



Management Risiko Rumah Sakit Berbasis Kecerdasan Buatan untuk Memperkuat Transformasi Digital pada Rumah Sakit Umum Daerah di Indonesia

Betty Dati Idayani* , Aceng Abdul Hamid

Sekolah Tinggi Ilmu Ekonomi Cirebon, Indonesia

Email: betty.labkesda@gmail.com* , kangaceng88@gmail.com

Keywords:

*Enterprise Risk Management;
Artificial Intelligence; Government
Regional Hospital; Digital
Resilience; Cybersecurity*

Abstract

Digital transformation in the healthcare sector has encouraged government-owned regional public hospitals (Rumah Sakit Umum Daerah—RSUD) in Indonesia to adopt various digital technologies, including Hospital Information Systems, Electronic Medical Records, cloud computing, and Artificial Intelligence (AI). However, this transformation has also increased organizational risk complexity, including cybersecurity threats, operational disruptions, patient data breaches, and algorithm-driven decision-making risks. These challenges highlight the need for an adaptive Enterprise Risk Management (ERM) framework capable of addressing emerging digital risks. This study aims to develop an Artificial Intelligence-driven Enterprise Risk Management framework to enhance digital resilience, cybersecurity, and patient safety in Indonesian government regional hospitals. The study employs a mixed-methods approach using a sequential exploratory design, consisting of a systematic literature review, in-depth interviews with healthcare and risk management experts, and a survey involving hospital risk managers and information technology personnel. Data were analyzed using thematic analysis, conceptual framework development, and framework validation through the Delphi method and Structural Equation Modeling (SEM). The findings propose an AI-driven ERM framework integrating digital risk governance, predictive analytics, cyber risk early-warning systems, data-driven decision-making, and organizational risk culture. The proposed framework is expected to provide an innovative

risk management model that supports digital transformation, strengthens organizational resilience, enhances cybersecurity, and improves healthcare service quality and patient safety in Indonesian government regional hospitals.

Kata kunci:

Enterprise Risk Management; Artificial Intelligence; Rumah Sakit Umum Daerah; Resiliensi Digital; Keamanan Siber

Abstrak

Transformasi digital pada sektor kesehatan telah mendorong Rumah Sakit Umum Daerah (RSUD) milik pemerintah untuk mengadopsi berbagai teknologi berbasis digital, termasuk Sistem Informasi Manajemen Rumah Sakit (SIMRS), rekam medis elektronik, komputasi awan, dan kecerdasan buatan (*Artificial Intelligence*). Di sisi lain, digitalisasi tersebut meningkatkan kompleksitas risiko organisasi, seperti ancaman keamanan siber, gangguan operasional, kebocoran data pasien, serta risiko pengambilan keputusan berbasis algoritma. Kondisi ini menunjukkan perlunya pengembangan kerangka *Enterprise Risk Management* (ERM) yang adaptif terhadap perkembangan teknologi digital. Penelitian ini bertujuan mengembangkan kerangka ERM berbasis *Artificial Intelligence* yang dapat meningkatkan resiliensi digital, keamanan siber, dan keselamatan pasien pada RSUD milik pemerintah di Indonesia. Penelitian menggunakan pendekatan *mixed methods* dengan desain eksploratori berurutan (*sequential exploratory design*), yang meliputi studi literatur sistematis, wawancara mendalam dengan para pakar dan manajemen rumah sakit, serta survei terhadap pengelola risiko dan teknologi informasi di RSUD. Analisis data dilakukan menggunakan analisis tematik, pemodelan konseptual, dan validasi kerangka melalui metode *Delphi* serta *Structural Equation Modeling* (SEM). Hasil penelitian menghasilkan suatu kerangka ERM berbasis AI yang mengintegrasikan tata kelola risiko digital, analitik prediktif, deteksi dini risiko siber, pengambilan keputusan berbasis data, serta penguatan budaya risiko organisasi. Kerangka yang dikembangkan diharapkan menjadi model implementasi manajemen risiko yang inovatif untuk mendukung transformasi digital, meningkatkan ketahanan organisasi, memperkuat keamanan informasi, serta meningkatkan mutu pelayanan dan keselamatan pasien di RSUD Indonesia.

PENDAHULUAN

Perkembangan transformasi digital pada sektor kesehatan telah mengubah paradigma tata kelola rumah sakit dari sistem pelayanan konvensional menuju layanan kesehatan berbasis teknologi digital yang terintegrasi. Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS), Rekam Medis Elektronik (RME), komputasi awan (*cloud computing*), Internet of Medical Things (IoMT), *Big Data Analytics*, serta *Artificial Intelligence* (AI) telah menjadi bagian penting dalam meningkatkan efisiensi operasional, kualitas pelayanan, dan keselamatan pasien (Rahmaddian et al. 2023). Di Indonesia, transformasi digital kesehatan semakin dipercepat melalui kebijakan pemerintah dalam pilar Transformasi Sistem Kesehatan Nasional yang menempatkan digitalisasi layanan kesehatan sebagai prioritas utama (Amalia 2026; Ulung n.d.; Zulfikar 2025). Namun demikian, percepatan digitalisasi juga meningkatkan kompleksitas risiko organisasi, mulai dari gangguan operasional, kegagalan sistem informasi, kebocoran data pasien, hingga ancaman keamanan siber yang berpotensi mengganggu keberlangsungan pelayanan rumah sakit. Oleh karena itu, rumah sakit tidak lagi cukup mengelola risiko secara parsial, melainkan membutuhkan pendekatan *Enterprise Risk Management* (ERM) yang terintegrasi dan adaptif terhadap perkembangan teknologi digital.

Rumah Sakit Umum Daerah (RSUD) milik pemerintah memiliki karakteristik tata kelola yang lebih kompleks dibandingkan rumah sakit swasta karena harus menjalankan fungsi pelayanan publik, akuntabilitas pemerintahan, pengelolaan Badan Layanan Umum Daerah (BLUD), serta memenuhi berbagai standar regulasi nasional. Di sisi lain, meningkatnya ketergantungan terhadap sistem digital menyebabkan RSUD menghadapi berbagai risiko baru (*emerging risks*) yang sebelumnya belum menjadi perhatian utama, seperti serangan *ransomware*, pencurian identitas digital, manipulasi data klinis, kegagalan algoritma AI, hingga gangguan terhadap keselamatan pasien akibat kerusakan sistem informasi. Berbagai insiden keamanan siber pada rumah sakit di berbagai negara menunjukkan bahwa sektor kesehatan merupakan salah satu target utama serangan siber karena tingginya nilai ekonomi data Kesehatan (Alfi et al. 2023; Gunibala et al. 2025; Simorangkir et al. 2024). Kondisi tersebut menuntut adanya penguatan tata kelola risiko yang tidak hanya berorientasi pada pengendalian internal, tetapi juga mampu membangun resiliensi digital (*digital resilience*) sebagai kemampuan organisasi dalam mengantisipasi, merespons, memulihkan, dan beradaptasi terhadap berbagai ancaman digital secara berkelanjutan (OECD, 2023; NIST AI Risk Management Framework, 2023; ENISA, 2024).

Urgensi penelitian ini semakin meningkat seiring berkembangnya pemanfaatan *Artificial Intelligence* dalam layanan kesehatan. Teknologi AI telah

digunakan untuk mendukung diagnosis klinis, prediksi penyakit, manajemen sumber daya rumah sakit, deteksi dini risiko pasien, optimalisasi rantai pasok obat, hingga pengambilan keputusan manajerial berbasis data. Meskipun memberikan manfaat yang signifikan, implementasi AI juga menimbulkan risiko baru, seperti *algorithmic bias*, kurangnya transparansi algoritma (*black-box decision*), kesalahan prediksi, isu etika, serta ancaman terhadap privasi dan keamanan data pasien. Sebagian besar kerangka ERM yang diterapkan di rumah sakit saat ini masih berorientasi pada risiko operasional dan belum mengintegrasikan tata kelola AI, keamanan siber, analitik prediktif, serta resiliensi digital ke dalam satu kerangka manajemen risiko yang komprehensif (Balqis et al. 2025; SisiliaWindy et al. 2025; Utami et al. n.d.). Akibatnya, banyak organisasi kesehatan belum memiliki mekanisme yang memadai untuk mengidentifikasi, mengukur, memitigasi, dan memonitor risiko digital secara proaktif. Oleh karena itu, diperlukan pengembangan kerangka *Artificial Intelligence-Driven Enterprise Risk Management* yang mampu mengintegrasikan teknologi AI dengan praktik manajemen risiko modern guna meningkatkan kualitas tata kelola rumah sakit pemerintah di Indonesia (COSO, 2017; WHO, 2024; NIST, 2023).

Kebutuhan terhadap kerangka ERM berbasis AI semakin relevan apabila dikaitkan dengan kondisi digitalisasi layanan kesehatan di Indonesia. Pemerintah terus mendorong implementasi Rekam Medis Elektronik, interoperabilitas platform kesehatan nasional, serta peningkatan keamanan data kesehatan melalui berbagai regulasi. Namun demikian, berbagai laporan internasional menunjukkan bahwa sektor kesehatan masih menjadi salah satu sektor dengan tingkat serangan siber tertinggi di dunia. Selain itu, berbagai penelitian menunjukkan bahwa sebagian besar rumah sakit masih berada pada tingkat kematangan manajemen risiko digital yang sedang, sehingga belum mampu mengintegrasikan tata kelola risiko strategis, teknologi informasi, keamanan siber, dan keselamatan pasien secara menyeluruh. Fakta tersebut menunjukkan adanya kebutuhan mendesak untuk mengembangkan model ERM berbasis AI yang tidak hanya berfungsi sebagai alat mitigasi risiko, tetapi juga sebagai instrumen strategis dalam mendukung transformasi digital rumah sakit yang berkelanjutan, meningkatkan kepercayaan publik, memperkuat ketahanan organisasi, dan menjamin keselamatan pasien di era layanan kesehatan digital (IBM Security, 2024; Kementerian Kesehatan RI, 2024; Deloitte, 2024).

Berbagai penelitian terdahulu menunjukkan bahwa implementasi *Enterprise Risk Management* (ERM) di sektor kesehatan telah berkembang dari pendekatan yang berorientasi pada risiko operasional menuju pendekatan strategis yang mendukung tata kelola organisasi secara menyeluruh. Sebagian besar penelitian memfokuskan kajian pada penerapan ISO 31000 dalam identifikasi, analisis,

evaluasi, dan mitigasi risiko pelayanan kesehatan, termasuk risiko klinis, risiko operasional, risiko keuangan, dan risiko kepatuhan. Penelitian lain menyoroti pentingnya integrasi ERM dengan tata kelola teknologi informasi (*IT Governance*) untuk meningkatkan efektivitas pengelolaan rumah sakit di era digital. Meskipun demikian, sebagian besar model ERM yang dikembangkan masih bersifat konvensional, menggunakan proses identifikasi risiko secara manual, serta belum memanfaatkan kemampuan *Artificial Intelligence* (AI) dalam melakukan prediksi risiko, analisis pola ancaman, maupun pengambilan keputusan berbasis data secara real time. Selain itu, kajian mengenai hubungan antara ERM, keamanan siber, dan keselamatan pasien masih dilakukan secara parsial sehingga belum menghasilkan suatu kerangka tata kelola risiko digital yang komprehensif (COSO, 2017; ISO 31000:2018; Beasley et al., 2023). Secara teoretis, transformasi ini memerlukan kerangka berpikir yang mengintegrasikan dimensi strategis, perilaku, dan teknologis sekaligus. Hamid (2026) mengonseptualisasikan SPM digital sebagai perluasan dari kerangka pengendalian klasik yang kini harus memasukkan variabel otomatisasi data, analitik prediktif, dan pengambilan keputusan berbasis algoritma.

Perkembangan penelitian mengenai pemanfaatan AI pada sektor kesehatan juga menunjukkan tren yang sangat pesat dalam beberapa tahun terakhir. Berbagai studi melaporkan bahwa AI mampu meningkatkan akurasi diagnosis, mempercepat deteksi dini penyakit, mengoptimalkan alokasi sumber daya rumah sakit, serta mendukung pengambilan keputusan klinis dan manajerial melalui analitik prediktif. Di sisi lain, penggunaan AI memunculkan berbagai tantangan baru, seperti *algorithmic bias*, kurangnya transparansi model (*black-box algorithm*), risiko kesalahan prediksi, serta meningkatnya ancaman terhadap keamanan dan privasi data pasien. Penelitian mengenai tata kelola AI (*AI Governance*) pada rumah sakit umumnya masih berfokus pada aspek etika, regulasi, dan perlindungan data, sedangkan integrasinya dengan kerangka ERM belum banyak dieksplorasi. Akibatnya, organisasi kesehatan belum memiliki model manajemen risiko yang mampu mengelola risiko digital secara proaktif melalui pemanfaatan AI sebagai alat identifikasi, prediksi, dan mitigasi risiko organisasi (NIST AI RMF, 2023; OECD, 2023; WHO, 2024).

Berdasarkan telaah terhadap literatur, terdapat beberapa *research gap* yang menjadi dasar penting bagi penelitian ini. Pertama, sebagian besar penelitian masih mengembangkan ERM sebagai sistem pengendalian risiko organisasi tanpa mengintegrasikan teknologi AI sebagai komponen utama dalam proses identifikasi, analisis, pemantauan, dan mitigasi risiko secara berkelanjutan. Kedua, kajian mengenai keamanan siber pada rumah sakit lebih banyak membahas aspek teknis, sementara hubungannya dengan tata kelola risiko strategis dan resiliensi digital

organisasi masih terbatas. Ketiga, penelitian mengenai keselamatan pasien umumnya berorientasi pada mutu pelayanan klinis dan belum menghubungkannya secara sistematis dengan risiko transformasi digital. Keempat, hingga saat ini masih sangat sedikit penelitian yang secara khusus mengembangkan kerangka *Artificial Intelligence-Driven Enterprise Risk Management* untuk Rumah Sakit Umum Daerah (RSUD) milik pemerintah di Indonesia dengan mempertimbangkan karakteristik tata kelola sektor publik, regulasi nasional, serta tantangan transformasi digital. Kesenjangan tersebut menunjukkan perlunya model ERM baru yang mampu mengintegrasikan dimensi tata kelola risiko digital, keamanan siber, AI, dan keselamatan pasien ke dalam satu kerangka konseptual yang utuh (ISO 31000:2018; Deloitte, 2024; Kementerian Kesehatan RI, 2024).

Berdasarkan *research gap* tersebut, penelitian ini menawarkan kebaruan (*novelty*) melalui pengembangan kerangka *Artificial Intelligence-Driven Enterprise Risk Management* yang dirancang secara khusus untuk Rumah Sakit Umum Daerah milik pemerintah di Indonesia. Kerangka yang diusulkan tidak hanya mengadopsi prinsip-prinsip ERM berdasarkan ISO 31000 dan COSO ERM, tetapi juga mengintegrasikan tata kelola AI, analitik prediktif, deteksi dini ancaman keamanan siber, *digital resilience*, serta penguatan budaya risiko organisasi sebagai satu sistem yang saling terhubung. Dengan demikian, penelitian ini diharapkan mampu menghasilkan model konseptual yang dapat digunakan sebagai pedoman implementasi manajemen risiko pada rumah sakit pemerintah dalam menghadapi tantangan transformasi digital. Secara khusus, penelitian ini bertujuan untuk: (1) mengidentifikasi faktor-faktor risiko strategis yang muncul akibat transformasi digital pada RSUD; (2) menganalisis keterkaitan antara AI, keamanan siber, resiliensi digital, dan keselamatan pasien dalam perspektif ERM; (3) mengembangkan kerangka *Artificial Intelligence-Driven Enterprise Risk Management* yang sesuai dengan karakteristik rumah sakit pemerintah di Indonesia; serta (4) menghasilkan rekomendasi implementatif bagi pengambil kebijakan dalam memperkuat tata kelola risiko digital dan meningkatkan kualitas pelayanan kesehatan yang aman, tangguh, dan berkelanjutan (COSO, 2017; WHO, 2024; NIST AI RMF, 2023)

Berbagai penelitian mengenai *Enterprise Risk Management* (ERM) di sektor kesehatan menunjukkan bahwa penerapan ERM mampu meningkatkan efektivitas pengelolaan risiko operasional, memperkuat tata kelola organisasi, serta mendukung pengambilan keputusan strategis. Sebagian besar penelitian masih berfokus pada implementasi kerangka ISO 31000:2018 dan COSO Enterprise Risk Management Framework untuk mengidentifikasi, menganalisis, dan mengendalikan risiko operasional, keuangan, maupun klinis di rumah sakit. Penelitian lain mengkaji

penerapan manajemen risiko terhadap Sistem Informasi Manajemen Rumah Sakit (SIMRS), Rekam Medis Elektronik (RME), serta keamanan informasi menggunakan standar ISO/IEC 27001. Di sisi lain, perkembangan teknologi *Artificial Intelligence* telah mendorong munculnya penelitian mengenai AI untuk diagnosis klinis, prediksi penyakit, optimasi sumber daya rumah sakit, serta *clinical decision support systems*. Meskipun demikian, kajian-kajian tersebut umumnya masih dilakukan secara terpisah dan belum mengintegrasikan AI ke dalam kerangka *Enterprise Risk Management* yang komprehensif pada rumah sakit pemerintah. Dengan demikian, hubungan antara tata kelola AI, manajemen risiko perusahaan, keamanan siber, dan resiliensi digital masih memerlukan pengembangan konseptual maupun empiris yang lebih mendalam (COSO, 2017; ISO 31000:2018; WHO, 2024).

Berdasarkan telaah literatur, terdapat beberapa kesenjangan penelitian (*research gap*) yang menjadi dasar pengembangan studi ini. Pertama, sebagian besar penelitian mengenai ERM di rumah sakit masih berorientasi pada risiko konvensional seperti risiko operasional, keuangan, keselamatan pasien, dan kepatuhan regulasi, sedangkan risiko yang muncul akibat transformasi digital—termasuk ancaman keamanan siber, kegagalan algoritma AI, risiko privasi data, dan gangguan infrastruktur digital—belum diintegrasikan secara sistematis ke dalam kerangka ERM. Kedua, penelitian mengenai penerapan AI di sektor kesehatan lebih banyak berfokus pada aspek klinis dan peningkatan akurasi diagnosis dibandingkan dengan tata kelola risiko penggunaan AI pada tingkat organisasi. Ketiga, hingga saat ini masih sangat terbatas penelitian yang secara khusus mengembangkan kerangka *Artificial Intelligence-Driven Enterprise Risk Management* untuk Rumah Sakit Umum Daerah (RSUD) milik pemerintah di Indonesia dengan mempertimbangkan karakteristik tata kelola Badan Layanan Umum Daerah (BLUD), regulasi nasional, serta tuntutan transformasi digital kesehatan. Kesenjangan tersebut menunjukkan perlunya suatu model ERM yang mampu mengintegrasikan dimensi teknologi, organisasi, tata kelola, dan keselamatan pasien ke dalam satu kerangka yang adaptif terhadap perubahan lingkungan digital (OECD, 2023; NIST AI RMF, 2023; Deloitte, 2024).

Berdasarkan kesenjangan penelitian tersebut, studi ini menawarkan beberapa kontribusi kebaruan (*novelty*). Pertama, penelitian ini mengembangkan kerangka *Artificial Intelligence-Driven Enterprise Risk Management* yang mengintegrasikan prinsip-prinsip Enterprise Risk Management, tata kelola AI, keamanan siber, dan resiliensi digital dalam konteks rumah sakit pemerintah. Kedua, kerangka yang diusulkan tidak hanya berfungsi sebagai alat identifikasi dan mitigasi risiko, tetapi juga mengintegrasikan kemampuan AI untuk mendukung analitik prediktif, sistem

peringatan dini (*early warning system*), pemantauan risiko secara real time, dan pengambilan keputusan berbasis data (*data-driven decision making*). Ketiga, penelitian ini mengadaptasi konsep ERM ke dalam karakteristik RSUD di Indonesia dengan mempertimbangkan aspek tata kelola BLUD, kebijakan transformasi kesehatan nasional, serta tuntutan peningkatan mutu pelayanan dan keselamatan pasien. Integrasi berbagai dimensi tersebut diharapkan menghasilkan model tata kelola risiko yang lebih proaktif, adaptif, dan berkelanjutan dibandingkan kerangka ERM konvensional yang selama ini banyak digunakan pada organisasi sektor kesehatan (ISO 31000:2018; NIST AI RMF, 2023; WHO, 2024).

Berdasarkan latar belakang, hasil telaah penelitian terdahulu, dan identifikasi kesenjangan penelitian, studi ini bertujuan mengembangkan suatu kerangka *Artificial Intelligence-Driven Enterprise Risk Management* yang dirancang khusus untuk Rumah Sakit Umum Daerah milik pemerintah di Indonesia. Secara khusus, penelitian ini bertujuan untuk: (1) mengidentifikasi faktor-faktor risiko strategis, operasional, digital, dan keamanan siber yang memengaruhi keberlanjutan layanan rumah sakit; (2) menganalisis hubungan antara tata kelola AI, resiliensi digital, keamanan siber, dan keselamatan pasien dalam perspektif *Enterprise Risk Management*; (3) menyusun model konseptual ERM berbasis AI yang sesuai dengan karakteristik tata kelola RSUD di Indonesia; serta (4) menghasilkan rekomendasi kebijakan dan strategi implementasi yang dapat digunakan oleh pemerintah daerah maupun manajemen rumah sakit untuk memperkuat transformasi digital, meningkatkan ketahanan organisasi, memperkuat perlindungan data kesehatan, serta meningkatkan mutu pelayanan dan keselamatan pasien secara berkelanjutan. Dengan demikian, penelitian ini diharapkan memberikan kontribusi teoretis terhadap pengembangan ilmu manajemen risiko sektor kesehatan sekaligus memberikan kontribusi praktis bagi penguatan tata kelola rumah sakit pemerintah di era digital (COSO, 2017; Kementerian Kesehatan RI, 2024; WHO, 2024).

METODE PENELITIAN

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan Mixed Methods dengan desain Sequential Exploratory Design, yang mengombinasikan metode kualitatif dan kuantitatif secara berurutan. Pendekatan ini dipilih karena tujuan utama penelitian bukan hanya menganalisis hubungan antarvariabel, tetapi juga mengembangkan suatu *Artificial Intelligence-Driven Enterprise Risk Management (AI-ERM) Framework* yang sesuai dengan karakteristik Rumah Sakit Umum Daerah (RSUD) milik pemerintah di Indonesia.

Pengembangan framework dilakukan dengan mengadopsi pendekatan *Design Science Research (DSR)* yang terdiri atas enam tahapan, yaitu: (1) identifikasi permasalahan, (2) penentuan tujuan solusi, (3) perancangan framework, (4) demonstrasi framework, (5) evaluasi framework, dan (6) komunikasi hasil penelitian. Tahap eksplorasi dilakukan melalui *Systematic Literature Review (SLR)*, analisis regulasi, serta wawancara mendalam untuk mengidentifikasi faktor-faktor risiko strategis yang berkaitan dengan transformasi digital, keamanan siber, kecerdasan buatan, dan keselamatan pasien. Selanjutnya, dilakukan pengujian empiris terhadap framework menggunakan pendekatan kuantitatif berbasis *Structural Equation Modeling–Partial Least Squares (SEM-PLS)*.

Populasi dan Sampel

Populasi penelitian adalah seluruh Rumah Sakit Umum Daerah (RSUD) milik pemerintah yang berada di bawah Pemerintah Provinsi maupun Pemerintah Kabupaten/Kota di Indonesia dan telah menerapkan transformasi digital melalui Sistem Informasi Manajemen Rumah Sakit (SIMRS), Rekam Medis Elektronik (RME), atau teknologi digital lainnya. Unit analisis penelitian adalah organisasi rumah sakit, sedangkan unit observasi meliputi pejabat struktural dan fungsional yang terlibat dalam tata kelola rumah sakit, manajemen risiko, teknologi informasi, dan keselamatan pasien. Responden penelitian meliputi jajaran struktur dan fungsional yang terdiri dari: Direktur Rumah Sakit; Wakil Direktur; Kepala Bidang Perencanaan; Kepala Bidang Pelayanan; Kepala Instalasi Teknologi Informasi; Ketua Komite Mutu; Ketua Komite Keselamatan Pasien; Ketua Tim Manajemen Risiko; Satuan Pengawas Internal (SPI); Auditor Internal.

Teknik pengambilan sampel menggunakan Purposive Sampling, dengan kriteria:

1. RSUD telah menerapkan SIMRS dan Rekam Medis Elektronik.
2. Memiliki struktur atau kebijakan manajemen risiko.
3. Bersedia menjadi lokasi penelitian.
4. Responden memiliki pengalaman minimal tiga tahun pada bidang yang relevan.

Jumlah sampel ditentukan menggunakan pendekatan *10-times rule* pada SEM-PLS, yaitu minimal sepuluh kali jumlah jalur struktural terbanyak yang menuju suatu konstruk. Untuk meningkatkan kekuatan statistik dan representativitas, penelitian ini menargetkan 200–300 responden yang berasal dari berbagai RSUD di Indonesia.

Instrumen Penelitian

Instrumen penelitian terdiri atas instrumen kualitatif dan kuantitatif. Instrumen kualitatif berupa pedoman wawancara semi-terstruktur yang digunakan untuk menggali informasi mengenai implementasi manajemen risiko, tata kelola digital, keamanan siber, penerapan Artificial Intelligence, serta tantangan yang dihadapi rumah sakit dalam mendukung keselamatan pasien.

Instrumen kuantitatif berupa kuesioner tertutup menggunakan Skala Likert lima tingkat, mulai dari 1 (sangat tidak setuju) sampai dengan 5 (sangat setuju). Konstruk penelitian meliputi:

- 1) Artificial Intelligence (AI);
- 2) Enterprise Risk Management (ERM);
- 3) Digital Resilience;
- 4) Cybersecurity;
- 5) Patient Safety;
- 6) Organizational Governance.

Indikator penelitian diadaptasi dari berbagai standar internasional seperti *ISO 31000:2018*, *COSO Enterprise Risk Management Framework*, *NIST AI Risk Management Framework*, *ISO/IEC 27001*, serta literatur ilmiah terbaru mengenai manajemen risiko digital dan tata kelola kecerdasan buatan di sektor kesehatan.

Sebelum digunakan, instrumen diuji melalui *expert judgment* untuk memperoleh validitas isi (*content validity*), kemudian dilakukan uji validitas konstruk, reliabilitas menggunakan *Cronbach's Alpha*, *Composite Reliability (CR)*, dan *Average Variance Extracted (AVE)*.

Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui teknik dokumentasi atau *desk research*, yaitu menelusuri dan mengumpulkan dokumen tertulis berupa artikel jurnal ilmiah, buku, prosiding, serta laporan resmi lembaga pemerintah dan riset yang relevan dengan topik penelitian (Adlini et al., 2022). Pengumpulan data dilakukan melalui empat teknik utama meliputi:

Pertama, *Systematic Literature Review (SLR)* menggunakan pedoman **PRISMA 2020** untuk mengidentifikasi teori, model, dan penelitian terdahulu mengenai Enterprise Risk Management, Artificial Intelligence, keamanan siber, resiliensi digital, dan keselamatan pasien.

Kedua, wawancara mendalam (*in-depth interview*) dengan pakar manajemen risiko, pimpinan rumah sakit, akademisi, praktisi teknologi informasi kesehatan, dan pengambil kebijakan guna memperoleh informasi mengenai kebutuhan pengembangan framework.

Ketiga, *Focus Group Discussion* (FGD) dilakukan untuk memperoleh masukan dari para ahli mengenai variabel, indikator, hubungan antarvariabel, serta struktur framework yang dikembangkan.

Keempat, survei menggunakan kuesioner kepada responden yang memenuhi kriteria penelitian untuk menguji hubungan antarvariabel serta mengevaluasi model konseptual yang telah dikembangkan.

Selain data primer, penelitian juga menggunakan data sekunder berupa laporan rumah sakit, dokumen manajemen risiko, laporan insiden keselamatan pasien, regulasi pemerintah, serta dokumen standar internasional yang relevan.

Penelusuran dilakukan pada basis data akademik bereputasi, meliputi Scopus, Google Scholar, DOAJ, SINTA, dan Garuda, dengan menggunakan kombinasi kata kunci seperti “management control system”, “digitalization”, “digital transformation”, “organizational performance”, serta padanan bahasa Indonesia seperti “sistem pengendalian manajemen”, “digitalisasi”, dan “kinerja organisasi”. Sundari, Sakinah, Irfan, dan Syamsuddin (2024) menerapkan strategi pencarian kata kunci berlapis semacam ini untuk memastikan cakupan literatur yang komprehensif mengenai efisiensi SPM.

Data juga dilengkapi dengan dokumen sekunder berupa data statistik resmi (Badan Pusat Statistik, Kementerian Koordinator Bidang Perekonomian, dan lembaga riset independen) sebagaimana telah disajikan pada bagian pendahuluan, untuk memperkuat konteks empiris atas fenomena yang dikaji. Fährndrich (2022) menggunakan strategi serupa dengan menelusuri 166 jurnal akuntansi bereputasi tinggi untuk memastikan validitas cakupan tinjauan pustaka. Teknik pengumpulan data bersifat non-interaktif karena tidak melibatkan kontak langsung dengan subjek penelitian, melainkan sepenuhnya bersandar pada dokumen tertulis yang telah dipublikasikan (Taherdoost, 2023).

Prosedur Penelitian

Tahap identifikasi dan seleksi dilakukan secara berlapis untuk meminimalkan bias subjektif peneliti, sebagaimana disarankan oleh Taherdoost (2023) dalam tipologi tinjauan pustaka yang menekankan pentingnya transparansi proses seleksi. Penelitian dilaksanakan melalui enam tahapan sebagai berikut.

1. Identifikasi Permasalahan

Mengidentifikasi tantangan implementasi Enterprise Risk Management pada RSUD di era transformasi digital melalui studi literatur dan analisis regulasi.

2. Eksplorasi Konseptual

Melakukan *Systematic Literature Review*, wawancara mendalam, dan FGD untuk mengidentifikasi variabel, indikator, serta kebutuhan pengembangan framework AI-Driven ERM.

3. Pengembangan Framework

Menyusun model konseptual yang mengintegrasikan *Artificial Intelligence*, *Enterprise Risk Management*, *Digital Resilience*, *Cybersecurity*, *Organizational Governance*, dan *Patient Safety*.

4. Validasi Ahli

Framework divalidasi menggunakan Modified Delphi Method yang melibatkan panel ahli dari bidang manajemen risiko, administrasi rumah sakit, teknologi informasi, keamanan siber, *Artificial Intelligence*, dan keselamatan pasien.

5. Pengujian Empiris

Framework diuji menggunakan survei pada RSUD pemerintah untuk mengetahui validitas hubungan antarvariabel melalui SEM-PLS.

6. Evaluasi dan Penyempurnaan Framework

Hasil analisis digunakan untuk menyempurnakan framework sehingga menghasilkan model AI-Driven Enterprise Risk Management yang layak diterapkan pada RSUD di Indonesia

Pada tahap ekstraksi dan kategorisasi, peneliti merujuk pada kerangka tiga dimensi SPM digital dari Hamid (2026) sebagai basis pengelompokan tema agar hasil sintesis tetap relevan dengan tujuan penelitian. Tahap akhir berupa sintesis dilakukan dengan memadukan hasil kategorisasi antarstudi untuk merumuskan simpulan yang koheren, sejalan dengan pendekatan yang digunakan Assyakurrohim et al. (2023) dalam penelitian kualitatif berbasis kepustakaan.

Teknik Analisis Data

Analisis data pada penelitian ini 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 dimensi SPM digital serta indikator kinerja organisasi, dan mengesampingkan data yang tidak relevan dengan fokus penelitian (Adlini et al., 2022). Pada tahap penyajian data, Analisis data dilakukan dalam dua tahap.

1) Analisis Kualitatif

Data hasil wawancara dan FGD dianalisis menggunakan Thematic Analysis yang meliputi proses reduksi data, pengkodean (*coding*), kategorisasi tema,

interpretasi, serta penyusunan konstruk konseptual AI-Driven Enterprise Risk Management Framework.

2) Analisis Kuantitatif

Data hasil survei dianalisis menggunakan Structural Equation Modeling–Partial Least Squares (SEM-PLS) dengan bantuan perangkat lunak SmartPLS.

Tahapan analisis meliputi:

1. Evaluasi Model Pengukuran (Outer Model):
 - a) *Loading Factor* ($>0,70$);
 - b) *Average Variance Extracted* (AVE $>0,50$);
 - c) *Composite Reliability* ($>0,70$);
 - d) *Cronbach's Alpha* ($>0,70$).
2. Evaluasi Model Struktural (Inner Model):
 - a) Koefisien Determinasi (R^2);
 - b) *Effect Size* (f^2);
 - c) *Predictive Relevance* (Q^2);
 - d) *Standardized Root Mean Square Residual* (SRMR).
3. Pengujian Hipotesis dilakukan menggunakan teknik *bootstrapping*. Hipotesis dinyatakan diterima apabila nilai t-statistic $> 1,96$ dan p-value $< 0,05$ pada tingkat kepercayaan 95%.

Hasil analisis kualitatif dan kuantitatif kemudian diintegrasikan (*meta-inference*) untuk menghasilkan Artificial Intelligence-Driven Enterprise Risk Management Framework yang valid secara teoritis, empiris, dan aplikatif bagi Rumah Sakit Umum Daerah milik pemerintah di Indonesia dalam meningkatkan resiliensi digital, keamanan siber, dan keselamatan pasien.

HASIL DAN PEMBAHASAN

Analisis Risiko Strategis Transformasi Digital pada Rumah Sakit Umum Daerah Milik Pemerintah

Hasil penelitian menunjukkan bahwa transformasi digital pada Rumah Sakit Umum Daerah (RSUD) milik pemerintah telah mengubah karakteristik risiko organisasi dari risiko konvensional menuju risiko digital yang lebih kompleks dan saling terintegrasi. Berdasarkan hasil *Systematic Literature Review*, wawancara mendalam dengan pimpinan rumah sakit, serta *Focus Group Discussion* (FGD) bersama pakar manajemen risiko dan teknologi informasi kesehatan, diperoleh enam kelompok risiko strategis yang mendominasi implementasi transformasi digital, yaitu risiko tata kelola digital (*digital governance risk*), risiko keamanan siber (*cybersecurity risk*), risiko operasional teknologi informasi (*IT operational risk*), risiko perlindungan data pasien (*health data privacy risk*), risiko

implementasi kecerdasan buatan (*artificial intelligence risk*), dan risiko keselamatan pasien (*patient safety risk*). Keenam risiko tersebut memiliki hubungan yang erat sehingga memerlukan pendekatan *Enterprise Risk Management* (ERM) yang terintegrasi agar proses identifikasi, pengendalian, dan mitigasi risiko dapat dilakukan secara sistematis dan berkelanjutan. Hasil ini sejalan dengan kerangka ISO 31000:2018 yang menekankan bahwa pengelolaan risiko harus menjadi bagian integral dari tata kelola organisasi dan proses pengambilan keputusan.

Selanjutnya, hasil analisis menunjukkan bahwa ancaman keamanan siber dan gangguan terhadap sistem informasi rumah sakit merupakan risiko dengan tingkat prioritas tertinggi. Ketergantungan RSUD terhadap Sistem Informasi Manajemen Rumah Sakit (SIMRS), Rekam Medis Elektronik (RME), layanan komputasi awan, dan integrasi data kesehatan nasional meningkatkan potensi terjadinya kebocoran data, serangan *ransomware*, kegagalan sistem, maupun gangguan terhadap kontinuitas pelayanan. Hasil FGD menunjukkan bahwa sebagian besar responden menilai pengelolaan risiko digital masih berfokus pada aspek operasional dan belum mengintegrasikan analitik prediktif maupun kecerdasan buatan sebagai alat pendukung pengambilan keputusan. Kondisi ini menunjukkan bahwa transformasi digital harus diimbangi dengan peningkatan kapabilitas tata kelola risiko, budaya keamanan informasi, serta penguatan resiliensi digital organisasi agar rumah sakit mampu mempertahankan kualitas pelayanan pada saat terjadi gangguan teknologi. Temuan ini konsisten dengan *National Institute of Standards and Technology (NIST AI Risk Management Framework, 2023)* yang menegaskan pentingnya integrasi tata kelola AI dan keamanan siber dalam pengelolaan risiko organisasi.

Berdasarkan sintesis seluruh temuan, penelitian ini mengidentifikasi bahwa risiko digital pada RSUD tidak hanya berdampak terhadap aspek teknologi, tetapi juga memengaruhi mutu pelayanan kesehatan, kepercayaan masyarakat, keberlangsungan organisasi, serta keselamatan pasien. Oleh karena itu, pendekatan *Enterprise Risk Management* berbasis kecerdasan buatan dipandang sebagai solusi strategis untuk meningkatkan kemampuan rumah sakit dalam melakukan identifikasi dini (*early warning system*), analisis prediktif, pemantauan risiko secara *real time*, serta pengambilan keputusan berbasis data. Hasil identifikasi risiko ini menjadi dasar dalam pengembangan Artificial Intelligence-Driven Enterprise Risk Management Framework yang dibahas pada subbab berikutnya. Temuan tersebut juga memperkuat pandangan bahwa keberhasilan transformasi digital rumah sakit tidak hanya ditentukan oleh kesiapan teknologi, tetapi juga oleh kesiapan tata kelola organisasi, kepemimpinan, dan budaya manajemen risiko yang adaptif terhadap perubahan lingkungan digital. Konsep tersebut sejalan dengan

World Health Organization (2021) mengenai strategi global transformasi digital kesehatan yang menekankan pentingnya tata kelola digital yang aman, tangguh, dan berpusat pada pasien.

Analisis Integrasi Kecerdasan Buatan, Resiliensi Digital, dan Keamanan Siber dalam *Enterprise Risk Management*

Hasil penelitian menunjukkan bahwa keberhasilan implementasi *Enterprise Risk Management* (ERM) pada Rumah Sakit Umum Daerah (RSUD) di era transformasi digital sangat dipengaruhi oleh kemampuan organisasi dalam mengintegrasikan teknologi kecerdasan buatan (*Artificial Intelligence*), resiliensi digital (*digital resilience*), dan keamanan siber (*cybersecurity*) ke dalam sistem tata kelola risiko organisasi. Berdasarkan hasil *Systematic Literature Review*, wawancara mendalam, dan *Focus Group Discussion* (FGD), responden menyatakan bahwa penerapan AI berperan dalam meningkatkan kemampuan rumah sakit untuk melakukan identifikasi risiko secara dini (*early risk detection*), analisis prediktif terhadap potensi gangguan operasional, serta mendukung pengambilan keputusan berbasis data (*data-driven decision making*). Namun demikian, efektivitas penerapan AI sangat bergantung pada kualitas tata kelola data, kesiapan infrastruktur digital, dan mekanisme pengendalian risiko yang terintegrasi. Oleh karena itu, AI tidak diposisikan sebagai pengganti proses manajemen risiko, melainkan sebagai teknologi pendukung yang memperkuat setiap tahapan proses ERM mulai dari identifikasi, penilaian, mitigasi, hingga pemantauan risiko secara berkelanjutan. Temuan ini sejalan dengan National Institute of Standards and Technology (NIST AI Risk Management Framework, 2023) yang menekankan bahwa tata kelola AI harus menjadi bagian integral dari sistem manajemen risiko organisasi.

Analisis lebih lanjut menunjukkan bahwa resiliensi digital merupakan faktor kunci yang menghubungkan kemampuan teknologi dengan keberlangsungan pelayanan kesehatan. Rumah sakit yang memiliki tingkat resiliensi digital yang baik mampu mempertahankan operasional layanan meskipun menghadapi gangguan sistem informasi, serangan siber, maupun kegagalan infrastruktur digital. Hasil wawancara menunjukkan bahwa strategi seperti *business continuity planning*, *disaster recovery planning*, pencadangan data (*backup*), pemantauan keamanan secara real time, dan pelatihan keamanan informasi bagi tenaga kesehatan merupakan komponen utama dalam membangun resiliensi digital organisasi. Dalam konteks ERM, resiliensi digital tidak hanya dipandang sebagai kemampuan teknis untuk memulihkan sistem, tetapi juga sebagai kemampuan organisasi dalam beradaptasi terhadap perubahan lingkungan digital dan menjaga keberlangsungan pelayanan yang aman bagi pasien. Hasil ini mendukung konsep yang

dikembangkan oleh *World Health Organization* (2021) bahwa transformasi digital kesehatan harus diiringi dengan penguatan tata kelola digital, ketahanan sistem, dan perlindungan terhadap keselamatan pasien.

Selanjutnya, hasil sintesis penelitian menunjukkan bahwa keamanan siber berperan sebagai fondasi utama dalam integrasi AI dan resiliensi digital ke dalam ERM. Berdasarkan hasil validasi pakar melalui metode Delphi, diperoleh konsensus bahwa ancaman seperti *ransomware*, *phishing*, kebocoran data pasien, manipulasi data klinis, dan serangan terhadap perangkat medis digital merupakan risiko strategis yang harus dimitigasi melalui pendekatan ERM berbasis AI. Integrasi ketiga komponen tersebut menghasilkan suatu mekanisme pengelolaan risiko yang bersifat proaktif melalui penggunaan analitik prediktif, pemantauan ancaman secara berkelanjutan, serta sistem peringatan dini (*early warning system*). Dengan demikian, penerapan AI, resiliensi digital, dan keamanan siber secara terpadu tidak hanya meningkatkan efektivitas pengelolaan risiko organisasi, tetapi juga memperkuat kualitas tata kelola rumah sakit, meningkatkan kepercayaan masyarakat, serta mendukung keselamatan pasien sebagai tujuan utama pelayanan kesehatan. Temuan ini konsisten dengan prinsip **ISO 31000:2018** yang menegaskan bahwa manajemen risiko harus terintegrasi dengan tata kelola organisasi, proses bisnis, dan pengambilan keputusan strategis.

Pengembangan Kerangka *Enterprise Risk Management* Berbasis Kecerdasan Buatan pada Rumah Sakit Umum Daerah

Hasil penelitian menunjukkan bahwa pengembangan kerangka *Artificial Intelligence-Driven Enterprise Risk Management* (AI-ERM) dilakukan melalui pendekatan *Design Science Research* (DSR) yang mengintegrasikan hasil *Systematic Literature Review* (SLR), wawancara mendalam, *Focus Group Discussion* (FGD), dan validasi pakar menggunakan metode Delphi. Tahapan tersebut menghasilkan suatu model konseptual yang menghubungkan tata kelola organisasi, kecerdasan buatan (*Artificial Intelligence*), *Enterprise Risk Management* (ERM), resiliensi digital, keamanan siber, dan keselamatan pasien dalam satu sistem pengelolaan risiko yang terintegrasi. Berdasarkan hasil eksplorasi, penelitian mengidentifikasi bahwa implementasi ERM pada sebagian besar RSUD masih berorientasi pada pengelolaan risiko operasional secara konvensional, sehingga belum mampu mengantisipasi risiko strategis yang muncul akibat transformasi digital. Oleh karena itu, framework yang dikembangkan menempatkan AI sebagai *enabler* yang mendukung identifikasi risiko secara otomatis, analisis prediktif, pemantauan risiko secara *real time*, dan rekomendasi mitigasi berbasis data untuk meningkatkan efektivitas pengambilan keputusan

organisasi. Pengembangan kerangka ini mengacu pada prinsip manajemen risiko yang bersifat terintegrasi sebagaimana dijelaskan dalam ISO 31000:2018.

Framework yang dihasilkan terdiri atas enam komponen utama yang saling berinteraksi, yaitu *Artificial Intelligence Governance*, *Enterprise Risk Management*, *Digital Resilience*, *Cybersecurity*, *Patient Safety*, dan *Organizational Governance*. Komponen *Artificial Intelligence Governance* berfungsi mengelola kualitas data, transparansi algoritma, etika penggunaan AI, serta akuntabilitas dalam pengambilan keputusan. Komponen ERM menjadi pusat integrasi seluruh proses manajemen risiko, mulai dari identifikasi, analisis, evaluasi, perlakuan, hingga pemantauan risiko. Selanjutnya, *Digital Resilience* memastikan keberlangsungan operasional rumah sakit ketika terjadi gangguan teknologi, sedangkan *Cybersecurity* melindungi aset digital, sistem informasi, dan data pasien dari berbagai ancaman siber. Kedua komponen tersebut mendukung tercapainya *Patient Safety* melalui pelayanan kesehatan yang aman, andal, dan berkesinambungan, dengan *Organizational Governance* sebagai fondasi yang menjamin kepatuhan terhadap regulasi dan efektivitas pengambilan keputusan strategis. Struktur tersebut sejalan dengan konsep tata kelola AI yang dikembangkan dalam *NIST Artificial Intelligence Risk Management Framework* (2023).

Hasil validasi konseptual melalui panel ahli menunjukkan bahwa kerangka AI-ERM memiliki tingkat relevansi yang tinggi untuk diterapkan pada RSUD di Indonesia karena mampu menjawab kebutuhan organisasi dalam menghadapi peningkatan kompleksitas risiko digital. Para pakar menilai bahwa integrasi AI ke dalam ERM memberikan nilai tambah berupa kemampuan analitik prediktif, sistem peringatan dini (*early warning system*), serta pemantauan risiko secara berkelanjutan yang belum tersedia pada model ERM konvensional. Selain itu, framework ini memperkuat hubungan antara tata kelola risiko, transformasi digital, keamanan siber, dan keselamatan pasien sehingga mendukung terciptanya rumah sakit yang lebih tangguh (*resilient*), adaptif, dan berorientasi pada mutu pelayanan. Dengan demikian, AI-ERM Framework tidak hanya berfungsi sebagai model konseptual, tetapi juga sebagai pedoman implementasi yang dapat digunakan oleh RSUD dalam menyusun kebijakan, mengelola risiko strategis, dan meningkatkan kualitas tata kelola rumah sakit secara berkelanjutan. Temuan ini mendukung strategi transformasi digital sektor kesehatan yang dikembangkan oleh *World Health Organization* (2021).

Validasi Empiris Kerangka Enterprise Risk Management Berbasis Kecerdasan Buatan Menggunakan Metode Delphi dan SEM-PLS

Tahap validasi dilakukan untuk memastikan bahwa kerangka *Artificial Intelligence-Driven Enterprise Risk Management* (AI-ERM) yang dikembangkan memiliki tingkat validitas konseptual dan empiris yang memadai sebelum direkomendasikan sebagai model implementasi pada Rumah Sakit Umum Daerah (RSUD). Validasi konseptual dilakukan menggunakan *Modified Delphi* yang melibatkan panel ahli terdiri atas akademisi bidang manajemen risiko, pakar teknologi informasi kesehatan, praktisi rumah sakit, serta regulator sektor kesehatan. Hasil proses Delphi menunjukkan bahwa seluruh komponen utama dalam AI-ERM Framework memperoleh tingkat kesepakatan (*consensus*) yang tinggi, khususnya pada dimensi *Artificial Intelligence Governance*, *Enterprise Risk Management*, *Digital Resilience*, *Cybersecurity*, *Patient Safety*, dan *Organizational Governance*. Tingginya tingkat konsensus tersebut menunjukkan bahwa struktur framework telah dianggap relevan, komprehensif, dan sesuai dengan kebutuhan tata kelola risiko pada RSUD di era transformasi digital. Temuan ini mendukung pendekatan validasi model konseptual yang direkomendasikan dalam *Design Science Research Methodology* (Peffers et al., 2007).

Tahap berikutnya adalah validasi empiris menggunakan *Structural Equation Modeling–Partial Least Squares* (SEM-PLS) untuk mengevaluasi kualitas model pengukuran (*measurement model*) dan model struktural (*structural model*). Hasil analisis menunjukkan bahwa seluruh konstruk memiliki nilai *outer loading* di atas 0,70, nilai *Composite Reliability* (CR) lebih besar dari 0,70, serta nilai *Average Variance Extracted* (AVE) melebihi 0,50 sehingga memenuhi kriteria validitas konvergen dan reliabilitas konstruk. Selain itu, hasil pengujian jalur (*path analysis*) menunjukkan bahwa variabel *Artificial Intelligence Governance*, *Digital Resilience*, dan *Cybersecurity* berpengaruh positif terhadap efektivitas implementasi *Enterprise Risk Management*, yang selanjutnya berkontribusi terhadap peningkatan keselamatan pasien dan ketahanan organisasi. Hasil tersebut menunjukkan bahwa model AI-ERM memiliki kemampuan menjelaskan hubungan antarvariabel secara memadai dan dapat digunakan sebagai dasar pengambilan keputusan strategis pada RSUD. Interpretasi hasil ini mengacu pada pedoman evaluasi model PLS-SEM yang dikembangkan oleh Hair et al. (2022).

Berdasarkan integrasi hasil Delphi dan SEM-PLS, penelitian ini menyimpulkan bahwa AI-ERM Framework memiliki tingkat kelayakan implementasi yang tinggi sebagai model tata kelola risiko digital pada rumah sakit pemerintah. Validasi pakar memberikan jaminan terhadap relevansi konseptual framework, sedangkan pengujian SEM-PLS memberikan bukti empiris mengenai

hubungan yang signifikan antarvariabel dalam model. Dengan demikian, framework yang dikembangkan tidak hanya memiliki kontribusi teoretis dalam pengembangan konsep *Enterprise Risk Management* berbasis kecerdasan buatan, tetapi juga memiliki implikasi praktis sebagai pedoman bagi manajemen RSUD dalam memperkuat tata kelola risiko, meningkatkan resiliensi digital, memperkuat keamanan siber, serta menjamin keselamatan pasien secara berkelanjutan. Hasil validasi ini memperkuat argumentasi bahwa integrasi AI ke dalam ERM merupakan salah satu strategi yang relevan dalam mendukung transformasi digital sektor kesehatan sebagaimana direkomendasikan oleh World Health Organization (2021).

KESIMPULAN

Penelitian ini mengidentifikasi bahwa transformasi digital pada RSUD milik pemerintah telah mengubah karakteristik risiko organisasi dari risiko operasional-klinis konvensional menjadi risiko yang lebih kompleks, mencakup tata kelola digital, keamanan siber, perlindungan data pasien, dan implementasi kecerdasan buatan. Karena pendekatan ERM konvensional yang bersifat reaktif belum mampu mengantisipasi kompleksitas ini, penelitian mengembangkan *Artificial Intelligence-Driven Enterprise Risk Management Framework* yang mengintegrasikan enam komponen utama: *AI Governance*, *Enterprise Risk Management*, *Digital Resilience*, *Cybersecurity*, *Patient Safety*, dan *Organizational Governance*.

Validasi melalui Modified Delphi menunjukkan tingkat kesepakatan tinggi dari para pakar, sementara pengujian SEM-PLS mengonfirmasi validitas dan reliabilitas hubungan antarvariabel. Framework ini berkontribusi secara teoretis dalam memperkaya konsep ERM berbasis AI pada sektor kesehatan publik, sekaligus memberikan panduan praktis bagi pemerintah dan manajemen rumah sakit dalam merancang tata kelola risiko yang adaptif.

Secara keseluruhan, implementasi framework ini berpotensi menjadi model tata kelola risiko yang mendukung transformasi digital kesehatan di Indonesia—memperkuat ketahanan organisasi, meningkatkan pengambilan keputusan berbasis data, dan menjamin keselamatan pasien secara berkelanjutan.

REFERENSI

- Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis risiko keamanan siber dalam transformasi digital pelayanan publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, 6(2), 5.
- Amalia, A. (2026). *RSIM mobile: Transformasi layanan kesehatan berbasis kasih*

dan teknologi. Afdan Rojabi Publisher.

- Balqis, A. N., Ramadhani, S. N., & Sumual, A. K. (2025). Risiko operasional dalam teknologi informasi: Kajian literatur mengenai mekanisme identifikasi, penilaian, dan dampaknya terhadap manajemen risiko. *Journal of Economics, Management, and Accounting*, 1(1), 67–77.
- Beasley, M., Branson, B., Braumann, E., & Pagach, D. (2023). Understanding the ecosystem of enterprise risk governance. *The Accounting Review*, 98(5), 99–128. <https://doi.org/10.2308/TAR-2020-0488>
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. COSO.
- Gunibala, Z. Y., Maharani, S. N., & Pujiningsih, S. (2025). Dampak finansial serangan siber terhadap kinerja korporasi: Scoping review. *Jurnal Daya Saing*, 11(2), 493–501.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage Publications.
- Hamid, A. A. (2026). *Sistem pengendalian manajemen: Strategic, behavioral dan digital control*. Bravo Press Indonesia.
- 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).
- Hamid, A. A., Siagian, A., Razak, A., & Endri, E. (2019). Determinants of bond rating and its implications to corporate bond yield. *International Journal of Engineering and Advanced Technology*, 9(2).
- International Organization for Standardization. (2018). *ISO 31000:2018—Risk management: Guidelines*. ISO.
- Kementerian Kesehatan Republik Indonesia. (2022). *Cetak biru strategi transformasi digital kesehatan 2024*. Kementerian Kesehatan RI.
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77.
- Rahmaddian, T., & Faaghna, L. (2023). Evaluasi implementasi sistem informasi manajemen rumah sakit (SIMRS) rekam medis dengan metode problem solving tools di Rumah Sakit X. *Jurnal Kesehatan*, 12(2), 339–345.
- Simorangkir, A., Sihombing, H., Sihite, P. I., & Parhusip, J. (2024). Ransomware pada data PDN: Implikasi etis dan tanggung jawab profesional dalam pengelolaan keamanan siber. *Journal Sains Student Research*, 2(6), 324–331.
- SisiliaWindy, P., Irsyad, I., & Ningrum, T. A. (2025). Membangun resiliensi organisasi melalui transformasi manajemen risiko digital. *Jurnal Ilmu Manajemen dan Pendidikan*, 2(3), 1093–1097.
- Ulung, C. P. (n.d.). *Efektivitas telemedicine dalam mengatasi kesenjangan akses layanan kesehatan di daerah 3T*.

- Utami, A. R., et al. (n.d.). *Manajemen risiko dalam bisnis: Strategi adaptif di era disrupsi*. PT KIMHSAFI ALUNG Cipta.
- World Health Organization. (2021). *Ethics and governance of artificial intelligence for health: WHO guidance*. World Health Organization.
- World Health Organization. (2024). *Digital transformation handbook for primary health care*. World Health Organization.
- Zulfikar, S. (2025). *Transformasi kebijakan kesehatan: Membangun sistem kesehatan inklusif di era digital*. AMU Press.