HIJM
HORIZON: Indonesian Journal of Multidisciplinary

p-ISSN: 2987-7776
e-ISSN: 2987-7180
Vol. 4, No. 3, 2026

PENGEMBANGAN KERANGKA KONSEPTUAL RISIKO MIGRASI HYBRID CLOUD COMPUTING: TINJAUAN LITERATUR NARATIF PERSPEKTIF SISTEM INFORMASI

Cakra Trinata[1], Vita Nurul Fathya[2], Besse Hartati[3],
Arief Febrianto[4], Pascalis Danny Kristi Wibowo[5]
[1, 3, 4, 5]Politeknik Imigrasi dan Pemasyarakatan Indonesia, Jl. Raya Gandul No.4, Depok, Jawa Barat, Indonesia
[2]Politeknik Pengayoman Indonesia, Jl. Raya Gandul No.4, Depok, Jawa Barat, Indonesia
Email: trinatacakra@gmail.com

Article History

Received: 27-04-2026

Revision: 09-05-2026

Accepted: 11-05-2026

Published: 13-05-2026

Abstract. Migration to hybrid cloud computing is increasingly being implemented by organizations to achieve a balance between flexibility, security, and cost efficiency in supporting digital transformation. However, integration across private and public cloud environments and the use of multi-cloud environments creates technical and socio-technical complexities that increase operational risks. This study aims to develop a conceptual framework for hybrid cloud migration risks from an Information Systems perspective. The research method uses a narrative literature review of 23 relevant scientific articles. The analysis process is carried out in two stages: grouping literature findings into operational risk domains and mapping risks using Threat, Vulnerability, Risk Factors, Impact, and Damage components. The results identify eight key risk domains, including information security and privacy, compliance and regulation, migration costs, downtime and service availability, existing system integration and compatibility, interoperability and lock-in risk, observability and cross-cloud monitoring, and socio-technical readiness and information technology governance. The resulting conceptual framework emphasizes the importance of integrated risk management through a combination of technical controls and governance mechanisms. Practically, this framework can be utilized to help organizations identify, prioritize, and mitigate hybrid cloud migration risks more systematically.

Keywords: Hybrid Cloud, Cloud Migration, Risk Management, Conceptual Framework, Information Systems, Narrative Literature Review

Abstrak. Migrasi ke hybrid cloud computing semakin banyak diterapkan oleh organisasi untuk mencapai keseimbangan antara fleksibilitas, keamanan, dan efisiensi biaya dalam mendukung transformasi digital. Namun, integrasi lintas lingkungan private dan public cloud serta penggunaan multi-cloud menimbulkan kompleksitas teknis dan sosio-teknis yang meningkatkan risiko operasional. Penelitian ini bertujuan mengembangkan kerangka konseptual risiko migrasi hybrid cloud dari perspektif Sistem Informasi. Metode penelitian menggunakan tinjauan literatur naratif terhadap 23 artikel ilmiah yang relevan. Proses analisis dilakukan melalui dua tahap, yaitu pengelompokan temuan literatur ke dalam domain risiko yang bersifat operasional dan pemetaan risiko menggunakan komponen Threat, Vulnerability, Risk Factors, Impact, dan Damage. Hasil penelitian mengidentifikasi delapan domain risiko utama, meliputi keamanan informasi dan privasi, kepatuhan dan regulasi, biaya migrasi, downtime dan ketersediaan layanan, integrasi sistem eksisting dan kompatibilitas, interoperabilitas dan risiko lock-in, observability serta monitoring lintas cloud, dan kesiapan sosio-teknis serta tata kelola teknologi informasi. Kerangka konseptual yang dihasilkan menegaskan pentingnya pengelolaan risiko secara terpadu melalui kombinasi kontrol teknis dan mekanisme tata kelola. Secara praktis, kerangka ini dapat dimanfaatkan untuk membantu organisasi dalam mengidentifikasi, memprioritaskan, dan memitigasi risiko migrasi hybrid cloud secara lebih sistematis.

Kata Kunci: *Hybrid Cloud*, Migrasi *Cloud*, Manajemen Risiko, Kerangka Konseptual, Sistem Informasi, Tinjauan Literatur Naratif

How to Cite: Trinata, C., Fathya, V. N., Hartati, B., Febrianto, A., & Wibowo, P. D. K. (2026). Pengembangan Kerangka Konseptual Risiko Migrasi *Hybrid Cloud Computing*: Tinjauan Literatur Naratif Perspektif Sistem Informasi. *HORIZON: Indonesian Journal of Multidisciplinary*, 4 (3), 461-472. http://doi.org/10.54373/hijm.v4i3.5485

PENDAHULUAN

Transformasi digital mendorong organisasi untuk memodernisasi sistem informasi melalui adopsi *cloud computing* karena kemampuannya meningkatkan efisiensi operasional, fleksibilitas, dan skalabilitas layanan (Modisane & Jokonya, 2021; Merlo et al., 2025; Nahla et al., 2025; Sudianto & Sutopo, 2025). Pemanfaatan *cloud* tidak hanya dipahami sebagai perubahan teknologi, tetapi juga sebagai pengungkit transformasi proses bisnis dan penguatan kapabilitas digital organisasi. Oleh karena itu, keputusan migrasi ke *cloud* menjadi bagian dari strategi transformasi yang berdampak pada tata kelola, proses organisasi, serta kinerja layanan (Merlo et al., 2025; Mulyana et al., 2024).

Dalam praktiknya, migrasi menuju cloud menghadapi berbagai tantangan, terutama terkait keamanan, kepatuhan regulasi, pengendalian biaya, dan keberlangsungan layanan. Tantangan tersebut menuntut pendekatan mitigasi risiko yang sistematis dan terencana (Adabala, 2024; Ghebreselassie et al., 2025; Sharma, 2023). Kompleksitas ini semakin meningkat ketika organisasi mengadopsi *hybrid cloud* yang mengombinasikan infrastruktur on-premise atau *private cloud* dengan *public cloud* (Anh, 2025; Kommisetty & Abhireddy, 2024).

Arsitektur *hybrid* dan *multi-cloud* membawa konsekuensi pada meningkatnya kompleksitas integrasi dan operasi sistem akibat heterogenitas platform, kebutuhan orkestrasi sumber daya, serta dinamika migrasi lintas lingkungan (Altahat et al., 2025; Waseem et al., 2025). Pada sistem eksisting berskala besar, proses migrasi sering kali menuntut refactoring kode atau perancangan ulang arsitektur, yang berimplikasi pada jadwal implementasi, kebutuhan sumber daya, pembengkakan biaya, dan potensi *downtime* layanan (Kommareddy, 2025; Althani, 2025).

Sejumlah kajian mengelompokkan risiko migrasi *cloud* ke dalam beberapa fokus utama, yaitu keamanan dan ancaman siber termasuk penerapan *Zero Trust* dan deteksi ancaman real-time (Awan, 2025; Bellamkonda, 2022; Lilhore et al., 2025; Rashid & Yaseen, 2025; Tanjung et al., 2025), privasi dan kepatuhan pengelolaan data lintas yurisdiksi (Adabala, 2024; Junior et al., 2025; Sharma, 2023), serta isu biaya, interoperabilitas, dan *observability* pada lingkungan *multi-cloud* (Altahat et al., 2025; Putra et al., 2025; Waseem et al., 2025). Pada aspek monitoring dan keamanan, pendekatan analitik berbasis jejak proses juga digunakan untuk mendeteksi anomali pemrosesan data dalam sistem *multi-cloud* (Zhang et al., 2023).

Meskipun demikian, sebagian besar kajian masih membahas risiko secara parsial dan terpisah. Padahal, migrasi *hybrid cloud* memerlukan kerangka terintegrasi dari perspektif Sistem Informasi yang mengaitkan aspek teknologi, proses, dan tata kelola. Struktur *Threat–Vulnerability–Risk Factors–Impact–Damage* telah digunakan dalam analisis risiko migrasi

cloud (Maniah et al., 2022), namun penerapannya belum secara eksplisit dikaitkan dengan domain risiko *hybrid cloud* serta belum diperkuat oleh dimensi kesiapan sosio-teknis dan tata kelola teknologi informasi yang berperan penting dalam efektivitas pengendalian risiko (Merlo et al., 2025; Mulyana et al., 2024).

Berdasarkan celah tersebut, kebaruan artikel ini terletak pada pengembangan kerangka konseptual risiko migrasi *hybrid cloud* yang mengintegrasikan domain risiko *hybrid* dan *multi-cloud* dengan struktur penilaian *Threat–Vulnerability–Risk Factors–Impact–Damage*, serta menempatkan kesiapan sosio-teknis dan tata kelola teknologi informasi sebagai domain kunci lintas risiko (Anh, 2025; Junior et al., 2025; Maniah et al., 2022; Mulyana et al., 2024; Waseem et al., 2025). Permasalahan kajian dirumuskan sebagai upaya menyusun kerangka konseptual terintegrasi untuk memetakan dan menilai risiko migrasi *hybrid cloud* yang dapat digunakan sebagai dasar mitigasi dan prioritisasi kontrol. Untuk menjawab permasalahan tersebut, penelitian ini menggunakan metode tinjauan literatur naratif yang disusun secara terstruktur.

METODE

Penelitian ini menggunakan metode tinjauan literatur naratif untuk menyusun sintesis konseptual mengenai risiko migrasi *hybrid cloud computing* dari perspektif Sistem Informasi. Pendekatan naratif dipilih karena tujuan penelitian tidak berfokus pada pengujian hipotesis atau penghitungan efek kuantitatif, melainkan pada integrasi temuan lintas studi menjadi kerangka konseptual yang koheren dan operasional. Tahapan penelitian diawali dengan penetapan fokus kajian, yang meliputi: (1) identifikasi domain risiko migrasi *hybrid cloud*; (2) pemetaan risiko ke dalam komponen *Threat–Vulnerability–Risk Factors–Impact–Damage*; dan (3) perumusan kerangka konseptual risiko migrasi *hybrid cloud* (Maniah et al., 2022). Fokus ini digunakan sebagai dasar dalam penelusuran dan seleksi literatur.

Penelusuran literatur dilakukan menggunakan kata kunci yang relevan dengan konteks migrasi *hybrid* dan *multi-cloud*, antara lain *hybrid/multi-cloud migration*, *threat detection*, *cloud security risks*, *Zero Trust*, *cloud data privacy*, *cloud compliance*, *containerization*, *legacy migration*, *virtual machine migration management*, serta *observability* dan *monitoring*. Kata kunci tersebut dirancang untuk mencakup aspek tantangan migrasi, strategi teknis, keamanan, privasi, dan operasi lintas *cloud* (Adabala, 2024; Altahat et al., 2025; Ghebreselassie et al., 2025; Junior et al., 2025; Sharma, 2023; Waseem et al., 2025).

Literatur yang dianalisis dipilih berdasarkan kriteria inklusi dan eksklusi. Kriteria inklusi meliputi artikel yang membahas migrasi *cloud*, *hybrid cloud*, atau *multi-cloud* serta memuat pembahasan mengenai risiko, tantangan, atau strategi mitigasi yang dapat disintesis secara

konseptual. Kriteria eksklusi mencakup sumber yang tidak secara langsung terkait dengan konteks migrasi *cloud* atau tidak menyediakan temuan yang bersifat operasional dan relevan dengan tujuan penelitian.

Teknik analisis data dilakukan melalui sintesis kualitatif tematik. Setiap artikel dianalisis untuk mengidentifikasi isu risiko utama, kemudian diklasifikasikan ke dalam domain risiko yang sejenis. Selanjutnya, risiko-risiko tersebut dipetakan ke dalam komponen *Threat, Vulnerability, Risk Factors, Impact,* dan *Damage* untuk memperjelas hubungan sebab akibat dan implikasi operasionalnya. Tahap akhir analisis adalah merangkai domain risiko dan komponen penilaian risiko tersebut menjadi kerangka konseptual terintegrasi yang menggambarkan struktur risiko migrasi *hybrid cloud* secara sistematis.

HASIL

Hasil tinjauan menunjukkan bahwa risiko migrasi hybrid cloud terbentuk dari kombinasi faktor teknis dan organisasi yang saling berinteraksi, sehingga perlu dipetakan dalam domain operasional untuk mendukung penilaian risiko dan prioritas kontrol (Maniah et al., 2022; Ghebreselassie et al., 2025; Adabala, 2024; Sharma, 2023). Pada hybrid dan multi-cloud, kompleksitas meningkat karena heterogenitas platform, integrasi lintas lingkungan, dan kebutuhan orkestrasi yang konsisten (Waseem et al., 2025; Altahat et al., 2025).

Tabel 1. Klasifikasi domain risiko migrasi *hybrid cloud* (hasil sintesis literatur).

Kode	Domain risiko	Definisi operasional (konteks migrasi hybrid)	Indikator/isu kunci yang sering muncul	Risiko saat migrasi	Rujukan utama (author–year)
R1	Keamanan informasi & privasi	Risiko gangguan CIA (*confidentiality–integrity–availability*) lintas private–public cloud	kontrol akses, enkripsi, *Zero Trust*, deteksi ancaman, konfigurasi	*breach/unauthorized access*, *malware*, permukaan serangan meningkat	(Bellamkonda, 2022); (Lilhore et al., 2025); (Rashid & Yaseen, 2025); (Awan, 2025); (Tanjung et al., 2025).
R2	Kepatuhan & regulasi	Risiko pelanggaran regulasi lintas yurisdiksi	*data residency*, *privacy law*, *auditability*	penalti, *distrust*, reputasi turun	(Junior et al., 2025); (Sharma, 2023); (Adabala, 2024).
R3	Finansial & biaya migrasi	Risiko pembengkakan biaya migrasi/operasi hybrid	*hidden cost*, *egress*, *bill shock*, *over-provisioning*	*cost overruns*, biaya pengeluaran biaya tak terduga	(Adabala, 2024); (Anh, 2025); (Kommisetty & Abhireddy, 2024).
R4	Ketersediaan layanan & *downtime*	Risiko gangguan saat	*Business Continuity Planning*	*downtime*, produktivitas turun	(Ghebreselassie et al., 2025); (Adabala, 2024).

		cutover/sinkronisasi	(BCP) / *Disaster Recovery* (DR), *rollback, service interruption*		
R5	Integrasi sistem eksisting & kompatibilitas	Risiko integrasi sistem eksisting ke *hybrid cloud*	*dependency*, kompatibilitas, *refactor/re-architect*	*incompatibility*, *timeline* memanjang	(Althani, 2025); (Kommareddy, 2025).
R6	Interoperabilitas/portabilitas & *lock-in*	Risiko vendor *lock-in* dan portabilitas rendah	*proprietary components*, *licensing*, *portability limits*	*switching cost* tinggi	(Waseem et al., 2025); (Putra et al., 2025); (Sharma, 2023).
R7	*Observability* /monitoring lintas cloud	Risiko visibilitas telemetri rendah lintas *cloud*	fragmentasi log, monitoring limitation, QoS	deteksi insiden terlambat, *Quality of Service (QoS)* turun	(Waseem et al., 2025); (Altahat et al., 2025); (Zhang et al., 2023).
R8	*Socio-technical readiness/governance*	Risiko karena *skill gap* & *governance* lemah	IT *governance*, kompetensi, *resource constraints*	misconfiguration, inefisiensi, manfaat tak tercapai	(Maniah et al., 2022); (Mulyana et al., 2024); (Merlo et al., 2025).

Sumber: Berdasarkan sintesis literatur

Pembahasan pada Tabel 1 memperlihatkan bahwa risiko migrasi hybrid cloud tidak berdiri sendiri, melainkan saling terkait antar domain. Tabel tersebut merangkum delapan domain risiko (R1–R8) yang mencerminkan interaksi antara aspek teknis dan organisasional dalam proses migrasi hybrid cloud. Domain R8, yaitu kesiapan sosio-teknis dan tata kelola teknologi informasi, tampak berperan sebagai pengungkit utama karena menentukan efektivitas penerapan kontrol keamanan, pengendalian biaya, serta keberlanjutan transformasi digital secara keseluruhan (Mulyana et al., 2024; Merlo et al., 2025). Dari sisi teknis, tabel menunjukkan bahwa arsitektur hybrid dan multi-cloud meningkatkan kebutuhan akan kontrol keamanan yang adaptif, termasuk penerapan Zero Trust dan mekanisme deteksi ancaman secara real-time, sebagai respons terhadap meningkatnya permukaan serangan dan kompleksitas integrasi lintas platform (Lilhore et al., 2025; Rashid & Yaseen, 2025). Selain itu, penggunaan containerization pada lingkungan multi-cloud juga memperkuat urgensi observability dan monitoring lintas cloud untuk menjaga kualitas layanan dan ketersediaan sistem (Waseem et al., 2025).

Secara keseluruhan, isi tabel menegaskan keterkaitan langsung dengan topik penelitian ini, yaitu perlunya kerangka konseptual risiko yang terintegrasi dalam migrasi hybrid cloud. Meskipun cloud menawarkan efisiensi dan skalabilitas, tabel menunjukkan bahwa manfaat tersebut hanya dapat dicapai apabila organisasi mampu mengelola risiko biaya, downtime, dan integrasi sistem secara sistematis melalui tata kelola dan kesiapan organisasi yang memadai (Modisane & Jokonya, 2021; Nahla et al., 2025; Sudianto & Sutopo, 2025).

Pemetaan Komponen Penilaian Risiko (*Threat–Vulnerability–Risk Factors–Impact–Damage*)

Untuk menurunkan domain R1–R8 menjadi penilaian operasional, risiko dipetakan menggunakan komponen Threat–Vulnerability–Risk Factors–Impact–Damage (Maniah et al., 2022). Struktur ini menghubungkan penyebab teknis dan organisasional dengan konsekuensi layanan serta dampak bisnis (Adabala, 2024; Sharma, 2023).

Tabel 2. Pemetaan ringkas komponen risiko migrasi hybrid cloud (R1–R8)..

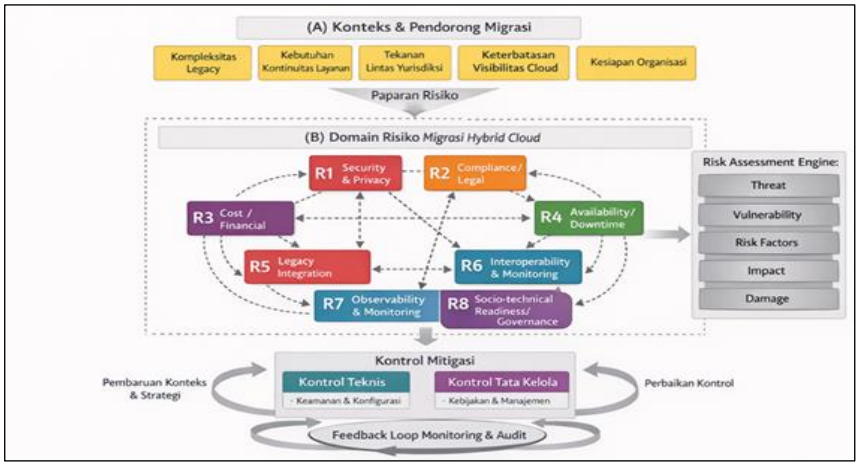
Domain	***Threat***	***Vulnerability***	***Risk Factors***	***Impact***	***Damage***
R1	*breach/unauthorized access; malware*	*misconfiguration ;* kontrol akses tak konsisten	*hybrid complexity*; ancaman meningkat	*compromise* data/layanan	kerugian finansial; reputasi turun
R2	*non-compliance* lintas yurisdiksi	*auditability* tidak konsisten	variasi regulasi/standar	penalties; distrust	kerusakan reputasi; risiko legal
R3	*bill shock/cost overruns*	estimasi biaya tak akurat	pengeluaran biaya tak terduga*; parallel run*	biaya melampaui rencana	tekanan anggaran; proyek tertunda
R4	*service disruption* saat *cutover*	*rollback/BCP readiness* rendah	*dependency chain* kompleks	*downtime*; produktivitas turun	kehilangan pendapatan; ketidakpuasan
R5	*integration failure/compatibility issues*	*dependency legacy* tinggi	*refactor/re-architect*	*timeline* memanjang; biaya naik	beban Sumber Daya Manusia; biaya jangka panjang
R6	*lock-in/portability constraints*	*proprietary components*	heterogenitas *provider*	sulit pindah lintas *cloud*	Biaya pengalihan tinggi
R7	*detection delay*; telemetri terfragmentasi	*monitoring tools limitation*	orkestrasi *multi-cloud* kompleks	*QoS* turun; respon lambat	beban operasi meningkat
R8	*readiness gap (skill/governance)*	*skill gap*; koordinasi lemah	resistensi perubahan	*error* konfigurasi; inefisiensi	manfaat *cloud* tidak optimal

Sumber: Berdasarkan sintesis literature

Pemetaan pada Tabel 2 memperlihatkan bahwa banyak risiko berawal dari vulnerability berbasis konfigurasi dan proses, sehingga aspek kesiapan organisasi dan tata kelola teknologi informasi berperan sebagai faktor penentu yang memengaruhi seluruh domain risiko (Maniah et al., 2022; Mulyana et al., 2024). Pada multi-cloud, observability menjadi penting untuk mencegah telemetri yang terfragmentasi dan keterlambatan respons insiden (Waseem et al., 2025), serta dapat diperkuat melalui pendekatan analitik keamanan berbasis proses (Zhang et al., 2023). Pada aspek privasi dan kepatuhan, perlindungan data merupakan prasyarat utama agar risiko regulasi dapat ditekan (Junior et al., 2025).

DISKUSI

Sintesis domain risiko pada Tabel 1 dan pemetaan komponen penilaian pada Tabel 2 menjadi dasar penyusunan kerangka konseptual penelitian ini. Kerangka tersebut mengaitkan konteks migrasi hybrid cloud dengan paparan risiko R1–R8, proses penilaian risiko, strategi kontrol mitigasi, serta mekanisme umpan balik melalui monitoring dan audit sebagai satu kesatuan yang saling terhubung (Maniah et al., 2022; Adabala, 2024; Sharma, 2023; Waseem et al., 2025; Junior et al., 2025).



Gambar 1. Kerangka konseptual risiko migrasi *hybrid cloud computing*

Secara terpadu, kerangka konseptual ini menegaskan bahwa risiko migrasi hybrid cloud dipicu oleh keterkaitan langsung antara karakteristik teknis sistem dan kapasitas pengelolaan organisasi. Kompleksitas sistem legacy yang menuntut proses refactoring atau re-architecting tidak hanya meningkatkan beban integrasi, tetapi juga berdampak nyata pada eskalasi biaya migrasi dan risiko downtime layanan, terutama ketika ketergantungan antarkomponen sistem belum terdokumentasi dengan baik (Kommareddy, 2025; Althani, 2025). Pada saat yang sama, heterogenitas platform dalam lingkungan hybrid dan multi-cloud memperbesar tantangan

interoperabilitas dan portabilitas aplikasi, sehingga risiko lock-in tidak semata bersifat teknis, melainkan juga membatasi fleksibilitas strategis organisasi dalam jangka panjang (Waseem et al., 2025; Putra et al., 2025).

Kebutuhan observability lintas cloud muncul sebagai penghubung kritis antara aspek teknis dan kinerja layanan. Fragmentasi telemetri dan kurangnya visibilitas end-to-end berimplikasi langsung pada penurunan kualitas layanan (QoS) serta keterlambatan respons insiden, sehingga observability tidak dapat diposisikan sebagai fungsi operasional semata, melainkan sebagai kontrol risiko inti dalam arsitektur hybrid cloud (Waseem et al., 2025; Altahat et al., 2025). Dari perspektif keamanan, kerangka ini memperjelas bahwa efektivitas mitigasi risiko sangat bergantung pada konsistensi penerapan kontrol pencegahan dan deteksi, termasuk deteksi ancaman real-time, Zero Trust, dan pendekatan keamanan berbasis kecerdasan buatan, yang berfungsi untuk mengimbangi dinamika ancaman pada lingkungan lintas cloud (Bellamkonda, 2022; Lilhore et al., 2025; Rashid & Yaseen, 2025). Dukungan analitik berbasis proses semakin memperkuat kemampuan deteksi anomali dengan mengaitkan pola teknis dengan konteks operasional layanan (Zhang et al., 2023).

Pada ranah kepatuhan, kerangka ini menegaskan bahwa perlindungan data dan auditability merupakan prasyarat utama untuk menekan risiko regulasi, khususnya dalam pengelolaan data lintas yurisdiksi. Kegagalan mengintegrasikan kontrol privasi dan mekanisme audit ke dalam desain migrasi berpotensi mengubah risiko kepatuhan menjadi risiko strategis yang berdampak langsung pada reputasi dan keberlanjutan organisasi (Junior et al., 2025; Sharma, 2023). Dengan demikian, hubungan antarreferensi dalam kerangka ini tidak bersifat paralel, tetapi saling menguatkan dalam menjelaskan bagaimana risiko hybrid cloud terbentuk, berkembang, dan dapat dikendalikan secara sistematis.

Implikasi Teoretis

Secara teoretis, penelitian ini memperkuat pemahaman bahwa risiko migrasi hybrid cloud merupakan fenomena sosio-teknis yang harus dijelaskan melalui integrasi antara aspek teknologi, proses organisasi, dan tata kelola Sistem Informasi. Temuan ini menegaskan bahwa pendekatan risiko yang hanya berorientasi teknis tidak memadai untuk menjelaskan dinamika migrasi *hybrid cloud* yang melibatkan keputusan strategis, koordinasi lintas unit, serta perubahan pola kerja dan pengelolaan layanan. Kerangka konseptual yang dikembangkan memberikan kontribusi teoretis dengan menyatukan domain risiko yang sebelumnya banyak dibahas secara terpisah ke dalam struktur yang lebih komprehensif dan operasional. Dengan memetakan risiko ke dalam komponen *Threat–Vulnerability–Risk Factors–Impact–Damage*,

penelitian ini memperluas penggunaan kerangka penilaian risiko ke konteks hybrid dan multi-cloud, sehingga memperjelas hubungan sebab-akibat antara sumber risiko, kerentanan, dan dampaknya terhadap kinerja layanan serta tujuan organisasi.

Implikasi teoretis lainnya terletak pada penegasan peran kesiapan sosio-teknis dan tata kelola teknologi informasi sebagai konstruk kunci lintas domain risiko. Temuan ini memperkaya kajian Sistem Informasi dengan menunjukkan bahwa efektivitas kontrol keamanan, pengendalian biaya, dan keberhasilan integrasi sistem sangat dipengaruhi oleh kapasitas organisasi dalam mengelola perubahan dan menetapkan mekanisme pengambilan keputusan. Dengan demikian, penelitian ini memberikan dasar teoretis bagi pengembangan model risiko dan tata kelola migrasi *cloud* yang lebih holistik dan kontekstual.

Implikasi Praktis

Secara praktis, hasil penelitian ini memiliki implikasi langsung terhadap perencanaan migrasi *hybrid cloud* yang perlu dipandang sebagai proses strategis dan bertahap, bukan sekadar proyek pemindahan infrastruktur. Kerangka yang dikembangkan menunjukkan bahwa perencanaan migrasi harus dimulai dengan pemetaan risiko lintas domain secara menyeluruh, mencakup aspek keamanan, biaya, ketersediaan layanan, integrasi sistem, hingga kesiapan organisasi. Dengan demikian, organisasi perlu memastikan bahwa keputusan arsitektural, jadwal migrasi, dan pemilihan teknologi sejak awal sudah selaras dengan kapasitas tata kelola dan sumber daya yang dimiliki.

Implikasi berikutnya adalah pentingnya menjadikan kesiapan sosio-teknis sebagai bagian dari perencanaan migrasi. Perencanaan yang hanya berfokus pada kesiapan teknis berisiko gagal ketika organisasi tidak siap dari sisi proses, koordinasi antarunit, dan pengambilan keputusan. Hasil penelitian ini menegaskan bahwa tata kelola teknologi informasi berperan sebagai mekanisme pengendali utama yang memastikan konsistensi kebijakan keamanan, pengelolaan biaya, serta pengendalian risiko operasional selama dan setelah migrasi berlangsung. Selain itu, struktur pemetaan risiko yang digunakan dalam penelitian ini dapat dimanfaatkan sebagai alat bantu perencanaan untuk menurunkan tujuan migrasi ke dalam daftar risiko operasional dan rencana mitigasi yang konkret. Dalam praktiknya, hal ini membantu organisasi menetapkan prioritas kontrol, menentukan titik kritis yang memerlukan monitoring intensif, serta merancang mekanisme evaluasi berkelanjutan melalui monitoring dan audit.

KESIMPULAN

Penelitian ini menyimpulkan bahwa risiko migrasi hybrid cloud computing bersifat multidimensi, saling terkait, dan tidak dapat dikelola secara parsial. Hasil tinjauan literatur menunjukkan bahwa risiko migrasi muncul dari interaksi antara faktor teknis dan organisasional, sehingga membutuhkan pendekatan terintegrasi dalam perspektif Sistem Informasi. Penelitian ini berhasil mengidentifikasi delapan domain risiko (R1–R8) yang bersifat operasional dan merepresentasikan tantangan utama migrasi hybrid cloud, mulai dari keamanan dan kepatuhan hingga integrasi sistem, biaya, ketersediaan layanan, serta kesiapan organisasi.

Kerangka konseptual yang dikembangkan memetakan domain risiko tersebut ke dalam struktur Threat–Vulnerability–Risk Factors–Impact–Damage, sehingga memperjelas hubungan sebab-akibat antara sumber risiko, kerentanan, dan dampaknya terhadap layanan serta tujuan bisnis. Temuan utama penelitian menegaskan bahwa keberhasilan migrasi hybrid cloud sangat ditentukan oleh kemampuan organisasi menyeimbangkan fleksibilitas, keamanan, dan biaya melalui kontrol teknis yang konsisten serta kesiapan sosio-teknis dan tata kelola teknologi informasi yang memadai. Dengan demikian, penelitian ini memberikan dasar konseptual yang dapat digunakan untuk mendukung identifikasi, penilaian, dan prioritisasi risiko migrasi hybrid cloud secara lebih sistematis. Penelitian selanjutnya disarankan untuk menguji kerangka ini melalui studi kasus empiris dan mengembangkan instrumen pengukuran risiko berbasis domain R1–R8.

REFERENSI

Adabala, S. K. (2024). Cloud migration: Overcoming challenges and ensuring successful transition. Journal of Artificial Intelligence & Cloud Computing, 3(1), 1-6. https://doi.org/10.47363/JAICC/2024(3)E220

Altahat, M. A., Daradkeh, T., & Agarwal, A. (2025). Virtual machine scheduling and migration management across multi-cloud data centers: Blockchain-based versus centralized frameworks. Journal of Cloud Computing: Advances, Systems and Applications, 14(1). https://doi.org/10.1186/s13677-024-00724-7

Althani, B. (2025). Migration challenges of legacy software to the cloud: A socio-technical perspective. Cogent Business & Management, 12(1), 2503421. https://doi.org/10.1080/23311975.2025.2503421

Anh, N. H. (2025). Hybrid cloud migration strategies: Balancing flexibility, security, and cost in a multi-cloud environment. Monteinstitute, 14-26.

Awan. (2025). Strategi keamanan dalam cloud computing: Analisis ancaman dan solusi mitigasi. ST, 2(1), 8-17.

Bellamkonda, S. (2022). Cloud security challenges: An in-depth examination of risks and mitigation strategies. International Journal of Intelligent Systems and Applications in Engineering, 10(3), 477-485.

Ghebreselassie, M. Y., Hammen, H., & Hustad, E. (2025). Challenges and considerations in migration to cloud solutions: A systematic literature review. Procedia Computer Science, 256, 214-221. https://doi.org/10.1016/j.procs.2025.02.114

Junior, M. A., Appiahene, P., Asante, O. A., & Khatib, E. J. (2025). Cloud data privacy protection with homomorphic algorithm: A systematic literature review. Journal of Cloud Computing: Advances, Systems and Applications, 14, Article 84. https://doi.org/10.1186/s13677-025-00774-5

Kommisetty, P. D. N. K., & Abhireddy, N. (2024). Cloud migration strategies: Ensuring seamless integration and scalability in dynamic business environments. International Journal of Engineering and Computer Science, 13(4), 26146-26156. https://doi.org/10.18535/ijecs/v13i04.4812

Kommareddy, R. R. (2025). Migration strategies for large-scale legacy applications to AWS cloud ecosystems. World Journal of Advanced Engineering Technology and Sciences, 15(3), 1673–1681. https://doi.org/10.30574/wjaets.2025.15.3.0992

Lilhore, U. K., Simaiya, S., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Alhazmi, A., & Khan, M. M. (2025). SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust architecture. Journal of Cloud Computing: Advances, Systems and Applications, 14, Article 35. https://doi.org/10.1186/s13677-025-00764-7

Maniah, Soewito, B., Gaol, F. L., & Abdurachman, E. (2022). A systematic literature review: Risk analysis in cloud migration. Journal of King Saud University - Computer and Information Sciences, 34, 3111-3120. https://doi.org/10.1016/j.jksuci.2021.01.008

Merlo, T. R., Fard, F., & Hawamdeh, S. (2025). Cloud computing's impact on the digital transformation of the enterprise: A mixed-methods approach. Sustainability, 17, 5755. https://doi.org/10.3390/su17135755

Modisane, P., & Jokonya, O. (2021). Evaluating the benefits of cloud computing in small, medium and micro-sized enterprises (SMMEs). Procedia Computer Science, 181, 784–792. https://doi.org/10.1016/j.procs.2021.01.231

Mulyana, R., Rusu, L., & Perjons, E. (2024). Key ambidextrous IT governance mechanisms for successful digital transformation: A case study of Bank Rakyat Indonesia (BRI). Digital Business, 4, 100083. https://doi.org/10.1016/j.digbus.2024.100083

Nahla, F., Zulaikha, S. R., & Asnawi. (2025). Pemanfaatan cloud computing untuk meningkatkan efisiensi dan skalabilitas sistem informasi perpustakaan digital. Indonesian Journal of Library and Information Science, 6(1), 51-57. https://doi.org/10.22373/ijlis.v6i1.4955

Putra, F. P. E., Saputri, N. D., Rosi, F., & Loati, R. (2025). Optimalisasi infrastruktur cloud networking melalui integrasi SDN, NFV, dan multi-cloud. Jurnal Informatika dan Teknologi Komputer, 5(1), 118-125. https://doi.org/10.55606/jitek.v5i1.6099

Rashid, M. M., & Yaseen, O. M. (2025). AI-driven cybersecurity measures for hybrid cloud environments: A framework for multi-cloud security management. International Journal on Engineering Artificial Intelligence Management, Decision Support, and Policies, 2(1), 30-39.

Sharma, R. K. (2023). Overcoming cloud migration challenges: Security, compliance, and cost. International Journal of Computer Technology and Electronics Communication, 6(6). https://doi.org/10.15680/IJCTECE.2023.0606001

Sudianto, & Sutopo. (2025). Optimalisasi implementasi sistem informasi manajemen berbasis cloud untuk meningkatkan efisiensi operasional di sektor industri: Studi literatur. Jurnal Rekayasa Sistem Informasi dan Teknologi, 2(4), 1206-1219.

Tanjung, A. M., Lase, W. A., Zega, O., & Lafau, R. O. (2025). Keamanan siber dalam sistem informasi berbasis cloud: Tantangan dan solusi. IDENTIK: Jurnal Ilmu Ekonomi, Pendidikan dan Teknik, 2(1), 127-133.

Waseem, M., Ahmad, A., Liang, P., Akbar, M. A., Khan, A. A., Ahmad, I., Setälä, M., & Mikkonen, T. (2025). Containerization in multi-cloud environment: Roles, strategies, challenges, and solutions for effective implementation. Journal of Systems and Software, 230, 112558. https://doi.org/10.1016/j.jss.2025.112558

Zhang, X., Cui, L., Shen, W., Zeng, J., Du, L., He, H., & Cheng, L. (2023). File processing security detection in multi-cloud environments: A process mining approach. Journal of Cloud Computing: Advances, Systems and Applications, 12(100). https://doi.org/10.1186/s13677-023-00474-y