Jurnal Ekonomi, Teknologi dan Bisnis (JETBIS)
Volume 5, Number 5 Mei 2026
p-ISSN 2964-903X; e-ISSN 2962-9330

Tata Kelola Data dan Pengendalian Digital di Era Kecerdasan Buatan: Kajian Kepustakaan tentang Integrasi Data *Governance*, *Artificial Intelligence*, dan *Cyber Control* dalam Sistem Pengendalian Manajemen

Aceng Abdul Hamid[1*], Komarudin[2],
Sekolah Tinggi Ilmu Ekonomi Cirebon, Indonesia
Email: kangaceng88@gmail.com, jrxkomarudin21@gmail.com

ABSTRAK

Transformasi digital memperluas cakupan Sistem Pengendalian Manajemen (SPM) dari pengendalian strategis dan perilaku menuju pengendalian digital yang bertumpu pada tiga pilar teknis: tata kelola data (data governance), kecerdasan buatan *(artificial intelligence),* dan pengendalian keamanan siber *(cyber control).* Penelitian ini bertujuan memetakan konsep dan ruang lingkup ketiga pilar sebagai perluasan pengendalian digital dalam kerangka SPM, menganalisis keterkaitan integratif ketiganya sebagai satu ekosistem tata kelola digital yang saling memperkuat dan merumuskan proposisi teoretis mengenai hubungan integrasi tata kelola digital dengan kematangan digital dan kinerja organisasi. Penelitian menggunakan pendekatan kualitatif berjenis studi kepustakaan *(library research)* dengan sumber utama buku Tata Kelola Data dan Pengendalian Digital, dilengkapi literatur pendukung, regulasi, dan laporan lembaga resmi, yang dianalisis melalui analisis isi dan analisis tematik. Hasil kajian menunjukkan tata kelola data menjadi fondasi yang menjamin kualitas dan keandalan informasi; kecerdasan buatan memperkuat perencanaan, pengukuran kinerja, dan deteksi risiko, tetapi menuntut tata kelola algoritma yang bertanggung jawab agar tidak menimbulkan bias; sedangkan *cyber control* melindungi aset data dan sistem AI dari ancaman siber. Ketiga pilar saling bergantung dan membentuk ekosistem tata kelola digital yang hubungannya dengan kinerja organisasi bersifat kontingen, dipengaruhi kepemimpinan digital, kesiapan sumber daya manusia, dan budaya berbasis data. Penelitian ini berkontribusi berupa kerangka integratif tiga pilar tata kelola digital sebagai landasan konseptual bagi penelitian empiris lanjutan dan praktik pengendalian manajemen di era kecerdasan buatan.

Kata Kunci: tata kelola data; kecerdasan buatan; pengendalian siber; sistem pengendalian manajemen; transformasi digital

ABSTRACT

Digital transformation has expanded the scope of Management Control Systems (MCS) from strategic and behavioral control toward digital control resting on three technical pillars: data governance, artificial intelligence, and cyber control. This study aims to map the concept and scope of the three pillars as an extension of digital control within the MCS framework, analyze their integrative interrelation as a mutually reinforcing digital governance ecosystem and formulate theoretical propositions on the relationship between digital governance integration and organizational digital maturity and performance. It employs a qualitative library research approach, drawing primarily on the book Tata Kelola Data dan Pengendalian Digital, supplemented by supporting literature, regulations, and official institutional reports, analyzed through content and thematic analysis. The findings show that data governance provides the foundation ensuring information quality and reliability; artificial intelligence strengthens planning, performance measurement, and risk detection but requires responsible algorithmic governance to avoid bias; while cyber control protects data assets and AI systems from evolving cyber threats. The three pillars are interdependent and form a digital governance ecosystem whose relationship with organizational performance is contingent, influenced by digital leadership, human resource readiness, and a data-driven culture. This study contributes an integrative

three-pillar framework of digital governance as a conceptual foundation for further empirical research and management control practice in the age of artificial intelligence.

Keywords: *data governance; artificial intelligence; cyber control; management control system; digital transformation.*

PENDAHULUAN

Abad ke-21 menjadi saksi bagi transformasi fundamental dalam cara organisasi mengelola dan memanfaatkan informasi. Revolusi industri keempat yang ditandai konvergensi antara dunia fisik, digital, dan biologis telah mengubah secara radikal lanskap manajemen organisasi di seluruh dunia (Schwab, 2016). Di tengah transformasi ini, data telah menjelma menjadi aset strategis yang nilainya dapat melampaui aset fisik konvensional, sementara kecerdasan buatan dan ancaman siber menjadi dua sisi mata uang yang sama-sama menuntut perhatian serius dari pengendalian manajemen organisasi.Dalam perspektif Sistem Pengendalian Manajemen (SPM), Haro et al. (2025) menegaskan bahwa sistem pengendalian yang efektif harus mampu beradaptasi dengan lingkungan bisnis yang terus berubah, termasuk mengintegrasikan dimensi digital ke dalam setiap aspek pengendalian organisasi. Pandangan ini diperkuat oleh Riadi & Hamid (2026) yang secara khusus mengelaborasi SPM dari dimensi strategic, behavioral, dan digital control sebagai satu kesatuan yang tidak dapat dipisahkan dalam organisasi modern. Namun demikian, dimensi digital control itu sendiri masih memerlukan elaborasi lebih lanjut mengenai komponen teknis apa saja yang menyusunnya serta bagaimana komponen-komponen tersebut saling berkaitan satu sama lain.

Skala transformasi digital tersebut tergambar dari berbagai data kuantitatif. Tamtelahitu et al. (2026) melaporkan bahwa volume data global yang diciptakan, direplikasi, dan dikonsumsi diperkirakan mencapai 120 zettabyte pada tahun 2023 dan diproyeksikan melampaui 180 zettabyte pada tahun 2025. Di sisi lain, (IBM Security, 2023) mencatat rata-rata biaya kebocoran data global mencapai USD 4,45 juta per insiden, sementara (Hutasuhut, 2026) melaporkan lebih dari 400 juta anomali trafik siber di Indonesia sepanjang tahun 2022. Data ini menegaskan bahwa peluang nilai dari data dan kecerdasan buatan senantiasa berdampingan dengan risiko yang setara besarnya.Urgensi tata kelola digital semakin diperkuat oleh munculnya berbagai regulasi yang mengharuskan organisasi mengelola data dan keamanan digital secara bertanggung jawab. Pemberlakuan General Data Protection Regulation (GDPR) oleh Uni Eropa pada 2018 menjadi titik balik regulasi perlindungan data global (Cavoukian, 2009; EUROPEIA, 2021), sementara di Indonesia lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menandai komitmen negara memasuki era baru tata kelola data yang lebih bertanggung jawab. Pada domain keamanan siber, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik serta berbagai peraturan BSSN melengkapi kerangka kepatuhan yang harus dipenuhi organisasi di Indonesia.

Pada saat yang sama, adopsi kecerdasan buatan berkembang sangat pesat namun tidak selalu diimbangi kesiapan tata kelola yang memadai. (Chui et al., 2023) memperkirakan bahwa AI generatif dapat menghasilkan nilai ekonomi global antara USD 2,6 triliun hingga USD 4,4 triliun per tahun, sementara (Dhakal et al., 2024) menemukan bahwa kesenjangan kompetensi digital (*skill gaps*) masih menjadi hambatan terbesar transformasi digital di kawasan Asia Pasifik. Kondisi ini memperlihatkan bahwa kapabilitas teknis semata tidak cukup; organisasi memerlukan kerangka pengendalian yang mengintegrasikan tata kelola data, kecerdasan buatan, dan keamanan siber secara

koheren.Kajian terdahulu memberikan fondasi konseptual yang kuat namun cenderung membahas ketiga domain tersebut secara terpisah. Verhoef et al. (2021) memetakan tahapan digitisasi, digitalisasi, dan transformasi digital pada level organisasi secara umum tanpa menautkannya secara eksplisit dengan kerangka SPM. Fähndrich (2023) melalui tinjauan sistematis terhadap literatur akuntansi manajemen menunjukkan bahwa digitalisasi mengubah dimensi tugas, instrumen, organisasi, dan perilaku pengendalian manajemen, namun pembahasannya belum secara spesifik menyentuh tata kelola data, AI, dan keamanan siber sebagai komponen konkret dari pengendalian digital. Sementara itu, Zhang et al. (2025) mengkaji manajemen algoritmik secara mendalam, namun terbatas pada dimensi perilaku dan belum menghubungkannya dengan tata kelola data maupun keamanan siber secara terintegrasi.

Kesenjangan tersebut ditegaskan pula oleh literatur teknis yang masing-masing berkembang secara independen dalam disiplinnya sendiri. Kerangka data governance seperti (International, 2017) dan COBIT 2019 (De Haes et al., 2019) dikembangkan dari perspektif manajemen data dan tata kelola TI, sementara kerangka keamanan siber seperti NIST Cybersecurity Framework ((Cybersecurity, 2018; Folorunso et al., 2024; (US) & (US), 2024) dikembangkan dari perspektif keamanan informasi. Kedua rumpun literatur ini jarang secara eksplisit diposisikan sebagai bagian dari Sistem Pengendalian Manajemen sebagaimana dikonseptualisasikan Hamid (2021, 2022, 2023, 2026e), padahal secara substantif keduanya adalah mekanisme pengendalian formal yang menjadi bagian tak terpisahkan dari SPM organisasi di era digital.Berdasarkan kesenjangan tersebut, artikel ini menawarkan novelty berupa sintesis kepustakaan yang memposisikan tata kelola data, kecerdasan buatan, dan cyber control sebagai tiga pilar yang saling terkait dalam satu ekosistem pengendalian digital, mengacu pada buku Tata Kelola Data dan Pengendalian Digital: Data Governance, Artificial Intelligence, dan Cyber Control (Harahap et al., 2025) sebagai rujukan utama yang secara eksplisit mengintegrasikan kerangka teoretis SPM dengan praktik-praktik terkini pada ketiga domain tersebut.

Rujukan utama tersebut merupakan kelanjutan dari agenda riset Hamid yang secara konsisten mengaitkan kualitas informasi, tata kelola, dan kinerja pada berbagai konteks dan tingkatan organisasi. Pada tingkat pemerintah daerah, Hamid (2018) menemukan bahwa kinerja keuangan daerah berpengaruh terhadap tingkat kesejahteraan masyarakat, sebuah bukti awal bahwa kualitas pengelolaan informasi keuangan memiliki konsekuensi nyata terhadap pemangku kepentingan yang lebih luas. Pada tingkat korporasi, Hamid et al. (2023) menunjukkan bahwa determinan tata kelola dan sistem informasi memengaruhi peringkat obligasi dan yield obligasi korporasi, temuan yang kemudian diperdalam (Budiarsyah, 2025a) dalam kajian konsep, risiko, dan kinerja obligasi korporasi di Bursa Efek Indonesia. Pada tingkat manajemen keuangan strategis, Hamid (2026a) mengembangkan kerangka corporate financial management and investment analysis, sementara (Hamid, 2026b) mengonseptualisasikan manajemen keuangan sebagai sociocybernetic control system yang menekankan umpan balik (feedback), adaptasi, dan sensemakingsebuah perspektif yang sangat relevan dengan gagasan pengendalian digital berbasis data dan algoritma yang dibahas dalam artikel ini. Kesinambungan agenda riset tersebut kemudian dirangkum secara terintegrasi oleh Moyer et al. (2003) dalam Financial Management: Integrated Theory, Strategy, Governance, and Future Finance, yang memosisikan tata kelola dan pengendalian sebagai inti dari manajemen keuangan masa depan. Pada tingkat komunitas, Hamid & Yanthi (2025) menunjukkan bahwa strategi digitalisasi mampu meningkatkan kepatuhan masyarakat dalam menunaikan

kewajiban zakat, memperlihatkan bahwa prinsip tata kelola dan pengendalian berbasis data yang sama juga relevan pada level akuntabilitas sosial, bukan hanya level korporasi.

Berdasarkan pemetaan di atas, kesenjangan penelitian (research gap) yang dituju artikel ini adalah belum tersedianya kerangka yang secara eksplisit memposisikan tata kelola data, kecerdasan buatan, dan cyber control sebagai satu kesatuan pilar pengendalian digital di dalam Sistem Pengendalian Manajemen, sebagaimana ketiga domain tersebut selama ini dikaji secara terpisah (Verhoef et al., 2021); (Fähndrich, 2023); (Zhang et al., 2025). Kesenjangan ini bersifat mendesak (urgensi) mengingat pesatnya adopsi teknologi digital yang belum diimbangi kesiapan tata kelola (Chui et al., 2023); (Dhakal et al., 2024). Kebaruan (novelty) penelitian terletak pada sintesis kepustakaan yang mengintegrasikan ketiga pilar tersebut ke dalam satu ekosistem pengendalian digital dengan merujuk buku Harahap et al. (2025) sebagai rujukan utama.

Secara teoretis, penelitian ini bermanfaat (manfaat) memperkaya khazanah teori SPM di era digital; secara praktis, hasilnya bermanfaat sebagai panduan bagi manajemen dalam merancang tata kelola digital yang adaptif. Adapun implikasi penelitian mencakup penyediaan landasan konseptual bagi pengujian empiris lanjutan sekaligus rujukan bagi perumusan kebijakan pengendalian digital pada tingkat organisasi.Berdasarkan uraian latar belakang, urgensi, data pendukung, dan kesenjangan penelitian di atas, artikel ini bertujuan untuk mengkaji secara komprehensif melalui pendekatan kajian kepustakaan mengenai: (1) memetakan konsep dan ruang lingkup tata kelola data, kecerdasan buatan, dan cyber control sebagai perluasan pengendalian digital dalam kerangka SPM (Hamid, 2021, 2026e); (2) menganalisis keterkaitan integratif antara ketiga pilar tersebut sebagai satu ekosistem tata kelola digital yang saling memperkuat (Harahap et al., 2025); serta (3) merumuskan proposisi teoretis mengenai hubungan integrasi tata kelola digital dengan kematangan digital dan kinerja organisasi. Dengan demikian, artikel ini diharapkan memberikan kontribusi konseptual bagi pengembangan teori pengendalian manajemen sekaligus implikasi praktis bagi organisasi dalam merancang tata kelola digital yang adaptif di era kecerdasan buatan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan jenis studi kepustakaan (library research), yaitu penelitian yang mengkaji dan mensintesis gagasan, konsep, serta temuan yang terdapat pada literatur akademik dan sumber tepercaya lain untuk merumuskan kontribusi teoretis atas suatu topik tertentu(Adlini et al., 2022). Pendekatan ini dipilih karena tujuan penelitian bersifat konseptual, yaitu memetakan dan mensintesis keterkaitan antara tata kelola data, kecerdasan buatan, dan cyber control dalam kerangka Sistem Pengendalian Manajemen, sehingga tidak memerlukan pengumpulan data primer di lapangan.Pendekatan ini bersifat deskriptif-analitis: peneliti tidak hanya memaparkan temuan dari sumber secara naratif, tetapi juga menganalisis pola dan keterkaitan antarpilar untuk membangun proposisi konseptual baru. Buku Tata Kelola Data dan Pengendalian Digital: Data Governance, Artificial Intelligence, dan Cyber Control ((Harahap et al., 2025) menjadi sumber primer utama karena secara eksplisit mengintegrasikan kerangka teoretis SPM dengan praktik-praktik terkini pada ketiga pilar tersebut, sejalan dengan judul dan tujuan penelitian ini.

Sejalan dengan karakteristik penelitian kualitatif, instrumen utama dalam penelitian ini adalah peneliti sendiri *(human instrument),* yang berperan menentukan kata kunci penelusuran, menyeleksi sumber, mengekstraksi data, dan menginterpretasikan temuan literatur. Untuk menjaga konsistensi proses, peneliti menggunakan instrumen bantu berupa matriks sintesis literatur yang

memuat kolom: pilar tata kelola digital (*data governance, artificial intelligence, atau cyber control*), konsep/kerangka kerja kunci, keterkaitan dengan prinsip SPM, temuan utama, dan relevansinya terhadap kerangka konseptual penelitian. Instrumen ini disusun mengikuti tiga pilar utama yang dikembangkan (Harahap et al., 2025). Selain matriks sintesis, peneliti menggunakan pedoman kriteria inklusi dan eksklusi untuk menyaring sumber. Kriteria inklusi mencakup: (1) buku, artikel, regulasi, atau laporan resmi lembaga yang membahas tata kelola data, kecerdasan buatan, atau keamanan siber dalam konteks pengendalian organisasi; (2) dipublikasikan dalam rentang tahun 2001--2026 dengan penekanan utama pada publikasi lima tahun terakhir; serta (3) memiliki relevansi tematik langsung dengan judul penelitian.

Pengumpulan data dilakukan melalui teknik dokumentasi (*desk research*), yaitu menelusuri dan mengumpulkan dokumen tertulis berupa buku, regulasi, standar teknis, serta laporan resmi lembaga pemerintah dan riset yang relevan (Adlini et al., 2022). Sumber utama adalah buku Tata Kelola Data dan Pengendalian Digital (Harahap et al., 2025) yang ditelusuri bab per bab, mencakup Bab I (Transformasi Digital dan Tata Kelola Organisasi), Bab II (Data Governance), Bab III (*Artificial Intelligence*), Bab IV (*Cyber Control*), dan Bab V (Integrasi Tata Kelola Digital).Data primer tersebut dilengkapi dengan penelusuran silang (*cross-check*) terhadap sumber-sumber yang dirujuk di dalamnya, meliputi kerangka kerja teknis DAMA-DMBOK, COBIT , NIST Cybersecurity Framework, (Folorunso et al., 2024), regulasi GDPR, UU PDP, UU ITE, PP PSTE, serta laporan lembaga riset dan pemerintah Gartner, IBM, McKinsey Global Institute, PwC, Verizon, World Economic Forum, BSSN, Kominfo. Teknik pengumpulan data bersifat non-interaktif karena sepenuhnya bersandar pada dokumen tertulis yang telah dipublikasikan (Taherdoost, 2023).

Prosedur penelitian dilaksanakan melalui lima tahap yang saling berkesinambungan, diadaptasi dari tahapan studi kepustakaan yang dirumuskan Adlini et al. (2022):

Tabel 1. Tahapan Studi Kepustakaan

Tahap	Kegiatan	Luaran
1. Identifikasi	Menentukan kata kunci dan menelusuri sumber primer (buku) serta sumber pendukung pada basis data akademik dan lembaga resmi	Daftar awal sumber potensial
2. Seleksi *(screening)*	Menyaring sumber berdasarkan kriteria inklusi/eksklusi (tahun terbit, relevansi tema, kredibilitas penerbit)	Daftar sumber terpilih
3. Ekstraksi data	Mengisi matriks sintesis literatur untuk setiap pilar (*data governance, AI, cyber control)*	Data terstruktur per pilar
4. Kategorisasi tematik	Mengelompokkan temuan ke dalam tema besar: fondasi data, penguatan AI, dan perlindungan siber	Peta tematik tiga pilar
5. Sintesis dan interpretasi	Menghubungkan antarpilar untuk membangun proposisi konseptual dan menjawab tujuan penelitian	Simpulan dan model integratif

Sumber: Diadaptasi dari Adlini et al. (2022)

Analisis data menggunakan teknik analisis isi *(content analysis)* yang dipadukan dengan analisis tematik *(thematic analysis),* mengikuti tiga alur kegiatan yang saling terkait: reduksi data, penyajian data, dan penarikan simpulan/verifikasi (Safarudin et al., 2023). Pada tahap reduksi data, peneliti memilih dan memfokuskan informasi dari matriks sintesis yang relevan dengan tiga pilar tata kelola digital serta keterkaitannya dengan SPM, dan mengesampingkan data yang tidak relevan

dengan fokus penelitian.Pada tahap penyajian data, temuan yang telah direduksi disusun ke dalam bentuk naratif, tabel, dan matriks tematik untuk memudahkan identifikasi pola hubungan antara tata kelola data, kecerdasan buatan, dan cyber control. Pada tahap akhir, peneliti melakukan penarikan simpulan melalui triangulasi sumber, yaitu membandingkan temuan dari buku primer, regulasi, dan laporan lembaga resmi untuk memastikan konsistensi dan kredibilitas hasil sintesis. Hasil akhir dari proses analisis ini adalah proposisi konseptual mengenai integrasi tata kelola digital serta implikasinya terhadap kematangan dan kinerja organisasi, yang dipaparkan pada bagian berikut.

HASIL DAN PEMBAHASAN

Tata Kelola Data *(Data Governance)* sebagai Fondasi Pengendalian Digital dalam SPM

Sub-pembahasan ini menjawab tujuan pertama penelitian pada dimensi tata kelola data. Konsep tata kelola data tidak muncul secara tiba-tiba, melainkan hasil evolusi panjang pemikiran manajemen informasi: dari perhatian pada kualitas basis data relasional pada dekade 1980-an, konsep data warehouse dan business intelligence pada dekade 1990-an, dorongan regulasi pasca skandal Enron dan WorldCom yang melahirkan Sarbanes-Oxley Act pada awal 2000-an, hingga era big data dan cloud computing sejak 2010 yang melahirkan model 5V (Volume, Velocity, Variety, Veracity, Value) sebagaimana dirumuskan Laney (2001). Dalam perspektif SPM, Haro et al. (2025) menegaskan bahwa pengendalian internal yang efektif merupakan fondasi tata kelola organisasi yang baik, dan tata kelola data merupakan manifestasi konkret dari prinsip tersebut pada era digital.

Secara konseptual, Eryurek et al. (2021) mendefinisikan tata kelola data sebagai keseluruhan sistem hak keputusan dan akuntabilitas atas proses yang berkaitan dengan data, sementara International (2017) Pratama (2026) memposisikan tata kelola data sebagai bagian dari sistem pengendalian yang lebih luas, karena sistem informasi manajemen yang menjadi komponen inti SPM (Hamid, 2021) sepenuhnya bergantung pada kualitas data yang dikelolanya.Berbagai kerangka kerja telah dikembangkan untuk membantu implementasi tata kelola data secara sistematis, masing-masing dengan penekanan berbeda. DAMA-DMBOK mengidentifikasi sebelas domain manajemen data yang saling terkait; COBIT 2019 (De Haes et al., 2019) mengintegrasikan tata kelola data ke dalam lima domain evaluasi, pengarahan, dan pemantauan; sementara IBM Data Governance Council Maturity Model menawarkan pendekatan berjenjang dari tingkat initial hingga optimizing yang sejalan dengan prinsip evaluasi kinerja berkelanjutan dalam SPM (Hamid, 2021).

Tabel 2. Kerangka Kerja Data Governance Utama

Kerangka	Fokus Utama	Kekuatan
DAMA-DMBOK	Manajemen data komprehensif	Cakupan domain lengkap (11 domain)
COBIT 2019	Tata kelola TI dan data	Integrasi dengan audit dan compliance
IBM DG Maturity Model	Kematangan tata kelola data	Roadmap peningkatan bertahap yang jelas
ISO 8000	Kualitas data	Standar internasional yang diakui

Sumber: International (2017)(De Haes et al., 2019); Mansfield-Devine (2022)

Kebijakan data *(data policy)* menjadi fondasi normatif program tata kelola data, berfungsi sebagai mekanisme pengendalian formal yang mengikat seluruh anggota organisasi (Hamid, 2021).

Klasifikasi data ke dalam tingkat sensitivitas publik, internal, konfidensial, dan sangat rahasia menjadi dasar penerapan kontrol teknis seperti enkripsi dan pembatasan akses. Kualitas data, yang diukur melalui dimensi akurasi, kelengkapan, konsistensi, ketepatan waktu, validitas, dan keunikan (International, 2017); (Loshin, 2010) memiliki konsekuensi finansial yang nyata:Krasner (2021) memperkirakan kerugian rata-rata akibat data berkualitas buruk mencapai USD 12,9 juta per tahun per organisasi. Haro et al. (2025) mengaitkan kualitas data dengan prinsip pengendalian kualitas (quality control) dalam SPM, karena data yang tidak andal akan menghasilkan keputusan manajerial yang keliru meskipun instrumen analitiknya canggih.Pada dimensi regulasi, pemberlakuan GDPR oleh Uni Eropa pada 2018 menjadi tonggak global perlindungan data dengan prinsip lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, serta integrity and confidentiality.

Di Indonesia, UU PDP No. 27 Tahun 2022 menjadi regulasi komprehensif pertama yang mengatur hak subjek data, kewajiban pengendali dan pemroses data, serta sanksi pidana dan denda yang signifikan. Kepatuhan terhadap regulasi ini, sebagaimana ditekankan (Haro et al., 2025) tidak boleh dipandang semata sebagai kewajiban hukum, melainkan sebagai bagian dari akuntabilitas pengendalian manajemen yang lebih luas.Adopsi Big Data dan Cloud Computing menambah kompleksitas tata kelola data melalui isu data sovereignty, shared responsibility, dan multi-cloud governance; survei Maliye (2024) menemukan bahwa 87 persen organisasi telah mengadopsi strategi multi-cloud. (Haro et al., 2025) menegaskan bahwa investasi infrastruktur Big Data dan Cloud harus selalu diimbangi investasi tata kelola yang proporsional, karena ketidakseimbangan antara kapabilitas teknis dan tata kelola justru menghasilkan risiko yang lebih besar daripada manfaatnya. Implementasi program data governance yang komprehensif umumnya berlangsung tiga hingga lima tahun melalui empat fase berjenjang: assessment dan foundation building, pengembangan kebijakan dan standar, implementasi teknologi, serta pengukuran dan peningkatan berkelanjutan (continuous improvement) yang sejalan dengan prinsip SPM (Hamid, 2021, 2022).Sintesis pada sub-pembahasan ini menegaskan bahwa tata kelola data berfungsi sebagai fondasi yang tidak dapat digantikan bagi seluruh ekosistem pengendalian digital: tanpa data yang berkualitas, konsisten, dan patuh terhadap regulasi, dua pilar berikutnyakecerdasan buatan dan cyber controltidak akan dapat berfungsi secara optimal, sebagaimana akan diuraikan pada sub-pembahasan berikutnya.

Kecerdasan Buatan dalam Penguatan Sistem Pengendalian Manajemen: Peluang, Aplikasi, dan Tantangan Etis

Sub-pembahasan ini menjawab tujuan pertama dan kedua penelitian pada dimensi kecerdasan buatan. Kecerdasan buatan (*artificial intelligence*/AI) merupakan bidang ilmu komputer yang bertujuan menciptakan sistem yang mampu menjalankan tugas yang biasanya memerlukan kecerdasan manusia. Revolusi AI kontemporer didorong oleh konvergensi tiga faktor: ketersediaan data dalam skala tak tertandingi, peningkatan daya komputasi, dan kemajuan arsitektur algoritma khususnya deep learning dan transformer (Goodfellow, 2016), Bengio, & Courville, 2016). Aprilia et al. (2025) memandang AI dari perspektif SPM sebagai alat yang memperkuat, bukan menggantikan, penilaian manusia dalam pengambilan keputusan strategis.Penerapan AI dalam SPM membuka dimensi baru pada domain perencanaan dan penganggaranmelalui *driver-based forecasting* dan *continuous planning* yang mempertimbangkan ratusan variabel secara simultanserta

pada domain pengukuran kinerja, di mana dashboard berbasis AI memberikan peringatan dini *(early warning signals)* atas penyimpangan sebelum berkembang menjadi masalah signifikan (Hamid, 2022, 2023). Relevansi ini semakin kuat pada domain manajemen keuangan korporasi dan analisis investasi, di mana (Hamid, 2026a) menegaskan bahwa keputusan pendanaan dan investasi yang berkualitas kini semakin bergantung pada kapasitas organisasi mengolah data secara analitis dan berbasis algoritma, bukan semata pada penilaian manual berbasis pengalaman.

Salah satu aplikasi AI yang paling matang dan terbukti memberikan nilai bisnis adalah deteksi kecurangan *(fraud detection)* dan manajemen risiko kredit di sektor perbankan, dengan (Chui et al., 2023) menemukan bahwa implementasi AI dapat mengurangi kerugian akibat kecurangan hingga 20-40 persen dibandingkan sistem konvensional. Kemampuan deteksi dini semacam ini juga relevan bagi identifikasi sinyal awal *financial distress* pada level korporasi, yang menurut Budiarsyah (2025b) dapat dikenali jauh sebelum terjadinya gagal bayar sepanjang organisasi memiliki sistem data dan analitik yang memadai. Namun demikian, meluasnya peran AI dalam pengambilan keputusan memunculkan tantangan etika yang serius, yang dirangkum dalam prinsip *fairness, accountability, transparency*, dan *explainability* (FATE). Bias algoritmikyang dapat muncul dari data pelatihan yang tidak representatif, desain fitur yang bias, maupun cara model menginterpretasikan hubungan dalam databersifat lebih berbahaya daripada bias manusia karena sifatnya yang tersembunyi. Haro et al. (2025) mengaitkan tata kelola algoritma dengan prinsip akuntabilitas dalam SPM: setiap keputusan signifikan harus dapat ditelusuri kepada individu atau proses yang bertanggung jawab, sehingga penggunaan AI menuntut struktur *human-in-the-loop* yang jelas untuk keputusan kritis.

Tabel 3. Prinsip-Prinsip Etika AI dan Implikasi Praktisnya

Prinsip	**Implikasi Praktis**
Transparansi	Dokumentasi model, explainability tools (SHAP, LIME), audit log keputusan AI
Keadilan (Fairness)	Uji bias dataset pelatihan, monitoring disparate impact
Akuntabilitas	Penetapan AI Owner, human-in-the-loop untuk keputusan kritis
Privasi	Privacy by design, minimisasi data pelatihan, differential privacy
Keamanan	Robustness testing, adversarial attack testing, monitoring berkelanjutan

Sumber: EUROPEIA (2021); OECD (2019); Aprilia et al. (2025)

Masa depan AI dalam pengendalian organisasi ditandai oleh tren AI generatif berbasis Large Language Models yang berpotensi mengotomatisasi hingga 70 persen tugas berbasis pengetahuan di sektor keuangan (Chui et al., 2023), federated learning yang memungkinkan kolaborasi model lintas organisasi tanpa memusatkan data sensitif, serta Explainable AI (XAI) yang akan semakin menjadi persyaratan wajib seiring regulasi seperti GDPR dan UU PDP yang mensyaratkan hak atas penjelasan (right to explanation). Natural Language Processing (NLP) turut memperluas kapasitas analisis organisasi melalui analisis sentimen, pemrosesan dokumen cerdas (Intelligent Document Processing), dan analisis teks hukum, meskipun disertai risiko hallucination pada Large Language Models yang perlu dikelola melalui kebijakan penggunaan AI yang ketat.Kerangka Responsible AI menjadi jawaban atas tantangan etika tersebut, mencakup struktur tata kelola AI di level board, proses penilaian risiko AI sebelum deployment, pengujian dan validasi termasuk pengujian bias, pemantauan berkelanjutan, serta prosedur respons insiden AI.

EUROPEIA (2021) yang mengklasifikasikan sistem AI berdasarkan tingkat risiko menjadi rujukan regulasi global pertama yang komprehensif pada domain ini. Hamid (2021, 2022, 2023) menegaskan bahwa dari perspektif SPM, Responsible AI bukan sekadar kepatuhan regulasi, melainkan komponen fundamental tata kelola organisasi yang baik, karena organisasi yang menerapkan AI secara bertanggung jawab membangun kepercayaan berkelanjutan dari pelanggan, karyawan, dan regulatorsebuah bentuk kendali perilaku yang dimediasi teknologi sebagaimana juga ditemukan pada literatur manajemen algoritmik (Zhang et al., 2025).Sintesis pada sub-pembahasan ini menegaskan bahwa kecerdasan buatan memperkuat SPM secara signifikan pada domain perencanaan, pengukuran kinerja, dan deteksi risiko, tetapi kekuatan tersebut hanya dapat direalisasikan secara berkelanjutan apabila diimbangi tata kelola algoritma yang etis dan akuntabelyang pada gilirannya kembali bertumpu pada kualitas tata kelola data sebagaimana dibahas pada sub-pembahasan sebelumnya, sekaligus memerlukan perlindungan keamanan siber yang memadai sebagaimana akan diuraikan berikutnya.

Cyber Control: Pengendalian Keamanan Siber sebagai Pilar Ketiga SPM Digital

Sub-pembahasan ini menjawab tujuan pertama dan kedua penelitian pada dimensi cyber control. Keamanan siber telah bertransformasi dari isu teknis departemen IT menjadi isu strategis level dewan direksi yang berimplikasi langsung pada kelangsungan bisnis dan reputasi organisasi. Lanskap ancaman kontemporer ditandai oleh profesionalisasi pelaku kejahatan siber dan motif yang semakin beragam, mulai dari pencurian finansial hingga spionase industri dan sabotase infrastruktur kritis. (Spencer, 2024) mengidentifikasi phishing dan eksploitasi kerentanan yang belum ditambal sebagai vektor serangan yang paling mendominasi, sementara ransomware menjadi ancaman dengan dampak paling menghancurkan, sebagaimana ditunjukkan oleh insiden Colonial Pipeline (2021)

Berbagai kerangka pengendalian keamanan siber telah dikembangkan untuk membantu organisasi membangun postur keamanan yang sistematis. NIST *Cybersecurity Framework* mengorganisir aktivitas keamanan siber ke dalam enam fungsi inti pada versi terbarunya: *Govern, Identify, Protect, Detect, Respond,* dan *Recover* (Cybersecurity, 2018; & 2024) sementara Folorunso et al. (2024) menjadi standar internasional Sistem Manajemen Keamanan Informasi yang dapat disertifikasi. *Zero Trust Architecture* yang beroperasi dengan prinsip *'never trust, always verify'* semakin populer seiring maraknya cloud computing dan kerja jarak jauh. Dalam perspektif SPM, Haro et al. (2025) menjelaskan bahwa kerangka pengendalian yang baik harus mencakup struktur, proses, dan pengukuran kinerja pengendalian yang jelasketiga elemen yang secara konsisten dipenuhi oleh kerangka keamanan siber yang matang.

Manajemen risiko siber merupakan aplikasi prinsip manajemen risiko ke dalam domain keamanan siber, mengikuti siklus identifikasi, analisis, evaluasi, dan penanganan risiko. (Haro et al., 2025) menekankan pentingnya mengintegrasikan manajemen risiko siber ke dalam *Enterprise Risk Management* (ERM) organisasi secara keseluruhan, bukan dikelola secara silo oleh departemen IT semata, agar selaras dengan risiko finansial, operasional, kepatuhan, dan reputasional yang lebih luas. Keterkaitan antara risiko digital dan risiko finansial ini juga tampak pada pasar modal, sebagaimana ditunjukkan Budiarsyah (2025a) dalam kajiannya tentang konsep, risiko, dan kinerja obligasi korporasi di Bursa Efek Indonesia, di mana kualitas pengendalian dan keterbukaan informasi organisasitermasuk keandalan sistem digitalnyaturut menjadi pertimbangan penting dalam penilaian risiko oleh investor dan lembaga pemeringkat.

Tabel 4. Matriks Risiko Siber Utama

Risiko	Kemungkinan	Dampak
Data Breach (kebocoran data)	Tinggi	Sangat Tinggi
Ransomware	Tinggi	Sangat Tinggi
DDoS Attack	Sedang-Tinggi	Tinggi
Insider Threat	Sedang	Tinggi
Supply Chain Attack	Sedang	Tinggi
Zero-Day Exploit	Rendah	Sangat Tinggi

Sumber: Diadaptasi dari (Cybersecurity, 2018) dan (Haro et al., 2025)

Pengendalian internal digital mencakup kontrol teknis (identity and access management, enkripsi, firewall, IDS/IPS), kontrol administratif (kebijakan keamanan informasi, security awareness training), dan kontrol fisik, yang secara bersama-sama diperiksa melalui audit siber independen. Continuous auditing yang memanfaatkan pemantauan log dan transaksi secara real-time menjadi pendekatan yang semakin relevan di tengah ancaman yang dapat muncul kapan saja (Hamid, 2021). Di Indonesia, kerangka kepatuhan meliputi UU ITE No. 11 Tahun 2008, PP No. 71 Tahun 2019 tentang PSTE, serta berbagai peraturan BSSN termasuk Peraturan BSSN No. 8 Tahun 2020, yang menurut (Haro et al., 2025) harus dipandang sebagai baseline minimum, bukan tujuan akhir dari program keamanan siber organisasi.

Security Operations Center (SOC) yang mengintegrasikan *Security Information and Event Management* (SIEM) dan *Security Orchestration, Automation, and Response* (SOAR) memberikan kemampuan pemantauan dan *respons insiden secara real-time,* yang oleh Haro et al. (2025) dikaitkan langsung dengan *prinsip continuous monitoring* dalam SPM. Kesiapan menghadapi insiden yang tak terhindarkan diwujudkan melalui Incident Response Plan yang mencakup enam fasepersiapan, identifikasi, penahanan, pembasmian, pemulihan, dan pembelajaran pasca-*insidenserta Business Continuity Plan* dan *Disaster Recovery Plan* yang diukur melalui *Recovery Time Objective* dan *Recovery Point Objective.* Haro et al. (2025) menegaskan bahwa perencanaan SPM yang efektif harus mencakup skenario merugikan (adverse scenarios), bukan hanya skenario normal, karena respons yang terburu-buru justru dapat memperburuk dampak insiden siber.Sintesis pada sub-pembahasan ini menegaskan bahwa cyber control berfungsi sebagai pelindung yang memastikan investasi pada tata kelola data dan kecerdasan buatan tidak hancur dalam hitungan jam oleh serangan siber yang berhasil, sekaligus melengkapi kedua pilar sebelumnya menjadi satu ekosistem pengendalian digital yang utuh, sebagaimana akan disintesiskan pada bagian berikut.

Model Integrasi Tiga Pilar dan Proposisi Hubungannya dengan Kematangan serta Kinerja Tata Kelola Digital

Sub-pembahasan ini menjawab tujuan kedua dan ketiga penelitian. Ketiga pilar yang telah dibahasdata governance, artificial intelligence, dan cyber controlbukan entitas yang terpisah, melainkan komponen yang saling berkaitan erat dalam sebuah ekosistem tata kelola digital yang terintegrasi. Data governance menyediakan fondasi bagi seluruh ekosistem: tanpa data yang berkualitas dan dapat dipercaya, secanggih apa pun model AI tidak dapat menghasilkan wawasan yang andal (garbage in, garbage out), sementara klasifikasi dan konteks sensitivitas data yang dihasilkannya menjadi dasar penentuan tingkat perlindungan yang diperlukan cyber control. Artificial intelligence, pada gilirannya, memperkuat efektivitas data governance melalui katalogisasi metadata otomatis dan deteksi anomali kualitas data, serta memperkuat cyber control melalui deteksi

ancaman yang lebih cepat dan akurat. Cyber control melengkapi ekosistem ini dengan memastikan data dan sistem AI yang menjadi aset strategis organisasi terlindungi dari ancaman yang terus berkembang(Harahap et al., 2025) menegaskan bahwa integrasi ketiga pilar ini ke dalam sistem pengendalian manajemen yang kohesif merupakan tantangan kepemimpinan paling mendesak bagi organisasi di era digitalbukan semata tantangan teknis, melainkan juga tantangan budaya dan tata kelola.

Keberhasilan integrasi tersebut sangat bergantung pada kepemimpinan organisasi. Survei Chui et al. (2023) atas lebih dari 1.500 eksekutif global menemukan bahwa komitmen CEO dan dukungan aktif dewan direksi merupakan faktor pembeda terpenting antara transformasi digital yang berhasil dan yang gagal, sementara (Zukis, 2022) merekomendasikan agar setiap dewan direksi memiliki sekurang-kurangnya satu anggota dengan keahlian siber memadai. Haro et al. (2025) mengidentifikasi komitmen manajemen puncak sebagai prasyarat keberhasilan implementasi sistem pengendalian baru, sementara kesenjangan kompetensi digital sumber daya manusiayang menurut Dhakal et al. (2024) menjadi hambatan terbesar transformasi digital di Asia Pasifikmenuntut program reskilling dan upskilling yang berkelanjutan.

Kematangan digital organisasi, yang mengacu pada sejauh mana organisasi berhasil mengintegrasikan teknologi digital ke dalam operasional, model bisnis, dan budayanya, menjadi indikator penting untuk memetakan posisi organisasi pada ketiga pilar tersebut. Hamid (2021, 2022, 2023) mengintegrasikan konsep kematangan dengan prinsip continuous improvement dalam SPM: organisasi yang matang secara digital tidak berhenti pada tingkat kematangan tertentu, melainkan terus berinvestasi seiring perkembangan teknologi dan kebutuhan bisnis

Tabel 5. Model Integratif Tiga Pilar Tata Kelola Digital

Pilar	Fokus Utama	Kontribusi terhadap Ekosistem	Sumber Pendukung
Data Governance	Kualitas, kebijakan, dan kepatuhan data	Fondasi informasi bagi AI dan basis klasifikasi bagi cyber control	International (2017); Hamid (2021, 2022)
Artificial Intelligence	Analitik, deteksi risiko, otomasi keputusan	Memperkuat deteksi anomali data dan deteksi ancaman siber	Goodfellow (2016); Hamid (2022, 2023)
Cyber Control	Perlindungan aset digital dan respons insiden	Melindungi integritas data dan sistem AI dari ancaman siber	NIST (2024); ISO/IEC (2022); Hamid (2021, 2022)

Sumber: Hasil sintesis penelitian, diadaptasi dari Harahap et al. (2025)

Secara konseptual, ketiga pilar tersebut dapat dipahami melalui lensa sociocybernetic control system yang dikembangkan Hamid (2026b), yaitu pandangan bahwa sistem pengendalian manajemen pada hakikatnya adalah sistem umpan balik (feedback) yang terus beradaptasi dan membentuk sensemaking kolektif organisasi terhadap kondisi lingkungannya. Dalam kerangka ini, data governance menyediakan sinyal umpan balik yang andal, artificial intelligence mempercepat proses adaptasi melalui analitik dan otomasi, sedangkan cyber control menjaga integritas siklus umpan balik tersebut dari gangguan eksternalsehingga ketiganya secara koheren membentuk satu siklus sociocybernetic yang utuh dalam pengendalian digital.Pengukuran kinerja tata kelola digital memerlukan indikator kunci (KPI) yang meliputi seluruh pilar: pada domain data governance meliputi Data Quality Score dan Data Asset Coverage; pada domain AI governance meliputi Model Performance Drift, Bias Index, dan Explainability Score; sedangkan pada domain cyber control

meliputi Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), dan Vulnerability Remediation Rate. Haro et al. (2025) menegaskan prinsip 'apa yang tidak diukur tidak dapat dikelola' sebagai landasan mengapa KPI yang bermakna (meaningful metrics), bukan sekadar mudah diukur (vanity metrics), menjadi kunci keberhasilan program tata kelola digital. Balanced Scorecard dapat diadaptasi untuk mengintegrasikan KPI ketiga pilar tersebut ke dalam perspektif pemangku kepentingan, internal, inovasi-pembelajaran, dan finansial secara komprehensif.

Faktor budaya organisasi turut menentukan keberhasilan integrasi ketiga pilar. Budaya berbasis data (data-driven culture), di mana keputusan dibuat berdasarkan analisis data yang objektif, sering terhambat oleh fear of transparency, data hoarding, aversion to change, dan HiPPO effect. Haro et al. (2025) mengidentifikasi manajemen perubahan sebagai kompetensi kritis yang sering diabaikan dalam program transformasi digital, sementara keberlanjutan program tata kelola digital menurut Aprilia et al. (2025) memerlukan pemimpin yang berkomitmen jangka panjang, mekanisme akuntabilitas yang kuat, dan budaya pembelajaran berkelanjutanbukan sekadar ketergantungan pada satu individu seperti Chief Data Officer sebagai single point of failure.Berdasarkan keseluruhan sintesis di atas, penelitian ini merumuskan proposisi konseptual bahwa integrasi tiga pilar tata kelola digitaldata governance, artificial intelligence, dan cyber controlberhubungan positif dengan kematangan digital dan kinerja organisasi, dengan syarat ketiganya diterapkan secara seimbang dan saling memperkuat, serta didukung oleh kepemimpinan digital yang berkomitmen, kesiapan sumber daya manusia, dan budaya organisasi yang berbasis data. Hubungan ini bersifat kontingen: investasi teknologi yang besar pada satu pilar tanpa kesiapan pada pilar lainnya, misalnya adopsi AI tanpa fondasi data governance yang memadai atau tanpa perlindungan cyber control yang setara, berisiko menghasilkan ketimpangan pengendalian yang justru dapat meningkatkan risiko organisasi alih-alih menurunkannya

Komparasi, Interpretasi, Refleksi, dan Implikasi Kebijakan

Komparasi dengan Penelitian Terdahulu. Hasil sintesis ini memperluas temuan penelitian terdahulu yang mengkaji transformasi digital dan pengendalian manajemen secara parsialVerhoef et al. (2021) memetakan tahapan digitisasi hingga transformasi digital pada level organisasi, tetapi tidak menautkannya dengan kerangka SPM; penelitian ini melengkapinya dengan menempatkan transformasi tersebut ke dalam tiga pilar pengendalian digital yang konkret. Fähndrich (2023) menunjukkan bahwa digitalisasi mengubah dimensi tugas, instrumen, dan perilaku pengendalian manajemen, namun belum menyentuh tata kelola data, AI, dan keamanan siber sebagai komponen teknis; temuan penelitian ini memberikan spesifikasi komponen tersebut. Sementara Zhang et al. (2025) berfokus pada dimensi perilaku manajemen algoritmik, penelitian ini menautkan dimensi tersebut dengan fondasi tata kelola data dan perlindungan cyber control secara terintegrasi. Dengan demikian, penelitian ini menegaskan sekaligus memperluas temuan terdahulu melalui kerangka integratif yang belum dirumuskan sebelumnya.

Interpretasi Makna Hasil. Secara substantif, hasil kajian menunjukkan bahwa keunggulan pengendalian digital tidak ditentukan oleh kecanggihan salah satu pilar, melainkan oleh keseimbangan dan keterpaduan ketiganya. Tata kelola data yang kuat tanpa perlindungan siber yang setara, atau adopsi AI tanpa fondasi data yang andal, justru menimbulkan ketimpangan pengendalian. Makna teoretis temuan ini adalah bahwa Sistem Pengendalian Manajemen di era digital paling tepat dipahami sebagai sistem umpan balik sosiosibernetik (Hamid, 2026b), yakni

ketiga pilar bekerja sebagai satu siklus adaptif yang saling menopang, bukan sebagai modul teknologi yang berdiri sendiri.Refleksi Implikasi Hasil. Bagi pengembangan teori, kerangka integratif tiga pilar memperkaya literatur SPM dengan memasukkan dimensi pengendalian digital yang selama ini belum tersistematisasi. Bagi praktik manajemen, hasil ini merefleksikan perlunya pergeseran cara pandang: investasi teknologi harus disertai penguatan kepemimpinan digital, kompetensi sumber daya manusia, dan budaya berbasis data agar menghasilkan kinerja yang berkelanjutan. Refleksi ini juga menyiratkan bahwa hubungan antara integrasi tata kelola digital dan kinerja organisasi bersifat kontingen, sehingga tidak dapat digeneralisasi tanpa mempertimbangkan konteks kepemimpinan dan kematangan digital organisasi.

Implikasi Kebijakan dan Rencana Aksi. Berdasarkan sintesis di atas, penelitian ini merekomendasikan rencana aksi bertahap bagi organisasi. Pertama, membangun fondasi tata kelola data melalui penetapan kebijakan data, klasifikasi sensitivitas, dan pengukuran kualitas data (International, 2017); Hamid, 2021). Kedua, menerapkan kerangka Responsible AI yang mencakup penilaian risiko, pengujian bias, dan mekanisme human-in-the-loop sebelum penerapan sistem AI kritis (EUROPEIA, 2021); OECD, 2019). Ketiga, memperkuat postur keamanan siber dengan mengadopsi NIST Cybersecurity Framework 2.0 dan (Folorunso et al., 2024) serta mengintegrasikannya ke dalam Enterprise Risk Management (((US) & (US), 2024); (Folorunso et al., 2024); Hamid, 2022). Keempat, menempatkan tata kelola digital pada agenda dewan direksi disertai indikator kinerja lintas pilar dan program peningkatan kompetensi digital yang berkelanjutan (Zukis, 2022); (Dhakal et al., 2024). Rangkaian tindakan ini menautkan temuan konseptual dengan langkah kebijakan yang dapat dioperasionalkan organisasi.

KESIMPULAN

Sejalan dengan tujuan penelitian, studi ini memetakan konsep dan ruang lingkup data governance, artificial intelligence (AI), dan cyber control sebagai tiga pilar utama tata kelola digital dalam kerangka Sistem Pengendalian Manajemen (SPM), menganalisis keterkaitan integratif di antara ketiganya, serta merumuskan proposisi teoretis mengenai hubungannya dengan kematangan digital dan kinerja organisasi. Hasil sintesis literatur menunjukkan bahwa data governance menjadi fondasi yang menjamin kualitas dan keandalan data, AI memperkuat kemampuan analitik dan deteksi risiko melalui tata kelola algoritma yang etis dan akuntabel, sedangkan cyber control melindungi data dan sistem AI dari ancaman siber. Ketiga pilar tersebut saling melengkapi sehingga tata kelola digital perlu diterapkan sebagai suatu sistem yang terintegrasi, bukan sekadar adopsi teknologi secara parsial.

Lebih lanjut, sintesis literatur menunjukkan bahwa integrasi ketiga pilar tata kelola digital berhubungan positif dengan kematangan digital dan kinerja organisasi, meskipun efektivitasnya dipengaruhi oleh kepemimpinan digital, kompetensi sumber daya manusia, dan budaya organisasi berbasis data. Secara konseptual, penelitian ini menawarkan kerangka integratif yang menjawab kesenjangan penelitian terdahulu yang masih mengkaji ketiga pilar secara terpisah. Temuan ini mengimplikasikan bahwa organisasi perlu membangun pengendalian digital secara holistik dengan menyeimbangkan pengelolaan data, pemanfaatan AI, dan penguatan keamanan siber. Selain memberikan kontribusi konseptual terhadap pengembangan Sistem Pengendalian Manajemen di era digital, kerangka yang dihasilkan juga diharapkan menjadi landasan bagi penelitian empiris

selanjutnya untuk menguji hubungan antarpilar tata kelola digital dengan kematangan digital dan berbagai indikator kinerja organisasi pada beragam sektor dan konteks.

DAFTAR PUSTAKA

Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Metode penelitian kualitatif studi pustaka. *Jurnal Edumaspul*, *6*(1), 974–980.

Aprilia, R., Kartika, D. A., Siregar, Y. D., & Darma, J. (2025). Management Control Systems in the Digital Age: Concepts, Implementation, and Implications. *Ilmu Ekonomi Manajemen Dan Akuntansi*, *6*(2), 191–201.

Budiarsyah, G. G. (2025a). Pengaruh Leverage Terhadap Risiko Financial Distress: Pendekatan Altman, Ohlson Dan Zmijewski. *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, 1424–1433.

Budiarsyah, G. G. (2025b). Pengaruh Leverage Terhadap Risiko Financial Distress: Pendekatan Altman, Ohlson Dan Zmijewski. *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, 1424–1433.

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*, *5*(2009), 12.

Chui, M., Hazan, E., Roberts, R., Singla, A., & Smaje, K. (2023). *The economic potential of generative AI*.

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: Https://Nvlpubs. Nist. Gov/Nistpubs/CSWP/NIST. CSWP*, *4162018*(7).

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). COBIT as a Framework for Enterprise Governance of IT. In *Enterprise governance of information technology: Achieving alignment and value in digital organizations* (pp. 125–162). Springer.

Dhakal, S. P., Nankervis, A., & Burgess, J. (2024). *The Future of Work in the Asia Pacifc*.

Eryurek, E., Gilad, U., Lakshmanan, V., Kibunguchy-Grant, A., & Ashdown, J. (2021). *Data governance: The definitive guide*. " O'Reilly Media, Inc."

EUROPEIA, C. (2021). Proposal for a Regulation on a European approach for Artificial Intelligence. *Bruxelas: Comissão Europeia*.

Fähndrich, J. (2023). A literature review on the impact of digitalisation on management control. *Journal of Management Control*, *34*(1), 9–65.

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, *24*(1), 2582–2595.

Goodfellow, I. (2016). *Deep learning*. MIT press.

Hamid, A. A. (2018). Analisis Pengaruh Kinerja Keuangan Daerah Terhadap Tingkat Kesejahteraan Masyarakat Kabupaten Majalengka–Jawa Barat. *Jurnal SEKURITAS (Saham, Ekonomi, Keuangan Dan Investasi)*, *1*.

Hamid, A. A. (2026a). *Corporate financial management & investment analysis*. Aceng Abdul Hamid.

Hamid, A. A. (2026b). *Corporate financial management & investment analysis*. Aceng Abdul Hamid.

Hamid, A. A., Razak, A., & Endri, E. (2023). *Bukri Corresponding Author: Determinants of bond*

rating and its implications to corporate bond yield.

Hamid, A. A., & Yanthi, W. D. (2025). Strategies To Increase Community Compliance In Paying Zakat Through Digitalization. *Journal of Social and Economics Research*, *7*(1), 43–48.

Harahap, I. N., Segara, K. G., Hutasuhut, S. A. H., & Nurbaiti, N. (2025). Konsep Dasar Sistem Data Governance Dalam Era Digitalisasi. *Journal Sains Student Research*, *3*(4), 295–303.

Haro, A., Judijanto, L., Khasanah, M., Saputra, K., Pratama, Y. H. C., Sinambela, A. T. P., & Siallagan, F. (2025). *Sistem Informasi Manajemen*. PT. Sonpedia Publishing Indonesia.

Hutasuhut, C. A. (2026). Eksplorasi Peran Manajemen Risiko Dalam Meningkatkan Efektivitas Keamanan Siber Pada Badan Siber Dan Sandi Negara. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(2), 1971–1986.

IBM Security, M. (2023). Cost of a data breach report 2023. *Ibm. Com*.

International, D. (2017). *DAMA-DMBOK: Data management body of knowledge*. Technics Publications, LLC.

Krasner, H. (2021). The cost of poor software quality in the US: A 2020 report. *Proc. Consortium Inf. Softw. QualityTM (CISQTM)*, *2*(3).

Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. *META Group Research Note*, *6*(70), 1.

Loshin, D. (2010). *The practitioner's guide to data quality improvement*. Elsevier.

Maliye, S. K. (2024). Multi-Cloud Automation: A Strategic Approach to Cloud Infrastructure Management. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, *10*(6), 183–190.

Mansfield-Devine, S. (2022). *IBM: cost of a data breach*. MA Business London.

Moyer, R. C., McGuigan, J. R., & Kretlow, W. J. (2003). *Contemporary financial management*. Thomson/South-Western.

Riadi, A., & Hamid, A. A. (2026). Desain Sistem Pengendalian Manajemen Sebagai Faktor Penentu Keberhasilan Implementasi Strategi Perusahaan. *Jurnal Riset Multidisiplin Edukasi*, *3*(7), 596–605.

Safarudin, R., Zulfamanna, Z., Kustati, M., & Sepriyanti, N. (2023). Penelitian kualitatif. *Innovative: Journal Of Social Science Research*, *3*(2), 9680–9694.

Schwab, K. (2016). The fourth industrial revolution. *World Economic Forum*, *12*.

Spencer, P. E. (2024). 2024 Sensitive Content Communications Privacy and Compliance Report. *Kiteworks*.

Taherdoost, H. (2023). Towards nuts and bolts of conducting literature review: A typology of literature review. *Electronics*, *12*(4), 800.

Tamtelahitu, T. M., Thaniket, R. M., Hanitha, V., & Sari, R. M. (2026). *Big Data Analytics*. Serasi Media Teknologi.

(US), N. I. of S. and T., & (US), N. I. of S. and T. (2024). *NIST Cybersecurity Framework 2.0: Quick-start Guide for Creating and Using Organizational Profiles*. US Department of Commerce, National Institute of Standards and Technology.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889–901.

Zhang, M. M., Cooke, F. L., Ahlstrom, D., & McNeil, N. (2025). The rise of algorithmic

management and implications for work and organisations. *New Technology, Work and Employment*, *40*(3), 659–671.

Zukis, B. (2022). Digital and cybersecurity governance around the world. *Annals of Corporate Governance*, *7*(1), 1–92.