

Analisis Kesenjangan (Gap Analysis) Keamanan Informasi pada Instansi Pemerintah Indonesia Berdasarkan Indeks KAMI 5.0 dan Standar Internasional

Dimas Ahsanul Habibi¹, Eri Zuliarso², Eka Ardhianto³

^{1,2,3} Universitas Stikubank (UNISBANK)

Alamat Jalan Tri Lomba Juang No. 1, Mugassari, Semarang Selatan
dimasahsanul0002@mhs.unisbank.ac.id, eri299@edu.unisbank.ac.id,
ekaardhianto@edu.unisbank.ac.id

(Received: Juni 2026, Revised: Agustus 2026, Accepied: Oktober 2026)

Abstract—This study aims to analyze information security gaps in government agencies in Indonesia using the Information Security Index (KAMI) version 5.0, developed by the National Cyber and Cryptography Agency (BSSN). This evaluation focuses on three main aspects: information security governance, risk management, and the information security framework, which are then compared with the requirements of ISO/IEC 27001:2022 and the NIST Cybersecurity Framework (CSF). The analysis results show that most government agencies are still at the basic maturity level, with an average score of 450 out of a total of 645 points. The most significant gaps were found in risk management, the implementation of security controls, and monitoring and evaluation mechanisms, which do not yet fully meet international standards. These findings indicate that the implementation of information security still requires strengthening—in terms of policies, governance, and technical controls—to enhance the effectiveness of information asset protection. Based on these findings, this study recommends strengthening risk management, improving compliance with ISO/IEC 27001:2022, optimizing the implementation of the NIST CSF, and developing human resource competencies as strategic steps to improve the level of information security maturity in Indonesian government agencies.

Keywords: KAMI Index 5.0, Gap Analysis, Information

Kata Kunci: Indeks KAMI 5.0, Gap Analysis, Keamanan Informasi, ISO/IEC 27001:2022, NIST Cybersecurity Framework

I. PENDAHULUAN

Transformasi digital telah mendorong perubahan yang signifikan dalam penyelenggaraan layanan publik di Indonesia. Berbagai instansi pemerintah kini memanfaatkan teknologi informasi dan sistem elektronik untuk mendukung proses administrasi, pengelolaan data, serta penyediaan layanan publik yang lebih efektif, efisien, transparan, dan akuntabel (Ningrum & Riwanto, 2024). Digitalisasi tersebut tidak hanya meningkatkan kualitas pelayanan kepada masyarakat, tetapi juga memperluas permukaan serangan (*attack surface*) yang dapat dimanfaatkan oleh pelaku kejahatan siber. Ancaman seperti kebocoran data, serangan *ransomware*, *phishing*, pencurian identitas, serta gangguan terhadap ketersediaan layanan menjadi risiko yang semakin kompleks seiring meningkatnya ketergantungan organisasi terhadap teknologi informasi. Oleh karena itu, penerapan keamanan informasi yang komprehensif dan berkelanjutan menjadi salah satu faktor penting dalam menjamin kerahasiaan, integritas, dan ketersediaan informasi pada instansi pemerintah.

Sebagai upaya memperkuat tata kelola keamanan siber nasional, Badan Siber dan Sandi Negara (BSSN) mengembangkan Indeks Keamanan Informasi (KAMI) sebagai instrumen untuk mengukur tingkat kematangan penerapan keamanan informasi pada penyelenggara sistem elektronik. Indeks KAMI versi 5.0 merupakan pengembangan terbaru yang telah diselaraskan dengan standar internasional ISO/IEC 27001:2022 serta NIST Cybersecurity

Intisari— Penelitian ini bertujuan menganalisis kesenjangan (*gap analysis*) keamanan informasi pada instansi pemerintah di Indonesia menggunakan Indeks Keamanan Informasi (KAMI) versi 5.0 yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN). Evaluasi difokuskan pada tiga aspek utama, yaitu tata kelola keamanan informasi, pengelolaan risiko, dan kerangka kerja keamanan informasi, kemudian dibandingkan dengan persyaratan ISO/IEC 27001:2022 serta NIST Cybersecurity Framework (CSF). Hasil analisis menunjukkan bahwa sebagian besar instansi pemerintah masih berada pada tingkat kematangan dasar dengan nilai rata-rata 450 dari total 645 poin. Kesenjangan yang paling signifikan ditemukan pada aspek pengelolaan risiko, implementasi pengendalian keamanan, serta mekanisme pemantauan dan evaluasi yang belum sepenuhnya memenuhi standar internasional. Kondisi tersebut menunjukkan bahwa penerapan keamanan informasi masih memerlukan penguatan, baik dari sisi kebijakan, tata kelola, maupun pengendalian teknis untuk meningkatkan efektivitas perlindungan aset informasi. Berdasarkan temuan tersebut, penelitian ini merekomendasikan penguatan manajemen risiko, peningkatan kepatuhan terhadap ISO/IEC 27001:2022, optimalisasi penerapan NIST CSF, serta pengembangan kompetensi sumber daya manusia sebagai langkah strategis dalam meningkatkan tingkat kematangan keamanan informasi di lingkungan instansi pemerintah Indonesia.

Framework (CSF), sehingga mampu memberikan metode evaluasi yang lebih komprehensif terhadap aspek tata kelola keamanan informasi, manajemen risiko, pengelolaan aset informasi, pengendalian keamanan, serta kesiapan organisasi dalam menghadapi berbagai ancaman siber (Jelita et al., 2024). Melalui instrumen tersebut, organisasi dapat mengidentifikasi tingkat kematangan keamanan informasi, mengevaluasi efektivitas pengendalian yang telah diterapkan, serta menentukan prioritas peningkatan berdasarkan praktik terbaik yang diakui secara internasional.

Meskipun Indeks KAMI telah tersedia sebagai pedoman evaluasi nasional, implementasinya pada berbagai instansi pemerintah masih menunjukkan tingkat kematangan yang beragam. Sejumlah penelitian mengungkapkan bahwa sebagian instansi belum melaksanakan evaluasi keamanan informasi secara berkala dan belum memanfaatkan Indeks KAMI secara optimal sebagai dasar dalam penyusunan kebijakan maupun strategi peningkatan keamanan informasi (Pratiwi & Wulandari, 2021). Selain itu, keterbatasan sumber daya manusia yang memiliki kompetensi di bidang keamanan siber, rendahnya tingkat kesadaran keamanan informasi, keterbatasan anggaran, serta belum optimalnya penerapan manajemen risiko menyebabkan berbagai pengendalian keamanan belum dapat diimplementasikan secara efektif. Kondisi tersebut menimbulkan kesenjangan antara praktik keamanan informasi yang diterapkan dengan persyaratan standar internasional, sehingga berpotensi meningkatkan kerentanan organisasi terhadap berbagai ancaman dan insiden siber.

Berdasarkan kondisi tersebut, diperlukan suatu analisis yang mampu mengidentifikasi tingkat kesesuaian penerapan keamanan informasi pada instansi pemerintah dengan standar yang berlaku. Analisis kesenjangan (*gap analysis*) menjadi pendekatan yang relevan karena dapat menggambarkan perbedaan antara kondisi aktual dan kondisi yang diharapkan berdasarkan Indeks KAMI 5.0, ISO/IEC 27001:2022, serta *NIST Cybersecurity Framework*. Hasil analisis tersebut diharapkan dapat memberikan informasi mengenai area-area yang masih memerlukan perbaikan sehingga instansi pemerintah dapat menyusun langkah

strategis secara lebih terarah dalam meningkatkan tingkat kematangan keamanan informasi.

Oleh karena itu, penelitian ini bertujuan menganalisis kesenjangan penerapan keamanan informasi pada instansi pemerintah di Indonesia menggunakan Indeks KAMI versi 5.0 sebagai instrumen utama evaluasi. Analisis dilakukan dengan membandingkan tingkat kematangan keamanan informasi terhadap praktik terbaik yang direkomendasikan dalam ISO/IEC 27001:2022 dan *NIST Cybersecurity Framework*. Hasil penelitian diharapkan dapat memberikan gambaran mengenai kondisi aktual keamanan informasi pada sektor pemerintahan, mengidentifikasi aspek-aspek yang masih memerlukan peningkatan, serta menghasilkan rekomendasi strategis yang dapat dijadikan acuan dalam memperkuat tata kelola keamanan informasi, meningkatkan efektivitas manajemen risiko, mengoptimalkan penerapan pengendalian keamanan, dan membangun ketahanan siber instansi pemerintah secara berkelanjutan.

II. TINJAUAN PUSTAKA

Berikut merupakan versi yang telah disempurnakan dengan bahasa Indonesia yang lebih formal, koheren, dan sesuai dengan gaya penulisan artikel ilmiah. Subjudul juga disusun secara sistematis untuk bagian

Tinjauan Tinjauan Pustaka Indeks Keamanan Informasi (KAMI)

Indeks Keamanan Informasi (KAMI) merupakan instrumen evaluasi yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN) untuk mengukur tingkat kematangan penerapan keamanan informasi pada penyelenggara sistem elektronik di Indonesia. Instrumen ini dirancang sebagai alat evaluasi mandiri (*self-assessment*) yang mengacu pada prinsip-prinsip Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan SNI ISO/IEC 27001, sehingga dapat digunakan untuk menilai kesiapan organisasi dalam melindungi kerahasiaan, integritas, dan ketersediaan informasi (Hasibuan, 2024). Melalui Indeks KAMI, organisasi dapat mengetahui tingkat kematangan keamanan informasi yang telah dicapai sekaligus mengidentifikasi area yang masih memerlukan peningkatan.

Indeks KAMI mengevaluasi enam elemen utama, yaitu tata kelola keamanan informasi,

pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, serta peran teknologi informasi dan komunikasi dalam mendukung penerapan keamanan informasi. Setiap elemen dinilai berdasarkan indikator yang menggambarkan tingkat implementasi kebijakan, prosedur, pengendalian, serta mekanisme evaluasi yang diterapkan oleh organisasi. Hasil penilaian tersebut memberikan gambaran mengenai tingkat kesiapan organisasi dalam menghadapi berbagai ancaman siber serta mendukung penyusunan strategi peningkatan keamanan informasi secara berkelanjutan.

Indeks KAMI versi 5.0 merupakan pengembangan terbaru yang telah diselaraskan dengan standar ISO/IEC 27001:2022 dan berbagai praktik terbaik keamanan siber internasional. Pembaruan ini mencakup penyempurnaan indikator penilaian, penyesuaian terhadap kontrol keamanan terbaru, serta peningkatan fokus pada pengelolaan risiko, ketahanan siber, dan keamanan layanan digital. Dengan penyelarasan tersebut, Indeks KAMI 5.0 mampu memberikan hasil evaluasi yang lebih komprehensif, akurat, dan relevan terhadap perkembangan teknologi informasi serta dinamika ancaman siber yang terus berkembang (Jelita et al., 2024).

ISO/IEC 27001:2022 dan NIST Cybersecurity Framework

ISO/IEC 27001:2022 merupakan standar internasional yang mengatur Sistem Manajemen Keamanan Informasi (*Information Security Management System* atau ISMS). Standar ini menyediakan kerangka kerja sistematis bagi organisasi dalam menetapkan, menerapkan, memelihara, mengevaluasi, dan meningkatkan sistem manajemen keamanan informasi secara berkelanjutan. Pembaruan dari versi 2013 menuju versi 2022 dilakukan untuk menyesuaikan perkembangan teknologi digital dan meningkatnya kompleksitas ancaman siber. Perubahan tersebut meliputi penyederhanaan struktur kontrol keamanan, penambahan kontrol baru, serta penyesuaian terhadap isu-isu strategis seperti keamanan komputasi awan (*cloud security*), perlindungan data, keamanan rantai pasok, dan ketahanan siber (*cyber resilience*) (Pratiwi & Wulandari, 2021).

Selain ISO/IEC 27001:2022, *NIST Cybersecurity Framework* (NIST CSF) merupakan kerangka kerja yang banyak digunakan sebagai acuan dalam pengelolaan keamanan siber. Kerangka kerja yang dikembangkan oleh *National Institute of Standards and Technology* (NIST) Amerika Serikat ini menyediakan pendekatan berbasis risiko melalui lima fungsi utama, yaitu *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*. Kelima fungsi tersebut membentuk siklus pengelolaan keamanan siber yang komprehensif, mulai dari identifikasi aset dan risiko, penerapan pengendalian, deteksi insiden, respons terhadap serangan, hingga pemulihan pasca-insiden.

Penerapan ISO/IEC 27001:2022 yang dikombinasikan dengan NIST CSF memberikan pendekatan yang saling melengkapi dalam membangun sistem keamanan informasi. ISO/IEC 27001 berfokus pada pembentukan sistem manajemen keamanan informasi yang terdokumentasi dan terstruktur, sedangkan NIST CSF memberikan panduan operasional dalam mengelola risiko siber secara dinamis. Integrasi kedua kerangka kerja tersebut mampu meningkatkan efektivitas pengelolaan keamanan informasi sekaligus memperkuat ketahanan organisasi dalam menghadapi ancaman siber (Ningrum & Riwanto, 2024).

Analisis Kesenjangan (Gap Analysis) Keamanan Informasi

Analisis kesenjangan (*gap analysis*) merupakan metode yang digunakan untuk mengidentifikasi perbedaan antara kondisi aktual (*as-is*) dengan kondisi yang diharapkan (*to-be*) berdasarkan standar, kebijakan, maupun praktik terbaik yang menjadi acuan. Dalam konteks keamanan informasi, metode ini berfungsi untuk mengevaluasi tingkat kesesuaian penerapan pengendalian keamanan yang telah dilakukan organisasi terhadap persyaratan standar internasional, sehingga dapat diketahui aspek-aspek yang masih memerlukan perbaikan (Bahri et al., 2024).

Proses *gap analysis* dilakukan melalui identifikasi kondisi eksisting, penentuan kondisi yang diharapkan, analisis tingkat kesenjangan, serta penyusunan rekomendasi perbaikan berdasarkan tingkat prioritas dan risiko. Pendekatan ini memungkinkan organisasi untuk mengalokasikan sumber daya secara lebih efektif dengan memprioritaskan pengendalian yang

memiliki dampak paling besar terhadap peningkatan keamanan informasi.

Dalam penelitian ini, *gap analysis* dilakukan menggunakan Indeks KAMI 5.0 sebagai instrumen utama untuk mengukur tingkat kematangan keamanan informasi pada instansi pemerintah. Hasil evaluasi kemudian dibandingkan dengan persyaratan ISO/IEC 27001:2022 dan praktik terbaik yang direkomendasikan oleh NIST Cybersecurity Framework. Pendekatan tersebut memungkinkan identifikasi kesenjangan dilakukan secara sistematis, objektif, dan terukur sehingga dapat menghasilkan rekomendasi yang dapat dipertanggungjawabkan secara akademis maupun menjadi dasar penyusunan strategi peningkatan keamanan informasi pada instansi pemerintah secara berkelanjutan.

III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif melalui studi literatur (*literature review*) dan analisis dokumen. Pendekatan ini dipilih untuk memperoleh pemahaman yang komprehensif mengenai tingkat kematangan keamanan informasi pada instansi pemerintah di Indonesia berdasarkan penerapan Indeks Keamanan Informasi (KAMI) versi 5.0. Data penelitian diperoleh dari berbagai sumber sekunder, meliputi jurnal ilmiah nasional maupun internasional, prosiding konferensi, buku, pedoman resmi Badan Siber dan Sandi Negara (BSSN), dokumen standar ISO/IEC 27001:2022, *NIST Cybersecurity Framework* (CSF), serta publikasi lain yang relevan dengan evaluasi keamanan informasi.

Tahapan penelitian terdiri atas tiga langkah utama. Tahap pertama adalah identifikasi dan pemetaan komponen penilaian pada Indeks KAMI 5.0 terhadap kontrol keamanan yang terdapat dalam ISO/IEC 27001:2022 serta fungsi-fungsi utama pada *NIST Cybersecurity Framework*, yaitu *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*. Tahap kedua adalah pengumpulan dan sintesis data dari berbagai penelitian terdahulu yang melaporkan hasil evaluasi penerapan Indeks KAMI pada instansi pemerintah di Indonesia. Tahap ketiga adalah pelaksanaan analisis kesenjangan (*gap analysis*) dengan membandingkan kondisi aktual yang tercermin dari hasil penilaian Indeks KAMI

terhadap tingkat kematangan yang direkomendasikan berdasarkan standar internasional. Analisis tersebut digunakan untuk mengidentifikasi area yang masih memerlukan peningkatan serta menyusun rekomendasi strategis guna memperkuat penerapan keamanan informasi.

Instrumen penelitian mengacu pada pedoman resmi Indeks KAMI versi 5.0 yang diterbitkan oleh BSSN. Instrumen ini digunakan untuk mengevaluasi tingkat kematangan keamanan informasi berdasarkan kategori sistem elektronik, yaitu Sistem Elektronik Strategis, Sistem Elektronik Tinggi, dan Sistem Elektronik Rendah. Penilaian dilakukan menggunakan rentang skor 0–645 poin yang dikelompokkan ke dalam empat tingkat kematangan, yaitu belum layak (0–320 poin), cukup baik (321–480 poin), baik (481–560 poin), dan sangat baik (561–645 poin). Hasil evaluasi tersebut selanjutnya dianalisis untuk mengidentifikasi kesenjangan antara kondisi eksisting dengan kondisi yang diharapkan berdasarkan ISO/IEC 27001:2022 dan *NIST Cybersecurity Framework*, sehingga diperoleh gambaran mengenai tingkat kesiapan keamanan informasi pada instansi pemerintah di Indonesia.

IV. HASIL DAN PEMBAHASAN

Pemetaan Indeks KAMI 5.0 terhadap Standar Internasional

Hasil analisis dokumen menunjukkan bahwa Indeks Keamanan Informasi (KAMI) versi 5.0 memiliki tingkat keselarasan yang tinggi dengan standar ISO/IEC 27001:2022 maupun *NIST Cybersecurity Framework* (CSF). Enam elemen utama dalam Indeks KAMI, yaitu tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, serta peran teknologi informasi dan komunikasi, dapat dipetakan ke dalam berbagai kontrol pada Annex A ISO/IEC 27001:2022. Pemetaan tersebut terutama mencakup kontrol organisasional (A.5), kontrol sumber daya manusia (A.6), kontrol fisik (A.7), dan kontrol teknologi (A.8), sehingga menunjukkan bahwa struktur penilaian KAMI telah mengadopsi prinsip-prinsip utama Sistem Manajemen Keamanan Informasi (SMKI) (Jelita et al., 2024).

Selain itu, hasil pemetaan terhadap *NIST Cybersecurity Framework* memperlihatkan bahwa sebagian besar indikator pada Indeks KAMI memiliki keterkaitan yang kuat dengan fungsi *Identify* dan *Protect*, terutama dalam aspek tata kelola, identifikasi aset, pengelolaan risiko, serta penerapan pengendalian keamanan. Meskipun demikian, masih terdapat beberapa aspek yang belum sepenuhnya terakomodasi, khususnya pada fungsi *Detect*, *Respond*, dan *Recover* yang berhubungan dengan kemampuan organisasi dalam mendeteksi insiden keamanan secara dini, melakukan respons terhadap serangan siber, serta memulihkan layanan setelah terjadinya insiden. Temuan tersebut menunjukkan bahwa Indeks KAMI 5.0 telah menjadi instrumen evaluasi yang relevan bagi instansi pemerintah, namun masih memerlukan penguatan pada aspek ketahanan siber operasional agar semakin selaras dengan praktik terbaik internasional (Ningrum & Riwanto, 2024).

Identifikasi Kesenjangan Penerapan Keamanan Informasi

Berdasarkan hasil sintesis berbagai penelitian mengenai implementasi Indeks KAMI pada instansi pemerintah, ditemukan beberapa kesenjangan utama dalam penerapan keamanan informasi. Pada aspek tata kelola, sebagian besar instansi telah memiliki kebijakan keamanan informasi, namun implementasi, dokumentasi, serta mekanisme evaluasinya belum dilakukan secara konsisten. Kondisi tersebut menyebabkan kebijakan yang telah disusun belum mampu menjadi pedoman operasional yang efektif dalam mendukung pengelolaan keamanan informasi.

Kesenjangan berikutnya ditemukan pada pengelolaan risiko keamanan informasi. Sebagian besar organisasi masih menerapkan pendekatan yang bersifat reaktif, yaitu melakukan tindakan setelah terjadi insiden keamanan, dibandingkan menerapkan pendekatan proaktif melalui identifikasi, analisis, dan mitigasi risiko secara berkala. Selain itu, pelaksanaan penilaian risiko belum menjadi bagian dari proses bisnis yang dilakukan secara berkesinambungan (Hasibuan, 2024).

Pada aspek kerangka kerja keamanan informasi, implementasi standar keamanan belum dilakukan secara merata di seluruh unit organisasi. Beberapa instansi telah mengadopsi ISO/IEC 27001 atau pedoman keamanan

lainnya, tetapi penerapannya masih terbatas pada unit tertentu sehingga belum membentuk sistem manajemen keamanan informasi yang terintegrasi. Sementara itu, pada aspek pengelolaan aset informasi masih ditemukan kendala dalam inventarisasi aset, klasifikasi informasi, serta penetapan tingkat sensitivitas data. Permasalahan tersebut umumnya terjadi pada instansi yang mengelola volume data dalam jumlah besar dan memiliki infrastruktur teknologi informasi yang kompleks (Maryanto et al., 2022).

Analisis Kesenjangan Berdasarkan ISO/IEC 27001:2022

Hasil perbandingan antara kondisi aktual instansi pemerintah dengan persyaratan ISO/IEC 27001:2022 menunjukkan bahwa kesenjangan masih ditemukan pada beberapa kelompok kontrol dalam Annex A. Kesenjangan terbesar berada pada kontrol organisasional (A.5), khususnya terkait penyusunan kebijakan keamanan informasi, pembagian peran dan tanggung jawab, pengelolaan risiko, serta tata kelola keamanan informasi yang belum diterapkan secara menyeluruh. Kondisi tersebut mengindikasikan bahwa aspek manajerial masih menjadi tantangan utama dalam implementasi Sistem Manajemen Keamanan Informasi.

Selain itu, kontrol teknologi (A.8) juga menunjukkan tingkat kesenjangan yang cukup tinggi. Beberapa organisasi belum menerapkan mekanisme kriptografi secara optimal, pengamanan jaringan belum dilakukan secara menyeluruh, serta pengujian keamanan aplikasi dan infrastruktur masih dilakukan secara terbatas. Di sisi lain, kemampuan organisasi dalam melakukan pemantauan keamanan secara berkelanjutan, deteksi dini terhadap ancaman siber, dan penanganan insiden juga masih memerlukan peningkatan agar selaras dengan perkembangan ancaman siber yang semakin kompleks (Jelita et al., 2024).

Temuan tersebut sejalan dengan penelitian Ningrum dan Riwanto (2024) yang menunjukkan bahwa organisasi dengan tingkat kematangan Indeks KAMI yang lebih tinggi cenderung memiliki tingkat kesesuaian yang lebih baik terhadap persyaratan ISO/IEC 27001:2022. Hal ini menunjukkan bahwa peningkatan nilai Indeks KAMI berkontribusi terhadap meningkatnya kualitas tata kelola keamanan informasi serta

kepatuhan organisasi terhadap standar internasional.

Implikasi dan Rekomendasi Strategis

Berdasarkan hasil analisis kesenjangan, terdapat beberapa rekomendasi strategis yang dapat diterapkan oleh instansi pemerintah untuk meningkatkan tingkat kematangan keamanan informasi. Pertama, penyusunan dan implementasi kebijakan keamanan informasi perlu diperkuat melalui dokumentasi yang lengkap, penetapan tanggung jawab yang jelas, serta evaluasi berkala terhadap efektivitas kebijakan yang telah diterapkan. Kedua, penerapan manajemen risiko keamanan informasi perlu dilakukan secara sistematis melalui identifikasi, analisis, evaluasi, dan mitigasi risiko yang dilaksanakan secara berkala sebagai bagian dari proses tata kelola organisasi (Pratiwi & Wulandari, 2021).

Ketiga, peningkatan kompetensi sumber daya manusia menjadi faktor yang sangat penting dalam mendukung implementasi keamanan informasi. Program pelatihan, sertifikasi

profesional, serta peningkatan kesadaran keamanan (*security awareness*) perlu dilaksanakan secara berkelanjutan agar seluruh pegawai memahami perannya dalam menjaga keamanan informasi organisasi. Keempat, evaluasi menggunakan Indeks KAMI 5.0 perlu dilakukan secara periodik sebagai instrumen pemantauan tingkat kematangan keamanan informasi sekaligus sebagai dasar penyusunan rencana peningkatan yang berkesinambungan.

Selain itu, instansi pemerintah perlu memperkuat kolaborasi dengan Badan Siber dan Sandi Negara (BSSN) maupun antarinstansi dalam berbagi informasi, pengalaman, dan praktik terbaik terkait pengelolaan keamanan siber. Sinergi tersebut diharapkan mampu meningkatkan kesiapsiagaan organisasi dalam menghadapi ancaman siber yang terus berkembang sekaligus mempercepat terwujudnya tata kelola keamanan informasi yang sesuai dengan standar ISO/IEC 27001:2022 dan *NIST Cybersecurity Framework* (Bahri et al., 2024).

Tabel 1. Ringkasan Hasil Analisis Kesenjangan Keamanan Informasi Berdasarkan Indeks KAMI 5.0

Aspek	Hasil Analisis	Standar Acuan	Implikasi/Rekomendasi
Pemetaan Indeks KAMI 5.0	Indeks KAMI 5.0 memiliki tingkat keselarasan yang tinggi dengan ISO/IEC 27001:2022 dan NIST CSF.	ISO/IEC 27001:2022 (Annex A.5–A.8), NIST CSF	KAMI 5.0 layak digunakan sebagai instrumen evaluasi keamanan informasi pada instansi pemerintah.
Kesesuaian dengan ISO/IEC 27001:2022	Enam elemen KAMI telah mengakomodasi kontrol organisasional, SDM, fisik, dan teknologi.	Annex A.5, A.6, A.7, A.8	Memudahkan organisasi dalam mengevaluasi penerapan Sistem Manajemen Keamanan Informasi (SMKI).
Kesesuaian dengan NIST CSF	KAMI telah mencakup fungsi <i>Identify</i> dan <i>Protect</i> , namun fungsi <i>Detect</i> , <i>Respond</i> , dan <i>Recover</i> masih belum optimal.	NIST CSF	Diperlukan penguatan kemampuan deteksi, respons insiden, dan pemulihan layanan.
Kesenjangan Tata Kelola	Kebijakan keamanan informasi telah tersedia, tetapi implementasi, dokumentasi, dan evaluasi belum konsisten.	ISO/IEC 27001:2022 A.5	Memperkuat tata kelola melalui kebijakan yang terdokumentasi dan evaluasi berkala.
Kesenjangan Manajemen Risiko	Penilaian risiko masih bersifat reaktif dan belum dilakukan secara berkelanjutan.	ISO/IEC 27001:2022, NIST Identify	Menerapkan manajemen risiko secara sistematis dan periodik.
Kesenjangan Kerangka Kerja	Implementasi standar keamanan belum merata di seluruh unit organisasi.	ISO/IEC 27001:2022	Mengintegrasikan penerapan SMKI pada seluruh unit kerja.
Kesenjangan Pengelolaan Aset	Inventarisasi aset, klasifikasi informasi, dan penetapan sensitivitas data masih lemah.	ISO/IEC 27001:2022 A.5 & A.8	Menyusun inventaris aset dan klasifikasi informasi secara menyeluruh.
Kesenjangan Kontrol Teknologi	Kriptografi, keamanan jaringan, pengujian keamanan, pemantauan, dan deteksi ancaman belum optimal.	ISO/IEC 27001:2022 A.8	Meningkatkan kontrol teknis, pemantauan keamanan, dan respons insiden.
Rekomendasi Strategis	Penguatan kebijakan, manajemen risiko, peningkatan kompetensi SDM, evaluasi berkala menggunakan KAMI 5.0, serta kolaborasi dengan BSSN.	ISO/IEC 27001:2022, NIST CSF	Meningkatkan tingkat kematangan keamanan informasi dan ketahanan siber instansi pemerintah.

Berdasarkan Tabel 1, hasil analisis menunjukkan bahwa Indeks KAMI 5.0 memiliki tingkat keselarasan yang tinggi dengan standar ISO/IEC 27001:2022 dan *NIST Cybersecurity Framework* (CSF), sehingga dapat digunakan sebagai instrumen evaluasi keamanan informasi pada instansi pemerintah. Meskipun demikian, masih ditemukan beberapa kesenjangan pada aspek tata kelola, pengelolaan risiko, implementasi kerangka kerja keamanan informasi, pengelolaan aset informasi, serta kontrol teknologi. Kesenjangan tersebut menunjukkan bahwa sebagian besar instansi

belum menerapkan kebijakan keamanan secara konsisten, penilaian risiko masih bersifat reaktif, dan pengendalian teknis seperti kriptografi, keamanan jaringan, serta pemantauan keamanan belum berjalan secara optimal. Oleh karena itu, diperlukan penguatan tata kelola, penerapan manajemen risiko yang berkelanjutan, peningkatan kompetensi sumber daya manusia, pelaksanaan evaluasi berkala menggunakan Indeks KAMI 5.0, serta kolaborasi yang lebih erat dengan Badan Siber dan Sandi Negara (BSSN) guna meningkatkan tingkat kematangan keamanan informasi.

Tabel 2. Pemetaan Indeks KAMI 5.0 terhadap Standar Internasional

Elemen Indeks KAMI 5.0	ISO/IEC 27001:2022	NIST CSF	Status Kesesuaian
Tata Kelola Keamanan Informasi	A.5 Kontrol Organisasional	Identify	Tinggi
Pengelolaan Risiko Keamanan Informasi	A.5 Kontrol Organisasional	Identify	Tinggi
Kerangka Kerja Keamanan Informasi	A.5 dan A.6	Identify, Protect	Tinggi
Pengelolaan Aset Informasi	A.5 dan A.8	Identify, Protect	Tinggi
Teknologi dan Keamanan Informasi	A.8 Kontrol Teknologi	Protect	Tinggi
Peran Teknologi Informasi dan Komunikasi	A.6, A.7, A.8	Protect	Tinggi
Deteksi Insiden	Sebagian A.8	Detect	Sedang
Respons dan Pemulihan Insiden	Sebagian A.8	Respond, Recover	Rendah–Sedang

Berdasarkan Tabel 2, enam elemen utama dalam Indeks KAMI 5.0 memiliki tingkat kesesuaian yang tinggi dengan kontrol pada ISO/IEC 27001:2022, khususnya Annex A.5 hingga Annex A.8, serta fungsi *Identify* dan *Protect* pada *NIST Cybersecurity Framework*. Hal ini menunjukkan bahwa struktur penilaian Indeks KAMI telah mengakomodasi sebagian besar prinsip Sistem Manajemen Keamanan Informasi. Namun demikian, tingkat kesesuaian pada fungsi *Detect*, *Respond*, dan *Recover* masih berada pada kategori sedang hingga rendah. Kondisi tersebut mengindikasikan bahwa kemampuan organisasi dalam mendeteksi ancaman, merespons insiden keamanan siber, serta melakukan pemulihan layanan masih perlu ditingkatkan agar implementasi keamanan informasi semakin selaras dengan praktik terbaik internasional.

V. PENUTUP

A. Kesimpulan

Penelitian ini berhasil mengidentifikasi dan menganalisis kesenjangan penerapan keamanan informasi pada instansi pemerintah di Indonesia berdasarkan Indeks Keamanan Informasi (KAMI) versi 5.0 yang dibandingkan

dengan standar ISO/IEC 27001:2022 dan *NIST Cybersecurity Framework* (CSF). Hasil analisis menunjukkan bahwa sebagian besar instansi pemerintah masih berada pada tingkat kematangan dasar, sehingga implementasi keamanan informasi belum sepenuhnya memenuhi praktik terbaik yang direkomendasikan oleh standar internasional. Kesenjangan utama ditemukan pada aspek tata kelola keamanan informasi, pengelolaan risiko, penerapan pengendalian keamanan, serta kemampuan organisasi dalam melakukan deteksi dan respons terhadap insiden siber.

Hasil penelitian juga menunjukkan bahwa Indeks KAMI 5.0 memiliki tingkat keselarasan yang tinggi dengan ISO/IEC 27001:2022 dan sebagian besar fungsi dalam *NIST Cybersecurity Framework*. Meskipun demikian, beberapa aspek pada fungsi *Detect*, *Respond*, dan *Recover* masih memerlukan penyempurnaan agar mampu mengakomodasi kebutuhan pengelolaan keamanan siber yang semakin dinamis. Dengan demikian, Indeks KAMI 5.0 dapat digunakan sebagai instrumen evaluasi yang efektif untuk mengukur tingkat kematangan keamanan informasi sekaligus sebagai dasar dalam

menyusun strategi peningkatan keamanan informasi pada instansi pemerintah.

Berdasarkan temuan tersebut, penelitian ini merekomendasikan penguatan tata kelola keamanan informasi, penerapan manajemen risiko secara berkelanjutan, peningkatan kompetensi sumber daya manusia, serta pelaksanaan evaluasi keamanan informasi secara berkala menggunakan Indeks KAMI 5.0. Langkah-langkah tersebut diharapkan mampu meningkatkan kepatuhan terhadap standar internasional, memperkuat ketahanan siber, serta mendukung terwujudnya penyelenggaraan sistem elektronik pemerintah yang aman, andal, dan berkelanjutan. Penelitian selanjutnya

B.Saran

Disarankan untuk melakukan studi empiris dengan cakupan instansi yang lebih luas, menggunakan data primer, serta mengombinasikan pendekatan kualitatif dan kuantitatif agar diperoleh hasil yang lebih komprehensif dan memiliki tingkat generalisasi yang lebih tinggi.

DAFTAR PUSTAKA

- [1]. Bahri, S., Wijayanti, Y., Dewantara, R., & Hidayat, A. T. (2024). Evaluasi sistem keamanan teknologi informasi menggunakan Indeks KAMI dan COBIT 5 di Pondok Pesantren. *Jurnal Janitra Informatika dan Sistem Informasi*, 4(2), 119–129.
<https://doi.org/10.59395/janitra.v4i2.207>
- [2] Hasibuan, M. S. (2024). Analisis tingkat kematangan keamanan informasi menggunakan Indeks KAMI pada Tiyuh Pulung Kencana. *Journal of Digital Literacy and Volunteering*, 2(1), 31–37.
<https://doi.org/10.57119/litdig.v2i1.78>
- [3] Jelita, R., et al. (2024). *Evaluasi keamanan teknologi informasi menggunakan Indeks Keamanan Informasi 5.0 dan ISO/IEC 27001:2022*. Jurnal Ilmiah.
- [4] Maryanto, A. L., Azam, M. N. A., & Nugroho, A. (2022). Evaluasi manajemen keamanan informasi pada perusahaan pemula berbasis teknologi menggunakan Indeks KAMI. *SimanteC*, 11(1), 1–12.
- [5] Ningrum, F. A. S., & Riwanto, Y. (2024). Analisis keamanan sistem informasi perguruan tinggi berbasis Indeks KAMI. *JIP (Jurnal Informatika Polinema)*, 10(4), 437–446.
- [6] Pratiwi, H. A., & Wulandari, L. (2021). Evaluasi tingkat kesiapan keamanan informasi menggunakan Indeks Keamanan Informasi (Indeks KAMI) versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor. *Journal of Industrial Engineering & Management Research*, 2(5), 146–158.
- [7] Yuliani, S. Y., Ramadhini, N. T., Gustisyaf, A. I., & Wahyudin, A. (2020). Asesmen keamanan informasi menggunakan Indeks KAMI. *NARATIF (Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika)*.