Jurnal Manajemen dan Penelitian Akuntansi (JUMPA)
Vol 19, No.1, Januari-Juni (2026)
E-ISSN2746-7147
P-ISSN 1693-3907

Eksplorasi Peran *Cybersecurity Audit* dan Audit Investigatif Dalam Pengendalian *Fraud* Berbasis Teknologi

Annisa Ayuningtyas[1], Mikanti Annisa Sugrining Rahayu[2], Agus Widarsono[3]

[1,2,3] Program Studi Akuntansi, Universitas Pendidikan Indonesia, Bandung, Jawa Barat, Indonesia

Abstrak

Perkembangan transformasi digital meningkatkan kompleksitas risiko *fraud* berbasis teknologi informasi dan menuntut pendekatan audit yang adaptif serta terintegrasi. Penelitian ini bertujuan untuk menganalisis dan mengeksplorasi perkembangan *cybersecurity audit* dan audit investigatif dalam pengelolaan risiko *fraud* berbasis teknologi informasi melalui metode *Systematic Literature Review* (SLR) dengan pedoman PRISMA. Data bersumber dari basis data Science Direct, Emerald Insight, dan Google Scholar dengan rentang publikasi 2021–2026, memperoleh 36 artikel yang dianalisis secara tematik. Hasil sintesis menunjukkan bahwa *cybersecurity audit* telah berevolusi dari fungsi kepatuhan teknis menjadi mekanisme tata kelola risiko berbasis maturitas yang memanfaatkan AI, *blockchain*, *zero-trust architecture*, dan pemantauan *real-time* untuk pencegahan hingga deteksi *fraud*. Di sisi lain, audit investigatif berperan dalam pembuktian dan penanganan *fraud* melalui pemanfaatan CAATs, *red flags*, *digital forensics*, dan integrasi akuntansi forensik dalam kerangka manajemen risiko. Kombinasi kedua pendekatan ini membentuk siklus pengelolaan risiko *fraud* yang saling melengkapi. Kombinasi kedua pendekatan menjadi strategi yang optimal untuk menghadapi kompleksitas *fraud* di era digital karena mencakup aspek pencegahan, deteksi, dan pembuktian hukum secara terintegrasi.

Kata Kunci: *Cybersecurity audit*, Audit Investigatif, *Fraud*, *Digital*, *Literature Review*

Abstract

The rapid development of digital transformation has increased the complexity of information technology-based fraud risks and demands adaptive and integrated auditing approaches. This study aims to analyze and explore the development of cybersecurity audits and investigative audits in managing information technology-based fraud risks using the Systematic Literature Review (SLR) method with PRISMA guidelines. The data were collected from the ScienceDirect, Emerald Insight, and Google Scholar databases, covering publications from 2021–2026, resulting in 36 articles analyzed thematically. The findings indicate that cybersecurity audits have evolved from a technical compliance function into a risk governance mechanism based on maturity models by utilizing artificial intelligence (AI), blockchain, zero-trust architecture, and real-time monitoring for fraud prevention and detection. Meanwhile, investigative audits play a role in fraud verification and resolution through the application of Computer-Assisted Audit Techniques (CAATs), red flags analysis, digital forensics, and the integration of forensic accounting within risk management frameworks. The combination of these two approaches forms a complementary fraud risk management cycle. The integration of cybersecurity audits and investigative audits represents an optimal strategy for addressing the complexity of fraud in the digital era, as it encompasses prevention, detection, and legal evidence processes in an integrated manner.

Keywords: *Cybersecurity audit, Investigative Audit, Fraud, Digital, Literature Review*

Korespondensi:
Annisa Ayuningtyas
(annisaayuning@upi.edu)

Submit: 22 Maret 2026s
Revisi: 24 Mei 2026
Diterima: 10 Juni 2026
Terbit: 18 Juni 2026

1. Pendahuluan

Era digital telah mempercepat transformasi model bisnis melalui integrasi sistem informasi yang semakin kompleks dan terotomatisasi. Namun, pada saat yang sama membuka ruang baru bagi *fraud* berbasis teknologi yang adaptif dan sulit dilacak, seperti intrusi data, manipulasi transaksi elektronik, serta eksploitasi celah sistem (Hajiyev et al., 2025). Ketergantungan organisasi pada *cloud computing*, *Internet of Things* (IoT), dan *fintech* memperluas bidang serangan serta meningkatkan eksposur terhadap risiko siber yang secara langsung mengancam integritas laporan keuangan dan stabilitas operasional (Khan et al., 2026). Dalam lingkungan digital yang dinamis ini, risiko *fraud* tidak lagi bersifat linier, melainkan membentuk siklus yang melibatkan kegagalan kontrol, eksploitasi teknologi, dan penyalahgunaan akses sehingga memerlukan pendekatan audit yang terintegrasi antara dimensi preventif dan investigatif untuk mengelola risiko secara menyeluruh.

Dalam konteks tersebut, *cybersecurity audit* diposisikan sebagai mekanisme preventif utama yang bertujuan mengevaluasi tingkat keamanan sistem informasi, mengidentifikasi kerentanan, dan menilai efektivitas pengendalian (Sabillon et al., 2024). Melalui pendekatan berbasis *governance* dan manajemen risiko, audit ini tidak hanya memastikan kepatuhan terhadap standar, tetapi juga berfungsi sebagai sistem peringatan dini terhadap anomali yang berpotensi mengindikasikan *fraud* (Umbet et al., 2025). Integrasi teknologi mutakhir, seperti *artificial intelligence* dan *blockchain* semakin memperkuat fungsi ini dengan memungkinkan deteksi pola tidak wajar secara otomatis serta penciptaan jejak transaksi yang bersifat permanen sehingga peluang manipulasi dapat ditekan sebelum berkembang menjadi kasus *fraud* yang signifikan (Thanasas et al., 2026). Dengan demikian, *cybersecurity audit* bergerak melampaui fungsi kepatuhan teknis menuju instrumen strategis pencegahan *fraud* berbasis sistem informasi.

Meskipun demikian, fungsi preventif tidak selalu mampu mengeliminasi seluruh risiko, terutama ketika pelaku berhasil melewati kontrol atau memanfaatkan celah internal. Pada titik inilah audit investigatif memainkan peran krusial sebagai mekanisme lanjutan yang berfokus pada pembuktian dan penanganan *fraud*. Ketika *cybersecurity audit* mengidentifikasi indikasi kecurangan, temuan tersebut menjadi pemicu transisi menuju proses investigatif yang lebih mendalam, bukti digital dari sistem *monitoring* dianalisis secara forensik untuk kepentingan pembuktian hukum dan penegakan akuntabilitas (Ferreira et al., 2025). Audit investigatif memanfaatkan teknik, seperti *Computer Assisted Audit Techniques and Tools* (CAATTs), analisis log, serta rekonstruksi jejak transaksi untuk mengungkap modus operandi dan memastikan validitas bukti (Bonrath & Eulerich, 2024). Dalam kerangka ini, *cybersecurity audit* berfungsi memperkuat pengendalian dan mencegah peningkatan risiko, sedangkan audit investigatif memastikan penyelesaian kasus serta perbaikan sistem berdasarkan temuan empiris.

Meskipun hubungan konseptual antara kedua pendekatan tersebut tampak saling melengkapi, literatur masih menunjukkan ketidakselarasan. *Cybersecurity audit* cenderung dikaji sebagai mekanisme preventif berbasis tata kelola TI dengan fokus pada mitigasi Risiko. Sementara itu, audit investigatif lebih banyak dibahas dalam konteks reaktif dan pembuktian *fraud* setelah kejadian terjadi (Abu-Dabaseh et al., 2025). Kurangnya penjelasan eksplisit mengenai alur integratif dari deteksi dini hingga pembuktian hukum menunjukkan adanya kesenjangan konseptual dalam penelitian terdahulu. Akibatnya, pemahaman mengenai bagaimana kedua pendekatan tersebut dapat disinergikan dalam satu siklus manajemen risiko *fraud* berbasis sistem informasi masih belum terstruktur secara sistematis dalam literatur akademik. Oleh karena itu, penelitian ini bertujuan untuk menganalisis dan mengeksplorasi perkembangan *cybersecurity audit* dan audit investigatif dalam pengelolaan risiko *fraud* berbasis teknologi informasi, melalui tiga pertanyaan penelitian, yaitu 1) bagaimana literatur mendefinisikan dan mengkonseptualisasikan peran *cybersecurity audit* dalam konteks pencegahan dan deteksi *fraud*, 2) bagaimana literatur menggambarkan peran audit investigatif dalam pembuktian dan penanganan *fraud* berbasis sistem informasi/teknologi, 3) bagaimana integrasi antara *cybersecurity audit* dan audit investigatif dalam pengelolaan risiko *fraud* berbasis TI.

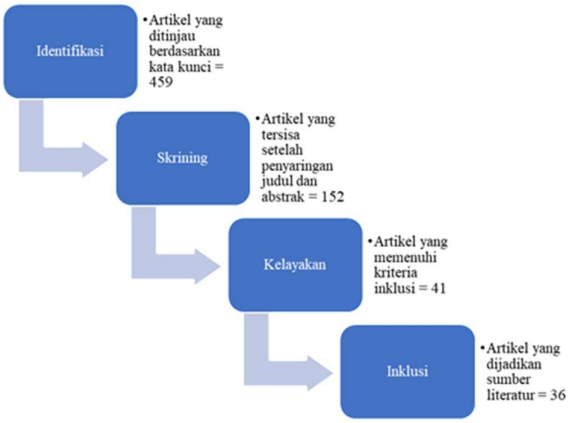
2. Metode

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) untuk mengidentifikasi dan mensintesis penelitian terdahulu mengenai *cybersecurity audit* dan audit investigatif. Prosedur penelitian mengikuti pedoman yang dikemukakan oleh Tranfield et al. (2003) serta mengacu pada prinsip kerangka PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Literatur yang relevan dikumpulkan dari basis data akademik seperti Science Direct, Emerald Insight, dan Google Scholar dengan menggunakan kata kunci utama "*Cybersecurity audit*" dan "Audit Investigatif." Pencarian dibatasi pada artikel jurnal nasional maupun internasional bereputasi yang diterbitkan dalam enam tahun terakhir untuk menangkap perkembangan terkini mengenai peran *cybersecurity audit* dan audit investigatif. Kriteria inklusi dan eksklusi ditetapkan untuk memastikan relevansi dan kualitas literatur. Rincian kriteria tersebut disajikan pada tabel berikut.

Tabel 1. Kriteria Inklusi dan Eksklusi

Kriteria	Inklusi	Eksklusi
Tipe literatur	Artikel ilmiah	Esai, makalah, prosiding, dsb.
Tahun publikasi	≥ 2021	< 2021
Fokus topik	Peran *cybersecurity audit* dan audit investigatif serta kaitannya	Di luar peran *cybersecurity audit* dan audit investigatif

Proses seleksi literatur mengikuti empat tahap utama kerangka PRISMA, yaitu identifikasi, skrining, kelayakan, dan inklusi. Tahapan tersebut memastikan bahwa hanya literatur yang memenuhi seluruh kriteria yang dipertahankan.



Gambar 1. Kerangka PRISMA

Pada tahap identifikasi, seluruh literatur potensial dikumpulkan dari basis data menggunakan kata kunci yang telah ditentukan. Hasil pencarian kemudian digabungkan, duplikasi dihapus, dan basis data awal dibentuk untuk memastikan cakupan literatur yang luas sebelum melanjutkan ke tahap berikutnya. Selanjutnya pada tahap skrining, judul dan abstrak literatur ditinjau untuk menilai relevansinya dengan topik peran *cybersecurity audit* dan audit investigatif, sedangkan literatur yang tidak relevan dengan topik penelitian dieliminasi. Literatur yang relevan kemudian masuk ke tahap kelayakan. Pada tahap kelayakan, keseluruhan isi literatur diperiksa untuk mengevaluasi kesesuaian fokus penelitian. Terakhir, pada tahap inklusi, seluruh artikel yang memenuhi kriteria dianalisis dalam SLR untuk menjawab pertanyaan penelitian.

3. Hasil dan Pembahasan

Penelitian ini mengkaji perkembangan literatur mengenai *cybersecurity audit* dan audit investigatif dalam pengelolaan risiko *fraud* berbasis teknologi informasi melalui pendekatan *Systematic Literature Review* (SLR). Dataset final yang digunakan dalam kajian ini terdiri dari 36 artikel akademik yang dipilih secara sistematis berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan. Berikut disajikan analisis distribusi berdasarkan tahun publikasi, metodologi penelitian, dan sintesis tematik dari temuan-temuan utama untuk memberikan gambaran menyeluruh mengenai karakteristik literatur yang dikaji,

Tabel 2. Klasifikasi Berdasarkan Tahun Penelitian

Tahun	Jumlah	Persentase
2026	4	11%
2025	18	50%
2024	3	8%
2023	6	17%
2022	1	3%
2021	4	11%
Total	**36**	**100%**

Tabel 2 menunjukkan tren peningkatan signifikan pada jumlah studi sepanjang 2021–2026, dengan 50% artikel diterbitkan pada 2025 (18 studi), 17% pada 2023 (6 studi), 11% pada 2026 dan 2021 (8 studi), 8% pada 2024 (3 studi), serta 3% pada 2022 (1 studi). Hal ini mencerminkan momentum riset yang kuat di bidang audit *cybersecurity* dan investigatif pasca-pandemi serta percepatan transformasi digital. Distribusi tersebut mengindikasikan maturitas literatur, di mana studi 2021–2023 mewakili fondasi awal, sedangkan lonjakan 2025–

2026 menandakan respons terhadap munculnya ancaman siber seperti *fraud* yang dihasilkan oleh AI dan kebutuhan kerangka investigatif berbasis teknologi.

Tabel 3. Klasifikasi Berdasarkan Metode Penelitian

Jenis	Jumlah	Persentase	Teknik
Kuantitatif	17	47%	Regresi (OLS, Multivariat, Logistik, Linear Berganda); SEM; PLS-SEM; Survei; Eksperimen; Analisis Diskriminan;
Kualitatif	5	14%	Survei; Kerangka Konseptual; Analisis Konten; Studi Kasus; STRIDE
Mixed Method	3	8%	Analisis Tematik & Deskriptif; Studi Kasus; PLS-SEM
Multi Method	1	3%	Analisis Konten
Literature Review	9	25%	SLR; Bibliometrik; Analisis Komparatif; Analisis Tematik; Studi Kasus; Analisis Naratif
Kausalitas	1	3%	PLS-SEM
Total	**36**	**100%**	

Tabel 3 metodologi menggambarkan keragaman pendekatan empiris dengan dominasi kuantitatif (47%, 17 studi), seperti regresi dan SEM, diikuti *literature review* (25%, 9 studi) termasuk SLR dan bibliometrik, serta kualitatif (14%, 5 studi) berbasis survei dan kerangka konseptual. Pendekatan *mixed-method* dan *multi method* (11%, 4 studi) mengintegrasikan analisis tematik & deskriptif serta analisis konten, sedangkan kausalitas (3%, 1 studi) menggunakan SEM. Komposisi ini mencerminkan diversifikasi metodologi dengan dominasi pendekatan kuantitatif, tetapi tetap memberi ruang bagi kajian literatur, eksplorasi kualitatif, dan integrasi metode lainnya.

Tabel 4. Klasifikasi Berdasarkan Sintesis Temuan

Kategori Tematik	Jumlah	Referensi Kunci
Cybersecurity audit		
Deteksi *Fraud* Berbasis AI & *Explainable* AI	4	Amraoui et al. (2026); Ghosh (2025); Mollik & Majeed (2025); Alhashmi et al. (2023)
Blockchain, Enkripsi & *Zero-Trust Architecture*	4	Khan et al. (2026); Xu et al. (2025); Hajiyev et al. (2025); Goundar & Gondal (2025)
Pemantauan Berkelanjutan & Deteksi *Real-Time*	5	Thanasas et al. (2026); Jha et al. (2025); Wadesango & Maveneka (2025); Almajali et al. (2024); Fetaji et al. (2025)
Kerangka Audit TI & Tata Kelola Risiko	5	Umbet et al. (2025); Abu-Dabaseh et al. (2025); Tharwat et al. (2025); Sabillon et al. (2024); Klumpes (2023)
Ancaman Internal & Pengendalian Internal	4	Kanyogo & Wadesango (2025); Idensohn & Flowerday (2025); Lois et al. (2021); Buil-Gil et al. (2021)
Audit Investigatif		
Teknik Audit Berbasis Komputer (CAATs)	3	Jayanti et al. (2026); Aulia et al. (2025); Daoud et al. (2021)
Akuntansi Forensik & Integrasi Audit Investigatif	5	Sumardi et al. (2025); Prasetiyo et al. (2023); Encarnación (2023); Sudarmadi (2023); Laupe et al. (2022)
Identifikasi *Red Flags* & Deteksi *Fraud*	2	Suryani & Syahrudin (2025); Meiryani et al. (2023)
Fungsi Audit Internal & Pencegahan *Fraud*	3	Ferreira et al. (2025); Bonrath & Eulerich (2024); Nurlaela et al. (2021)
Model Audit Terintegrasi Berbasis Risiko	1	Patskan et al. (2025)

Tabel 4 sintesis temuan dikelompokkan ke dalam 10 kategori tematik (5 per domain) dengan 2 topik yang berbeda, yakni *cybersecurity audit* dan audit investigatif. Sintesis *cybersecurity audit* mengklasifikasikan 22 artikel yang mencerminkan evolusi praktik audit keamanan siber di era digital. Kategori deteksi *fraud* berbasis AI & *explainable* AI (4 studi) menyoroti pemanfaatan *machine learning* dan XAI untuk deteksi *fraud* secara *real-time* melalui interpretabilitas LIME. *Blockchain*, enkripsi & *zero-trust architecture* (4 studi) menekankan jejak audit

tahan rusak dan pengujian penetrasi untuk kekekalan data. Pemantauan berkelanjutan & deteksi *real-time* (5 studi) mengintegrasikan *Big Data*, IoT, dan AI untuk pemantauan berkelanjutan, sedangkan kerangka audit TI & tata kelola risiko (5 studi) fokus pada COBIT/ISACA untuk penilaian kematangan serta ancaman internal & pengendalian internal (4 studi) mengatasi risiko internal melalui kerangka STRIDE.

Selanjutnya, sintesis audit investigatif mengklasifikasikan 14 artikel yang menggambarkan sinergi akuntansi forensik, audit investigatif, dan teknologi CAATs dalam pencegahan *fraud* dengan *Technology Acceptance Model* (TAM) sebagai fondasi utama. Kategori teknik audit berbasis komputer (CAATs) (3 studi) menunjukkan pengaruh PEOU/PU terhadap efektivitas deteksi *fraud*. Kategori tematik akuntansi forensik & integrasi audit investigatif (5 studi) membuktikan efek preventif melalui dokumentasi bukti yang dapat diterima dan perbaikan pengendalian internal. Identifikasi *red flags* & deteksi *fraud* (2 studi) menekankan deteksi indikator awal berbasis TI. Fungsi audit internal & pencegahan *fraud* (3 studi) memposisikan IAF sebagai *third line of defense*, dan model audit terintegrasi berbasis risiko (1 studi) mengusulkan integrasi tiga jalur untuk pengelolaan risiko holistik.

Peran *Cybersecurity audit* dalam Pencegahan dan Deteksi *Fraud*

Berdasarkan sintesis terhadap 22 artikel dalam domain *cybersecurity audit*, penelitian ini mengkonfirmasi bahwa *cybersecurity audit* telah berkembang jauh melampaui fungsinya sebagai pemeriksaan teknis semata. Secara konseptual, *cybersecurity audit* didefinisikan sebagai proses sistematis untuk menilai sejauh mana kebijakan, prosedur, dan kontrol keamanan suatu organisasi telah dirancang serta dijalankan secara efektif guna melindungi kerahasiaan, integritas, hingga ketersediaan informasi dan infrastruktur TI dari ancaman siber dengan mengacu pada kerangka kerja atau standar tertentu seperti NIST, ISO 27001, dan CSAM 2.0 (Lois et al., 2021; Sabillon et al., 2024; Tharwat et al., 2025). Definisi tersebut mencakup aktivitas perencanaan, pengujian kontrol, pengukuran tingkat kematangan, serta pemberian rekomendasi perbaikan sebagai dasar peningkatan berkelanjutan tata kelola dan manajemen risiko siber. Dalam konteks pencegahan dan deteksi *fraud*, *cybersecurity audit* diposisikan oleh literatur terkini sebagai mekanisme tata kelola risiko yang terintegrasi dengan teknologi, kontrol internal, dan kapasitas organisasi. Amraoui et al. (2026) memposisikan *cybersecurity audit* sebagai fungsi yang berevolusi menuju pemantauan *real-time* dan deteksi anomali prediktif. Sementara itu, Abu-Dabaseh et al. (2025) memandang peran *cybersecurity audit* sebagai moderator dalam memastikan transformasi digital berpengaruh mitigasi *fraud* melalui kerangka kematangan yang sistematis.

Dari dimensi pencegahan, sintesis literatur menunjukkan bahwa *cybersecurity audit* beroperasi melalui dua jalur utama, yakni penguatan arsitektur keamanan dan peningkatan risiko deteksi bagi calon pelaku *fraud*. Khan et al. (2026) memandang *cybersecurity audit* sebagai lapisan kepercayaan yang memverifikasi output AI menjadi bukti forensik sah sehingga secara efektif meningkatkan risiko deteksi dan menurunkan insentif untuk melakukan *fraud*. Gagasan ini diperkuat oleh Thanasas et al. (2026) dan Hajiyev et al. (2025) yang menekankan integrasi *blockchain*, arsitektur *zero-trust*, serta kepatuhan terhadap standar ISO 27001 sebagai pilar untuk menjaga integritas data dan mencegah manipulasi. Pada level operasional, Idensohn & Flowerday (2025), Jha et al. (2025), dan Kanyongo & Wadesango (2025) menunjukkan bahwa kontrol akses berbasis MFA, pengujian penetrasi, dan audit rutin secara langsung membatasi peluang terjadinya *fraud* baik dari sumber internal maupun eksternal. Dalam konteks sektor publik, Umbet et al. (2025) dan Wadesango & Maveneka (2025) menegaskan bahwa *cybersecurity audit* yang dikaitkan dengan tata kelola TI dan transparansi digital terbukti mampu menekan diskresi dan praktik koruptif. Temuan-temuan ini secara simultan menjawab rumusan masalah pertama penelitian ini, yaitu bahwa literatur mendefinisikan *cybersecurity audit* bukan sekadar sebagai mekanisme kepatuhan teknis, melainkan sebagai instrumen strategis pencegahan *fraud* yang bekerja melalui penguatan arsitektur, tata kelola, dan peningkatan kapasitas deteksi.

Pada dimensi deteksi, perkembangan teknologi AI dan *blockchain* secara signifikan memperluas kapabilitas *cybersecurity audit* dalam mengidentifikasi anomali secara cepat dan akurat. Fetaji et al. (2025) dan Tharwat et al. (2025) menekankan integrasi AI, log *Intrusion Detection System* (IDS), dan *blockchain* untuk pemantauan *real-time* dan respons cepat terhadap anomali transaksi. Pendekatan ini dikembangkan lebih lanjut oleh Alhashmi et al. (2023) melalui model *ensemble* adaptif yang meningkatkan akurasi deteksi serta oleh Ghosh (2025) dan Mollik & Majeed (2025) melalui *Explainable AI* (XAI) yang tidak hanya meningkatkan akurasi, tetapi juga transparansi serta pengendalian atas *false positives*. Kendati demikian, Xu et al. (2025) memberikan peringatan kritis bahwa kemunculan *Generative AI* berpotensi melemahkan keandalan log audit dan meningkatkan risiko *false negatives* sehingga penguatan tata kelola menjadi syarat mutlak bagi keandalan sistem deteksi. Sabillon et al. (2024) dan Almajali et al. (2024) memperkuat argumen dengan menekankan pentingnya evaluasi kematangan kontrol yang berkelanjutan dan integrasi prinsip transparansi serta akuntabilitas dalam desain sistem audit. Temuan-temuan tersebut menunjukkan bahwa keunggulan teknologis dalam deteksi sangat bergantung pada kualitas tata kelola dan kompetensi sumber daya manusia yang mengelolanya.

Lebih jauh, efektivitas *cybersecurity audit* dalam pengendalian *fraud* tidak semata-mata ditentukan oleh kecanggihan teknologi yang digunakan, tetapi terdapat peran faktor manusia dan kelembagaan yang melingkupinya. Lois et al. (2021) memandang *cybersecurity audit* sebagai fungsi konsultatif yang mampu menutup kesenjangan kebijakan antara desain kontrol dan implementasinya di lapangan. Buil-Gil et al. (2021)

menemukan bahwa kapasitas dan pelatihan *in-house* terbukti lebih efektif dalam meningkatkan ketahanan terhadap ancaman siber dibandingkan ketergantungan semata pada teknologi atau praktik *outsourcing*. Klumpes (2023) menambahkan perspektif sistemik dengan menyoroti pentingnya koordinasi regulatif lintas lembaga untuk menghadapi risiko *fraud* siber yang bersifat lintas batas dan semakin kompleks. Temuan tersebut membedakan penelitian ini dari penelitian terdahulu yang cenderung terlalu menekankan solusi teknologis tanpa mempertimbangkan faktor kapasitas kelembagaan secara proporsional. Dengan demikian, sintesis penelitian ini menegaskan bahwa pendekatan *cybersecurity audit* yang efektif bersifat holistik, mengintegrasikan dimensi teknologi, sumber daya manusia, dan tata kelola kelembagaan dalam satu kerangka yang koheren.

Peran Audit Investigatif dalam Pembuktian dan Penanganan *Fraud*

Berdasarkan sintesis terhadap 14 artikel dalam domain audit investigatif, penelitian ini mengkonfirmasi bahwa audit investigatif berperan dalam mendeteksi, menangani, serta mencegah *fraud* melalui kombinasi antara prosedur audit yang ketat dan teknik berorientasi forensik. Secara definitif, audit investigatif mencakup pemeriksaan mendalam atas catatan keuangan, evaluasi pengendalian internal, investigasi yang terarah, dan pemanfaatan mekanisme *whistleblowing* untuk mengungkap skema kecurangan (Encarnación, 2023). Efektivitas pelaksanaannya secara empiris dipengaruhi oleh struktur tata kelola organisasi dan posisi strategis auditor internal dalam hierarki pengawasan. Bonrath & Eulerich (2024) secara spesifik menunjukkan bahwa keterlibatan aktif fungsi audit internal dengan manajemen puncak memperkuat efektivitas pencegahan *fraud*, sedangkan hubungan audit internal dengan komite audit turut memengaruhi intensitas pengawasan yang dilakukan. Temuan tersebut secara langsung menjawab rumusan masalah kedua penelitian ini, yaitu bahwa efektivitas audit investigatif tidak dapat dipisahkan dari kualitas struktur tata kelola yang menjadi landasannya.

Salah satu kompetensi inti dalam pelaksanaan audit investigatif adalah kemampuan menelusuri, mengidentifikasi, dan mengungkap fakta berdasarkan bukti yang diperoleh secara metodis (Prasetiyo et al., 2023). Literatur mengidentifikasi pemanfaatan *red flags* sebagai salah satu metode utama dalam proses investigatif, di mana indikator-indikator perilaku tidak wajar, anomali proses operasional, maupun ketidakberesan keuangan berfungsi sebagai pemicu bagi auditor untuk melakukan pemeriksaan yang lebih mendalam dan berbasis bukti. Suryani & Syahrudin (2025) dan Meiryani et al. (2023) menekankan bahwa penerapan metode *red flags* dalam audit investigatif juga berkaitan erat dengan upaya mengurangi *expectation gap* antara pengguna laporan keuangan dan auditor, yakni kesenjangan antara harapan publik dan realitas peran auditor dalam pendeteksian kecurangan. Hasil audit investigatif mampu mengonversi temuan audit menjadi bukti yang dapat diterima secara hukum sehingga mendukung proses penegakan dan memperkuat akuntabilitas (Encarnación, 2023). Kompetensi ini menjadikan audit investigatif sebagai mekanisme yang tidak hanya relevan pada tahap penanganan, tetapi juga pada tahap pembuktian formal dalam proses hukum.

Integrasi teknologi secara signifikan meningkatkan efektivitas dan jangkauan audit investigatif dalam menghadapi skema *fraud* yang semakin canggih. Pemanfaatan *Computer Assisted Audit Techniques* (CAATs), *digital forensics*, dan sistem informasi analitik mendorong auditor untuk mengidentifikasi anomali dan pola mencurigakan secara lebih efisien dan komprehensif dibandingkan teknik manual konvensional (Nurlaela et al., 2021). Namun, keberhasilan integrasi teknologi dalam praktik audit investigatif sangat bergantung pada kompetensi auditor dan komitmen terhadap pengembangan profesional yang berkelanjutan karena skema *fraud* turut berevolusi seiring peningkatan kompleksitas teknologi. Daoud et al. (2021) dan Jayanti et al. (2026) secara konsisten menunjukkan bahwa dukungan organisasional, terutama komitmen manajemen puncak dan kesiapan infrastruktur TI merupakan prasyarat bagi keberhasilan implementasi CAATs dalam konteks audit investigatif. Dibandingkan dengan penelitian sebelumnya yang cenderung membahas CAATs secara deskriptif, literatur terkini mulai mengkaji efektivitas CAATs dalam kerangka penerimaan teknologi (*Technology Acceptance Model*/TAM) sehingga memberikan landasan teoritis yang lebih kuat untuk memahami faktor-faktor yang menentukan keberhasilannya (Aulia et al., 2025; Jayanti et al., 2026).

Penerapan audit investigatif yang konsisten dan profesional terbukti memberikan kontribusi nyata dalam penanganan *fraud* yang telah terjadi serta pencegahan terulangnya kecurangan di masa mendatang. Laupe et al. (2022) menemukan bahwa konsistensi entitas dalam menindaklanjuti temuan secara investigatif terbukti mampu menurunkan probabilitas terulangnya *fraud* melalui penguatan efek jera. Sudarmadi (2023) menambahkan bahwa hasil audit investigatif menyediakan informasi strategis yang dapat digunakan oleh manajemen untuk merancang, mengembangkan, dan menyempurnakan kebijakan serta prosedur pengendalian internal yang berlaku. Patskan et al. (2025) mengajukan proposisi yang lebih komprehensif melalui model audit terintegrasi berbasis risiko, Diagnostik forensik, audit anti korupsi, dan audit internal disinergikan dalam kerangka manajemen berbasis risiko untuk memperkuat ketahanan entitas terhadap berbagai bentuk *fraud*. Dengan demikian, sintesis penelitian ini menegaskan bahwa audit investigatif merupakan instrumen strategis multidimensi yang menjaga integritas dan transparansi keuangan melalui kombinasi praktik forensik, analitik berbasis teknologi, dan tata kelola internal yang kuat sekaligus berkontribusi pada penutupan celah pengendalian yang menjadi akar penyebab terjadinya *fraud*.

Integrasi *Cybersecurity audit* dan Audit Investigatif dalam Pengelolaan Risiko *Fraud*

Temuan sintesis dari kedua domain yang dikaji menunjukkan bahwa integrasi *cybersecurity audit* dan audit investigatif merepresentasikan kombinasi optimal dalam menghadapi *fraud* yang semakin kompleks di era digital. Secara konseptual, *cybersecurity audit* beroperasi sebagai mekanisme preventif yang memperkuat lapisan pertahanan sebelum *fraud* terjadi, sedangkan audit investigatif berfungsi sebagai mekanisme reaktif sekaligus represif yang mengonfirmasi indikasi kecurangan menjadi bukti yang dapat dipertanggungjawabkan secara hukum (Sumardi et al., 2025). Kedua pendekatan tersebut, meskipun memiliki orientasi yang berbeda, saling melengkapi dalam membentuk siklus manajemen risiko *fraud* yang menyeluruh, mulai dari identifikasi kerentanan, deteksi anomali, investigasi forensik, pembuktian hukum, hingga pemulihan dan perbaikan sistem pasca insiden. Siklus tersebut secara empiris didukung oleh berbagai temuan dalam dataset penelitian ini yang secara bersamaan menunjukkan bahwa pendekatan tunggal tanpa integrasi lintas fungsi tidak cukup efektif menghadapi kompleksitas ancaman *fraud* berbasis TI yang bersifat adaptif. Dengan demikian, integrasi kedua pendekatan menjadi kebutuhan strategis yang mendesak bagi organisasi di era digital.

Dalam praktiknya, integrasi antara *cybersecurity audit* dan audit investigatif diwujudkan melalui pengembangan kerangka terpadu yang menggabungkan pengendalian keamanan siber dengan teknik investigasi forensik. Pemanfaatan teknologi seperti AI dan *blockchain* terbukti mampu meningkatkan kemampuan deteksi, pencatatan, dan verifikasi insiden siber secara bersamaan sehingga mendukung kebutuhan audit preventif serta proses pembuktian forensik (Goundar & Gondal, 2025; Khan et al., 2026). Fungsi audit internal diposisikan sebagai pengawasan independen yang strategis dalam tata kelola keamanan siber meliputi aktivitas penilaian risiko, pengujian penetrasi, dan evaluasi kontrol yang secara langsung menjembatani fungsi preventif serta investigatif (Ferreira et al., 2025). Di sisi lain, Buil-Gil et al. (2021) dan Klumpes (2023) menjelaskan bahwa efektivitas integrasi ini tidak hanya ditentukan oleh kerangka teknologis yang digunakan, tetapi juga oleh penguatan kapasitas sumber daya manusia melalui pelatihan *in-house* yang terstruktur dan koordinasi regulatif lintas lembaga yang memastikan konsistensi standar pengendalian. Proses identifikasi anomali, penelusuran jejak digital, hingga dokumentasi temuan yang dilakukan dalam kerangka terpadu ini memungkinkan pengelolaan risiko *fraud* yang lebih komprehensif, terstruktur, dan dapat dipertanggungjawabkan secara hukum.

Dibandingkan dengan berbagai penelitian terdahulu, penelitian ini memberikan kontribusi konseptual yang berbeda melalui upaya mensintesis secara sistematis bagaimana kedua pendekatan dapat disinergikan dalam satu siklus manajemen risiko *fraud* berbasis TI. Penelitian terdahulu umumnya mengkaji *cybersecurity audit* dan audit investigatif secara terpisah. *Cybersecurity audit* dikaji dalam konteks tata kelola TI dan kepatuhan standar keamanan, sedangkan audit investigatif lebih banyak dibahas dalam konteks pembuktian *fraud* pasca kejadian (Abu-Dabaseh et al., 2025). Penelitian ini, melalui pendekatan SLR yang sistematis, berhasil mengidentifikasi titik-titik pertemuan konseptual antara kedua domain tersebut, termasuk peran audit internal sebagai jembatan antara fungsi preventif dan investigatif serta peran teknologi forensik digital sebagai instrumen yang melayani kebutuhan kedua fungsi secara bersamaan. Implikasi teoretis dari temuan ini adalah perlunya pengembangan kerangka konseptual integratif yang secara eksplisit memetakan alur dari deteksi dini berbasis *cybersecurity audit* menuju pembuktian hukum berbasis audit investigatif. Implikasi praktisnya adalah perlunya organisasi merancang sistem pengendalian *fraud* yang tidak hanya berorientasi pada pencegahan teknis, tetapi juga mempersiapkan kapasitas investigatif dan forensik yang memadai sebagai bagian integral dari strategi manajemen risiko yang komprehensif.

4. Kesimpulan

Penelitian ini menjawab ketiga rumusan masalah yang ditetapkan melalui sintesis sistematis terhadap 36 artikel akademik periode 2021–2026. Literatur mengonseptualisasikan *cybersecurity audit* sebagai kerangka pengendalian strategis yang mengintegrasikan teknologi, kebijakan, dan kapasitas organisasi secara holistik dalam memitigasi *fraud*, bukan sekadar pemeriksaan teknis kepatuhan. Sementara itu, audit investigatif diposisikan sebagai mekanisme represif berbasis bukti yang mengonfirmasi indikasi kecurangan menjadi alat pembuktian yang sah secara hukum melalui pemanfaatan *red flags*, CAATs, dan *digital forensics*. Integrasi keduanya membentuk siklus manajemen risiko *fraud* yang komprehensif, mulai dari identifikasi kerentanan hingga pemulihan sistem pasca *fraud*, dan merepresentasikan pendekatan paling adaptif dalam menghadapi kompleksitas *fraud* berbasis TI. Secara teoritis, penelitian ini berkontribusi mengisi kesenjangan literatur dengan menawarkan perspektif integratif yang memetakan sinergi kedua pendekatan dalam satu kerangka manajemen Risiko. Secara praktis, temuan ini menegaskan urgensi organisasi untuk membangun kapasitas investigatif dan forensik sebagai bagian integral dari strategi pengendalian *fraud* yang menyeluruh. Penelitian ini memiliki keterbatasan pada cakupan literatur dan sifat pendekatan SLR yang kualitatif-interpretatif sehingga belum dapat menguji hubungan kausal antarvariabel secara empiris. Oleh karena itu, penelitian selanjutnya disarankan untuk menguji kerangka integratif ini menggunakan pendekatan kuantitatif atau studi kasus komparatif lintas sektor.

Daftar Pustaka

Abu-Dabaseh, F., Khtatbeh, M. M., Al'Ararah, K., & Alassuli, A. (2025). Exploring the role of digital transformation in mitigating accounting fraud: A cybersecurity perspective. *International Review of Management and Marketing*, *15*(3), 398–405. https://doi.org/10.32479/irmm.18490

Alhashmi, A. A., Alashjaee, A. M., Darem, A. A., Alanazi, A. F., & Effghi, R. (2023). An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures. *Engineering, Technology & Applied Science Research*, *13*(6), 12433–12439. https://doi.org/10.48084/etasr.6401

Almajali, M. H., Alshanty, A. G., Althnaibat, O. H., & ALmahasnah, M. J. (2024). The role of governance supported by cybersecurity in reducing financial and administrative corruption in public institutions in Jordan. *International Journal of Advanced Soft Computing Applications*, *16*(3). https://doi.org/10.15849/IJASCA.241130.13

Amraoui, S., Elmaallam, M., & Nassar, M. (2026). A dynamic AI maturity model for agile audit: A roadmap for enhanced effectiveness and innovation. *Journal of Computer Science*, *22*(1), 87–99. https://doi.org/10.3844/jcssp.2026.87.99

Aulia, E. S., Kusuma, I. C., & Didi. (2025). Pengaruh Caatts dan pengalaman auditor terhadap pendeteksian fraud melalui keahlian forensik dan audit investigatif. *AKUA: Jurnal Akuntansi Dan Keuangan*, *4*(3), 576–590. https://doi.org/10.54259/akua.v4i3.5196

Bonrath, A., & Eulerich, M. (2024). Internal auditing's role in preventing and detecting fraud: An empirical analysis. *International Journal of Auditing*, *28*(4), 615–631. https://doi.org/10.1111/ijau.12342

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. *Victims & Offenders*, *16*(3), 286–315. https://doi.org/10.1080/15564886.2020.1814468

Daoud, L., Marei, A., Al-Jabaly, S. M., & Aldaash, A. A. (2021). Moderating the role of top management commitment in usage of computer-assisted auditing techniques. *Accounting*, *7*(2), 457–468. https://doi.org/10.5267/j.ac.2020.11.005

Encarnación, V. R. E. (2023). Auditoría forense: Riesgo de auditoría, fraude y materialidad. *Suma de Negocios*, *14*(31), 122–135. https://doi.org/10.14349/sumneg/2023.V14.N31.A4

Ferreira, L. V. A., Alves, C. A. d. M., Peotta de Melo, L., & Nunes, R. R. (2025). Internal audit strategies for assessing cybersecurity controls in the Brazilian financial institutions. *Applied Sciences*, *15*(10), 5715. https://doi.org/10.3390/app15105715

Fetaji, B., Fetaji, M., Hasan, A., Rexhepi, S., & Armenski, G. (2025). FRAUD-X: An integrated AI, blockchain, and cybersecurity framework with early warning systems for mitigating online financial fraud: A case study from North Macedonia. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3547285

Ghosh, S. (2025). A novel framework for financial cybersecurity and fraud detection using XAI-RNN-SGRU. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3570216

Goundar, S., & Gondal, I. (2025). AI-blockchain integration for real-time cybersecurity: System design and evaluation. *Journal of Cybersecurity and Privacy*, *5*(3), 1–22. https://doi.org/10.3390/jcp5030059

Hajiyev, F., Babayev, N., & Gasimov, F. (2025). Organisation and areas of development of international audit in the digital economy. *Scientific Bulletin of Mukachevo State University, Series Economics*, *12*(2), 23–33. https://doi.org/10.52566/msu-econ2.2025.23

Idensohn, C. J., & Flowerday, S. (2025). Financial insider threats: A cybersecurity STRIDE analysis. *Issues in Information Systems*, *26*(1), 94–109. https://doi.org/10.48009/1_iis_108

Jayanti, C., Slamet, C. A., & Handoko, B. L. (2026). The impact of CAATS on financial auditor task effectiveness, moderated by computer literacy. *Multidisciplinary Science Journal*, *8*(1). https://doi.org/10.31893/multiscience.2026167

Jha, S. K., Verma, S., Gupta, S., & Kumar, K. K. (2025). Cybersecurity in FinTech: Strategies for protecting digital finance from cyber threats and ensuring secure transactions. *Journal of Discrete Mathematical Sciences & Cryptography*, *28*(8), 2977–2987. https://doi.org/10.47974/JDMSC-2442

Kanyongo, G., & Wadesango, N. (2025). Impact of cybersecurity on risk mitigation strategy by commercial banks in emerging markets: A legal perspective case study. *Corporate Law & Governance Review*, *7*(1), 28–37. https://doi.org/10.22495/clgrv7i1p3

Khan, M. U., Zhen, L., Tian, J., Farid, A., Chen, Z., & Liu, H. (2026). From detection to prevention: A cyber-secure AI ecosystem for mitigating milk adulteration and dairy fraud. *Trends in Food Science & Technology*. https://doi.org/https://doi.org/10.1016/j.tifs.2025.105503

Klumpes, P. (2023). Coordination of cybersecurity risk management in the U.K. insurance sector. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *48*(3), 332–371. https://doi.org/10.1057/s41288-023-00287-9

Laupe, S., Abdullah, M. I., Kahar, A., Saleh, F. M., Zahra, F., & Syamsuddin, N. A. (2022). Auditor's skepticism, forensic accounting, investigation audit and fraud disclosure of corruption cases. *Journal of Governance &*

Regulation, *11*(3), 189–196. https://doi.org/10.22495/jgrv11i3art16

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, *13*(1), 1–21.

Meiryani, Sampelino, Y. R., Witjaksono, A., Sihotang, P., Anwar, Y., & Mulyadi, M. S. (2023). The role of information technology in the practice of forensic investigation analysis for fraud disclosure in Indonesia. *E3S Web of Conferences*, *388*, 3002. https://doi.org/10.1051/e3sconf/202338803002

Mollik, E., & Majeed, F. (2025). AI-driven cybersecurity in mobile financial services: Enhancing fraud detection and privacy in emerging markets. *Journal of Cybersecurity and Privacy*, *5*(3), 77. https://doi.org/10.3390/jcp5030077

Nurlaela, E., Mappanyukki, R., & Surjandari, D. A. (2021). The effect of the internal audit roles and auditor professionalism on fraud prevention. *Studies in Media and Communication*, *9*(2), 52–61. https://doi.org/10.111114/smc.v9i2.5324

Patskan, Y., Nazarova, K., Kopotiienko, T., Miniailo, V., Pavlov, V., & Novikova, N. (2025). Forensic diagnostics, anti-corruption, and internal audit in ensuring efficient company management in an open economy. *Financial and Credit Activity: Problems of Theory and Practice*, *4*(63), 11–22. https://doi.org/10.55643/fcaptp.4.63.2025.4776

Prasetiyo, Y., Paramitha, D., Riyani, E. I., & Mubarok, F. (2023). Integrasi penerapan akuntansi forensik dan audit investigatif dalam mendeteksi fraud: Studi literatur. *Jurnal Buana Akuntansi*, *8*(1), 16–29. https://doi.org/10.36805/akuntansi.v8i1.3062

Sabillon, R., Higuera, J. R. B., Cano, J., Higuera, J. B., & Montalvo, J. A. S. (2024). Assessing the effectiveness of cyber domain controls when conducting cybersecurity audits: Insights from higher education institutions in Canada. *Electronics*, *13*(16), 3257. https://doi.org/10.3390/electronics13163257

Sudarmadi, D. (2023). Forensic accounting and investigative audit on the effectiveness of implementing audit procedures in fraud disclosure. *JASa (Jurnal Akuntansi, Audit Dan Sistem Informasi Akuntansi)*, *7*(2), 2350. https://doi.org/10.36555/jasa.v7i2.2350

Sumardi, Rahmadi, H., & Darminto, D. P. (2025). Sinergi akuntansi forensik, audit investigatif, dan budaya organisasi terhadap pencegahan dan pengungkapan fraud: Sebuah systematic literature review. *EKUILNOMI: Jurnal Ekonomi Pembangunan*, *7*(3), 912–922. https://doi.org/10.36985/e23vfs45

Suryani, I., & Syahrudin, M. (2025). Investigative auditing and fraud: A systematic literature review through a theoretical and bibliometric lens. *Asia Pacific Fraud Journal*, *10*(1), 139–151. https://doi.org/10.21532/apfjournal.v10i1.400

Thanasas, G., Kampiotis, G., & Halkiopoulos, C. (2026). Transforming digital accounting: Big Data, IoT, and Industry 4.0 technologies—A comprehensive survey. *Journal of Risk and Financial Management*, *19*(1), 92.

Tharwat, H., Hafez, S. T., Elgohary, I. E., & Hassanein, A. (2025). A decade of cybersecurity research in internal auditing: Bibliometric mapping and future research agenda. *Discover Sustainability*, *6*, 1066. https://doi.org/10.1007/s43621-025-02031-w

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Managemen*, *14*, 207–222. https://doi.org/https://doi.org/10.1111/1467-8551.00375

Umbet, M., Askarov, D., Rudžionienė, K., Christauskas, Č., & Alikulova, L. (2025). Evaluating the implementation of information technology audit systems within tax administration: A risk governance perspective for enhancing digital fiscal integrity. *Journal of Risk and Financial Management*, *18*(8), 422. https://doi.org/10.3390/jrfm18080422

Wadesango, N., & Maveneka, E. (2025). Cyberthreats and their impact on financial integrity: Evaluating the effectiveness of local authorities' cybersecurity policies in preventing and detecting fraud. *Corporate Law & Governance Review*, *7*(2), 32–40. https://doi.org/10.22495/clgrv7i2p3

Xu, D., Gondal, I., Yi, X., Susnjak, T., Watters, P., & McIntosh, T. R. (2025). The erosion of cybersecurity zero-trust principles through generative AI: A survey on the challenges and future directions. *Journal of Cybersecurity and Privacy*, *5*(4), 87. https://doi.org/10.3390/jcp5040087