actor* biasanya akan menampilkan diri mereka sebagai pemberi pengaruh atau orang dalam yang telah berhasil berinvestasi di dalam mata uang *crypto*. Seiring waktu, mereka akan mengunggul-unggulkan manfaat mata uang *crypto* sebagai upaya untuk membuat korban mentransfer aset kepada mereka. Dalam beberapa kasus, pelaku kecurangan bahkan memberikan laporan keuangan palsu untuk kepada korban agar tampak ada keuntungan besar yang dihasilkan.

Meskipun mudah untuk membaca tanda-tanda ini dan cukup jelas untuk dikenali, pelaku kecurangan dalam kasus ini telah menjadi sangat canggih. Tim penipu yang berbasis di negara-negara seperti Kamboja dan Tiongkok, misalnya, telah mendapatkan pelatihan mendalam dari para psikolog tentang cara membuat orang paling rentan untuk membuat keputusan yang tidak tepat.

"Mereka telah dilatih oleh psikolog untuk mencari tahu cara terbaik dalam untuk memanipulasi orang lain," kata Jeff Rosen, seorang jaksa wilayah Santa Clara County, California dalam sebuah wawancara dengan CNN. "Anda sedang berurusan dengan orang yang akan menggunakan berbagai teknik psikologi untuk membuat Anda rentan dan tertarik untuk menyisihkan uang Anda," [1]

Pump and dump

Bentuk kecurangan besar lain dalam dunia*cryptosphere* dan juga telah lama diketahui oleh para pengamat pasar saham: dikenal dengan sebutan skema *"pump and dump"*.

"Skema ini pada umumnya dimulai dari adanya sekelompok orang yang membuat proyek *crypto* baru, misalnya token, lalu menggunakan sumber daya (biasanya dengan bantuan *influencer*) untuk membuat promosi dalam platform seperti Twitter atau Discord," kata Lawrence. "Selalu terdapat fluktuasi dalam pasar kripto yang disebabkan likuiditas. Artinya, bila sejumlah orang membeli suatu aset secara bersamaan, maka terjadi guncangan di pasar sehingga harga naik. Saat ini terjadi, para pelaku kejahatan yang memegang aset dalam jumlah besar tiba-tiba akan menjualnya untuk mendapatkan keuntungan, seketika harga akan turun dan meninggalkan para investor lain dengan aset yang pada dasarnya bernilai nol."

Red flag dalam situasi ini, kata Lawrence, adalah kurangnya pengungkapan kepada para investor bahwa kehilangan segalanya merupakan kemungkinan yang nyata. Para pelaku juga biasanya menggunakan pesan *copy-paste* dalam media sosial maupun ruang diskusi dengan menggunakan nama-nama yang mirip. Ketika skema ini berhasil, nama-nama ini biasanya akan menghilang dan para pelaku akan tetap anonim (tidak diketahui nama sebenarnya).

Contoh kecurangan lainnya dalam konteks aset *crypto*

Kecurangan berbasis *crypto* tidaklah selalu rumit. Dalam dunia *crypto*, seringkali yang dibutuhkan pelaku kejahatan hanyalah sebuah kesempatan yang tepat. Misalnya, sementara *blockchain* menjaga aset digital tetap aman, semua yang diperlukan untuk melewati keamanan dan mencuri isi dompet *crypto* adalah dengan mendapatkan *private key* — sebuah rangkaian nomor yang dapat dimuat pada serbet restoran yang tertinggal di mana saja sehingga siapa pun bisa menemukannya.

"*Private key* adalah identitas digital anda dalam pasar *crypto*, dan siapapun yang memilikinya dapat melakukan transaksi atau mencuri koin *crypto* Anda," kata Lawrence. "Bila seseorang mendapat akses, dan menguras Bitcoin saya, tidak ada yang bisa saya lakukan. Saya tidak bisa menagih kembali atau mengadu kepada siapa pun, tidak ada lembaga perlindungan konsumen atau pun regulator untuk menanganinya – aset saya benar-benar hilang."

Seiring meningkatnya maturitas pasar *crypto*, layanan keamanan *crypto* pun muncul untuk melindungi *key,* baik milik individu maupun perusahaan, dari kecerobohan dalam penyimpanan, namun cukup mengejutkant bahwa metodologi yang digunakan dalam beberapa kasus masih primitif. Menurut Lawrence, solusi yang digunakan adalah menyimpan *key* tersebut dalam brankas di pegunungan terpencil. Di samping itu, asuransi *crypto* juga tersedia sebagai jaring pengaman bagi perusahaan yang mampu membelinya, tetapi

[1]. Isobel Rafferty, "Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments," Insurance Times, July 18, 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

pada tahap ini seluruh industri sedang berjuang dengan profitabilitas, sehingga memaksa perusahaan asuransi untuk menjadi sangat selektif sambal terus menawarkan perlindungan yang justru sedang menyusut dari tahun ke tahun.

Dalam sebuah artikel yang diterbitkan di Insurance Times, Inggris, seorang mitra grup Asuransi RPC, James Wickes, membahas tantangan asuransi *crypto*. "Penjamin yang saat ini masih aktif di asuransi aset *crypto* cenderung ingin meninjau pernyataan pada kebijakan untuk membatasi potensi paparan dari volatilitas pasar *crypto*, seperti terjadinya *market crash* baru-baru ini," katanya. "Pasar asuransi ini masih sangat muda dan masih harus dilihat apakah penyedia asuransi akan siap untuk menyediakan kapasitas yang cukup dalam memenuhi permintaan dan seberapa berani mereka memperluas cakupan perlindungan di luar risiko pencurian tradisional." [2]

Terlepas dari tindakan pencegahan ini, masih ada alat yang dapat digunakan oleh *bad actor* untuk menggunakan aset *crypto* dan *blockchain* tanpa secara langsung melakukan *bypass* melalui akun yang sudah ada — yaitu *mixer*, juga dikenal sebagai *tumbler*. Salah satu fitur inti dari *blockchain* adalah transparansinya; dalam *blockchain explorer* mana pun, siapa pun dapat melihat catatan semua transaksi *blockchain* sejak peluncuran *cryptocurrency* pada tahun 2009. *Mixer* memungkinkan penggunanya untuk mencampuradukkan jumlah aset *crypto* sebelum mengirimkannya ke penerima yang dituju, memberi mereka anonimitas karena sangat sulit untuk menguraikan dengan tepat siapa yang mengirim aset, berapa banyak, dan kepada siapa. Dengan menggunakan *mixer*, yang akan ditampilkan oleh *explorer* adalah bahwa satu orang, serta beberapa orang lainnya, mengirimkan aset ke *mixer*, lalu mengirimkan aset dalam jumlah yang bervariasi ke berbagai orang lainnya. Hasilnya, pada intinya, menyerupai bentuk pencucian uang yang disempurnakan.

Menghadapi kenyataan ini, organisasi yang memilih untuk eksis di *cryptosphere* harus menerima bahwa mereka bertanggung jawab sendiri dalam hal mitigasi risiko. Ini tidak berarti bahwa *crypto* harus dihindari, tetapi ini berarti bahwa kepatuhan, kontrol internal yang baik, deteksi penipuan dan upaya pencegahan, serta audit internal harus memainkan peran besar dalam bidang *crypto* dari tingkat dewan hingga ke tingkat bawah.

[2]. Isobel Rafferty, "Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments," Insurance Times, July 18, 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

Di Mana Audit Internal Dapat Dimulai

Regulasi yang telah ada dan beberapa yang akan terbit

Panduan yang telah diterbitkan

Seperti yang disebutkan sebelumnya, kerangka regulasi yang dapat digunakan perusahaan untuk menangani keamanan dan tata kelola terkait aset *crypto* serta risiko berbasis kecurangan masih sangat sedikit. Namun, industri tertentu seperti jasa keuangan tidak sepenuhnya kehilangan sumber daya terkait tata kelola yang tepat dalam perlindungan aset digital — banyak di antaranya berlaku untuk mata uang *crypto*.

Pada bulan Oktober 2022, Uni Eropa memperkenalkan sebuah teks kesepakatan dari The Markets in Crypto-Assets (MiCA) Regulation**,** yang merupakan salah satu upaya pertama secara global pada peraturan pemasaran *cryptocurrency* yang komprehensif, peraturan tersebut telah diajukan hingga April 2023 untuk diterjemahkan ke dalam 24 bahasa yang berbeda. Jika diadopsi secara formal, peraturan tersebut akan:

- Secara resmi mendefinisikan aset *crypto* sebagai "representasi digital dari nilai atau hak yang dapat ditransfer dan disimpan secara elektronik, menggunakan teknologi *ledger* terdistribusi atau teknologi serupa." Selain itu, ditawarkan empat kategori aset *crypto* yang berbeda: *asset-referenced tokens*, *e-money tokens*, *utility tokens*, dan kategori keempat untuk aset *crypto* yang tidak termasuk dalam tiga kategori lainnya.
- Secara resmi membuat penyedia *crypto* bertanggung jawab jika mereka kehilangan aset *crypto* milik investor.
- Mengharuskan para pelaku pasar aset *crypto* untuk menyatakan informasi tentang dampak lingkungan dan iklim.
- Tumpang tindih dengan undang-undang tentang anti pencucian uang, dan akan menugaskan European Banking Authority (EBA) untuk memelihara daftar publik penyedia layanan aset *crypto* yang tidak patuh.
- Mewajibkan penyedia aset *crypto* memiliki otorisasi untuk beroperasi di Uni Eropa.
- Memberikan kerangka kerja yang handal untuk "*stablecoin*" (*cryptocurrency* yang dipatok ke aset referensi eksternal), yang akan mengharuskan setiap pemegang *stablecoin* untuk ditawari klaim kapan saja oleh penerbit secara gratis.[3]

Di Amerika Serikat, sebuah pernyataan bersama dari *Federal Reserve, Federal Deposit Insurance Corporation* (FDIC), dan *Office of the Comptroller of the Currency* (OCC) menawarkan beberapa sumber daya bagi perusahaan di Amerika Serikat dalam bentuk panduan yang dirancang untuk membantu "organisasi perbankan terlibat dalam pengawasan aktivitas terkait aset kripto yang telah ada maupun yang masih diusulkan."[4] Ini termasuk:

- OCC Interpretive Letter 1179 "Klarifikasi Penafsiran Kepala Penasihat: (1) Kewenangan Bank untuk Terlibat dalam Aktivitas *Cryptocurrency* Tertentu; dan (2) Kewenangan OCC terhadap Piagam National Trust Bank."
- Federal Reserve SR 22-6/ CA 22-6: "Keterlibatan dalam Aktivitas Terkait Aset Kripto oleh Organisasi Perbankan yang Diawasi Federal Reserve."

---

3. General Secretariat of the Council, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," Council of the European Union, October 5, 2022, https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.

4. "Joint Statement on Crypto-Asset Risks to Banking Organizations, Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Office of the Comptroller of the Currency, January 3, 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

- FDIC FIL-16-2022 “Prosedur Umpan Balik Pemberitahuan dan Pengawasan untuk Institusi yang Diawasi FDIC yang Terlibat dalam Kegiatan Terkait Kripto.”

Ini bukanlah satu-satunya sumber daya yang telah tersedia. Setelah keruntuhan FTX, SEC juga merilis panduan bagi perusahaan untuk mengungkapkan keterlibatan mereka dengan perusahaan komoditas digital.

Nilai edukasi

Dengan asumsi dokumen-dokumen tersebut diadopsi, undang-undang Uni Eropa yang diusulkan akan berlaku pada tahun 2024, tetapi hampir pasti tidak akan menjadi yang terakhir. Saat kondisi peraturan yang masih tambal sulam dari bulan ke bulan, tindakan paling tepat auditor internal adalah melakukan segala upaya untuk tetap mengikuti perubahan dan mengartikulasikan dengan jelas perubahan tersebut kepada dewan dan pemangku kepentingan yang terkait.

Saat ini, auditor internal juga harus mengartikulasikan kepada para pemangku kepentingan peraturan lain yang tersedia yang mungkin berlaku berkaitan dengan aktivitas *crypto* mereka. Misalnya, kata Lawrence, sebuah perusahaan yang menawarkan mata uang *crypto* mereka sendiri mungkin memerlukan pendaftaran di U.S. Financial Crimes Enforcement Network — hal penting yang dapat dengan mudah diabaikan karena *crypto* tidak secara khusus diatur dalam undang-undang. "Ada banyak ketidakpastian sekarang," katanya. “Tergantung dari pertimbangan auditor internal untuk memberi tahu para pemimpin tentang apa yang berlaku dan apa yang tidak.”

Berfokus pada teknologi baru juga tidak boleh mengalihkan perhatian perusahaan dari *best practice* dalam perlindungan aset digital, termasuk penggunaan *virtual private network* (VPN) dan keamanan yang tepat, pengumpulan, dan, jika diperlukan, pemusnahan informasi profil pengguna — terutama konsumen. “Profil pengguna adalah pengendalian organisasi yang kritis,” kata Miranda. “Ketika saya sedang mengaudit sebuah perusahaan, saya akan memeriksa untuk memastikan bahwa profil pengguna sesuai dengan aktivitas transaksionalnya. Misalnya, informasi geografis sangat penting dalam kepatuhan dan investigasi. Organisasi perlu menjaga keamanan informasi ini, serta mengetahui di mana lokasinya.” Dalam hal ini, Miranda mencatat bahwa organisasi sering mengabaikan *non-disclosure agreements* (NDAs), yang berisi informasi profil seperti alamat fisik yang penting dalam penyelidikan kecurangan.

Untuk informasi lebih lanjut, The IIA’s Supplemental Guidance “Internal Audit and Fraud: Assessing Fraud Risk Governance” menawarkan panduan yang jelas mengenai peran dan tanggung jawab organisasi untuk tata kelola dan manajemen risiko kecurangan yang baik, serta rekomendasi untuk panduan tambahan seperti COSO’s Fraud Risk Management Guide.

Kesimpulan

Audit internal telah siap

***Cryptocurrency* dan teknologi yang menjadi dasarnya** terlalu besar untuk diabaikan oleh audit internal, dengan tingkat kepentingan yang lebih dari layak untuk mendapat perhatian dewan. Penilaian risiko yang mengabaikannya menimbulkan *blind spot* yang kritis. *Cryptocurrency* mungkin merupakan konsep yang relatif baru bagi banyak orang, namun hal itu tidak mengurangi pentingnya kerangka kerja manajemen risiko kecurangan yang diukur dan diuji oleh audit internal.

Meskipun mudah untuk mengeluh bahwa ada area risiko lain yang ditambahkan ke radar audit internal, kabar baiknya adalah tidak ada departemen lain yang memiliki posisi lebih baik untuk menangani hal ini. Sama seperti yang dilakukan Sarbanes-Oxley Act (SOX) pada tahun 2002, evolusi regulasi *cryptocurrency* memastikan audit internal memiliki posisi yang penting di tahun-tahun mendatang. Bahkan walau belum mengenal *crypto*, fungsi ini sudah mengenal kecurangan, dan memahami risiko; itu saja sudah cukup bagi audit internal untuk mengambil posisi penting mengatasi tantangan ke depan

Bagian 2

Auditor Internal dan Pemeriksa Kecurangan: Kemitraan yang Berharga

Tentang Para Ahli

Mason Wilder, CFE

Mason Wilder adalah Certified Fraud Examiner, dan manajer riset untuk ACFE. Dalam peran ini, dia mengawasi pembuatan dan pemutakhiran materi ACFE untuk keberlanjutan pendidikan profesional, membantu perencanaan dan pelaksanaan semua acara pelatihan ACFE, mengerjakan inisiatif penelitian seperti Report to the Nations dan laporan *benchmarking*, melakukan pelatihan, menulis untuk publikasi ACFE, dan menanggapi permintaan anggota dan media. Sebelum bergabung dengan ACFE, Wilder bekerja di intelijen dan investigasi keamanan perusahaan selama lebih dari satu dekade, dengan spesialisasi pada investigasi latar belakang dan *due diligence* serta analisis intelijen untuk keamanan fisik internasional dan respons krisis. Mason telah membangun karier dalam mengumpulkan informasi yang relevan dari semua sumber untuk dianalisis dan disaring untuk mendukung pengambilan keputusan penting dan bersemangat untuk membantu profesional anti-kecurangan agar terus meningkatkan kemampuan mereka untuk melawan kecurangan secara efektif.

Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB

Shawna Flanders, direktur pengembangan produk di The Institute of Internal Auditors (IIA), adalah seorang ahli teknologi dan profesional industri pelatihan teknis yang bersemangat untuk mengadaptasi percakapan teknis ke dalam bahasa bisnis yang umum. Shawna membawa kombinasi keterampilan yang unik untuk setiap penugasan, termasuk: Pengembangan/Kontribusi Konten UKM, Pembicaraan/Pelatihan, Risiko Terkait TI, Audit TI, Keamanan Informasi dan Siber, Kepatuhan TI, Tata Kelola TI, Manajemen Vendor, Generalis TI di Telekomunikasi, Pemrograman, Desain/Tinjauan Arsitektur Terkait Suara dan Data, Teknik, Analisis dan Manajemen Integrasi, Manajemen Proses Bisnis, Analisis Bisnis, Manajemen Proyek, Manajemen Program dan Peningkatan Proses/Six Sigma.

Pendahuluan

Auditor internal memberikan wawasan konstruktif tentang tata kelola, risiko, dan pengendalian internal yang membantu organisasi mengelola risiko, termasuk mengidentifikasi dan mengurangi kecurangan. Namun, sementara audit internal adalah bagian efektif dari deteksi dan pencegahan kecurangan, menemukan kecurangan bukanlah tugas auditor internal. Seorang Certified Fraud Examiner (CFE), di sisi lain, secara khusus ditugaskan untuk mengidentifikasi dan menyelidiki kecurangan. CFE membawa keterampilan khusus untuk memberantas kecurangan. Akibatnya, masuk akal bagi kedua jenis profesional ini untuk berkolaborasi dalam kemitraan yang melayani kepentingan terbaik organisasi.

Global Knowledge Brief ini, yang kedua dari seri yang terdiri atas tiga bagian tentang kecurangan, mengkaji manfaat membangun hubungan simbiosis antara auditor internal dan CFE.

Ruang Lingkup Kecurangan

Kerugian rata-rata hampir mencapai $1,8 juta

Kecurangan tetap merupakan risiko yang berdampak meluas

Kecurangan adalah setiap tindakan ilegal yang melibatkan penipuan, penyembunyian, atau pelanggaran kepercayaan yang dilakukan untuk keuntungan finansial atau pribadi. Orang atau organisasi yang melakukan kecurangan mungkin berusaha mencuri uang, properti, atau jasa; untuk menghindari membayar atau kehilangan sesuatu; atau untuk mendapatkan keuntungan pribadi atau bisnis. Selain pelaku penipuan eksternal, penipuan juga dapat dilakukan oleh karyawan perusahaan yang mengalami tekanan finansial atau yang merasa berhutang uang atau jasa yang mereka ambil karena mereka menganggap organisasi telah memperlakukan mereka dengan tidak adil atau karena keluhan lainnya. Setiap jenis organisasi dapat menjadi korban kecurangan, terlepas dari ukurannya atau apakah itu publik atau swasta, nirlaba, lembaga pemerintah atau utilitas publik atau swasta, atau entitas lainnya.

Kecurangan adalah risiko yang serius dan berdampak meluas bagi organisasi. Konsekuensi kecurangan dapat berkisar dari mengganggu hingga sangat serius. Konsekuensi tersebut tidak hanya mencakup tantangan dan kerugian finansial, tetapi juga inefisiensi yang merusak operasi, pendapatan, atau laba; pembatalan proyek; dan, tergantung pada ruang lingkupnya, berpotensi kegagalan organisasi.[5]

Survei CFE di seluruh dunia oleh Association of Certified Fraud Examiners (ACFE) mencakup 2.110 kasus kecurangan dari 133 negara. Dalam grup itu, kerugian global akibat kecurangan berjumlah lebih dari $3,6 miliar, dengan rata-rata kerugian per kasus hampir $1,8 juta. CFE memperkirakan bahwa organisasi kehilangan 5% pendapatannya karena kecurangan setiap tahun. Perusahaan yang lebih kecil jelas memiliki risiko kecurangan terbesar: Perusahaan dengan pekerja paling sedikit mengalami kerugian rata-rata tertinggi, sebesar $150.000.

Meskipun kerugian sebesar itu mungkin mudah dikenali, kecurangan sering kali terjadi dalam skala yang lebih kecil dari waktu ke waktu. Skema kecurangan tipikal dapat mengakibatkan kerugian sebesar $8.300 per bulan dan dapat memakan waktu 12 bulan untuk mendeteksinya, menurut survei tersebut. Penting juga untuk menyadari bahwa *cryptocurrency* terlibat dalam beberapa kecurangan. ACFE menemukan bahwa mereka terlibat dalam 8% kasus. Skenario yang biasa dilakukan adalah melakukan suap dan pembayaran sogokan, serta mengubah aset yang disalahgunakan.[6]

Kategori Kecurangan Kerja

Ada tiga kategori utama penipuan pekerjaan, menurut ACFE 2022 *Report to the Nations*.

Skema kecurangan laporan keuangan atau menyebabkan salah saji material atau penghilangan dalam laporan keuangan organisasi, adalah yang paling jarang (9%) tetapi paling mahal, dengan kerugian $593.000 per kasus.

Penyalahgunaan aset, di mana seorang karyawan mencuri atau menyalahgunakan sumber daya perusahaan, terjadi pada 86% kasus. Namun, penyalahgunaan aset bertanggung jawab atas kerugian rata-rata terendah: $100.000 per kasus.

Korupsi, yang meliputi suap, konflik kepentingan, dan pemerasan, terlibat dalam 50% kasus dan menyebabkan kerugian sebesar $150.000 per kasus.

Sumber: *Occupational Fraud 2022: A Report to the Nations*, Association of Certified Fraud Examiners.

[5] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[6] *Occupational Fraud 2022: A Report to the Nations*, the Association of Certified Fraud Examiners.

Peran Auditor Internal

Asurans/advis tentang pencegahan kecurangan

Deteksi/pencegahan kecurangan merupakan andalan audit internal

Menurut Institute of Internal Auditors (IIA), "audit internal adalah kegiatan asurans dan konsultasi yang independen dan objektif yang dirancang untuk menambah nilai dan meningkatkan operasi organisasi. Peran audit internal termasuk mendeteksi, mencegah, dan memantau risiko kecurangan dan menangani risiko-risiko tersebut dalam audit dan investigasi."[7]

Organisasi seharusnya tidak mengharapkan keahlian audit internal untuk mencakup investigasi kecurangan. Jika keadaan mengharuskan audit internal untuk mengambil peran investigasi, auditor internal harus melakukan kecermatan profesional dan tidak boleh melanjutkan jika mereka tidak memiliki pengalaman dan keahlian yang diperlukan.

Sementara pencegahan kecurangan adalah peran manajemen, audit internal mendukung upaya manajemen anti-kecurangan dengan menyediakan jasa asurans yang diperlukan atas pengendalian internal yang dirancang untuk mendeteksi dan mencegah kecurangan. Sering kali penipuan terjadi karena pengendalian yang dirancang dengan buruk dan tata kelola yang lemah yang merusak proses organisasi. Hampir setengah dari kasus dalam survei ACFE dikaitkan dengan kurangnya pengendalian internal (29%) atau pengesampingan pengendalian yang ada (20%). Auditor mempertimbangkan potensi risiko kecurangan dan kecukupan pengendalian internal di bidang yang mereka periksa. Ketika pengendalian anti-kecurangan diterapkan, kerugian akibat kecurangan cenderung lebih rendah dan deteksi kecurangan lebih cepat, menurut survei.

Kontribusi audit internal terhadap upaya anti-kecurangan tidak boleh diremehkan. Ketika IIA meminta Kepala Audit Eksekutif (CAE) untuk menyebutkan di mana fungsi audit internal memiliki keterlibatan yang signifikan, 57% menyebutkan kecurangan dan 56% menunjuk pada penilaian risiko secara keseluruhan.[8] Sementara itu, survei ACFE menemukan bahwa kerugian dari kecurangan rata-rata 50% lebih tinggi ($150.000 vs $100.000) ketika tidak ada departemen audit internal.

Memang, data dari laporan *North American Pulse of Internal Audit 2023* yang akan datang menemukan bahwa kecurangan adalah pertimbangan yang paling sering disebutkan dalam audit internal. Survei tahunan CAE di Amerika Utara meminta lebih dari 500 responden untuk menunjukkan area mana yang mereka masukkan sebagai bagian dari audit mereka secara umum. "Jawaban menunjukkan bahwa auditor sering mengambil pendekatan holistik dan mempertimbangkan berbagai masalah, termasuk keamanan dunia maya, pihak ketiga, dan tata kelola," menurut laporan tersebut, yang akan diluncurkan pada Maret di Konferensi GAM 2023. Secara keseluruhan, 89% CAE mengatakan mereka menyertakan pertimbangan kecurangan dalam setiap audit secara umum, yang merupakan kategori risiko yang paling sering disebutkan dengan pertimbangan TI berada di urutan kedua sebesar 80%.

Pertimbangan Diintegrasikan ke dalam Audit

Sumber: Laporan *North American Pulse of Internal Audit* 2023

Survei *North American Pulse of Internal Audit* IIA, 20 Oktober s.d. 2 Desember 2022. Pertanyaan 25: Saat Anda melakukan penugasan audit secara umum, bidang mana berikut ini yang biasanya Anda sertakan dalam pertimbangan Anda? (Pilih semua yang sesuai.) n = 555.

[7] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.

[8] 2022 Premier Global Research, *Internal Audit: A Global View*, Internal Audit Foundation, 2022.

Menurut IIA Position Paper mengenai *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*,[9] audit internal harus memiliki pengetahuan yang diperlukan tentang kecurangan untuk dapat melakukan:

- Identifikasi *red flag* yang mungkin mengindikasikan kecurangan telah dilakukan.
- Memahami karakteristik kecurangan dan teknik kecurangan yang digunakan, serta jenis skema dan skenario kecurangan.
- Dapat memutuskan apakah tindakan lebih lanjut diperlukan atau apakah penyelidikan harus direkomendasikan.
- Mengevaluasi efektivitas pengendalian untuk mencegah atau mendeteksi kecurangan dan mengidentifikasi peluang untuk perbaikan.

[9] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019

Peran Pemeriksa Kecurangan

Investigasi Kecurangan

Investigasi Kecurangan yang terampil sangatlah penting

Pemeriksa kecurangan berpartisipasi dan mendukung pemeriksaan kecurangan organisasi secara keseluruhan. Mereka melakukannya sebagian dengan melakukan investigasi kecurangan yang "mencoba mendapatkan fakta dan bukti untuk membantu menentukan apa yang terjadi, mengidentifikasi pihak yang bertanggung jawab, dan memberikan rekomendasi jika memungkinkan." "[10] Salah satu isu yang dipertimbangkan oleh pemeriksa dalam meluncurkan investigasi adalah predikasi, yang berarti keseluruhan keadaan harus masuk akal bagi para profesional terlatih untuk menentukan bahwa kecurangan telah terjadi.

Langkah-langkah yang dilakukan oleh pemeriksa kecurangan dalam investigasi dapat mencakup perolehan bukti, pelaporan apa yang ditemukan, kesaksian atas temuan tersebut sesuai kebutuhan, dan membantu dalam deteksi dan pencegahan kecurangan. Dua tujuan umum pemeriksaan kecurangan adalah investigasi potensi kecurangan atau tuduhan kecurangan dan review atas kebijakan dan pengendalian anti-kecurangan organisasi. Tujuan yang lebih spesifik di balik pemeriksaan kecurangan dapat mencakup:

- Menemukan perilaku tidak pantas yang terkait atau mungkin terkait dengan kecurangan, serta menentukan siapa yang bertanggung jawab atas perilaku tidak pantas tersebut.
- Menentukan kerugian atau kewajiban actual atau potensial dari kecurangan.
- Menunjukkan komitmen organisasi untuk mengidentifikasi dan memitigasi kecurangan,
- Membantu memfasilitasi pemulihan kerugian
- Mencegah kecurangan di masa depan dan kerugian atau kewajiban terkait.
- Mengatasi konsekuensi di luar kerugian finansial.
- Menemukan dan memperkuat kelemahan dalam pengendalian internal
- Ketika diminta dalam beberapa kasus, mematuhi undang-undang, peraturan, kontrak, atau tugas hukum umum.[11]

[10] "Planning and Conducting a Fraud Examination," *Fraud Examiners Manual: 2022 Edition*, ACFE.
[11] ibid

Membandingkan pendekatan

Tabel di bawah ini ini memperlihatkan ikhtisar mengenai beberapa perbedaan penting antara peran, pendekatan, dan tujuan auditor internal dan CFE.

Karakteristik	**Audit internal**	**Pemeriksaan Kecurangan**
Niat	Prosedur audit internal dapat mengungkap kecurangan, tetapi tidak menjamin bahwa kecurangan akan terdeteksi. Sebagai contoh, auditor dapat menemukan transaksi atau situasi yang mencurigakan dalam suatu reviu yang pada akhirnya dapat diidentifikasi sebagai kecurangan. Namun, menemukan kecurangan hanya akan menjadi salah satu aspek pemeriksaan pengenalian dan prosedur yang lebih besar dalam area yang diaudit.	Suatu pemeriksaan kecurangan secara langsung difokuskan untuk mengungkap kecurangan dan mempertimbangkan tindakan atau aktivitas anti kecurangan.
Kejadian	Audit biasanya dilakukan berulang secara rutin/teratur, walaupun audit *pop-up* /tidak rutin dapat dilakukan untuk mengatasi situasi atau pertanyaan khusus di suatu area.	Pemeriksaan kecurangan biasanya hanya dilakukan dengan predikasi yang memadai, walaupun dapat terjadi tanpa pemicu khusus sebagai bagian dari manajemen risiko atau program penilaian risiko kecurangan. Namun, sebagian besar dilakukan sebagai tanggapan atas *tip*/informasi atau dugaan. Survei ACFE menunjukkan bahwa 43% kecurangan terdeteksi dari adanya informasi, angka ini hampir tiga kali lipat dari angka metode paling umum lainnya untuk menemukan kecurangan. Lebih dari setengah dari semua informasi kecurangan berasal dari karyawan.
Bertentangan atau tidak?	Audit internal bersifat tidak bertentangan. Tujuan auditor adalah untuk menawarkan wawasan dan informasi yang dapat digunakan pemimpin dan anggota tim untuk meningkatkan pengendalian atau proses lainnya, misalnya.	Pemeriksaan kecurangan pada dasarnya bersifat bertentangan. Sebagian dari tujuannya adalah untuk menentukan kesalahan siapa pun yang melakukan kecurangan.
Standar	Auditor internal mengikuti *International Standards for the Professional Practice of Internal Auditing*, ditetapkan oleh the Institute of Internal Auditors (IIA).	CFE mengikut ACFE *Code of Professional Standards*. CFE dapat menggunakan ACFE fraud risk assessment tool dalam pemeriksaan mereka.

Agar Kolaborasi Berjalan

Saling Menghormati dan Tanggung Jawab

Pertempuran Melawan Kecurangan

Terdapat beberapa peluang untuk kolaborasi yang bermanfaat antara auditor dan pemeriksa kecurangan. Keduanya dapat saling berkonsultasi mengenai:

- Peluncuran sebuah investigasi kecurangan
- Perencanaan audit tahunan dan pemeriksaan kecurangan
- Evaluasi Risiko
- Evaluasi dan penilaian pengendalian dan program anti kecurangan
- Penyampaian temuan audit yang berimplikasi kecurangan
- Remediasi kekurangan pengendalian.

Banyak organisasi memiliki aturan yang mengatur protokol ketika audit internal menyerahkan temuan kecurangan kepada tim pemeriksa kecurangan eksternal ataupun internal. Tim audit internal mencatat temuan kecurangan dan kemudian menyiapkan laporan bersama dengan pemeriksa kecurangan di akhir tinjauan.

Selain itu, audit internal dapat mengaudit departemen anti kecurangan organisasi untuk memastikan bahwa pengendalian departemen tersebut memadai. Tim anti kecurangan dapat melapor ke tim manajemen risiko perusahaan atau hukum, di antara bidang-bidang lain,termasuk audit internal. Jika tim kecurangan melapor ke audit internal, setiap audit dari departemen tersebut harus dialihdayakan untuk memastikan objektivitas.

Studi kasus menggambarkan kolaborasi di tempat kerja

Studi kasus berikut menunjukkan bagaimana kedua tim dapat bekerja sama. Hal ini berdasarkan diskusi antara Shawna Flanders, **CRISC, CISA, CISM, SSGB, SSBB,** direktur pengembangan produk di IIA, dalam webinar IIA dan ACFE baru-baru ini, ***Fostering Collaboration: The Auditor and the Fraud Examiner.***

Pada umumnya, audit internal menemukan pola yang meniru kecurangan dan mengingatkan pemeriksa kecurangan. Dalam kasus yang disampaikan oleh Flanders, suatu audit internal mencakup tinjauan atas kredit mobil. Salah satu langkah yang diambil oleh timnya adalah mengevaluasi akun tunggakan. Dalam sebuah kelompok yang terdiri dari 40 akun semacam itu, lima akun di antaranya mencolok. Sistem tersebut diatur untuk memberikan tanda peringatan atas tunggakan pinjaman yang harus ditindaklanjuti, namun karena beberapa alasan kelima akun tersebut tidak ditandai. Selain itu, semuanya diatur untuk memiliki karakteristik yang sangat tidak biasa: suku bunga 0%, jangka waktu 72 bulan, dan tanpa pembayaran minimum.

Saat Flanders menyelidiki, ia menemukan bahwa ID pengguna yang terkait dengan pinjaman tersebut adalah milik perwakilan layanan pelanggan, yang tidak masuk akal. Seseorang dalam peran ini biasanya tidak menyetujui pinjaman. Kemuadian ia meninjau catatan berkas terkait dengan pinjaman dan menemukan bahwa sekitar satu jam sebelum masing-masing pinjaman diajukan dan disetujui, pemegang ID pengguna diberi akses tambahan ke sistem. Akses itu dihapus sekitar satu jam setelah pinjaman disetujui dan diaktifkan.

Mengingat persyaratan pinjaman yang tidak biasa, keterlibatan perwakilan layanan pelanggan, dan perubahan dalam akses sistem, tim audit tahu sudah waktunya untuk menyerahkan kasus tersebut ke departemen kecurangan perusahaan.

Bergantung pada kebijakan dan prosedur organisasi, langkah-langkah yang mungkin diambil oleh departemen kecurangan dalam kasus ini ketika diperingatkan tentang aktivitas mencurigakan meliputi:

- Menguatkan informasi yang diterima dari audit.
- Memeriksa seluruh ruang lingkup kegiatan yang terkait dengan akun-akun tersebut.
- Menentukan apakah pembuatan lima akun ini merupakan tindakan khusus atau bagian dari skema potensial yang sedang berlangsung.
- Mengidentifikasi rekan konspirator.
- Mempertimbangkan apakah cabang atau kantor lain terlibat dan cakupan kecurangan secara keseluruhan.

Pemeriksa kecurangan pada titik ini juga dapat mempertimbangkan apakah dan bagaimana kecurangan harus dihentikan. Jika diperlukan lebih banyak bukti atau informasi, dapat diputuskan bahwa kecurangan harus dibiarkan setidaknya untuk sementara. Ini adalah penentuan rumit yang akan bergantung pada seberapa banyak perusahaan telah merugi, seberapa banyak potensi kerugian jika kecurangan berlanjut, dan selera risiko organisasi, menurut Mason Wilder, CFE, manajer riset di ACFE, yang juga berpartisipasi di webinar. Dalam hal ini, langkah-langkah yang harus diambil sebelum menghentikan kecurangan dapat termasuk mewawancarai perwakilan layanan pelanggan untuk mendapatkan lebih banyak informasi dan mengidentifikasi ruang lingkup kecurangan, dan berpotensi mengungkap kecurangan atau rencana tambahan untuk lebih banyak kecurangan.

Setelah mereka mengumpulkan dan menganalisis bukti, pemeriksa kecurangan kemudian akan melaporkan temuan mereka—secara lisan atau tertulis—kepada orang yang tepat di organisasi. Ini mungkin termasuk manajemen, dewan direksi/komisaris, atau komite audit. “Laporan pemeriksaan kecurangan adalah narasi dari aktivitas khusus pemeriksa kecurangan, temuan, dan, jika sesuai, rekomendasi,” berdasarkan Manual Pemeriksa Kecurangan ACFE. Manajemen organisasi kemudian dapat menggunakan laporan tersebut untuk menentukan langkah tepat untuk tahap selanjutnya.

Seandainya pemeriksa kecurangan meninjau laporan dugaan kecurangan dan tidak menemukan kecurangan yang sebenarnya, mereka dapat mengembalikan kasus tersebut apabila mereka menentukan bahwa tanda peringatan kecurangan muncul karena kekurangan dalam pengendalian manajemen risiko kecurangan. Audit internal kemudian dapat memasukkan kekurangan ini dalam laporannya.

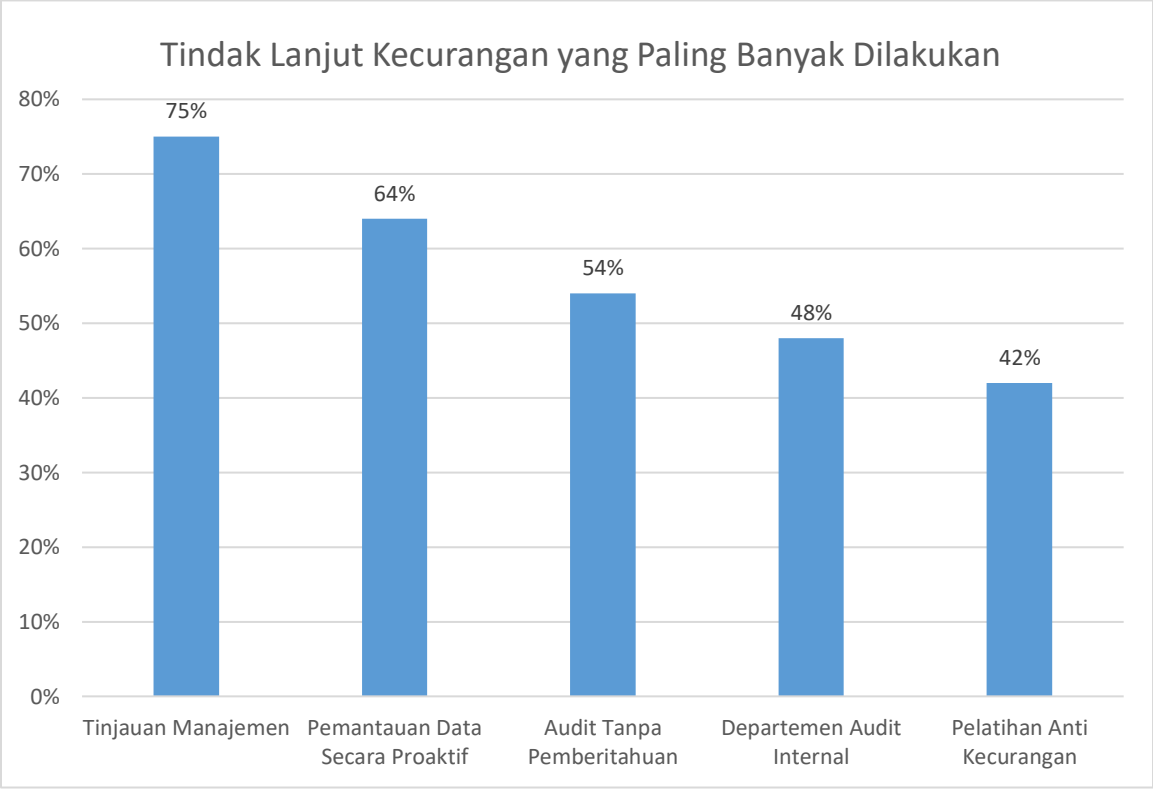
Menggabungkan kekuatan

Orang-orang yang peduli dengan kecurangan harus ingat bahwa mitigasi itu penting. Laporan survei ACFE mencatat bahwa langkah-langkah proaktif untuk menemukan kecurangan dapat mengarah pada deteksi dini dan kerugian yang lebih rendah, sementara upaya reaktif memungkinkan skema berjalan lebih lama dan meningkatkan dampak keuangan bagi korban.

Namun, organisasi tidak dapat mengidentifikasi atau menghilangkan seluruh risiko kecurangan. Mereka menghadapi berbagai jenis kecurangan, berbagai motivasi di belakang mereka, dan berbagai macam pelaku. Namun, semakin berpengetahuan orang-orang di seluruh tingkatan — manajemen, dewan direksi/komisaris, dan staf — semakin baik mereka dalam menerapkan upaya mitigasi yang wajar dan mengidentifikasi kecurangan atau tanda bahaya yang dapat menunjukkan keberadaannya. Dengan menggabungkan keterampilan dan pengalaman mereka yang khusus, auditor internal dan pemeriksa kecurangan dapat memberikan kontribusi yang kuat terhadap upaya organisasi secara keseluruhan. Organisasi dapat menggunakan hasil kerja mereka untuk membuat keputusan yang lebih tepat atas pendekatan manajemen risiko kecurangan.

Langkah-langkah untuk mencegah kejadian berulang

Sebanyak 81% organisasi pada survei ACFE melakukan modifikasi pada pengendalian anti kecurangan mereka setelah terjadi sebuah kecurangan. Grafik di bawah menunjukkan perubahan paling umum pada pendengalian yang diterapkan atau dimodifikasi oleh organisasi. Pengendalian anti kecurangan lain yang direkomendasikan oleh ACFE mencakup pemantauan transaksi/data secara otomatis, pengawasan, dan rekonsiliasi akun.



Sumber: *Occupational Fraud 2022: A Report to the Nations*, the Association of Certified Fraud Examiners.

Kesimpulan

Peran audit internal sebagai penyedia asurans lini ketiga atas tata kelola, risiko, dan pengendalian internal membutuhkan struktur, proses, dan praktik yang mempromosikan asurans yang objektif dan independen. Namun, seperti dicatat dalam Model Tiga Lini IIA, independensi tidak berarti isolasi.

“Harus ada interaksi reguler antara audit internal dan manajemen untuk memastikan pekerjaan audit internal tetap relevan dan selaras dengan kebutuhan strategis dan operasional organisasi. Melalui semua aktivitasnya, audit internal membangun pengetahuan dan pemahamannya tentang organisasi, yang berkontribusi pada asurans dan saran yang disampaikan sebagai penasihat yang dapat dipercaya dan mitra strategis,” menurut Model.

Hal ini jelas terjadi ketika audit internal dan pemeriksa kercurangan bersertifikat menemukan titik temu sebagai sekutu dalam pertempuran melawan kecurangan.

Bagian 3

Efek Setelah Kejadian: Kecurangan pada Era Pasca COVID

Tentang Ahli

David Dominguez, CIA, CRMA, CPA, CFE

David adalah Direktur Audit dan Kepatuhan di Itafos, Houston. Dalam karirnya, David telah bekerja dengan perusahaan multi nasional di berbagai industri untuk membangun, mengarahkan, dan mentransformasikan fungsi audit internal di regional dan perusahaan secara luas. Dia telah memimpin dan melaksanakan proyek-proyek keuangan, operasional, dan asurans Teknologi Informasi (TI) dan konsultasi di Amerika Utara, Amerika Latin, Eropa, dan Asia. Dia juga telah mengelola dan berpartisipasi dalam berbagai investigasi multi-yurisdiksi, inisiatif analitik data, dan berbagai audit yang terkait dengan pemegang saham internasional, usaha patungan, dan vendor. Bidang keahliannya meliputi tata kelola perusahaan dan organisasi, manajemen risiko perusahaan, manajemen risiko *kecurangan*, *Sarbanes-Oxley Act* 2002, dan program etika dan kepatuhan.

Pendahuluan

Selama lebih dari dua tahun, COVID-19 menyebabkan gangguan di seluruh lini, mulai dari cara orang bekerja, di mana mereka bekerja, bagaimana organisasi mereka menangani masalah pemasok dan rantai pasokan, dan bagaimana mereka menangani masalah yang signifikan, seperti mempertahankan pengendalian internal serta mendeteksi dan mencegah kecurangan.

Saat ini, dunia bernafas lebih lega karena pandemi terburuk perlahan memudar menjadi sejarah, tetapi meskipun demikian, orang tidak boleh berasumsi bahwa risiko yang terkait dengan COVID-19 tidak lagi menjadi perhatian. Tentu saja, organisasi yang membuat asumsi tersebut bisa saja membuat kesalahan besar. RIngkasan Pengetahuan Global ini, merupakan bagian ketiga dari seri yang terdiri atas tiga bagian tentang kecurangan dari The Institute of Internal Auditors (IIA), yang membahas berbagai faktor kecurangan terkait pandemi yang diidentifikasi dalam Laporan *2022 ACFE Report to the Nations*, bagaimana faktor tersebut dapat memengaruhi organisasi, dan peran audit internal dalam upaya organisasi untuk mengurangi faktor risiko kecurangan tersebut.

Kecurangan dan Risiko Kecurangan yang Berkepanjangan

Perubahan terkait pandemi akan tetap menjadi perhatian

Kecurangan baru yang terinspirasi COVID akan muncul

Dalam laporan terbaru *Report to the Nations* tentang *kecurangan* di lingkungan pekerjaan, *The Association of Certified Fraud Examiners* (ACFE) menemukan bahwa durasi rata-rata kecurangan — yaitu, waktu tipikal antara saat kecurangan dimulai dan saat terdeteksi — adalah 12 bulan[12]. artinya, organisasi terus menghadapi kecurangan terkait pandemi yang belum ditemukan.

Ada banyak alasan mengapa perubahan terkait pandemi terus berdampak pada risiko kecurangan. Misalnya, adopsi bekerja secara jarak jauh dimaksudkan untuk sementara, tetapi telah berubah menjadi prosedur operasi standar di banyak perusahaan. Bekerja secara jarak jauh sering membawa serta perubahan signifikan — dan dalam beberapa kasus melonggarkan — praktik dan prosedur yang dirancang untuk mengidentifikasi atau mengurangi kecurangan. Akibatnya, risiko terkait terus menjadi ancaman bagi perusahaan bahkan ketika gangguan terkait pandemi telah berkurang.

Audit internal telah dan akan terus memainkan peran kunci dalam menangani risiko kecurangan terkait pandemi yang sedang berlangsung. Dalam studi anggota IIA di seluruh dunia yang dilakukan oleh *Internal Audit Foundation* (IAF) dan Kroll, banyak peserta dalam diskusi terkait merasa bahwa pandemi "menempatkan audit internal lebih berperan dalam manajemen risiko kecurangan." [13] Hal ini termasuk keterlibatan tambahan dalam pertimbangan strategis tantangan operasional, memberikan jaminan berkelanjutan, dan meningkatkan kolaborasi di seluruh fungsi bisnis — sambil mempertahankan independensi auditor.

[12] *Occupational Fraud 2022: A Report to the Nations*, ACFE.
[13] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.

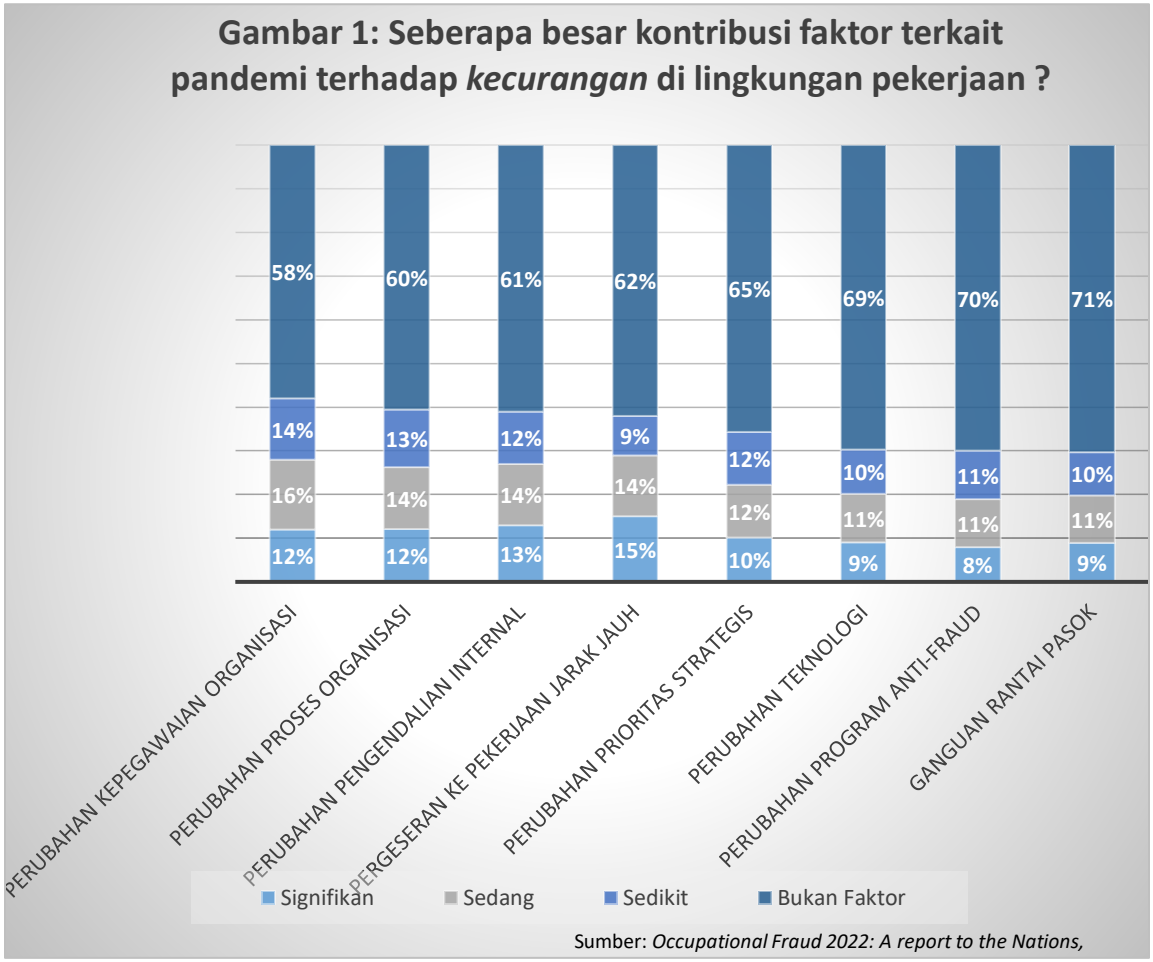
Risiko Kecurangan Teratas Terkait Pandemi

Perubahan terkait kepegawaian, bekerja secara jarak jauh merupakan perhatian terbesar

Lebih dari setengah melihat faktor pandemi berkontribusi terhadap kecurangan

Dalam menyiapkan laporan tentang kecurangan di lingkungan pekerjaan, ACFE menemukan bahwa 52% responden melaporkan bahwa, dalam insiden kecurangan yang telah mereka selidiki, setidaknya satu dari beberapa masalah terkait pandemi berkontribusi pada kecurangan tersebut. Di antaranya adalah perubahan kepegawaian di dalam organisasi terkait pandemi adalah yang paling umum. Sebanyak 42% responden mengatakan perubahan kepegawaian adalah faktor yang signifikan, sedang, atau sedikit yang berkontribusi terhadap kecurangan di pekerjaan. Pergeseran ke bekerja secara jarak jauh adalah faktor yang paling sering dianggap signifikan (15%), diikuti oleh pengendalian internal (13%) (Lihat Gambar 1).

Gambar 1: Seberapa besar kontribusi faktor terkait pandemi terhadap *kecurangan* di lingkungan pekerjaan ?



Sumber: *Occupational Fraud 2022: A report to the Nations,*

Penelitian lebih dalam terhadap beberapa masalah utama terkait pandemi yang diidentifikasi dalam laporan ACFE menunjukkan bahwa dampak seringkali kompleks dan tidak terlihat.

Perubahan kepegawaian menimbulkan berbagai risiko kecurangan

Pandemi memaksa banyak organisasi untuk mencari solusi atau jalan pintas untuk mengatasi banyak gangguan yang mereka hadapi, termasuk mengubah atau memperluas tanggung jawab pekerja atau mendatangkan orang baru yang memiliki waktu terbatas untuk menyesuaikan diri dengan pekerjaan mereka. Selain itu, pemutusan hubungan kerja (PHK) sementara atau cuti akibat ketidakpastian ekonomi terkait pandemi sering menjadi permanen, kata David Dominquez, Direktur Audit dan Kepatuhan di Itafos, sebuah perusahaan fosfat dan pupuk khusus. "Ini jelas meningkatkan risiko dari berbagai sudut," ujarnya.

Mengingat banyaknya penyesuaian dan penyesuaian terhadap praktik dan protokol kerja yang mungkin telah diciptakan oleh pandemi — dan kurva pembelajaran potensial bagi mereka yang mengambil tugas baru — organisasi harus mempertimbangkan jenis dampak tidak disengaja apa yang mungkin ditimbulkan oleh perubahan ini. Berikut beberapa area yang perlu dipertimbangkan:

Budaya

Terdapat sejumlah alasan untuk menilai kembali dan mungkin menegaskan kembali budaya dan nilai perusahaan setelah pandemi. "Membuatnya berhasil" adalah keutamaan selama pandemi, tetapi itu mungkin berarti beberapa praktik dan sikap etis yang penting telah dilupakan. Pekerja baru juga mungkin belum pernah mengalami pengenalan yang tepat tentang nilai-nilai etika perusahaan. Jika hal itu adalah masalahnya, organisasi akan disarankan untuk mengingatkan pegawai tentang harapan mereka tentang perilaku etis.

"Pendekatan proaktif terhadap budaya dapat mencegah berbagai jenis pelanggaran dan mempromosikan perilaku yang dapat meningkatkan moral dan produktivitas," kata ACFE dalam laporannya. "Budaya memiliki kemampuan yang kuat untuk mempengaruhi cara orang melakukan pekerjaannya; bagaimana keputusan tentang kualitas, kepatuhan, dan masalah penting lainnya dibuat; dan bagaimana organisasi dirasakan baik secara internal maupun eksternal." [14]

Pertimbangan sumber daya manusia

Kekurangan tenaga kerja dan pergeseran kebijakan pada bekerja secara campuran (*hybrid*) dan jarak jauh telah membalikkan beberapa praktik sumber daya manusia yang sudah berlangsung lama, seperti *hotline whistleblower* anonim.

Salah satu alat penting terkait sumber daya manusia (SDM) dalam pencegahan kecurangan adalah *hotline whistleblower* anonim. Memang, 42% penipuan terdeteksi oleh laporan/informasi, menurut laporan ACFE, lebih dari tiga kali lipat metode paling umum berikutnya.

Audit internal dapat mendukung proses ini dengan memeriksa apakah *hotline* berjalan sebagaimana mestinya. Langkah pertama mungkin menentukan seberapa baik *hotline* ini dipantau dan apakah pengaduan ditindaklanjuti dan dilacak, kata Dominquez. Dia merekomendasikan untuk mengajukan pertanyaan pemantauan *hotline*, seperti berikut:

- **Bagaimana cara orang mengakses *hotline*?** Pilihannya termasuk menyampaikan laporan di *drop box* di kantor, menelepon nomor *hotline*, atau melaporkan keluhan secara daring (*online*). Ingatlah bahwa *drop box* — dan poster yang mempromosikan *hotline* — tidak akan membantu pekerja yang bekerja secara jarak jauh.
- **Dapatkah hotline tersedia dalam berbagai Bahasa, jika perlu?**
- **Seberapa baik upaya dilacak?** Dominquez mencatat bahwa beberapa perusahaan memberi apresiasi kepada diri mereka sendiri untuk jumlah keluhan yang rendah. Ini bisa menjadi cerminan akurat dari organisasi yang dikelola dengan baik, tetapi juga dapat menunjukkan bahwa beberapa panggilan *hotline* tidak dijawab atau keluhan jarang ditindaklanjuti.

Audit internal dapat meninjau proses dalam menanggapi keluhan untuk memastikan waktu yang tepat dari penerimaan hingga penyelesaian dan apakah keputusan untuk menindaklanjuti atau tidak cukup beralasan. Organisasi terkadang melewatkan laporan/informasi kecurangan yang valid karena takut akan pembalasan setelah ada keluhan. Audit internal dapat meninjau apakah buku panduan perusahaan atau kode etik secara eksplisit melarang pembalasan. Lebih jauh, audit internal juga dapat membantu

[14] *Assessing Corporate Culture: A Proactive Approach to Deter Misconduct*, Anti-Fraud Collaboration, March 2020.

perusahaan melacak apakah *whistleblower* cenderung mendapatkan promosi atau lebih cenderung mendapatkan tinjauan kinerja yang buruk, catat Dominquez. Bahkan ketika pengaduan tidak berdasar, perusahaan dapat menemukan kebijakan proses tanggapan yang perlu diperbarui atau diklarifikasi, katanya

Tindakan pencegahan/pengendalian yang berharga lainnya yang harus dilakukan atau dijalankan oleh organisasi termasuk:

- Pemeriksaan latar belakang untuk mengidentifikasi riwayat kredit sebelumnya atau masalah keuangan lainnya atau riwayat pemotongan upah, hak gadai, atau putusan yang mungkin terkait dengan penggelapan.
- Verifikasi *credentials*/kualifikasi.

ACFE melaporkan bahwa 50% pelaku kecurangan (*fraudsters*) menunjukkan setidaknya satu petunjuk (*red flag*) terkait kepegawaian sebelum atau selama terjadinya kejadian kecurangan. Dalam hal petunjuk perilaku, hidup di luar kemampuan seseorang telah menjadi petunjuk yang paling umum di setiap penelitian ACFE sejak 2008. Hal ini teridentifikasi dalam 39% kasus, jauh di depan faktor paling umum yang kedua, yaitu kesulitan keuangan, di 25%.

Ketidakpastian pekerjaan

ACFE mengidentifikasi sejumlah contoh ketidakpastian pekerjaan yang dapat berkontribusi terhadap kecurangan, dan kondisi keuangan yang menantang dapat meningkatkan ketidakamanan. Petunjuk tersebut termasuk:

- Rasa takut akan kehilangan pekerjaan.
- Penolakan atas kenaikan atau promosi.
- Pemotongan manfaat.
- Pemotongan gaji.
- Pemotongan paksa atas hitungan jam.
- Penurunan pangkat.

Sementara iklim ekonomi telah stabil sejak hari-hari terburuk di masa pandemi, tantangan tetap ada dalam iklim bisnis global. Tidak mengherankan, dampak isu terkait ketidakpastian pekerjaan tetap signifikan di 2022, menurut ACFE. Adalah masuk akal, bahwa beberapa ketidakpastian ini mungkin masih menjadi faktor yang mendorong pelanggaran oleh pegawai.

Petunjuk-petunjuk ini berlaku untuk pegawai secara keseluruhan, namun terdapat beberapa petunjuk tambahan yang dapat berlaku secara khusus terhadap eksekutif *C-suite*:

- **Pelecehan atau intimidasi**. 23% untuk pemilik/eksekutif; 8% untuk pihak selain pemilik/eksekutif.
- **Isu pengendalian.** 18% untuk pemilik/eksekutif; 12% untuk pihak selain pemilik/eksekutif.
- **Sikap "Wheeler-Dealer".** 17% untuk pemilik/eksekutif; 9% untuk pihak selain pemilik/eksekutif.
- **Tekanan yang berlebihan dari dalam organisasi.** 13% untuk pemilik/eksekutif; 6% untuk pihak selain pemilik/eksekutif.
- **Masalah hukum di masa lalu.** 11% untuk pemilik/eksekutif; 3% untuk pihak selain pemilik/eksekutif.

Perubahan pengendalian internal terkait COVID harus ditinjau kembali

Pengendalian internal adalah prosedur-prosedur yang diadopsi untuk meyakinkan bahwa tindakan dan keputusan di seluruh organisasi sesuai dengan kebijakan, persyaratan pelaporan, dan kepatuhan yang diamanatkan. Pengendalian anti kecurangan dapat mengurangi kerugian akibat kecurangan dan dapat lebih cepat atau memudahkan pendeteksian kecurangan. Dalam penelitian ACFE, hampir setengah dari kerugian kecurangan dapat dilacak karena dua faktor: kurangnya pengendalian internal (29%) dan mengesampingkan pengendalian internal yang ada (20%). Menerapkan dan memperkuat pengendalian internal tentunya dapat

memberikan manfaat positif yang signifikan bagi organisasi. Audit Internal memiliki peran yang penting dalam melaporkan kondisi pengendalian internal dan merekomendasikan perbaikan atas pengendalian internal. Memang, survei yang dilakukan oleh ACFE menemukan bahwa nilai tengah (*median*) dari kerugian kecurangan adalah 50% lebih tinggi ($150,000 vs $100,000) ketika tidak ada Departemen Audit Internal yang berfungsi seperti seharusnya.

Audit internal yang merespon penelitian oleh IAF/Kroll survey meyakini bahwa "kerangka kerja pengendalian internal telah melemah karena kendala bekerja secara jarak jauh (*remote working*) dan, di berbagai kasus, pengurangan pegawai karena penyakit, cuti, dan jumlah pegawai."[15]

Pegawai-pegawai baru yang bergabung dengan organisasi selama masa krisis mungkin tidak menerima pelatihan atau transfer pengetahuan yang cukup, atau mereka mungkin hanya mempelajari protokol darurat yang tidak termasuk proses dan pengendalian yang lama/seharusnya, menurut Dominquez. "Pengendalian telah berkurang atau mungkin menjadi lemah begitu saja," menurutnya. Seiring berjalannya waktu, jalan pintas tersebut dapat menjadi — dan mungkin tetap menjadi — prosedur operasional standar meskipun sebenarnya hanya dimaksudkan untuk dipakai selama jangka waktu tertentu atau dalam situasi tertentu.

Kekhawatiran ini telah membawa perubahan positif di banyak organisasi. Sebagai contoh, sekitar tiga-per-empat dari anggota Komite Audit yang memberikan respon terhadap survei yang dilakukan bersamaan oleh *Deloitte's Center for Board Effectiveness* dan *Center for Audit Quality* menyampaikan bahwa mereka telah mengkinikan pengendalian internalnya setidaknya di satu tahun terakhir karena lingkungan bekerja secara jarak jauh.[16]

Kelemahan dalam pengendalian internal dapat berkontribusi terhadap kecurangan dengan menciptakan atau mempromosikan lingkungan dimana lebih mudah melakukan pengabaian atau mengesampingkan tindakan anti kecurangan yang kuat. Sebagai contoh, selama pandemi, pemisahan tugas — Tindakan anti kecurangan yang umum dan efektif — mungkin telah diabaikan karena lebih sulit menyelesaikan pekerjaan dengan pegawai yang berada di berbagai lokasi berbeda atau karena pengurangan atau kekurangan pegawai. Hal ini merupakan tipe pengendalian internal yang mana sebuah perusahaan harus meninjaunya sekarang untuk meyakinkan pengendalian internal ini telah terpulihkan dan telah bekerja dengan efektif.

Audit Internal dapat membantu organisasi mengatasi risiko ini dengan meyakinkan protokol dan proses vital telah memadai. Dengan menggunakan teknologi proses pemetaan, Audit Internal melacak proses-proses selama periode tertentu — enam bulan atau setahun — dan mengidentifikasi variasi terhadap petunjuk kerja yang benar atau praktik terbaik (*best practices)*. "Anda dapat melihat adanya penyimpangan atas standar prosedur atau kebijakan dan mengidentifikasi proses-proses mana yang perlu dikinikan atau diperkuat," menurut Dominquez.

Area lain untuk ditinjau adalah termasuk pengendalian internal terkait pengadaan, penulisan cek, rekonsiliasi bank, penggantian biaya, atau area lain yang melibatkan pertimbangan keuangan.

Bekerja secara jarak jauh tetap menjadi faktor kecurangan yang kritikal

Poros dramatis dari bekerja secara jarak jauh — penutupan kantor-kantor dan diperbolehkannya pegawai melakukan pekerjaannya di rumah — mungkin adalah perubahan paling signifikan bagi sebagian besar organisasi selama pandemi. Sebagai konsekuensinya, pendekatan baru ini merupakan faktor yang paling banyak dikutip sebagai yang paling signifikan kontribusinya terhadap kecurangan, dalam laporan ACFE. Dalam keadaan normal, sebuah perusahaan dapat menghabiskan beberapa bulan mempertimbangkan dampak strategis dari sebuah keputusan bisnis, namun ini pada dasarnya tidak mungkin di tengah ketidakpastian dan kegentingan di minggu-minggu awal pandemi. Jika tidak ada yang lain, bekerja sendiri dan tidak terlihat oleh rekan kerja dan penyelia dapat mempermudah melakukan berbagai kecurangan. Mereka yang membuat atau telah melakukan perpindahan permanen ke bekerja secara jarak jauh

[15] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[16] *Audit Committee Practices Report: Common Threads Across Audit Committees*, Deloitte's Center for Board Effectiveness and the Center for Audit Quality, January 25, 2022.

atau *hybrid* harus terlibat dalam perencanaan manajemen perubahan "untuk menemukan garis kesalahan yang dapat memiliki dampak katastrofi jika dibiarkan tidak tertangani," menurut ACFE.[17]

Dalam proses ini, terdapat beberapa potensi batasan-batasan kesalahan yang dapat menjadi fokus audit internal. Sebagai contoh, kesulitan mengelola orang secara efektif di lingkungan terpencil yang terfragmentasi dan dampaknya terhadap budaya disebutkan sebagai bidang utama untuk ditangani, menurut laporan IAF/ Kroll.[18] Perilaku etis seringkali merupakan sesuatu yang dipelajari dan diperkuat melalui interaksi dengan pegawai lain yang menunjukkannya di tempat kerja. Akses ke rekan yang lebih berpengalaman dapat membantu memahami bagaimana merespon keadaan yang membingunkan atau mencurigakan, seperti pada saat pegawai lain tampaknya bertindak tidak tepat atau ilegal.

Di antara tipe-tipe kecurangan, yang secara khusus terkait dengan bekerja secara jarak jauh adalah:

- **Pencurian waktu atau membuat klaim yang tidak akurat tentang jam kerja.** Hal ini dapat dengan mudah dilakukan ketika seseorang tidak diawasi secara langsung.
- **Pencurian atau penyalahgunaan data atau berbagi informasi rahasia atau sensitif.** Hal ini dapat dilakukan oleh orang dapat memiliki akses ke perangkat pegawai atau oleh pegawai yang merasa lebih nyaman menyalahgunakan data ketika tidak di kantor.[19]

Kekhawatiran terkait adalah pegawai mengambil pekerjaan sampingan. Sebagai contoh, pegawai dapat melakukan konsultasi atau penugasan temporer untuk perusahaan lain selama jam-jam dimana mereka seharusnya bekerja untuk pemberi gaji utama mereka, menurut Dominquez. Ini tentu saja pencurian waktu, tapi penyalahgunaan sumber daya perusahaan, seperti laptop atau telepon, juga dapat memaparkan perusahaan terhadap isu keamanan siber. Pekerjaan sampingan juga dapat menjadi konflik kepentingan jika pegawai bekerja untuk pesaing, khususnya jika mereka membagi informasi yang bermanfaat bagi pesaing. Audit Internal dapat membantu mengatasi masalah ini dengan mempertanyakan tipe pelatihan yang diterima pegawai dan apakah buku pegangan dan kebijakan kepegawaian telah dikinikan sesuai lingkungan kerja yang baru, demikian dikatakan Dominquez.

Perubahan teknologi menciptakan kecurangan memberi dan menerima (*give and take*)

Teknologi dapat memungkinkan organisasi menerapkan prosedur yang efektif di berbagai area seperti pengendalian internal dan bekerja secara jarak jauh. Organisasi telah membuat perbaikan dan investasi di teknologi untuk mengatasi kekhawatiran keamanan siber, dan pandemi mendorong perusahaan untuk berakselerasi dan memperkuat sistem mereka. Banyak fungsi audit internal yang termasuk dalam peningkatan teknologi. Memang, 29% dari audit internal telah menambahkan *data analysis* sebagai alat bantu untuk mengidentifikasi kecurangan dan korupsi sejak mulainya pandemi.[20]

Di waktu yang bersamaan, penyalahgunaan atau pengabaian alat bantu teknologi dapat mempermudah suksesnya skema kecurangan. Sebagai catatan, pencurian data adalah salah satu kekhawatiran yang terkait dengan bekerja secara jarak jauh. Solusi yang mungkin dilakukan atas risiko pencurian data, menurut ACFE, termasuk meminta pegawai mengamankan jaringan di rumah mereka — dan tidak membaginya dengan anggota keluarga yang lain. Penggunaan VPN dan kata sandi (*password*) yang lebih kuat dan lebih kompleks serta pengaturan untuk mengamankan komputer rumah juga menjadi kunci. Pilihan lainnya termasuk otentikasi multi-faktor dan pelatihan tahunan untuk pegawai atas keamanan dan privasi data. Organisasi juga dapat mengembangkan kebijakan penggunaan perangkat elektronik yang dapat diterima, media sosial, dan data perusahaan, dan juga meminta pegawai untuk membaca dan mengakui bahwa mereka telah memahami kebijakan tersebut.

[17] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[18] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[19] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[20] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.

Organisasi di lingkungan bekerja secara jarak jauh atau *hybrid* juga perlu meyakinkan bahwa pegawai mereka mengkinikan perangkat lunak dan perbaikan keamanan (*security patch*) di perangkat elektronik di rumah mereka, serta mendidik pegawai tentang cara terbaik menghindari *phishing* dan ancaman peretas (*hacker)* lainnya.[21] Tentunya, perusahaan yang berusaha keras mengikuti dampak pandemi harus meninjau tindakan keamanan siber mereka untuk memastikan perusahaan selalu dalam kondisi terkini.

Untuk membantu mangatasi kekhawatiran ini, Dominquez merekomendasikan bahwa audit internal dapat menginvestigasi apakah protokol keamanan telah memadai, alat bantu pencegahan kerugian data yang digunakan oleh organisasi, apakah diperlukan otentikasi multi-faktor dan VPN, serta apakah akun telah secara tepat waktu di-nonaktifkan ketika pegawai meninggalkan perusahaan

"*Quiet Quitting*" berdampak pada kepatuhan, upaya etika

"*Quiet quitting*" mengacu pada praktik di mana pegawai hanya melakukan pekerjaan minimum dari persyaratan pekerjaan mereka. Menurut salah satu estimasi dari Gallup, pekerja-pekerja seperti ini setidaknya 50% dari tenaga kerja U.S. Tingkat perkerja yang terlibat dengan perusahaan adalah 32%, namun pekerja yang secara aktif tidak terlibat adalah 18%. Gallup mencatat hal ini sangat bermasalah ketika banyak pekerjaan bersifat kolaboratif atau ketika diperlukan langkah ektra untuk memenuhi kebutuhan konsumen. Dan ketika tren menuju *quiet quitting* ini mendapat banyak perhatian, pegawai harus sadar bahwa *loud quitters* — atau orang yang secara aktif mengekspresikan dan mungkin menyebarkan ketidakpuasan mereka — masih ada.[22]

Tren ini dapat menjadi berita buruk untuk produktifitas, efisiensi, dan retensi. Di saat yang sama, hal ini dapat memiliki dampak negatif pada manajemen risiko. "Orang tidak memberikan banyak perhatian terhadap apa yang to harus mereka lakukan," menurut Dominquez. Dan, seperti catatan *Corporate Compliance Insights*, program kepatuhan dan etika yang sukses mensyaratkan partisipasi dan dukungan semua orang di organisasi. "Ketika anda mengkombinasikan pandangan yang relatif negatif pada pekerjaan dengan pendekatan minimum-layak-kerja-produk, hal-hal tambahan yang diandalkan oleh profesional kepatuhan dan etika untuk memastikan seseorang mengangkat isu, seringkali hilang," demikian catatannya.[23]

Ini juga berlaku terhadap sebuah program manajemen risiko kecurangan. pegawai dapat sekedar menjadi cap untuk persetujuan dan transaksi atau mengabaikan anomali, atau mereka mungkin juga mengeskalasi anomali hanya untuk menemukan bahwa manajer/atasan mereka mengabaikannya karena mereka *quiet quitting*.

Audit Internal dapat memeriksa survei kepuasan pegawai, tingkat perputaran pegawai, dan wawancara kepada pegawai yang meninggalkan perusahaan (*exit interview*) untuk mendapatkan permasalahan-permasalahan dalam keterlibatan pegawai. Tren terkini dapat diperbandingkan dengan aktifitas sebelum pandemi untuk memahami kemungkinan adanya dampak tersebut, menurut Dominquez.

[21] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[22] "Is Quiet Quitting Real?" Jim Harter, Gallup Workplace, September 6, 2022.
[23] "Why 'Quiet Quitting' Could Harm Ethics and Compliance Functions," Lisa Beth Lentini Walker, *Corporate Compliance Insights*, September 14, 2022.

Kesimpulan

Apa artinya semua ini? Menurut ACFE', organisasi kehilangan sekitar 5% pendapatannya karena kecurangan setiap tahunnya, dengan nilai tengah kerugian di angka $117,000 dan rata-rata kerugian sebesar $1,783,000. Umumnya, kerugian karena skema kecurangan dapat mencapai rata-rata sekitar $8,300 per bulan. Hal ini menjadi perhatian serius bagi setiap organisasi.

Selama dan sejak memburuknya pandemi, organisasi telah beralih ke audit internal untuk membantu pengambil keputusan stratejik dalam menilai kembali dan meningkatkan proses operasional. Praktik ini harus terus diterapkan, khususnya dalam mengevaluasi pengendalian internal anti kecurangan. Dunia mungkin telah keluar dari pandemi, tetapi belum tentu menghilangkan ancaman kecurangan terkait pandemi.

Sejak mulainya pandemi, telah terdapat penghargaan yang lebih besar atas kontribusi yang dapat diberikan oleh audit internal dalam mengurangi atau menghentikan kecurangan. Di masa lalu, audit internal sering baru dilibatkan setelah sebuah kejadian kecurangan terjadi. Hal ini mulai berubah; organisasi sekarang lebih sedikit kemungkinan menunggu untuk kecurangan terdeteksi dan berharap dapat segera mengatasinya sebelum terlalu banyak dampak kerusakannya. Untuk membantu mencapai hal ini, organisasi mengikutsertakan auditor internal dalam pembicaraan untuk pencegahan (*prevention-based conversations*), atau dengan kata lain, meminta auditor internal untuk mempertimbangkan pengendalian anti kecurangan sebelum kecurangan terjadi, menurut Dominquez. Audit Internal juga memfasilitasi diskusi di area penilaian risiko kecurangan (*fraud risk assessment*) dan kerangka kerjanya, dengan mempertimbangkan frekuensi dan efektifitas penilaian tersebut berikut pengendalian internal yang diuji, dan selalu mencatat adanya perubahan berkelanjutan di profil risiko organisasi. "Alih-alih menunggu untuk mendeteksi kecurangan, auditor internal saat ini beralih menuju sisi pencegahan," demikian dikatakan Dominquez.

Tentang IIA

The Institute of Internal Auditors (IIA) adalah sebuah asosiasi profesional internasional nirlaba yang melayani lebih dari 230.000 anggota global dan telah memberikan lebih dari 185.000 sertifikasi *Certified Internal Auditor* (CIA) di seluruh dunia. Didirikan di tahun 1941, *The IIA* dikenal di seluruh dunia sebagai pemimpin profesi audit internal dalam standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis. Untuk informasi lebih lanjut, kunjungi theiia.org.

Disclaimer

IIA mempublikasikan dokumen ini hanya untuk tujuan informasi dan pendidikan. Materi ini tidak dimaksudkan untuk menyediakan jawaban pasti atas situasi individual yang spesifik dan hanya bertujuan sebagai pedoman. IIA merekomendasikan mencari masukan langsung dari tenaga ahli independent atas situasi yang spesifik. IIA tidak bertanggungjawab atas siapapun yang bergantung hanya kepada materi ini.

Copyright

April 2023

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101