TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

Model Konseptual Penguatan Instrumen Penilaian Kematangan Keamanan Siber (IKAS) menggunakan Pendekatan Sosioteknis melalui Pemetaan Keselarasan terhadap NIST CSF 2.0 dan ISO/IEC 27001:2022

Muhammad Arif Ali Wasi[*], Agung Budi Susanto, Winarni

Program Studi Magister Teknik Informatika, Program Pascasarjana, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1,*]aliwasiarif@gmail.com, [2]dosen02680@unpam.ac.id, [3]wina005@brin.go.id
Email Penulis Korespondensi: aliwasiarif@gmail.com

Abstrak–Instrumen Penilaian Kematangan Keamanan Siber (IKAS) menjadi dasar penyusunan peta jalan pelindungan Infrastruktur Informasi Vital di Indonesia, sehingga setiap kelemahan rancangannya merambat langsung pada arah kebijakan nasional. Meskipun demikian, keselarasan IKAS terhadap kerangka kerja internasional sekaligus keseimbangan komposisi sosioteknisnya belum pernah dikaji secara akademis. Penelitian ini memetakan keselarasan IKAS versi 1.2.1 terhadap NIST CSF 2.0 dan ISO/IEC 27001:2022 secara dua arah, mendiagnosis kesenjangannya melalui *Leavitt's Diamond*, serta merancang model konseptual penguatan bernama IKAS-ST. Metode kualitatif deskriptif berbasis analisis isi diterapkan pada 181 butir kontrol penilaian IKAS, 106 subkategori NIST CSF 2.0, dan 93 kontrol *Annex A* ISO/IEC 27001:2022. Hasilnya, IKAS terbukti selaras secara substansial dengan indeks cakupan maju rata-rata 81,2% berkategori *Largely Achieved*, namun menyisakan 12 titik buta yang terkonsentrasi pada fungsi tata kelola dan pemulihan. Temuan yang paling menentukan adalah ruang lingkup Tugas sebagai satu-satunya dimensi yang kurang terwakili, dengan defisit ekstrem pada Domain Deteksi yang butirnya mengukur kepemilikan teknologi deteksi dan bukan prosedur yang menjalankannya. Keunggulan IKAS-ST tidak terletak pada bertambahnya jumlah butir, melainkan pada tiga sifat yang dapat diuji, yaitu setiap butir tambahan tertelusur pada titik buta yang teridentifikasi sehingga tidak ada penambahan spekulatif, restrukturisasi ruang lingkup menyentuh akar kesenjangan berupa ketiadaan dimensi prosedural yang eksplisit, serta seluruh 181 butir asli dipertahankan sehingga keterbandingan hasil penilaian historis tetap terjaga. Model ini bersifat konseptual dan menunggu validasi pakar serta uji coba lapangan.

Kata Kunci: Analisis Kesenjangan; ISO/IEC 27001:2022; Kematangan Keamanan Siber; *Leavitt's Diamond*; NIST CSF 2.0; Sosioteknis

Abstract–The Cybersecurity Maturity Assessment Instrument (IKAS) underpins the protection roadmap of Vital Information Infrastructure in Indonesia, so any weakness in its design propagates directly into national policy. Its alignment with international frameworks and the balance of its sociotechnical composition, however, have never been examined academically. This study maps the alignment of IKAS version 1.2.1 against NIST CSF 2.0 and ISO/IEC 27001:2022 bidirectionally, diagnoses the gaps through Leavitt's Diamond, and designs a conceptual strengthening model named IKAS-ST. A descriptive qualitative content analysis was applied to 181 IKAS items, 106 NIST CSF 2.0 subcategories, and 93 ISO/IEC 27001:2022 Annex A controls. The instrument proves substantially aligned, with an average forward coverage of 81.2% (Largely Achieved), yet 12 white spots remain, concentrated in the governance and recovery functions. The decisive finding is that Task is the only under-represented scope, with an extreme deficit in the Detection domain where items measure the ownership of detection technology rather than the procedures that operate it. The merit of IKAS-ST lies not in adding items but in three testable properties: every added item is traceable to an identified white spot, so no addition is speculative; the restructuring addresses the root cause, namely the absence of an explicit procedural scope; and all 181 original items are retained, preserving the comparability of historical assessment results. The model is conceptual and awaits expert validation and field testing.

Keywords: Cybersecurity Maturity; Gap Analysis; ISO/IEC 27001:2022; Leavitt's Diamond; NIST CSF 2.0; Sociotechnical

1. PENDAHULUAN

Percepatan adopsi teknologi digital memperluas permukaan serangan siber seiring bertambahnya data dan sistem yang saling terhubung (*United Nations Conference on Trade and Development*, 2021). Di Indonesia, konsekuensi perluasan tersebut terekam pada lanskap keamanan siber nasional tahun 2025 yang mencatat 5.515.394.886 anomali trafik, dengan sektor Administrasi Pemerintahan sebagai sasaran paling terdampak melalui 2.013 dari 2.855 notifikasi indikasi insiden (Badan Siber dan Sandi Negara, 2026). Konsentrasi insiden pada sektor pemerintahan tersebut justru berlangsung ketika penyelenggara Infrastruktur Informasi Vital telah memiliki instrumen pengukuran kematangan nasional, sehingga persoalannya tidak terletak pada ketiadaan alat ukur melainkan pada kemampuan alat ukur menangkap dimensi yang benar-benar menentukan ketahanan. Instrumen yang menilai keberadaan kontrol tanpa menguji keterlaksanaan prosedurnya berpotensi menghasilkan skor kematangan tinggi yang tidak sebanding dengan ketahanan operasional, dan celah itulah yang diuji pada penelitian ini.

Kerangka regulasi pelindungan Infrastruktur Informasi Vital (IIV) di Indonesia bertumpu pada Peraturan Presiden Nomor 82 Tahun 2022 (Presiden Republik Indonesia, 2022) yang diturunkan melalui Peraturan BSSN Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan IIV (Badan Siber dan Sandi Negara, 2023) serta Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber (Badan Siber dan Sandi Negara, 2023). Instrumen Penilaian Kematangan Keamanan Siber (IKAS) merupakan instrumen operasional dari kerangka kerja tersebut. IKAS versi 1.2.1 memuat 181 butir kontrol penilaian yang terdistribusi pada empat domain, yaitu Identifikasi, Proteksi, Deteksi, serta Penanggulangan dan Pemulihan, terbagi ke dalam 18 kategori dan 90 subkategori, dengan tiga

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

ruang lingkup operasional berupa sumber daya manusia (SDM), teknologi, dan tata kelola. Hasil pengukuran IKAS menjadi dasar penyusunan peta jalan pelindungan IIV pada setiap sektor, sehingga mutu instrumen berdampak langsung pada arah kebijakan pelindungan nasional.

Pada tataran internasional, NIST *Cybersecurity Framework* (CSF) 2.0 dan ISO/IEC 27001:2022 merupakan dua rujukan yang paling luas digunakan. NIST CSF 2.0 mengorganisasikan 106 subkategori luaran keamanan siber ke dalam enam fungsi dan menempatkan fungsi *Govern* sebagai fungsi baru yang menaungi strategi, kebijakan, peran, serta pengawasan organisasi (NIST, 2024). ISO/IEC 27001:2022 menetapkan persyaratan sistem manajemen keamanan informasi yang dilengkapi 93 kontrol *Annex A* pada empat tema, yaitu *organizational*, *people*, *physical*, dan *technological* (*International Organization for Standardization & International Electrotechnical Commission*, 2022). Kehadiran fungsi *Govern* menjadikan NIST CSF 2.0 relevan untuk menguji kedalaman ruang lingkup tata kelola pada IKAS, sedangkan struktur *Annex A* relevan untuk menguji kelengkapan katalog kontrol.

Pendekatan yang bertumpu pada teknologi semata tidak memadai untuk menjamin ketahanan siber. Teori sosioteknis yang berakar pada Teori Sistem Sosioteknis klasik (Trist & Bamforth, 1951) menyatakan bahwa kinerja organisasi ditentukan oleh keselarasan antarkomponen, bukan oleh keunggulan satu komponen. Model *Leavitt's Diamond* memformulasikan keterkaitan tersebut ke dalam empat komponen yang saling bergantung, yaitu manusia, teknologi, struktur, dan tugas, sehingga perubahan atau kelemahan pada satu komponen niscaya merambat ke komponen lain (Leavitt, 1965). Pada ranah keamanan siber, tinjauan atas pemodelan keamanan sosioteknis pada infrastruktur industri kritis (Ani et al., 2022), kerangka sosioteknis untuk sektor kesehatan (Ewoh et al., 2025), serta model kematangan sosioteknis untuk kebijakan perangkat pribadi di rumah sakit (Wani et al., 2025) menunjukkan bahwa lensa sosioteknis telah diterima sebagai alat diagnosis, meskipun umumnya diterapkan pada organisasi, bukan pada instrumen penilaiannya.

Penelitian terdahulu di Indonesia sebagian besar mengevaluasi organisasi menggunakan Indeks KAMI dan menyandingkannya dengan standar internasional (Supriyanto et al., 2025; Apriany & Wibowo, 2024; Jelita et al., 2024; Wibawa et al., 2024). Pengembangan instrumen kematangan bagi instansi pemerintah juga telah dirintis, namun menyasar objek regulasi yang berbeda dari Infrastruktur Informasi Vital, yaitu Sistem Pemerintahan Berbasis Elektronik (Hardiana & Suhardi, 2025) dan kerangka penilaian kematangan berbasis NIST CSF v1.1 dan CIS Controls v8 (Irawan et al., 2024) serta penyesuaian model ketahanan siber usaha mikro, kecil, dan menengah terhadap NIST CSF (Balafif, 2023).

Literatur internasional termutakhir memperkuat argumen kesenjangan tersebut dari dua sisi. Pada sisi metodologis, kajian kematangan mutakhir bergerak dari sekadar memetakan keberadaan kontrol menuju pengujian kemampuan organisasi menjalankannya, sebagaimana ditunjukkan kerangka evaluasi berbasis NIST CSF yang mengalibrasi bobot butir melalui penilaian pakar (Bernardo et al., 2025) serta tinjauan sistematis yang menemukan bahwa adopsi kerangka kerja tidak berbanding lurus dengan efektivitas perlindungan karena hambatan justru muncul pada tataran penerapan (Salas-Riega et al., 2025). Pada sisi teoretis, penelitian terhadap pemerintah daerah menegaskan bahwa kerangka kerja seperti NIST CSF dan ISO/IEC 27001 baru menjadi kapabilitas nyata apabila ditopang keselarasan antara teknologi, manusia, dan struktur organisasi (Vestad & Yang, 2025), sedangkan model kematangan untuk perguruan tinggi memperlihatkan perlunya penyesuaian struktur instrumen terhadap konteks penggunanya (Salam et al., 2025). Kedua arah temuan tersebut menyiratkan bahwa evaluasi terhadap sebuah instrumen penilaian perlu menyasar komposisi dimensinya dan bukan semata kelengkapan daftar kontrolnya, dan justru pada titik inilah IKAS belum pernah diperiksa.

Sintesis atas kajian tersebut memperlihatkan tiga keterbatasan yang belum terjawab. Pertama, objek evaluasi masih terpusat pada Indeks KAMI atau pada organisasi pengguna, sedangkan IKAS versi 1.2.1 sebagai instrumen resmi bagi penyelenggara IIV belum pernah diuji keselarasannya secara sistematis. Kedua, keselarasan lazim diukur satu arah, yaitu sejauh mana butir instrumen memiliki padanan pada kerangka kerja acuan, sehingga elemen kerangka kerja internasional yang sama sekali tidak tertangkap instrumen tidak pernah terungkap. Ketiga, keseimbangan sosioteknis instrumen itu sendiri belum pernah dibongkar, padahal ketimpangan komposisi butir berpotensi mengarahkan organisasi pada capaian kematangan yang tampak tinggi tetapi timpang secara struktural.

Kebaruan penelitian ini terletak pada tiga hal yang menjawab keterbatasan tersebut. Pertama, keselarasan diukur dua arah pada tingkat butir penilaian melalui indeks cakupan maju (*Forward Coverage Index*, FCI) dan indeks cakupan balik (*Reverse Coverage Index*, RCI). Kedua arah tersebut memisahkan dua sifat yang selama ini bercampur, yaitu kesesuaian isi instrumen terhadap praktik internasional yang diukur FCI, dan kelengkapan cakupannya terhadap kedua kerangka kerja yang diukur RCI. Kedua, *Leavitt's Diamond* diposisikan sebagai lensa evaluatif terhadap komposisi instrumen kebijakan, bukan terhadap organisasi, sehingga ketimpangan terdeteksi pada tingkat rancangan alat ukur. Ketiga, hasil kedua analisis tersebut dikonversi menjadi model konseptual IKAS Sosioteknis (IKAS-ST) yang bersifat augmentatif dan seluruh penambahannya tertelusur pada titik buta yang teridentifikasi. Sejalan dengan itu, penelitian ini bertujuan memetakan keselarasan IKAS versi 1.2.1 terhadap NIST CSF 2.0 dan ISO/IEC 27001:2022, mengidentifikasi kesenjangan sosioteknis IKAS melalui *Leavitt's Diamond*, serta merumuskan model konseptual penguatan IKAS yang mengintegrasikan aspek sosioteknis. Kontribusi yang dihasilkan berupa bukti keselarasan dua arah pada tingkat butir, diagnosis ketimpangan sosioteknis instrumen kebijakan, dan rancangan penguatan yang siap dipertimbangkan pada siklus pemutakhiran instrumen berikutnya.

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

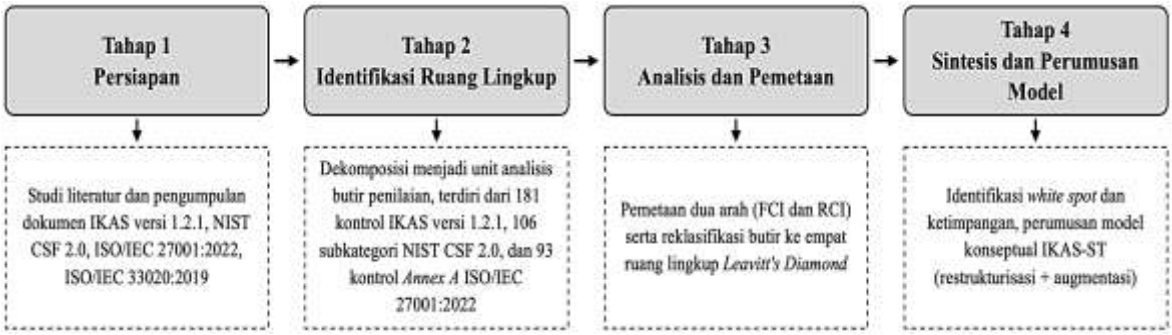
Penelitian ini menggunakan metode kualitatif deskriptif dengan desain studi komparatif dan evaluatif terhadap dokumen, yang dioperasionalkan melalui teknik analisis kesenjangan (*gap analysis*). Teknik pembedahan dokumen yang digunakan adalah analisis isi kualitatif, yaitu prosedur sistematis untuk mereduksi teks menjadi kategori yang dapat direplikasi (Elo & Kyngäs, 2008; Krippendorff, 2018). Kuantifikasi sederhana berupa persentase cakupan dimanfaatkan semata-mata sebagai instrumen deskriptif untuk memvisualisasikan magnitudo kesenjangan, bukan sebagai dasar inferensi statistik atau uji hipotesis, sehingga penelitian ini tidak mengajukan hipotesis dan tidak melibatkan responden.

Data yang digunakan seluruhnya bersifat sekunder dan dipilih melalui *purposive sampling* berdasarkan relevansi langsung terhadap tujuan penelitian. Sumber data utama terdiri atas dokumen resmi IKAS versi 1.2.1 beserta panduan pengisiannya (Badan Siber dan Sandi Negara, 2023), dokumen NIST CSF 2.0 (NIST, 2024), dan dokumen ISO/IEC 27001:2022 (*International Organization for Standardization & International Electrotechnical Commission*, 2022). Unit analisis terkecil adalah butir penilaian, yaitu 181 butir kontrol penilaian IKAS versi 1.2.1, 106 subkategori NIST CSF 2.0, dan 93 kontrol *Annex A* ISO/IEC 27001:2022. Unit penilaian keselarasan adalah pasangan selaras, yaitu relasi antara satu butir IKAS dengan satu butir penilaian kerangka kerja internasional.

Kerangka pemikiran penelitian bertumpu pada premis bahwa mutu instrumen penilaian ditentukan oleh dua sifat yang berbeda, yaitu keselarasan substantif terhadap praktik yang diakui secara internasional dan keseimbangan komposisi antarkomponen sosioteknis. Sifat pertama diuji melalui pemetaan dua arah terhadap NIST CSF 2.0 dan ISO/IEC 27001:2022, sedangkan sifat kedua diuji melalui reklasifikasi seluruh butir ke empat komponen *Leavitt's Diamond*. Kedua hasil pengujian kemudian disintesiskan menjadi rancangan penguatan, sehingga alur berpikir penelitian bergerak dari diagnosis keselarasan, ke diagnosis keseimbangan, lalu ke perumusan model.

2.2 Tahapan Penelitian

Penelitian dilaksanakan melalui empat tahapan utama yang berurutan sebagaimana disajikan pada Gambar 1. Tahap pertama adalah persiapan, berupa studi literatur dan pengumpulan dokumen regulasi IKAS, kerangka kerja NIST CSF 2.0 dan ISO/IEC 27001:2022, model *Leavitt's Diamond*, serta skema *rating Not, Partially, Largely, Fully Achieved* (NPLF) berbasis ISO/IEC 33020:2019 (*International Organization for Standardization & International Electrotechnical Commission*, 2019). Tahap kedua adalah identifikasi ruang lingkup, yaitu dekomposisi setiap dokumen menjadi unit analisis terkecil berupa butir penilaian sehingga ketiga dokumen berada pada granularitas yang setara dan layak dibandingkan. Tahap ketiga adalah analisis dan pemetaan, yang mencakup pemetaan silang setiap butir IKAS versi 1.2.1 terhadap subkategori NIST CSF 2.0 dan kontrol *Annex A* ISO/IEC 27001:2022, perhitungan indeks keselarasan dua arah, serta pelabelan ruang lingkup sosioteknis pada setiap butir dari ketiga dokumen. Tahap keempat adalah sintesis dan perumusan model, yaitu penerjemahan titik buta dan ketimpangan proporsi menjadi intervensi rancangan yang membentuk model konseptual IKAS-ST. Keluaran setiap tahap menjadi masukan tahap berikutnya sehingga seluruh unsur model usulan dapat ditelusuri kembali ke temuan empiris pada tahap sebelumnya.



Gambar 1. Tahapan Penelitian Analisis Keselarasan dan Penguatan IKAS versi 1.2.1

2.3 Klausul Penetapan Keselarasan

Penetapan keselarasan tidak dilakukan secara intuitif, melainkan melalui klausul penilaian agar hasil pemetaan dapat dipertanggungjawabkan dan direplikasi. Setiap pasangan dinilai pada tiga dimensi yang dinilai secara berurutan. Dimensi pertama adalah kesetaraan makna, yaitu kesamaan sasaran kontrol yang mencakup objek yang dilindungi, ancaman yang dimitigasi, dan hasil yang diharapkan, dengan penilaian berbasis kesamaan maksud dan bukan kemiripan istilah. Dimensi kedua adalah tumpang-tindih cakupan, yang mengenali tiga pola relasi, yaitu ekuivalen (1:1) ketika cakupan kedua kontrol setara, komposit (1:n) ketika satu butir IKAS mencakup beberapa butir kerangka kerja internasional, dan parsial (n:1) ketika beberapa butir IKAS bersama-sama memetakan satu butir kerangka kerja yang lebih luas. Dimensi ketiga adalah kesamaan maksud pengendalian dalam siklus keamanan, yaitu preventif, detektif, korektif, atau direktif. Status keselarasan setiap butir kemudian disimpulkan sebagaimana Tabel 1.

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

Tabel 1. Klausul Penetapan Status Keselarasan Butir IKAS

Status	Kriteria Penetapan
Fully Aligned	Butir IKAS memiliki keselarasan pada kedua kerangka kerja internasional, minimal satu subkategori NIST CSF 2.0 dan minimal satu kontrol *Annex A* ISO/IEC 27001:2022.
Partially Aligned	Butir IKAS memiliki keselarasan hanya pada salah satu kerangka kerja internasional, yaitu NIST CSF 2.0 saja atau ISO/IEC 27001:2022 saja.
Not Aligned	Butir IKAS tidak memiliki keselarasan pada kedua kerangka kerja, sehingga diinterpretasikan sebagai kontrol khas regulasi nasional.

Tiga prinsip diterapkan untuk menekan subjektivitas penetapan padanan, sejalan dengan protokol penilaian keselarasan yang digunakan. Pertama, ketiga dimensi tersebut dipertimbangkan secara bersama pada setiap pasangan dan tidak satu pun diperlakukan sebagai penentu tunggal, sehingga keputusan akhir mempertimbangkan kesetaraan makna, tumpang-tindih cakupan, dan kesamaan maksud pengendalian sekaligus. Kedua, setiap penetapan padanan harus dapat ditelusuri ke rumusan kontrol pada dokumen sumber, yaitu Lampiran Peraturan BSSN Nomor 8 Tahun 2023 untuk IKAS, teks resmi NIST CSF 2.0, dan ISO/IEC 27001:2022, sehingga klaim keselarasan tidak dapat ditegakkan hanya atas dasar kemiripan tema. Ketiga, apabila keselarasan suatu pasangan diragukan dan tidak memenuhi ambang minimal, pasangan tersebut tidak dipetakan untuk menjaga validitas hasil, bukan dipaksakan. Penerapan klausul penilaian keselarasan pada seluruh 181 butir IKAS beserta matriks pemetaan lengkap dan rincian 12 titik buta tersedia secara terbuka pada tautan *https://drive.google.com/file/d/1T5HYJsY3VQ2iIM0Yc0ryjoBTi8uqp0xL/view?usp=drive_link* berupa tabel Penerapan Klausul Penilaian Keselarasan pada 181 butir kontrol IKAS, serta Matriks Pemetaan IKAS disampaikan pada tautan *https://docs.google.com/spreadsheets/d/1jpoEROjzvkXBQuFif33tbPwysbbjZAG_/edit?usp=sharing*. Dokumentasi ini menekan subjektivitas tetapi tidak meniadakannya, sehingga uji kesepakatan antarpenilai yang melibatkan pengode kedua serta penilaian panel pakar tetap diposisikan sebagai agenda penelitian lanjutan sebagaimana disampaikan pada bagian keterbatasan.

2.4 Indeks Cakupan Maju dan Cakupan Balik

Keselarasan diukur pada dua arah yang objek ukurnya berbeda dan tidak dapat dipertukarkan. Cakupan maju menjadikan 181 butir IKAS sebagai acuan dan mengukur proporsi butir yang berhasil dipetakan ke kerangka kerja internasional, sehingga menggambarkan konvergensi instrumen. Cakupan balik membalik sudut pandang dengan menjadikan butir penilaian kerangka kerja internasional sebagai acuan dan mengukur proporsi butir yang berhasil ditangkap IKAS, sehingga menggambarkan kelengkapan instrumen dan sekaligus mendeteksi titik buta. Kedua indeks diformulasikan pada persamaan (1) dan (2), sedangkan indeks rata-rata dinyatakan pada persamaan (3).

$$FCI_{*k*} = (n_{\text{selaras,k}} / N_{\text{IKAS}}) \times 100\% \quad (1)$$

$$RCI_{*k*} = (m_{\text{tertangkap,k}} / M_{*k*}) \times 100\% \quad (2)$$

$$FCI_{\text{rata-rata}} = (FCI_{\text{NIST}} + FCI_{\text{ISO}}) / 2 \quad (3)$$

Notasi k menyatakan kerangka kerja acuan, $n_{\text{selaras,k}}$ menyatakan jumlah butir IKAS yang selaras terhadap kerangka k, N_{IKAS} menyatakan total butir IKAS, $m_{\text{tertangkap,k}}$ menyatakan jumlah butir penilaian kerangka k yang tertangkap IKAS, dan M_{k} menyatakan total butir penilaian kerangka k. Nilai kedua indeks diinterpretasikan menggunakan skala *rating* NPLF dari ISO/IEC 33020:2019 *(International Organization for Standardization & International Electrotechnical Commission*, 2019) sebagaimana Tabel 2. Skema *Rating* NPLF Berdasarkan ISO/IEC 33020:2019. Skala NPLF digunakan secara utuh berikut ambang aslinya, tetapi hanya diterapkan pada objek ukur yang sesuai, yaitu interpretasi indeks agregat berbasis persentase, sedangkan klasifikasi status keselarasan pada Tabel 1. Klausul Penetapan Status Keselarasan Butir IKAS tetap bersifat nominal.

Tabel 2. Skema *Rating* NPLF Berdasarkan ISO/IEC 33020:2019

Rating	Label	Rentang	Interpretasi Kematangan
N	*Not Achieved*	0%–15%	Sedikit atau tidak ada bukti pencapaian
P	*Partially Achieved*	>15%–50%	Ada pendekatan dan sebagian pencapaian, belum sistematis
L	*Largely Achieved*	>50%–85%	Pendekatan sistematis, pencapaian signifikan dengan kelemahan minor
F	*Fully Achieved*	>85%–100%	Pendekatan sistematis dengan pencapaian penuh

2.5 Klasifikasi Sosioteknis dan Indeks Kesenjangan

Seluruh butir penilaian pada ketiga dokumen direklasifikasi ke empat ruang lingkup *Leavitt's Diamond* melalui analisis kata kunci operasional dan tujuan akhir kontrol. Ruang lingkup SDM mencakup kontrol yang berfokus pada kompetensi, kesadaran, budaya keamanan, pelatihan, dan kedisiplinan personel. Ruang lingkup Teknologi mencakup kontrol yang mensyaratkan perangkat keras, perangkat lunak, sistem kriptografi, arsitektur jaringan, atau solusi teknis lain. Ruang lingkup Struktur mencakup kontrol yang mengatur penetapan wewenang, pengorganisasian unit kerja, hierarki pelaporan, kebijakan formal pimpinan, dan mekanisme pengawasan strategis. Ruang lingkup Tugas mencakup

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

kontrol yang memuat instruksi operasional, prosedur baku, alur kerja fungsional, dan eksekusi proses bisnis keamanan siber. Klasifikasi bersifat multi ruang lingkup sehingga satu butir dapat menerima lebih dari satu penandaan, dan persentase dihitung terhadap jumlah butir, bukan terhadap jumlah penandaan. Kesenjangan setiap ruang lingkup dihitung melalui persamaan (4).

$$Gap_{*s*} = IKAS\%_{*s*} - (NIST\%_{*s*} + ISO\%_{*s*}) / 2 \quad (4)$$

Notasi *s* menyatakan ruang lingkup sosioteknis. Nilai positif menunjukkan representasi IKAS setara atau lebih tinggi daripada rata-rata kerangka kerja internasional, sedangkan nilai negatif menunjukkan kondisi *underrepresented*. Perhitungan yang sama diterapkan pada tingkat domain dengan menyandingkan pasangan domain IKAS dan fungsi NIST CSF 2.0 yang paralel, yaitu fungsi *Govern* dan *Identify* terhadap Domain Identifikasi, *Protect* terhadap Domain Proteksi, *Detect* terhadap Domain Deteksi, serta *Respond* dan *Recover* terhadap Domain Penanggulangan dan Pemulihan.

Pemilihan *Leavitt's Diamond* sebagai alat diagnosis tidak semata didasarkan pada kemudahan pelabelan, melainkan pada tiga sifat model yang sesuai dengan objek penelitian. Pertama, model ini bersifat konfiguratif, yaitu menilai keseimbangan antarkomponen dan bukan capaian tiap komponen secara terpisah, sehingga sesuai untuk menguji komposisi sebuah instrumen yang keseluruhan butirnya membentuk satu alat ukur. Kedua, model ini menempatkan tugas sebagai komponen yang setara dengan teknologi dan struktur, sedangkan sebagian besar kerangka kematangan memperlakukan proses sebagai turunan tata kelola, sehingga model ini mampu mengungkap dimensi yang tersembunyi pada klasifikasi bawaan instrumen. Ketiga, proposisi saling ketergantungan antarkomponen memberikan dasar teoretis untuk menafsirkan defisit satu ruang lingkup sebagai risiko sistemik, bukan sekadar kekurangan jumlah kontrol (Leavitt, 1965). Relevansi lensa ini pada ranah keamanan siber kontemporer ditunjukkan oleh studi yang menempatkan keselarasan antara teknologi, manusia, dan struktur organisasi sebagai penentu kapabilitas keamanan yang berkelanjutan (Vestad & Yang, 2025). Agar pelabelan tidak berhenti pada kecocokan kata kunci, setiap penandaan diverifikasi terhadap tujuan akhir kontrol, yaitu kata kunci hanya digunakan sebagai penanda awal sedangkan keputusan akhir mengikuti luaran yang hendak dicapai butir tersebut, dan butir yang luarannya menuntut lebih dari satu komponen memperoleh penandaan ganda.

2.6 Sintesis Temuan dan Perumusan Model

Seluruh temuan titik buta dan ketimpangan proporsi ditransformasikan menjadi empat prinsip desain model. Prinsip pertama adalah restrukturisasi dimensional, yaitu pemisahan ruang lingkup Tata Kelola menjadi Struktur dan Tugas melalui analisis kata kunci. Prinsip kedua adalah augmentasi pengawasan, yaitu penambahan kategori khusus yang mewadahi fungsi pengawasan pimpinan apabila hasil analisis menunjukkan absennya mekanisme tersebut. Prinsip ketiga adalah augmentasi selektif titik buta, yaitu penambahan butir baru yang diprioritaskan pada ruang lingkup yang terbukti *underrepresented*. Prinsip keempat adalah adopsi skema pengukuran standar berupa skala NPLF sebagai rubrik kematangan model usulan. Rancangan yang dihasilkan bersifat konseptual, sehingga validasi pakar dan uji coba lapangan diposisikan sebagai agenda penelitian lanjutan.

3. HASIL DAN PEMBAHASAN

3.1 Keselarasan IKAS pada Cakupan Maju

Pemetaan terhadap 181 butir memperlihatkan bahwa mayoritas kontrol IKAS memiliki padanan pada kerangka kerja internasional. Sebanyak 156 butir (86,2%) selaras dengan NIST CSF 2.0 dan 138 butir (76,2%) selaras dengan ISO/IEC 27001:2022, sedangkan butir yang selaras pada kedua kerangka sekaligus berjumlah 134 butir (74,0%). Rekapitulasi status keselarasan disajikan pada Tabel 3. Rekapitulasi Status Keselarasan IKAS v1.2.1 (n = 181 Butir)

Tabel 3. Rekapitulasi Status Keselarasan IKAS v1.2.1 (n = 181 Butir)

Status / Metrik	Jumlah	Persentase
Memiliki keselarasan NIST CSF 2.0	156	86,20%
Memiliki keselarasan ISO/IEC 27001:2022	138	76,20%
Fully Aligned (kedua kerangka)	134	74,00%
Partially Aligned: hanya NIST CSF 2.0	22	12,20%
Partially Aligned: hanya ISO/IEC 27001:2022	4	2,20%
Not Aligned (tanpa padanan keduanya)	21	11,60%

Indeks keselarasan cakupan maju per domain disajikan pada Tabel 4. Indeks Keselarasan per Domain IKAS pada Cakupan Maju. Domain Proteksi dan Domain Identifikasi mencapai kategori *Fully Achieved*, sedangkan Domain Deteksi serta Domain Penanggulangan dan Pemulihan berada pada kategori *Largely Achieved*. Nilai agregat sebesar 81,2% menempatkan IKAS versi 1.2.1 pada kategori *Largely Achieved*.

Cakupan terhadap NIST CSF 2.0 secara konsisten lebih tinggi daripada terhadap ISO/IEC 27001:2022. Pola tersebut mengindikasikan bahwa orientasi IKAS lebih dekat pada model berbasis fungsi luaran dibanding pada katalog kontrol *Annex A*. Domain Penanggulangan dan Pemulihan menjadi domain dengan indeks terendah pada kedua

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

kerangka, yaitu 61,2%, yang mengisyaratkan bahwa aspek respons dan pemulihan merupakan area paling longgar keselarasannya.

Tabel 4. Indeks Keselarasan per Domain IKAS pada Cakupan Maju

Domain	Butir	Ke NIST	Ke ISO	Rerata	Kategori
D1 Identifikasi	51	98,00%	78,40%	88,20%	*Fully Achieved*
D2 Proteksi	62	88,70%	91,90%	90,30%	*Fully Achieved*
D3 Deteksi	19	89,50%	78,90%	84,20%	*Largely Achieved*
D4 Penanggulangan dan Pemulihan	49	69,40%	53,10%	61,20%	*Largely Achieved*
Total	181	86,20%	76,20%	81,20%	Largely Achieved

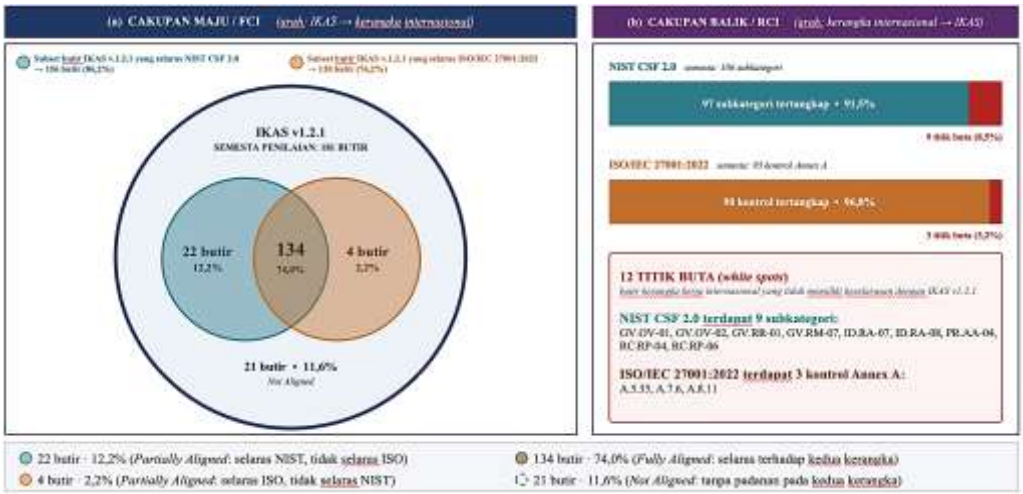
3.2 Keselarasan pada Cakupan Balik dan Titik Buta

Cakupan balik mengukur kelengkapan IKAS versi 1.2.1 dari sudut pandang kerangka kerja internasional. Indeks cakupan balik mencapai 91,5% terhadap NIST CSF 2.0, yaitu 97 dari 106 subkategori, dan 96,8% terhadap ISO/IEC 27001:2022, yaitu 90 dari 93 kontrol. Kedua nilai berada pada kategori *Fully Achieved*. Rincian disajikan pada Tabel 5. Indeks Cakupan Balik NIST CSF 2.0 dan *Annex A* ISO/IEC 27001:2022 terhadap IKAS v1.2.1.

Tabel 5. Indeks Cakupan Balik NIST CSF 2.0 dan *Annex A* ISO/IEC 27001:2022 terhadap IKAS v1.2.1

Fungsi / Tema	Total Butir	Tertangkap IKAS	Cakupan
GV (*Govern*)	31	27	87,10%
ID (*Identify*)	21	19	90,50%
PR (*Protect*)	22	21	95,50%
DE (*Detect*)	11	11	100%
RS (*Respond*)	13	13	100%
RC (*Recover*)	8	6	75,00%
Subtotal NIST CSF 2.0	106	97	91,50%
A.5 *Organizational*	37	36	97,30%
A.6 *People*	8	8	100%
A.7 *Physical*	14	13	92,90%
A.8 *Technological*	34	33	97,10%
Subtotal ISO/IEC 27001:2022	93	90	96,80%

Dua temuan menonjol dari cakupan balik. Pertama, fungsi *Recover* memiliki cakupan terendah sebesar 75,0% dan menjadi satu-satunya fungsi yang berada di bawah ambang *Fully Achieved*, sehingga aspek pemulihan terbukti belum tertangkap secara lengkap. Kedua, kekurangan pada ISO/IEC 27001:2022 tersebar merata, yaitu masing-masing satu kontrol pada tema *organizational*, *physical*, dan *technological*.



Gambar 2. Hubungan IKAS v1.2.1, NIST CSF 2.0, dan ISO/IEC 27001:2022 pada Cakupan Maju (a) dan Cakupan Balik (b)

Dari sisi sebaliknya, sebanyak 21 butir IKAS (11,6%) tidak memiliki padanan pada kedua kerangka. Butir tersebut terkonsentrasi pada Kategori 4.3 Domain Penanggulangan dan Pemulihan sebanyak 12 dari 21 butir, dan diinterpretasikan sebagai kontrol khas regulasi nasional yang berpotensi menjadi kebaruan IKAS sepanjang relevansinya terhadap konteks penyelenggara IIV dapat dijustifikasi. Adapun titik buta berjumlah 12 butir, terdiri atas sembilan subkategori NIST CSF 2.0, yaitu GV.OV-01, GV.OV-02, GV.RR-01, GV.RM-07, ID.RA-07, ID.RA-08, PR.AA-04, RC.RP-04, dan RC.RP-06, serta tiga kontrol *Annex A* ISO/IEC 27001:2022, yaitu A.5.35, A.7.6, dan

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

A.8.11. Titik buta NIST CSF 2.0 terkonsentrasi pada sub-fungsi *Govern Oversight* dan *Recover*. Rangkuman hubungan ketiga kerangka pada dua unit analisis yang berbeda disajikan pada Gambar 2. Hubungan IKAS v1.2.1, NIST CSF 2.0, dan ISO/IEC 27001:2022 pada Cakupan Maju (a) dan Cakupan Balik (b)

Gambar 2. Hubungan IKAS v1.2.1, NIST CSF 2.0, dan ISO/IEC 27001:2022 pada Cakupan Maju (a) dan Cakupan Balik (b)memisahkan kedua arah pengukuran karena relasi pemetaan bersifat banyak-ke-banyak. Bagian (a) memartisi 181 butir IKAS secara lengkap dan saling lepas menjadi 134 butir *Fully Aligned*, 22 butir yang selaras hanya pada NIST CSF 2.0, 4 butir yang selaras hanya pada ISO/IEC 27001:2022, dan 21 butir *Not Aligned*, sehingga keempat segmen sah dijumlahkan. Bagian (b) menggunakan unit analisis butir kerangka kerja internasional dan menyisakan 12 titik buta. Kedua bagian tidak boleh dijumlahkan silang karena unit analisisnya berbeda.

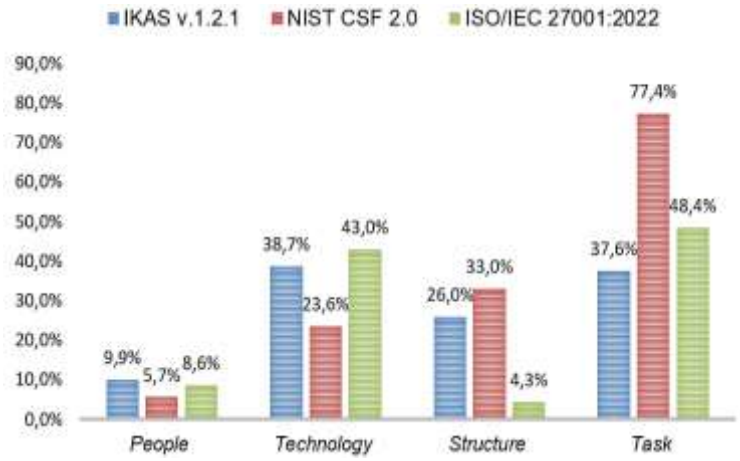
3.3 Kesenjangan Sosioteknis

Dekonstruksi 181 butir menghasilkan 203 penandaan ruang lingkup, sehingga rerata satu butir membawa 1,12 penandaan. Distribusi ruang lingkup IKAS beserta perbandingannya terhadap kerangka kerja internasional disajikan pada Tabel 6. Distribusi Ruang Lingkup Sosioteknis dan Indeks Kesenjangan dan divisualisasikan pada Gambar 3. Perbandingan Distribusi Ruang Lingkup Sosioteknis IKAS v1.2.1 terhadap NIST CSF 2.0 dan ISO/IEC 27001:2022.

Tabel 6. Distribusi Ruang Lingkup Sosioteknis dan Indeks Kesenjangan

Ruang Lingkup	IKAS	NIST	ISO	Rerata Internasional	Kesenjangan
SDM (*People*)	9,90%	5,70%	8,60%	7,10%	2,80%
Teknologi (*Technology*)	38,70%	23,60%	43,00%	33,30%	5,40%
Struktur (*Structure*)	26,00%	33,00%	4,30%	18,70%	7,30%
Tugas (*Task*)	37,60%	77,40%	48,40%	62,90%	−25,3%

Keterangan: Kesenjangan dihitung sebagai persentase IKAS dikurangi rata-rata persentase NIST CSF 2.0 dan ISO/IEC 27001:2022. Nilai positif menyatakan representasi setara atau lebih tinggi, nilai negatif menyatakan kondisi *underrepresented*. Klasifikasi bersifat multi ruang lingkup sehingga jumlah kolom persentase dapat melampaui 100%.



Gambar 3. Perbandingan Distribusi Ruang Lingkup Sosioteknis IKAS v1.2.1 terhadap NIST CSF 2.0 dan ISO/IEC 27001:2022

Gambar 3. Perbandingan Distribusi Ruang Lingkup Sosioteknis IKAS v1.2.1 terhadap NIST CSF 2.0 dan ISO/IEC 27001:2022 memperlihatkan bahwa tiga ruang lingkup memiliki kesenjangan positif, sehingga representasinya pada IKAS setara atau lebih tinggi dibanding rata-rata kerangka kerja internasional. Ruang lingkup Tugas menjadi satu-satunya ruang lingkup dengan kesenjangan negatif, yaitu 25,3 poin persentase. Kesenjangan positif tertinggi terdapat pada ruang lingkup Struktur sebesar 7,3 poin persentase, yang menunjukkan karakter instrumen yang berat pada tata kelola. Kondisi tersebut berakar pada rancangan IKAS versi 1.2.1 yang belum memisahkan dimensi Tugas dari Tata Kelola, sehingga kontrol prosedural tidak memiliki klasifikasi tersendiri dan terserap ke dalam aspek struktural.

Analisis pada tingkat domain memperjelas letak ketimpangan tersebut. Distribusi internal IKAS memperlihatkan Domain Identifikasi didominasi ruang lingkup Struktur (62,7%) dan menjadi satu-satunya domain tanpa butir berdimensi SDM, Domain Proteksi dan Domain Deteksi didominasi ruang lingkup Teknologi (62,9% dan 63,2%), sedangkan Domain Penanggulangan dan Pemulihan didominasi ruang lingkup Tugas (69,4%). Pada NIST CSF 2.0, ruang lingkup Tugas dominan di seluruh fungsi dengan rentang 73,1% hingga 100%. Matriks selisih antarpasangan domain dan fungsi disajikan pada Tabel 7. Matriks Kesenjangan Ruang Lingkup per Domain (Δ = Persentase IKAS − Persentase NIST).

Tabel 7. Matriks Kesenjangan Ruang Lingkup per Domain (Δ = Persentase IKAS − Persentase NIST)

Domain IKAS	Δ SDM	Δ Teknologi	Δ Struktur	Δ Tugas

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

D1 Identifikasi	−7,7%	11,80%	−4,6%	−39,7%
D2 Proteksi	11,90%	−28,0%	6,50%	−30,4%
D3 Deteksi	5,30%	17,70%	21,10%	−89,5%
D4 Penanggulangan dan Pemulihan	8,20%	26,50%	14,30%	−30,6%

Tabel 7. Matriks Kesenjangan Ruang Lingkup per Domain (Δ = Persentase IKAS − Persentase NIST)menegaskan bahwa ruang lingkup Tugas bernilai negatif pada seluruh domain. Kesenjangan terbesar terjadi pada Domain Deteksi sebesar 89,5 poin persentase, karena IKAS hanya memuat 10,5% kontrol berdimensi Tugas pada domain tersebut sedangkan seluruh subkategori fungsi *Detect* bersifat prosedural. Perbandingan lanjutan memperlihatkan bahwa hanya 22 dari 181 butir IKAS versi 1.2.1 (12,2%) membawa penandaan ganda, sementara 42 dari 106 subkategori NIST CSF 2.0 (39,6%) bersifat lintas ruang lingkup, sehingga butir IKAS cenderung berdimensi tunggal dan kurang terintegrasi secara sosioteknis pada tingkat butir.

Kesenjangan pada Domain Deteksi perlu ditelusuri sampai tataran operasional karena merupakan temuan paling menentukan pada penelitian ini. Dari 19 butir pada domain tersebut, 12 butir (63,2%) berdimensi Teknologi dan hanya 2 butir (10,5%) berdimensi Tugas, sehingga rumusan butir terpusat pada keberadaan kapabilitas deteksi seperti sistem pemantauan, pencatatan *log*, dan mekanisme perolehan informasi ancaman. Sebaliknya, seluruh subkategori fungsi *Detect* NIST CSF 2.0 dirumuskan sebagai luaran prosedural, yaitu analisis atas peristiwa yang terpantau, korelasi informasi dari berbagai sumber, penetapan ambang eskalasi, serta pemberitahuan kepada pihak yang berkepentingan. Konsekuensi praktisnya bersifat langsung. Organisasi yang telah memasang perangkat pemantauan akan memperoleh skor kematangan deteksi yang tinggi meskipun belum memiliki prosedur triase peringatan, ambang eskalasi, dan penugasan analis yang menjalankannya, padahal justru rangkaian prosedur itulah yang menentukan apakah sebuah anomali berakhir sebagai peringatan yang ditindaklanjuti atau sebagai catatan yang terlewat. Kesenjangan sebesar 89,5 poin persentase pada domain ini dengan demikian bukan sekadar ketimpangan statistik, melainkan indikasi bahwa instrumen berpotensi menilai kepemilikan perangkat deteksi sebagai kematangan deteksi, dan hal ini sejalan dengan rendahnya cakupan balik fungsi *Recover* yang juga bekerja berbasis prosedur.

Tiga temuan utama menjawab pertanyaan penelitian kedua. Temuan pertama, ruang lingkup Tugas merupakan kesenjangan struktural pada seluruh domain dengan magnitudo ekstrem pada Domain Deteksi, dan akar masalahnya adalah ketiadaan ruang lingkup Tugas yang eksplisit pada IKAS versi 1.2.1. Temuan kedua, ruang lingkup SDM konsisten rendah dengan proporsi agregat 9,9% dan absen sama sekali pada Domain Identifikasi, padahal pemahaman risiko pada tahap identifikasi membutuhkan kompetensi dan kesadaran personel. Temuan ketiga, distribusi ruang lingkup Struktur tampak proporsional tetapi menyembunyikan celah pengawasan, karena kebijakan dan peran telah tersedia sebagai kontrol sedangkan mekanisme tinjauan capaian oleh pimpinan yang diwakili GV.OV-01 dan GV.OV-02 belum menjadi butir penilaian.

3.4 Rancangan Model Konseptual IKAS-ST

Ketiga temuan tersebut diterjemahkan menjadi tiga intervensi rancangan. Intervensi pertama adalah restrukturisasi dimensional, yaitu pemekaran tiga ruang lingkup IKAS versi 1.2.1 menjadi empat ruang lingkup sosioteknis dengan memisahkan Tata Kelola menjadi Struktur yang memuat kebijakan, peran, dan pengawasan, serta Tugas yang memuat prosedur, pelaksanaan, dan pengujian. Reklasifikasi 181 butir menghasilkan komposisi 18 butir SDM, 70 butir Teknologi, 47 butir Struktur, dan 68 butir Tugas.

Intervensi kedua adalah penambahan Kategori 1.6 Pengawasan dan Reviu Strategis pada Domain Identifikasi. Kategori ini mewadahi tiga mekanisme yang selama ini menjadi titik buta, yaitu tinjauan capaian strategi keamanan siber oleh pimpinan (GV.OV-01), tinjauan dan penyesuaian strategi manajemen risiko keamanan siber (GV.OV-02), serta tinjauan independen keamanan informasi (A.5.35). Nomor kategori ditetapkan 1.6 karena Kategori 1.5 telah terisi oleh Manajemen Risiko Rantai Pasok pada instrumen berjalan.

Intervensi ketiga adalah augmentasi 12 butir penilaian yang mengadopsi seluruh titik buta hasil pemetaan. Komposisi penandaan augmentasi memprioritaskan ruang lingkup Tugas dengan sembilan penandaan, disusul Struktur dengan tiga penandaan, SDM dengan dua penandaan, dan Teknologi dengan dua penandaan, sehingga total 16 penandaan pada 12 butir. Prioritas tersebut konsisten dengan diagnosis kesenjangan, yaitu ruang lingkup Tugas memperoleh porsi terbesar sedangkan ruang lingkup Teknologi yang telah *overrepresented* hanya memperoleh penambahan selektif berupa proteksi asersi identitas (PR.AA-04) dan pengaburan data (A.8.11). Butir GV.RR-01 secara khusus mengisi ruang lingkup SDM pada Domain Identifikasi yang semula kosong. Perbandingan struktur instrumen sebelum dan sesudah penguatan disajikan pada Tabel 8. Perbandingan Struktur IKAS v1.2.1 dan IKAS-ST.

Kedua belas butir augmentasi terdistribusi pada satu kategori baru dan enam kategori berjalan. Kategori 1.6 menampung tiga butir, sedangkan sembilan butir lainnya melekat pada Kategori 1.1, 1.4, 2.1, 2.2, 2.3, dan 4.3 mengikuti kedekatan substansi. Sebanyak tujuh butir memperkuat Domain Identifikasi, tiga butir memperkuat Domain Proteksi, dan dua butir memperkuat Domain Penanggulangan dan Pemulihan.

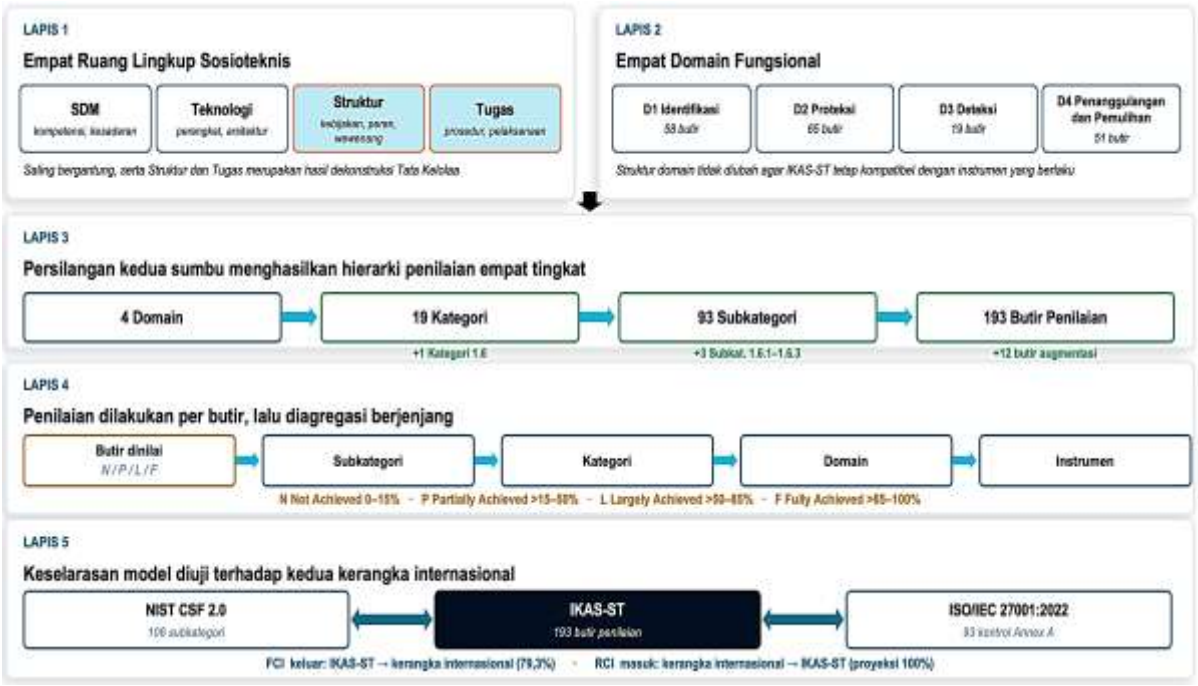
Tabel 8. Perbandingan Struktur IKAS v1.2.1 dan IKAS-ST

Aspek	IKAS v1.2.1	IKAS-ST
Ruang lingkup	3 (SDM, Teknologi, Tata Kelola)	4 (SDM, Teknologi, Struktur, Tugas)
Jumlah domain	4	4 (tetap)

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

Jumlah kategori	18	19 (+ Kategori 1.6)
Jumlah subkategori	90	93 (+ Subkategori 1.6.1–1.6.3)
Jumlah butir penilaian	181	193 (+12; +6,6%)

Karena setiap titik buta memperoleh butir penilaian yang secara khusus mengadopsinya, cakupan balik IKAS-ST terhadap NIST CSF 2.0 maupun ISO/IEC 27001:2022 menjadi lengkap secara konstruksi. Nilai tersebut perlu dibaca sebagai konsekuensi logis dari rancangan dan bukan sebagai hasil pengukuran empiris, karena yang dihitung adalah kelengkapan pada tataran dokumen instrumen, sedangkan kelengkapan pada tataran penerapan baru dapat dipastikan setelah rumusan butir augmentasi dinilai oleh pakar dan diujicobakan pada penyelenggara Infrastruktur Informasi Vital. Klaim kelengkapan ini karenanya bersifat akan gugur apabila validasi pakar menilai suatu butir augmentasi tidak benar-benar mewakili luaran titik buta yang diadopsinya, dan pengujian itulah yang diposisikan sebagai agenda penelitian lanjutan. Arsitektur IKAS-ST disajikan secara utuh pada Gambar 4. Model Konseptual IKAS-STagar susunan dan asal-usul setiap unsurnya terbaca sebagai satu kesatuan. Model disusun dalam lima lapis yang berurutan. Dua lapis pertama merupakan sumbu penyusun model, lapis ketiga merupakan hierarki penilaian yang dihasilkan dari persilangan kedua sumbu, lapis keempat merupakan mekanisme penilaian dan agregasi, dan lapis kelima merupakan mekanisme pengujian keselarasan model terhadap kedua kerangka kerja internasional.



Gambar 4. Model Konseptual IKAS-ST

3.5 Pembahasan

Keselarasan maju yang tinggi menunjukkan bahwa IKAS versi 1.2.1 bukan instrumen yang usang atau menyimpang dari praktik global, melainkan telah memuat sebagian besar kontrol esensial. Temuan ini memperkuat hasil kajian penyelarasan instrumen nasional terhadap standar internasional yang melaporkan tingkat kesesuaian substansial namun tidak sempurna (Apriany & Wibowo, 2024; Supriyanto et al., 2025). Kajian atas Indeks KAMI melaporkan tingkat keselarasan 56% terhadap ISO/IEC 27001 dan NIST melalui pemetaan ontologis berbasis prinsip *confidentiality*, *integrity*, dan *availability* (Supriyanto et al., 2025), sedangkan penelitian ini memperoleh indeks cakupan maju 81,2% pada IKAS versi 1.2.1. Kedua angka tidak dapat dibandingkan secara langsung karena berbeda instrumen, granularitas unit analisis, dan dasar pemetaan, namun keduanya menunjuk pada simpulan yang sama, yaitu instrumen nasional selaras secara substansial dengan standar internasional dan menyisakan celah harmonisasi yang terbatas serta dapat ditutup secara terarah. Nilai tambah penelitian ini terletak pada dimensi yang belum dilaporkan kajian tersebut, yaitu asimetri antarfungsi yang hanya terungkap melalui pengukuran arah balik. Karakter IKAS yang kuat pada pencegahan namun lemah pada pemulihan sejalan dengan pola yang teramati pada kerangka kematangan sektoral lain (Bernardo et al., 2025; Salam et al., 2025), dan memberikan justifikasi empiris bahwa penguatan paling bernilai berada pada aspek pengawasan strategis serta pemulihan, bukan pada area yang telah jenuh.

Perbandingan langsung antara indeks maju IKAS versi 1.2.1 dan IKAS-ST berpotensi menimbulkan tafsir keliru, karena nilai agregat justru menurun dari 81,2% menjadi 79,3%. Tafsir tersebut tidak tepat karena kedua arah metrik mengukur konstruk yang berbeda. Indeks maju mengukur konvergensi, sedangkan indeks balik mengukur kelengkapan cakupan. Tujuan penguatan diarahkan pada penutupan celah cakupan dan penyeimbangan komposisi sosioteknis, sehingga metrik keberhasilan yang relevan adalah indeks balik beserta distribusi ruang lingkup, bukan indeks maju.

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

Perbandingan kedua arah metrik disajikan pada Tabel 9. Perbandingan Dual-Metrik Keselarasan IKAS v1.2.1 dan IKAS-ST

Tabel 9. Perbandingan Dual-Metrik Keselarasan IKAS v1.2.1 dan IKAS-ST

Metrik	Arah Pengukuran	IKAS v1.2.1 (181 butir)	IKAS-ST (193 butir)	Perubahan
FCI-NIST	IKAS ke internasional	86,2% (156/181)	85,5% (165/193)	−0,7%
FCI-ISO	IKAS ke internasional	76,2% (138/181)	73,1% (141/193)	−3,2%
FCI rata-rata	IKAS ke internasional	81,20%	79,30%	−1,9%
RCI-NIST	Internasional ke IKAS	91,5% (97/106)	100% (106/106)	8,50%
RCI-ISO	Internasional ke IKAS	96,8% (90/93)	100% (93/93)	3,20%

Penurunan indeks maju sebesar 1,9 poin persentase bersifat aritmetis dan melekat pada desain augmentasi, bukan indikasi kemunduran substansi. Kedua belas butir augmentasi diadopsi dari titik buta pada satu kerangka saja sehingga, menurut klausul pada Tabel 1. Klausul Penetapan Status Keselarasan Butir IKAS, seluruhnya berstatus *Partially Aligned* dan menyumbang 50% per butir terhadap rata-rata dua kerangka, yaitu jauh di bawah rerata dasar 81,2%. Efek dilusi tersebut dapat ditelusuri melalui persamaan (5).

$FCI_{\text{IKAS-ST}} = (181 \times 81{,}2\% + 12 \times 50{,}0\%) / 193 = 79{,}3\%$

Dilusi tersebut tidak menggeser kategori kualitatif karena kedua nilai tetap berada pada rentang *Largely Achieved*. Keberhasilan model karenanya dinilai dari tiga capaian, yaitu tertutupnya seluruh titik buta sehingga indeks balik terproyeksi 100% pada kedua kerangka, tereksplisitkannya ruang lingkup Struktur dan Tugas yang sebelumnya tidak terdefinisi sebagai dimensi formal instrumen, serta terisinya ruang lingkup SDM pada Domain Identifikasi yang semula tidak memuat satu pun butir.

Lensa sosioteknis memberikan penjelasan atas ketidakmerataan cakupan balik antarfungsi. Kesenjangan ruang lingkup Tugas yang negatif pada seluruh domain bukan sekadar kekurangan jumlah kontrol, melainkan akibat rancangan instrumen yang tidak menyediakan klasifikasi bagi kontrol prosedural sehingga kontrol tersebut terserap ke dalam Tata Kelola. Konsekuensinya paling terasa pada fungsi yang bekerja berbasis prosedur, yaitu Domain Deteksi yang mengalami kesenjangan ekstrem dan fungsi *Recover* yang menjadi satu-satunya fungsi di bawah ambang *Fully Achieved*, karena deteksi dan pemulihan pada dasarnya merupakan rangkaian prosedur dan bukan sekadar perangkat. Temuan ini menguatkan proposisi *Leavitt's Diamond* bahwa kelemahan pada satu komponen mengganggu keseimbangan komponen lain (Leavitt, 1965), dan memperluas penerapan lensa sosioteknis yang selama ini digunakan untuk mendiagnosis organisasi (Ani et al., 2022; Ewoh et al., 2025; Wani et al., 2025) menjadi alat diagnosis terhadap instrumen kebijakan.

Kontribusi penelitian ini berada pada dua tataran. Secara teoretis, penelitian mendemonstrasikan penggunaan *Leavitt's Diamond* sebagai lensa evaluatif atas komposisi instrumen kebijakan keamanan siber, sebuah pendekatan yang melengkapi metode komparasi berbasis pemetaan kontrol semata sebagaimana lazim dilakukan pada kajian antarstandar (Kurii & Opirskyy, 2022; Zakiy & Angresti, 2024). Secara praktis, IKAS-ST menyediakan rancangan penguatan yang spesifik dan tertelusur, dan karena sifatnya augmentatif dengan mempertahankan seluruh 181 butir asli, model ini kompatibel dengan instrumen yang berlaku serta layak dipertimbangkan sebagai basis revisi pada siklus pemutakhiran berikutnya. Sebanyak 21 butir *Not Aligned* dipertahankan dan didokumentasikan sebagai kekhasan regulasi nasional, bukan diperlakukan sebagai kekurangan instrumen.

Penelitian ini memiliki tiga keterbatasan yang perlu disampaikan secara terbuka. Model IKAS-ST baru tersusun secara metodologis dan belum melalui validasi pakar formal maupun uji coba lapangan, sehingga kelengkapan cakupan balik yang dilaporkan berlaku pada tataran rancangan dokumen instrumen dan belum pada tataran penerapan. Penetapan padanan bertumpu pada *expert judgment* sehingga melekat unsur subjektivitas, risiko tersebut ditekan melalui klausul penilaian, pembakuan urutan keputusan, dan pendokumentasian seluruh keputusan padanan pada matriks yang dilampirkan sebagai data suplementer, namun tidak hilang sepenuhnya karena uji kesepakatan antarpenilai dengan melibatkan pengode kedua belum dilakukan pada tahap ini. Kajian ini disusun oleh praktisi yang bertugas pada instansi penerbit instrumen, sehingga objektivitas perlu dijaga melalui validasi lintas unsur pada penelitian lanjutan.

4. KESIMPULAN

Pemetaan dua arah terhadap 181 butir IKAS versi 1.2.1 menunjukkan keselarasan yang substansial terhadap kerangka kerja internasional, dengan indeks cakupan maju rata-rata 81,2% berkategori *Largely Achieved* serta indeks cakupan balik 91,5% terhadap NIST CSF 2.0 dan 96,8% terhadap ISO/IEC 27001:2022 yang keduanya berkategori *Fully Achieved*, disertai 21 butir kontrol khas nasional dan 12 titik buta yang terkonsentrasi pada fungsi *Govern* dan *Recover*. Analisis melalui *Leavitt's Diamond* melokalisasi kesenjangan pada ruang lingkup Tugas sebagai satu-satunya ruang lingkup yang kurang terwakili dengan simpangan 25,3 poin persentase dan magnitudo ekstrem 89,5 poin persentase pada Domain Deteksi, ditambah ketiadaan ruang lingkup SDM pada Domain Identifikasi dan absennya mekanisme pengawasan strategis meskipun proporsi Struktur tampak memadai, yang seluruhnya berakar pada ketiadaan dimensi Tugas yang eksplisit sehingga kontrol prosedural terserap ke dalam Tata Kelola. Ketiga temuan tersebut dirumuskan

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

menjadi model konseptual IKAS-ST melalui restrukturisasi menjadi empat ruang lingkup sosioteknis, penambahan Kategori 1.6 Pengawasan dan Reviu Strategis, serta augmentasi 12 butir menjadi 193 butir dalam 19 kategori dan 93 subkategori, sehingga cakupan balik terproyeksi lengkap pada kedua kerangka sementara penurunan indeks maju menjadi 79,3% terbukti merupakan efek dilusi aritmetis dan bukan kemunduran mutu keselarasan. Keunggulan model tidak terletak pada bertambahnya jumlah butir, melainkan pada ketertelusuran setiap butir tambahan pada titik buta yang teridentifikasi dan pada restrukturisasi yang menyentuh akar kesenjangan. Pada tataran kebijakan, tiga langkah dapat ditempuh tanpa menunggu revisi peraturan secara menyeluruh, yaitu menjadikan ruang lingkup Tugas sebagai penandaan wajib pada setiap butir agar keterlaksanaan prosedur terukur terpisah dari keberadaan kebijakan, memprioritaskan Domain Deteksi dan fungsi pemulihan pada siklus pemutakhiran terdekat karena keduanya paling terdampak oleh ketiadaan dimensi prosedural, serta menempatkan Kategori 1.6 sebagai butir wajib bagi penyelenggara Infrastruktur Informasi Vital dengan tingkat kekritisan tertinggi mengingat pengawasan strategis merupakan kontrol berbiaya rendah dengan daya ungkit tata kelola yang besar. Penyelenggara Infrastruktur Informasi Vital disarankan tidak memperlakukan skor kematangan yang tinggi sebagai jaminan ketahanan sebelum memastikan prosedur pendukungnya benar-benar berjalan. Keterbatasan penelitian terletak pada sifat rancangan model yang belum divalidasi pakar secara formal dan belum diujicobakan di lapangan, serta pada unsur subjektivitas penetapan padanan yang baru dimitigasi melalui klausul penilaian dan pendokumentasian matriks, sehingga kelengkapan cakupan balik masih berstatus klaim rancangan yang menunggu pengujian. Penelitian lanjutan karenanya diarahkan pada validasi pakar lintas unsur menggunakan indeks validitas isi, uji kesepakatan antarpenilai atas hasil pemetaan, uji coba penerapan pada penyelenggara Infrastruktur Informasi Vital untuk menilai beban penilaian dan akurasi pengukuran, serta perluasan komparasi ke kerangka lain yang relevan seperti CIS Controls dan COBIT 2019.

REFERENCES

Ani, U. D., Watson, J. M., Tuptuk, N., Hailes, S., & Jawar, A. (2022). *Socio-technical security modelling: Analysis of state-of-the-art, application, and maturity in critical industrial infrastructure environments/domains.* PETRAS National Centre of Excellence in IoT Systems Cybersecurity. https://shura.shu.ac.uk/32206/1/2305.05108.pdf.

Apriany, A., & Wibowo, A. (2024). Analysis of the implementation of ISO 27001:2022 and KAMI index in enhancing the information security management system in consulting firms. *Indonesian Journal of Computing and Cybernetics Systems, 18*, 417-428. https://doi.org/10.22146/ijccs.100385.

Badan Siber dan Sandi Negara. (2023). *Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital.* Jakarta. https://peraturan.bpk.go.id/Details/291265/peraturan-bssn-no-8-tahun-2023

Badan Siber dan Sandi Negara. (2023). *Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber.* Jakarta. https://peraturan.bpk.go.id/Details/291280/peraturan-bssn-no-10-tahun-2023.

Badan Siber dan Sandi Negara. (2026). *Lanskap keamanan siber Indonesia 2025.* Jakarta. https://www.bssn.go.id/layanan/

Balafif, S. (2023). Penyesuaian model ketahanan siber UMKM di Indonesia dengan NIST cybersecurity framework (CSF). *Jurnal Informatika: Jurnal Pengembangan IT, 8*(3), 291-301. Retrieved from https://doi.org/10.30591/jpit.v8i3.5662

Bernardo, L., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. *Electronics, 14*, 1-20. https://doi.org/10.3390/electronics14071364.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107-115. https://doi.org/10.1111/j.1365-2648.2007.04569.x.

Ewoh, P., Vartiainen, T., & Mantere, T. (2025). Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: Scoping review. *Journal of Medical Internet Research, 27*, e75584. Retrieved from https://doi.org/10.2196/75584

Hardiana, T., & Suhardi. (2025). Desain instrumen pengukuran tingkat kematangan keamanan siber sektor pemerintahan. *Jurnal Pendidikan dan Teknologi Indonesia, 5*(11), 3288-3305. https://doi.org/10.52436/1.jpti.1124

International Organization for Standardization & International Electrotechnical Commission. (2019). *ISO/IEC 33020:2019 Information technology — Process assessment — Process measurement framework for assessment of process capability.* Geneva, Switzerland. https://www.iso.org/standard/78526.html

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Geneva, Switzerland. https://www.iso.org/standard/27001

Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of cybersecurity maturity assessment framework using NIST CSF v1.1 and CIS Controls v8. *Jurnal Inovtek Polbeng — Seri Informatika, 9*, 126-139. DOI:10.35314/isi.v9i1.3973.

Jelita, L. D., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi keamanan teknologi informasi menggunakan indeks keamanan informasi 5.0 dan ISO/IEC 27001:2022. *Jurnal Saintekom, 14*(1), 84-94. https://doi.org/10.33020/saintekom.v14i1.623.

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1413-1424
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10813

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications. https://methods.sagepub.com/book/mono/content-analysis-4e/toc#_

Kurii, Y., & Opirskyy, I. (2022). Analysis and comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *CEUR Workshop Proceedings*, *3288*, pp. 21-32. https://ceur-ws.org/Vol-3288/paper3.pdf.

Leavitt, H. J. (1965). *Applied organizational change in industry: Structural, technological and humanistic approaches.* Rand McNally. https://openlibrary.org/books/OL19794500M/Applied_organizational_change_in_industry.

NIST. (2024). *The NIST cybersecurity framework (CSF) 2.0.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Presiden Republik Indonesia. (2022). *Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.* Jakarta. https://peraturan.bpk.go.id/Details/211029/perpres-no-

Salam, M., Bakar, K. A., & Aman, A. H. (2025). Building cyber-resilient universities: A tailored maturity model for strengthening cybersecurity in higher education. *International Journal of Advanced Computer Science and Applications*, *16*, 95-104. https://doi.org/10.14569/IJACSA.2025.0160510.

Salas-Riega, J. L., Viru, Y. R., Soto, M. N., & Salas-Riega, J. M. (2025). Cybersecurity and the NIST framework: A systematic review of its implementation and effectiveness against cyber threats. *International Journal of Advanced Computer Science and Applications*, *16*, 723-735. https://doi.org/10.14569/IJACSA.2025.0160672.

Supriyanto, A., Jananto, A., Razaq, J. A., Hartono, B., & Damaryanti, F. (2025). Alignment of KAMI index with global security standards in information security risk maturity evaluation. *Cybernetics and Information Technologies, 25*(2), 173-192. Retrieved from https://doi.org/10.2478/cait-2025-0018

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations*, *4*(1), 3-38. Retrieved from https://doi.org/10.1177/001872675100400101

United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development.* United Nations. https://unctad.org/system/files/official-document/der2021_en.pdf.

Vestad, A., & Yang, B. (2025). From security frameworks to sustainable municipal cybersecurity capabilities. *Journal of Cybersecurity and Privacy*, *5*, 1-28. https://doi.org/10.3390/jcp5020019.

Wani, T. A., Mendoza, A., & Gray, K. (2025). A sociotechnical approach to bring-your-own-device security in hospitals: Development and pilot testing of a maturity model using mixed methods action research. *JMIR Human Factors*, *12*, e71912. Retrieved from https://doi.org/10.2196/71912

Wibawa, I. A., Susila, A. A., & Pasirullah, M. A. (2024). Information security evaluation at hospital using index KAMI 5.0 and recommendations based on ISO/IEC 27001:2022. *Journal of Information Systems and Informatics*, *6*(4), 3070-3086. https://doi.org/10.51519/journalisi.v6i4.949

Zakiy, F. W., & Angresti, N. D. (2024). Comparative analysis of cybersecurity maturity frameworks: NIST-CSF and C2M2. *JOISTECH: Journal of Information System and Technology*, *1*, 82-87. https://ejournal.darunnajah.ac.id/index.php/joistech/article/view/317.