Jurnal Cybernetic Inovatif Vol.9 No.12, November 2025

PENGEMBANGAN KERANGKA KERJA MANAJEMEN RISIKO UNTUK ORGANISASI BERBASIS DIGITAL: SINERGI MULTIDISIPLIN DAN KETAHANAN SIBER

Nadia Arsita Handayani[1], Elni Dwi Putri[2], Mia Faradila[3], Riska Fitria Rahmadani[4], Illiya Faiza[5], Reffy Angellina[6]
UIN STS Jambi
E-mail: nadiaarsita554@gmail.com[1], elnidwiputri363@gmail.com[2], miafaradilaazwar@gmail.com[3], riskafitria133@gmail.com[4], illiyafaiza02@gmail.com[5], onyourrreffy2@gmail.com[6]

Abstrak

Transformasi digital (DT) telah meningkatkan risiko dengan kompleksitas yang cepat meningkat di era Industri 4. 0. Situasi ini mengharuskan organisasi beralih dari manajemen risiko yang reaktif ke pendekatan yang lebih proaktif, terpadu, dan berfokus pada ketahanan siber. Artikel ini bertujuan untuk merancang kerangka kerja manajemen risiko (MR) yang komprehensif melalui integrasi studi dari berbagai disiplin ilmu. Analisis ini menekankan pentingnya sinergi antara Hukum (untuk kepatuhan dan pengelolaan risiko kontraktual), Teknik Industri (untuk metode analisis, prinsip efisiensi, dan lean), serta Teknologi Informasi (TI) (untuk aspek keamanan dan standar sistematis). Kerangka kerja ini sangat penting untuk mengurangi ancaman cyber-physical di era Industri 4. 0, risiko dalam rantai pasok digital, serta pelanggaran kebijakan. Keberhasilan dalam penerapan sangat dipengaruhi oleh faktor manusia, terutama Kepemimpinan Adaptif dan kultur yang mendukung Learning Agility serta Psychological Safety. Kerangka yang diusulkan menggabungkan model tata kelola (GCG) dan standar teknis (ISO 31000, COBIT, NIST) untuk memastikan transparansi finansial, ketahanan siber fisik, serta kemampuan organisasi untuk beradaptasi.

Kata Kunci — Manajemen Risiko, Transformasi Digital, Kepemimpinan Adaptif, Keamanan Siber, Learning Agility.

Abstract

Digital Digital transformation (DT) has increased risks with rapidly increasing complexity in the era of Industry 4.0. This situation requires organizations to shift from reactive risk management to a more proactive, integrated, and cyber-resilient approach. This article aims to design a comprehensive risk management (RM) framework through the integration of studies from various disciplines. This analysis emphasizes the importance of synergy between Law (for compliance and contractual risk management), Industrial Engineering (for analysis methods, efficiency principles, and lean), and Information Technology (IT) (for security aspects and systematic standards). This framework is crucial for mitigating cyber-physical threats in the Industry 4.0 era, risks in the digital supply chain, and policy violations. Successful implementation is highly influenced by human factors, particularly Adaptive Leadership and a culture that supports Learning Agility and Psychological Safety. The proposed framework combines governance models (GCG) and technical standards (ISO 31000, COBIT, NIST) to ensure financial transparency, cyber-physical resilience, and organizational adaptability.

Keywords *— Risk Management, Digital Transformation, Adaptive Leadership, Cyber Security, Learning Agility.*

PENDAHULUAN

Gelombang Transformasi Digital (DT), yang didorong oleh Revolusi Industri 4.0, telah mengubah cara bisnis dan operasional organisasi berjalan secara mendasar. Kini, organisasi sangat bergantung pada teknologi informasi, sistem cloud, dan jaringan cyber-physical (OT), tetapi hal ini juga membawa risiko yang semakin rumit dan kompleks (Mulianingsih, Fajar, & Suharyati, 2025; Nufuz et al., 2025). Risiko di era digital tidak lagi hanya berupa ancaman yang statis atau terbatas pada operasional biasa, melainkan memiliki ciri khas yang bisa mengancam kelangsungan hidup organisasi, seperti kemampuan berkembang pesat, dampak yang melintasi batas, dan hubungan yang saling tergantung (Wala, 2025). Kompleksitas risiko ini mencakup beberapa aspek, seperti ancaman siber yang semakin canggih (seperti ransomware yang menyerang infrastruktur kritis), risiko pelanggaran aturan data (seperti GDPR atau UU PDP), serta kerentanan dalam rantai pasok digital yang kini sering menjadi target serangan baru (Mulianingsih, Fajar, & Suharyati, 2025). Kegagalan dalam mengelola risiko dapat menyebabkan kerugian besar, pelanggaran data, gangguan dalam operasional, hingga hilangnya reputasi dan kepercayaan dari para pemangku kepentingan (Muliati, Supriadi, & Junaedi, 2025). Selain itu, kelemahan dalam sistem juga bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab, sehingga penting adanya kerja sama antara Good Corporate Governance (GCG) dan manajemen risiko untuk mencegah penipuan sejak dini (Febriansyah, Nasruddin, & Darni, 2025). Menghadapi tantangan ini, pendekatan manajemen risiko yang hanya reaktif, terpisah, dan hanya fokus pada penanganan insiden secara individual, ternyata tidak lagi cukup (Muliati, Supriadi, & Junaedi, 2025). Di era cyber-physical, kerangka manajemen risiko harus berubah menjadi model yang menyeluruh, proaktif, dan berfokus pada ketahanan (resilience), bukan hanya pencegahan (Mulianingsih, Fajar, & Suharyati, 2025). Kebutuhan ini mendorong perlu adanya penyatuan pengetahuan dan metode dari berbagai bidang ilmu untuk membangun kerangka kerja yang lengkap (Wala, 2025).

Oleh karena itu, artikel ini mengusulkan integrasi sinergis dari tiga pilar utama sebagai solusi dalam membangun kerangka manajemen risiko digital yang kuat. Pilar pertama adalah Pendekatan Hukum, yang diperlukan untuk membentuk aturan yang jelas, memastikan kepatuhan terhadap regulasi yang terus berubah, melindungi aset digital dan data, serta menyediakan alat kontrak seperti Service Level Agreement (SLA) untuk membagi risiko secara jelas (Wala, 2025). Pilar kedua adalah Pendekatan Teknik Industri, yang memberikan metode analisis, prinsip manajemen yang efisien, serta teknik penilaian risiko kuantitatif seperti Failure Mode and Effects Analysis (FMEA), untuk memperbaiki proses bisnis, meningkatkan efisiensi, dan mengembangkan sistem yang mencegah kesalahan (Poka-Yoke) (Wala, 2025). Pilar ketiga adalah Pendekatan Teknologi Informasi (TI), yang fokus pada keamanan siber, penggunaan framework sistematis seperti COBIT 5, ISO 31000, atau NIST untuk mengelola risiko TI, serta membantu pengambilan keputusan berbasis data melalui sistem manajemen risiko yang terintegrasi (Illah & Ilham, 2025; Muliati, Supriadi, & Junaedi, 2025). Integrasi harmonis dari ketiga pilar ini adalah fondasi yang mentransformasi manajemen risiko dari fungsi kepatuhan yang terfragmentasi menjadi kapabilitas strategis yang adaptif. Selain pilar teknis dan struktural, keberhasilan digitalisasi dan manajemen risiko juga bergantung pada faktor manusia (Nufuz et al., 2025) Penelitian menunjukkan bahwa organisasi harus memiliki kepemimpinan yang adaptif, bisa mengambil keputusan cepat dan fleksibel di tengah ketidakpastian (Setiyowati, 2025). Kepemimpinan seperti ini harus didukung oleh budaya organisasi yang mendorong kemampuan belajar dan beradaptasi para karyawan terhadap teknologi baru, serta menciptakan lingkungan yang aman secara psikologis untuk mendorong eksperimen dan inovasi (Sari et al., 2025). Kegagalan seringkali berasal dari resistensi dan kurangnya keahlian sumber daya manusia, yang bisa diatasi dengan mengintegrasikan manajemen

risiko dalam program pengembangan SDM (Rizkyah et al., 2025).

TINJAUAN LITERATUR

Manajemen Manajemen risiko dalam organisasi digital memerlukan keseimbangan antara kepatuhan terhadap hukum dan efisiensi serta keandalan dalam operasional. Perubahan digital telah mempengaruhi cara risiko muncul, menjadikannya lebih terintegrasi dan sistematik. Risiko di era digital kini bukan hanya masalah kegagalan sistem yang lama, tapi telah berkembang menjadi ancaman cyber-physical yang dapat berdampak pada dunia nyata. Ketergantungan kita pada teknologi informasi menjadikan kita lebih rentan terhadap ancaman siber yang semakin kompleks. Risiko ini tidak lagi hanya menyerang sistem secara individual, tetapi juga dapat mengganggu seluruh jaringan industri dan sistem Teknologi Operasional. Hal ini dapat mengancam perkembangan Industri 4. 0, di mana serangan ransomware dapat mengganggu proses produksi secara fisik. Kerugian finansial yang ditimbulkan sangat signifikan, dengan rata-rata kerugian global mencapai 4,35 juta dolar untuk setiap insiden kebocoran data. Di samping itu, ancaman juga dapat muncul dari faktor internal, seperti kegagalan sistem atau kesalahan manusia. Saat ini, manajemen risiko harus menghadapi kerumitan hukum terkait privasi data yang ketat di berbagai yurisdiksi. Selain itu, risiko operasional dalam rantai pasok digital menjadi semakin penting, mengingat keterlibatan pihak ketiga yang membentuk titik lemah di seluruh sistem. Jika tidak dikelola dengan baik, risiko ini dapat mengakibatkan denda serta gangguan operasional yang dampaknya sangat besar.

Untuk menghadapi risiko yang rumit ini, organisasi mengandalkan kerangka yang terstruktur. ISO 31000:2018 menawarkan panduan dan prinsip umum untuk mengelola berbagai bentuk risiko secara teratur, terbuka, dan dapat dipercaya. Standar ini menekankan pendekatan yang berlandaskan probabilitas dan mendukung organisasi dalam mengintegrasikan manajemen risiko ke dalam semua tahap pengambilan keputusan. COBIT 5/2019 berfokus terutama pada tata kelola dan manajemen risiko teknologi informasi. COBIT 5 efektif dalam mendeteksi kekurangan dalam kemampuan manajemen risiko TI, khususnya dalam domain seperti EDM03 (Optimasi Risiko) dan APO12 (Pengelolaan Risiko). Audit yang dilakukan dengan COBIT sering kali mengindikasikan perlunya perbaikan pada kemampuan pengelolaan risiko TI dari status saat ini ke tingkat yang lebih berkembang. Di pihak lain, Kerangka NIST memberikan pendekatan dasar untuk keamanan siber dan ketahanan. Kerangka ini mencakup lima fungsi penting yang harus dilaksanakan secara terus-menerus: Identifikasi, Perlindungan, Deteksi, Tanggapan, dan Pemulihan. Selain kerangka teknis, model adopsi teknologi seperti TAM (Model Penerimaan Teknologi) dan UTAUT 2 (Teori Terpadu Penerimaan dan Penggunaan Teknologi) berperan dalam memahami elemen yang memengaruhi penerimaan pengguna terhadap layanan digital (seperti persepsi kemudahan dan keuntungan), yang sangat penting untuk membangun kepercayaan dan penerimaan. Pendekatan Pendekatan luas dalam manajemen risiko muncul sebagai hasil dari kolaborasi yang kokoh di antara berbagai disiplin. Sinergi antara bidang Hukum dan Teknik Industri membawa kepada metode yang melampaui sekadar kepatuhan formal, yaitu Compliance by Design. Sumbangan dari Hukum menawarkan perlindungan untuk aset digital, menyediakan kerangka hukum, dan memanfaatkan perjanjian kontrak (SLA) sebagai sarana utama dalam mengelola serta mengurangi risiko yang berhubungan dengan kontrak. Di sisi lain, Teknik Industri menyumbangkan metode analisis proses (seperti FMEA dan Pemetaan Proses) serta prinsip manajemen Lean (seperti Poka-Yoke atau pencegahan kesalahan) untuk meminimalkan risiko pemborosan dan meningkatkan performa sistem. Kolaborasi ini memberi manfaat yang signifikan, yakni pengurangan biaya insiden rata-rata hingga 43% dan peningkatan

efisiensi proses kepatuhan sampai 27%. Fundamental dalam manajemen risiko adalah Good Corporate Governance (GCG). Penerapan prinsip-prinsip GCG seperti akuntabilitas, transparansi, dan independensi dapat secara signifikan menekan elemen "peluang" dalam segitiga penipuan (Fraud Triangle), sehingga berfungsi sebagai alat pencegahan penipuan yang efektif. Sistem manajemen risiko, khususnya Enterprise Risk Management (ERM), yang terhubung dengan GCG, berfungsi sebagai alat deteksi dini yang secara sistematis mengurangi risiko penipuan finansial.

Faktor manusia dan budaya memainkan peran krusial serta sering kali menjadi penyebab utama kegagalan dalam transformasi digital. Di tengah era yang serba berubah, kepemimpinan dituntut untuk bersifat fleksibel dan dapat merubah diri. Kepemimpinan yang adaptif sangat diperlukan untuk menghadapi situasi yang tidak stabil dan penuh ketidakpastian, didukung oleh praktik manajemen risiko serta transformasi digital. Keberhasilan dalam jangka panjang sangat tergantung pada kemampuan individu untuk belajar secara terus-menerus dan beradaptasi. Kemampuan untuk belajar dengan cepat menjadi penting untuk mempercepat perubahan dalam perilaku karyawan sehingga sejalan dengan kompetensi digital yang diperlukan. Membangun lingkungan yang aman secara psikologis adalah syarat utama untuk membentuk budaya inovatif, di mana karyawan merasa aman untuk mencoba hal-hal baru, bereksperimen, dan mengambil pelajaran dari kesalahan. Organisasi juga perlu menginvestasikan sumber daya dalam pelatihan dan pengembangan karyawan guna menciptakan kompetensi hibrida, yaitu kemampuan untuk menyatukan keahlian digital dengan pengetahuan operasional serta keterampilan sosial. Hal ini sangat relevan dalam pengelolaan sumber daya manusia untuk meningkatkan efektivitas pelatihan yang didasarkan pada pendekatan berbasis risiko.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-deskriptif dengan metode Studi Literatur Sistematis (Systematic Literature Review/SLR). Metode SLR dipilih karena dianggap paling sesuai untuk mengidentifikasi, mengevaluasi, dan menyatukan hasil dari penelitian-penelitian primer yang relevan dan sudah dipublikasikan. Tujuannya utamanya adalah membentuk kerangka konseptual yang komprehensif (teori tingkat menengah) di tengah kompleksitas manajemen risiko digital yang terus berubah. Data dikumpulkan melalui pencarian yang luas pada basis data akademik terkemuka seperti Scopus, Google Scholar, ScienceDirect, dan IEEE Xplore, serta laporan teknis industri yang dapat dipercaya. Proses pemilihan literatur dilakukan berdasarkan kriteria yang ketat. Kriteria Inklusi Berdasarkan Waktu mengharuskan publikasi yang digunakan harus bersifat terbaru, yaitu diterbitkan dalam lima (5) tahun terakhir (2020 hingga 2025), sesuai dengan kebutuhan ilmiah untuk merujuk pada perkembangan pengetahuan terkini di masa digital yang terus berkembang. Selain itu, publikasi harus bersifat primer, seperti artikel jurnal ilmiah atau prosiding konferensi, dan mengandung kata kunci spesifik yang relevan dengan topik yang diteliti. Sebagai Kriteria Eksklusi, artikel yang bersifat sekunder, buku teks, atau publikasi yang tidak melewati proses peer-review yang ketat (seperti blog atau white paper biasa), tidak termasuk, kecuali laporan teknis dari lembaga standar seperti NIST atau ISO. Setelah seleksi, diperoleh 11 artikel ilmiah primer yang sangat relevan, membahas topik multidisiplin seperti Hukum, Teknik Industri, dan Teknologi Informasi.

Analisis dilakukan secara sistematis dan berulang, menggabungkan teknik Analisis Konten (Content Analysis) dan Sintesis Tematik untuk mencapai pemahaman konseptual yang dalam. Proses ini dibagi menjadi beberapa tahap. Pada tahap awal, kata kunci spesifik digunakan untuk memetakan cakupan literatur. Fokus pada "Manajemen Risiko", "Transformasi Digital", "Kepemimpinan Adaptif", dan "Keamanan Siber" memastikan data yang diperoleh mencakup dimensi teknologi, kebijakan, dan faktor manusia. Data yang diekstrak mencakup metode penelitian, temuan utama, dan kerangka konseptual yang

diajukan oleh setiap studi. Selanjutnya, dilakukan reduksi data untuk memisahkan informasi penting dari informasi yang hanya menjelaskan konteks. Informasi inti tersebut kemudian dibagi ke dalam empat dimensi strategis utama: Teknologi dan Arsitektur (membahas topik seperti Zero Trust, Cyber Resilience, serta teknologi pendukung lainnya seperti AI dan OT); Organisasi dan Proses (meliputi perbandingan model MRTI seperti ISO 31000, COBIT 5, dan NIST, serta penerapan prinsip Teknik Industri seperti Lean Management dan Poka-Yoke dalam proses operasional digital); Faktor Manusia (mencakup variabel seperti perilaku, budaya, dan kemampuan, termasuk Learning Agility dan Psychological Safety); dan Tata Kelola (mencakup sinergi antara GCG dan MR dalam mencegah fraud serta mengatur risiko kontraktual).

Tahap terakhir adalah Analisis Tematik Mendalam dan Sintesis Kerangka Konseptual. Tahap ini merupakan bagian terpenting dari SLR, di mana hasil kategori yang sudah diperoleh disusun ulang untuk membentuk argumen yang konsisten dan kerangka kerja baru. Analisis berfokus pada Integrasi Model Perubahan, menggabungkan temuan tentang manajemen perubahan yang berhasil, khususnya sinergi antara model struktural (top-down) seperti Kotter's 8-Step Model dan model berbasis individu (bottom-up) seperti ADKAR. Hasilnya adalah Perumusan Kerangka Konseptual MR digital yang terpadu, yang tidak hanya menyarankan penggunaan standar teknis tetapi juga menekankan pentingnya Kepemimpinan Adaptif sebagai penggerak utama Learning Agility dan budaya yang mendukung ketahanan siber sebagai hasil dari kolaborasi antar disiplin. Proses analisis yang mendalam dan terstruktur ini memastikan kerangka kerja yang dihasilkan memiliki validitas internal yang kuat, didukung oleh bukti terbaru dari literatur akademik yang relevan.

HASIL DAN PEMBAHASAN

Kerangka kerja MR digital yang efektif harus bergerak dari keamanan berbasis perimeter statis menuju arsitektur pertahanan berlapis, berfokus pada Zero Trust dan Ketahanan Cyber-Physical. Strategi ini melibatkan lima dimensi inti:

Tabel 1: Kerangka Kerja MR Digital Integratif dan Ketahanan Siber.

Dimensi Strategis	**Fokus Kontribusi Multi-Disiplin**	**Keterkaitan Model**
Intelijen Ancaman Proaktif	TI/MRTI: Pemantauan berkelanjutan, Analisis anomali bertenaga AI.	NIST (Deteksi) + Teknik Industri (Analisis Prediktif)
Keamanan-sejak-Desain	Hukum: *Compliance by Design*. Teknik Industri: *Poka-Yoke*	ISO 31000 (Prinsip) + Hukum (Kepatuhan Intrinsik)
Infrastruktur Berfokus Ketahanan	TI/MRTI: Arsitektur *Zero Trust*, segmentasi jaringan, prosedur pemulihan khusus OT.	COBIT 5 (DSS - *Manage Operations*) + Teknik Industri (Redundansi Strategis)
Keamanan Berpusat Manusia	SDM: Program kesadaran kontekstual, Kompetensi Hibrida Lintas-Fungsi	Kepemimpinan Adaptif + Learning Agility + PS.
Tata Kelola Kolaboratif	Hukum/GCG: Pengawasan tingkat dewan, Alokasi akuntabilitas yang jelas	GCG + ERM (COSO) + Hukum (Kepatuhan Regulasi)

Tata Kelola Perusahaan yang Baik (GCG) berfungsi sebagai landasan dalam pengelolaan perusahaan yang memastikan adanya transparansi, tanggung jawab, dan pengawasan yang baik. Penerapan GCG yang efektif terbukti mampu mengurangi salah satu elemen dalam segitiga penipuan, yaitu “kesempatan”. Sistem MRTI yang berbasis pada

Manajemen Risiko Enterprise (ERM) berperan untuk mendeteksi permasalahan sejak awal. COBIT 5 (EDM03 dan APO12) terbukti sangat berguna dalam menilai dan meningkatkan pengelolaan risiko dalam teknologi informasi. ISO 31000 menawarkan pendekatan yang terstruktur dan berdasarkan probabilitas. Pemilihan model harus disesuaikan dengan kebutuhan spesifik. Sektor Keuangan menggunakan ISO 27001 sebesar 75%, sedangkan Sektor Pemerintahan lebih mengutamakan NIST sebesar 80%, dan Sektor Pendidikan lebih cenderung menggunakan OCTAVE sebesar 60%. Manajemen risiko digital pada dasarnya mencakup pengelolaan perubahan di dalam organisasi, di mana teknologi hanya berfungsi sebagai alat bantu. Keberhasilan bergantung pada kemampuan organisasi dalam menangani aspek yang berkaitan dengan manusia dan budaya. Untuk strategi perubahan yang sukses, diperlukan pendekatan komprehensif. Pendekatan ini secara sistematis menyelaraskan usaha dari sisi struktur (dari atas ke bawah) seperti model 8 Langkah Kotter dengan pendekatan dari sisi perilaku (dari bawah ke atas) seperti model ADKAR. Adanya gangguan digital dan risiko yang selalu berubah mengharuskan gaya kepemimpinan untuk berkembang. Penelitian menunjukkan bahwa Manajemen Risiko dan Transformasi Digital memiliki dampak positif pada Kepemimpinan Adaptif (KA). Pemimpin yang adaptif memainkan peran kunci dalam menghadapi perubahan yang cepat dan tidak pasti. Mereka mampu membuat keputusan dengan cepat dan tepat, bahkan di tengah situasi yang tidak jelas. Di samping itu, mereka mampu memimpin tim melalui situasi yang sulit. Kepemimpinan yang adaptif memastikan organisasi tidak hanya bertahan, tetapi juga dapat belajar dan merespons ancaman secara langsung.

Di sisi lain, Kepemimpinan Transformasional (KT) berperan krusial dalam menciptakan sebuah budaya yang mendukung inovasi serta mendorong karyawan untuk mengambil risiko yang telah diperhitungkan. Pemimpin yang bersifat transformasional memiliki kemampuan untuk memberikan semangat kepada karyawan melalui visi yang terang tentang masa depan digital, mendorong mereka untuk mengutamakan kepentingan bersama di atas kepentingan pribadi, sambil menciptakan suasana yang mendukung penerimaan perubahan. Komitmen yang jelas dari manajemen puncak, termasuk dewan direksi, merupakan faktor kunci dalam keberhasilan pelaksanaan strategi manajemen risiko digital. Kecepatan dalam adopsi oleh karyawan sangat bergantung pada budaya yang mendukung. Learning Agility (LA) yaitu kemampuan individu untuk belajar dengan cepat dari pengalaman dan kemudian dapat mengaplikasikan pengetahuan tersebut secara fleksibel dalam situasi baru yang kompleks. Dalam konteks manajemen risiko digital, LA menjadi alat utama yang mempercepat adaptasi karyawan terhadap teknologi baru, prosedur mitigasi risiko yang terbaru, serta tuntutan kompetensi yang beragam. Selain itu, Psychological Safety (PS) merupakan fondasi utama bagi budaya inovasi dan Learning Agility. Lingkungan dengan tingkat PS yang tinggi memberikan kesempatan bagi karyawan untuk bersikap terbuka dalam mencoba hal-hal baru, bertanya, dan melaporkan kesalahan atau situasi berisiko tanpa merasa takut akan konsekuensi negatif. Budaya yang mendorong strategi "gagal dengan cepat, belajar lebih cepat" sangat penting dalam mendeteksi dan memperbaiki kelemahan sistem dengan cepat. Secara keseluruhan, keberadaan budaya organisasi yang kuat dan positif memengaruhi efektivitas sistem formal seperti GCG dan MR. Budaya ini menentukan apakah sikap patuh hanya merupakan formalitas belaka atau benar-benar diintegrasikan sebagai bagian dari perilaku kerja sehari-hari.

Transformasi digital memerlukan pergeseran pada sumber daya manusia menjadi "bakal hibrida," yaitu individu yang memiliki keahlian teknis serta pengetahuan tentang operasional dan tingkah laku. Integrasi Keahlian sangat dibutuhkan. Program pelatihan dan peningkatan keterampilan (reskilling/upskilling) yang menyeluruh harus dilakukan untuk menciptakan talenta yang mampu menghubungkan area IT/Siber dan Teknologi Operasional (OT), yang merupakan titik lemah kritis di era Industri 4. 0. Selain itu, kemampuan digital dari para karyawan secara umum perlu ditingkatkan sebagai langkah awal dalam menangkal ancaman siber seperti phishing dan social engineering. Manajemen Risiko dalam pelatihan juga perlu diperkuat; mengintegrasikan MR dalam pelatihan

(pelatihan berbasis skenario risiko di tempat kerja) telah terbukti dapat meningkatkan kemampuan program pelatihan serta produktivitas karyawan. Strategi untuk mengelola risiko SDM pun seharusnya berorientasi pada pengembangan kapasitas SDM agar dapat mengelola risiko teknis dan operasional secara mandiri. Hal ini didukung oleh Struktur Tim Lintas-Fungsi, di mana pembentukan tim yang mencakup berbagai disiplin seperti hukum, teknik, dan TI menjadi strategi penting untuk mengatasi kekurangan keahlian internal dan memperkuat kolaborasi lintas bidang dalam pengambilan keputusan yang berkaitan dengan risiko.

KESIMPULAN

Penelitian ini menegaskan bahwa kerangka kerja manajemen risiko (MR) yang efektif dan berkelanjutan untuk organisasi berbasis digital harus merupakan model integratif multidisiplin. Kombinasi harmonis antara dimensi Hukum, Teknik Industri, dan Teknologi Informasi (TI) sangat penting untuk mengubah MR dari fungsi kepatuhan yang reaktif menjadi kemampuan strategis yang mendorong ketahanan organisasi di tengah kompleksnya lanskap risiko digital.

Keberlanjutan manajemen risiko digital didasarkan pada tiga pilar utama: Ketahanan Cyber-Physical, Kapabilitas Adaptif Manusia, dan Pengendalian Sistematis serta Tata Kelola. Ketahanan Cyber-Physical berfokus pada mitigasi ancaman Industri 4.0 dengan menerapkan Compliance by Design—di mana kepatuhan privasi data diintegrasikan langsung ke dalam desain sistem sejak awal—dan model keamanan Zero Trust untuk melindungi ekosistem yang terhubung serta aset operasional (OT). Kapabilitas Adaptif Manusia didukung oleh Kepemimpinan Adaptif yang mampu memengaruhi positif praktik MR dan Digital Transformation (DT). Kepemimpinan ini wajib menumbuhkan budaya Psychological Safety sebagai prasyarat untuk meningkatkan Learning Agility karyawan melalui investasi pada kompetensi hibrida (reskilling/upskilling). Pengendalian Sistematis dicapai melalui integrasi Enterprise Risk Management (ERM) dengan Good Corporate Governance (GCG). Sinergi ini memastikan GCG mencegah fraud dengan mengurangi peluang, sementara ERM memberikan alat deteksi dini dan mitigasi risiko keuangan secara sistematis. Standar MRTI (ISO 31000, COBIT, NIST) harus diterapkan secara adaptif dan terukur, bukan sekadar pemenuhan formalitas. Secara keseluruhan, organisasi yang mampu mengembangkan kemampuan di seluruh dimensi ini—yaitu arsitektur teknis yang tangguh, sumber daya manusia yang adaptif, dan tata kelola yang terpadu—akan mampu tidak hanya bertahan di tengah lanskap risiko kompleks, tetapi juga memanfaatkan peluang dan keunggulan kompetitif dari teknologi digital secara jangka panjang.

DAFTAR PUSTAKA

G. N. Wala, "Mitigasi Risiko Bisnis melalui Pendekatan Hukum dan Teknik Industri: Strategi Komprehensif di Era Digital," Dinasti Information and Technology, vol. 2, no. 4, pp. 156–169, 2025.

S. F. Muliati, F. Supriadi, and D. I. Junaedi, "Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur," Jurnal TeIKa, vol. 15, no. 1, pp. 65–74, 2025.

A. N. Illah and Ilham, "Analisis Risiko, Keamanan, Dan Efektivitas Framework Pada Layanan Pembayaran Digital Menggunakan Systematic Literature Review," Jurnal Teknologi Sistem Informasi, vol. 6, no. 1, pp. 89–102, 2025.

S. Febriansyah, Nasruddin, and S. Darni, "Mewujudkan Transparansi Keuangan: Kolaborasi GCG dan Manajemen Risiko dalam Mengurangi Fraud," Journal of Economics, Management, and Accounting, vol. 3, no. 1, 2025.

D. A. Nufuz et al., "Strategi Efektif Dalam Manajemen Perubahan: Membangun Ketahanan Organisasi Di Era Digital," Jurnal Penelitian Nusantara, vol. 1, no. 6, pp. 540–547, 2025.

R. K. Sari et al., "Strategi Manajemen Perubahan Holistik dalam Membentuk Adaptabilitas Karyawan Berbasis Learning Agility di Era Transformasi Digital," Fatih: Journal of Contemporary Research, vol. 2, no. 2, pp. 942–950, 2025.

A. Setiyowati, "Determinasi Kepemimpinan Adaptif: Manajemen Risiko, Transformasi Digital dan Adaptif Perusahaan," JPSN: Jurnal Pendidikan Siber Nusantara, vol. 3, no. 1, pp. 37–47, 2025.
M. A. Kurniawan and S. Hartati, "Manajemen Risiko Dalam Pengembangan Program Pendidikan Inovatif Berbasis Teknologi Digital Di Sekolah Islam Swasta," Jurnal Pendidikan Islam, vol. 7, no. 1, 2025.
A. N. Rizkyah et al., "Strategi Manajemen Risiko Dalam Meningkatkan Efektivitas Pelatihan Dan Produktivitas Karyawan Di PT Semen Indonesia Logistik," J-ESA Jurnal Ekonomi Syariah, vol. 8, no. 1, pp. 57–64, 2025.
F. Mulianingsih, Fajar, and Suharyati, "Manajemen Risiko Digital: Strategi Keamanan Siber untuk Mitigasi Ancaman di Era Revolusi Industri 4.0," Indonesian Research Journal on Education, vol. 5, no. 2, pp. 888–898, 2025.
M. N. Afgani, T. P. Yoga, and C. Habibi, "Audit Manajemen Resiko Teknologi Informasi Pospay Menggunakan Framework COBIT 5," SisInfo Jurnal Sistem Informasi dan Informatika, vol. 6, no. 1, pp. 61–76, 2024.