E-ISSN : 2988-1986
https://ejournal.cahayailmubangsa.institute/index.php/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 10 No 6 Tahun 2025

PENERAPAN KEBIJAKAN KEAMANAN INFORMASI TERINTEGRASI DALAM MEMBANGUN TATA KELOLA PENGGUNAAN TEKNOLOGI YANG AMAN

Dimas Kurniawan [1], Rhois Aghil[2], Syalvina[3]
[1,2,3]Program Studi Sistem Informasi , Fakultas Sains dan Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi
E-mail:kurndimas9@gmail.com[1], rhzaghil@gmail.com[2], syalvinacndra@gmail.com[3]

ABSTRACT

This research analyzes the implementation of integrated information security policies in building governance for safe use of technology through a Systematic Literature Review (SLR) approach to 27 articles obtained from Google Scholar (12), Garuda (9), and Neliti (6) with selection procedures following the PRISMA protocol. The synthesis results show that information security policies designed based on standard frameworks such as ISO/IEC 27001, COBIT 5/2019, and the KAMI Index are able to increase the effectiveness of security control mechanisms, strengthen digital risk management, and support the protection of aspects of confidentiality, integrity, and availability of information for society and technology users in general. The literature also highlights a number of implementation challenges, such as lack of information security awareness, limited resources, and inconsistency in policy updates, which also influence the level of digital environment security. Overall, this research confirms that the integration of information security policies is a strategic step in creating governance for the use of technology that is safer, more adaptive and sustainable, and can be a reference in developing security policies in various contexts of the use of modern technology.

Keywords: Information security policy, IT governance, ISO/IEC 27001, COBIT, SLR.

ABSTRAK

Penelitian ini menganalisis penerapan kebijakan keamanan informasi terintegrasi dalam membangun tata kelola penggunaan teknologi yang aman melalui pendekatan Systematic Literature Review (SLR) terhadap 27 artikel yang diperoleh dari Google Scholar (12), Garuda (9), dan Neliti (6) dengan prosedur seleksi mengikuti protokol PRISMA. Hasil sintesis menunjukkan bahwa kebijakan keamanan informasi yang dirancang berdasarkan kerangka standar seperti ISO/IEC 27001, COBIT 5/2019, dan Indeks KAMI mampu meningkatkan efektivitas mekanisme kontrol keamanan, memperkuat pengelolaan risiko digital, serta mendukung perlindungan aspek kerahasiaan, integritas, dan ketersediaan informasi bagi masyarakat dan pengguna teknologi secara umum. Literatur sekaligus menyoroti sejumlah tantangan implementatif, seperti kurangnya kesadaran keamanan informasi, keterbatasan sumber daya, dan ketidakkonsistenan pembaruan

Article History
Received: November 2025
Reviewed:November 2025
Published: November 2025

Plagiarism Checker No 235
Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

kebijakan yang turut memengaruhi tingkat keamanan lingkungan digital. Secara keseluruhan, penelitian ini menegaskan bahwa integrasi kebijakan keamanan informasi merupakan langkah strategis dalam menciptakan tata kelola penggunaan teknologi yang lebih aman, adaptif, dan berkelanjutan, serta dapat menjadi acuan dalam pengembangan kebijakan keamanan di berbagai konteks penggunaan teknologi modern.

Kata Kunci: ***Kebijakan keamanan informasi, Tata kelola TI, ISO/IEC 27001, COBIT, SLR.***

1. PENDAHULUAN

Perkembangan pesat teknologi informasi dan digitalisasi membawa manfaat yang besar bagi masyarakat, tetapi juga meningkatkan eksposur terhadap berbagai ancaman keamanan informasi. Ketergantungan masyarakat pada layanan digital mulai dari transaksi daring, media sosial, hingga pemerintahan berbasis elektronik menuntut kebijakan keamanan informasi yang tidak hanya reaktif tetapi juga proaktif dan terintegrasi untuk melindungi kerahasiaan, integritas, dan ketersediaan data pengguna (Djatmiko et al., 2025).

Tata kelola keamanan informasi (information security governance) menjadi komponen penting dalam mengelola risiko digital, karena mengatur struktur kebijakan, peran dan tanggung jawab, serta mekanisme kontrol risiko yang selaras dengan tujuan strategis penggunaan teknologi di masyarakat (AlGhamdi et al., 2020). Dalam konteks publik atau masyarakat secara umum, penelitian terkini menunjukkan bahwa kelemahan dalam tata kelola misalnya kurangnya indikator kinerja keamanan, audit kepatuhan, dan model kematangan risiko masih menjadi akar dari kegagalan pengamanan yang sistemik (Magnusson et al., 2025).

Standar dan kerangka kerja seperti ISO/IEC 27001, COBIT, dan Kerangka NIST Cybersecurity Framework (CSF) menyediakan pedoman yang diakui secara internasional untuk merumuskan kebijakan keamanan informasi. Integrasi standar-standar ini dalam kebijakan keamanan informasi memungkinkan organisasi dan komunitas digital masyarakat untuk membangun kebijakan yang komprehensif, berkelanjutan, dan berbasis risiko. Sebagai contoh, penerapan ISO 27001 secara terstruktur tidak hanya mengatur kontrol teknis tetapi juga menetapkan kebijakan manajemen keamanan yang berdasar analisis risiko (Ghozie Afiansyah et al., n.d.).

Meskipun demikian, implementasi kebijakan keamanan informasi secara terintegrasi tidak lepas dari tantangan. Penelitian terhadap lembaga publik menunjukkan bahwa komitmen manajemen, ketersediaan sumber daya, dan upaya pembaruan kebijakan secara reguler menjadi hambatan utama untuk mempertahankan sistem keamanan yang efektif (Yudistira et

al., 2024). Oleh karena itu, perlu sebuah kajian sistematis literatur untuk memahami sejauh mana kebijakan keamanan informasi terintegrasi telah diterapkan dan bagaimana hal tersebut berkontribusi pada tata kelola penggunaan teknologi yang aman di masyarakat.

2. METODE PENELITIAN

Penelitian ini menggunakan metode Systematic Literature Review (SLR) sebagai pendekatan utama untuk mengidentifikasi, mengevaluasi, dan mensintesis penelitian terkait penerapan kebijakan keamanan informasi terintegrasi dalam membangun tata kelola penggunaan teknologi yang aman. Metode SLR dipilih karena menyediakan proses yang sistematis, terstruktur, dan dapat direplikasi dalam menelusuri literatur ilmiah secara komprehensif.

2.1 Rumusan Pertanyaan Penelitian

Adapun research questions (RQ) yang digunakan adalah sebagai berikut:

RQ1: Bagaimana penerapan kebijakan keamanan informasi terintegrasi dalam berbagai konteks penggunaan teknologi?

RQ2: Kerangka kerja atau standar keamanan informasi apa saja yang digunakan dalam implementasi kebijakan keamanan informasi terintegrasi?

RQ3: Tantangan apa yang dihadapi dalam penerapan kebijakan keamanan informasi terintegrasi?

RQ4: Bagaimana kontribusi kebijakan keamanan informasi terhadap peningkatan tata kelola penggunaan teknologi yang aman?

2.2 Sumber Data dan Strategi Pencarian

Pencarian literatur dilakukan pada tiga basis data yang relevan dan dapat diakses secara terbuka, yaitu: Google Scholar, Garuda Ristekdikti, dan Neliti. Ketiga sumber tersebut dipilih karena menyediakan publikasi ilmiah dalam beragam bidang serta mendukung akses terbuka terhadap artikel.

Strategi pencarian dilakukan menggunakan kombinasi kata kunci dalam Bahasa Indonesia dan Bahasa Inggris, antara lain:

“kebijakan keamanan informasi”, “tata kelola teknologi informasi”, “integrated information security policy”, “information security governance”, “ISO/IEC 27001”, “COBIT”, dan “integrated security framework”.

Kata kunci dikombinasikan dengan operator AND, OR, dan NOT untuk memperluas hasil pencarian sesuai kebutuhan.

2.3 Kriteria Inklusi dan Ekslusi

Artikel yang ditemukan kemudian diseleksi berdasarkan kriteria berikut:

Kriteria Inklusi:

a. Membahas kebijakan keamanan informasi, tata kelola teknologi, atau integrasi kerangka kerja keamanan.
b. Tersedia dalam bentuk teks lengkap (full access) dan dapat diunduh secara gratis.
c. Termasuk kategori artikel ilmiah, prosiding, laporan penelitian, atau jurnal terakreditasi.

Kriteria Eksklusi:

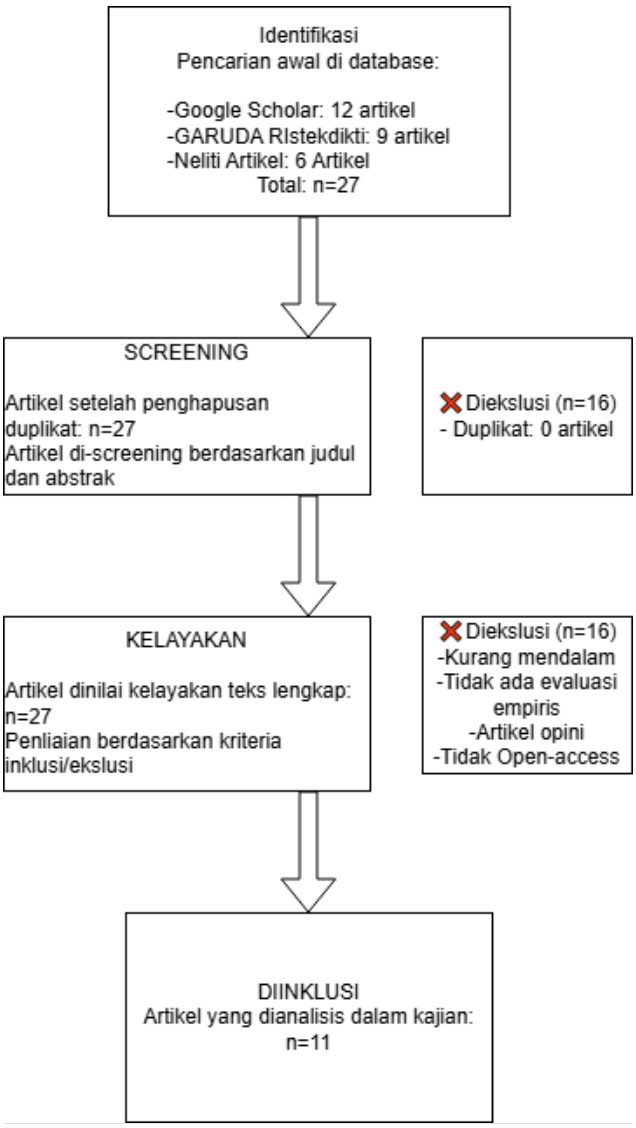
a. Artikel bersifat opini atau tidak memiliki dasar metodologis.
b. Pembahasan tidak relevan dengan keamanan informasi atau tata kelola teknologi.
c. Tidak tersedia sebagai open access.
d. Tidak memenuhi kedalaman analisis yang sesuai dengan fokus penelitian.

2.4 Proses Seleksi dan Ekstraksi Data

Dari proses pencarian awal diperoleh 27 dokumen dari ketiga sumber utama. Seluruh dokumen tersebut disaring melalui beberapa tahap: pemeriksaan duplikasi, penilaian judul dan abstrak, serta evaluasi isi penuh. Pada proses screening, sebanyak 16 artikel dieliminasi dengan alasan: tidak membahas kebijakan keamanan informasi secara mendalam (7 artikel), tidak memuat evaluasi empiris atau analisis yang relevan (4 artikel), bersifat opini tanpa metodologi (3 artikel), dan tidak tersedia dalam bentuk open access (2 artikel).

Dengan demikian, tersisa 11 artikel yang memenuhi kriteria inklusi dan dianalisis lebih lanjut melalui proses ekstraksi data.

Ekstraksi data dilakukan menggunakan lembar kerja terstruktur yang mencakup elemen: tujuan penelitian, kerangka kerja keamanan informasi yang digunakan (misalnya ISO/IEC 27001, COBIT, Indeks KAMI), metode penelitian, temuan utama, serta tantangan implementasi. Data yang terkumpul kemudian dianalisis menggunakan pendekatan sintesis tematik untuk menemukan pola dan hubungan antar temuan.



2.1 Diagram PRISMA Flow

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil sintesis dari 11 artikel yang lolos proses seleksi serta pembahasan temuan berdasarkan tema-tema yang relevan dengan pertanyaan penelitian. Analisis dilakukan secara tematik untuk mengidentifikasi pola, kesamaan, serta perbedaan antar studi terkait penerapan kebijakan keamanan informasi terintegrasi.

3.1 Gambaran Umum Artikel Terpilih

Sebanyak 11 artikel yang memenuhi kriteria inklusi memuat pembahasan terkait penerapan kebijakan keamanan informasi, tata kelola teknologi informasi, integrasi kerangka kerja keamanan, serta analisis tantangan implementasinya. Artikel tersebut mencakup berbagai konteks penggunaan teknologi, mulai dari layanan publik, sektor pendidikan, sistem

kelembagaan, hingga penggunaan teknologi secara umum oleh masyarakat. Rentang publikasi dari 2018 hingga 2025 memungkinkan tergambar jelasnya perkembangan kebijakan keamanan informasi dalam lingkungan digital yang semakin kompleks.

3.2 RQ1 - Penerapan Kebijakan Keamanan Informasi Terintegrasi

Sebagian besar artikel menunjukkan bahwa penerapan kebijakan keamanan informasi terintegrasi dilakukan melalui kombinasi tiga pendekatan utama:

1. Perumusan kebijakan berbasis standar internasional, terutama ISO/IEC 27001, ISO/IEC 27002, COBIT 5/2019, dan NIST Cybersecurity Framework.
2. Penguatan tata kelola dan manajemen risiko, melalui pengaturan peran, prosedur, audit, dan pengendalian akses.
3. Integrasi kebijakan secara lintas-domain, meliputi manajemen aset informasi, kontrol teknologi, keamanan fisik, dan keamanan sumber daya manusia.

Implementasi kebijakan terintegrasi secara konsisten memberikan dampak positif terhadap perlindungan kerahasiaan, integritas, dan ketersediaan informasi (CIA Triad). Beberapa studi juga menegaskan bahwa integrasi kebijakan membantu meningkatkan konsistensi antar unit kerja, meminimalkan risiko operasional, dan memperjelas tanggung jawab pengamanan teknologi.

3.3 RQ2 - Kerangka Kerja dan Standar yang Paling Banyak Digunakan

Dari analisis 11 artikel, ditemukan bahwa kerangka kerja yang paling banyak digunakan dalam implementasi kebijakan keamanan informasi adalah:

a. ISO/IEC 27001

Kerangka ini menjadi standar paling dominan dalam penelitian, terutama dalam evaluasi kontrol keamanan, manajemen risiko, serta perumusan kebijakan organisasi atau layanan digital.

b. COBIT 5/2019

COBIT digunakan terutama untuk menganalisis aspek tata kelola (governance), seperti pengawasan manajemen, evaluasi kematangan, penetapan peran dan tanggung jawab, serta integrasi kebijakan ke dalam proses organisasi.

c. Indeks KAMI

Banyak artikel memanfaatkan Indeks KAMI untuk mengukur kesiapan keamanan informasi, terutama pada konteks lembaga publik dan penyedia layanan.

d. NIST Cybersecurity Framework (CSF)

NIST digunakan untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan insiden, serta mengatur mekanisme manajemen risiko digital.

Hasil sintesis menunjukkan bahwa kombinasi ISO/IEC 27001 dan COBIT memberikan hasil paling komprehensif karena mencakup aspek security controls dan governance secara bersamaan.

3.4 RQ3 - Tantangan dalam Penerapan Kebijakan Keamanan Informasi

Tantangan paling signifikan yang muncul dari 11 artikel meliputi:

a. Keterbatasan Sumber Daya Manusia (SDM)

Kurangnya tenaga ahli keamanan informasi menjadi hambatan utama dalam menjaga konsistensi implementasi kebijakan.

b. Kurangnya Komitmen Manajemen dan Pengambilan Keputusan

Beberapa artikel menekankan bahwa kebijakan hanya bersifat administratif tanpa dukungan kuat dari pimpinan, sehingga implementasi di lapangan tidak maksimal.

c. Kesadaran Keamanan yang Rendah pada Pengguna

Rendahnya literasi digital masyarakat menyebabkan tindakan tidak aman seperti penggunaan kata sandi lemah, akses tanpa proteksi, dan kurangnya kewaspadaan terhadap ancaman siber.

d. Ketidakteraturan Pembaruan Kebijakan

Banyak kebijakan tidak diperbaharui secara berkala mengikuti perkembangan ancaman dan teknologi.

e. Minimnya audit keamanan dan dokumentasi risiko

Audit yang tidak terjadwal dan kurangnya dokumentasi risiko menyebabkan lemahnya deteksi dini potensi kerentanan.

Temuan-temuan ini menunjukkan bahwa kebijakan keamanan informasi tidak dapat berjalan efektif tanpa dukungan budaya keamanan dan tata kelola organisasi yang kuat.

3.5 RQ4 - Kontribusi Kebijakan Keamanan Informasi terhadap Tata Kelola Teknologi yang Aman

Kebijakan keamanan informasi terintegrasi memberikan sejumlah kontribusi penting, di antaranya:

a. Meningkatkan Kejelasan Peran dan Prosedur

Kebijakan yang terstruktur membantu masyarakat atau pengguna layanan digital memahami prosedur keamanan dan tanggung jawab masing-masing.

b. Memperkuat Mekanisme Kontrol Keamanan

Integrasi kebijakan meningkatkan efektivitas kontrol teknis dan administratif, sehingga meminimalkan risiko pelanggaran keamanan.

c. Mengoptimalkan Manajemen Risiko

Kerangka berbasis risiko, terutama ISO 31000, memungkinkan organisasi dan masyarakat memprioritaskan pengamanan berdasarkan tingkat ancaman.

d. Mendukung Ketahanan Digital (Cyber Resilience)

Kebijakan keamanan yang terintegrasi meningkatkan kemampuan sistem untuk bertahan, mendeteksi, dan memulihkan diri dari insiden keamanan.

e. Mendorong Tata Kelola Teknologi yang Adaptif dan Berkelanjutan

Kebijakan yang jelas dan terukur mampu meningkatkan akuntabilitas, kepatuhan, dan kualitas pengelolaan teknologi secara menyeluruh.

3.6 Sintesis Tematik

Secara keseluruhan, sintesis 11 artikel mengungkap bahwa integrasi kebijakan keamanan informasi bukan hanya berfungsi sebagai pedoman teknis, tetapi juga menjadi pilar penting dalam tata kelola penggunaan teknologi yang aman. Efektivitas kebijakan sangat ditentukan oleh kombinasi antara aspek teknis, budaya keamanan, manajemen risiko, serta dukungan lembaga atau komunitas pengguna teknologi.

KESIMPULAN

Penelitian ini menegaskan bahwa penerapan kebijakan keamanan informasi terintegrasi memiliki peran yang sangat signifikan dalam membangun tata kelola penggunaan teknologi yang aman bagi masyarakat dan berbagai pemangku kepentingan digital. Melalui analisis sistematis terhadap 11 artikel terpilih dari total 27 dokumen yang diperoleh, ditemukan bahwa kebijakan keamanan informasi yang komprehensif mampu menyediakan fondasi yang kuat bagi pengendalian risiko serta perlindungan aset informasi pada berbagai konteks penggunaan teknologi.

Temuan penelitian menunjukkan bahwa kebijakan keamanan informasi yang efektif umumnya memuat kerangka pengendalian yang terstandarisasi—seperti ISO/IEC 27001 dan

dokumen pendukungnya—serta mengintegrasikan berbagai aspek teknis dan non-teknis. Integrasi tersebut mencakup mekanisme kontrol teknis, prosedur operasional, peran manusia, kepatuhan regulatif, serta budaya keamanan yang harus dibangun secara berkelanjutan. Kebijakan yang berlapis dan adaptif terbukti lebih mampu mengantisipasi dinamika ancaman digital yang terus berkembang.

Selain itu, hasil sintesis memperlihatkan bahwa keberhasilan implementasi kebijakan sangat dipengaruhi oleh tingkat literasi keamanan informasi pada masyarakat, kedisiplinan dalam menerapkan standar keamanan, serta kesiapan organisasi atau lingkungan digital dalam mengadopsi kebijakan secara holistik. Ketidaksiapan pada salah satu aspek tersebut seringkali menyebabkan kebijakan tidak berjalan efektif, meskipun kerangka regulasi dan kontrol teknis telah tersedia.

Selanjutnya, kebijakan yang dirancang dan diterapkan secara terintegrasi terbukti mampu menekan risiko insiden keamanan, meningkatkan kepercayaan pengguna terhadap layanan digital, serta memperkuat tata kelola teknologi yang berkelanjutan. Hal ini menunjukkan bahwa pendekatan kebijakan yang strategis dan menyeluruh bukan hanya menjadi kebutuhan teknis, tetapi juga menjadi faktor kunci dalam menjaga stabilitas ekosistem digital secara keseluruhan.

Dengan demikian, penelitian ini memberikan gambaran komprehensif mengenai praktik-praktik terbaik yang dapat dijadikan acuan dalam pengembangan kebijakan keamanan informasi. Selain itu, penelitian ini membuka peluang bagi kajian lanjutan, seperti pengembangan model evaluasi efektivitas kebijakan pada sektor tertentu, studi terkait adaptasi kebijakan pada lingkungan teknologi yang terus berubah, serta penyusunan strategi peningkatan kesadaran keamanan pada tingkat masyarakat luas.

DAFTAR PUSTAKA

[1] Syahputra, A. (2022). *Perencanaan Sistem Manajemen Keamanan Informasi pada Organisasi*. https://media.neliti.com/media/publications/583532-perencanaan-sistem-manajemen-keamanan-in-670a2888.pdf

[2]Yusuf, M. (2019). *Analisis dan Penerapan Sistem Manajemen Keamanan Informasi*. https://media.neliti.com/media/publications/300954-analisis-dan-penerapan-sistem-manajemen-0a739362.pdf

[3] Wibisono, I. (2017). *Perencanaan Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*.

https://media.neliti.com/media/publications/227023-perencanaan-sistem-manajemen-

keamanan-in-291ab8b5.pdf

[4] Fathurrahman, A. (2020). *Standar dan Manajemen Keamanan Komputer*. https://media.neliti.com/media/publications/242349-standar-dan-manajemen-keamanan-komputer-3f34eecc.pdf

[5] Ramadhan, R. (2018). *Kajian Kesiapan Keamanan Informasi Instansi Pemerintah*. https://media.neliti.com/media/publications/233786-kajian-kesiapan-keamanan-informasi-insta-672e52c2.pdf

[6] Najib, M. (2019). *Implementasi Keamanan Pemanfaatan Teknologi Informasi pada Lembaga Pendidikan*. https://media.neliti.com/media/publications/243318-implementasi-keamanan-pemanfaatan-teknol-5511b199.pdf

[7] Priandoyo, A. (2006). *Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi*. https://d1wqtxts1xzle7.cloudfront.net/37650751/2006-06-Maranatha-Vulnerability_assessment_to_increase_IS_sec._awareness__ISSN19071221-libre.pdf

[8] Putra, R. G., Fauzi, A., Prasetyo, E. T., Pratama, S. R., Ramadhan, I. D., Febriyanti, F., & Nurlela, S. (2023). *Pentingnya Manajemen Security di Era Digitalisasi*. https://pdfs.semanticscholar.org/19df/314770fb75d05bab64ed4064027d85463c84.pdf

[9] Maulana, G. R., Aqila, S. W., Sakinah, N. H., Wulandari, N. I., & Nurhayati, C. (2023). *Manfaat Manajemen Keamanan Informasi terhadap Pengamanan Data Pribadi Mahasiswa Prodi Akuntansi Universitas Trunojoyo Madura*. https://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/23715/9535

[10] Utomo, M., Ali, A. H. N., & Affandi, I. (2012). *Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 pada Kantor Pelayanan Perbendaharaan Surabaya*. https://d1wqtxts1xzle7.cloudfront.net/42687888/jurnal_audit_pembuatan_tata_kelola-libre.pdf

[11] Salsabila, N. (2025). *Analisis Pengendalian Sistem Informasi Akuntansi (SIA) terhadap Keamanan Data dan Informasi Akuntansi*. https://calamus.id/index.php/edutik/article/view/25/25

Dewi, A. K., Sibarani, B. K., Saputra, E., Norazlina, S., Susanti, S., Syafira, Y., & Munakalla, Y. (2025). *Strategi Efektif Pengendalian Internal dalam Keamanan Sistem Informasi Akuntansi untuk Perlindungan Data Keuangan*. https://www.ejournal.polraf.ac.id/index.php/JIRA/article/view/838/615

[12] Bakri, M., & Irmayana, N. (2017). *Analisis dan Penerapan Sistem Manajemen Keamanan*

Informasi SIMHP BPKP Menggunakan Standar ISO 27001. https://d1wqtxts1xzle7.cloudfront.net/98337509/131-libre.pdf

[13] Mardiyana, I., Hariyanti, E., Arrasyid, N. N., Handayani, A. T., Suryadewi, K. S., Akhlaqulkarimah, F., & Pramiyas, N. H. (2023). *Penerapan Kerangka Kerja Keamanan Informasi di Rumah Sakit: Tinjauan Literatur Sistematis*. https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/article/download/1260/791

[14] Safina, W. D., Damayanti, P., & Akhmarozi, F. (2025). *Metode Pengendalian dan Pengelolaan SDM: Kajian Literatur Sistematis Tahun 2020-2024*. https://jurnalmahasiswa.uma.ac.id/index.php/jimbi/article/view/6226

[15] Ujung, A. M., & Nasution, M. I. P. (2023). *Pentingnya Sistem Keamanan Database untuk Melindungi Data Pribadi*. https://jurnal.unidha.ac.id/index.php/jiska/article/view/929/546

[17] Mafiana, A. I., Hanun, L., Ilmi, H. M., & Febriliani, S. (2023). *Implementasi Manajemen Keamanan Informasi Berbasis ISO 27001 pada Sistem Informasi Akademik*. https://ejournal.unesa.ac.id/index.php/jdbim/article/download/57580/45323

[18] ISO/IEC. (2013). *ISO/IEC 27001:2013 — Information Security Management Systems — Requirements*. International Organization for Standardization. https://www.iso.org/standard/54534.html

[19] ISO/IEC. (2018). *ISO/IEC 27002:2018 — Information Security Controls*. International Organization for Standardization. https://www.iso.org/standard/73906.html

[20] ISO/IEC. (2022). *ISO/IEC 27001:2022 — Information Security Management Systems — Requirements*. International Organization for Standardization. https://www.iso.org/standard/82875.html

[21] AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & Security, 99, 102030. https://doi.org/10.1016/J.COSE.2020.102030

[22] Djatmiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital Transformation and Social Inclusion in Public Services: A Qualitative Analysis of E-Government Adoption for Marginalized Communities in Sustainable Governance. Sustainability (Switzerland), 17(7). https://doi.org/10.3390/su17072908

[23] Ghozie Afiansyah, H., Annisa, N., & Febriyani, K. (n.d.). Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022.

[24] Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. International Journal of Information Security, 24(4). https://doi.org/10.1007/s10207-025-01097-x

[25] Yudistira, A., Zaini, F., Sugiantoro, B., Riwanto, Y., Islam, U., Kalijaga, N. S., & Yogyakarta, U. A. (2024). Analisis Evaluasi Keamanan Informasi Pada Badan pemerintahan Pemerintahan XYZ Menggunakan Indeks KAMI 4.2 Analysis Information Security Evaluation On Governnment Agency XYZ Using KAMI Index 4.2 (Vol. 7, Issue 2).