Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari,Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

Integrasi Fraud Pentagon COSO dan Teknologi Audit untuk Pencegahan Fraud: Kasus Wirecard & Jiwasraya

Ardiansyah[1)], Erol Y.A. Fabanyo[2)],Indri Widyasari[3)], Tikkos Sitanggang[4)]
[1,2,3,4]STIE YAI Jakarta, Indonesia
e-mail: [1]ardiansyah@iblam.ac.id,[2]eaf57398@gmail.com,[3]indri.widyasari02@gmail.com,[4]tikkos.cpa@gmail.com

Article Information	Submit: 12-12-2025	Revised: 20-01-2026	Accepted: 28-01-2026

Abstrak

Penelitian ini bertujuan mengintegrasikan model Fraud Pentagon dengan kerangka pengendalian internal COSO serta teknologi audit modern untuk memperkuat pencegahan fraud. Studi kasus komparatif dilakukan pada Wirecard (Jerman) dan Jiwasraya (Indonesia) menggunakan data sekunder dari laporan audit, dokumen regulator, dan literatur akademik. Analisis dilakukan melalui thematic coding yang memetakan lima elemen Fraud Pentagon (Pressure, Opportunity, Rationalization, Capability, Arrogance) ke titik lemah COSO (Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring). Temuan menunjukkan bahwa fraud dipicu oleh kombinasi tekanan dan kesempatan yang diperkuat oleh kapabilitas dan arogansi, sementara kegagalan kontrol berulang pada control environment, control activities, dan monitoring. Peran manajemen sebagai garis pertahanan utama dan auditor independen sebagai garis pertahanan kedua terbukti krusial, namun sering gagal ketika override kebijakan dan skeptisisme profesional lemah. Integrasi Continuous Auditing dan Explainable AI (XAI) direkomendasikan untuk pemantauan real-time dan transparansi deteksi anomali. Kesimpulan: sinergi Fraud Pentagon–COSO–ISA 240 yang didukung CA/XAI dapat mentransformasi pencegahan fraud dari pendekatan reaktif menjadi proaktif. Implikasi praktis meliputi penetapan konfirmasi kas independen lintas yurisdiksi, penguatan SoD/otorisasi berbasis risiko, serta adopsi continuous auditing untuk near real-time monitoring. Explainable AI (mis. SHAP/LIME) direkomendasikan untuk meningkatkan transparansi keputusan deteksi anomali dan akuntabilitas kepada TCWG. Bagi regulator, diperlukan standar verifikasi pihak ketiga dan perlindungan whistleblower untuk memutus opportunity yang persisten.
Kata kunci: Continuous Auditing, COSO, Explainable AI, Fraud Pentagon, Pencegahan Fraud

Abstract

This study aims to integrate the Fraud Pentagon model with the COSO internal control framework and modern audit technologies to strengthen fraud prevention. A comparative case study was conducted on Wirecard (Germany) and Jiwasraya (Indonesia) using secondary data from audit reports, regulatory documents, and academic literature. Analysis was performed through thematic coding that maps the five elements of the Fraud Pentagon (Pressure, Opportunity, Rationalization, Capability, Arrogance) to COSO control weaknesses (Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring). The findings indicate that fraud is triggered by a combination of pressure and opportunity, amplified by capability and arrogance, while control failures recurred within the control environment, control activities, and monitoring. The roles of management as the first line of defense and independent auditors as the second line proved crucial, yet they frequently fail when policy overrides occur and professional skepticism is weak. The integration of Continuous Auditing (CA) and Explainable AI (XAI) is recommended to enable real-time monitoring and transparency in anomaly detection. Conclusion: The synergy of Fraud Pentagon–COSO–ISA 240, supported by CA/XAI, can transform fraud prevention from a reactive to a proactive approach. Practical implications include mandating independent cash confirmations across jurisdictions, strengthening risk-based segregation of duties (SoD) and authorization controls, and adopting continuous auditing to enable near real-time monitoring. Explainable AI (e.g., SHAP/LIME) is recommended to enhance the transparency of anomaly-detection decisions and the accountability to those charged with governance (TCWG). For regulators, third-party verification standards and robust whistleblower protection are required to disrupt persistent opportunity structures.
Keywords: *Continuous Auditing, COSO, Explainable AI, Fraud Pentagon, Fraud Prevention*

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

PENDAHULUAN

Kecurangan (*fraud*) di sektor keuangan merupakan ancaman serius terhadap stabilitas ekonomi dan kepercayaan publik. *(Association of Certified Fraud Examiners, 2024)* memperkirakan bahwa organisasi kehilangan sekitar 5% dari pendapatan tahunan akibat fraud, dengan waktu median pendeteksian mencapai 12 bulan, yang menunjukkan tingginya persistensi kecurangan yang tidak terdeteksi. Seiring dengan meningkatnya digitalisasi dan integrasi global dalam proses bisnis, skema fraud menjadi semakin kompleks, sehingga menuntut sistem pengendalian internal yang adaptif serta praktik audit yang lebih responsif. Dampak fraud tidak terbatas pada kerugian finansial, tetapi juga merusak reputasi institusi, melemahkan kepercayaan investor, dan berpotensi berkembang menjadi risiko sistemik yang memengaruhi stabilitas ekonomi secara lebih luas (Organisation for Economic Co-operation & Development, 2024).

Kasus besar seperti Wirecard di Jerman dan Jiwasraya di Indonesia menunjukkan bahwa fraud berskala besar jarang disebabkan oleh perilaku individu semata, melainkan mencerminkan kelemahan struktural dalam tata kelola, pengendalian internal, dan pengawasan eksternal. Wirecard runtuh setelah terungkap adanya saldo kas fiktif sebesar €1,9 miliar, yang menyingkap kegagalan audit serta lemahnya penerapan skeptisisme profesional dalam konteks lintas yurisdiksi (Bloch et al., 2024; Heese & Schmid, 2021). Demikian pula, Jiwasraya mengalami kerugian sekitar Rp16,81 triliun akibat praktik investasi berisiko tinggi yang menyimpang dari prinsip kehati-hatian, diperparah oleh lemahnya aktivitas pengendalian dan pengawasan tata kelola (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Otoritas Jasa Keuangan Republik Indonesia, 2021). Meskipun berada dalam konteks regulasi dan institusional yang berbeda, kedua kasus tersebut memperlihatkan pola berulang, di mana fraud tidak hanya dipicu oleh tekanan dan kesempatan, tetapi juga diperkuat oleh kapabilitas manajerial dan budaya organisasi yang permisif, sehingga memungkinkan override pengendalian dan penundaan deteksi.

Model Fraud Triangle (Cressey, 1953) yang selama ini digunakan untuk menjelaskan perilaku fraud melalui elemen tekanan (pressure), kesempatan (opportunity), dan rasionalisasi (rationalization) dinilai tidak lagi memadai untuk menjelaskan skandal berskala besar. Perkembangan teori ke Fraud Diamond (Wolfe & Hermanson, 2004) menambahkan dimensi kapabilitas (capability), dan Fraud Pentagon (Burlacu et al., 2025; Crowe Horwath LLP, 2011) menambahkan arogansi (arrogance), yang relevan untuk kasus management override dan kolusi tingkat tinggi. Namun, literatur masih jarang mengintegrasikan Fraud Pentagon dengan kerangka pengendalian internal COSO (COSO & ACFE, 2023) dan standar audit ISA 240 (International Auditing & Board, 2024), serta mengkaji peran teknologi audit modern seperti continuous auditing dan Explainable AI (XAI) dalam memperkuat pencegahan fraud.

Temuan tambahan dari studi lintas yurisdiksi juga menegaskan bahwa Fraud Pentagon memiliki relevansi kuat dalam memetakan faktor risiko perilaku dan kelemahan kontrol internal yang diatur oleh kerangka COSO. Analisis empiris menunjukkan bahwa tekanan, kesempatan, kapabilitas, etika personal, serta rasionalisasi manajerial berinteraksi langsung dengan variabel efektivitas kontrol, terutama pada control activities dan monitoring. Hal ini memperkuat argumen bahwa integrasi Fraud Pentagon–COSO memberikan pendekatan yang lebih komprehensif untuk memprediksi dan mencegah fraud dalam organisasi sektor publik maupun privat (Vutumu et al., 2025).

Perkembangan teknologi audit seperti data analytics, machine learning, dan XAI menawarkan peluang untuk meningkatkan efektivitas deteksi fraud melalui pemantauan real-time dan transparansi pengambilan keputusan (Hernandez Aros & Perez, 2024). Konsep continuous auditing memungkinkan pengujian populasi transaksi dan pemantauan berkelanjutan, sehingga mengatasi keterbatasan audit periodik yang cenderung bersifat post-mortem (Elder & Allen, 2022; Eulerich et al., 2020). Namun, adopsi teknologi ini masih menghadapi tantangan, terutama dalam hal integrasi dengan prosedur audit tradisional dan penerimaan oleh auditor serta manajemen. Kontribusi teoritis: Secara teoretis, penelitian ini berkontribusi dalam memvalidasi relevansi Fraud Pentagon pada skandal berskala besar dan mengintegrasikan kerangka COSO serta ISA 240 dengan teknologi audit modern. Kontribusi praktis: Secara praktis, penelitian ini menawarkan rancangan kontrol berbasis teknologi yang dapat meningkatkan ketahanan sistem keuangan terhadap fraud.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain studi kasus komparatif. Dua kasus besar dipilih, yaitu Wirecard (Jerman) dan Jiwasraya (Indonesia), karena keduanya

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

merepresentasikan skandal fraud berskala besar dengan karakteristik berbeda (fintech vs asuransi) dan memiliki ketersediaan bukti publik yang memadai. Desain ini memungkinkan analisis mendalam atas dinamika fraud, kegagalan kontrol internal, dan peran manajemen serta auditor independen, sekaligus menilai relevansi Fraud Pentagon dalam konteks lintas yurisdiksi (Bloch et al., 2024; Teichmann et al., 2024). Pemilihan desain studi kasus komparatif juga didasarkan pada kebutuhan untuk menghubungkan teori dengan praktik, khususnya integrasi kerangka COSO dan standar audit ISA 240 dengan teknologi audit modern seperti continuous auditing dan Explainable AI (XAI). Pendekatan ini sejalan dengan tren penelitian terkini yang menekankan penggunaan analitik data dan machine learning untuk meningkatkan efektivitas pengawasan (Duan et al., 2025).

1. Unit Analisis

Unit analisis penelitian mencakup:

1. Entitas perusahaan (struktur bisnis, model pendapatan, eksposur risiko).
2. Sistem pengendalian internal berbasis COSO (control environment, risk assessment, control activities, information & communication, monitoring).
3. Peran aktor kunci manajemen (garis pertahanan utama) dan auditor independen (garis pertahanan kedua) dalam pencegahan dan deteksi fraud sesuai ISA 240 (International Auditing & Board, 2024).

2. Sumber Data

Penelitian memanfaatkan data sekunder yang diperoleh dari:

a. Laporan audit dan regulator: Laporan pemeriksaan BPK RI dan publikasi OJK untuk Jiwasraya; laporan investigasi dan literatur akademik terkait Wirecard (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Heese & Schmid, 2021; Otoritas Jasa Keuangan Republik Indonesia, 2021).
b. Dokumen hukum: Putusan pengadilan dan dokumen penyidikan yang mendokumentasikan bukti fraud dan kegagalan kontrol.
c. Laporan tahunan perusahaan: Informasi kebijakan kontrol, governance, dan kinerja keuangan.
d. Literatur akademik mutakhir: Kerangka COSO (COSO & ACFE, 2023), ISA 240 (International Auditing & Board, 2024), evolusi teori fraud (Burlacu et al., 2025; Cressey, 1953; Wolfe & Hermanson, 2004), serta teknologi audit modern (Duan et al., 2025; Hernandez Aros & Perez, 2024; Leocadio et al., 2024).

Studi ini tidak menggunakan data primer karena (i) fokus pada triangulasi dokumen resmi (laporan audit/regulator, putusan, annual report) lintas yurisdiksi; (ii) keterbatasan akses ledger/transaksi granular; dan (iii) pertimbangan etika serta reliabilitas jejak audit formal sebagai bukti. Pendekatan studi kasus komparatif berbasis dokumenter memungkinkan *thematic coding* yang dapat diuji silang dan diaudit (audit trail)

3. Teknik Analisis Data

Analisis dilakukan dengan thematic coding menggunakan skema a priori yang diturunkan dari Fraud Pentagon {Pressure, Opportunity, Rationalization, Capability, Arrogance} dan dipetakan ke komponen COSO untuk menilai titik kegagalan kontrol. Prosedur analitik meliputi:

1. Identifikasi tema dari dokumen resmi, laporan audit/regulator, dan literatur.
2. Koding tematik yang menautkan setiap bukti ke elemen Fraud Pentagon dan komponen COSO.
3. Pemetaan bukti ke peran manajemen dan auditor independen dalam konteks ISA 240 (skeptisisme profesional, bukti independen, uji populasi).
4. Sintesis komparatif (Wirecard vs Jiwasraya) untuk menemukan pola berulang dan perbedaan kontekstual.

Pendekatan ini diperkuat dengan integrasi analitik berbasis teknologi untuk mendukung validitas interpretasi. Studi oleh (Duan et al., 2025) menunjukkan bahwa penggunaan process mining

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

dan machine learning dalam audit internal dapat meningkatkan efektivitas evaluasi kontrol dan mempercepat deteksi fraud. Meskipun penelitian ini tidak mengimplementasikan algoritma secara langsung, kerangka analitik tersebut menjadi referensi untuk mengkaji potensi integrasi teknologi audit dalam pencegahan fraud.

4. Validitas dan Keandalan

Untuk menjaga trustworthiness, diterapkan:

a. Triangulasi sumber: Membandingkan temuan dari laporan audit, dokumen regulator/hukum, laporan tahunan, dan literatur akademik (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Bloch et al., 2024).
b. Audit trail: Pencatatan jejak analisis (daftar dokumen, tanggal akses, keputusan koding) yang transparan dan dapat diaudit.
c. Peer debriefing: Diskusi interpretasi dengan praktisi audit/tata kelola untuk meminimalkan bias.
d. Negative case analysis: Pengujian temuan terhadap bukti yang berlawanan untuk mengonfirmasi konsistensi atau merevisi pemaknaan (Elder & Allen, 2022; Eulerich et al., 2020).

5. Keterbatasan Penelitian

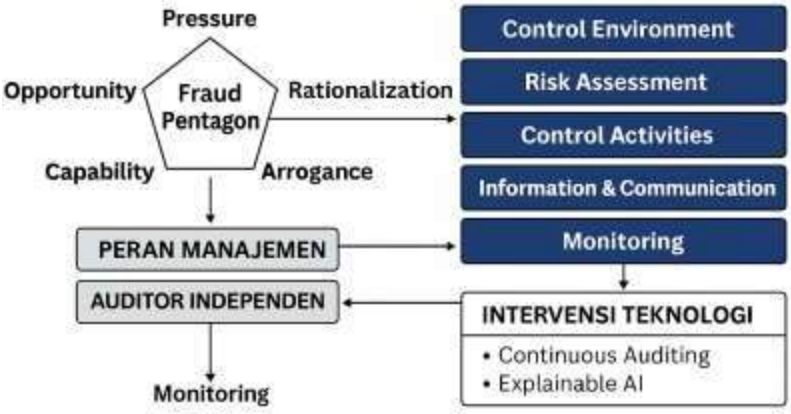
Penelitian tidak mengakses data transaksi granular/ledger dan tidak melakukan observasi lapangan langsung; karena itu, temuan bersifat generalisasi analitik yang ditopang bukti dokumenter, bukan inferensi statistik populasi. Selain itu, bias publikasi (fokus pada kasus besar yang terdokumentasi baik) mungkin memengaruhi generalisasi ke kasus berukuran kecil/menengah (International Auditing & Board, 2024; Otoritas Jasa Keuangan Republik Indonesia, 2021).

6. Kerangka Konseptual

Kerangka konseptual penelitian ini memodelkan hubungan antara faktor pendorong fraud yang dijelaskan oleh Fraud Pentagon (Pressure, Opportunity, Rationalization, Capability, Arrogance) dengan kegagalan kontrol internal yang diatur dalam kerangka COSO. Elemen Fraud Pentagon berperan sebagai pemicu fraud, sedangkan kelemahan pada komponen COSO (Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring) menjadi jalur yang memungkinkan fraud terjadi. Peran Manajemen ditempatkan sebagai garis pertahanan utama untuk menciptakan lingkungan pengendalian yang sehat, sedangkan Auditor Independen berfungsi sebagai garis pertahanan kedua untuk mendeteksi salah saji material akibat fraud sesuai ISA 240. Ketika kedua peran ini gagal, risiko fraud meningkat secara signifikan.

Sebagai intervensi, teknologi audit modern seperti Continuous Auditing dan Explainable AI (XAI) diintegrasikan untuk memperkuat pengawasan dan transparansi. Continuous Auditing memungkinkan pemantauan real-time atas transaksi, sedangkan XAI memberikan penjelasan yang dapat dipahami atas hasil deteksi anomali, sehingga meningkatkan kepercayaan dan akuntabilitas.

Gambar 1. Kerangka Konsepsional Pencegahan Fraud



DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

Penjelasan Gambar:

a. Fraud Pentagon: Lima elemen (Pressure, Opportunity, Rationalization, Capability, Arrogance) sebagai faktor pendorong fraud.
b. Peran Manajemen (Garis Pertahanan Utama): Mengelola *tone at the top*, budaya etika, dan pengendalian internal.
c. Auditor Independen (Garis Pertahanan Kedua): Menegakkan skeptisisme profesional, melakukan konfirmasi independen, dan pengujian populasi transaksi.
d. Komponen COSO: Lima pilar pengendalian internal yang harus diperkuat untuk menutup celah fraud.
e. Intervensi Teknologi: Continuous Auditing dan XAI sebagai penguat monitoring dan transparansi pengambilan keputusan.

HASIL PENELITIAN DAN PEMBAHASAN

Temuan Kasus Wirecard (Jerman, 2019–2020)

Analisis dokumen akademik dan regulasi menunjukkan bahwa skandal Wirecard dibangun oleh kombinasi elemen Fraud Pentagon yang saling menguatkan. Tekanan (pressure) berasal dari ekspektasi pasar DAX terhadap pertumbuhan agresif, yang membentuk narasi ekspansi global dan kinerja superior sebagai *tone* komunikasi eksternal (Bloch et al., 2024; Heese & Schmid, 2021). Dorongan untuk "memenuhi pasar" ini menempatkan manajemen pada jalur penetapan target yang tidak realistis dan mendorong penggunaan taktik pelaporan yang oportunistik.

Kesempatan (opportunity) terbuka luas melalui kelemahan control activities terkait konfirmasi kas pada rekening *trust* lintas yurisdiksi yang kemudian terbukti tidak benar sebesar ±€1,9 miliar serta ketergantungan pada pihak ketiga yang tidak diaudit memadai; (Teichmann et al., 2024). Lemahnya verifikasi independen atas saldo kas dan prosedur *bank confirmation* lintas negara menciptakan celah yang sulit ditutup oleh audit tradisional yang dominan berbasis sampling, alih-alih uji populasi transaksi (International Auditing & Board, 2024).

Rasionalisasi (rationalization) tampak pada normalisasi kompleksitas lintas yurisdiksi sebagai alasan penundaan atau pengaburan anomali, misalnya dengan menyebut perbedaan rezim hukum/perbankan sebagai kendala *timing* dan akses bukti (Zimmermann, 2020). Rasionalisasi ini memperpanjang toleransi terhadap deviasi bukti, mengurangi urgensi korektif auditor/manajemen atas *red flags*.

Kapabilitas (capability) manajemen dalam menguasai struktur opak dan akses ke sistem pelaporan ditambah kemampuan mengelola jejak dokumenter lintas entitas memungkinkan rekayasa berulang yang sulit ditangkap oleh monitoring periodik (Bloch et al., 2024). Arogansi (arrogance) termanifestasi pada persepsi kebal terhadap kontrol dan keyakinan bahwa struktur organisasi/perantara dapat "mengakomodasi" narasi kinerja tanpa deteksi cepat (Teichmann et al., 2024).

Temuan Kasus Jiwasraya (Indonesia, 2008–2020)

Pada Jiwasraya, tekanan (pressure) berakar pada likuiditas dan komitmen imbal hasil tinggi kepada nasabah, yang mendorong keputusan investasi berisiko di luar profil risiko portofolio (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Otoritas Jasa Keuangan Republik Indonesia, 2021). Dorongan untuk memenuhi janji imbal hasil secara jangka pendek menempatkan manajemen pada pilihan strategi yang tidak sejalan dengan prinsip kehati-hatian (*prudential principle*). Kesempatan (opportunity) muncul dari lemahnya segregation of duties (SoD), batas/otorisasi investasi yang tidak ketat, serta monitoring portofolio yang tidak *near real-time*. Kelemahan ini mengakibatkan proses investasi berjalan dengan akses yang terlalu terkonsentrasi, sehingga pembatasan risiko (limit, *stop-loss*, atau *early warning*) tidak diaktifkan secara efektif ketika terjadi deviasi

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

(Sahrul & Lie, 2024)

Rasionalisasi (rationalization) muncul melalui normalisasi imbal hasil tinggi sebagai "wajar" di tengah pasar yang volatil, sehingga penyimpangan performa dianggap dapat "ditutup" oleh momentum pasar di periode berikutnya (Sahrul & Lie, 2024). Rasionalisasi seperti ini menunda pengakuan kerugian dan memperkuat keberlanjutan strategi berisiko. Kapabilitas (capability) ditunjukkan oleh kemampuan pelaku mengeksploitasi celah proses dan jaringan pihak terkait dalam siklus investasi, sedangkan arogansi (arrogance) tampak pada override kebijakan dan pelanggaran prinsip Good Corporate Governance (GCG) saat keputusan tidak diawasi secara ketat oleh komite audit/board ((Badan Pemeriksa Keuangan Republik Indonesia, 2020; Otoritas Jasa Keuangan Republik Indonesia, 2021).

Komparasi dan Pola Berulang

Komparasi kedua kasus memperlihatkan pola berulang yang konsisten: kombinasi pressure dan opportunity yang diperkuat oleh capability dan arrogance di lingkungan kontrol yang lemah. Pada Wirecard, titik lemah paling kritis berada pada konfirmasi kas lintas yurisdiksi dan ketergantungan pihak ketiga; pada Jiwasraya, titik lemah berpusat pada SoD/limit investasi dan monitoring portofolio (Bloch et al., 2024; BPK RI, 2020). Dalam kedua konteks, rasionalisasi (kompleksitas global atau wajar-nya imbal hasil tinggi) berfungsi sebagai "perekat psikologis" yang menunda tindakan korektif dan mengurangi urgensi auditor/manajemen untuk menutup celah kontrol (Sahrul & Lie, 2024; Zimmermann, 2020)

Tabel 1. Komparasi Elemen Fraud Pentagon: Wirecard vs Jiwasraya

Elemen Fraud Pentagon	Wirecard (Jerman)	Jiwasraya (Indonesia)
Pressure	Ekspektasi pasar DAX atas pertumbuhan agresif; narasi ekspansi global.	Tekanan likuiditas & komitmen imbal hasil tinggi kepada nasabah.
Opportunity	Konfirmasi kas pada *trust accounts* lemah; ketergantungan pihak ketiga tidak diaudit.	SoD lemah; limit/otorisasi investasi tidak ketat; monitoring portofolio lambat.
Rationalization	Normalisasi "kompleksitas global" untuk menunda klarifikasi anomali.	Normalisasi imbal hasil tinggi sebagai wajar meski tidak berkelanjutan.
Capability	Akses superuser & struktur opak memungkinkan rekayasa berulang.	Eksploitasi celah proses & jaringan pihak terkait dalam siklus investasi.
Arrogance	*Tone at the top* permisif; keyakinan kebal terhadap kontrol.	Override kebijakan; pelanggaran GCG; pengabaian prinsip kehati-hatian.

Sumber: Disusun dari (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Bloch et al., 2024; Heese & Schmid, 2021; Otoritas Jasa Keuangan Republik Indonesia, 2021; Teichmann et al., 2024)

Dari sudut pandang COSO, kegagalan control environment dan monitoring adalah pembuka jalan bagi control activities yang tidak efektif. Ketika tone at the top permisif dan pemantauan tidak berkelanjutan, maka limit, otorisasi, dan konfirmasi pihak ketiga menjadi paper controls yang mudah di-override (COSO & ACFE, 2023; Tricker, 2019). Keterkaitan ini menguatkan argumentasi bahwa Fraud Pentagon lebih kompatibel dibanding Fraud Triangle/Diamond dalam menjelaskan durasi dan intensitas fraud pada skandal besar(Burlacu et al., 2025).

Tabel 2. Pemetaan Kegagalan Kontrol → Komponen COSO

Komponen COSO	Wirecard (Jerman)	Jiwasraya (Indonesia)
Control Environment	Budaya skeptisisme rendah; *tone at the top* permisif.	Tone at the top lemah; budaya etika tidak menahan override.
Risk Assessment	Penilaian risiko pihak ketiga/trust accounts	Penilaian risiko produk/portofolio tidak

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

	tidakmemadai.	memadai; risk appetite tidak jelas.
Control Activities	Konfirmasi kas tidak independen; prosedur pihakketiga tidak diuji memadai.	Limit/otorisasi investasi lemah; SoD tidak efektif.
Information & Communication	Transparansi bukti audit rendah; pelaporan tidakmengurai anomali lintas entitas.	Informasi risiko tidak mengalir efektif ke komite audit/board.
Monitoring	Audit internal/eksternal gagal mendeteksi red flags tepat waktu.	Monitoring portofolio tidak kontinu; early warning tidak aktif.

Sumber: Disusun dari (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Bloch et al., 2024; Heese & Schmid, 2021; Otoritas Jasa Keuangan Republik Indonesia, 2021; Teichmann et al., 2024).

Kondisi audit turut mempengaruhi persistensi fraud: pada Wirecard, prosedur audit kurang menekankan bukti independen atas saldo kas dan uji populasi transaksi; pada Jiwasraya, skeptisisme profesional atas keberlanjutan imbal hasil dan konsistensi dengan risk appetite tidak memadai (Heese & Schmid, 2021; International Auditing & Board, 2024). Secara faktual, hal ini menjelaskan mengapa indikator awal (*red flags*) tidak segera berujung pada remediasi yang efektif di level organisasi maupun auditor (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Otoritas Jasa Keuangan Republik Indonesia, 2021).

Indikasi Efektivitas Intervensi Teknologi

Literatur mutakhir memberikan indikasi kuat bahwa continuous auditing (CA) dan Explainable AI (XAI) dapat memperkuat pencegahan fraud. Continuous auditing memungkinkan pemantauan real-time dan pengujian populasi transaksi, sehingga mempercepat deteksi anomali dan menutup ruang *opportunity* (Elder & Allen, 2022; Eulerich et al., 2020). Dalam konteks Wirecard, CA dengan konfirmasi kas otomatis lintas yurisdiksi dapat mengurangi risiko trust accounts fiktif; pada Jiwasraya, CA dapat mengaktifkan sistem peringatan dini untuk portofolio berisiko (COSO & ACFE, 2023). Perkembangan terbaru mengenai implementasi continuous auditing menunjukkan bahwa organisasi di sektor publik maupun lembaga keuangan semakin mengadopsi pendekatan pemantauan berkelanjutan untuk memperkuat tata kelola dan mendeteksi anomali secara real-time. Studi terbaru menyoroti bahwa CA menghadapi tantangan implementasi, seperti kesiapan teknologi, rigiditas organisasi, serta kebutuhan peningkatan kompetensi auditor internal. Namun demikian, CA terbukti memberikan kemampuan monitoring yang lebih adaptif, memungkinkan auditor untuk menilai risiko dan efektivitas kontrol secara lebih akurat (Minkkinen et al., 2022; Polizzi & Scannella, 2023).

Perkembangan teknologi audit menunjukkan bahwa integrasi Explainable AI (XAI) semakin dipandang sebagai langkah esensial dalam meningkatkan transparansi model deteksi anomali. XAI memungkinkan auditor memahami dasar keputusan model AI melalui penjelasan yang terstruktur dan dapat diaudit, sehingga meningkatkan kepercayaan serta akuntabilitas dalam proses audit berbasis data. Studi terbaru memperlihatkan bahwa XAI tidak hanya meningkatkan kualitas penilaian risiko, tetapi juga mengurangi potensi bias algoritmik melalui pelacakan logika prediksi model (Kokina & Davenport, 2017; Leocadio et al., 2024; Zhong & Goel, 2024). XAI, melalui metode seperti SHAP dan LIME, memberikan penjelasan transparan atas hasil deteksi anomali, meningkatkan akuntabilitas dan kepercayaan pemangku kepentingan (Hernandez Aros & Perez, 2024; Leocadio et al., 2024). Studi oleh (Duan et al., 2025) menunjukkan bahwa integrasi machine learning dan process mining dalam audit internal mempercepat evaluasi kontrol dan mendukung pengambilan keputusan berbasis data. Dengan demikian, CA dan XAI bukan sekadar pelengkap, tetapi menjadi prasyarat untuk skeptisisme profesional yang efektif di era digital.

PEMBAHASAN

Teori vs Bukti: Mengapa Fraud Pentagon Lebih Memadai dibanding Triangle/Diamond

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

Temuan empiris pada Wirecard dan Jiwasraya menunjukkan bahwa dinamika fraud berskala besar tidak dapat dijelaskan secara memadai hanya dengan tekanan, kesempatan, dan rasionalisasi; kapabilitas pelaku dan arogansi manajerial bertindak sebagai penguat yang memungkinkan *override* pengendalian dan memperpanjang durasi fraud (Bloch et al., 2024; Heese & Schmid, 2021; Teichmann et al., 2024). Hal ini konsisten dengan perluasan kerangka dari Triangle/Diamond ke Fraud Pentagon yang menambahkan dimensi capability dan arrogance, sehingga lebih komprehensif untuk menjelaskan skandal besar lintas yurisdiksi dan kolusi tingkat manajemen (Burlacu et al., 2025; Crowe Horwath LLP, 2011).

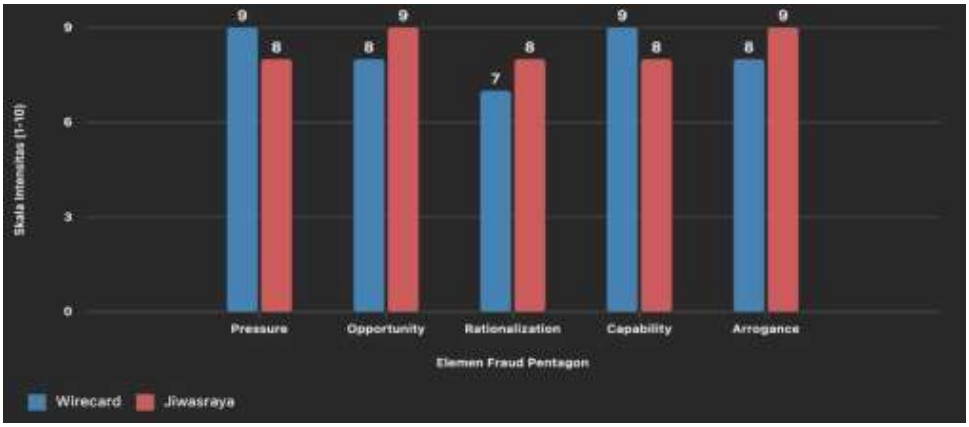
Tabel 3. Perbandingan Model Fraud dan Studi Kasus

Model	Elemen Utama	Kelebihan	Kelemahan	Contoh Studi Kasus
Fraud Triangle	Pressure, Opportunity, Rationalization	Sederhana, mudah dipahami, banyak dipakai	Tidak mempertimbangkan kapabilitas & perilaku manajerial	Penggelapan kas karyawan (petty cash)
Fraud Diamond	+ Capability	Menangkap kemampuan pelaku mengeksploitasi celah	Masih mengabaikan arogansi manajemen	Enron (AS): kapabilitas manajemen manipulasi laporan
Fraud Pentagon	+ Arrogance	Komprehensif untuk management override & kolusi	Analisis lebih kompleks (budaya organisasi)	Wirecard & Jiwasraya

Sumber: Disusun dari (Bloch et al., 2024; Burlacu et al., 2025; Cressey, 1953; Crowe Horwath LLP, 2011; Teichmann et al., 2024; Wolfe & Hermanson, 2004)

Keterkaitan ini juga terlihat pada visualisasi komparatif intensitas elemen Pentagon yang memperlihatkan dominasi opportunity dan arrogance pada Jiwasraya, sedangkan capability dan pressure lebih menonjol pada Wirecard. Grafik tersebut mempertegas bahwa meskipun kedua kasus sama-sama didorong kombinasi lima elemen, profil dominan elemen berbeda membentuk jalur risiko yang spesifik per konteks industri

Gambar 2. Grafik Perbandingan Intensitas Elemen Fraud Pentagon Antara Wirecard Dan Jiwasraya



Sumber: Disusun dari (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Bloch et al., 2024; Heese & Schmid, 2021; Otoritas Jasa Keuangan Republik Indonesia, 2021; Teichmann et al., 2024).

Penjelasan Grafik

a. Sumbu X: Lima elemen Fraud Pentagon (Pressure, Opportunity, Rationalization, Capability, Arrogance).
b. Sumbu Y: Skala intensitas (1–10) berdasarkan analisis naratif.
c. Warna biru (Wirecard): Tekanan pasar DAX dan kapabilitas teknis sangat tinggi; kelemahan konfirmasi kas signifikan.

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

d. Warna merah (Jiwasraya): Kesempatan investasi dan override kebijakan lebih dominan; arogansi manajemen sangat kuat.

Interpretasi:

a. Kedua kasus menunjukkan skor tinggi pada Pressure dan Opportunity, tetapi Jiwasraya lebih ekstrem pada Opportunity (SoD lemah, limit investasi longgar), sedangkan Wirecard unggul pada Capability (struktur opak, akses sistem).
b. Arrogance tinggi di kedua kasus, menandakan *tone at the top* permisif dan override kebijakan sebagai penguat fraud.

Peran Manajemen sebagai *First Line of Defense*

Secara teoritis dan normatif, manajemen memikul kewajiban membentuk control environment yang kuat melalui tone at the top, integritas, serta disiplin kebijakan yang meresap ke risk assessment dan control activities. Bukti kasus memperlihatkan bahwa di Wirecard, target pertumbuhan non-realistis dan normalisasi kompleksitas lintas yurisdiksi memfasilitasi *override* atas prosedur konfirmasi kas; di Jiwasraya, lemahnya SoD, otorisasi investasi, dan budaya etika memicu kerentanan sistemik (Badan Pemeriksa Keuangan Republik Indonesia, 2020; Bloch et al., 2024; Otoritas Jasa Keuangan Republik Indonesia, 2021). (COSO & ACFE, 2023) menegaskan pentingnya mengintegrasikan program manajemen risiko fraud dengan kerangka kontrol internal dan kanal pelaporan risiko yang jelas, termasuk perlindungan *whistleblower*. Dengan demikian, komitmen manajemen terhadap tata kelola harus terlihat dalam praktik kontrol yang teruji, bukan sebatas pernyataan kebijakan.

Peran Auditor Independen sebagai *Second Line of Defense*

Dalam konteks ISA 240, auditor independen berkewajiban menegakkan skeptisisme profesional dan merancang prosedur respons atas risiko salah saji material akibat fraud. Bukti kasus menunjukkan kegagalan auditor menangkap *red flags* ketika verifikasi kas bergantung pada representasi manajemen (Wirecard) atau ketika keberlanjutan imbal hasil tidak dinilai memadai (Jiwasraya) (Heese & Schmid, 2021; Teichmann et al., 2024). Exposure Draft ISA 240 memperkuat ekspektasi atas independent confirmations, population testing pada area berisiko tinggi, serta transparansi komunikasi dengan *those charged with governance* (International Auditing & Board, 2024) Penerapan prosedur ini krusial untuk memutus opportunity yang bertahan karena capability pelaku.

Integrasi Teknologi Audit: Continuous Auditing dan Explainable AI

Literatur dan indikasi empiris menunjukkan continuous auditing (CA) dan explainable AI (XAI) berpotensi mengatasi keterbatasan audit periodik dan pengendalian manual. CA memungkinkan pemantauan berkelanjutan dengan cakupan populasi transaksi, mempercepat deteksi anomali dan penutupan celah *opportunity* (Elder & Allen, 2022; Eulerich et al., 2020). XAI (mis. SHAP/LIME) meningkatkan transparansi keputusan deteksi dan akuntabilitas kepada *those charged with governance*, sehingga memperkuat skeptisisme profesional di lingkungan digital (Hernandez Aros & Perez, 2024; Leocadio et al., 2024). Bukti tambahan menunjukkan integrasi process mining + ML/XAI mendukung evaluasi kontrol berbasis data dan pengungkapan pola risiko yang sebelumnya tersembunyi (Awasthi, 2025; Duan et al., 2025; Koppireddy & Devi, 2025).

Pembaruan Kerangka dan Regulasi: Menjembatani Teori–Praktik

Perkembangan IAASB (International Auditing & Board, 2024) mempertegas lensa fraud dalam identifikasi risiko, respons audit, dan transparansi pelaporan; ringkasan industri menyoroti perubahan pada dokumentasi, komunikasi, dan prosedur atas area berisiko tinggi. Di sisi kontrol, COSO 2023 melalui FRMG menautkan ICIF 2013 dan ERM 2017 dengan kebutuhan monitoring

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

berbasis analytics. Kombinasi pembaruan kerangka audit-kontrol dengan implementasi CA/XAI menghadirkan jalur translasional dari konsep ke praktik (COSO & ACFE, 2023; International Auditing & Board, 2024).

Sintesis: Dari Pola Berulang ke Agenda Aksi

Sintesis pembahasan mengerucut pada tiga pilar aksi: (i) Manajemen berintegritas yang menegakkan *tone at the top*, memperjelas risk appetite, memperketat SoD/otorisasi dan kanal pelaporan risiko; (ii) Auditor berbasis data yang menegakkan skeptisisme profesional melalui independent confirmations, population testing, dan multi-source corroboration; (iii) Teknologi yang transparan CA/XAI untuk near real-time monitoring, penjelasan keputusan model, dan audit trail yang dapat diaudit. Prioritas implementasi diarahkan ke area paling rawan: trust accounts/pihak ketiga (Wirecard) dan portofolio investasi/SoD (Jiwasraya) (COSO & ACFE, 2023; International Auditing & Board, 2024).

Tabel 4. Matriks Analisis Perbandingan: Dimensi *Fraud Pentagon* → Bukti Kasus → Implikasi Audit (ISA 240) & Kontrol (COSO)

Dimensi	Wirecard (Bukti Utama)	Jiwasraya (Bukti Utama)	Interpretasi Teoretis (Pentagon)	Implikasi Audit (ISA 240)	Implikasi Kontrol (COSO)
Pressure	Target pertumbuhan & narasi ekspansi agresif	Likuiditas ketat & komitmen imbal hasil tinggi	Pressure mempercepat taktik oportunistik; durasi dijelaskan oleh capability/arrogance	*Risk brainstorming* atas asumsi kinerja/imbal hasil; uji sensitivitas; pelaporan ke TCWG	Perkuat risk assessment & *board challenge*; selaraskan risk appetite
Opportunity	Konfirmasi kas *trust accounts* lemah; pihak ketiga tidak diaudit	SoD lemah; limit/otorisasi tidak ketat; monitoring lambat	Opportunity bertahan karena capability pelaku mengakali jalur proses/bukti	Independent confirmations Lintas yurisdiksi; population testing; audit komponen pihak ketiga	Ketatkan control activities & aktifkan monitoring near real-time
Rationalization	Normalisasi "kompleksitas global"	Normalisasi "imbal hasil tinggi"	Rasionalisasi menopang delay koreksi; memperkuat arrogance	Challenge narratives dengan data independen; dokumentasi alasan kebijakan	Tingkatkan information & communication; jalur eskalasi & *whistleblower*
Capability	Akses superuser & struktur opak	Eksploitasi celah proses & jaringan	Capability memanjangkan fraud melalui akses/keahlian	Uji akses sistem/log activity; analitik process mining + ML	Terapkan least-privilege; SoD berbasis risiko; *audit trail* terukur
Arrogance	*Tone at the top* permisif	Override kebijakan; pelanggaran GCG	Arrogance menundukkan *paper controls*	Observasi tone/board minutes; gunakan XAI (SHAP/LIME) untuk transparansi temuan	Perkuat control environment; KPI etika; proteksi whistleblower

Sumber: Tabel disusun dari sumber primer & sekunder: (Awasthi, 2025; Badan Pemeriksa Keuangan Republik Indonesia, 2020; Bloch et al., 2024; Burlacu et al., 2025; COSO & ACFE, 2023; Duan et al., 2025; Heese & Schmid, 2021; International Auditing & Board, 2024; Koppireddy & Devi, 2025; Teichmann et al., 2024; Zimmermann, 2020)

Implikasi Praktik dan Kebijakan

Implikasi praktik: (i) menetapkan konfirmasi kas independen lintas yurisdiksi pada entitas dengan trust accounts atau ketergantungan pihak ketiga; (ii) memperkuat SoD/otorisasi berbasis

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Jurnal Manajemen, Akuntansi, Ekonomi
Vol. 4 No. 3 Tahun 2026
e:ISSN: 2828-7770, p-ISSN: 2985-573x, Hal 1048-1061
Ardiansyah, Erol Y.A. Fabanyo, Indri Widyasari, Tikkos Sitanggang
Available Online at: https://jurnal.erapublikasi.id/index.php/JMAE/index

risiko dan kontrol akses least-privilege; (iii) mengadopsi CA untuk pelaporan risiko berkelanjutan; dan (iv) menerapkan dashboard XAI (SHAP/LIME) agar alasan *flagging* dapat diaudit. Implikasi kebijakan: regulator mendorong standar konfirmasi kas lintas yurisdiksi, audit komponen pihak ketiga, dan perlindungan whistleblower serta mempercepat adopsi analytics/XAI di sektor keuangan (COSO & ACFE, 2023; International Auditing & Board, 2024).

Pembahasan ini mengonfirmasi jalur teori → bukti → aksi: Fraud Pentagon menjelaskan perilaku kunci (pressure–opportunity–rationalization–capability–arrogance), COSO memetakan titik lemah kontrol, ISA 240 menuntun respons audit yang tepat, dan CA/XAI menyediakan mekanisme implementasi yang efektif serta dapat diaudit. Integrasi keempat komponen tersebut mentransformasikan organisasi dari compliance oriented menjadi resilience oriented, menutup ruang opportunity, menahan dampak capability/arrogance, dan membangun kembali trust atas keputusan audit berbasis data (Awasthi, 2025; COSO & ACFE, 2023; International Auditing & Board, 2024; Koppireddy & Devi, 2025).

KESIMPULAN

Penelitian ini menegaskan bahwa Fraud Pentagon merupakan kerangka yang paling memadai untuk menjelaskan skandal berskala besar melampaui ketercukupan model klasik (Fraud Triangle/Diamond) karena dua dimensi penguat (capability dan arrogance) secara nyata memperpanjang durasi fraud dan menekan efektivitas kontrol formal. Bukti komparatif pada Wirecard dan Jiwasraya menunjukkan pola berulang: kombinasi pressure–opportunity yang disangga oleh rationalization, lalu diperkuat oleh capability (akses/keahlian atas proses dan sistem) serta arrogance (tone at the top permisif, override kebijakan). Pola ini berpeta langsung ke titik lemah COSO, terutama control environment, control activities, dan monitoring, serta diperburuk oleh penerapan ISA 240 yang tidak optimal (skeptisisme profesional lemah, bukti independen tidak memadai, pengujian berbasis sampel alih-alih populasi).

Dari sisi governance & assurance, penelitian ini menyimpulkan tiga pilar pertahanan yang saling menguatkan:

1. Manajemen berintegritas (garis pertahanan utama): membangun control environment yang tegas melalui *tone at the top*, memperjelas risk appetite, memperketat segregation of duties/otorisasi berbasis risiko, dan memastikan information & communication mengalir efektif ke komite audit/board. Tanpa komitmen manajerial yang terwujud dalam praktik kontrol dan bukti proses, *paper controls* akan selalu mudah di-*override*.
2. Auditor independen berbasis data (garis pertahanan kedua): menegakkan skeptisisme profesional sesuai ISA 240 melalui independent confirmations (lintas yurisdiksi/pihak ketiga), population testing pada area akses kritikal, multi-source corroboration atas narasi manajemen, serta komunikasi transparan kepada *those charged with governance*. Ini adalah syarat minimum untuk memutus *opportunity* yang bertahan karena capability pelaku.
3. Teknologi audit yang transparan: continuous auditing (CA) dan Explainable AI (XAI) harus diadopsi sebagai standar operasional. CA menggeser audit dari *point-in-time* menjadi monitoring berkelanjutan dengan cakupan populasi transaksi dan ambang deteksi adaptif; XAI (mis. SHAP/LIME) men-*decodify* alasan *flagging* sehingga temuan berbasis ML dapat diaudit dan dipercaya. CA + XAI adalah pasangan komplementer: yang satu memperluas dan memperkaya bukti, yang lain menjelaskan pengambilan keputusan model bersama-sama menutup celah opportunity, mengekang efek capability/arrogance, dan memulihkan trust pemangku kepentingan.

Kontribusi penelitian: (i) Teoretis menguatkan operasionalisasi Fraud Pentagon lintas yurisdiksi dan memetakan langsung ke komponen COSO; (ii) Metodologis menawarkan kerangka analitik tematik yang dapat diintegrasikan dengan process mining/ML/XAI; (iii) Praktis menyediakan agenda aksi yang dapat ditranslasikan ke kebijakan internal (konfirmasi kas

DOI: https://doi.org/10.59066/jmae.v4i3.2014

independen, audit pihak ketiga, SoD/otorisasi berbasis risiko) dan eksternal (standar verifikasi lintas yurisdiksi, perlindungan *whistleblower*, dorongan *disclosure* yang lebih sering). Keterbatasan: penggunaan data sekunder dan ketiadaan akses ledger/transaksi granular membuat temuan bersifat generalisasi analitik, bukan inferensi statistik populasi. Namun, triangulasi sumber, *audit trail* analisis, dan rujukan empiris mutakhir (CA/XAI) memberikan keandalan yang memadai untuk menyusun rekomendasi implementasi.

Refleksi strategis: bergerak dari compliance-oriented menuju resilience-oriented. Dengan menempatkan Manajemen berintegritas, Auditor independen berbasis data, dan Teknologi audit yang transparan (CA/XAI) sebagai pertahanan berlapis, organisasi akan mampu menutup ruang *opportunity*, mengendalikan dampak capability/arrogance, serta membuktikan akuntabilitas keputusan pengawasan berbasis data. Ini bukan sekadar peningkatan proses; ini adalah pergeseran paradigma yang menempatkan kepercayaan (trust) sebagai keluaran utama tata kelola dan pada akhirnya, ketahanan anti-fraud sebagai standar baru operasi di sektor keuangan.

SARAN

a. Untuk Organisasi: Organisasi perlu mengembangkan risk profiling berbasis Fraud Pentagon agar penilaian risiko tidak hanya mencakup tekanan (*pressure*) dan kesempatan (*opportunity*), tetapi juga indikator perilaku seperti capability (akses istimewa) dan arrogance (override kebijakan). Profil risiko ini harus diintegrasikan dengan penguatan kerangka COSO, khususnya pada control activities dan monitoring. Implementasi konfirmasi kas independen lintas yurisdiksi, penguatan segregation of duties (SoD), serta pemantauan berkelanjutan (*continuous monitoring*) menjadi prioritas untuk menutup ruang *opportunity* yang berulang.
b. Untuk Manajemen: Manajemen sebagai garis pertahanan utama harus menegakkan tone at the top yang konsisten dengan nilai integritas dan tata kelola. Hal ini dapat diwujudkan melalui KPI etika yang terukur, pelatihan tata kelola berkala, dan mekanisme eskalasi risiko yang transparan. Program governance refresh perlu dilakukan untuk memastikan kebijakan pengendalian internal tidak hanya bersifat formal, tetapi juga efektif dalam praktik. Komitmen ini harus tercermin dalam penguatan risk appetite dan pengawasan aktif terhadap area berisiko tinggi.
c. Untuk Auditor Independen: Auditor perlu memperluas skeptisisme profesional sesuai pedoman ISA 240 dengan mengadopsi prosedur berbasis data. Langkah ini mencakup konfirmasi independen atas saldo kas dan aset pihak ketiga, uji populasi transaksi pada area kritikal, serta evaluasi indikator budaya organisasi (misalnya pola override dan respons terhadap red flags). Penggunaan analitik data dan Explainable AI (XAI) harus menjadi bagian dari metodologi audit untuk meningkatkan akurasi dan transparansi temuan.
d. Untuk Regulator: Regulator perlu menetapkan standar wajib untuk konfirmasi kas lintas yurisdiksi, memperkuat prosedur audit pihak ketiga, dan mendorong disclosure yang lebih sering bagi entitas berisiko tinggi. Selain itu, kebijakan perlindungan whistleblower harus diperkuat agar jalur pelaporan risiko berjalan efektif. Regulasi juga perlu mengakomodasi penggunaan teknologi audit seperti continuous auditing dan XAI sebagai bagian dari praktik pengawasan yang diakui.
e. Untuk Penelitian Lanjutan: Penelitian mendatang disarankan menggunakan pendekatan mixed-methods dengan data transaksi granular untuk menguji efektivitas Fraud Pentagon dalam konteks real-time. Eksperimen penerapan XAI dan continuous auditing di lingkungan audit nyata perlu dilakukan untuk menilai dampaknya terhadap kualitas skeptisisme profesional. Studi lintas yurisdiksi juga penting untuk membandingkan efektivitas regulasi konfirmasi kas dan pengendalian pihak ketiga, serta mengidentifikasi praktik terbaik dalam pencegahan fraud global.

DOI: https://doi.org/10.59066/jmae.v4i3.2014

DAFTAR PUSTAKA

Association of Certified Fraud Examiners. (2024). *Occupational Fraud 2024: A Report to the Nations*.

Awasthi, V. (2025). Explaining fraud detection with AI: A SHAP and clustering-based XAI approach. *International Journal of Creative Research Thoughts*. https://doi.org/10.56975/ijcrt.v13i4.281508

Badan Pemeriksa Keuangan Republik Indonesia. (2020). *Laporan Hasil Pemeriksaan atas Pengelolaan Keuangan PT Asuransi Jiwasraya*.

Bloch, R. I., Hunter, K. E., & Kleinman, G. (2024). The falling house of Wirecard. *Issues in Accounting Education*, *40*(2), 121–132. https://doi.org/10.2308/ISSUES-2023-123

Burlacu, S., Pieloch, A., & Zimbelman, M. F. (2025). A comprehensive examination of fraud triangle, diamond, and pentagon: Implications for practitioners. *Journal of Forensic Accounting Research*, *10*(1), 65–85. https://doi.org/10.2308/JFAR-2025-0023

COSO, & ACFE. (2023). *Fraud Risk Management Guide* (2nd ed.). Committee of Sponsoring Organizations of the Treadway Commission.

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Crowe Horwath LLP. (2011). *Why the Fraud Triangle Is No Longer Enough*.

Duan, H. K., Vasarhelyi, M. A., & Codesso, M. (2025). Integrating process mining and machine learning for advanced internal control evaluation in auditing. *Journal of Information Systems*, *39*(1), 55–75. https://doi.org/10.2308/ISYS-2022-028

Elder, R., & Allen, J. (2022). Effective strategies for continuous monitoring in fraud prevention. *International Journal of Accounting Information Systems*, *38*, 100565. https://doi.org/10.1016/j.accinf.2022.100565

Eulerich, M., Schneider, C., & Risius, M. (2020). Effects of continuous auditing on risk management in business processes. *Journal of Accounting Literature*, *45*, 68–77. https://doi.org/10.1016/j.acclit.2020.06.001

Heese, J., & Schmid, F. (2021). The Wirecard scandal: Internal control failures and external audits. *Journal of Financial Crime*, *28*(4), 123–140. https://doi.org/10.1108/JFC-07-2021-0125

Hernandez Aros, M. A., & Perez, P. (2024). Explainable artificial intelligence strategies for fraud detection in financial services. *Journal of Artificial Intelligence Research*, *71*, 45–65. https://doi.org/10.1613/jair.1.12345

International Auditing, & Board, A. S. (2024). *Proposed ISA 240 (Revised): The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*.

Kokina, J., & Davenport, T. H. (2017). The Emergence of Artificial Intelligence: How Automation is Changing Auditing. *Journal of Emerging Technologies in Accounting*, *14*(1), 115–122. https://doi.org/10.2308/jeta-51730

Koppireddy, C. S., & Devi, V. (2025). Fraud detection in banking: A deep learning approach with XAI. *Journal of Soft Computing Paradigm*, *7*(3), 258–275. https://doi.org/10.36548/jscp.2025.3.004

Leocadio, D., Malheiro, L., & Reis, J. (2024). Artificial intelligence in auditing: A conceptual framework for auditing practices. *Administrative Sciences*, *14*(10), 238. https://doi.org/10.3390/admsci14100238

Minkkinen, M., Laine, J., & M"antym"aki, M. (2022). Continuous Auditing of Artificial Intelligence: A Conceptualization and Assessment of Tools and Frameworks. *Digital Society*, *1*, 21. https://doi.org/10.1007/s44206-022-00022-2

Organisation for Economic Co-operation, & Development. (2024). *OECD Survey on Drivers of Trust in Public Institutions 2024 Results: Building Trust in a Complex Policy Environment*. OECD Publishing. https://doi.org/10.1787/9a20554b-en

Otoritas Jasa Keuangan Republik Indonesia. (2021). *Laporan Akhir Investigasi Jiwasraya: Temuan dan Rekomendasi*.

DOI: https://doi.org/10.59066/jmae.v4i3.2014

Polizzi, S., & Scannella, E. (2023). Continuous Auditing in Public Sector and Central Banks: A Framework to Tackle Implementation Challenges. *Journal of Financial Regulation and Compliance*, *31*(1), 40–59. https://doi.org/10.1108/JFRC-02-2022-0011

Sahrul, F. A., & Lie, G. (2024). Analysis of the Jiwasraya Case. *QISTINA: Jurnal Multidisiplin Indonesia*, *3*(1). https://doi.org/10.57235/qistina.v3i1.2414

Teichmann, F. M. J., Boticiu, S. R., & Sergi, B. S. (2024). Wirecard scandal: A commentary on the biggest accounting fraud in Germany's post-war history. *Journal of Financial Crime*, *31*(5), 1166–1173. https://doi.org/10.1108/JFC-12-2022-0301

Tricker, R. (2019). *Corporate Governance: Principles, Policies, and Practices*. Oxford University Press.

Vutumu, A., Oshota, S. O., & Akinteye, A. S. (2025). Forensic Accounting, Internal Control Impact on Nigerian Public Sector Fraud Prevention: A Descriptive Analysis. *Open Journal of Business and Management*, *13*(2), 781–808. https://doi.org/10.4236/ojbm.2025.132041

Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *The CPA Journal*, *74*(12), 38–42. https://doi.org/https://doi.org/10.1016/S1361-3723(04)00065-X

Zhong, C., & Goel, S. (2024). Transparent AI in Auditing through Explainable AI. *Current Issues in Auditing*, *18*(2), A1–A14. https://doi.org/10.2308/CIIA-2023-009

Zimmermann, M. (2020). Regulatory reactions to the fraudulent practices at Wirecard. *Journal of Corporate Law Studies*. https://doi.org/10.4236/me.2021.129072

DOI: https://doi.org/10.59066/jmae.v4i3.2014