JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Analisis dan Perancangan Strategi Manajemen Keamanan Informasi pada Penggunaan Sistem Berbasis *Cloud* di Perusahaan Jasa

Aisyah Praudita[1]*, Robbi Rahim [2]
[1,2] Sekolah Tinggi Ilmu Manajemen Sukma, Indonesia
* E-mail: aira280603@mail.com

Information Article
History Article
Submission: 08-07-2026
Revision: 06-08-2026
Published: 08-08-2026

DOI Article:
10.62421/jibema.v4i1.693

A B S T R A K

Transformasi digital mendorong perusahaan jasa memanfaatkan sistem berbasis *cloud* untuk mendukung operasional bisnis, namun perpindahan pengelolaan data ke lingkungan *cloud* turut meningkatkan kompleksitas risiko keamanan informasi. Penelitian ini bertujuan menganalisis kondisi keamanan informasi berdasarkan prinsip *Confidentiality, Integrity*, dan *Availability* (CIA *Triad*), menganalisis risiko keamanan informasi berdasarkan ISO/IEC 27001:2022 dan NIST *Cybersecurity Framework* (CSF) 2.0, serta merancang strategi manajemen keamanan informasi yang dapat diterapkan pada perusahaan jasa. Penelitian menggunakan metode kualitatif dengan pendekatan *Systematic Literature Review* (SLR) mengikuti tahapan PRISMA pada basis data *ScienceDirect, SpringerLink*, *Scientific Reports,* dan MDPI, sehingga diperoleh lima belas artikel yang memenuhi kriteria inklusi tahun 2022-2026. Hasil analisis menunjukkan bahwa risiko dominan meliputi akses tidak sah, kebocoran data, kesalahan konfigurasi, kerentanan aplikasi, dan lemahnya kesadaran keamanan pengguna. ISO/IEC 27001:2022 dan NIST CSF 2.0 terbukti saling melengkapi: ISO/IEC 27001:2022 memperkuat tata kelola melalui *Information Security Management System* (ISMS), sedangkan NIST CSF 2.0 memperkuat kesiapsiagaan operasional melalui fungsi *Govern, Identify, Protect, Detect, Respond, dan Recover*. Penelitian ini menghasilkan model strategi konseptual terintegrasi yang mencakup enam tahapan, yaitu tata kelola, identifikasi risiko, implementasi kontrol, pemantauan, respons insiden, serta evaluasi berkelanjutan, sebagai rekomendasi bagi perusahaan jasa dalam memperkuat keamanan sistem berbasis *cloud*.

Kata Kunci: Keamanan Informasi, *Cloud Computing,* ISO/IEC 27001:2022, NIST CSF 2.0, Perusahaan Jasa

A B S T R A C T

Digital transformation has encouraged service companies to adopt cloud-based systems to support business operations, yet the shift of data management to the cloud environment increases the complexity of information security risks. This study aims to analyze the condition of information security based on the Confidentiality, Integrity, and Availability (CIA Triad) principles, to analyze information security risks based on ISO/IEC 27001:2022 and the NIST Cybersecurity Framework (CSF) 2.0, and to design an information security management strategy applicable to service companies. The study employs a qualitative method through a Systematic Literature Review (SLR) approach following the PRISMA stages across the

Acknowledgment

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

ScienceDirect, SpringerLink, Scientific Reports, and MDPI databases, resulting in fifteen articles published between 2022 and 2026 that met the inclusion criteria. The results indicate that the dominant risks include unauthorized access, data leakage, misconfiguration, application vulnerabilities, and low user security awareness. ISO/IEC 27001:2022 and NIST CSF 2.0 were found to be complementary: ISO/IEC 27001:2022 strengthens governance through an Information Security Management System (ISMS), while NIST CSF 2.0 strengthens operational readiness through the Govern, Identify, Protect, Detect, Respond, and Recover functions. This study produces an integrated conceptual strategy model consisting of six stages-governance, risk identification, control implementation, monitoring, incident response, and continuous evaluation-as a recommendation for service companies to strengthen the security of their cloud-based systems.

Key word: *Information Security, Cloud Computing, ISO/IEC 27001:2022, NIST CSF 2.0, Service Company*

PENDAHULUAN

Perkembangan teknologi informasi mendorong transformasi digital di berbagai sektor industri, termasuk sektor jasa, salah satunya melalui pemanfaatan *cloud computing* sebagai infrastruktur utama operasional bisnis. Model layanan *cloud*, seperti *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), dan *Software as a Service* (SaaS), memberikan fleksibilitas, efisiensi biaya, dan skalabilitas sehingga menjadi komponen penting dalam strategi transformasi digital organisasi (Bajdor, 2024; Bitkowska et al., 2024). Perusahaan jasa termasuk sektor yang paling aktif mengadopsi teknologi ini karena karakteristik bisnisnya yang sangat bergantung pada kecepatan layanan, mobilitas informasi, dan ketersediaan data secara berkelanjutan, sehingga kemampuan mengakses data secara *real-time* memberikan keunggulan kompetitif dalam pengambilan keputusan bisnis (Kahraman & Rigopoulos, 2024).

Di balik berbagai manfaat tersebut, penerapan sistem berbasis *cloud* turut menghadirkan tantangan keamanan informasi. Perpindahan data organisasi ke lingkungan *cloud* yang dikelola pihak ketiga meningkatkan kompleksitas pengelolaan keamanan, karena organisasi tidak lagi memiliki kendali penuh terhadap infrastruktur yang digunakan. Ancaman seperti kebocoran data, penyalahgunaan hak akses, *malware*, *ransomware*, serangan *Distributed Denial of Service* (DDoS), hingga kesalahan konfigurasi sistem dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi (Morol et al., 2022). Laporan lembaga keamanan siber nasional menunjukkan bahwa ancaman terhadap layanan berbasis *cloud* terus meningkat setiap tahun, dan sebagian besar insiden keamanan tidak hanya disebabkan oleh kelemahan teknologi, tetapi juga oleh lemahnya tata kelola keamanan, minimnya kebijakan, serta rendahnya kesadaran pengguna atau *security awareness* (BSSN, 2023; Khader et al., 2021).

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Kondisi ini menegaskan bahwa keberhasilan implementasi *cloud computing* tidak semata bergantung pada kecanggihan teknologi, tetapi juga pada kemampuan organisasi mengelola risiko keamanan informasi secara sistematis (Oyeniyi et al., 2025).

Manajemen keamanan informasi merupakan upaya melindungi aset informasi organisasi melalui kebijakan, prosedur, dan pengendalian yang mampu meminimalkan risiko keamanan. ISO/IEC 27001:2022 menjadi salah satu kerangka kerja yang banyak diadopsi organisasi dalam membangun *Information Security Management System* (ISMS) dengan pendekatan berbasis risiko (Frangky & Sinaga, 2024; Marhad et al., 2023). Selain itu, NIST *Cybersecurity Framework* (CSF) 2.0 menjadi acuan penting dalam memperkuat ketahanan siber organisasi melalui fungsi *Govern, Identify, Protect, Detect, Respond, dan Recover*. Kombinasi kedua kerangka kerja tersebut memberikan pendekatan yang lebih komprehensif dalam mengelola keamanan informasi pada lingkungan *cloud* (Essien et al., 2022).

Sebagian besar penelitian terdahulu masih berfokus pada dampak *cloud computing* terhadap efisiensi operasional dan transformasi digital (Bajdor, 2024; Bitkowska et al., 2024), atau membahas aspek teknis keamanan *cloud* secara terpisah, seperti enkripsi data dan mekanisme autentikasi (Morol et al., 2022). Kajian yang secara eksplisit mengintegrasikan analisis risiko keamanan informasi dengan perancangan strategi manajemen keamanan berdasarkan ISO/IEC 27001:2022 dan NIST CSF 2.0 pada konteks perusahaan jasa secara umum masih terbatas. Kesenjangan inilah yang mendasari penelitian ini, dengan tujuan: (1) menganalisis kondisi keamanan informasi pada penggunaan sistem berbasis *cloud* di perusahaan jasa berdasarkan aspek kerahasiaan, integritas, dan ketersediaan informasi; (2) menganalisis risiko keamanan informasi berdasarkan ISO/IEC 27001:2022 dan NIST CSF 2.0; dan (3) merancang strategi manajemen keamanan informasi yang dapat dijadikan rekomendasi bagi perusahaan jasa dalam meningkatkan keamanan penggunaan sistem berbasis *cloud*.

METODE PENELITIAN

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) yaitu proses yang terstruktur, transparan, dan dapat diulang untuk mengidentifikasi, menilai, serta menyintesis temuan penelitian yang relevan dengan topik tertentu (Hashim et al., 2022). Pendekatan ini dipilih karena tujuan penelitian adalah memperoleh pemahaman mendalam mengenai strategi manajemen keamanan informasi pada penggunaan sistem berbasis *cloud* melalui kajian terhadap teori, hasil penelitian terdahulu, dan standar internasional yang relevan.

Proses pencarian literatur mengikuti tahapan *Preferred Reporting Items for Systematic Reviews and Meta-Analysis* (PRISMA) melalui empat tahap, yaitu identifikasi, penyaringan *(screening)*, penilaian kelayakan *(eligibility)*, dan penentuan artikel yang digunakan *(included)*. Pencarian dilakukan pada basis data *ScienceDirect, SpringerLink, Scientific Reports*, dan MDPI menggunakan kata kunci

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

cloud security, information security risk management, ISO/IEC 27001, dan NIST *cybersecurity framework*. Kriteria inklusi meliputi artikel terbitan tahun 2022-2026, berbahasa Indonesia atau Inggris, membahas topik keamanan informasi, *cloud computing*, ISMS, ISO 27001, atau NIST CSF, bersifat *open access*, serta memiliki DOI atau identitas publikasi yang jelas.

Tahap identifikasi menghasilkan 100 artikel, kemudian 22 artikel duplikat dieliminasi sehingga tersisa 88 artikel. Proses *screening* berdasarkan kriteria inklusi dan eksklusi mengeliminasi 43 artikel yang tidak relevan, sehingga diperoleh 45 artikel untuk tahap *eligibility*. Pada tahap ini, 7 artikel dieliminasi karena hanya membahas aspek teknis tanpa keterkaitan dengan strategi keamanan informasi, sehingga diperoleh 15 artikel final yang memenuhi seluruh kriteria dan digunakan sebagai sumber utama analisis. Kualitas seluruh artikel dinilai menggunakan lima kriteria *quality assessment*, yaitu kesesuaian tujuan, metode, hasil, kontribusi terhadap strategi keamanan informasi, dan kelayakan sebagai dasar sintesis, dengan skor 1 untuk setiap kriteria yang terpenuhi. Artikel dengan skor total 4-5 dikategorikan layak dianalisis lebih lanjut; seluruh 15 artikel terpilih memenuhi ambang batas tersebut.

Analisis data menggunakan pendekatan deskriptif kualitatif dengan tahapan reduksi data, penyajian data, analisis risiko, *gap analysis*, dan penyusunan strategi (Dahal, 2025; Fadli, 2021). Analisis risiko difokuskan pada identifikasi aset, ancaman, kerentanan, dan konsekuensi, kemudian dikategorikan ke dalam tingkat risiko yang memerlukan penanganan (Nugroho & Legowo, 2022). *Gap analysis* dilakukan untuk mengevaluasi hasil identifikasi risiko terhadap kontrol keamanan pada ISO/IEC 27001:2022 dan NIST CSF 2.0 guna mengidentifikasi area yang belum tercakup atau memerlukan penguatan (Innomesanghan et al., 2025). Selanjutnya, strategi disusun secara *hybrid* dengan memadukan pendekatan berbasis dokumentasi ISO/IEC 27001:2022 dan fleksibilitas fungsional NIST CSF 2.0 (Rambau et al., 2026). Kerangka analisis penelitian mengacu pada siklus *Plan-Do-Check-Act* (PDCA) dalam ISO/IEC 27001:2022, sehingga proses identifikasi risiko, penerapan kontrol, evaluasi, dan perbaikan dapat dilakukan secara berkelanjutan.

HASIL DAN PEMBAHASAN

HASIL

Proses seleksi literatur menghasilkan 15 artikel akhir yang bersumber dari empat basis data, sebagaimana disajikan pada Tabel 1.

Tabel 1. Hasil Seleksi Literatur Review

Database	Jumlah Artikel
MDPI	5
SpringerLink	4
Elsevier	5
Scientific Reports	1
Total	15

Sumber: data diolah (2026)

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Kelima belas artikel tersebut membahas topik yang beragam namun saling berkaitan, mencakup tujuan dan legitimasi keamanan informasi dalam ISO/IEC 27001 (Kamil et al., 2023), terminologi manajemen risiko keamanan informasi (Schmidt, 2023), survei keamanan informasi pada organisasi layanan kesehatan (Hsu & Shih, 2023), mekanisme *privacy preserving* pada *cloud computing* berbasis IoT (Kuldeep & Zhang, 2022), deteksi risiko *real-time* pada jaringan *cloud* (Guo & Guo, 2023), evaluasi keamanan sistem *cloud* ERP berdasarkan NIST dan ISO (Qazi et al., 2026), pengelolaan kunci enkripsi berbasis *blockchain* dan digital *twins* (Huang & Yi, 2024), kerangka kerja keamanan *cloud* multilayer VIRTUOSO (Anwar et al., 2026), serta penguatan CIA *Triad* melalui model keamanan berbasis ISO/IEC 27001:2022 (Vasovic et al., 2026).

Kondisi Keamanan Informasi Berdasarkan CIA *Triad*

Hasil sintesis terhadap 15 artikel menunjukkan bahwa keberhasilan penerapan *cloud computing* sangat dipengaruhi oleh kemampuan organisasi menjaga kerahasiaan *(confidentiality), integritas (integrity),* dan ketersediaan *(availability)* informasi, yang dikenal sebagai CIA *Triad* dan tetap menjadi landasan utama keamanan informasi modern (Vasovic et al., 2026).

Pada aspek kerahasiaan, ancaman yang paling banyak diidentifikasi adalah akses tidak sah, pencurian kredensial, kesalahan konfigurasi layanan *cloud*, lemahnya manajemen identitas dan hak akses, serta pengelolaan kunci enkripsi yang belum optimal. Studi tentang pengelolaan kunci enkripsi berbasis *blockchain* dan digital *twins* menunjukkan bahwa penguatan *encryption key management* mampu menurunkan risiko kebocoran data pada penyimpanan *cloud* (Huang & Yi, 2024), sedangkan pendekatan *privacy-preserving* pada lingkungan IoT menekankan pentingnya mekanisme yang menjaga privasi data pengguna selama proses maupun pertukaran data (Kuldeep & Zhang, 2022). Studi lain menunjukkan bahwa kombinasi ISO/IEC 27001:2022 dan NIST CSF 2.0 memperkuat perlindungan kerahasiaan melalui autentikasi, kontrol akses, dan enkripsi data pada sistem ERP berbasis *cloud* (Qazi et al., 2026).

Pada aspek integritas, risiko yang teridentifikasi meliputi manipulasi data, serangan *malware*, kesalahan konfigurasi sistem, serta lemahnya mekanisme audit. Studi mengenai deteksi risiko *real time* pada jaringan *cloud* menunjukkan bahwa mekanisme deteksi dini mampu meningkatkan akurasi pengenalan serangan sekaligus menurunkan tingkat kesalahan deteksi dibandingkan pendekatan konvensional (Guo & Guo, 2023). Kerangka kerja keamanan *cloud multilayer* yang mengintegrasikan otomatisasi keamanan, analisis *log*, dan deteksi anomali berbasis machine learning turut memperkuat kemampuan organisasi menjaga integritas data melalui pemantauan berkelanjutan (Anwar et al., 2026).

Pada aspek ketersediaan, ancaman yang umum ditemukan berupa gangguan layanan, serangan DDoS, kegagalan infrastruktur, serta mekanisme pemulihan yang belum optimal. Penerapan ISO/IEC

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

27001 pada organisasi layanan kesehatan terbukti mendukung keberlangsungan operasional sistem informasi melalui pengelolaan risiko dan kebijakan keamanan yang terstruktur (Hsu & Shih, 2023), sementara evaluasi keamanan berbasis NIST dan ISO pada sistem ERP *cloud* menunjukkan bahwa peningkatan kesiapan keamanan berkontribusi terhadap ketersediaan layanan yang lebih baik (Qazi et al., 2026).

Secara keseluruhan, hasil sintesis menegaskan bahwa strategi perlindungan informasi pada perusahaan jasa berbasis *cloud* perlu mengintegrasikan penerapan ISMS, *autentikasi multifaktor* (MFA), enkripsi data, pengelolaan identitas dan hak akses (IAM), pemantauan berkelanjutan, serta rencana keberlangsungan bisnis dan pemulihan bencana agar ketiga aspek CIA *Triad* terjaga secara seimbang.

Analisis Risiko Berdasarkan ISO/IEC 27001:2022 dan NIST CSF 2.0

Analisis risiko keamanan informasi dilakukan dengan memetakan hasil sintesis literatur terhadap tujuh klausul utama ISO/IEC 27001:2022 dan enam fungsi NIST CSF 2.0. Hasil pemetaan disajikan secara ringkas pada Tabel 2 dan Tabel 3.

Tabel 2. Ringkasan Analisis Risiko Berdasarkan ISO/IEC 27001:2022

Klausul	Temuan Utama
Context of the Organization	Karakteristik organisasi memengaruhi kebutuhan pengamanan informasi dan ruang lingkup ISMS.
Leadership	Komitmen manajemen puncak menentukan efektivitas penerapan kebijakan keamanan.
Planning	Perencanaan risiko sistematis menjadi dasar mitigasi sesuai karakteristik *cloud*.
Support	Kompetensi SDM dan dokumentasi memadai mendukung keberhasilan pengendalian.
Operation	Kontrol teknis (autentikasi, enkripsi, kontrol akses, manajemen kerentanan) paling dominan.
Performance Evaluation	Evaluasi kematangan keamanan diperlukan untuk mengukur efektivitas kontrol.
Improvement	Tindakan korektif berkelanjutan diperlukan untuk menutup celah keamanan.

Sumber: data diolah (2026)

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Tabel 3. Ringkasan Analisis Risiko Berdasarkan NIST CSF 2.0

Fungsi	Temuan Utama
Govern	Menyelaraskan kebijakan keamanan dengan tujuan organisasi dan ekspektasi pemangku kepentingan.
Identify	Mengenali aset, ancaman, dan kerentanan yang memengaruhi keberlangsungan layanan *cloud*.
Protect	Fungsi paling dominan; mencakup MFA, RBAC, enkripsi, dan manajemen kerentanan.
Detect	Pemantauan berkelanjutan untuk deteksi ancaman secara dini.
Respond	Penanganan insiden secara cepat dan terkoordinasi.
Recover	Pemulihan layanan dan peningkatan ketahanan pasca-insiden.

Sumber: data diolah (2026)

Perbandingan kedua kerangka kerja menunjukkan bahwa ISO/IEC 27001:2022 dan NIST CSF 2.0 memiliki tujuan yang sama, yaitu meningkatkan keamanan informasi melalui pengendalian risiko yang sistematis, tetapi menggunakan pendekatan yang berbeda. ISO/IEC 27001:2022 menitikberatkan pada pembangunan *Information Security Management System* (ISMS) yang berorientasi tata kelola, sedangkan NIST CSF 2.0 berorientasi pada pengelolaan risiko keamanan siber yang lebih operasional dan adaptif (Essien et al., 2022). Ringkasan perbandingan disajikan pada Tabel 4.

Tabel 4. Perbandingan ISO/IEC 27001:2022 dan NIST CSF 2.0

Aspek	ISO/IEC 27001:2022	NIST CSF 2.0
Tujuan	Membangun ISMS yang sistematis dan terdokumentasi	Mengelola risiko keamanan siber secara adaptif
Pendekatan	Berbasis klausul organisasi	Berbasis enam fungsi
Keunggulan	Struktur tata kelola terdokumentasi, mendukung sertifikasi internasional	Fleksibel dan adaptif terhadap ancaman siber
Keterbatasan	Memerlukan dokumentasi dan sumber daya besar	Tidak menyediakan sertifikasi formal

Sumber: data diolah (2026)

Hasil sintesis menunjukkan bahwa risiko keamanan informasi yang paling dominan pada penggunaan sistem berbasis *cloud* di perusahaan jasa meliputi akses tidak sah, kebocoran data, kesalahan konfigurasi *(misconfiguration)*, kerentanan aplikasi dan jaringan, serta rendahnya kesadaran keamanan pengguna. Kontrol keamanan yang paling banyak direkomendasikan meliputi *Multi-Factor Authentication* (MFA), enkripsi data, *Role-Based Access Control* (RBAC), manajemen kerentanan berkala, pemantauan berkelanjutan, audit keamanan, serta *security awareness training* (Morol et al., 2022;

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Nugroho & Legowo, 2022). Ringkasan risiko dominan beserta kontrol yang direkomendasikan disajikan pada Tabel 5.

Tabel 5. Ringkasan Risiko Dominan dan Kontrol Keamanan yang Direkomendasikan

Fungsi	Temuan Utama
Akses tidak sah *(unauthorized access)*	MFA, RBAC, *Identity and Access Management* (IAM)
Kebocoran data *(data leakage)*	Enkripsi data, *Data Loss Prevention* (DLP), klasifikasi data
Kesalahan konfigurasi *(misconfiguration)*	Audit konfigurasi berkala, *secure configuration baseline*
Kerentanan aplikasi dan jaringan	Manajemen kerentanan *(patch management)*, pengujian keamanan berkala
Keterlambatan deteksi insiden	*Continuous monitoring*, SIEM, *Intrusion Detection System* (IDS)
Rendahnya kesadaran keamanan pengguna	*Security awareness training*, kebijakan keamanan informasi

Sumber: data diolah (2026)

PEMBAHASAN

Hasil analisis menunjukkan bahwa pengelolaan keamanan informasi pada sistem berbasis *cloud* di perusahaan jasa tidak dapat hanya mengandalkan pengendalian teknis maupun tata kelola organisasi secara terpisah. Kedua unsur tersebut perlu diintegrasikan agar organisasi mampu menjawab risiko yang bersifat teknis maupun risiko yang bersumber dari tata kelola, proses bisnis, dan kesiapan sumber daya manusia. Temuan ini konsisten dengan pandangan bahwa ISO/IEC 27001:2022 dan NIST CSF 2.0 bersifat komplementer, bukan saling menggantikan (Essien et al., 2022; Rambau et al., 2026): ISO/IEC 27001:2022 memberikan landasan tata kelola melalui ISMS, sedangkan NIST CSF 2.0 memperkuat kemampuan operasional organisasi dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan diri dari insiden keamanan siber.

Berdasarkan hasil sintesis terhadap CIA *Triad*, ISO/IEC 27001:2022, dan NIST CSF 2.0, penelitian ini mengusulkan model strategi manajemen keamanan informasi terintegrasi yang terdiri atas enam tahapan. Pertama, penyelarasan tata kelola *(governance alignment)*, yaitu penetapan ruang lingkup ISMS, kebijakan keamanan, serta peran dan tanggung jawab, yang mengintegrasikan klausul *Context of the Organization* dan *Leadership* dengan fungsi *Govern*. Kedua, identifikasi aset dan analisis risiko, mencakup inventarisasi aset informasi, klasifikasi data, serta identifikasi ancaman dan kerentanan menggunakan pendekatan CIA *Triad*. Ketiga, implementasi kontrol keamanan, meliputi penerapan MFA, RBAC, enkripsi data, *Data Loss Prevention* (DLP), manajemen kerentanan, dan *security awareness training*. Keempat, pemantauan dan deteksi ancaman melalui *continuous monitoring*, analisis ilog, dan *Security Information and Event Management* (SIEM), yang mengintegrasikan klausul

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Performance Evaluation dengan fungsi *Detect*. Kelima, respons insiden melalui *Incident Response Plan* (IRP) dan pembentukan *Computer Security Incident Response Team* (CSIRT), sejalan dengan fungsi *Respond* dan *Recover* pada NIST CSF 2.0, termasuk penyusunan *Disaster Recovery Plan* (DRP) dan *Business Continuity Plan* (BCP). Keenam, evaluasi dan peningkatan berkelanjutan melalui audit keamanan, penilaian tingkat kematangan, dan tindakan korektif, sesuai prinsip *Plan-Do-Check-Act* (PDCA) pada ISO/IEC 27001:2022.

Penerapan model strategi ini diharapkan memberikan sejumlah implikasi bagi perusahaan jasa. Dari sisi tata kelola, organisasi memperoleh struktur pengelolaan keamanan yang lebih sistematis melalui ISMS dan fungsi *Govern*. Dari sisi manajemen risiko, mengidentifikasi, memprioritaskan organisasi menganalisis, pengendalian mampu dan keamanan berdasarkan tingkat risiko, sehingga penerapan kontrol seperti MFA, RBAC, dan enkripsi data dapat menekan risiko akses tidak sah dan kebocoran data. Dari sisi deteksi dan respons, pemantauan berkelanjutan serta keberadaan IRP dan CSIRT memungkinkan organisasi mendeteksi ancaman lebih dini dan merespons insiden secara lebih cepat dan terkoordinasi, sedangkan DRP dan BCP mendukung pemulihan layanan sehingga dampak gangguan terhadap operasional dapat diminimalkan.

Penelitian ini memiliki keterbatasan karena model strategi yang dihasilkan bersifat konseptual dan disusun berdasarkan sintesis literatur (SLR), sehingga belum diuji secara empiris pada perusahaan jasa tertentu. Oleh karena itu, hasil penelitian ini lebih tepat dimaknai sebagai kerangka acuan awal yang perlu divalidasi lebih lanjut melalui studi kasus atau penerapan langsung pada organisasi penyedia layanan berbasis *cloud*.

SIMPULAN

Penelitian ini menganalisis kondisi keamanan informasi, risiko keamanan, dan strategi manajemen keamanan informasi pada penggunaan sistem berbasis *cloud* di perusahaan jasa melalui pendekatan *Systematic Literature Review* terhadap lima belas artikel ilmiah. Hasil analisis menunjukkan bahwa aspek *Confidentiality, Integrity*, dan *Availability* (CIA *Triad*) tetap menjadi tiga pilar utama keamanan informasi, dengan ancaman dominan berupa akses tidak sah dan kebocoran data pada aspek kerahasiaan, manipulasi data dan kesalahan konfigurasi pada aspek integritas, serta gangguan layanan dan kegagalan infrastruktur pada aspek ketersediaan. Analisis risiko berdasarkan ISO/IEC 27001:2022 dan NIST *Cybersecurity Framework* (CSF) 2.0 menunjukkan bahwa kedua kerangka kerja bersifat saling melengkapi: ISO/IEC 27001:2022 memperkuat tata kelola keamanan informasi melalui *Information Security Management System* (ISMS), sedangkan NIST CSF 2.0 memperkuat kesiapan operasional organisasi melalui fungsi *Govern, Identify, Protect, Detect, Respond, dan Recover*.

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Berdasarkan hasil sintesis tersebut, penelitian ini menghasilkan model strategi manajemen keamanan informasi terintegrasi yang mencakup enam tahapan, yaitu penyelarasan tata kelola, identifikasi aset dan analisis risiko, implementasi kontrol keamanan, pemantauan dan deteksi ancaman, respons insiden, serta evaluasi dan peningkatan berkelanjutan. Perusahaan jasa disarankan membangun ISMS sesuai ISO/IEC 27001:2022 sebagai landasan tata kelola, menerapkan kontrol teknis seperti *Multi-Factor Authentication, Role-Based Access Control*, dan enkripsi data untuk menekan risiko akses tidak sah dan kebocoran data, membangun mekanisme pemantauan berkelanjutan serta rencana respons insiden, dan melaksanakan audit maupun evaluasi kematangan keamanan secara berkala agar strategi keamanan informasi dapat terus disesuaikan dengan perkembangan ancaman siber. Mengingat model strategi yang dihasilkan masih bersifat konseptual, penelitian selanjutnya disarankan melakukan validasi empiris melalui studi kasus pada perusahaan jasa yang telah mengimplementasikan sistem berbasis *cloud*.

DAFTAR PUSTAKA

Anwar, R. W., Pastore, F., & Abdullah, T. (2026). VIRTUOSO : A Multilayer Cloud Security and Risk Management Framework. *Computers*, *15*(272), 1–34. https://doi.org/https://doi.org/10.3390/computers15050272

Bajdor, P. (2024). Evaluating Current and Future Impacts of Cloud Computing on Enterprise Operations: A Comparative Analysis. *Procedia Computer Science*, *246*, 5185–5194. https://doi.org/10.1016/j.procs.2024.09.614

Bitkowska, A., Dziembek, D., & Gzik, T. (2024). Enterprise Resource Planning based on Cloud Computing (Cloud ERP). *Journal of Software & Systems Development*, *2024*, 16. https://doi.org/https://doi.org/10.5171/2024.206232

BSSN. (2023). Lanskap Keamanan Siber Indonesia 2023. *TLP Clear*, 1–105.

Dahal, N. (2025). Qualitative Data Analysis Reflections, Procedures, and Some Points for Consideration. *Front. Res. Metr. Anal*, *10*. https://doi.org/https://doi.org/10.3389/frma.2025.1669578

Essien, I. A., Cadet, E., Ajayi, J. O., Erigh, E. D., Obuse, E., Ayanbode, N., & Babatunde, L. A. (2022). Optimizing Cyber Risk Governance Using Global Frameworks: ISO, NIST, and COBIT Alignment. *Journal of Frontiers in Multidisciplinary Research*, *03*(01), 618–629. https://doi.org/https://doi.org/10.54660/.JFMR.2022.3.1.618-629

Fadli, M. R. (2021). Memahami Desain Metode Penelitian Kualitatif. *Humanika*, *21*(1), 33–54. https://doi.org/10.21831/hum.v21i1. 38075. 33-54

Frangky, & Sinaga, R. (2024). Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala. *NUANSA INFORMATIKA*, *18*(2), 46–54. https://doi.org/https://doi.org/10.25134/ilkom.v18i2.205

Guo, J., & Guo, H. (2023). Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing. *Symmetry*, *15*, 988. https://doi.org/https://doi.org/10.3390/sym15050988

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Hashim, S., Omar, M. K., Jalil, H. A., & Sharef, N. M. (2022). Trends on Technologies and Artificial Intelligence in Education for Personalized Learning: Systematic Literature Review Trends on Technologies and Artificial Intelligence in Education for Personalized Learning : Systematic Literature Review. *International Journal of Academic Research in Progressive Education and Development*, *11*(1), 884–903. https://doi.org/10.6007/IJARPED/v11-i1/12230

Hsu, H.-H., & Shih, J.-R. (2023). ISO 27001 Information Security Survey of Medical Service Organizations. *Engineering Proceedings*, *55*(19), 2–7. https://doi.org/https://doi.org/10.3390/engproc2023055019

Huang, J., & Yi, J. (2024). The Key Security Management Scheme of Cloud Storage Based on Blockchain and Digital Twins. *Journal of Cloud Computing*. https://doi.org/10.1186/s13677-023-00587-4

Innomesanghan, D., Kiwamu, E., Butakov, S., & Abdallah, E. G. (2025). Streamlining Security: Mapping NIST SP 800-53, SOC 2, and US CJIS Policy to ISO/IEC 27001:2022 for Service Provider SMEs. *Proceedings of the 10th International Conference on Computer and Information Science and Technology*, 1–8. https://doi.org/10.11159/cist25.112

Kahraman, Z., & Rigopoulos, G. (2024). Digital Transformation and Operational Efficiency for SMEs in the Food Sector. *International Journal of Management and Commerce Innovations*, *11*(2), 208–213. https://doi.org/https://doi.org/10.5281/zenodo.10438688

Kamil, Y., Lund, S., & Islam, M. S. (2023). Information Security Objectives and the Output Legitimacy of ISO/IEC 27001: Stakeholders' Perspective on Expectations in Private Organizations in Sweden. *Information Systems and E-Business Management*, *21*, 699–722.

Khader, M., Karam, M., & Fares, H. (2021). *Cybersecurity Awareness Framework for Academia*. *12*(10), 1–20. https://doi.org/https://doi.org/10.3390/info12100417

Kuldeep, G., & Zhang, Q. (2022). Multi-class Privacy-preserving Cloud Computing Based on Compressive Sensing for IoT. *Journal of Information Security and Applications*. https://doi.org/https://doi.org/10.1016/j.jisa.2022.103139

Marhad, S. S., Goni, S. Z. A., & Sani, M. K. J. abdullah. (2023). Implementation of Information Security Management Systems for Data Protection in Organizations: A Systematic Literature Review. *Environment-Behaviour Proceedings Journal*, 197–203. https://doi.org/https://doi.org/10.21834/e-bpj.v9iSI18.5483

Morol, K., Das, S. S., & Mahmood, S. (2022). Data Security and Privacy in Cloud Computing Platforms: A Comprehensive Review. *International Journal of Current Science Research and Review*, *05*(05), 1453–1463. https://doi.org/10.47191/ijcsrr/V5-i5-09

Nugroho, A. R., & Legowo, N. (2022). Risk Assessment at it Company by Focusing on Information Security Area Using Iso 27001:2022. *Syntax Literate: Jurnal Ilmiah Indonesia*, *7*(12).

Oyeniyi, Olusegun, J., Oyeniran, & Akinloye, O. (2025). Optimizing Information Security In Cloud Environments: A Risk Management Approach And Guide For Enterprise Cloud Security Optimizing Information Security In Cloud Environments : A Risk Management. *Journal of Cybersecurity Education, Research and Practice*, *2025*(1). https://doi.org/https://doi.org/10.62915/2472-2707.1213

Qazi, A., Arshad, S., Ali, A., & Jadoon, K. (2026). Security Evaluation Framework for Cloud ERP Systems Using NIST and ISO Standards. *Scientific Reports*, 1–18. https://doi.org/https://doi.org/10.1038/s41598-026-45550-w

JIBEMA: Jurnal Ilmu Bisnis, Ekonomi, Manajemen, dan Akuntansi
Volume 4, No. 1, July 2026, p. 2507-2517

Rambau, T. M., Munyoka, W., Phahlamohlaka, L. J., & Kadyamatimba, A. (2026). Evaluating Cyber Resilience Frameworks for E-government: Applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in Developing Country Contexts. *Information and Computer Security, Vol. Ahead-of-Print No. Ahead-of-Print*. https://doi.org/10.1108/ICS-09-2025-0376

Schmidt, M. (2023). Information Security Risk Management Terminology and Key Concepts. *Risk Management*, *25*(1), 1–23. https://doi.org/10.1057/s41283-022-00108-8

Vasovic, D., Jana´ckovi´, G., Vranjanac, Ž., Stamenkovi´, S., & BojanVasovi´c. (2026). Enhancing CIA Triad — Confidentiality, Integrity and Availability in Educational Information Systems Through Next-Generation ISO/IEC 27001:2022-Aligned Security Model. *Applied Sciences*, *16*(12), 6260. https://doi.org/https://doi.org/10.3390/app16126260

