

# ANALISIS RISIKO IMPLEMENTASI SISTEM INFORMASI AKADEMIK BERBASIS CLOUD MENGGUNAKAN ISO 31000:2018 (STUDI KASUS: UNIBI BANDUNG)

Roofi Dwi Rahmawati<sup>1\*</sup>, Roni Surya<sup>2</sup>, Yudhiawan Dwi Nugraha<sup>3</sup>

Program Studi Informatika<sup>1,2,3</sup>

Universitas Informatika dan Bisnis Indonesia

Jl. Soekarno-Hatta No.643, Sukapura, Kec. Kiaracondong, Kota Bandung, Jawa Barat 40285

roofitkj@gmail.com<sup>1</sup>, ronisurya23@student.unibi.ac.id<sup>2</sup>, dwiyudhiawan@gmail.com<sup>3</sup>

## Abstrak

Sistem Informasi Akademik (SIKAD) merupakan tulang punggung layanan akademik perguruan tinggi, sehingga keandalannya menjadi krusial. Universitas Informatika dan Bisnis Indonesia (UNIBI) saat ini mengoperasikan SIKAD pada infrastruktur Virtual Private Server dan mulai mempertimbangkan migrasi ke lingkungan cloud computing. Namun, wacana tersebut belum disertai dasar analisis risiko yang terstruktur, sementara penelitian terdahulu umumnya berfokus pada infrastruktur on-premise dan belum mengkaji konteks perencanaan migrasi cloud. Penelitian ini bertujuan mengidentifikasi, menganalisis, dan mengevaluasi kelayakan rencana migrasi SIKAD UNIBI ke cloud dari sudut pandang manajemen risiko menggunakan kerangka kerja ISO 31000:2018. Pendekatan yang digunakan adalah kuantitatif deskriptif berbasis kuesioner terhadap empat staf pengelola infrastruktur, dengan penilaian likelihood dan consequence pada skala 1-5 yang menghasilkan Risk Score. Hasil penelitian mengidentifikasi empat belas risiko pada empat klaster, dengan dua risiko berkategori Extreme (benturan regulasi privasi data dan pembengkakan biaya operasional), tujuh risiko High yang didominasi aspek keamanan dan sumber daya manusia, serta lima risiko Medium, tanpa risiko berkategori Low. Temuan juga menunjukkan kesenjangan antara skor kuantitatif dan persepsi praktisi, di mana human error dipandang sebagai risiko paling kritis meski tidak menempati skor tertinggi. Penelitian menyimpulkan bahwa migrasi layak dipertimbangkan namun belum layak dieksekusi tanpa pemenuhan prasyarat mitigasi, terutama kepatuhan regulasi, perhitungan biaya menyeluruh, penguatan kompetensi sumber daya

manusia, dan uji coba migrasi bertahap. Penggunaan empat responden secara eksplisit disebutkan di sini untuk mempertegas gambaran mengenai ruang lingkup penelitian.

Kata kunci:

manajemen Risiko, ISO 31000, cloud computing, sistem informasi akademik, migrasi cloud

## Abstract

*The Academic Information System (SIKAD) is the backbone of higher education academic services, making its reliability crucial. Universitas Informatika dan Bisnis Indonesia (UNIBI) currently operates SIKAD on a Virtual Private Server infrastructure and is beginning to consider a migration to a cloud computing environment. However, this discourse has not been accompanied by a structured risk analysis foundation, while previous studies generally focused on on-premise infrastructure and have not examined the context of cloud migration planning. This study aims to identify, analyze, and evaluate the feasibility of UNIBI's SIKAD cloud migration plan from a risk management perspective using the ISO 31000:2018 framework. The approach used is descriptive quantitative based on a questionnaire administered to four infrastructure management staff, assessing likelihood and consequence on a scale of 1-5 to produce a Risk Score. The results identified fourteen risks across four clusters, with two risks categorized as Extreme (data privacy regulatory conflicts and operational cost overruns), seven High risks dominated by security and human resources aspects, and five Medium risks, with no risks categorized as*

*Low. The findings also indicate a gap between quantitative scores and practitioner perceptions, where human error is viewed as the most critical risk despite not having the highest score. The study concludes that the migration is worth considering but is not yet feasible for execution without fulfilling mitigation prerequisites, particularly regulatory compliance, comprehensive cost calculations, strengthening human resource competencies, and phased migration trials. The use of four respondents is explicitly stated here to provide a clear picture of the research scope.*

**Keywords :**

*risk management, ISO 31000, cloud computing, academic information system, cloud migration*

## **I. PENDAHULUAN**

Sistem Informasi Akademik (SIKAD) merupakan infrastruktur teknologi informasi yang berperan sebagai tulang punggung pengelolaan data dan layanan akademik di perguruan tinggi, mencakup pengelolaan data mahasiswa dan dosen, proses administrasi akademik seperti Kartu Rencana Studi (KRS), Kartu Hasil Studi (KHS), input nilai, presensi perkuliahan, hingga penerbitan dokumen akademik seperti kartu ujian dan surat keterangan (R. Fahlepi et al, 2023). Keberadaan SIKAD yang andal menjadi krusial karena seluruh civitas akademika bergantung pada sistem ini untuk menjalankan proses bisnis akademik secara berkelanjutan.

Universitas Informatika dan Bisnis Indonesia (UNIBI) saat ini mengoperasikan SIKAD menggunakan infrastruktur Virtual Private Server (VPS) yang dikelola secara on-premise. Seiring meningkatnya beban penggunaan, mulai muncul indikasi bahwa kapasitas infrastruktur saat ini perlu dievaluasi. Salah satu gejala yang teramati adalah keterbatasan kapasitas pada operasi unggah berkas (upload) secara konkuren yang berdampak pada performa sistem bagi pengguna aktif, khususnya pada periode Ujian Tengah Semester (UTS) dan Ujian Akhir Semester (UAS). Gejala semacam ini, beserta ketergantungan layanan pada keandalan penyedia VPS, menjadi penanda bahwa keberlanjutan layanan akademik UNIBI memerlukan peninjauan terhadap arah pengembangan infrastruktur ke depan. Perlu ditegaskan bahwa kendala teknis seperti ini tidak

serta-merta mengharuskan migrasi, karena pada dasarnya dapat pula ditangani melalui optimasi sistem maupun peningkatan kapasitas pada infrastruktur yang ada. Dengan kata lain, gejala tersebut bukan alasan tunggal untuk bermigrasi, melainkan pendorong bagi institusi untuk mengevaluasi pilihan-pilihan strategis yang tersedia.

Salah satu opsi strategis yang mulai dipertimbangkan UNIBI adalah migrasi SIKAD ke ekosistem cloud computing, mengingat cloud menawarkan model penyediaan sumber daya komputasi sesuai permintaan (on-demand) (P. Mell & T. Grance, 2011) serta kemampuan elastisitas yang memungkinkan penyesuaian sumber daya secara dinamis (M. Armbrust et al, 2010). Akan tetapi, keputusan migrasi tidak dapat semata-mata didasarkan pada pertimbangan skalabilitas teknis. Migrasi ke cloud merupakan transformasi arsitektur teknologi informasi secara menyeluruh yang memunculkan profil risiko baru pada berbagai dimensi bukan hanya performa, melainkan juga keamanan, kepatuhan regulasi, kesiapan sumber daya manusia, hingga kelayakan finansial jangka panjang. Risiko-risiko tersebut di antaranya mencakup ancaman keamanan pada lingkungan multi-tenant yang melekat pada layanan cloud (Y. I. Syuhardi & E. T. Asmoro, 2024), kesalahan konfigurasi (human error) dalam pengelolaan layanan, potensi pembengkakan biaya operasional dengan skema pembayaran berbasis penggunaan (pay-as-you-go), serta kepatuhan terhadap regulasi perlindungan data pribadi yang semakin ketat di Indonesia (Republik Indonesia, 2025).

Dengan demikian, pertanyaan yang lebih mendasar bagi UNIBI bukanlah sekadar "bagaimana mengatasi kendala performa saat ini", melainkan "apakah migrasi ke cloud merupakan keputusan yang layak dan tepat untuk dijalankan" dengan mempertimbangkan seluruh aspek risiko secara menyeluruh. Pertanyaan ini menjadi semakin relevan karena migrasi cloud telah menjadi wacana yang berkembang di lingkungan institusi, namun belum disertai dasar analisis risiko yang terstruktur sebagai landasan pengambilan keputusan.

Penelitian terdahulu mengenai manajemen risiko teknologi informasi pada sistem informasi akademik menggunakan ISO 31000 telah banyak dilakukan, di antaranya pada SIKAD Sekolah Tinggi Teknologi

Pekanbaru (P. Mell & T. Grance, 2011), Sistem Informasi Akademik UIN Sunan Kalijaga (M. N. Putra, 2019), SIAK Universitas Muhammadiyah Sukabumi (A. N. Rahmatika et al, 2024), serta Tracer Study Universitas Sebelas April (A. A. Herlambang et al, 2024). Penelitian-penelitian tersebut secara konsisten menunjukkan bahwa pendekatan ISO 31000 efektif dalam mengidentifikasi dan memetakan risiko teknologi informasi pada lingkungan akademik. Namun demikian, penelitian-penelitian tersebut umumnya berfokus pada infrastruktur on-premise atau sistem yang sudah berjalan. Di sisi lain, kajian mengenai risiko migrasi cloud computing memang telah mulai berkembang, baik dalam bentuk kerangka konseptual risiko migrasi (C. Trinata et al, 2026) maupun analisis migrasi infrastruktur dari on-premise ke cloud pada lingkungan perguruan tinggi (Y. Fitriani, 2026). Akan tetapi, kajian-kajian tersebut belum secara spesifik mengintegrasikan analisis risiko migrasi cloud ke dalam konteks perencanaan sistem informasi akademik dengan kerangka kerja ISO 31000. Celah inilah yang coba diisi oleh penelitian ini.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengidentifikasi, menganalisis, serta mengevaluasi kelayakan rencana migrasi Sistem Informasi Akademik UNIBI ke lingkungan cloud computing dari sudut pandang manajemen risiko, dengan menggunakan kerangka kerja ISO 31000:2018 (ISO, 2018) sebagai acuan sistematis. Pendekatan penilaian risiko mengadopsi metode likelihood dan consequence sebagaimana diterapkan dalam penelitian analisis risiko proyek pengembangan perangkat lunak (A. M. Nuris et al, 2021), guna menghasilkan gambaran komprehensif mengenai layak atau tidaknya migrasi tersebut dijalankan, beserta rekomendasi perlakuan risiko yang dapat menjadi acuan bagi institusi sebelum keputusan dieksekusi secara penuh.

Kontribusi penelitian ini dibandingkan penelitian sebelumnya semakin dipertegas, khususnya mengenai penerapan standar tersebut secara spesifik pada tahap perencanaan migrasi cloud. Penggunaan kerangka kerja ISO 31000:2018 dalam riset ini sangat relevan karena menyediakan pendekatan yang sistematis mulai dari tahap penetapan konteks hingga perlakuan risiko.

## II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif deskriptif berbasis data survei dengan mengikuti kerangka kerja manajemen risiko ISO 31000:2018 (ISO, 2018). Pendekatan ini dipilih karena mampu menggambarkan profil risiko perencanaan migrasi Sistem Informasi Akademik (SIKAD) ke lingkungan cloud computing berdasarkan konteks nyata di institusi, sekaligus menghasilkan ukuran kuantitatif berupa Risk Score yang dapat digunakan untuk memprioritaskan penanganan risiko (A. M. Nuris et al, 2021). Data kualitatif berupa tanggapan terbuka responden digunakan sebagai pelengkap untuk memperkaya interpretasi pada tahap perlakuan risiko.

Penelitian ini dilakukan pada SIAKAD Universitas Informatika dan Bisnis Indonesia (UNIBI), yang saat ini dioperasikan menggunakan infrastruktur Virtual Private Server (VPS) dengan spesifikasi prosesor 8 core, memori 8 GB, dan ruang penyimpanan 1 TB. Lingkup penelitian difokuskan pada tahap perencanaan migrasi, mengingat SIAKAD UNIBI belum diimplementasikan pada lingkungan cloud computing. Dengan demikian, penilaian risiko dalam penelitian ini bersifat antisipatif terhadap kondisi yang berpotensi muncul apabila migrasi dilaksanakan.

Responden penelitian berjumlah empat orang, terdiri dari staf Teknologi Informasi dan staf Sistem Informasi yang terlibat langsung dalam pengelolaan infrastruktur server SIAKAD UNIBI. Pemilihan responden dilakukan secara purposive berdasarkan keterlibatan teknis langsung dan pemahaman terhadap manajemen server serta konsep cloud computing, dengan pengalaman kerja yang bervariasi antara satu hingga lebih dari lima tahun. Jumlah responden yang terbatas merupakan konsekuensi dari lingkup penelitian yang spesifik pada pengelola infrastruktur SIAKAD UNIBI, dan keterbatasan ini dibahas lebih lanjut sebagai bagian dari limitasi penelitian. Mengingat jumlah responden hanya empat orang, hal ini diperkuat dengan alasan yang kuat mengenai pemilihan responden dan dampaknya terhadap keterwakilan hasil penelitian. Penguatan argumen juga dibutuhkan untuk menegaskan bahwa dengan 4 responden saja sudah dianggap cukup memadai untuk menggali temuan pada lingkup teknis yang spesifik ini.

Pengumpulan data semula direncanakan melalui wawancara langsung kepada pengelola infrastruktur SIAKAD. Namun, dengan mempertimbangkan keterbatasan waktu dan ketersediaan responden, teknik pengumpulan data disesuaikan menjadi kuesioner terstruktur yang didistribusikan secara daring. Kuesioner disusun mengikuti tahapan proses manajemen risiko ISO 31000:2018, terdiri atas empat bagian utama, yaitu (1) profil responden, (2) konteks infrastruktur SIAKAD saat ini, (3) penilaian likelihood dan consequence terhadap empat belas risiko yang teridentifikasi, serta (4) tanggapan terbuka mengenai prioritas dan rekomendasi perlakuan risiko berdasarkan perspektif responden. Penilaian risiko pada instrumen ini sepenuhnya bersumber dari persepsi responden tanpa adanya tahap verifikasi.

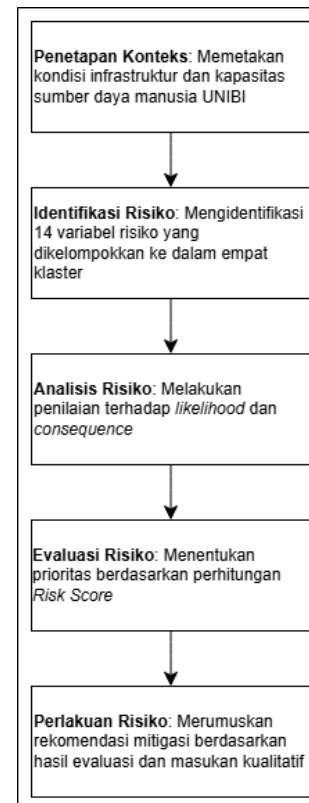
Identifikasi risiko dilakukan melalui kombinasi studi literatur terhadap penelitian terdahulu mengenai risiko keamanan dan migrasi cloud computing (Republik Indonesia, 2025), (C. Trinata et al, 2026), (Y. Fitriani, 2026) serta observasi awal terhadap kondisi infrastruktur SIAKAD UNIBI. Proses ini menghasilkan empat belas risiko yang dikelompokkan ke dalam empat klaster, yaitu risiko infrastruktur (ketergantungan internet, gangguan layanan vendor, keterbatasan bandwidth, kehilangan data), risiko keamanan (kebocoran data, akses tidak sah, serangan siber, benturan regulasi privasi data), risiko sumber daya manusia (kompetensi staf, human error, resistensi pengguna), serta risiko organisasi dan kepatuhan (vendor lock-in, biaya operasional, SLA vendor).

Setiap risiko dinilai oleh responden berdasarkan dua parameter, yaitu likelihood (kemungkinan terjadinya risiko) dan consequence (dampak yang ditimbulkan), masing-masing menggunakan skala 1 hingga 5 (A. M. Nuris et al, 2021). Nilai dari seluruh responden kemudian dirata-ratakan (mean) untuk memperoleh nilai likelihood dan consequence agregat pada masing-masing risiko. Pemilihan nilai rata-rata sebagai metode agregasi didasarkan pada kesesuaiannya dengan penelitian sejenis. Serta kemudahan interpretasi sebagai langkah verifikasi, kecenderungan hasil juga diperiksa dengan nilai median dan menunjukkan pola yang konsisten.

Selanjutnya, nilai Risk Score dihitung menggunakan persamaan berikut (A. M. Nuris et al, 2021):

$$\text{Risk Score (R)} = \text{Likelihood (L)} \times \text{Consequence (C)} \dots (1)$$

Nilai Risk Score agregat yang diperoleh kemudian dipetakan ke dalam matriks risiko 5×5 dan dikategorikan ke dalam empat tingkat prioritas, yaitu Low (skor 1-5), Medium (skor 6-10), High (skor 11-15), dan Extreme (skor 16-25) (A. M. Nuris et al, 2021). Kategorisasi ini menjadi dasar penentuan prioritas perlakuan risiko pada tahap evaluasi.



**Gambar 1. Tahapan Penelitian**

Proses penelitian mengikuti alur manajemen risiko ISO 31000:2018, yang dimulai dari penetapan konteks (memetakan kondisi infrastruktur dan kapasitas sumber daya manusia UNIBI), identifikasi risiko, analisis risiko (penilaian likelihood dan consequence), evaluasi risiko (penentuan prioritas berdasarkan Risk Score), hingga perumusan perlakuan risiko berupa rekomendasi mitigasi yang didasarkan pada hasil kuesioner dan studi literatur pendukung.

### III. ANALISIS DAN PERANCANGAN

Judul bab selanjutnya dapat disesuaikan dengan konten artikel, misalnya dapat berupa analisis dan perancangan, atau hasil analisis data, atau pengolahan data, dan seterusnya.

#### III.1 Penerapan Konteks Infrastruktur dan Sumber Daya Manusia

Berdasarkan hasil kuesioner terhadap empat responden, diketahui bahwa SIAKAD UNIBI saat ini beroperasi pada infrastruktur Virtual Private Server (VPS) dengan kapasitas prosesor 8 core, memori 8 GB, dan ruang penyimpanan 1 TB, yang telah disewa sejak tahun 2021. Seluruh responden secara konsisten menyatakan bahwa prosedur pencadangan data (backup) telah berjalan secara rutin. Riwayat gangguan operasional yang pernah dialami bersumber dari gangguan kelistrikan di sisi penyedia layanan VPS, bukan dari kegagalan internal sistem SIAKAD itu sendiri.

Dari sisi kapabilitas sumber daya manusia, mayoritas responden (3 dari 4) menyatakan memiliki pemahaman "cukup paham" terhadap konsep cloud computing, sementara satu responden menyatakan "sangat paham". Pengalaman responden dalam mengelola infrastruktur IT bervariasi antara 1 hingga lebih dari 5 tahun, mengindikasikan adanya kombinasi staf senior dan staf yang relatif baru dalam tim pengelola infrastruktur. Seluruh responden juga menyatakan bahwa rencana migrasi SIAKAD ke cloud "pernah dibahas tapi belum diputuskan", yang menegaskan posisi penelitian ini sebagai kajian pada tahap perencanaan, bukan implementasi yang sudah berjalan.

#### III.2 Identifikasi dan Analisis Risiko

Berdasarkan hasil identifikasi pada tahap penetapan konteks, penelitian ini mengidentifikasi empat belas variabel risiko yang dikelompokkan ke dalam empat klaster: infrastruktur, keamanan, sumber daya manusia, serta organisasi dan kepatuhan. Setiap risiko dinilai oleh responden berdasarkan parameter likelihood dan consequence dengan skala 1–5, kemudian dihitung Risk Score menggunakan Persamaan (1). Hasil perhitungan disajikan pada

#### Kategori *Extreme*:

1. Risiko tertinggi adalah benturan regulasi privasi data (server luar negeri) dari klaster keamanan. Risiko ini memiliki rata – rata likelihood 4.00 dan consequence 4.25, dan menghasilkan risk score tertinggi sekitar 17.00.
2. Selanjutnya adalah biaya operasional cloud yang tidak terduga dari klaster organisasi, dengan rata – rata likelihood 3.75, consequence 4.50, dan total skor 16.88.

#### Kategori *High*:

1. Resistensi pengguna terhadap perubahan sistem dari klaster SDM dengan risk score skor 13.00, rata-rata Likelihood nya 3.25 dan Consequence 4.00
2. Terdapat empat risiko yang sama-sama memiliki skor 12.00 (rata-rata Likelihood 3.00 dan Consequence 4.00). Tiga di antaranya berada di klaster Keamanan, yaitu serangan siber (ransomware, DDoS, dll), kebocoran data mahasiswa akibat celah keamanan, dan akses tidak sah atau pembobolan akun. Satu risiko lainnya di skor ini adalah kurangnya kompetensi staf IT dalam mengelola cloud yang masuk dalam klaster SDM
3. Dua risiko terakhir di kategori ini masing-masing memiliki skor 11.69 (rata-rata Likelihood 2.75 dan Consequence 4.25), yakni risiko human error dalam konfigurasi sistem cloud (klaster SDM) dan ancaman vendor lock-in (klaster Organisasi)

#### Kategori *Medium*:

1. Risiko kehilangan data akibat kegagalan sistem cloud pada klaster Infrastruktur memiliki risk skor 8.44, yang berasal dari rata-rata Likelihood 2.25 dan Consequence 3.75
2. Tiga risiko selanjutnya memiliki skor yang seragam, yaitu 7.50 (rata-rata Likelihood 2.00 dan Consequence 3.75). Risiko tersebut

meliputi ketergantungan pada koneksi internet dan gangguan layanan dari penyedia cloud (keduanya dari klaster Infrastruktur), serta SLA vendor cloud yang tidak memadai pada klaster Organisasi

3. Risiko dengan skor paling rendah dalam daftar ini adalah keterbatasan bandwidth jaringan kampus dari klaster Infrastruktur. Risiko ini memiliki skor 7.00, dengan rata-rata Likelihood 2.00 dan Consequence 3.50

Berdasarkan hasil analisis diatas, tidak satu pun dari empat belas risiko yang teridentifikasi berada pada kategori Low. Dua risiko berada pada kategori Extreme, tujuh risiko pada kategori High, dan lima risiko pada kategori Medium. Temuan ini mengindikasikan bahwa migrasi SIAKAD ke cloud, dari perspektif staf IT UNIBI, merupakan keputusan dengan tingkat risiko yang signifikan pada hampir seluruh dimensi, bukan hanya pada aspek teknis semata.

### **III.3 Evaluasi Risiko: Gap Antara Persepsi Kualitatif dan Kuantitatif**

Temuan menarik muncul ketika hasil Risk Score dibandingkan dengan jawaban kualitatif responden pada pertanyaan terbuka mengenai risiko paling kritis. Secara kuantitatif, risiko benturan regulasi privasi data dan pembengkakan biaya operasional menempati dua peringkat teratas dengan kategori Extreme. Namun demikian, tiga dari empat responden secara eksplisit menyebutkan human error dalam konfigurasi sistem cloud sebagai risiko yang paling kritis untuk ditangani, meskipun secara skor numerik risiko ini berada pada peringkat kedelapan dengan kategori High.

Alasan yang dikemukakan responden cukup konsisten: kesalahan konfigurasi dipandang sebagai risiko akar (root risk) yang berpotensi memicu munculnya risiko-risiko lain, seperti kebocoran data atau gangguan layanan. Pandangan ini sejalan dengan temuan (R. Fahlepi et al, 2023) yang juga mengidentifikasi human error sebagai salah satu risiko dengan prioritas tertinggi pada SIAKAD berbasis on-premise. Gap antara hasil kuantitatif dan persepsi kualitatif ini menunjukkan pentingnya mengkombinasikan kedua pendekatan analisis, sebagaimana direkomendasikan oleh (A. M. Nuris et al, 2021), karena risiko yang secara matematis tidak

menempati peringkat tertinggi belum tentu kurang penting untuk diwaspadai dari sudut pandang praktisi di lapangan.

Pada klaster keamanan, tingginya Risk Score untuk risiko benturan regulasi privasi data sejalan dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Republik Indonesia, 2025), yang mewajibkan pengendali data memastikan data pribadi warga negara Indonesia dikelola sesuai prinsip perlindungan yang berlaku, termasuk pertimbangan lokasi penyimpanan data. Temuan ini juga konsisten dengan tantangan keamanan cloud computing yang diidentifikasi oleh Syuhardi dan Asmoro (Y. I. Syuhardi & E. T. Asmoro, 2024), khususnya terkait kepatuhan terhadap regulasi sebagai salah satu tantangan utama dalam adopsi cloud.

### **III.4 Perlakuan Risiko**

Berdasarkan hasil evaluasi risiko dan masukan kualitatif dari responden, dirumuskan strategi perlakuan risiko yang dikelompokkan berdasarkan kategori prioritas. Untuk risiko berkategori Extreme dan High, strategi yang direkomendasikan bersifat immediate action, yaitu penanganan yang harus segera dipersiapkan sebelum keputusan migrasi dieksekusi.

Pada aspek regulasi privasi data, UNIBI direkomendasikan untuk menyeleksi penyedia layanan cloud yang mengoperasikan pusat data di dalam wilayah yurisdiksi Indonesia, guna memastikan kepatuhan terhadap UU PDP (Republik Indonesia, 2025). Pada aspek biaya operasional, diperlukan kalkulasi Total Cost of Ownership (TCO) secara cermat sebelum migrasi, mengingat skema pembayaran cloud yang umumnya bersifat pay-as-you-go berpotensi menimbulkan biaya tidak terduga apabila tidak direncanakan dengan matang.

Untuk menangani risiko human error yang menjadi perhatian utama responden secara kualitatif, pelaksanaan uji coba migrasi pada lingkungan staging sebelum migrasi penuh menjadi langkah mitigasi yang krusial, sebagaimana disarankan oleh salah satu responden. Langkah ini memungkinkan staf IT membiasakan diri dengan kontrol dan konfigurasi sistem cloud tanpa risiko terhadap data produksi. Selain itu, responden juga menekankan pentingnya dukungan teknis yang responsif dari penyedia cloud,

idealnya dengan akses ke operator manusia, bukan hanya sistem otomatis, untuk mempercepat penanganan apabila insiden terjadi.

Risiko organisasional lain yang perlu diantisipasi adalah ketergantungan pada satu penyedia (vendor lock-in), yang juga berada pada kategori High. Untuk memitigasi risiko ini, UNIBI dapat mempertimbangkan penggunaan arsitektur yang portabel serta menghindari ketergantungan penuh pada layanan proprietary satu vendor, sebagaimana ditekankan dalam kajian risiko migrasi cloud yang memandang lock-in tidak hanya sebagai persoalan teknis, melainkan juga sebagai pembatas fleksibilitas strategis organisasi dalam jangka panjang (C. Trinata et al, 2026).

Secara ringkas, langkah-langkah persiapan yang direkomendasikan sebelum migrasi mencakup: (1) asesmen menyeluruh terhadap kesiapan sistem dan keamanan data, (2) penyusunan rencana pencadangan dan disaster recovery, (3) pelaksanaan uji coba migrasi pada lingkungan staging, (4) penguatan kompetensi SDM terkait konfigurasi dan pengelolaan cloud, serta (5) pemilihan penyedia cloud yang memenuhi kriteria kepatuhan regulasi, transparansi biaya, dan dukungan teknis yang responsif.

#### **IV. KESIMPULAN**

Penelitian ini mengidentifikasi, menganalisis, dan mengevaluasi risiko perencanaan migrasi Sistem Informasi Akademik (SIKAD) UNIBI ke lingkungan cloud computing menggunakan kerangka kerja ISO 31000:2018. Dari empat belas risiko yang teridentifikasi pada empat klaster (infrastruktur, keamanan, sumber daya manusia, serta organisasi dan kepatuhan), hasil penilaian menunjukkan dua risiko berkategori Extreme, yaitu benturan regulasi privasi data dan pembengkakan biaya operasional, tujuh risiko berkategori High yang didominasi aspek keamanan dan sumber daya manusia, serta lima risiko berkategori Medium yang umumnya bersifat teknis-infrastruktur. Tidak ditemukan risiko berkategori Low.

Profil risiko tersebut menunjukkan bahwa tantangan utama migrasi SIKAD UNIBI ke cloud justru tidak terletak pada aspek teknis-infrastruktur yang menjadi pemicu awal wacana, melainkan pada dimensi keamanan, kepatuhan regulasi, kesiapan

sumber daya manusia, dan kelayakan finansial. Selain itu, ditemukan adanya kesenjangan antara hasil penilaian kuantitatif dan persepsi kualitatif responden: meskipun secara skor human error berada pada peringkat kedelapan, mayoritas responden memandangnya sebagai risiko paling kritis karena berpotensi menjadi pemicu risiko-risiko lainnya. Temuan ini menegaskan bahwa penilaian risiko berbasis skor numerik perlu dilengkapi dengan perspektif praktisi di lapangan.

Berdasarkan keseluruhan temuan, dapat disimpulkan bahwa rencana migrasi SIKAD UNIBI ke cloud layak untuk dipertimbangkan sebagai arah pengembangan, namun belum layak untuk dieksekusi pada kondisi saat ini. Kelayakan eksekusi bergantung pada terpenuhinya sejumlah prasyarat mitigasi, terutama pemilihan penyedia cloud yang patuh terhadap UU Pelindungan Data Pribadi, perhitungan Total Cost of Ownership yang cermat, penguatan kompetensi sumber daya manusia, serta pelaksanaan uji coba migrasi pada lingkungan staging sebelum migrasi penuh. Dengan demikian, penelitian ini memposisikan analisis risiko sebagai dasar pengambilan keputusan yang terstruktur bagi institusi sebelum keputusan migrasi dieksekusi secara penuh.

Penelitian ini memiliki sejumlah keterbatasan yang perlu diperhatikan dalam menafsirkan hasilnya. Pertama, jumlah responden terbatas pada empat orang pengelola infrastruktur SIKAD UNIBI. Meskipun pemilihan responden bersifat purposive dan mencakup pihak yang memiliki keterlibatan teknis langsung, jumlah ini membatasi keterwakilan persepsi dan menjadikan hasil penilaian tidak dapat digeneralisasi ke institusi lain. Kedua, penilaian risiko sepenuhnya bersumber dari persepsi responden tanpa tahap verifikasi balik (member checking) maupun validasi silang dengan data teknis kuantitatif, sehingga terdapat kemungkinan variasi penilaian antar responden, sebagaimana teramati pada sebagian jawaban. Ketiga, penelitian ini berhenti pada tahap perencanaan dan evaluasi risiko, sehingga efektivitas strategi perlakuan risiko yang direkomendasikan belum dapat diuji secara empiris pada lingkungan migrasi yang sesungguhnya. Pembahasan temuan utama pada tahap evaluasi risiko ini akan menjadi lebih kuat dan komprehensif apabila dikaitkan dengan lebih banyak penelitian terdahulu sehingga terlihat persamaan maupun perbedaannya secara mendalam.

Untuk penelitian selanjutnya, disarankan untuk memperluas jumlah dan ragam responden dengan melibatkan pemangku kepentingan non-teknis seperti pimpinan institusi dan pengguna akhir, menambahkan tahap validasi hasil melalui wawancara mendalam atau diskusi terfokus, serta melakukan kajian lanjutan pada tahap implementasi untuk menguji efektivitas strategi mitigasi yang diusulkan secara nyata.

## REFERENSI

- A. A. Herlambang, A. A. Gani, dan D. D. Alvianto, "Pendekatan ISO 31000:2018 dalam Manajemen Risiko Teknologi Informasi pada Tracer Study Universitas Sebelas April," *Jurnal Intelek dan Cendekiawan Nusantara (JICN)*, vol. 1, no. 4, hlm. 5651–5660, 2024.
- A. M. Nuris, A. Maharani, dan R. N. Rachmadita, "Analisis Risiko Proyek Pengembangan Perangkat Lunak Menggunakan Kerangka Kerja ISO 31000," *Jurnal Metris*, vol. 22, no. 2, hlm. 73–81, 2021.
- A. N. Rahmatika, M. F. Apriyadi, M. A. Kahfi, dan O. N. Aibi, "Analisis Manajemen Risiko Teknologi Informasi Pada Sistem Informasi Akademik (SIK) Universitas Muhammadiyah Sukabumi (UMMI) Menggunakan ISO 31000," *Jurnal Manajemen dan Teknologi Informasi (JMTI)*, vol. 14, no. 1, hlm. 48–57, 2024.
- Ahmad, N., & Naveed, Q. N. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. *Journal of Computer Information Systems*, 1–28.
- C. Trinata, V. N. Fathya, B. Hartati, A. Febrianto, dan P. D. K. Wibowo, "Pengembangan Kerangka Konseptual Risiko Migrasi Hybrid Cloud Computing: Tinjauan Literatur Naratif Perspektif Sistem Informasi," *HORIZON: Indonesian Journal of Multidisciplinary*, vol. 4, no. 3, hlm. 461–472, 2026.
- Daulay, D. F., & Sayekti, R. (2025). Strategi menjamin sistem keamanan data perpustakaan digital Universitas Negeri Medan berbasis cloud computing. *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, 7(3), 1464–1472.
- International Organization for Standardization, ISO 31000:2018 Risk Management Guidelines. Geneva, Switzerland: ISO, 2018.
- M. Armbrust et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, hlm. 50–58, 2010.
- M. N. Putra, "Analisis Manajemen Risiko Teknologi Sistem Informasi Akademik Berbasis ISO 31000 (Studi Kasus: UIN Sunan Kalijaga)," Skripsi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta, 2019.
- P. Mell & T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology (NIST), Special Publication 800-145, 2011.
- Pentury, C., & Tambotih, J. J. C. (2022). Information technology risk analysis and mitigation using ISO 31000 and House of Risk (HOR) for SIAK in Western Seram Regency. *Jurnal AKSI (Akuntansi dan Sistem Informasi)*, 7(2).
- R. Fahlepi, M. Fronita, E. Saputra, M. L. Hamzah, A. Marsal, dan S. Daulay, "Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000," *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, vol. 7, no. 2, hlm. 663–674, 2023.
- Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Jakarta: JDIH BPK RI, 2022.
- Y. Fitriani, "Transformasi Infrastruktur IT Perguruan Tinggi: Analisis Strategis dan Teknis Migrasi dari on-Premise ke Cloud Computing," *Jurnal Siber Multi Disiplin (JSMD)*, vol. 3, no. 4, hlm. 280–286, 2026.
- Y. I. Syuhardi & E. T. Asmoro, "Keamanan Cloud Computing: Tantangan dan Solusi," *MISTER: Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research*, vol. 1, no. 4, hlm. 1997–2004, 2024.