Wacana Ekonomi: Jurnal Ekonomi, Bisnis dan Akuntansi
Volume 24, Nomor 1, 2025, pp 9-22
https://doi.org/10.22225/we.24.1.2025.9-22

OPEN ACCESS

Diterima: 10 Februari 2025 | Direvisi: 23 Juni 2025 | Dipublikasikan: 23 Juni 2025

Analisis Kinerja Layanan Fraud Detecting System di Perusahaan Konsultan Keamanan Informasi

Muhammad Raihan Alfikri[1] | Sukartini[1] | Ferdawati[1]

1. Politeknik Negeri Padang

Correspondence addressed to:
Muhammad Raihan Alfikri, Politeknik Negeri Padang
Email: raihanalfikri2001@gmail.com

Alfikri, M, R., Sukartini, S., Ferdawati, F. (2025). Analisis Kinerja Layanan Fraud Detecting System di Perusahaan Konsultan Keamanan Informasi. *Wacana Ekonomi: Jurnal Ekonomi, Bisnis dan Akuntansi*, *24*(1), 9-22

Abstract. *This research aims to find out in depth about the performance of Fraud Detecting System services in information security consulting companies to prevent financial fraud. The research took a qualitative method, in which direct interviews were conducted related to the object under study. Assumed on the action of the experience handled directly by the relevant division which of course can be proven scientifically. The results of the study concluded that PT ITSEC Asia Tbk has a fraud detection strategy through a managed system, namely the Fraud Management System which is able to detect, analyze and monitor fraud risks effectively and complexly. However, the company certainly also faces a variety of major challenges, including regulatory constraints in various regional countries of the ITSEC Asia office, as well as the challenge of the growing threat of fraud. Financial and audit assessments show that PT ITSEC Asia Tbk has implemented rigorous internal and external controls, supported by employee training that enhances fraud awareness and skills. In addition, the company has implemented various technologies and systems to detect and prevent fraud, such as the Cyber Fraud Fusion Center, and has complied with various international standards, including ISO 27001 and Financial Services Authority (OJK) regulations. Overall, PT ITSEC Asia Tbk continues to innovate and adapt to technological changes to protect clients' businesses from all cyber threats to ensure their business continuity*

Keywords: *fraud detecting system; itsec asia ltd; performance analysis*

Pendahuluan

Perkembangan teknologi merupakan suatu kondisi dan bukti mulai memprioritasnya praktik kerja berbasis penerapan teknologi informasi. Tidak bisa dipungkiri, hampir semua sektor menggunakan sistem kerja yang sudah difasilitasi oleh platform tertentu untuk mempermudah *handle* kerja. Dalam konteks halnya akuntansi, untuk pencatatan laporan keuangan suatu perusahaan juga sudah menggunakan banyak aplikasi khusus untuk mempermudah pencatatan transaksi. profesi lain dibidang akuntan yang sedang *hight demand* yaitu *fraud investigasi*. *Fraud* secara umum yaitu aktifitas yang merugikan individu, organisasi, maupun perusahaan, yang berdampak terhadap perekonomian yang serius ((Maulidi, 2016). Dalam hal kaitannya dengan penyelewengan keuangan, pelaku *fraud* memanipulasi informasi keuangan dengan maksud menipu, demi mendapatkan keuntungan pribadi ((Afiani, 2022). Tentunya semua jenis kasus *fraud* tergolong sebagai aktifitas *cyber criminal*. Bahkan tak tanggung-tanggung, beberapa kasus *fraud* di perusahaan melibatkan para petingginya yang tentu ini menjadi *fraud* skala besar (Handayani, 2016). Insiden kecurangan laporan keuangan ini, dalam pencegahannya membutuhkan ahli dibidang keamanan informasi terkait keuangan, yaitu akuntan forensik atau auditor forensic ((Dandi, 2021)). Peningkatan risiko penyelewengan keuangan *(Financial Fraud)* di berbagai sektor industri, termasuk sektor keuangan dan layanan siber semakin menuntut perusahaan untuk memperkuat sistem pengendalian internal guna mencegah dan mendeteksi tindakan

penipuan. Salah satu pendekatan yang semakin populer ialah *Whistleblowing System*, yaitu sistem pelaporan yang memungkinkan individu dalam organisasi untuk melaporkan tindakan *fraud* atau kecurangan bentuk lainnya secara privasi ((Irawan, 2018).

Whistleblowing System menjalankan target penting dalam upaya mendukung standar kepatuhan dan transparansi dalam suatu perusahaan. Menurut penelitian *Association of Certified Fraud Examiners* (ACFE), 45% kasus *fraud* terungkap melalui laporan staf atau pihak ketiga menggunakan *Whistleblowing System* (Moyes, 2006). Sistem ini membantu organisasi dan instansi dalam deteksi penyelewengan yang mungkin tidak teridentifikasi melalui audit atau sistem berbasis manual lainnya. Terlebih *fraud* sering melibatkan pihak internal yang memiliki akses luas terhadap database keuangan serta data privasi perusahaan lainnya ((Oktaviany, 2023). Dalam konteks perusahaan keamanan siber seperti PT ITSEC Asia Tbk, implementasi *Whistleblowing System* tentunya sangat efektif mengingat tingginya kerentanan terhadap kejahatan dunia maya dan *fraud* digital. Sistem ini berfungsi sebagai garis pertahanan tambahan yang memungkinkan karyawan atau pihak ketiga yang terlibat operasional untuk melaporkan tindakan tidak etis seperti manipulasi data keuangan, tanpa khawatir balasan dari pihak manajemen (Winatasari, 2023). Dengan adanya *Whistleblowing System* ini, risiko penyelewengan dapat ditekan karena adanya mekanisme pelaporan yang aman dan terintegrasi, yang memungkinkan organisasi untuk segera merespon tindakan yang berdampak merugikan (Siregar, 2015). Pada saat perusahaan publik menerbitkan laporannya, sebenarnya perusahaan ingin menggambarkan situasi dan kondisinya dalam keadaan terbaik (Skousen, 2008).

Ketika ada salah dalam penyajian material pada laporan keuangan, maka informasi yang disampaikan tersebut menjadi tidak relevan sebagai dasar dalam pengambilan keputusan, karena tidak menggunakan informasi yang sebenarnya (Pourhabibi, 2020). Beberapa tindakan, pencegahan, dan mitigasi tentunya harus dilakukan oleh divisi yang berperan terhadap pencegahan *fraud* ini, yakni dari manajemen perusahaan serta pengecekan secara berkala oleh pihak internal audit dan mitra audit dari luar. Selain pencegahan secara teknisi, juga dibutuhkan edukasi secara meluas untuk menyampaikan 3 dampak dan resiko dari aktifitas *fraud* tersebut. Marshall B. Romney (2014), seorang ahli dibidang akuntansi dan sistem informasi mengatakan definisi *fraud* sebagai tindakan yang disengaja untuk mendapatkan keuantungan pribadi yang tidak sah melalui penipuan ((R, 2021)). *Fraud* melibatkan manipulasi, penyembunyian, atau penyalahgunaan informasi baik dilakukan oleh individu, manajemen, staf, atau pihak ketiga. *Fraud* dapat terjadi dalam bentuk laporan keuangan yang menipu *(Fraudulent Financial Reporting)* atau penggelapan asset *(Misappropriation of Assets)*. Romney juga memperkenalkan teori *Fraud Triangle*, yang menjelaskan tiga elemen kunci penyebab terjadinya *fraud*, yakni Tekanan *(Pressure)*, Kesempatan *(Opportunity)*, dan Rasionalisasi *(Rasionalization)*. Berdasarkan pedoman anti kecurangan *(Fraud)*, ada beberapa poin dan landasan hukum yang mengatur tentang penanganan *fraud*, yakni: sebagai patokan yang diambil perusahaan dalam melakukan kontrol, dan mitigasi terhadap kemungkinan terjadinya kriminal yang merugikan perusahaan dari segi finansial maupun teknisi atau operasional ((Elisabeth, 2020)). Selain itu untuk pedoman ketegasan bagi perusahaan untuk memahami secara totalitas setiap level organisasi bahwa *fraud* ini adalah bentuk kriminal yang nyata dan berdampak terhadap reputasi perusahaan tersebut ((Aguiar, 2021)).

Analisis Kinerja Layanan *Fraud Detecting System* di Perusahaan Konsultan Keamanan Informasi untuk Mencegah Terjadinya *Fraud* Penyelewengan Keuangan membuat penulis dapat menarik fenomena yang relevan dengan perkembangan teknologi serta meningkatnya kebutuhan sistem pencegahan *fraud* di berbagai sektor industry ((Turner, 2003) dan (Widiyati, (2021, March).). Berikut diulas apa saja fenomena dari pemilihan judul oleh penulis:

Meningkatnya implemantasi teknologi informasi di sektor keuangan dan akuntansi perusahaan semakin bergantung pada teknologi informasi untuk mendukung 4 operasional, termasuk pencatatan

laporan keuangan. Teknologi informasi menfasilitasi prosedur akuntansi, dan juga menciptakan celah untuk penipuan finansial melalui manipulasi data

Peningkatan kasus *fraud* di tingkat internal dan eksternal *fraud* yang melibatkan manipulasi laporan keuangan oleh manajemen atau staf dengan akses luas terhadap sistem keuangan menjadi tantangan besar baru perusahaan, khususnya yang bergerak dibidang keamanan informasi. Kasus *fraud* skala besar ini memerlukan keahlian dalam akuntansi forensik untuk mendeteksi dan mencegah penipuan.

Kebutuhan sistem pengendalian yang lebih ketat adanya peningkatan risiko penyelewengan keuangan memicu perusahaan untuk menerapkan sistem pengendalian internal yang lebih efisien dan efektif, seperti implementasi *Whistleblowing System*. Sistem ini menjadi mekanisme yang sangat dibutuhkan untuk mendukung transparansi dan akuntabilitas, sekaligus memberi jalur aman bagi pelaporan tindakan *fraud* oleh karyawan.

Kerentanan perusahaan terhadap kejahatan dunia maya dan *fraud* digital khususnya dalam konteks perusahaan konsultan keamanan informasi seperti PT ITSEC Asia, Tbk, kerentanan terhadap kejahatan ruang digital dan *fraud* digital sangat tinggi. Oleh karenanya, sistem deteksi *fraud* yang kuat berbasis teknologi informasi sangat penting untuk melindungi data keuangan Perusahaan.

Kajian Pustaka

Teori Fraud

Salah satu cara dalam mendeteksi manipulasi pada laporan keuangan ialah menggunakan teori *fraud hexagon* yang dikembangkan oleh (Vousinas, 2019). Teori fraud hexagon adalah sebuah teori pengembangan yang melengkapi teori-teori kecurangan sebelumnya yaitu: teori fraud triangle, teori fraud diamond, dan teori fraud pentagon (Lucas, 2022). *Fraud hexagon* dipilih karena keterbaruan dari teori ini bisa memberikan gambaran yang lebih luas lagi karena bertambahnya faktor yang menjadi penyebab seseorang melakukan kecurangan. Hal ini dikarenakan dalam teori ini, terdapat 6 faktor yang menjadi landasan mengapa seseorang melakukan kecurangan dan memiliki faktor yang lebih kompleks dibandingkan teori fraud sebelumnya, yaitu Tekanan/Stimulus (Pressure/Stimulus), Kesempatan (Opportunity), Kapabilitas (Capability), Ego/Arogansi(Ego), Rasionalisasi (Rationalization), dan Kolusi (Collusion) (Elsayed, 2017) dan (Kaminski, 2017).

Kategori Fraud

Fraud dalam Laporan Keuangan (*Financial Statement Fraud*). Kategori ini mencakup tindakan manipulasi laporan keuangan untuk memberikan dampak yang salah kepada pemangku kepentingan seperti investor, auditor. Tindakan ini bertujuan untuk meningkatkan keuntungan dan mengurangi kerugian dengan cara menggembungkan pendapatan atau aset, menyembunyikan beban, dan mengubah catatan akuntansi untuk menciptakan laporan yang lebih baik dari kondisi nyatanya ((Christian, 2022).

Penggelapan Aset (*Asset Misappropriation*). Merupakan jenis fraud yang umum terjadi, dimana individual atau kelompok mencuri serta menyalahgunakan aset organisasi, yang mencakup pencurian kas dan properti, penyalahgunaan aset perusahaan, skimming (mengambil uang sebelum dicatat dalam buku)

Korupsi (*Corruption*). Korupsi terjadi ketika seseorang menyalahgunakan kekuasaan dalam organisasi demi meraup keuntungan pribadi, mencakup penyuapan, konflik kepentingan, dan pemerasan.

Pencurian Identitas (*Identity Theft*). Pencurian data identitas terjadi ketika seseorang mencuri data pribadi orang lain untuk mendapatkan keuntungan finansial. Sering menggunakan skema penipuan online seperti melalui kartu kredit.

Berikut diulas bagaimana penjelasan tentang pencegahan fraud berdasarkan referensi dari (Romney, 2014). Memeriksa pengendalian internal untuk menentukan efektivitas pengendalian internal adalah sistem dan prosedur yang dirancang untuk melindungi aset, mencegah kesalahan saji, serta memastikan keakuratan dan kehandalan informasi keuangan. Organisasi harus secara berkala memeriksa dan mengevaluasi pengendalian internal yang ada. Bertujuan untuk mengetahui apakah sistem pengendalian tersebut efektif dalam mendeteksi dan mencegah terjadinya kecurangan. Evaluasi pengendalian internal juga penting untuk mengidentifikasi kelemahan atau kerentanan yang bisa dimanfaatkan oleh para pelaku kecurangan dalam tujuan mengambil keuntungan.

Meletakkan pengendalian baru untuk mendeteksi penipuan setelah mengevaluasi efektivitas pengendalian internal yang ada, langkah berikutnya 10 ialah menerapkan pengendalian baru jika diperlukan. Pengendalian baru ini dirancang untuk meningkatkan kemampuan organisasi dalam mendeteksi dan mencegah potensi kecurangan. Misalnya, memperketat akses terhadap data keuangan menggunakan implementasi teknologi yang lebih canggih untuk mendeteksi pola penipuan, atau menerapkan audit independen secara berkala.

Melatih karyawan mengenai kesadaran penipuan, pengukuran keamanan, dan isu etis dengan pelatihan dan edukasi karyawan adalah langkah penting dalam pencegahan kecupangan. Dengan memberikan pelatihan tentang kesadaran kecurangan ini, karyawan menjadi lebih peka terhadap tanda tanda atau potensi penipuan dan lebih sadar akan tanggung jawab etis mereka. Pelatihan ini juga bertujuan untuk memberikan pengetahuan mengenai prosedur keamanan yang harus diikuti untuk melindungi data dan aset perusahaan. Melalui pelatihan, karyawan dapat dibekali keterampilan yang dibutuhkan untuk mengidentifikasi dan melaporkan tindakan mencurigakan sebelum kecurangan terjadi.

Berikut penjelasan tambahan mengenai teori deteksi anomali dan teori perilaku:

Teori Deteksi Anomali (*Anomaly Detection Theory*). Teori deteksi anomali ialah pendekatan yang digunakan untuk mengidentifikasi pola atau perilaku yang menyimpang dari etika data yang diharapkan dalam suatu sistem. Dalam konteks keamanan data dan keuangan, deteksi anomali berperan penting dalam menemukan indikasi penipuan atau aktivitas tidak wajar yang dapat merugikan organisasi. Pendekatan dalam deteksi anomali biasanya dilakukan dengan metode statistik, machine learning, atau algoritma tertentu.

Teori Analisis Perilaku (*Behavioral Analysis Theory*). Teori analisis perilaku berfokus pada analisis tindakan, kebiasaan, dan pola perilaku individu untuk mendeteksi potensi tindakan tidak wajar atau penipuan. Dalam konteks organisasi, memahami perilaku karyawan dan pihak tertentu sangat penting untuk mengidentifikasi tanda tanda awal kecurangan atau tindakan tidak etis.

Metode

Penelitian ini merupakan penelitian kualitatif yang bersifat subjektif, dalam artian penelitian yang mewawancarai langsung objek yang diteliti. Diasumsikan atas tindakan dari pengalaman yang ditangani langsung oleh pihak tertentu yang tentunya dapat dibuktikan secara keilmuan. Dalam paradigma ini, kebenaran data memberikan pandangan terhadap metodologi yang melandasinya. Penelitian ini menggunakan desain fenomena dan trend yang menggali pengalaman para praktisi berkaitan dengan fraud investigasi dalam menghadapi bentuk kecurangan terhadap finansial dan mengimplementasikan basis sistem deteksi dalam kinerja yang dijalani. Peneliti juga mengidentifikasi pentingnya investigasi

dan pencegahan fraud melalui kinerja praktisi dan layanan fraud detection di lingkungan perusahaan yang bergerak di bidang keamanan informasi ini. Peneliti pun juga melakukan kajian literatur atas penelitian terdahulu mengenai konsep fraud, dengan penjabaran berbagai aspek yang tentunya sangat penting untuk deteksi serta pencegahan *fraud*.

Pengumpulan data akan dilakukan dengan metode wawancara yang mendetail. Pada wawancara ini, peneliti mengumpulkan informasi dan informan dalam perihal penjabaran bagaimana kinerja layanan *Fraud Detection System* untuk membantu kinerja auditor investigasi pada perusahaan konsultan keamanan informasi tersebut. Pada penelitian ini, peneliti akan mengambil informan dari auditor investigasi dan Fraud Risk Management di perusahaan PT. ITSEC Asia Tbk.

Analisis data dalam penelitian ini menggunakan Analisis Naratif dan Wacana. Analisis Naratif adalah metode yang digunakan untuk menganalisa alur cerita dari informan atau kasus kasus kecurangan yang telah dideteksi oleh sistem. Fokusnya adalah bagaimana cerita tersebut disusun dan apa yang bisa dipelajari dari alur tersebut mengenai modus operandi dan pola kecurangan. Begitupun dengan analisis wacana, yang menjabarkan bagaimana para pengguna, praktisi, atau bahkan pelaku kecurangan berbicara tentang. Sistem pendeteksi fraud dan fenomena fraud itu sendiri. Karena di dalam penelitian ini memerlukan metode analisis yang dapat mengupas permasalahan secara detail dan terperinci terkait kinerja layanan Fraud Detection System di perusahaan konsultan keamanan informasi yaitu PT ITSEC Asia Tbk untuk mencegah terjadinya fraud penyelewengan terhadap keuangan serta dapat menjelaskan sejauh mana fenomena tersebut terjadi.

Penelitian ini juga berfokus untuk menganalisis berbagai faktor yang mempengaruhi terjadinya fraud dalam laporan keuangan serta mendeteksi tanda tanda awal terjadinya penipuan. Dengan meningkatnya kasus penipuan dan manipulasi dalam laporan keuangan, teknik seperti pengujian anomali, *forensic accounting*, dan *fraud detection* menjadi penting untuk mendukung transparansi dan akuntabilitas. Penelitian ini menyinggung berbagai aspek penting terkait dengan pencegahan, pendeteksian, dan investigasi *fraud*, termasuk tata kelola perusahaan (*corporate governance*), *whistleblowing system,* audit internal dan eksternal, tanda peringatan *fraud (red flags*), serta penyajian pelaporan keuangan yang curang (*fraudulent financial reporting*).

Analisis Data

Manajemen Puncak

PT ITSEC Asia Tbk telah menerapkan strategi yang canggih dalam mendeteksi fraud melalui pengembangan Fraud Management System (FMS), yang merupakan salah satu solusi terbesar di Asia Tenggara. Sistem ini tidak hanya berfungsi sebagai alat untuk mendeteksi penipuan, tetapi juga sebagai platform yang terintegrasi untuk melindungi bisnis klien dari berbagai aktivitas fraud yang kompleks. Melalui pemahaman yang mendalam mengenai teknik fraud yang terus berkembang, PT ITSEC Asia Tbk dapat memberikan solusi yang tepat dengan menggabungkan teknologi mutakhir dalam keahlian industri. Fraud Management System juga memiliki serangkaian kebijakan yang difokuskan terhadap kepentingan berbagai asset, yakni sebagai berikut:

Fraud Detection yang Komprehensif. FMS memiliki kemampuan menganalisis secara mendalam suatu insiden fraud secara real-time dengan pendekatan analitik yang komprehensif. Sistem ini mampu meminimalisasi kerugian di sektor finansial, serta melindungi reputasi organisasi. Keahlian deteksi fraud ini menjadi salah satu fondasi utama dalam menjaga kepercayaan klien.

Analisis dan Pemantauan Data Lanjutan. PT ITSEC Asia Tbk memiliki kebijakan yang mengkombinasikan kemampuan analisis data untuk mengidentifikasi skema fraud secara detail,

mengurangi kerugian finansial, dan memitigasi risiko reputasi. Data yang dianalisis mencakup pola aktivitas yang mencurigakan dan memungkinkan deteksi dini terhadap insiden yang merugikan.

Penilaian pada Risiko Fraud. PT ITSEC Asia Tbk secara pro-aktif mengidentifikasi dan memitigasi risiko fraud. Langkah ini bertujuan untuk meningkatkan kemampuan pencegahan fraud secara totalitas. Sehingga mengurangi kemungkinan kerugian finansial yang terjadi.

Selalu berinovasi dan berkelanjutan. PT ITSEC Asia Tbk selalu berupaya selangkah lebih maju dari ancaman para pelaku fraud dengan terus memperbaharui sistem pencegahan fraud, beradaptasi dengan teknik penipuan baru, dan meningkatkan efektivitas sistem Fraud Risk Management secara keseluruhan.

Kepatuhan terhadap Peraturan dan Pelaporan. PT ITSEC Asia Tbk selalu menerapkan kebijakan terhadap kepatuhan sesuai peraturan yang berlaku dan menunjukkan komitmen terhadap keamanan data serta pencegahan fraud, sehingga meningkatkan kepercayaan di antara para pemangku kepentingan.Berikut adalah hasil analisis statistik deskriptif untuk variabel.

Beberapa hal yang masih menjadi sebuah tantangan bagi PT ITSEC Asia Tbk dalam menghadapi strategi implementasi sistem deteksi fraud antara lain modus operandi atau prosedur operasi kejahatan yang semakin canggih menjadi tantangan utama PT ITSEC Asia Tbk. Pelaku fraud terus mengembangkan tekniknya dalam memanipulasi target hingga semakin sulit untuk dideteksi. PT ITSEC Asia Tbk juga menghadapi kendala regulasi dan beberapa kepatuhan di berbagai kewenangan tempat perusahaan beroperasi. Terlebih PT. ITSEC Asia Tbk memiliki 5 kantor yang tersebar di 5 negara, tentunya terdapat perbedaan dalam peraturan yang dapat menyulitkan perusahaan untuk mengembangkan sistem deteksi fraud yang konsisten dan efektif untuk semua lokasi. Serangan siber dapat mengganggu proses berlangsungnya operasi bisnis, mengakibatkan periode terhenti, dan berdampak terhadap *income*.

Penilaian Tim Keuangan dan Audit

Sistem Pengendalian dan Pengawasan (Internal dan Eksternal). PT ITSEC Asia Tbk menerapkan sistem pengawasan yang sangat ketat melalui *Fraud Management System*, didukung oleh kebijakan audit internal dan eksternal. *Fraud Management System* selalu menawarkan serangkaian tindakan berkala untuk membentengi bisnis klien dan organisasi dari segala aktivitas *fraud.*

Pelatihan dan Edukasi Karyawan. Mengingat pola ancaman fraud semakin berubah dan meningkat, tim keamanan harus memperbaharui kemampuan dan pemahaman mereka secara berkala. ITSEC mengambil pendekatan kohesif terhadap pelatihan keamanan yang menggabungkan program spesialis untuk team keamanan disamping Langkah peningkatan kesadaran yang lebih luas. Pertahanan siber secara umum masih rentan dan memiliki banyak celah serangan, oleh karena itu semua karyawan atau tim harus berperan dalam meminimalisasi ancaman keamanan tersebut. Pelatihan kesadaran keamanan siber bagi profesional non-keamanan juga bermanfaat sebagai komponen penting dalam mengurangi risiko. Program kesadaran keamanan siber ITSEC menyediakan serangkaian layanan keamanan yang luas untuk melatih para eksekutif perusahaan, karyawan, dan kontraktor guna meningkatkan ketahanan mereka terhadap segala bentuk serangan, termasuk fraud.

Pengalaman Dari Kasus Kasus Fraud Yang Pernah Terjadi. Beberapa waktu yang lalu, anggota klien menceritakan kejadian buruk yang terjadi di kantor nya. Salah satu staff keuangan menerima email yang mengklaim adanya perubahan nomor rekening bank untuk pembayaran sebuah tagihan dari supplier. Karena kebetulan memang ada pesanan yang harus dibayar, staff tersebut mengirim uang ke rekening yang tercantum di email tersebut. Setelah disetorkan, baru disadari uang tersebut tidak pernah sampai ke tujuan yang semestinya. Dilakukan penyelidikan lebih lanjut, ditemukan bukti bahwa alamat email yang digunakan memiliki domain yang berbeda atau manipulasi domain. Karena sekilas

domainnya terlihat mirip, sehingga cukup menipu bagi staff yang tidak teliti. Kejadian seperti ini bisa disebut sebagai online fraud atau cyber fraud yang menargetkan kerugian terhadap finansial. Sebenarnya, tujuan dari serangan tersebut bisa beragam. Jika menyebabkan kerugian dari sektor finansial, serangan ini bisa dikategorikan Financial Fraud.

Implementasi Teknologi dan Organisasi Dalam Deteksi *Fraud.* Untuk mengatasi permasalahan yang kompleks, konsep *Cyber Fraud Fusion Center* mulai diutamakan. Karenanya PT ITSEC Asia Tbk pun juga mengintegrasi personel, aplikasi, dan proses dari tim Cyber Security dan Fraud Risk Management ke dalam satu unit. Ini merupakan respon dalam menghadapi berkembangnya penyedia layanan serangan siber (*Cybercrime as a Service*) yang menawarkan berbagai jasa serangan siber dan penerimaan dana illegal.

Kolaborasi Tim IT Security dalam Upaya Keamanan Siber

Hasil penelitian mengungkap bahwa adanya audit internal mempunyai pengaruh signifikan terhadap kinerja dalam pencegahan fraud. Efektivitas peran audit internal juga memberikan kontribusi bagi suatu perusahaan, yang meliputi penilaian audit terhadap resiko manajemen, melakukan proses tata kelola serta pengawasan, mengevaluasi update rencana kegiatan audit, meningkatkan produktivitas para staff, meningkatkan efisien prosedur audit untuk mencapat target. Bersamaan dengan penyediaan audit, Audit Risiko sebagai bagian keamanan informasi PT ITSEC Asia Tbk membantu organisasi untuk lebih fokus dengan investasi keamanan secara berkelanjutan sesuai dengan kebijakan, prosedur, dan kontrol keamanan yang ada. Audit risiko mempunyai beberapa peran penting dalam halnya mendeteksi dan pencegahan fraud, seperti Identifikasi insiden fraud, Analisis risiko secara berkelanjutan, mengambangkan kebijakan yang akan dilaksanakan untuk prosedur anti-fraud, pelaksanaan audit serta pengawasan, kontroling sistem dan pelaporan insiden kepada pihak manajemen hingga dewan direksi komite audit.

Kepatuhan terhadap Peraturan Otoritas Jasa Keuangan (PJOK). PJOK ialah badan yang mengatur sektor jasa keuangan di Republik Indonesia. Semua Lembaga keuangan di Indonesia dan entitas luar negeri diwajibkan oleh hukum untuk mematuhi aturan kepatuhan OJK. ITSEC Asia hadir di Indonesia kurang lebih satu dekade dan penyedia layanan keamanan informasi terkemuka, termasuk kepatuhan keamanan berdasarkan aturan OJK. UU Perlindungan Data Pribadi Indonesia disahkan pada 17 Oktober 2022, mengatur pengumpulan, penggunaan, pengungkapan, dan pemprosesan data pribadi lainnya oleh organisasi internasional, entitas pemerintah dan swasta. Beberapa hal yang harus dipertimbangkan, seperti UU PDP akan berlaku bagi bisnis yang berkedudukan, baik di dalam maupun luar Negara Republik Indonesia, Sanksi administratif berdasarkan UU PDP antara lain dari peringatan tertulis, penghentian sementara kegiatan pemprosesan data pribadi, penghapusan atau pemusnahan data pribadi, atau denda yang berlaku. Selain itu, juga berlaku sanksi berat seperti hukuman pidana (penjara), penyitaan aset, pencabutan izin, bahkan pembekuan usaha. ITSEC Asia memiliki keahlian dan pengalaman dalam membantu otganisasi agar memenuhi serta mematuhi peraturan UU PDP, dengan menyediakan forum diskusi dan konsultasi untuk penerapan kebijakan kepatuhan UU PDP.

Audit Internal

Perencanaan Audit. Prosedur ini berfokus terhadap penentuan teknis audit yang berkaitan dengan identifikasi aktivitas fraud yang berisiko tinggi. Tim audit menggunakan informasi dari data laporan hasil audit tahun sebelum nya, serta mengidentifikasi bagian yang membutuhkan analisis khusus bersama pihak Fraud Risk Management.

Pengumpulan Data dan Bukti. Di prosedur ini, tim audit PT. ITSEC Asia TBk akan mengumpulkan data dan bukti bukti kegiatan operasional dan keuangan perusahaan. Selain itu, juga

dilakukan pemeriksaan terkaitsemua bentuk transaksi, baik itu melalui dokumen dokumen pendukung maupun analisis data melalui sistem.

Pengujian Pengendalian Internal. Tim audit ITSEC menguji dan mengevaluasi pelaksanaan pengendalian internal dan sistem manajemen resiko sesuai dengan kebijakan perusahaan.

Identifikasi dan Analisis Anomali. Selama proses, tim audit ITSEC melakukan pemeriksaan dan penilaian secara efisiensi terhadap aktivitas yang mencurigakan atau anomali berdasarkan temuan temuan, baik di bagian keuangan, akuntansi, operasional, teknologi informasi, pemasaran, dan aktivitas lainnya.

Pelaporan Temuan. Membuat laporan hasil pemeriksaan dan menyampaikan pelaporan tersebut kepada Presiden Direktur dan Komite Audit.

Tindak Lanjut Atas Temuan Audit. Tahap akhir, tim audit akan memantau, menganalisis, dan melaporkan pelaksanaan tindak lanjut perbaikan yang telah disarankan atas hasil kesepakatan pihak terkait.

Dalam audit internal yang pernah dilaksanakan pada waktu sebelumnya di perusahaan klien, anggota tim audit ITSEC Asia menemukan suatu insiden yang terbilang cukup buruk. Insiden bermula dari kecerobohan salah satu staff keuangan, telah menerima email yang mengklaim adanya perubahan nomor rekening bank untuk pembayaran tagihan dari Supplier. Karena bertepatan dengan adanya sebuah pesanan yang harus dibayar, staff tersebut mengirim uang ke rekening yang tercantum di email si penipu tersebut. Setelah disetorkan, baru disadari adanya abnormal yang telah terjadi, dimana uang setoran tersebut tidak pernah sampai ke rekening tujuan yg resmi. Dilakukan penyelidikan lebih lanjut oleh tim ITSEC Asia, ditemukanlah bukti bahwa alamat email yang digunakan hanyalah manipulasi domain yang sekilas terlihat mirip, sehingga membuat si staff tidak menyadari nya dan terlanjur melakukan transaksi ke nomor rekening penipu tersebut. Kasus seperti ini menjadi salah satu insiden paling umum yang disebut sebagai *Financial Fraud* (penipuan keuangan) yang tentunya menargetkan finansial sebagai target kerugian. Insiden seperti ini bisa terjadi akibat kelalaian internal perusahaan yang minimnya edukasi tentang keamanan ruang digital.

Kebijakan dan Prosedur Operasional Anti-Fraud

Kebijakan strategi anti-fraud dalam suatu perusahaan, terutama industri keamanan siber memang sangat penting untuk mengantisipasi terjadinya kecurangan yang berdampak terhadap kerugian serius dalam suatu bisnis. Penerapan anti-fraud tentunya sangat berpengaruh terhadap kinerja operasional di lingkungan kerja agar kondusif, menjaga reputasi atau value perusahaan, serta mencegah kerugian yang signifikan terhadap perusahaan. Fraud Management Consultant PT. ITSEC Asia Tbk, Bapak Joshua Cristopher, CFE mengatakan untuk menyatakan bahwa suatu aktivitas dianggap Fraud, harus memenuhi beberapa unsur, yakni penyelewengan yang disengaja dibiarkan untuk mengelabui, memanipulasi perusahaan, nasabah, serta pihak lain. Unsur kedua yaitu menyebabkan dampak kerugian bagi kinerja perusahaan. Unsur ketiga pelaku fraud mendapatkan keuntungan atas kerugian yang diperbuat baik secara langsung maupun tidak langsung. Dan unsur yang terakhir yaitu terdapat putusan dari hasil laporan investigasi yang telah diputuskan pihak berwenang terkait pendeteksian fraud. Dilain kebijakan dan prosedur yang dimiliki perusahaan, PT ITSEC Asia Tbk tentunya juga memiliki kode etik bagi Audit Internal atas kesungguhan dalam menjalankan tugasnya.

Integritas. Auditor internal PT ITSEC Asia Tbk harus memiliki integritas untuk membentuk keyakinan serta menjadi acuan kepercayaan auditee terhadap pertimbangan auditor internal. Oleh karenanya, auditor internal harus menunjukkan kejujuran, objektivitas, dan keseriusan dalam menjalankan tugas dan memenuhi tanggung ajwab profesinya. Auditor internal juga harus menunjukkan loyalitas, dan menjunjung tinggi aspek hukum, etika, dan standar perusahaan.

Objektivitas. Auditor internal PT. ITSEC Asia Tbk harus menunjukkan objektivitas professional dalam melaksanakan tugas. Auditor internal melakukan penilaian yang seimbang, tidak terpengaruh oleh kepentingan pribadi dan pihak lain dalam memberikan pertimbangan dan putusan. Karenanya, audit internal harus menahan diri dari unsur yang menimbulkan konflik dengan kebijakan perusahaan atau kegiatan yang berpotensi menimbulkan kecurigaan yang dapat menimbulkan keraguan atas kemampuannya untuk menjalankan tugas yang objektif dan professional. Dalam melaporkan hasil kinerjanya, audit internal PT. ITSEC Asia Tbk harus mengungkapkan semua fakta yang ditemukan, tidak mendistorsi dan menutupi adanya praktik praktik yang melanggar hukum seperti Fraud.

Kerahasiaan. Auditor internal PT ITSEC Asia Tbk harus menghormati nilai dan kepentingan kepemilihan informasi yang diterimanya dan tidak mengungkap informasi tersebut secara public tanpa otorisasi pejabat berwenang, kecuali diharuskan oleh hukum atau profesi tertentu untuk tujuan tertentu. Oleh karenanya, harus bersikap dan bertindak hati hati dalam menggunakan informasi yang diperoleh dalam pelaksanaa tugas. Serta tidak diperbolehkan menggunakan informasi untuk mencari keuntungan pribadi apalagi bertentangan dengan hukum dan etika yang berlaku di PT ITSEC Asia Tbk.

Kompetensi. Auditor internal PT ITSEC Asia Tbk harus menerapkan pengetahuan, kecakapan, dan pengalaman yang baik dalam setiap penugasan audit. Oleh karenanya, auditor internal harus melakukan setiap penugasan untuk pekerjaan dengan pengetahuan, keahlian, dan pengalaman

Data Operasional System

Dalam pembahasan sebelumnya, PT. ITSEC Asia Tbk memiliki mekanisme pelaporan efektif terhadap pelaksanaan penanganan *Fraud* manggunakan *Fraud Management System* (FMS). Menggunakan *Fraud Management System* untuk pelaporan penanganan insiden fraud tentunya mencakup serangkaian mekanisme yang dirancang untuk deteksi, investigasi, pelaporan, dan tindaklanjut insiden fraud secara efektif. Pendekatan yang digunakan PT. ITSEC Asia Tbk berbasis Fraud Hexagon Theory. Kerangka metode ini merupakan pengembangan dan penggabungan dari konsep fraud sebelumnya, yaitu *Triangle* dan *Pentagon*. *Fraud Triangle* sendiri menjelaskan 3 indikator seseorang melakukan fraud, yakni tekanan, kesempatan, dan resionalisasi. Sedangkan dalam konsep *Fraud Pentagon* ada 2 indikator penyebab seseorang melakukan aktivitas *fraud,* yaitu kompetensi dan arogansi. Berikut dijabarkan bagaimana penerapan *Fraud Hexagon* pada prosedur anti-fraud di sistem deteksi fraud PT. ITSEC Asia Tbk.

Kebutuhan/Tekanan. Kebijakan operasional perusahaan bersama Dewan Komite Audit dan *Fraud Risk Management* berfokus pada identifikasi tekanan internal dan eksternal yang mendorong karyawan atau pihak lain melakukan kejahatan fraud, seperti krisis finansial dan target yang tidak sesuai dengan realita.

Kesempatan. Mengkonfirmasi proses identifikasi kerentanan oleh seluruh divisi untuk memastikan celah terjadinya fraud dapat diminimalisasi. Fraud Management System secara otomatis memantau aktivitas anomali, menutup celah yang dapat dieksploitasi oleh pihak yang berniat melakukan fraud.

Rasionalisasi. Program edukasi dan sosialisasi anti-fraud yang menumbuhkan kesadaran di lingkungan perusahaan, dapat menekan perilaku fraud.

Kemampuan. Dengan penerapan *Fraud Management System* serta dukungan pelatihan secara intensif, perusahaan meningkatkan kemampuan tim dalam mendeteksi dan menangani fraud, sekaligus memantau peran yang memiliki akses lebih penuh terhadap potensi fraud.

Arogansi. Penerapan audit berkala dam pemantauan ketat oleh *Fraud Management System* bertujuan untuk mengurangi dan menekan arogansi para pelaku fraud yang awalnya mereka berpikir

aktivitas yang diperbuat tidak akan dikenai sanksi hukum karena pengaruh mereka dalam lingkungan perusahaan.

Budaya/Kepatuhan. Proses dokumentasi dan penyimpanan yang ketat, serta monitoring berkala oleh Dewan Komite Audit bersama *Fraud Risk* Management memastikan bahwa perusahaan tetap patuh terhadap kebijakan dan standar operasional yang berlaku, membentuk budaya organisasi yang berambisi terhadap integritas dan dan transparansi.

Pendekatan berbasis *Fraud Hexagon Theory* memastikan deteksi dan penanganan *fraud* yang lebih kompleks dan komprehensif, tidak hanya berfokus pada pencegahan secara teknis, tapi juga memperhatikan aspek aspek human dan culture yang akan menjadi faktor pendorong terjadinya kejahatan fraud. Dengan begitu, PT. ITSEC Asia Tbk mampu mengantisipasi risiko fraud secara efektif. Dengan menggunakan kerangka metode *Fraud Hexagon Theory*, PT. ITSEC Asia Tbk tidak hanya fokus dari segi mekanisme teknis, tetapi juga berpatokan terhadap aspek *humanity* dan *culture* untuk meminimalisasi risiko kejahatan *fraud.*

Insiden yang Pernah Diidentifikasi

Penipuan melalui email phising yang banyak menargetkan staf keuangan atau *system user*. Deteksi otomatis oleh *Fraud Management System* mampu menganalisis pola manipulasi email dan aktivitas transaksi dalam respon yang cepat. Kerugian mampu dicegah, karena dana dapat dikembalikan setelah investigasi tim audit risiko berdasarkan hasil deteksi sistem di awal tadi.

Kasus manipulasi data transaksi. Adanya sebuah laporan keuangan klien yang menunjukkan transaksi besar yang tidak biasa dilakukan oleh staf terkait. Staf tersebut berusaha mengalihkan dana ke rekening palsu atas nama pribadi yang dimanipulasi. *Fraud Management System* telah mengidentifikasi anomali pada pola transaksi dan mengeluarkan sistem peringatan. Tim audit risiko kemudian melakukan penyelidikan lebih lanjut untuk mengkonfirmasi keabsahan transaksi. Pada hasilnya, tim audit menemukan bukti pemalsuan dokumen dan segera menghentikan aktivitas transaksi. Staf yang terlibat kemudian dilaporkan ke pihak manajemen puncak perusahaan klien untuk selanjutnya diambil tindakan internal yang tegas.

Kasus kecurangan internal dalam pengadaan. Terdapat indikasi bahwa, seorang oknum staf di departemen pengadaan bekerja sama dengan pemasok untuk menaikkan harga barang dan menerima komisi ilegal. *Fraud Management System* melakukan monitoring pada seluruh transaksi pengadaan dan mendeteksi pola harga yang tidak konsisten. Sistem secara otomatis menandai transaksi transaksi yang mencurigakan untuk ditinjau lebih lanjut oleh tim audit risiko. Hasil investigasi menunjukkan adanya kolusi antara oknum staf dan pemasok. Tim ITSEC Asia Tbk menghentikan kerjasama dengan mengambil tindakan disipliner terhadap oknum staf yang terlibat, sekaligus memperketat kebijakan pengadaan.

Insiden yang Tidak Berhasil Diidentifikasi

Pada tahun 2018 silam, salah satu perusahaan klien PT ITSEC Asia Tbk yang bergerak dibidang *e-commerce* besar, mengalami kebocoran data 62 pelanggan yang serius. Staf departemen keuangan terlibat aktivitas penjualan informasi pelanggan, termasuk data kartu kredit dan alamat, melalui jaringan anonimitas di darkweb. Keterbatasan *Fraud Management System* yang belum mampu mendeteksi atau aktivitas yang terjadi di darkweb. Oleh karena itu, staf tersebut dapat dengan mudah menjual data tanpa terdeteksi dalam sistem internal. Insiden ini baru bisa terungkap setelah beberapa minggu, ketika agen intelijen berskala internasional yang berfokus pada tindak kejahatan siber melaporkan aktivitas penjualan data yang mencurigakan dari perusahaan klien PT ITSEC Asia Tbk. Setelah dilakukan penyelidikan bersama, agen intelijen memberitahu PT ITSEC Asia Tbk tentang potensi kebocoran data, sehingga manajemen dapat mengambil tindakan yang cepat dan tepat. Berkat bantuan agen

intelijen ini, tim PT ITSEC Asia Tbk berhasil mengidentifikasi staf yang terlibat dan melakukan tindakan disipliner. Dari kasus ini, mendorong PT ITSEC Asia Tbk untuk meningkatkan Fraud Management System dan bekerja sama dengan agen intelijen internasional dalam pemantauan aktivitas kejahatan di darkweb untuk mendeteksi potensi ancaman di masa mendatang.

Berdasarkan hasil investigasi kasus fraud secara menyeluruh yang pernah ditangani PT. ITSEC Asia Tbk, terdapat berbagai permasalahan terhadap operasional perusahaan, baik itu dalam halnya tantangan bagi para karyawan, maupun kinerja keuangan perusahaan. Perusahaan yang beroperasi dalam kondisi persaingan yang begitu ketat, belum begitu mampu mencapai kinerja yang ditargetkan. Dalam beberapa kasus, perusahaan membutuhkan dana lebih untuk mendukung pertumbuhan, pengembangan, atau keberlanjutan bisnis nya. Dana lebih ini tentunya diperoleh melalui investasi dari investor. Laporan keuangan dari perusahaan harus stabil agar dinilai menguntungkan bagi para investor. Dikarenakan banyaknya laporan keuangan dari perusahaan yang masih jauh dari target, maka pihak perusahaan nekat melakukan tindakan fraud dengan memanipulasi laporan keuangan mereka. Kasus manipulasi laporan keuangan masih marak terjadi meskipun sudah sering dilakukan upaya upaya pencegahan yang signifikan oleh perusahaan konsultan keamanan informasi, termasuk halnya ITSEC Asia. Salah satu teknik populer yang diterapkan untuk memanipulasi laporan keuangan ialah Financial Shenanigans. Teknik ini bertujuan memberikan informasi yang salah terkait kinerja laporan keuangan dari perusahaan. Beberapa kasus yang ditangani ITSEC Asia, ditemukan penipuan terhadap investor dengan cara mencatat pendapatan dengan asal asalan bahkan menyembunyikan biaya tertentu yang pada akhirnya setelah dideteksi, tim pun berkesimpulan bahwa pendapatannya telah dilakukan manipulasi. Berdasarkan analisis dari skema kasus fraud yang pernah ditangani, fraud manipulasi laporan keuanganlah yang sangat merugikan di Indonesia meskipun kasusnya lebih rendah ketimbang kasus fraud lainnya. Penelitian ini akan menyinggung sebuah analisis kasus manipulasi laporan keuangan oleh PT. Hanson International Tbk yang mana PT. ITSEC Asia Tbk ikut berkontribusi dalam menginvestigasinya. PT. Hanson International sudah terbukti melakukan tindakan manipulasi laporan keuangan setelah teridentifikasi oleh sistem manajemen fraud melakukan teknik teknik spesifik yakni *Cash Flow Shenanigans* (*Overstating Income*).

Praktik awal yang teridentifikasi ialah pengalihan arus kas bagian biaya ke bagian operasional. Praktik ini melibatkan perubahan klasifikasi dari arus kas yang seharusnya kategori pembiayaan tetapi menjadi operasional. Tujuannya mengelabui analisis manual dengan membuat laporan arus kas seolah terlihat positif atau stabil. Praktik berikutnya yakni meningkatkan arus kas operasional dengan aktivitas yang tidak berkelanjutan. Prosedur yang dilakukan dalam praktik ini antara lain:

1.Meningkatkan arus kas operasional dengan menunda nunda pembayaran ke vendor dengan tujuan perusahaan dapat mengurangi kas keluar dalam periode berlangsung.

2.Meningkatkan arus kas operasional secara cepat dengan menariknya dari pelanggan. Strategi ini cukup umum dilakukan untuk memperbaiki arus kas perusahaan. Perusahaan mempercepat tagihan piutang ke pelanggan agar kas masuk penjualan diterima lebih awal.

3.Meningkatkan arus kas operasional dengan pemanfaatan satu kali. Praktik ini melibatkan pengakuan atas penerimaan menfaat yang tidak berkaitan dengan jalannya operasional perusahaan.

Setelah kasus fraud ini berhasil diidentifikasi oleh tim dari PT. ITSEC Asia Tbk, langkah berikutnya yang dilakukan yakni Detailed Reporting. Out-put laporan yang telah di hasilkan oleh Sistem Manajemen Fraud milik PT. ITSEC Asia Tbk, selanjutnya dilakukan prosedur eskalasi kepada pihak berwenang dalam rangka evaluasi kasus. Dalam hal ini tentunya kepada pihak Otoritas Jasa Keungan yang berwenang melakukan pemeriksaan langsung terhadap PT Hanson International. OJK mempermasalahkan implementasi akuntansi metode akrual penuh oleh PT Hanson. Pihak PT Hanson

juga tidak mengungkap jika terdapat perjanjian pengikatan jual beli asset tanah di salah satu kawasan superblok daerah Tangerang. Hal ini mengakibatkan pendapatan perusahaan meningkat secara signifikan pada laporan keuangan tahunannya. Tentu, kasus ini sangat bertentangan dengan kebijakan yang berlaku dalam pasar modal.

Berikut ulasan atas pengembangan topik dari hasil wawancara dengan praktisi Fraud Consultant dari PT ITSEC Asia Tbk yang dilakukan pada tanggal 29 Maret 2024, 65 terkait topik "Kinerja Layanan Fraud Detecting System Untuk Mencegah Fraud Penyelewengan Keuangan" mengarah ke pertanyaan terkait bagaimana kebijakan pencegahan fraud pada PT ITSEC Asia, memuat hasil sebagai berikut:

Menurut *Fraud Consultant* di PT. ITSEC Asia Tbk menjelaskan bahwa potensi terjadinya fraud saat ini mengalami peningkatan yang signifikan, terutama dengan semakin meluasnya digitalisasi. Namun, hal ini juga menjadi penyebab meningkatnya risiko kejahatan fraud. Digitalisasi tidak hanya mempercepat kinerja, tetapi juga membuka celah bagi para pelaku fraud untuk mengeksploitasi celah keamanan yang ada. Untuk meminimalisasi risiko tersebut, perusahaan perlu memperkuat sistem kontrol internalnya. Termasuk dalam halnya penerapan basis teknologi keamanan tingkat tinggi serta program edukasi terkait dampak kejahatan, cara pencegahan, dan mitigasi risiko dari fraud yang terfokus kepada jajaran karyawan perusahaan. Dengan demikian, perusahaan dapat meningkatkan kinerja dalam upaya pencegahan *fraud* yang semakin canggih dan sulit terdeteksi. Di perusahaan konsultan keamanan siber sendiri, pasti ada kebijakan terkait anti-fraud. Oleh karenanya, penerapan anti-fraud sangatlah berpengaruh terhadap kinerja layanan fraud pada PT. ITSEC Asia Tbk, dan ini merupakan value bagi perusahaan untuk mengantisipasi segala kerugian bagi bisnis suatu perusahaan. Suatu aktivitas bisa dikategorikan sebagai insiden fraud, jika memenuhi standar ketetapan dari kebijakan perusahaan yakni penyelewengan yang dilakukan sengaja dibiarkan dengan tujuan mengelabui pihak tertentu yang mengakibatkan kerugian signifikan dan meraih keuntungan pribadi bagi para pelaku *fraud*. Standar ketetapan lainnya yakni masuk nya peringatan ke sistem deteksi, bahwa telah didapat aktivitas mencurigakan atau anomali pada pola transaksi yang biasa terjadi, maka segera dibuat laporan investigasi untuk selanjutnya diambil keputusan baik itu evaluasi bukti, pengawasan dan monitoring, pemulihan atas kerugian, hingga penetapan sanksi untuk diajukan putusan hukum oleh pihak berwenang. Dalam halnya PT. ITSEC Asia Tbk wewenang tersebut dipegang oleh Dewan Komite Audit dan *Fraud Risk Management*.

Berikutnya juga diulas hasil pengembangan wawancara terkait topik kinerja layanan *Fraud Detecting System* di perusahaan PT. ITSEC Asia Tbk dari sudut pandang divisi Direktur Keuangan. Direktur keuangan perusahaan, Responden tersebut mengidentifikasi peningkatan potensi insiden fraud sebagai dampak dari berbagai faktor internal maupun eksternal.

Lebih lanjut dikatakan, bahwa digitalisasi yang berkembang pesat berpeluang meningkatkan risiko kejahatan fraud, seperti manipulasi transaksi dan laporan keuangan melalui platform digital. Penerapan teknologi baru memang membawa pengaruh yang menguntungkan, tetapi juga ada tantangan besar yaitu membuka celah bagi para pelaku penipuan untuk beraksi. Risiko ini semakin diperparah dengan ketidakstabilan kondisi ekonomi yang menjadi penyebab tekanan finansial, sehingga memicu terjadinya aktivitas penyelewengan atau kecurangan demi memenuhi keuntungan pribadi. Perusahaan perlu meningkatkan pengawasan dan kesadaran akan potensi bahaya fraud. Hal ini menuntut integritas dan kepercayaan yang lebih tinggi bagi seluruh divisi terkait, agar tetap menjadi kepercayaan klien dalam pencegahan insiden *fraud*.

Narasumber menilai efektivitas deteksi *fraud* melalui berbagai indicator, diantaranya pendeteksian anomaly yang cepat, seberapa banyak kasus *fraud* yang berhasil diidentifikasi serta hasil evaluasi audit internal secara berkala yang akan memastikan seberapa akurat system deteksi tersebut.

Mengintegrasikan hasil dari system dengan kebijakan keuangan Perusahaan merupakan Langkah penting untuk mencegah dan mengelola semua risiko. Misalnya, adanya temuan atas transaksi yang rentan dimanipulasi, tim keuangan akan memperkuat sistematika prosedur dari transaksi tersebut. Integrasi juga membantu tim untuk membuat strategi manajemen risiko, sebagai bagian penilaian terhadap kinerja audit internal.

Simpulan

,PT. ITSEC Asia Tbk memiliki strategi pendeteksian *fraud* melalui sistem yang terkelola, yakni *Fraud Management System* yang mampu mendeteksi, analisis, dan memantau risiko *fraud* secara efektif dan kompleks. Namun, perusahaan tentunya juga menghadapi beberapa tantangan besar, termasuk halnya kendala regulasi di berbagai negara yang menjadi regional kantor PT. ITSEC Asia Tbk, serta tantangan ancaman fraud yang terus berkembang. Penilaian keuangan dan audit menunjukkan bahwa PT. ITSEC Asia Tbk telah menerapkan pengawasan internal dan eksternal yang ketat, didukung oleh pelatihan karyawan yang meningkatkan keahlian dan kesadaran menghadapi ancaman *fraud.* Selain itu, perusahaan telah mengimplementasikan berbagai teknologi dan sistem untuk mendeteksi dan mencegah *fraud*, seperti *Cyber Fraud Fusion Center*, dan telah mematuhi berbagai standar international, termasuk ISO 27001 dan peraturan Otoritas Jasa Keuangan (OJK). Dari data hasil wawancara di PT ITSEC Asia, dapat ditarik kesimpulan bahwa pandangan berbagai praktisi sangatlah serius terhadap potensi kejahatan *fraud*, terutama di era digitalisasi. Sistem deteksi *fraud* di perusahaan dinilai efektif jika dapat mendeteksi dan mencegah kasus fraud dengan cepat dan kompleks. Sistem deteksi *fraud* juga harus terintegrasi dengan kebijakan prosedur keuangan dari perusahaan untuk mengantisipasi serta menekan risiko secara komprehensif. Evaluasi berkala melalui audit internal dan update kebijakan berdasarkan hasil dari sistem deteksi merupakan bagian dari strategi untuk menjaga integritas dan kepercayaan dalam pengelolaan keuangan perusahaan. PT. ITSEC Asia Tbk menerapkan *Fraud Hexagon Theory* dalam sistem pelaporan dan penanganan fraud untuk mencapai deteksi dan pengendalian kejahatan fraud yang efektif. Pendekatan tersebut mencakup enam aspek, yakni kebutuhan/tekanan, kessempatan, rasionalisasi, kemampuan, arogansi, serta budaya/kepatuhan. Kebijakan anti-fraud PT. ITSEC Asia Tbk juga mencakup langkah yang proaktif untuk mengidentifikasi dan mencegah penyelewengan serta anomali transaksi yang membantu melindungi internal perusahaan dari potensi kerugian. Secara keseluruhan, meskipun terdapat beberapa kelemahan, keberhasilan dalam mengidentifikasi dan mencegah *fraud* lebih dominan, menegaskan pentingnya sistem deteksi yang kuat dan responsif dalam melindungi klien dari risiko keuangan dan reputasi.Hasil pengujian hipotesis menunjukkan bahwa *financial stability* dan *financial target* berpengaruh positif signifikan terhadap *fraudulent financial reporting*, sedangkan *variabel external pressure, ineffective monitoring, audit fee, change in director, change in auditor, rasio total akrual*, dan *CEO Duality* tidak berpengaruh signifikan terhadap kemungkinan terjadinya *fraudulent financial reporting.*

Daftar Pustaka

Afiani, J. R. (2022). Systematic Literature Review: Kecurangan Laporan Keuangan Di Indonesia Dan Malaysia. . JRAK (Jurnal Riset Akuntansi dan Bisnis), 8(2), 91-102.

Christian, N. (2022). Efek Mediasi Kesulitan Keuangan dalam Mendeteksi Corporate Fraud di Indonesia. . Jurnal Kajian Akuntansi, 6(1),, 44-69. .

Dandi, M. &. (2021). Pengaruh Bystander Effect terhadap Kecurangan Laporan Keuangan. Academia, 307-309.

Elisabeth, D. M. (2020). Analisis Review Pendeteksian Kecurangan (Fraud). METHOSIKA:Jurnal Akuntansi dan Keuangan Methodist, 4(1), , 9-18.

Elsayed, A. A. (2017). Indicators of the Financial Statement Fraud (Red Flags). SSRN. https://ssrn.com/abstract=3074187.

Handayani, T. &. (2016). Correlation of Financial Statement Components in Detecting Financial Fraud. . Asia Pacific Fraud Journal, 1(2), 275. https://doi.org/10.21532/apfj.001.16.01.02.22 .

Irawan, K. F. (2018). Analisis Pengaruh Pengalaman Audit, Beban kerja, Skeptisme Profesional, dan Independensi Terhadap Kemampuan Auditor Mendeteksi Fraud. Jurnal Akuntansi Dan Sistem Teknologi Informasi, 14(1), 146-160.

Kaminski, K. (. (2017). Dapatkah Rasio Keuangan Mendeteksi Kecurangan Laporan Keuangan ? . Kelola Audit Journal (19) 1. .

Lucas, S. G. (2022). Deteksi Anti Pencucian Uang Dan Penipuan Keuangan. Intellegent Systems in Accounting Finance & Management, 29 (3).

Maulidi. (2016). Dealing with Fraudulent Financial Statement in Business Organizations through Whistleblowing System and Staff Awareness of Fraud. ICAS. Malaysia: Universiti Utara Malaysia.

Moyes, G. D. (2006). Internal Auditors' Perceptions of the Effectiveness of Red Flags to Detect Fraudulent Financial Reporting. . Journal of Accounting, Ethics & Public Policy, 6(1)., http://ssrn.com/abstract=961457.

Oktaviany, F. (2023). Financial Statement Fraud: Pengujian Fraud Hexagon Dengan Moderasi Audit Committee. Jurnal Bisnis Dan Akuntansi, 25(1), 91-118.

Pourhabibi, T. D. (2020). Pendeteksian Fraud: Graph-Based Anomaly Detection (GBAD) Approaches. PulmX Metrics. Volume 133.

R, A. Y. (2021). Bagaimana Cara Mendeteksi Penipuan Layanan Kesehatan. Gac Sanit, 35(S2):S441-S449.

Romney, M. B. (2014). Sistem Informasi Akuntansi, Edisi ketigabelas, Diterjemahkan oleh : Kikin Sakinah, Nur Safira dan Novita Puspasari,. Jakarta: Penerbit Salemba Empat.

Siregar, S. V. (2015). Fraud Awareness Survey of Private Sector in Indonesia. . Journal of Financial Crime, 22(3), 329–346. https://doi.org/10.1108/JFC-03-2014-0016.

Skousen, J. C. (2008). Detecting and Predicting Financial Statement Fraud : The Effectiveness of The Fraud Triangle and SAS No. 99. . Jurnal dari http: //ssrn.com/abstract(diakses pada 10 Juni 2024).

Aguiar, L. U. (2021). Deteksi Fraud Menggunakan Fraud Triangle Theory dan Data Mining Techniques.Computers 10(10):20.

Turner, J. L. (2003). An Analysis of the Fraud Triangle. . In The University of Memphis, University of Southern California, University of Kansas.

Vousinas, G. (2019). Advancing theory of fraud: the S.C.O.R.E. model. Journal of Financial Crime 26(1). DOI:10.1108/JFC-12-2017-0128, 372-381.

Widiyati, D. ((2021, March).). Pengendalian Kecurangan Dan Pengembangan Etika Profesi Pada Industri Perbankan Di Indonesia. . In Conference on Economic and Business Innovation (CEBI), (hal. (pp. 1384-1394).).

Winatasari, Y. (2023). Fraud Hexagon Sebagai Pendeteksi Fraudulent Financial Statement. . Jurnal Akuntansi '45, 4(1), 116-122.