JURNAL AKUNTANSI
Volume 18 Nomor 2, November 2023 173 - 183
http://jurnal.unsil.ac.id/index.php/jak
ISSN: 1907-9958 (Print)| 2385-9246 (Online)

THE ROLE OF TECHNOLOGY IN DETECTING CYBER RISK AND IMPROVING INTERNAL AUDIT: A SYSTEMATIC REVIEW

Nadya Annisa N[a]*, Grace T. Pomtoh[b], Andi Kusumawati[c]

[a] Universitas Hasanuddin, Indonesia
[b] Universitas Hasanuddin, Indonesia
[c] Universitas Hasanuddin, Indonesia
**nadyaanisa28@gmail.com*

***Diterima**: April 2023. **Disetujui**: April 2023. **Dipublikasi**: November 2023*

ABSTRACT

This research aims to explore the literature that examines the role of technology in assisting cyber risk detection and improving company internal audits in the digital era. The method used in this research is a systematic literature review (SLR). Data samples collected using the Watase-Uake database and articles from other sources with the Q1-Q4 index starting from 2014-2023. The selected articles have passed several specified criteria to produce a total number of 25 articles. The result shows that technology plays an important role in increasing the efficiency and effectiveness of cyber risk detection and internal audit processes. This research contributes to providing an overview regarding the benefits of technology in helping companies detect cyber risks and improve the quality of their internal audits

***Keywords:** Technology, Detecting Cyber Risk, Internal Audit*

ABSTRAK

Penelitian ini bertujuan untuk menggali literatur yang mengkaji peran teknologi dalam membantu deteksi risiko *cyber* dan meningkatkan audit internal perusahaan di era digital. Metode yang digunakan dalam penelitian ini adalah *sistematic literature review* (SLR). Pengambilan sampel data menggunakan data Watase-Uake dan artikel dari sumber lain dengan indeks Q1-Q4 mulai tahun 2014-2023. Artikel terpilih telah melewati beberapa kriteria yang ditentukan sehingga menghasilkan total 25 artikel. Hasilnya menunjukkan bahwa teknologi berperan penting dalam meningkatkan efisiensi dan efektivitas deteksi risiko siber dan proses audit internal. Penelitian ini berkontribusi untuk memberikan gambaran mengenai manfaat teknologi dalam membantu perusahaan mendeteksi risiko *cyber* dan meningkatkan kualitas audit internalnya.

Kata Kunci: Teknologi, Pendeteksian Risiko Siber, Audit Internal

PENDAHULUAN

Internet sebagai jaringan global yang kompleks telah mengubah dan merevolusi dunia dalam hal bertukar informasi (Bonsón & Bednárová, 2019). Transformasi ini mengantarkan dunia ke dalam suatu era percepatan dan tentunya membutuhkan adaptasi yang cepat terhadap perkembangannya. Berkembangnya koneksi seluler, komputasi awan, pertumbuhan big data yang cepat, serta kecerdasan artifisial menjadi penggerak akselerasi digital yang selain itu juga berperan penting di dalam menjalankan fungsinya untuk memperluas akses publik terhadap data digital (Korol et al., 2022).

Lingkungan teknologi modern yang selalu berubah mendorong seluruh unit ekonomi untuk bergerak ke arah transformasi digital seperti misalnya di ranah keuangan kini timbul permintaan atas pelayanan atas dasar kenyamanan dan efektif secara biaya. Begitupun generasi muda yang semakin tertarik dalam penggunaan teknologi termasuk internet dan platform digital yang menandai pergerakan konsumen ke era keuangan digital (Jain & Raman, 2022; Kitsios et al., 2021).

Dibalik keuntungan yang dijanjikan, akan selalu ada sisi menantang dari fenomena transformasi digital yang tidak akan bisa dipisahkan. Bagaimanapun juga, perubahan yang cepat ini memicu makin maraknya risiko dan *cybercrime* (Chang et al., n.d.; Slapničar et al., 2022; Tiberius & Hirth, 2019). Risiko tersebut menyebar disebabkan berbagai alasan yang tidak terbatas hanya pada *fraud* keuangan semata, namun juga meliputi pencurian atau penyalahgunaan informasi, tidak kegagalan operasional sistem informasi, dan penyabotasean infrastruktur operasional dan pelayanan. (the impacts of foreignness) (PwC, n.d.). Tentu hal ini membutuhkan beberapa penyesuaian dan perlakuan khusus di dalam proses internal audit mengingat rumitnya pengendalian risiko semacam ini.

Adapun perusahaan dan profesi audit itu sendiri diharuskan untuk beradaptasi terhadap perkembangan teknologi seperti analisis big data, *artificial intelligence* (AI), dan teknologi *blockchain* (Tiberius & Hirth, 2019). Selain itu metode baru dari analisis data menyediakan kesempatan kepada peningkatan keakuntabilitasan audit keuangan serta mengatasi keterbatasan dari prosedur audit konvensional. Implementasi dari metode tersebut meningkatkan realibilitas auditor yang dibuktikan dengan semakin bergesernya prosedur audit manual (Korol et al., 2022).

Meski sedemikian banyaknya disebutkan kepentingannya, tinjauan teknologi untuk bidang audit terbilang jarang (Tiberius & Hirth, 2019). Pada akhirnya, keseluruhan aktivitas dan peran dari auditor internal akan berubah dan dengan mempelajari audit berkelanjutan, akan semakin terlihat bahwa metodologi audit membutuhkan inovasi teknologi untuk melaksanakan fungsinya sebaik mungkin dibandingkan dengan internal audit tradisional. Sehingga didapati kesimpulan bahwa internal audit di era digital akan mengubah ruang lingkup, peran, dan fungsi internal audit. Oleh karenanya manajemen senior cenderung lebih menyukai fungsi audit internal dalam memerani aktivitas konsultasi guna mendukung manajemen dalam menghadapi tantangan teknologi dibandingkan peran internal audit sebelumnya yang hanya menjadi pengontrol aktivitas manjemen (Betti & Sarens, 2021).

Ekonomi digital sangat berbahaya dan memerlukan pendekatan yang penuh kehati-hatian untuk menghindari atau meminimalisir terjadinya risiko (Chen,

https://doi.org/10.37058/jak.v18i2.7675

2022). Sedangkan kenyataannya sangat banyak auditor internal yang kurang mahir terhadap teknologi informasi dalam menggunakan sistem model analisis (Chang et al., n.d.; Si, 2022). Hal ini mendorong banyak penelitian yang mendukung pentingnya pelatihan kecakapan TI untuk meningkatkan kualitas audit (Bonsón & Bednárová, 2019; Johari et al., 2022; Lois et al., 2020; Plant et al., 2022).

Disamping meningkatkan kualitas auditor internal, pemanfaatan teknologi diharapkan dapat bersinergi sebagaimana peneliti-peneliti sebelumnya banyak mengusulkan kerangka kerja dan sistem yang dapat membantu auditor internal dalam melaksanakan perannya khususnya memberikan kepastian bagi manajemen. Sistem-sistem yang diusulkan ini kemudian akan diklasifikasikan sesuai dengan peruntukan dan lingkup pengoperasiannya sebagai berikut; (1) sistem pemrosesan audit digital pada lingkup departemen, (2) sistem mitigasi risiko siber pada lingkup blockchain, dan (3) sistem mitigasi risiko siber pada pembayaran digital. Pendekatan menggunakan paradigma DevOps,FAHP-MCGP,MOIP-GA, dan data driven intelligent risk system diusulkan sebagai pendekatan untuk mengoptimalkan audit digital serta memitigasi dan mengelola risiko audit (Akinbowale et al., 2022; Plant et al., 2022; Wang et al., 2021; Xie & Zhang, 2022). Di lingkup *blockchain technology* beberapa penelitian menyebutkan sistem seperti *a resilient micro-payment infrastructure* dan algoritma DNN untuk memerankan peran mitigasi *cyber risk* (Bel et al., n.d.; Chen, 2022). Adapun mitigasi *cyber risk* pada ranah pembayar digital diperkenalkan melalui 5 *model learning: algoritma logistic regression, decision tree, K-nearest neighbors, random forest, dan autoencoder* (Chang et al., n.d.).

Berdasarkan pendahuluan tersebut, peneliti membangun pertanyaan penelitian yaitu; Bagaimana pengelolaan risiko siber dan peran internal audit di era digitalisasi?

Peneliti melihat adanya fenomena risiko siber dan pergeseran peran internal audit di era digitalisasi yang membutuhkan review literatur untuk memperkaya subyek tersebut. Tujuan penelitian ini adalah untuk menyediakan pembahasan terstruktur bagi peneliti dan ahli bidang yang berkaitan dengan korelasi audit dan bisnis digital

METODE PENELITIAN

Review literatur sistematis (SLR) merupakan metode penelitian yang banyak digunakan khususnya di dalam riset bisnis dan sistem informasi guna menemukan seni dari pembuatan suatu topik penelitian dan membangun pengetahuan berdasarkan bukti empiris serta dapat menjadi panduan bagi peneliti dan ahli di area subyek yang diinvestigasi tersebut. Metode kajian literatur yang digunakan dalam penelitian ini adalah metode Prisma.

Pencarian lliteratur

Pada *review* literatur ini, peneliti menggunakan aplikasi Watase-Uake sebagai metode pengumpulan artikel. Aplikasi Watase menggunakan sumber basis data Scopus. Strategi pencarian spesifik meliputi kata kunci: *"internal audit", "technology", "cyber risk".*

Kriteria Elibilitas

Pada tahap identifikasi, peneliti memasukkan beberapa kata kunci yang memiliki kesesuaian dengan topik yang akan dibahas di dalam penelitian ini. Adapun kriteria tambahan yang diatur dalam proses identifikasi adalah cakupan tahun publikasi artikel yaitu dari tahun 2014-2023 dengan kualifikasi index quartil Q1-Q4.

https://doi.org/10.37058/jak.v18i2.7675

Skrining dan pemilihan

Artikel yang didapatkan dari proses identifikasi kemudian masuk ke dalam tahapan skrining dengan memfokuskan pada kualitas dan kesesuaian artikel dengan topik yang akan dibahas. Tulisan berupa hasil konferensi dan *review* literatur tidak dimasukkan ke dalam kriteria. Proses screening dilakun dengan memilih *"yes"* jika artikel sesuai dengan kriteria, *"no"* jika tidak sesuai dengan kriteria, dan *"maybe"* jika artikel masih dipertimbangkan. Aplikasi watase juga secara otomatis memisahkan artikel yang memiliki sitasi duplikasi.

Pada tahap ini, artikel yang telah terkumpul harus diakses melalui alamat DOI kemudian diunduh agar tercatat di dalam laporan Watase. Terdapat beberapa artikel yang berhasil diunduh dan adapula yang tidak memiliki akses yang terbuka sehingga untuk mencapai target artikel yang diharapkan, maka peneliti menambahkan artikel berindeks Scopus secara manual diluar dari aplikasi Watase.

HASIL DAN PEMBAHASAN

Berdasarkan proses pengumpulan data menggunakan aplikasi Watase, maka telah terkumpul sebanyak 25 artikel yang memiliki kesesuaian dengan dari peringkat artikel yang telah terkumpul.

Artikel yang diolah telah disesuaikan kata kunci spesifiknya berupa: *"internal audit", "technology",* dan *cyber risk"*. Kelemahan terletak pada artikel yang tidak dapat diakses, sehingga informasi yang tersedia terbatas pada akses yang terbuka. Berikut merupakan daftar artikel yang berhasil dianalisis:

Tabel 1 Sumber Jurnal

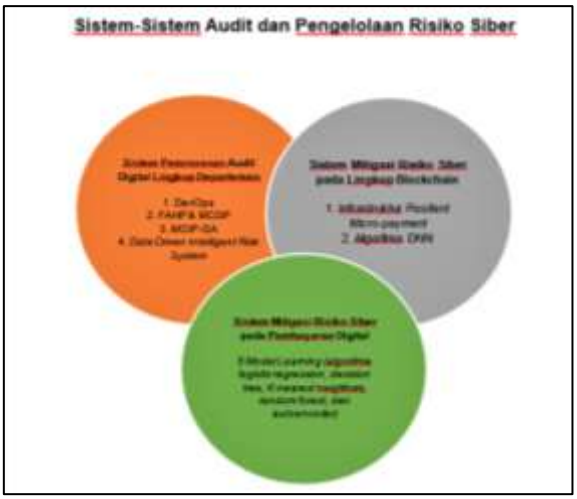
Jurnal	Penerbit	Jumlah Artikel
EuroMed Journal of Business	Emerald	1
Journal of Risk and Financial Management	MDPI	2
Journal of Accounting & Organizational Change	Emerald	1
International Journal of Accounting Information Systems	Elsevier	2
Computers & Industrial Engineering	Elsevier	1
European research on management and business economics	Elsevier	1
Journal of World Business	Elsevier	1
Journal of International Accounting, Auditing and Taxation	Elsevier	1
Cyberfraud mitigation	Emerald	2
Mathematical Problems in Engineering	Hindawi	1
Discrete Dynamics in Nature and Society	Hindawi	1
Complexity	Wiley Hindawi	1
Journal of Financial Services Marketing	Palgrave	1
Transfer of technologies: industry, energy, nanotechnology	Springer	1
Australasian Accounting, Business and Finance Journal	University of Wollongong Australia	1
Journal of Economics, Finance and Administrative Science	Emerald	1
Journal of Emerging Technologies in Accounting	Wiley	1
Meditary Accountancy Research	Emerald	1
Applied Energy	Elsevier	1

https://doi.org/10.37058/jak.v18i2.7675

Electronic Journal of Management & System	Elsevier	1
Applied Energy	Elsevier	1
Journal of Cleaner Production	Elsevier	1
Jumlah Artikel	25	

Sumber: Data Diolah (2023)

Setelah melakukan analisis dan



sintesis dari masing-masing artikel, maka dihasilkan temuan yang mendukung terkait peran teknologi dalam meningkatkan efektivitas dan efisiensi dalam pendeteksian risiko serta proses audit internal. Teknologi yang dalam hal ini diaplikasikan melalui penerapan sistem, metode, serta infrastruktur selanjutnya oleh peneliti diklasifikasikan berdasarkan 3 bagian sesuai lingkup penerapannya, yaitu: (1) sistem pemrosesan audit digital pada lingkup departemen, (2) sistem mitigasi risiko siber pada lingkup blockchain, dan (3) sistem mitigasi risiko siber pada pembayaran digital.

Gambar 1. Sistem Audit dan Pengelolaan Risiko Siber

Sumber: Data Diolah (2023).

Sistem Pemrosesan Audit Digital pada Lingkup Departemen

1. DevOps

Paradigma DevOps diusulkan sebagai panduan bagi perusahaan untuk memitigasi dan mengelola risiko dan kontrol di dalam lingkup internal departemen yang menerapkannya. Di dalam masa transisi kontrol internal ke era automasi, terlihat bahwa terdapat 2 faktor utama yang memengaruhi bagaimana departemen mengkonsepkan lingkungan DevOpsnya yaitu berdasarkan risk appetite dan kematangan DevOps. Selain itu, perusahaan cenderung menggabungkan kontrol TI manual dan kontrol terautomasi. DevOps memberikan keyakinan terhadap auditor dan pemangku kepentingan dalam upaya menerapkan manajemen risiko (Plant et al., 2022). Hasil ini sejalan dengan literatur terdahulu yang menyarankan kontrol preventif menggunakan DevOps sebab memungkinkan perusahaan untuk menjamin kualitas dan keamanan pada perangkat lunaknya (Mohan et al., 2018). Didukung dengan bukti bahwa banyaknya perusahaan yang sedang menjalankan pendekatan *hybrid* memperjelas pentingnya untuk tetap waspada dan terlibat dalam kontrol risiko berkelanjutan seperti yang disarankan oleh (Weber et al., n.d.) . (Plant et al., 2022) mengungkapkan bahwa DevOps pendekatan menghasilkan beberapa keunggulan dibandingkan metode pengembangan perangkat lunak tradisional.

2. *Fuzzy Analytic Hierarchy Process (FAHP) and Multi-Choice Goal Programming (MCGP)*

FAHP menjadi pendekatan yang populer untuk memecahkan masalah sosial dan ekonomi seperti di dalam penelitian (Ribas et al., 2019) sedangkan MCGP dapat memaksimalkan pemilihan keputusan sehingga tujuan dapat tercapai sedekat mungkin (Henry & Ravi Ravindran, 2005). Pendekatan FAHP-MCGP menjadi alat yang berguna untuk memilih proyek potensial dan alokasi waktu yang efektif

https://doi.org/10.37058/jak.v18i2.7675

selama perencanaan audit berbasis risiko guna mengoptimalkan fungsi preventif terhadap risiko (Wang et al., 2021). Hal ini sejalan dengan upaya peningkatan perencanaan internal audit yang efisien dan efektif di tengah fenomena digital yang serba cepat.

3. *Multi-Objectives Integer Programming Model (MOIP-GA)*

Kelayakan penerapan MOIP-GA untuk memaksimalkan alokasi sumber daya dan kapasitas pengelolaan *cyberfraud* (Akinbowale et al., 2022). Adapun GA di dalam model ini dianggap mampu memberikan solusi terhadap masalah yang tidak dapat diselesaikan dengan teknik lainnya (Barboza et al., 2016) MOIP-GA dapat mengatasi kekurangan diimplementasikan dengan baik maka akan mengatasi masalah kekurangan sumber daya manusia untuk merespon *cyberfraud* secara real time (Akinbowale et al., 2022).

4**.** *Data Driven Intelligent Risk System*

Audit keuangan perlu memecahkan masalah keterbatasan audit tradisional dengan memperbaiki pemahaman risiko dari tingkat perspektif makro (Xie & Zhang, 2022). Kontrol keuangan yang baik akan berkontribusi dalam inovasi ekonomi. Berdasarkan penelitian terkait data driven intelligent risk system, analisis risiko meningkat secara signifikan lebih dari 25% (Xie & Zhang, 2022).

Sistem Mitigasi Risiko Siber pada Lingkup Blockchain

1. *A Resilient Micro-payment Infrastructure*

Sistem pembayaran mikro sangat membutuhkan keamanan, efisiensi lebih tinggi, reaktivitas lebih baik, dan jaminan privasi (Bel et al., n.d.). (Pelc & Schwarzmann, 2015) memperlihatkan protokol pembayaran mikro yang menjamin keamanan dengan menggunakan hashed time-lock contracts sesuai kebutuhan keamanan, efisiensi, reaktivitas, dan privasi yang lebih baik. Infrastruktur yang mampu untuk: (1) mendeteksi perilaku menyimpang serta serangan dari pengguna, (2) menjadi pertahanan sebab mampu menganalisa risiko kehiangan yang terdeteksi, (3) mengurangi *delay* verifikasi pembayaran, mengontrol blok pada blockchain, serta mengeliminasi risiko kehingan akibat kesalahan *micro-payment,* dan (4) merespon serangan dengan sigap dan efektif (Bel et al., n.d.).

2. *Algoritma Deep Neutral Network (DNN)*

Algoritma DNN mampu memprediksi harga *bitcoin* dan mengurangi risiko keuangan (Chen, 2022). Prediksi yang akurat terhadap kurs digital menjadi kebutuhan darurat mengingat dampaknya terhadap komunitas ekonomi. DNN mampu menyelesaikan masalah model nonlinear dalam membuktikan kualitasnya dalam memprediksi *bitcoin* mengingat pentingnya *real time* di dalam proses akuisisi data dan analisis (Zhu et al., 2020).

Sistem Mitigasi Risiko Siber pada Pembayaran Digital

Lima *Model Learning: (algoritma logistic regression, decision tree, K-nearest neighbors, random forest, and autoencoder)* menjadi model yang stabil dan efektif untuk mendeteksi *fraud* (Chang et al., n.d.). Dari kelima model tersebut yang paling signifikan adalah model *random forest dan logistic regression*. (Fan et al., 2018) menunjukkan kesesuaian bahwa jaringan artifisial mampu menjadi metode dalam mendeteksi *fraud*. Hasil ini sesuai prediksi terkait keefektivitasannya sebagai metode untuk menghadapi masalah di era bisnis digital.

https://doi.org/10.37058/jak.v18i2.7675

Tabel 2. Keunggulan Sistem

Sistem/Metode	Keunggulan
Development Operational System	• Mempercepat kerja dan kualitas *software* • Membantu mitigasi dan pengelolaan risiko di departemen • Meningkatkan fungsi kontrol internal
FAHP & MCGP	• Mengoptimalkan prioritas proyek dan memaksimalkan waktu audit • Mengurangi risiko berdasarkan kategori risikonya • Memaksimalkan preferensi dan anggaran manajemen yang telah ditetapkan
MOIP-GA	• Mengoptimalkan mitigasi risiko siber • Memastikan keefektifitasan alokasi dan utilisasi sumber daya manusia
Data driven intelligent risk system	• Memberi peringatan ketika risiko mencapai batasan tertentu • Memperkuat koordinasi audit keuangan • Efektif secara waktu dan mampu menyediakan data yang berkualitas dan sistematis
Resilient risk micro-payment	• Menggunakan sistem *real time* • Memastikan kepercayaan pengguna dengan adanya riwayat dan pelacakan transaksi • Difasilitasi fitur verifikasi untuk perlindungan ganda
Algoritma DNN	• Mampu memprediksi harga Bitcoin dengan akurat • Mengurangi risiko transaksi digital
5 model learning	• Mendeteksi kecurangan pada transaksi digital • Meningkatkan keefektifitasan kontrol dan penggunaan eaktu dalam memitigasi risiko

Sumber: Data Diolah (2023).

Dengan demikian berdasarkan klasifikasi tersebut dapat dilihat bahwa risiko-risiko siber memiliki penanganan yang spesial yang disesuaikan dengan karakteristik masing-masing perusahaan atau organisasi tergantung dari keperluannya. Pada lingkup departemen, sistem dirancang sebagai pedoman dan infrastruktur oleh internal audit untuk mendeteksi dan mengelola risiko-risiko yang mungkin akan muncul. Langkah ini sangat membantu internal auditor untuk menyusun rencana dan strategi dalam perannya menyediakan informasi bagi manajer dalam membuat keputusan perusahaan oleh karenanya kini menjadi audit digital menjadi standar dalam proses audit (Tiberius & Hirth, 2019). Selanjutnya, sistem-sistem mitigasi di lingkup blockchain sebagaimana yang telah disebutkan diatas menjadi alat yang efektif dalam memastikan keamanan transaksi dan aktivitas bagi perusahaan yang bergerak di dalam area blockchain. Hal ini mengingat bahwa aktivitas di dalam *blockchain* dilakukan secara anonim dan digital yang sangat berbahaya dan harus didekati dengan kewaspadaan sehingga keamanan adalah hal yang utama dalam memastikan tidak adanya kebocoran maupun pencurian data yang akan sangat membahayakan bagi perusahaan (Chen, 2022). Lalu yang terakhir adalah sistem mitigasi pada pembayaran digital dimana pada era modern seperti sekarang transaksi yang melibatkan pertukaran uang sebagian besar telah beralih ke metode pembayaran non

https://doi.org/10.37058/jak.v18i2.7675

tunai. Fenomena tersebut tentu meningkatkan risiko lainnya yakni fraud atau kecurangan saat transaksi dan dengan adanya sistem seperti 5 model learning maka akan membantu tugas internal auditor dalam mendeteksi *fraud* dengan bantuan jaringan artifisial.

Tabel 3. Manfaat Teknologi Bagi Audit Internal

Manfaat Teknologi Secara Spesifik Bagi Audit Internal	
Kontrol internal	• Kontrol terautomatisasi (Bonsón & Bednárová, 2019; Plant et al., 2022; Si, 2022)
Proses audit	• Audit jarak jauh *(remote)* (Lois et al., 2020; Si, 2022) • Audit berkelanjutan (Bonsón & Bednárová, 2019; Korol et al., 2022; Lois et al., 2020; Tiberius & Hirth, 2019) • Fitur pelacakan item (Bel et al., n.d.; Plant et al., 2022) • Optimalisasi anggaran dan efisiensi waktu (Akinbowale et al., 2022; Bonsón & Bednárová, 2019; Kitsios et al., 2021; Korol et al., 2022; Sudarma & Kumalawati, 2022; Wang et al., 2021)
Keamanan	• Fitur kode keamanan (Bel et al., n.d.; Plant et al., 2022) • Pemisahan basis data dan aplikasi (Bonsón & Bednárová, 2019) • Analisis risiko/model ancaman (Bel et al., n.d.; Kitsios et al., 2021; Korol et al., 2022; Wang et al., 2021; Xie & Zhang, 2022)
Pengawasan	• Pengawasan berkelanjutan (Bel et al., n.d.; Si, 2022; Xie & Zhang, 2022) • Pelaporan dengan standar otomatis (Betti & Sarens, 2021; Bonsón & Bednárová, 2019)
Manajemen tim audit	• Memperjelas tugas dan tanggung jawab (Akinbowale et al., 2022; Eulerich et al., 2022; Korol et al., 2022; Wang et al., 2021) • Mendorong peningkatan kualitas komunikasi (Bonsón & Bednárová, 2019; Plant et al., 2022) • Tim otonom (Morales et al., 2022; Plant et al., 2022)

Sumber: Data Diolah (2023).

Sistem teknologi informasi di dunia bisnis kemudian menjadi revolusi yang sangat besar dalam memengaruhi pergeseran-pergeseran di bidang keakuntansian dan audit itu sendiri. Teknologi dan proses audit kini menjadi tidak terpisahkan sebagaimana di banyak kantor audit telah menerapkan program dan aplikasi seperti *Audit Command Language* atau *Interactive Data Extraction* and *Analysis, atau in-house software* seperti Aura oleh PwC atau eAudit oleh KPMG. Dalam melaksanakan auditnya (Tiberius & Hirth, 2019). Tentunya tidak terkecuali bagi perusahan-perusahaan yang juga melaksanakan auditnya secara internal. (Plant et al., 2022) dalam penelitiannya menyatakan bahwa sistem teknologi terbukti sangat baik dalam menjalankan tugas sebagai alat kontrol dan pengawasan sehingga berakibat pada ekspektasi terhadap peran auditor baik oleh klien maupun perusahaan. (Lois et al., 2020) menggaris bawahi beberapa fokus utama yang perlu dipenuhi auditor pada era digital yakni; kemampuan perlindungan data personal, pencegahan *cyber attack*, dan kompetensi personalisasi. Hal ini linear dengan penelitian (Betti & Sarens, 2021; Mat Ridzuan et al., 2022; Tiberius & Hirth, 2019) auditor yang memiliki kecakapan TI, profesional judgement, dan pengalaman akan mampu bersaing di tengah-tengah disrupsi tersebut dibandingkan auditor yang hanya mengandalkan kemampuan finansial.

https://doi.org/10.37058/jak.v18i2.7675

SIMPULAN

Peran sistem teknologi informasi di dalam lingkungan ekonomi dan bisnis merupakan sebuah kebaharuan yang tidak dapat terpisahkan lagi. Teknologi yang telah disusun dalam bentuk kerangka kerja, metode, serta sistem di dalam perusahaan ditujukan untuk mengefisiensikan aktivitas audit, menciptakan transparansi aset berwujud, optimalisasi anggaran, serta untuk memastikan keamanannya. Dibutuhkan keahlian dalam mengaplikasikan dan memahami output dari seluruh infrastruktur, algoritma, dan sistem tersebut oleh sebab itu auditor internal diharapkan mampu beradaptasi dan meningkatkan kecakapannya sehingga praktik audit menjadi efektif dan risiko-risiko yang ada mampu dikelola dengan baik. Perubahan-perubahan tersebut banyaknya mendorong pergeseran dalam peran auditor internal dari sebatas pemerhati dan pengendali hingga kini berperan menjadi konsultan perusahaan.

Hasil penelitian menjelaskan bahwa sistem-sistem digital telah dibangun oleh manajemen perusahaan dalam mendeteksi pelanggaran dan memberikan aturan preventif mengenai pengelolaan data dan keuangan. Namun, artikel-artikel yang ditemukan masih menggambarkan ruang lingkup perusahaan yang telah terdigitalisasi saja. Artikel terkait belum menjelaskan mengenai kriteria audit internal secara menyeluruh termasuk bahasan mengenai kasus hingga evaluasi manajemen, mengingat fungsi audit adalah sebagai wujud pengawasan manajemen. Sehingga, diharapkan kedepannya terdapat tambahan olahan referensi penelitian-penelitian yang lebih kaya dan jelas mengenai audit internal, terutama pada artikel-artikel yang memiliki akses terbatas.

REFERENSI

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2022). Development of a multi-objectives integer programming model for allocation of anti-fraud capacities during cyberfraud mitigation. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-10-2022-0245

Barboza, A. O., Junior, F. N., Bortolotti, S. L. V., & Souza, R. A. de. (2016). Programação Linear Inteira Mista e Algoritmo Genético aplicados ao Problema de Transferência e Estocagem de Produtos em uma Indústria Petrolífera. *Sistemas & Gestão*, *10*(4), 561–574. https://doi.org/10.20985/1980-5160.2015.v10n4.448

Bel, S., Youssef, H., & Boudriga, N. (n.d.). *A resilient micro-payment infrastructure: an approach based on blockchain technology*.

Betti, N., & Sarens, G. (2021). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting and Organizational Change*, *17*(2), 197–216. https://doi.org/10.1108/JAOC-11-2019-0114

Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. In *Meditari Accountancy Research* (Vol. 27, Issue 5, pp. 725–740). Emerald Group Holdings Ltd. https://doi.org/10.1108/MEDAR-11-2018-0406

Chang, V., Minh, L., Doan, T., Stefano, A. Di, Sun, Z., & Fortino, G. (n.d.). *Digital Payment Fraud Detection Methods in digital ages and Industry 4.0*.

https://doi.org/10.37058/jak.v18i2.7675

Chen, S. (2022). Cryptocurrency Financial Risk Analysis Based on Deep Machine Learning. *Complexity*, *2022*. https://doi.org/10.1155/2022/2611063

Eulerich, M., Pawlowski, J., Waddoups, N. J., & Wood, D. A. (2022). A Framework for Using Robotic Process Automation for Audit Tasks*. *Contemporary Accounting Research*, *39*(1), 691–720. https://doi.org/10.1111/1911-3846.12723

Fan, C., Xiao, F., Zhao, Y., & Wang, J. (2018). Analytical investigation of autoencoder-based methods for unsupervised anomaly detection in building energy data. *Applied Energy*, *211*, 1123–1135. https://doi.org/10.1016/j.apenergy.2017.12.005

Henry, T. M., & Ravi Ravindran, A. (2005). A Goal Programming application for Army Officer Accession Planning. *INFOR*, *43*(2), 111–119. https://doi.org/10.1080/03155986.2005.11732720

Jain, N., & Raman, T. V. (2022). A partial least squares approach to digital finance adoption. *Journal of Financial Services Marketing*, *27*(4), 308–321. https://doi.org/10.1057/s41264-021-00127-8

Johari, R. J., Mohd Razali, F., & Hashim, A. (2022). Enterprise Risk Management: Internal Auditor's Role Perspective. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *12*(1). https://doi.org/10.6007/ijarafms/v12-i1/11413

Kitsios, F., Giatsidis, I., & Kamariotou, M. (2021). Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(3). https://doi.org/10.3390/joitmc7030204

Korol, V., Dmytryk, O., Karpenko, O., Riadinska, V., Basiuk, O., Kobylnik, D., Moroz, V., Safronova, O., Alisov, E., & Mishchenko, T. (2022). ELABORATION OF RECOMMENDATIONS ON THE DEVELOPMENT OF THE STATE INTERNAL AUDIT SYSTEM WHEN APPLYING THE DIGITAL TECHNOLOGIES. *Eastern-European Journal of Enterprise Technologies*, *1*(13–115), 39–48. https://doi.org/10.15587/1729-4061.2022.252424

Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business*, *15*(2), 205–217. https://doi.org/10.1108/EMJB-07-2019-0097

Mat Ridzuan, N. I., Said, J., Razali, F. M., Abdul Manan, D. I., & Sulaiman, N. (2022). Examining the Role of Personality Traits, Digital Technology Skills and Competency on the Effectiveness of Fraud Risk Assessment among External Auditors. *Journal of Risk and Financial Management*, *15*(11). https://doi.org/10.3390/jrfm15110536

Mohan, V., Ben Othmane, L., & Kres, A. (2018). BP: Security concerns and best practices for automation of software deployment processes: An industrial case study. *Proceedings - 2018 IEEE Cybersecurity Development Conference, SecDev*

https://doi.org/10.37058/jak.v18i2.7675

2018, 21–28. https://doi.org/10.1109/SecDev.2018.00011

Morales, H. R., Porporato, M., & Epelbaum, N. (2022). Benford's law for integrity tests of high-volume databases: a case study of internal audit in a state-owned enterprise. *Journal of Economics, Finance and Administrative Science*, *27*(53), 154–174. https://doi.org/10.1108/JEFAS-07-2021-0113

Pelc, A., & Schwarzmann, A. A. (Eds.). (2015). *Stabilization, Safety, and Security of Distributed Systems* (Vol. 9212). Springer International Publishing. https://doi.org/10.1007/978-3-319-21741-3

Plant, O. H., van Hillegersberg, J., & Aldea, A. (2022). Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment. *International Journal of Accounting Information Systems*, *45*. https://doi.org/10.1016/j.accinf.2022.100560

PwC. (n.d.). *Shaping our future Our global network Our people Our revenues nues O O*. www.pwc.com/annualreview

PwC's-Global-Economic-Crime-and-Fraud-Survey-2022. (n.d.).

Ribas, J. R., Arce, M. E., Sohler, F. A., & Suárez-García, A. (2019). Multi-criteria risk assessment: Case study of a large hydroelectric project. *Journal of Cleaner Production*, *227*, 237–247. https://doi.org/10.1016/j.jclepro.2019.04.043

Si, Y. (2022). Construction and Application of Enterprise Internal Audit Data Analysis Model Based on Decision Tree Algorithm. *Discrete Dynamics in Nature and Society*, *2022*. https://doi.org/10.1155/2022/4892046

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*. https://doi.org/10.1016/j.accinf.2021.100548

Sudarma, M., & Kumalawati, L. (2022). Professional Considerations for Audit Risk in Creating Smart Governance in Indonesia. In *Sudarma & Kumalawati | Professional Considerations for Audit Risk* (Vol. 16, Issue 4).

Tiberius, V., & Hirth, S. (2019). Impacts of digitization on auditing: A Delphi study for Germany. *Journal of International Accounting, Auditing and Taxation*, *37*. https://doi.org/10.1016/j.intaccaudtax.2019.100288

Wang, X., Zhao, T., & Chang, C. Ter. (2021). An integrated FAHP-MCGP approach to project selection and resource allocation in risk-based internal audit planning: A case study. *Computers and Industrial Engineering*, *152*. https://doi.org/10.1016/j.cie.2020.107012

Weber, C., Bierwolf, R., Holzmann, T., IEEE Technology and Engineering Management Society., & Institute of Electrical and Electronics Engineers. (n.d.). *Proceedings of the 2017 IEEE European Technology and Engineering Management Summit (E-TEMS) : "Digital Innovation for Advanced Manufacturing, Managing Technological and Entrepreneurial Challenges" : Oktober, 2017*.

Xie, T., & Zhang, J. (2022). Data-Driven Intelligent Risk System in the Process

https://doi.org/10.37058/jak.v18i2.7675

of Financial Audit. *Mathematical Problems in Engineering*, *2022*. https://doi.org/10.1155/2022/9054209

Zhu, H., Sun, J., Xu, L., Tian, W., & Sun, S. (2020). Permittivity Reconstruction in Electrical Capacitance Tomography Based on Visual Representation of Deep Neural Network. *IEEE Sensors Journal*, *20*(9), 4803–4815. https://doi.org/10.1109/JSEN.2020.2964559

https://doi.org/10.37058/jak.v18i2.7675