Penilaian Keamanan Informasi Di Rumah Sakit Panti Wilasa Citarum Berdasar Indeks KAMI 5.0

Alpha Reandra Permana[1], Arif Kurniadi[2*], Agung Wardoyo[3]
[1,2,3]*Progdi D3 Rekam Medis dan Informai Keshatan, Fakultas Kesehatan, Universitas Dian Nuswantoro Semarang Gedung D Lantai 1,Kampus Utama Jl. Imam Bonjol No.207, Pendrikan Kidul, Kec. Semarang Tengah, Kota Semarang*
E-mail : alphareanda@gmail.com[1], arif.kurniadi@dsn.dinus.ac.id[2*)], agung.wardoyo@adm.dinus.ac.id[3]
*Koresponden author

Abstract— Indonesian Ministry of Health Regulation No. 24 of 2022 addresses Data Security and Protection in its fourth section. Regarding the quality standards used by Panti Wilasa Citarum Hospital—specifically those of the Hospital Accreditation Commission—there is one standard that has not yet been met: MRMIK 13, which pertains to regulations governing the implementation of information technology. The information security assessment uses the KAMI 5.0 Index from BSSN, which refers to the ISO/IEC 27001 standard to evaluate information security readiness in the SIMRS. Panti Wilasa Citarum as an implication of the implementation of Electronic Medical Records based on the KAMI Index. The study used a saturated sampling technique through interviews with 4 information system managers to complete the KAMI 5.0 index instrument. Results showed the following scores: electronic system category received 20 points (High), Governance 41 points (Maturity Level I plus), Risk Management 35 points (Level II), Information Security Framework 61 points (Level I plus), Asset Management 176 points (Level II), Information Security Technology 131 points (Level II), Personal Data Protection 60 points (Level II), and Third Party Security at 53%. The overall score was 504 points, reflecting a "Basic Framework Compliance" at Maturity Level II, which did not meet KAMI Index requirements. The hospital must enhance information security through training, awareness, and periodic assessments.
Keyword : Information Security, Data Protection, KAMI Index 5.0, ISO/IEC 27001

***Abstrak*—Permenkes RI Nomor 24 Tahun 2022 mengatur tentang Keamanan dan Perlindungan Data pada bagian keempat kemudian standar mutu yang digunakan Rumah Sakit Panti Wilasa Citarum yaitu Komisi Akreditasi Rumah Sakit terdapat salah satu standar yang belum dipenuhi yaitu MRMIK 13 terkait regulasi penyelenggaraan teknologi informasi. Penilaian keamanan informasi menggunakan Indeks KAMI 5.0 dari BSSN mengacu pada standar ISO/IEC 27001 untuk menilai kesiapan keamanan informasi pada SIMRS. Panti Wilasa Citarum sebagai implikasi dari implementasi Rekam Medis Elektronik berdasar Indeks KAMI. Penelitian menggunakan teknik sampel jenuh melalui wawancara kepada 4 responden pengelola sistem informasi untuk mengisi instrumen indeks KAMI 5.0. Hasil penelitian menunjukkan bahwa pada kategori sistem elektronik mendapat 20 poin dengan kategori "Tinggi", kemudian Tata Kelola 41 poin dengan tingkat kematangan I+, Pengelolaan Risiko 35 poin tingkat kematangan II, Kerangka Kerja Keamanan Informasi 61 poin tingkat kematangan I+, Pengelolaan Aset 176 poin tingkat kematangan II. Teknologi Keamanan Informasi 131 poin tingkat kematangan II, Perlindungan Data Pribadi 60 poin tingkat kematangan II, dan persentase Pengamanan Pihak Ketiga 53%. Total skor evaluasi akhir didapat 504 poin serta ditentukan definisi "Pemenuhan Kerangka Kerja Dasar" dalam tingkat kematangan II yang belum memenuhi ketentuan dari Indeks KAMI. Sehingga rumah sakit perlu meningkatkan penerapan keamanan informasi dengan pelatihan maupun sosialisasi sebagai peningkatan kepatuhan, kepedulian pengelolaan informasi dan perlindungan data pribadi, menyediakan layanan *cloud*, serta melaksanakan pengukuran keamanan informasi secara berkala menggunakan instrument Indeks KAMI.**
***Kata Kunci* : Keamanan informasi, Perlindungan data, Indeks KAMI 5.0, ISO/IEC 27001**

I. PENDAHULUAN

Di era digital saat ini, di mana ancaman siber terus berkembang dan menjadi semakin canggih, keamanan sistem informasi sangat penting untuk memastikan kerahasiaan, integritas, dan ketersediaan data. Seiring dengan kemajuan teknologi dan ancaman siber yang semakin canggih, sebuah organisasi harus tetap waspada dalam melindungi data sensitifnya. Satu kebocoran data dapat mengakibatkan kerugian finansial yang signifikan, konsekuensi hukum, bahkan bisa sampai terjadi rusaknya reputasi. Oleh karena itu langkah keamanan yang komprehensif menjadi hal yang sangat penting di era digital saat ini.

Berbagai upaya keamanan bisa dilakukan dalam bentuk enkripsi data, penerapan otentikasi multi-faktor, atau update rutin pada perangkat lunak guna antisipasi kerentanan. Selain itu, memiliki rencana tanggap darurat ketika terjadi insiden keamanan juga sangat penting untuk meminimalkan dampak buruk dan recovery dengan cepat. Langkah proaktif mengamankan sistem informasi pada organisasi akan berguna untuk mitigasi potensi kerusakan akibat serangan siber serta akan berdampak dalam mempertahankan kepercayaan pemangku kepentingan.

Keamanan sistem informasi merujuk pada perlindungan informasi dan data dalam suatu organisasi dari akses,

penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah. Hal ini melibatkan penerapan berbagai langkah keamanan, seperti firewall, enkripsi, kontrol akses, dan kebijakan keamanan, untuk melindungi informasi sensitif dan mencegah pelanggaran keamanan. Organisasi harus secara terus-menerus mengevaluasi dan meningkatkan langkah-langkah keamanan mereka untuk tetap selangkah di depan ancaman potensial dan melindungi aset informasi berharga mereka. Hal ini meliputi pelaksanaan audit keamanan secara rutin, pelatihan karyawan tentang praktik keamanan terbaik, dan tetap mengikuti perkembangan teknologi keamanan terbaru. Dengan memprioritaskan keamanan sistem informasi, organisasi dapat meminimalkan risiko yang terkait dengan serangan siber dan kebocoran data, pada akhirnya melindungi reputasi mereka dan mempertahankan kepercayaan pelanggan.

Rekam Medis sebagai dokumentasi layanan kesehatan yang dibuat oleh seorang tenaga medis pemberi layanan medis kepada pasien berisi kondisi pasien, riwayat kesehatan dan pengobatan sebelumnya. Rekam Medis berguna sebagai sumber informasi medis, statistik, pedoman dasar dan bukti hukum, serta dasar pengambilan keputusan klinis.[1][2]

Hadirnya transformasi teknologi bidang kesehatan dengan kegiatan utama integrasi dan pengembangan sistem data kesehatan berupa desain arsitektur Integrated Electronic Heatlh Record (EHR) pada tahun 2021, pengembangan big data Integrated EHR pada tahun 2022. Sementara untuk tahun 2023 berupa sistem analisis kesehatan berbasis AI sebagai perwujudan dari SatuSehat.[3]

Transformasi teknologi bidang kesehatan berbasis data individu dalam kemasan rekam medis elektronik melakukan pengelolaan basis data dengan mengumpulkan beragam sumber data medis dari fasilitas pelayanan kesehatan terintegrasi.[4] Rumah Sakit wajib membuat Rekam Medis Elektronik untuk pasien mulai dari kedatangan hingga pulang. Rumah Sakit sebagai salah satu pengendali dan prosesor data pribadi pasien, seperti nomor KTP, nomor telepon, dan data sensitif lainnya, termasuk riwayat kesehatan dan kondisi psikologis wajib mengelola dan mengamankan data maupun teknologi informasi untuk mengurangi ancaman keamanan serta menerapkan keamanan informasi.[5][6][7]

Meskipun manfaat dan dampak positif dari implementasi EHR ini, namun hal yang perlu diwaspadai adalah isu kemanan informasi. Sudah banyak kasus yang terjadi terkait dengan isu keamanan informasi ini misalnya pencurian data 230.000 pasien COVID-19 dan dijual di RaidForums, pembobolan lebih 1,3 juta data COVID-19 pengguna aplikasi Health Alert Card (eHAC)[8], dokumen berukuran 720 GB dalam 6 juta format data termasuk data pribadi termasuk foto pasien, asal Rumah Sakit, serta berbagai macam informasi medis bocor karena hacker dari server milik Kementerian Kesehatan.[9] Selain kebocoran data juga kasus serangan cyber berupa ransomware WannaCry pada tahun 2018 berdampak pada lumpuhnya sistem di Rumah Sakit.[10]

Menurut ISO/IEC 17799:2005 manajemen sistem keamanan informasi adalah upaya perlindungan dari ancaman guna menjamin keberlangsungan bisnis, meminimalkan risiko, meningkatkan investasi dan peluang bisnis. Aspek keamanan Informasi memiliki 3 aspek yaitu *Confidentiality, Integrity, Availability* (CIA) terhadap data dan informasi yang bersifat sensitif dan rahasia termasuk di dalamnya adalah data rekam medis pasien.[11][2] Sebagai langkah untuk melindungi informasi Rekam Medis Elektronik dan menghadapi ancaman keamanan dari serangan siber, BSSN menyediakan panduan untuk perlindungan sistem elektronik melalui evaluasi keamanan sistem informasi yang dikenal sebagai Indeks Keamanan Informasi (KAMI)[12].

Berbagai penelitian pendahulu yang dilakukan selama ini masih menggunakan instrumen indeks KAMI dari BSSN versi lama yaitu versi 4.0 [13] atau Indeks KAMI 4.2 [14]. Sementara penelelitian ini memberikan gambaran yang lebih mutakhir sesuai dengan standar ISO/IEC 27001:2022. Selain itu, sebagai noverlty penelitian ini dilakukan secara spesifik pada konteks Rumah Sakit pasca pemberlakuan Permenkes RI Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik (RME), yang memberikan tekanan regulasi baru bagi fasilitas kesehatan untuk memenuhi standar keamanan informasi tertentu demi integrasi program SatuSehat.

Indeks KAMI adalah instrumen evaluasi dalam mengukur tingkat kesiapan keamanan informasi terhadap suatu institusi dan tiidak tidak dimaksudkan untuk mengukur kelayakan atas upaya keamanan yang sudah dilakukan, namun untuk menggambarkan kesiapan kerangka kerja keamanan informasi pada suatu organisasi. Kerangka keamanan ini mengacu pada standar keamanan dari ISO/IEC27001:2022 hal tersebut mencakup *confidently* (kerahasiaan), *availability* (ketersediaan), dan *integrity* (integritas) pada aspek keamanan informasi.[15] Untuk meningkatkan keamanan data pasien, pengukuran dilakukan menggunakan instrument Indeks KAMI. Pada Indeks KAMI dapat diimplementasikan dalam mengukur kematangan sistem pada suatu Fasiltas Pelayanan Kesehatan apakah telah memenuhi dari prinsip keamanan dan informasi dari keamanan serta perlindungan data[13].

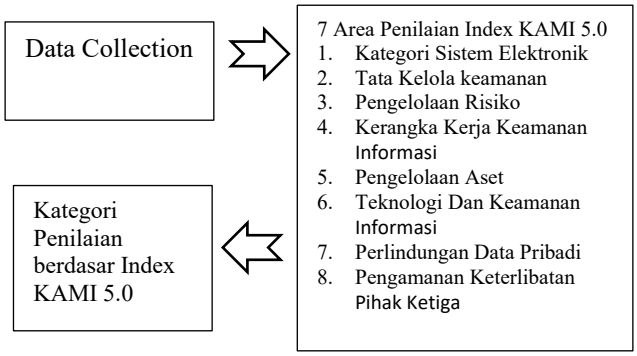
II. METODE PENELITIAN

Gambar 1 menunjukkan kerangka kerja dalam tahapan penelitian yang dilakukan. Data primer diambil setelah dinyatakan layak etik melalui etik No 000723/UNIVERSITAS DIAN NUSWANTORO/2025. Data deskriptif kuantitatif dikumpulkan melalui kuesioner dan wawancara kepada subyek penelitian menggunakan teknik sampling jenuh dengan cara mengambil semua anggota populasi sebagai sampel terdiri atas pengelola sistem informasi sebanyak 4 orang.[16]

Penggunaan jumlah responden yang terbatas ini dikarenakan penerapan teknik sampling jenuh dengan mengambil semua total populasi dengan alasan semua

responden sebagai pengelola teknologi informasi di RS Panti Wilasa Citarum untuk memastikan data berasal dari pihak yang memiliki otoritas dan pemahaman teknis mendalam mengenai tata kelola keamanan sistem informasi. Meskipun hal ini menyebabkan perspektif penilaian yang bersifat top-down dan hanya berfokus pada sisi manajerial serta teknis IT, dan belum mencakup persepsi atau kesadaran keamanan informasi dari pengguna akhir (end-users) seperti tenaga medis (dokter dan perawat) yang merupakan garda terdepan dalam penginputan data pasien pada sistem rekam medis elektronik.

Penelitian Fokus penelitian pada 7 area penilaian keamanan informasi berdasar Index KAMI versi 5.0 dari Badan Siber dan Sandi Negara (BSSN).



Gambar 1. Kerangka Kerja Penelitian

III. HASIL DAN PEMBAHASAN

Berdasarkan proses nilai tingkat kematangan keamanan informasi pada Rumah Sakit Panti Wilasa Citarum yang dibagi menjadi 7 area penilaian berdasar Indeks KAMI 5.0 dengan rician sebagai berikut :

A. Kategori Sistem Elektronik

Hasil penilaian pada area kategori sistem elektronik, RS Pantiwilasa Citarum telah menggunakan sistem elektronik dengan sekitar 500 pengguna dengan mengacu pada aturan akreditasi KARS. Dari 10 pertanyaan pada area ini diperoleh skor 20 dari 50 poin maksimal, sehingga masuk dalam kategori "Tinggi" dan hal ini menunjukkan bahwa Rumah Sakit mengarah pada ketergantungan "Tinggi" terhadap penggunaan sistem elektronik.

Hasil perolehan dari pengukuran area kategori sistem elektronik adalah 20 point, dengan tegori tingkat ketergantungan "Tinggi". Hal disebabkan beberapa pertanyaan dari 10 soal diperoleh skor terkecil yaitu pada alokasi total anggaran tahunan pengelolaan sistem elektronik. Selain itu karena masih menggunakan peraturan atau standar nasional.

Sementara hasil pengukuran keamanan informasi RS Panti Wilasa Citarum dengan menggunakan Indeks KAMI di dapatkan "Tinggi". Hhal ini sesuai dengan Permen Kominfo RI No.4 Tahun 2016 tentang Sistem Manajemen Keamanan Informasi Pasal 4 ayat (3) menyebutkan Sistem Elektronik yang Tinggi merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor atau daerah tertentu. Kemudian dari perolehan area yang tinggi di rumah sakit tersebut juga tertuang pada Bab III Pasal 7 ayat (2) Tentang Sistem Manajemen Keamanan Informasi menerangkan "Penyelenggara Sistem Elektronik Tinggi harus menerapkan standar SNI ISO/IEC 27001"[5]

B. Tata Kelola Keamanan Informasi

Tabel 1. Penilaian area Tata Kelola Keamanan Informasi

	Tingkat Kematangan II	Tingkat Kematangan III	Tingkat Kematangan IV	Total
Jumlah Pertanyaan	13	3	6	22
Skor pernyataan	33	8	0	41
Jawaban "Tidak Diterapkan"	0	0	0	0
Jawaban "Dalam Perencanaan"	3	2	2	7
Jawaban "Diterapkan Sebagian"	10	1	4	15
Jawaban "Diterapkan Secara Menyeluruh"	0	0	0	0
Tingkat Validitas Kematangan	I+	No	No	

Penilaian terhadap area Tata Kelola Keamanan Informasi diperoleh skor 41 poin dengan rincian 33 poin pada tingkat kematangan II yang sudah melewati batas skor minimum tingkat kematangan II dengan status I+, kemudian 8 poin pada skor tingkat kematangan III dengan status validitas "No". Sementara untuk tingkat kematangan IV diperoleh skor 0 dengan status validitas "No".

Dari 22 pertanyaan didapatkan 7 pertanyaan dengan jawaban "Dalam Perencanaan" dan 15 pertanyaan dengan jawaban "Diterapkan sebagian". Hal ini menyebabkan terjadinya validitas "No" karena dalam penilaian Indeks KAMI 5.0 jawaban paling rendah "diterapkan sebagian" maksimal sebanyak dua, maka dari itu jika melebihi atau lebih rendah dari yang telah ditetapkan validitas tingkat kematangan II+/III hingga III+/IV akan menghasilkan validitas menjadi "No". dengan demikian tingkat kematangan masuk dalam kategori I+.

Area Tata Kelola Keamanan Informasi didapatkan skor 41 poin diantaranya 33 poin dalam skor tingkat keamanan II sehingga mencapai skor yang lebih tinggi dari skor minimum tingkat kematangan II yaitu 12 poin, namun skor tingkat kematangan III hanya meraih 8 poin. hal ini tidak mencapai skor minimum 8 poin dengan validitas "No" tingkat kematangan III. Dengan demikian hasil penilaian pada area Tata Kelola Keamanan Informasi masuk dalam tingkat kematangan I+ yaitu masuk sebagai definisi kondisi awal, terkait dengan penyelenggaraan program peningkatan

kompetensi dari rumah sakit tidak rutin sehingga petugas melakukan secara mandiri dengan mencari informasi melalui internet, rumah sakit melaksanakan sosialisasi terkait satu user yang digunakan hanya satu akun saja pada setiap pertemuan sebagai program khusus untuk memastikan pencapaian tujuan dan sasaran dalam kepatuhan terhadap keamanan informasi. Selain itu standar ISO/IEC 27001 menetapkan batas minimum adalah tingkat III+ dengan sebutan "Terdefinisi dan Konsisten" maka dari itu Rumah Sakit Panti Wilasa Citarum yang ditentukan Indeks KAMI dengan tingkat kematangan I+ "Kondisi Awal" belum dapat mencapai batas minimum tersebut, hal ini dapat memberi dampak pada keamanan dan kepatuhan regulasi, serta Standar Sistem Manajemen Keamanan Informasi (SMKI).[15][17].

C. Pengelolaan Risiko Keamanan Informasi

Tabel 2. Penilaian Area Pengelolaan Risiko Keamanan Informasi

	Tingkat Kematangan II	Tingkat Kematangan III	Tingkat Kematangan IV	Tingkat Kematangan V	Total
Jumlah Pertanyaan	10	2	2	2	16
Skor pernyataan	21	6	8	0	35
Jawaban "Tidak Diterapkan"	0	0	0	0	0
Jawaban "Dalam Perencanaan"	2	1	1	0	4
Jawaban "Diterapkan Sebagian"	5	1	0	0	6
Jawaban "Diterapkan Secara Menyeluruh"	3	0	1	2	6
Tingkat Validitas Kematangan	II	No	No	No	

Dari 16 pertanyaan Pengelolaan Risiko Keamanan Informasi didapat beberapa jawaban yaitu 4 dijawab "Dalam Perencanaan", 6 jawaban "Diterapkan Sebagian", serta 6 sisanya "Diterapkan Secara Menyeluruh", diperoleh skor 35 poin diantaranya 21 poin yang sudah melebihi skor minimum dan pencapaian pada Skor tingkat kematangan II melalui status II , lalu tingkat kematangan III dengan skor 6 poin dengan validitas "No", selanjutnya tingkat kematangan IV dengan skor 8 poin yang disertai validitas "No", serta skor tingkat kematangan V didapat 0 poin validitas "No".

Keadaan ini menyebabkan terjadinya validitas "No" karena dalam penilaian Indeks KAMI 5.0 maksimal serta jawaban paling rendah adalah "Diterapkan Sebagian" sebanyak dua, maka dari itu jika melebihi atau lebih rendah dari yang telah ditetapkan validitas tingkat kematangan II+/III hingga IV+/V menjadi "No". Maka dari seluruh skor tersebut ditentukan tingkat kematangan II.

Penilaian terhadap area pengelolaan Risiko Keamanan Informasi didapatkan skor 35 poin dengan 21 poin pada tingkat kematangan II. Dengan kata lain sudah memenuhi skor minimum lalu melampaui poin skor pencapaian yang ditentukan, tetapi dalam skor tingkat kematangan III diperoleh skor 6 poin dengan validitas "No", maka ditentukan dengan status tingkat kematangan II didefiniskan "Penerapan Kerangka Kerja Dasar). Hal ini terjadi karena tidak terdapat dokumen pendukung yaitu kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan resmi, program kerja yang dilaksanakan untuk pengelolaan risiko membatasi akses internet sebagai antisipasi dalam keamanan informasi menggunakan antivirus berbayar dilengkapi dengan laporan harian terkait dengan upaya yang mengancam keamanan serta langsung di antisipasi secara otomatis. Berdasarkan ketentuan pada ISO/IEC 27001 pada tingkat kematangan minimal yaitu III+ yang didefinisikan "Terdefinisi dan Konsisten" untuk mencapai sertfikasi tersebut, maka dari itu Rumah Sakit Panti Wilasa Citarum dalam aspek Pengelolaan Risiko Keamanan Informasi belum dapat memenuhi target minimum karena hanya mendapatkan tingkat kematangan II "Penerapan Kerangka Kerja Dasar". Hal ini merupakan standarisasi yang diterbitkan International Security Systems sebagai persyaratan untuk mengelola keamanan informasi di suatu perusahaan maupun instansi.[15][17]

D. Kerangka Kerja Pengelolaan Keamanan Informasi

Tabel 2. Penilaian Area Kerangka Kerja Pengelolaan Keamanan Informasi

	Tingkat Kematangan II	Tingkat Kematangan III	Tingkat Kematangan IV	Tingkat Kematangan V	Total
Jumlah Pertanyaan	11	17	3	2	33
Skor pernyataan	23	38	0	0	61
Jawaban "Tidak Diterapkan"	1	0	0	1	2
Jawaban "Dalam Perencanaan"	3	6	0	0	9
Jawaban "Diterapkan Sebagian"	5	9	2	1	17
Jawaban "Diterapkan Secara Menyeluruh"	2	2	1	0	5
Tingkat Validitas Kematangan	**I+**	No	No	No	

Dari 32 pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi didapat total skor 61 poin diantaranya 23 poin pada tingkat kematangan II yang sudah melewati skor minimum sehingga status diberikan I+, selanjutnya 38 poin dengan validitas "No" di tingkat kematangan III, diikuti tingkat kematangan IV dan V skor 0 poin dengan validitas "No". Pada Kerangka Kerja Pengelolaan Keamanan

Informasi yang dibagi menjadi 2 bagian yaitu terkait penyusunan dan pengelolaan kebijakan & prosedur keamanan informasi, serta pengelolaan strategi dan program keamanan informasi terdapat jawaban keseluruhan yang diperoleh antara lain 2 jawaban "Tidak Dilakukan", 9 jawaban "Dalam Perencanaan", 17 jawaban "Diterapkan Sebagian" dan 5 jawaban "Diterapkan Secara Menyeluruh".

Hal ini disebabkan validitas "No" karena dalam penilaian Indeks KAMI 5.0 maksimal serta jawaban paling rendah adalah "diterapkan sebagian" sebanyak dua, maka dari itu jika melebihi atau lebih rendah dari yang telah ditetapkan validitas tingkat kematangan II+/III hingga IV+/V menjadi "No". Kemudian ditetapkan status kematangan adalah I+ berdasarkan Indeks Keamanan informasi.

Kerangka Kerja Pengelolaan Keamanan Informasi yang dilakukan di RS Panti Wilasa Citarum diperoleh skor 61 poin, tingkat kematangan I+ dengan sebutan "Kondisi Awal". Perolehan ini dengan rician 23 poin pada kematangan II, dimana poin ini melebihi skor minimum namun belum melewati skor pencapaiannya. selain itu 38 poin dalam skor tingkat kematangan III dengan mendapat validitas "No".

Perolehan kematangan tersebut karena dalam proses evaluasi yang dilaksanakan terdapat beberapa komponen yang berada di status "dalam perencanaan" dan "diterapkan sebagian". Tidak adanya dokumen yang mendukung dalam pelaksanaan, kebijakan dan prosedur evaluasi kelayakan secara berkala masih "dalam perencanaan" sehingga hal berpengaruh terhadap nilai yang dicapai. Ada konsekuensi dan langkah lanjutan yang diambil terhadap adanya pelanggaran. Sebagaimana perolehan Rumah Sakit Panti Wilasa Citarum dengan tingkat kematangan I+ disebut kondisi awal yang belum memenuhi ambang batas minimum sesuai dengan standar ISO/IEC27001 yaitu tingkat kematangan III+.[17] Tertuang pada Peraturan BSSN Republik Indonesia No 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital Pasal 2, pengaturan kerangka kerja bertujuan untuk memberikan pedoman bagi penyelenggara dalam pelindungan infrastruktur informasi vital serta menjadi acuan bagi Lembaga dalam menyusun dan menetapkan peta jalan pada tiap sektor.[17] Selain itu berdampak juga pada ancaman keamanan informasi seperti kegiatan operasional. Hal ini tertera pada Annex 5 tentang Organization Controls yang membahas mengenai penentuan kebijakan keamanan informasi[18]

E. Pengelolaan Aset Keamanan Informasi

Tabel 3. Penilaian Area Pengelolaan Aset Keamanan Informasi

	Tingkat Kematangan II	Tingkat Kematangan III	Total
Jumlah Pertanyaan	32	21	53
Skor pernyataan	98	78	176
Jawaban "Tidak Diterapkan"	0	0	0
Jawaban "Dalam Perencanaan"	0	0	0
Jawaban "Diterapkan Sebagian"	11	6	17
Jawaban "Diterapkan Secara Menyeluruh"	21	4	25
Jawaban "Tidak Berlaku/Relevan"	0	11	11
Tingkat Validitas Kematangan	II	No	

Dalam Pengelolaan Aset Keamanan Informasi ini terdapat 53 pertanyaan yang dibagi menjadi 3 kategori yaitu pengelolaan aset informasi, pengamanan layanan infrastruktur awan (cloud service) serta pengamanan fisik berdasarkan Indeks Keamanan informasi, diperoleh total skor 176 diantaranya 98 poin pada tingkat kematangan II yang sudah melewati skor pencapaian yang ditetapkan dengan status II, kemudian skor tingkat kematangan III dengan 78 poin namun validitas "No".

Perihal ini yang menyebabkan terjadinya validitas "No" karena dalam penilaian Indeks KAMI 5.0 maksimal serta jawaban paling rendah adalah "Diterapkan Sebagian" sebanyak dua, maka dari itu jika melebihi atau lebih rendah dari yang telah ditetapkan validitas tingkat kematangan II+/III hingga IV+/V menjadi "No". sehingga ditentukan menjadi tingkat kematangan II.

Pada area Pengelolaan Aset Informasi didapatkan skor 176 poin, dengan rincian 98 poin pada skor tingkat kematangan II yang melampaui skor minimum yaitu 39 poin serta skor pencapaian 88 poin, selain itu skor 78 poin diraih dalam tingkat kematangan III namun dengan validitas "No". Rumah Sakit sendiri memiliki tata tertib penggunaan internet dengan membatasi akses agar tidak mengggganggu fokus dalam bekerja dan memblokir otomatis web yang tidak dikenal. *Back-up* dilaksanakan 2 kali dalam setiap hari, setiap pengguna sudah memiliki *username* dan *password* sendiri dengan sanksi terberat dikeluarkan jika melanggar kebijakan tersebut. Untuk penilaian terhadap pelaksanaan layanan penyimpanan *cloud* masih "**dalam perencanaan"**. Hal ini masih belum sesuai dengan instrument Indeks KAMI. Menurut Arfan Bakhtian dkk, Layanan cloud sebaiknya menggunakan lebih dari satu sebagai cadangan, sehingga memiliki lebih dari satu penyimpanan ketika mengalami kendala.[14] Karena hal ini pada tingkat kematangan II. dianggap masih belum memenuhi standar batas minimum yang ditetapkan oleh ISO/IEC 27001 sehingga pada tingkat kematangan III+ terdefinisi dan konsisten, tidak tersetifikasinya dari ISO/IEC27001 sebagai dampak tidak tidak tercapainya ambang batas minimum yang telah ditentukan kemudian kesulitan dalam memenuhi persyaratan hukum dan regulasi(ISO). Sesuai dengan yang tertera pada Annex 5 mengenai *Organization Controls* yang menyebutkan

tentang penyimpanan aset-aset yang dimiliki.[13][17]

F. Teknologi dan Keamanan Informasi

Tabel 4. Penilaian Area Teknologi dan Keamanan Informasi

	Tingkat Kematangan II	Tingkat Kematangan III	Tingkat Kematangan IV	Total
Jumlah Pertanyaan	14	18	3	35
Skor pernyataan	33	89	9	131
Jawaban "Tidak Diterapkan"	0	0	1	1
Jawaban "Dalam Perencanaan"	0	1	0	1
Jawaban "Diterapkan Sebagian"	9	12	1	22
Jawaban "Diterapkan Secara Menyeluruh"	5	5	1	11
Tingkat Validitas Kematangan	II	No	No	

Pada jawaban dari total 35 pertanyaan Teknologi dan Keamanan Informasi diperoleh skor 131 poin diantaranya 33 poin terhadap tingkat kematangan II dengan status II dikarenakan sudah melampaui skor pencapaian, lalu pada tingkat kematangan III didapat 89 poin namun validitas "No", kemudian skor sebanyak 9 poin dari tingkat kematangan IV tetapi validitas "No". Terjadinya validitas "No" karena dalam penilaian Indeks KAMI 5.0 maksimal serta jawaban paling rendah adalah "Diterapkan Sebagian" sebanyak dua, maka dari itu jika melebihi atau lebih rendah dari yang telah ditetapkan validitas tingkat kematangan II+/III hingga IV+/V menjadi "No". sehingga ditetapkan tingkat kematangannya adalah II. Penilaian pada area teknologi dan keamanan informasi perolehan skor 131 poin terdiri atas 33 poin melampaui skor minimum dengan pencapaian tingkat kematangan II, 89 poin dalam tingkat kematangan III dengan validitas "No". sementara skor tingkat kematangan IV terdapat 9 poin dengan validitas "No".

Maka dari itu dari seluruh total yang ada ditentukan tingkat kematangan adalah II, hal yang paling mempengaruhi yaitu masih belum "**diterapkan secara menyeluruh**" mengenai keluarnya secara otomatis (*timeouts*) jika tidak terdeteksi pergerakan mouse pada komputer. Hal ini diartikan masih berada dibawah ambang batas minimal yaitu III+ (terdefinisi dan konsisten). Jika tidak memenuhi syarat sesuai maka belum dapat tersertifikasi ISO 27001.[17] Tertera pada Annex 7 *People Controls* mengenai kontrol fisik pada area maupun peralatan yang dimiliki seperti membatasi area serta keamanan informasi dalam media penyimpanan atau pembuangan *storage*, dan Annex 8 tentang *Technological Controls* mulai dari upaya pengamanan data dengan bentuk backup serta pembatasan akses[18].

G. Perlindungan Data Pribadi

Tabel 5. Penilaian Area Perlindungan Data Pribadi

	Tingkat Kematangan II	Tingkat Kematangan III	Total
Jumlah Pertanyaan	6	10	16
Skor pernyataan	14	46	60
Jawaban "Tidak Diterapkan"	0	0	0
Jawaban "Dalam Perencanaan"	1	1	2
Jawaban "Diterapkan Sebagian"	5	5	10
Jawaban "Diterapkan Secara Menyeluruh"	4	0	4
Tingkat Validitas Kematangan	**I+**	No	

Terdapat 16 pertanyaan pada Perlindungan Data Pribadi dengan perolehan total skor 60 poin diantaranya 14 poin di tingkat kematangan II yang sudah melewati skor minimum yang kemudian diberikan status I+, kemudian 46 poin pada skor tingkat kematangan III dengan validitas "No", terkait dengan perlindungan data pribadi dengan jawaban yang telah diisi oleh responden yaitu terdapat 2 jawaban "Dalam Perencanaan", 10 jawaban dalam "Diterapkan Sebagian", serta 4 jawaban "Diterapkan Secara Menyeluruh. Terjadinya validitas "No" dikarenakan dalam penilaian Indeks KAMI 5.0 maksimal serta jawaban paling rendah adalah "Diterapkan Sebagian" sebanyak dua, maka dari itu jika melebihi atau lebih rendah dari yang telah ditetapkan validitas tingkat kematangan II+/III hingga IV+/V menjadi "No". sehingga ditentukan status akhir adalah tingkat kematangan I+. Penilaian pada area Perlindungan Data Pribadi diperoleh skor 60 poin, 14 poin melewati skor minimum namun belum melampaui skor pencapaian tingkat kematangan II. Selanjutnya skor tingkat kematangan III didapat 46 poin dengan validitas "No", maka dari itu ditetapkan status Kematangan I+.

Masih belum terdapat fungsi atau unit yang secara spesifik memiliki wewenang dan tanggung jawab dalam Pelindung Data Pribadi. ketika terjadi pelanggaran terkait data pribadi misalnya perubahan tanpa izin, maka terdapat sanksi dengan paling berat dikeluarkan dari RS. Hal ini sudah sesuai dengan UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi di Pasal 60 Poin ke-3 yang berbunyi "Menjatuhkan sanksi administratif atas pelanggaran Perlindungan Data Pribadi yang dilakukan Pengendali Data Pribadi/atau Prosesor Data Pribadi".[5]. Oleh karena itu, setelah Indeks KAMI menentukan tingkat kematangan II pada Rumah Sakit Panti Wilasa Citarum yang mana masih belum memenuhi batas minimal yang

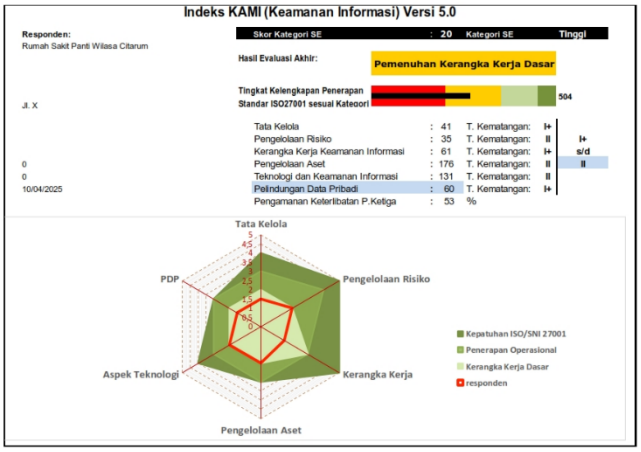
telah ditetapkan ISO/IEC27001 yaitu tingkat kematangan III+[17].

H. Pengamanan Keterlibatan Pihak Ketiga

Berdasarkan jawaban yang diisi oleh responden dari 27 pertanyaan Pengamanan Keterlibatan Pihak Ketiga, ditemukan 5 jawaban "tidak dilakukan", 3 jawaban "dalam perencanaan", 17 jawaban "dalam penerapan/diterapkan sebagian", serta 2 jawaban "diterapkan secara menyeluruh". Dari hasil jawaban tersebut didapat persentase yaitu 53% yang berdasarkan dari Indeks KAMI. Penilaian pada area keterlibatan pihak ketiga diperoleh skor 53%. Hal ini dikarenakan masih banyak jawaban "Tidak Dilakukan", "Dalam Perencanaan", dan "Diterapkan Sebagian". Terutama pada penetapkan peran tanggung jawab mengenai audit aspek keamanan informasi oleh pihak ketiga. Perlu ditingkatkan untuk mencapai persentase pengamanan 100%. Hal ini tertuang pada Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 8 Tahun 2023 Tentang Kerangka Kerja Perlindungan Infrastruktur Informasi Vital Pasal 7 ayat (5) di subkategori mengenai pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya.[17]

I. Indeks Penilaian KAMI

Berdasarkan data dari keseluruhan variabel dengan pengukuran Indeks KAMI pada bagian *dashboard*, hasil evaluasi akhir tingkat kesiapan dan kematangan keamanan informasi menunjukkan bahwa total skor yaitu 504 poin dengan skor Kategori Sistem Elektronik didapat 20 poin dengan kategori "Tinggi" lalu ditetapkan skor keseluruhan sesuai dengan kategori tersebut. Setiap variabel mulai dari Tata Kelola dengan skor 41 poin ditentukan tingkat kematangan I+, Pengelolaan Risiko 35 poin dengan tingkat kematangan II, Kerangka Kerja Keamanan Informasi 61 poin tingkat kematangan I+, Pengelolaan Aset 176 poin tingkat kematangan II, Teknologi dan Keamanan Informasi 131 poin tingkat kematangan II, setelah itu Perlindungan Data Pribadi perolehan 60 poin tingkat kematangan I+ serta Pengamanan Keterlibatan Pihak Ketiga persentase 53%. Dari seluruh variabel didapat tingkat kematangan II menjadi tingkat tertinggi yang diraih dengan 3 variabel terendah yaitu Tata Kelola Keamanan Informasi, Kerangka Kerja Keamanan Informasi dan Perlindungan Data Pribadi dengan meraih tingkat kematangan I+, sehingga rumah sakit dikategorikan "Pemenuhan Kerangka Kerja Dasar".



Gambar 2. Hasil Penilaian Indeks KAMI
Sumber : Data Primer, 2025

Dari penelitian yang dilaksanakan di Rumah Sakit Panti Wilasa Citarum dengan hasil penelitian pada Gambar 2 diperoleh evaluasi akhir dari dashboard Indeks KAMI yaitu "Pemenuhan Kerangka Kerja Dasar" dengan bar berhenti di area kuning hal ini karena ditentukan dari kategori Sistem Elektronik yaitu "Tinggi" dengan skor keseluruhan adalah 504. Hasil evaluasi akhir tersebut masuk ke tingkat II yang diartikan sudah diterapkannya pengamanan walaupun hanya ada beberapa di area teknis serta masih belum ada keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

Berdasar skor diatas, Rumah Sakit Panti Wilasa Citarum baru mencapai status tingkat kematangan II sehingga masih belum dapat meraih tingkat kematangan III+ sebagai syarat kesiapan sertifikasi ISO27001 dalam Standar Manajemen Keamanan Informasi (SMKI). Menurut aturan Permenkominfo jika kategori sistem elektronik "Tinggi" harus menerapkan standar SNI ISO 27001, serta dapat mempengaruhi pencapaian penilaian standar mutu Rumah Sakit MRMIK 13 dari KARS tentang regulasi penyelenggaraan teknologi informasi kesehatan.[19] Dari hal tersebut juga dapat mendukung transformasi teknologi kesehatan terhadap pengembangan sistem data kesehatan dalam mewujudkan program SatuSehat[20]

Temuan tingkat kematangan digital yang masih rendah dengan kategori **"Pemenuhan Kerangka Kerja Dasar" (Tingkat Kematangan II)** dan total skor 504 poin. Terdapat **kesenjangan kritis** antara tingkat ketergantungan terhadap sistem elektronik yang berkategori **"Tinggi" (skor 20)** dengan kesiapan kerangka kerja yang masih berada pada level **Kondisi Awal (I+)** untuk area Tata Kelola, Kerangka Kerja, dan Perlindungan Data Pribadi.

Secara kritis, rendahnya tingkat kematangan ini disebabkan oleh banyaknya jawaban **"Diterapkan Sebagian" dan "Dalam Perencanaan"**, yang mengakibatkan status validitas menjadi **"No"** pada berbagai parameter Indeks KAMI 5.0. Hal ini menunjukkan bahwa meskipun rumah sakit telah memiliki kesadaran akan pentingnya keamanan informasi, namun implementasinya masih bersifat **insidental dan bergantung pada motivasi**

individu pelaksana, bukan berdasarkan sistem yang terstandarisasi dan terdokumentasi secara formal. Tanpa dokumen kebijakan yang resmi dan program pelatihan yang rutin, dikhawatirkan rumah sakit berpotensi berada pada risiko tinggi terhadap ancaman siber seperti *ransomware* dan kebocoran data yang dapat melumpuhkan layanan operasional.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil penilaian menggunakan Indeks KAMI 5.0, Kategori Sistem Elektronik termasuk dalam klasifikasi "Tinggi" dengan nilai 20 poin. Dengan hasil kesiapan 504 poin tergolong ke tingkat kematagan II sehingga belum mencapai kualifikasi sesuai dengan standar ISO/IEC 27001:2022. Sebagian besar seluruh aspek masih berada pada tingkat kematangan I+ hingga II ditunjukan masih belum terdokumentasi secara formal mengenai kerangka kerja keamanan informasi, kemudian masih banyaknya penerapan Sebagian dan dalam perencanaan sehingga belum efektif dan konsisten dan dapat mempengaruhi penilaian akreditasi rumah sakit yaitu KARS khususnya standar MRMIK13 yang mengatur penyelenggaraan teknologi informasi kesehatan dan standar ISO/IEC 27001.

Rekomendasi untuk Rumah Sakit, perlu melakukan formalisasi dokumen dan kebijakan dengan menyusun dan mengesahkan kerangka kerja pengelolaan risiko serta kebijakan keamanan informasi secara tertulis untuk mengubah status "Dalam Perencanaan" menjadi "Diterapkan Secara Menyeluruh". Peningkatan Tata Kelola dan SDM dengan optimalisasi program pelatihan dan sosialisasi keamanan informasi secara rutin bagi petugas agar kepatuhan tidak hanya bergantung pada inisiatif mandiri. Segera membentuk unit atau fungsi khusus yang bertanggung jawab atas perlindungan data pribadi pasien sesuai amanat UU PDP dan Permenkes 24/2022. Penguatan kontrol teknis dengan mengaktifkan fitur *timeout* otomatis pada komputer layanan dan menyediakan layanan penyimpanan *cloud* lebih dari satu tempat untuk memastikan ketersediaan data (*backup*) yang lebih tangguh. RS perlu melakukan evaluasi berkala dengan melaksanakan pengukuran mandiri menggunakan Indeks KAMI secara berkala, minimal 2 kali dalam setahun, untuk memantau kemajuan menuju standar ISO/IEC 27001

DAFTAR PUSTAKA

[1] Amran, Rika, Apriyani, Anisah, Dewi, and Purnama Nadia, "Peran Penting Kelengkapan Rekam Medik di Rumah Sakit," *Baiturrahmah Med. J.*, vol. 1, no. 1, pp. 69–76, Sep. 2021.

[2] Kesehatan Kementerian, *Permenkes Nomor 24 Tahun 2022*. Indonesia, 2022. [Online]. Available: www.peraturan.go.id

[3] Kementerian Kesehatan RI, "Situasi dan Tantangan Kesehatan Digital Indonesia 1 CETAK BIRU STRATEGI TRANSFORMASI DIGITAL KESEHATAN 2024," 2021. [Online]. Available: https://www.kemkes.go.id/

[4] M. Amin *et al.*, "Implementasi Rekam Medik Elektronik: Sebuah Studi Kualitatif," vol. 8, no. 1, pp. 430–442, 2021, [Online]. Available: http://jurnal.mdp.ac.id

[5] M. K. dan I. RI, *PERLINDUNGAN DATA PRIBADI DALAM SISTEM ELEKTRONIK*. 2016.

[6] E. Tri Ardianto, L. Nurjanah, P. Studi Manajemen Informasi Kesehatan, J. Kesehatan, and P. Negeri Jember, "ANALISIS ASPEK KEAMANAN DATA PASIEN DALAM IMPLEMENTASI REKAM MEDIS ELEKTRONIK DI RUMAH SAKIT X," vol. 3, no. 2, pp. 2829–4777, 2024, doi: 10.47134/rammik.v3i2.54.

[7] L. R. Rimbun, E. L. D. Marisi, and T. Hidayati, "Tantangan Keamanan Data dalam Telemedicine Implikasi Terhadap Privasi Pasien dan Kepercayaan dalam Layanan Kesehatan Digital: Systematic Review," *MAHESA Malahayati Heal. Student J.*, vol. 4, no. 10, pp. 4398–4415, 2024, doi: 10.33024/mahesa.v4i10.15391.

[8] BBC News, "Data eHAC milik 1,3 juta penggunanya dilaporkan bocor, 'keamanan data tidak prioritas,'" 2021. https://www.bbc.com/indonesia/indonesia-58393345

[9] Tempo, "Data Pasien Bocor, Ahli Siber Ajari Berlindung dari Ransomware dan Extortionware," 2022. https://www.tempo.co/digital/data-pasien-bocor-ahl

[10] Diva Rizky Amanda Tiorentap and Hosizah, "Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronikdi Klinik Medical Check-Up MP," *Pros. 4 SENWODIPA*, pp. 53–66, Nov. 2020.

[11] C. Chazar, "STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005," *J. Inf.*, vol. VII, no. 1, pp. 58–82, 2015, [Online]. Available: https://informasi.stmik-im.ac.id/wp-content/uploads/2016/05/03-Haryoso-Wicaksono.pdf

[12] Haeruddin and A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6)," *Conf. Manag. Business, Innov. Educ. Soc. Sci.*, vol. 1, no. 1, pp. 508–515, Feb. 2021, [Online]. Available: https://journal.uib.ac.id/index.php/combines

[13] I. G. P. K. Juliharta, T. K. Werthi, and L. P. N. S. P. A. Astawa, "PENILAIAN KEAMANAN INFORMASI E-GOVERNMENT MENGGUNAKAN INDEX KEAMANAN INFORMASI (KAMI) 4.0," *J. Teknol. Inf. dan Komput.*, vol. 6, no. 2, pp. 238–244, Jan. 2020, [Online]. Available: https://bssn.go.id/mengenali-serangan-siber-

[14] A. Bakhtiar and F. Salsabila Hidayat, "EVALUASI

SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH," 2023.

[15] Bagaskara, "ISO 27001:2022 – Sistem Manajemen Keamanan Informasi." https://mutucertification.com/sertifikasi-iso-27001-2022/

[16] Sugiyono, *Metodelogi Penelitian Kuantitatif dan Kualitatif Dan R&D*. Bandung: Alfabeta, 2019.

[17] Badan Siber dan Sandi Negara, *KERANGKA KERJA PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL*. 2023.

[18] Bizplus, "TRANSISI ISO 27001:2013 MENUJU ISO 27001:2022." https://bizplus.id/Transisi-Iso-27001-2013-Menuju-Iso-27001-2022/

[19] Komisi Akreditasi RS, *Instrumen Survei Akreditasi KARS sesuai Standar Akreditasi RS Kemkes RI 2022*. Jakarta, 2022.

[20] K. RI, "Cetak Biru Situasi dan Tantangan Kesehatan Digital Kesehatan 2024," 2021.