Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

Penerapan Kerangka Kerja Keamanan Informasi di Rumah Sakit: Tinjauan Literatur Sistematis

Iin Mardiyana[1*], Eva Hariyanti[2], Novia Nurhasanah Arrasyid[3], Arum Tiyas Handayani[4], Kharristantie Sekarlangit Suryadewi[5], Fildzah Akhlaqulkarimah[6], Naurah Hedy Pramiyas[7]
Program Studi Sistem Informasi, Universitas Airlangga, Surabaya, Indonesia
*e-mail *Corresponding Author*: iin.mardiyana-2020@fst.unair.ac.id

Abstract

Hospitals are organizations that manage vital and complex data such as medical information and patient personal data that must be protected. The purpose of this paper is to analyze how IT security standards are implemented in hospitals in order to measure the level of maturity. Systematic Literature Review is the method used in this research. Of the 25 hospitals discussed in this paper, there are 3 standards and 8 models applied, namely ISO 27000 Family, COBIT, NIST, HDM, C2M2, HISMM, MD3M, PCMM, AHIMA, IMA and Fuzzy-ANP-TOPSIS integrated model. It was found that the implementation of models and standards for IT security has the same pattern, namely data collection, measuring the level of IT maturity and then providing recommendations for improvements based on measuring the level of IT maturity. While the difference between one model and another is in the domain, maturity attributes and the level or level of maturity used.
Keywords: *IT security standards; IT security model; Maturity level; Hospital*

Abstrak

Rumah sakit merupakan organisasi yang mengelola data vital dan kompleks seperti informasi medis dan data pribadi pasien yang harus dilindungi. Tujuan utama penulisan paper ini adalah untuk menganalisis bagaimana standar keamanan TI diimplementasikan di rumah sakit dalam rangka mengukur level kematangan. Systematic Literature Review adalah metode yang digunakan dalam penelitian ini. Dari 25 rumah sakit yang dibahas pada paper ini, terdapat 3 standar dan 8 model yang diterapkan, yaitu ISO 27000 Family, COBIT, NIST, HDM, C2M2, HISMM, MD3M, PCMM, AHIMA, IMA dan model terpadu Fuzzy-ANP-TOPSIS. Didapatkan temuan bahwa implementasi model maupun standar keamanan TI memiliki pola yang sama yaitu pengumpulan data, mengukur tingkat kematangan TI selanjutnya memberikan rekomendasi perbaikan berdasarkan pengukuran tingkat kematangan TI. Sedangkan perbedaan antara model yang satu dengan yang lainnya adalah pada domain, atribut kematangan dan level atau tingkat kematangan yang digunakan.
Kata kunci: *Standar keamanan TI; Model keamanan TI; Level kematangan; Rumah sakit*

1. Pendahuluan

Rumah sakit menjadi organisasi yang tidak tertinggal dalam menerapkan teknologi informasi untuk menyimpan dan mengelola data yang vital dan kompleks seperti informasi medis, data pribadi pasien, dan informasi keuangan. Namun, layaknya entitas yang menerapkan teknologi informasi lainnya, keamanan selalu menjadi tantangan agar data dan informasi tetap utuh, tersedia, akurat, dan rahasia [1]. Permasalahan keamanan data juga dapat mengintai rumah sakit dan diperlukan tindakan untuk melindungi organisasi serta pasien dari berbagai kasus akibat pencurian data. Dilansir dari *Fortified Health Security* dan *US Department of Health and Human Services*, telah terjadi 337 pelanggaran pada tahun 2022 di rumah sakit yang berpotensi mengancam keamanan 19.992.810 orang [2]. Tingginya statistik pencurian informasi kesehatan ini disebabkan bukan karena hebatnya peretas, namun akibat kelalaian organisasi, keamanan yang lemah, dan kurangnya kesadaran pegawai terhadap pentingnya keamanan data [3].

Dalam memperkuat kontrol keamanan informasi rumah sakit, diperlukan suatu tata kelola dan standar untuk menganalisis status keamanan sehingga organisasi dapat mengetahui

letak kerentanan dalam sistem, aset, dan manusia, untuk kemudian dapat diperbaiki dan ditingkatkan. Berbeda dengan organisasi lainnya, rumah sakit memerlukan analisis lebih dalam dan dikarenakan rumah sakit merawat pasien sekaligus mendidik tenaga kesehatan, memiliki proses bisnis yang rumit, serta membawahi berbagai tenaga kerja yang beragam [4]. Banyak studi yang telah berfokus pada bidang ini dengan mengambil studi kasus secara langsung di rumah sakit dengan menerapkan standar atau *framework* keamanan informasi. Namun, belum ada peninjauan lebih detail tentang bagaimana standar keamanan tersebut diimplementasikan di berbagai rumah sakit untuk mengukur level kematangan sistem informasi.

Penelitian [5] telah meninjau berbagai penelitian manajemen risiko keamanan untuk mengidentifikasi standar dan teknik yang paling relevan untuk penilaian risiko keamanan .Penelitian tersebut berfokus pada *multi criteria decision making* yang menganalisis pengelolaan keamanan dengan batasan informasi, sumber daya, dan waktu menggunakan penilaian kuantitatif. Penelitian tersebut tidak membahas implementasi standar keamanan di sistem informasi rumah sakit secara umum dan tidak mencakup area manajemen. Standar keamanan informasi seperti COBIT dan ISO dapat memberikan pandangan yang lebih luas beserta panduan dan *framework* untuk mengelola keamanan informasi dan menyediakan kerangka penilaian status kematangan.

Dengan melakukan tinjauan sistematis, penelitian ini bertujuan untuk menganalisis bagaimana standar keamanan diimplementasikan di rumah sakit dalam rangka mengukur level kematangan, berdasarkan berbagai studi kasus yang telah dilakukan sebelumnya. Arah penelitian ini berfokus pada implementasi dan tahapan penerapan standar keamanan seperti COBIT, ISO, NIST, dan model lain, serta karakteristik pengukuran level kematangan pada masing-masing rumah sakit.

2. Tinjauan Pustaka

Beberapa penelitian yang berkaitan dengan implementasi tata kelola teknologi informasi pada sistem informasi di rumah sakit telah dilakukan. Penelitian [6] mengadopsi model penerimaan pengguna *Hospital Information System* (HIS) yang berfokus pada karakteristik manusia, teknologi, dan organisasi untuk mendukung program *e Health* pemerintah. Penelitian ini menggunakan pendekatan kualitatif dan kuantitatif dengan studi kasus pada empat rumah sakit swasta dan tiga rumah sakit milik pemerintah yang merupakan rumah sakit umum di Indonesia. Berdasarkan hasil diskusi penelitian, model HIS paling cocok untuk rumah sakit milik pemerintah serta manajemen rumah sakit dan pengembang TI harus lebih memahami faktor non-teknologi untuk merencanakan implementasi HIS dengan lebih baik.

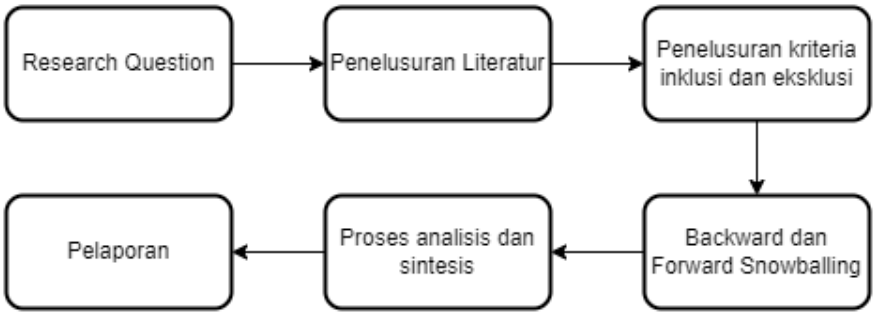
Sedangkan penelitian [7] telah melakukan evaluasi terhadap perbaikan dari segi tata kelola TI pada Rumah Sakit Rachmi Dewi Gresik. Kerangka model yang digunakan adalah COBIT 5 untuk menganalisis permasalahan yang ada yaitu kurangnya kesadaran dari manajemen rumah sakit tentang pentingnya tata kelola TI dan peraturan atau kebijakan pemerintah, sehingga pelaksanaan administrasi rumah sakit terhambat atau tidak optimal. Hasil penelitian ini menunjukkan bahwa Rumah Sakit Rachmi Dewi Gresik telah mencapai tingkat maturitas pada level 1 (satu) yang dapat disimpulkan bahwa proses *IT governance* perlu ditingkatkan.

Penelitian *Systematic Literature Review* [8] bertujuan untuk mengidentifikasi dan membandingkan model kematangan untuk manajemen sistem dan teknologi informasi (IST) dalam layanan kesehatan. Setiap model maturitas menjelaskan metodologi pengembangan dan validasi serta ruang lingkup, tahapan dan karakteristik berdasarkan dimensi atau faktor pengaruhnya. Penelitian dilakukan berdasarkan kata kunci yang telah ditetapkan seperti "*Maturity Model*" dan "*Health*" atau "*Maturity Model*" dan "*Hospital*". Pencarian jurnal dilakukan pada *platform web* utama literatur ilmiah AIS Electronic Library, ISI Web of Knowledge, SCOPUS, Springer, Elsevier/Science Direct dan IEEE Computer Society Digital Library. Kemudian dianalisis dan diidentifikasi kesamaan referensi yang berkaitan dengan topik jurnal dan kata kunci pencarian. Setelah diidentifikasi, menurut [9] perlu menentukan kriteria kualitas untuk pemilihan studi yang cocok dalam penelitian. Namun dalam menentukan kriteria kualitas pada penelitian dengan pendekatan kualitatif merupakan langkah yang sulit. Sehingga pencarian referensi dilakukan dengan memasukkan kata kunci pencarian berdasarkan topik penelitian dalam Bahasa Inggris. Penelitian tersebut menghasilkan level maturitas sistem informasi menggunakan berbagai model dan standar yang diusulkan, serta kebutuhan untuk mengembangkan model kematangan berdasarkan pendekatan holistik.

Berbeda dengan penelitian [6] yang hanya mengimplementasikan salah satu *framework* layanan TI sistem informasi untuk tujuan *digitalisasi* pada instansi rumah sakit, penelitian yang dilakukan saat ini memiliki kesamaan dengan penelitian [7] dan [8] yang berfokus pada manajemen sistem dan teknologi informasi (IST) dalam layanan kesehatan. Dengan perbedaan terletak pada tujuan penelitian, yaitu penelitian yang saat ini mengidentifikasi dan menganalisis implementasi standar keamanan TI dalam mengukur tingkat kematangan sistem informasi Rumah Sakit. Perbedaan juga terletak pada kata kunci untuk mencari referensi yaitu "Standar Keamanan TI di Rumah Sakit" dan "Tingkat Kematangan TI".

3. Metodologi

Metode yang digunakan dalam penelitian ini adalah *Systematic Literature Review* (SLR). SLR didefinisikan sebagai metode yang bertujuan untuk menemukan dan mensintesis secara komprehensif hasil penelitian atas pertanyaan spesifik secara terorganisir, transparan dan berulang pada setiap proses [10]. Gambar 1 menunjukkan tahapan SLR pada penelitian ini.



Gambar 1. Tahapan penelitian menggunakan metode SLR

A. *Research Question*

Tahap ini dilakukan dengan membuat pertanyaan yang disesuaikan dengan topik yang sudah dipilih. Adapun pertanyaan dari penelitian ini adalah:
RQ : Bagaimana Implementasi Standar Keamanan TI Untuk Mengukur Kematangan Sistem Informasi Rumah Sakit?

B. Penelusuran Literatur

Jurnal pada penelitian ini bersumber dari IEEE, Google Scholar, Scopus, SpringerLink, SINTA, Web Of Science, ScienceDirect dan PubMed. Proses penelusuran artikel dilakukan dengan mengidentifikasi kata kunci beserta kategorinya. Kumpulan kategori dan kata kunci yang diidentifikasi terdapat pada Tabel 1 berikut:

Tabel 1. Kategori dan Keyword Penelusuran Literatur

Kategori	Keyword
Standar Keamanan TI di Rumah Sakit	ISO, COBIT, NIST, ETSI, NERC
Tingkat Kematangan TI	Tingkat kematangan Keamanan TI, Tingkat kematangan Keamanan Teknologi Informasi

Berdasarkan kategori dan kata kunci yang telah diidentifikasi, untuk melakukan pencarian dihubungkan antara kategori dan kata kunci satu dengan lainnya. Penggabungan kategori dan kata kunci untuk melakukan pencarian adalah sebagai berikut pertama, Standar Keamanan TI di Rumah Sakit DAN "ISO" ATAU "COBIT " ATAU "NIST" ATAU "ETSI" ATAU "NERC". Kedua, ("Tingkat Kematangan TI" ATAU "Tingkat Kematangan Teknologi Informasi") DAN (Standar Keamanan TI di Rumah Sakit DAN "ISO" ATAU "COBIT " ATAU "NIST" ATAU "ETSI" ATAU "NERC"). Ketiga, penggunaan kategori dan kata kunci untuk mencari artikel yang dibutuhkan dalam format bahasa inggris dapat diterjemahkan kedalam bahasa inggris seperti *IT Security Standards in Hospitals AND "ISO" OR "COBIT" OR "NIST" OR "ETSI" OR "NERC"* dan

juga (*"IT Maturity Level" OR "Information Technology Maturity Level") AND (IT Security Standards in Hospitals AND "ISO" OR "COBIT " OR "NIST" OR "ETSI" OR "NERC"*). Pada tahap ini, didapatkan 73 studi pada pencarian berdasarkan kata kunci terkait.

C. Penelusuran Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi untuk memilih studi yang relevan dengan tujuan penelitian. Analisis dilakukan menggunakan abstrak, judul dan juga kata kunci untuk mengevaluasi artikel yang sesuai.

Kriteria Inklusi : Studi adalah (I1) artikel dalam bahasa Inggris dan Indonesia, (I2) diterbitkan dalam rentang waktu 2013-2023, (I3) artikel berkaitan dengan penerapan standar keamanan TI untuk mengukur tingkat kematangan sistem informasi di Rumah Sakit, pada artikel memuat (I4) Standar keamanan TI yang digunakan meliputi ISO, COBIT, NIST, ETSI, NERC, dan standar lain yang berkaitan dengan keamanan teknologi informasi, dan (I5) artikel bersumber dari IEEE, Google Scholar, Scopus, SpringerLink, SINTA, Web Of Science, ScienceDirect, dan PubMed.

Kriteria Eksklusi : (E1) Makalah pendek, makalah simposium doktoral, proposal, catatan kuliah, editorial, komentar, tutorial, dan makalah ulasan, (E2) diterbitkan dalam jurnal atau konferensi predator yang dapat dilihat melalui situs Beall's List – of Potential Predatory Journals and Publishers (beallslist.net) , dan (E3) artikel tidak dalam bentuk full text (tidak dapat diakses penuh).

Dari proses seleksi berdasarkan kriteria inklusi dan eksklusi, didapatkan 21 literatur terpilih yang digunakan sebagai artikel utama. Selanjutnya, artikel utama tersebut dilakukan tinjauan untuk mengidentifikasi implementasi standar keamanan teknologi informasi dalam mengukur kematangan sistem informasi rumah sakit.

D. *Backward dan Forward Snowballing*

Penelitian ini menerapkan teknik *forward* dan *backward snowballing* dengan tujuan mendapatkan hasil studi artikel yang komprehensif dan dapat mengurangi risiko kehilangan studi yang relevan untuk menjawab *research question* [11]. Pada tahap ini, didapatkan 4 literatur terpilih sehingga terdapat 25 artikel yang digunakan sebagai artikel utama.

E. Proses Analisis dan Sintesis

Literatur yang menjadi artikel utama akan dilakukan analisis dan sintesis sesuai dengan topik yang ditentukan sehingga dapat diketahui implementasi standar keamanan TI pada sistem informasi rumah sakit. Terdapat 3 standar dan 8 model keamanan TI yang akan dianalisis, diantaranya *ISO 27000 Family, COBIT, NIST, HDM, C2M2, HISMM, MD3M, PCMM, AHIMA, IMA dan model terpadu Fuzzy-ANP-TOPSIS.*

F. Pelaporan

Tahap pelaporan digunakan untuk memberikan gambaran secara keseluruhan terkait hasil analisis dan sintesis pada literatur yang sesuai dengan kriteria inklusi dan eksklusi. Hasil pelaporan akan dibahas pada bagian hasil dan pembahasan.

4. Hasil dan Pembahasan

Dalam penelitian ini, dijelaskan bahwa terdapat total 25 artikel yang menjadi fokus pembahasan. Dari jumlah tersebut, 21 artikel ditemukan melalui pencarian awal, sementara 4 artikel ditemukan melalui metode *forward backward*. Artikel utama yang digunakan dalam tinjauan literatur ini tidak hanya berasal dari Indonesia, tetapi juga dari berbagai negara lain. Artikel-artikel ini diperoleh dari berbagai sumber publikasi dan penelitian yang dilakukan di berbagai negara. Hal tersebut sejalan dengan tujuan penelitian untuk mengidentifikasi implementasi standar keamanan teknologi informasi dalam mengukur tingkat kematangan sistem informasi rumah sakit, baik di Indonesia maupun di luar negeri.

Artikel utama memberikan gambaran tentang bagaimana implementasi standar keamanan teknologi informasi dapat mengukur kematangan sistem informasi. Temuan dari artikel utama ini dapat diklasifikasikan berdasarkan implementasi standar keamanan teknologi informasi sesuai dengan standar yang digunakan. Identifikasi arah penelitian secara lengkap

dari hasil artikel utama yang telah dilakukan berdasarkan kategori tersebut disajikan pada Tabel 2.

4.1 Hasil

Tabel 2. Artikel Utama

No	Kategori Standar	Implementasi	Artikel relevan
1	ISO 27000 Family	Mengukur keamanan sistem informasi pada sejumlah klausul	[12] [13] [14] [15]
2	COBIT	Menilai kematangan pada domain DSS (*Deliver*, *Service and Support*) dan APO (*Align*, *Plan*, *Organize*)	[16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26]
3	NIST	Aspek keamanan informasi dan risiko	[27]
4	Model Pengukuran Lainnya	Model pengukuran *Hierarchical Decision Model* (HDM) untuk menilai kematangan keamanan informasi	[28]
		Model pengukuran keamanan informasi *Cyber Security Capability Maturity Model* (C2M2)	[29]
		Tingkat kematangan Sistem Informasi dengan menggunakan *Information System Maturity Model* (HISMM).	[30]
		Model Maturitas Manajemen Data Master (MD3M) oleh Spruitz dan Pietzka untuk menilai tingkat kematangan pengelolaan data master.	[31]
		People Capacity Maturity Model (PCMM) untuk mengukur kematangan kapasitas pegawai	[32]
		Skala penilaian kematangan *Public Record Office Victoria's* (PROV, 2018)	[33]
		Pengembangan *Infrastructure Maturity Assessment* (IMA) *Framework* berdasarkan CMM	[34]
		Metodologi terpadu logika fuzzy, ANP, dan TOPSIS	[35]

4.1.1 Standar Keamanan Teknologi Informasi ISO 27000 Family

Implementasi standar keamanan TI ISO 27000 *Family* untuk pengukuran kematangan keamanan sistem informasi di rumah sakit secara umum diterapkan dengan sejumlah tahapan. Tahapan yang dilakukan antara lain pengumpulan data yang diperoleh melalui studi literatur [12][15], observasi [12][13][14][15], wawancara [12][13][14][15], dan kuesioner [12]. Setelah data diperoleh, kemudian dilakukan perhitungan maturity berdasarkan klausul pada ISO 27000 Family. Dari hasil perhitungan kematangan tersebut kemudian dapat disusun rekomendasi perbaikan.

ISO 27000 *Family* diimplementasikan sebagai standar untuk melakukan pengukuran kematangan keamanan sistem informasi di sejumlah rumah sakit terdiri dari sejumlah ruang lingkup Kontrol Manajemen Aset (Klausul 7) [12], Keamanan Sumber Daya Manusia (Klausul 8), Keamanan Fisik dan Lingkungan (Klausul 9), Kontrol Akses (Klausul 11), serta Akuisisi Sistem Informasi, Pengembangan dan Pemeliharaan (Klausul 12) [12][13][14][15]. Implementasi ruang lingkup tersebut diantaranya kurangnya *awareness* dari pegawai terhadap keamanan sistem informasi rekam medis [12] seperti akses pegawai yang tidak berwenang, tidak menjaga data dan *password*, kerusakan peralatan, serta membiarkan unit komputernya menyala pada saat meninggalkan atau saat sedang jam istirahat [13][14], sehingga sering terjadi kebocoran

data yang tidak diinginkan [14]. Tidak hanya itu, implementasi lainnya seperti terjadinya kendala lambatnya penyampaian informasi, sehingga kebutuhan data yang diperlukan kurang, dan kesesuaian atau validasi hasil data juga kurang [15].

Karakteristik implementasi ISO 27000 Family sebagai standar keamanan dalam pengukuran keamanan sistem informasi yaitu pendekatan menggunakan manajemen risiko. Pendekatan ini berfokus pada risiko keamanan informasi yang berkaitan dengan kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*). Dengan melakukan penilaian risiko maka akan dapat diketahui juga tingkat kematangan dari keamanan sistem informasi. Setelah kedua hal tersebut ditemukan, maka dapat disusun rekomendasi perbaikan berupa kebijakan, prosedur dan pengendalian untuk mengamankan aset organisasi.

4.1.2 Standar Keamanan Teknologi Informasi COBIT

COBIT yang merupakan standar dalam melakukan tata kelola teknologi informasi terdiri dari sejumlah versi seperti COBIT 4.1, COBIT 2019, dan COBIT 5. Implementasi COBIT sebagai standar keamanan teknologi informasi untuk pengukuran kematangan sistem informasi rumah sakit secara umum diterapkan dengan sejumlah tahapan. Tahapan yang dilakukan antara lain pengumpulan data dengan melalui observasi [16][17][18][19][23][26], wawancara [16][17][18][19]20][21][22][23][25][26], kuesioner [16][21][22][23][25][26], dan studi literatur [17][18][19][20][22]. Setelah data diperoleh, data dilakukan perhitungan *maturity* berdasarkan pada atribut *maturity* COBIT [16][17][18][19][20][21][22][25][26]. Dari hasil perhitungan *maturity* kemudian dapat ditemukan gap dan dilakukan analisis gap tersebut. Dari analisis gap akan disusun rekomendasi perbaikan [16][17][18][19][20][21][22][25][26].

COBIT yang diimplementasikan sebagai standar untuk melakukan pengukuran kematangan keamanan sistem informasi di sejumlah rumah sakit menggunakan domain sejumlah domain yang berbeda-beda seperti domain DSS (*Deliver*, *Service and Support*) [16][20][22][25][26] dan APO (*Align*, *Plan*, *Organize*) [16][21][26]. Pengukuran yang dilakukan terdiri dari berbagai macam bagian sistem informasi di rumah rakit. Sejumlah implementasi COBIT sebagai standar untuk mengukur kematangan keamanan sistem informasi rumah sakit antara lain pada [17][20] yang berkaitan dengan penyalahgunaan *password* dan *username* pada sistem informasi pengelolaan pendaftaran pasien, [23] optimalisasi keamanan pelayanan waktu antrian pasien, [25] menjaga keamanan informasi dan data BPJS, [21] berkaitan dengan pengelolaan keamanan jaringan, [19][20][24] tidak adanya sistem konfigurasi dan pelacakan untuk mengakses data.

Karakteristik implementasi COBIT sebagai standar keamanan dalam pengukuran keamanan sistem informasi yaitu pada analisis *as-is*, *to-be*, dan *gap*. Dari ketiga hal tersebut selalu berkaitan dan selalu terlibat ketika melakukan pengukuran. Hal tersebut karena pengukuran dilakukan dari kondisi saat ini, kemudian dibandingkan dengan kondisi yang diharapkan mendatang. Setelah kedua hal tersebut ditemukan hasilnya akan dianalisis kesenjangannya dan dilakukan penyusunan rekomendasi perbaikan.

4.1.3 Standar Keamanan Teknologi Informasi NIST

Standar NIST berkaitan erat dalam pengelolaan risiko dan keamanan informasi yang menyediakan panduan, kerangka kerja, penilaian, dan praktik terbaik keamanan. Penelitian [27] menerapkan NIST untuk mendefinisikan 5 kategori penting dalam pengukuran keamanan yaitu orang, manajemen risiko, proses, teknologi, dan ketergantungan terhadap TI. Tahapan implementasi dimulai dengan pengambilan data melalui kuesioner dengan skala Likert 0-4 untuk menyatakan status belum diimplementasi, tahap perencanaan, diimplementasikan sebagian, hampir selesai, dan selesai di implementasi. Tahap berikutnya adalah penilaian, dimana masing-masing sub aspek diberi skor dan dipetakan ke sebuah diagram laba-laba. Kemudian ditarik penilaian secara umum dari kelima aspek sehingga didapatkan rata-rata tingkat keamanan informasi dan risiko serta mengetahui aspek apa yang paling mempengaruhi tingkat keamanan. Hasil penilaian tersebut memberi gambaran terhadap *stakeholder* yaitu sektor kesehatan di Turki untuk melakukan peningkatan pada masing-masing aspek keamanan informasi.

4.1.4 Model Pengukuran Keamanan Teknologi Informasi Lainnya

Implementasi model pengukuran keamanan teknologi informasi lainnya yang digunakan untuk mengukur kematangan sistem informasi rumah sakit diterapkan melalui sejumlah penyusunan dan tahapan implementasi model. Tahapan untuk mengimplementasikan model tersebut diantaranya pengumpulan data melalui kuesioner [29][31][32][33], wawancara [29], dan observasi [31]. Data yang telah terkumpul selanjutnya digunakan sebagai dasar untuk mengukur kematangan. Hasil pengukuran kematangan selanjutnya digunakan untuk menyusun rekomendasi perbaikan untuk keamanan sistem informasi yang diukur serta sebagai evaluasi untuk perbaikan model yang digunakan.

Implementasi sejumlah model untuk mengukur kematangan keamanan sistem informasi Rumah Sakit memiliki karakteristik yang berbeda-beda. Karakteristik tersebut ada pada domain dan atau perspektif yang diukur, tingkatan atau level kematangan, serta tujuan dibuatnya domain tersebut. Karakteristik domain atau perspektif yang berbeda seperti pada sejumlah model [28] yang menyoroti pentingnya peran manusia dalam keamanan informasi, [29] mengembangkan model secara mandiri dengan domain penilaian berdasarkan C2M2, [30] *Information System Maturity Model* (HISMM) yang menggunakan dan memanfaatkan enam dimensi yang relevan dalam bidang kesehatan, [32] menekankan pengembangan kemampuan manusia dalam organisasi, terutama dalam manajemen informasi, [31] mengadopsi model kematangan manajemen data master yang dirancang oleh Spruitz & Pietzka, serta [35] Model terpadu Fuzzy-ANP-TOPSIS yang menggunakan 5 faktor sebagai dasar proses penilaian dengan faktor-faktor tersebut antara lain faktor *confidentiality, satisfaction, integrity, availability*, dan *durability.* [33]menerapkan *Instrumen survei Cohasset Associates* dan AHIMA. Karakteristik lainnya ada pada tingkatan atau level pengukuran yang digunakan seperti [34] yang menerapkan IMA *framework* dengan 8 level yang digunakan dalam menggambarkan cara rumah sakit dalam mengelola infrastruktur dan [32] Model *People Capacity Maturity Model* (PCMM) yang menetapkan level pengukuran pada 5 level .

Dalam implementasi model-model tersebut terdapat tantangan dan keterbatasan yang menyertainya. Tantangan dan keterbatasan pada implementasi model yang dibuat terjadi karena model tidak dibuat secara umum dirancang untuk dapat digunakan secara massal. Hal tersebut dikarenakan model yang digunakan merupakan model dengan desain dan penyesuaian hanya pada tujuan dan objek yang akan diukur, sehingga jika akan menerapkan model tersebut ke tujuan dan objek lainnya maka perlu adanya penyesuaian kembali seperti contoh pada implementasi model pengukuran IMA *Framework* [34] dan model terpadu Fuzzy, AHP, dan Topsis [35]. Tantangan lainnya ada pada implementasi model dengan konsep penilaian yang kurang diketahui oleh responden [33]. Keterbatasan model yang dibuat secara mandiri ada pada proses validasi atribut maupun hasil akhir pengukuran [28] yang memerlukan ahli dalam melakukan validasi.

Pembuatan model pengukuran kematangan keamanan sistem informasi rumah sakit mempunyai alasan masing-masing mengapa model tersebut dibuat dan digunakan. Seperti pada model C2M2 yang dibuat karena diperlukan untuk mengintegrasikan Petunjuk Administratif No. 294-MINSA dan Undang-undang perlindungan data pribadi No 29733 [29]. Model lMA *Framework* dibuat karena tidak adanya model yang dapat digunakan untuk menilai infrastruktur TI di rumah sakit digital [34]. Model terpadu logika Fuzzy, AHP, dan TOPSIS dibuat dengan tujuan untuk memberikan solusi atas kesenjangan fungsionalitas keamanan pada *software* [35].

4.2 Diskusi

Pada penelitian ini, beberapa standar pengukuran keamanan sistem informasi di rumah sakit telah dianalisis, yaitu ISO 27000 *Family*, COBIT, NIST, dan beberapa model pengukuran lainnya. Setiap standar memiliki kelebihan dan kelemahan masing-masing. ISO 27000 *Family* memberikan panduan komprehensif dalam mengelola keamanan TI dengan fokus pada risiko, namun implementasi yang tidak selalu sesuai menjadi kelemahan. COBIT dapat memberikan pemahaman yang lebih baik tentang kesenjangan dan memungkinkan perbaikan yang tepat, namun proses analisis yang kompleks menjadi kendala. Standar NIST memberikan kerangka kerja komprehensif, tetapi implementasi yang kompleks membutuhkan pemahaman mendalam tentang standar dan praktik yang diusulkan. Model-model lain memiliki kelebihan dapat disesuaikan dengan kebutuhan spesifik, namun tantangan mungkin timbul dalam menerapkannya dan memerlukan penyesuaian kembali untuk objek yang berbeda. Secara keseluruhan, berbagai standar dan model pengukuran keamanan TI memiliki kelebihan dan

kelemahan masing-masing. Pemilihan pendekatan yang sesuai harus mempertimbangkan kebutuhan dan karakteristik khusus dari rumah sakit yang akan dievaluasi.

Implementasi standar maupun model yang digunakan dalam pengukuran keamanan sistem informasi di rumah sakit wajib memperhatikan karakteristik yang dimiliki. ISO 27000 *Family* melakukan pengukuran keamanan sistem rumah sakit menggunakan pendekatan manajemen risiko yang berkaitan mengenai kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) yang dimiliki oleh rumah sakit. Hasil pengukuran tingkat keamanan sistem informasi dinilai berdasarkan risiko yang dimiliki. COBIT secara khusus menggunakan domain DSS dan APO untuk mengukur keamanan sistem informasi. Sehingga hasil pengukuran tingkat keamanan sistem informasi pada rumah sakit diukur berdasarkan domain DSS dan APO. Standar NIST berkaitan erat dengan pengelolaan risiko dan keamanan informasi serta memiliki 5 kategori penting yang digunakan dalam pengukuran keamanan yaitu orang, manajemen risiko, proses, teknologi, dan ketergantungan terhadap TI. Model - model lain yang digunakan dalam mengukur keamanan sistem informasi rumah sakit memiliki karakteristik implementasi yang berbeda - beda ada yang berkaitan tentang peran manusia dalam keamanan informasi, menggunakan faktor *confidentiality, satisfaction, integrity, availability*, dan *durability* sebagai proses penilaian. Bahkan terdapat model yang secara mandiri dikembangkan menggunakan domain penilaian berdasarkan C2M2. sehingga setiap standar dan model yang digunakan dalam mengukur tingkat keamanan sistem informasi rumah sakit memiliki karakteristik yang berbeda - beda.

Setiap standar dan model yang digunakan dalam mengukur keamanan sistem informasi akan memberikan rekomendasi perbaikan kepada pihak rumah sakit. Rekomendasi tersebut diharapkan dapat memberikan masukkan kepada rumah sakit untuk meningkatkan keamanan sesuai dengan bagian yang memiliki tingkat keamanan yang kurang.

5. Simpulan

Penelitian ini menyajikan tinjauan literatur implementasi standar keamanan TI dalam mengukur kematangan sistem informasi rumah sakit. Penelitian ini mengidentifikasi 73 studi pada pencarian awal dan menghasilkan 21 artikel utama setelah menerapkan kriteria inklusi eksklusi. Penelitian ini juga melakukan teknik *forward backward snowballing* untuk melengkapi artikel utama yang menghasilkan 22 pada pencarian dan menghasilkan 4 artikel utama tambahan setelah seleksi inklusi eksklusi. Artikel utama selanjutnya dianalisis yang menghasilkan temuan utama antara lain pola implementasi model dan standar keamanan TI memiliki alur yang sama yaitu data dikumpulkan kemudian dilakukan proses pengukuran dari proses pengukuran hasil kematangan digunakan sebagai dasar dalam memberikan solusi atau rekomendasi perbaikan. Namun, yang membedakan antara standar dan model satu dengan lainnya adalah pada domain, atribut kematangan, dan level atau tingkatan kematangan. Standar dan model pengukuran keamanan TI yang diimplementasikan memiliki kelebihan dan kelemahan masing-masing sehingga dalam pemilihan pendekatan yang sesuai harus mempertimbangkan kebutuhan dan karakteristik khusus dari rumah sakit yang akan dievaluasi. Implementasi standar dan model pada rumah sakit juga perlu memperhatikan kerahasiaan data yang digunakan karena data-data yang terdapat di rumah sakit merupakan data dengan kerahasiaan tinggi dan menyangkut dengan riwayat medis seseorang serta catatan rahasia rumah sakit yang tidak untuk diketahui orang banyak.

Daftar Referensi

[1] A. Sardi, A. Rizzi, E. Sorano, and A. Guerrieri, “Sustainability-12-07002-V2.Pdf,” *Sustainability*, pp. 1–16, 2020.

[2] Fortified Health Security, "2022 Mid-Year Horizon Report," 2022. [Online]. Tersedia: https://fortifiedhealthsecurity.com/wp-content/uploads/2022/07/2022-Mid-Year-Horizon-Report.pdf. [Diakses: 21 Mei 2023].

[3] A. Mahfuth, S. Yussof, A. A. Baker, and N. Ali, “A systematic literature review: Information security culture,” *Int. Conf. Res. Innov. Inf. Syst. ICRIIS*, pp. 1–6, 2017, doi: 10.1109/ICRIIS.2017.8002442.

[4] Boonstra, A., Versluis, A. & Vos, J.F.J., “Implementing electronic health records in hospitals: a systematic literature review”, BMC Health Serv Res, vol. 14, no. 370, September 2014.

[5] D. Maček, I. Magdalenić, and N. B. Ređep, "A systematic literature review on the application of multicriteria decision making methods for information security risk assessment," *Int. J. Saf. Secur. Eng.*, vol. 10, no. 2, pp. 161–174, 2020, doi: 10.18280/ijsse.100202.
[6] P. W. Handayani, A. N. Hidayanto, A. A. Pinem, I. C. Hapsari, P. I. Sandhyaduhita, and I. Budi, "Acceptance model of a Hospital Information System," *Int. J. Med. Inform.*, vol. 99, pp. 11–28, 2017, doi: 10.1016/j.ijmedinf.2016.12.004.
[7] S. Rachmawati, R. Rosidin, and M. Lubis, "Information Technology Governance at Rachmi Dewi Gresik Hospital Using the Cobit 5 Framework," *2022 1st Int. Conf. Inf. Syst. Inf. Technol. ICISIT 2022*, pp. 301–305, 2022, doi: 10.1109/ICISIT54091.2022.9873099.
[8] J. V. Carvalho, Á. Rocha, and A. Abreu, "Maturity Models of Healthcare Information Systems and Technologies: a Literature Review," *J. Med. Syst.*, vol. 40, no. 6, 2016, doi: 10.1007/s10916-016-0486-5..
[9] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review* Introduction: the need for an evidence- informed approach," *Br. J. Manag.*, vol. 14, pp. 207–222, 2003.
[10] C. Ariati and D. Juandi, "Kemampuan Penalaran Matematis: Systematic Literature Review," *LEMMA Lett. Math. Educ.*, vol. 8, no. 2, pp. 61–75, 2022.
[11] I. K. Raharjana, D. Siahaan, and C. Fatichah, "User Stories and Natural Language Processing: A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 53811–53826, 2021, doi: 10.1109/ACCESS.2021.3070606..
[12] H. Setiawan, K. Mukhoyyaroh, M. D. Fauzi, and B. Sugiantoro, "Hospital Information System Audit Using The ISO 27001 Standard (Case Study In RSU PKU Muhammadiyah Bantul)," *Int. J. Informatics Dev.*, vol. 3, no. 1, pp. 2–5, 2014.
[13] A. D. Yaner, H. Tanuwijaya, and E. Sutomo, "Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Management (Sim-Rs) Berdasarkan Standar Iso 27002," *e-conversion - Propos. a Clust. Excell.*, vol. 27002, pp. 1–8, 2018.
[14] A. A. Rahman, P. G. Dharma, R. M. Fatchur, A. N. Freedrikson, B. P. Ari, and Y. Ruldeviyani, "Master data management maturity assessment: A case study of a Pasar Rebo Public Hospital," *2019 Int. Conf. Adv. Comput. Sci. Inf. Syst. ICACSIS 2019*, pp. 497–504, 2019, doi: 10.1109/ICACSIS47736.2019.8979656.
[15] W.R. Danastri, H. Tanuwijaya, and E. Sutomo, "Audit Keamanan Sistem Informasi Oada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002," vol. 3, no. 2, pp. 1–2, 2016.
[16] R. S. A. Gusni, K. Kraugusteeliana, and I. W. W. Pradnyana, "Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019," *Konf. Nas. Ilmu Komput. 2021*, no. September, pp. 434–439, 2021, [Online]. Available: https://prosiding.konik.id/index.php/konik/article/view/92
[17] Setiyowati and S. Siswanti, "Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1," *SATIN - Sains dan Teknol. Inf.*, vol. 7, no. 1, pp. 123–133, 2021, doi: 10.33372/stn.v7i1.694.
[18] A. Ambarwati and F. Zulkarnain, "Analisis Implementasi Teknologi Informasi Pada IT Process DS5 (Ensure System Security) di RS UHS," *Pros. Semin. Nas. Teknol. dan Rekayasa Inf.*, vol. 5, no. November, pp. 7–11, 2017.
[19] W. W. Widiyanto and Z. Arifin, "Manajemen Rumah Sakit Menggunakan Framework Cobit 4 . 1 (Studi Kasus Di Rs Mata Undaan Surabaya)," *J. Manaj. Inf. dan Adm. Kesehat.*, vol. 5, no. 24, pp. 1–8, 2022.
[20] T. Natanael, L. W. Santoso, and A. Noertjahyana, "Analisa Keamanan Sistem Informasi RSUD Dr . Soetomo Dengan Framework COBIT," *J. INFRA*, vol. 6, no. 2, pp. 1–4, 2018.
[21] N. Agitha, S. E. Anjarwani, M. I. Azizah, I. R. Yunus, and R. W. Witjaksono, "Implementation of COBIT 4.1 to Define and Maintain Infrastructure of Information Technology at Regional Public Hospital in West Nusa Tenggara," *2020 Int. Conf. Adv. Data Sci. E-Learning Inf. Syst. ICADEIS 2020*, pp. 5–9, 2020, doi: 10.1109/ICADEIS49811.2020.9277015.
[22] Rusadi, B. Helpiono. "Analisis Tingkat Kematangan Sistem Informasi Manajemen Rumah Sakit Menggunakan Cobit 4.1 (Studi Kasus: Rumah Sakit Universitas Muhammadiyah Malang)." Diss. University of Muhammadiyah Malang, 2018.

[23] I. B. L. M. Suta and M. Sudarma, "Application of COBIT 5 for Hospital Services Management Information System Audit," *Int. J. Eng. dan Emerg. Technol.*, vol. 3, no. 2, pp. 18–23, 2018.
[24] K. Nistrina and H. A. T. Bin Bon, "Information security for hospital information system using COBIT 5 framework," *Proc. Int. Conf. Ind. Eng. Oper. Manag.*, vol. 2019, no. MAR, pp. 3369–3374, 2019.
[25] N. Made, N. Putri, I. G. Juliana, E. Putra, I. G. Putu, and K. Juliharta, "Analisis Tata Kelola dan Audit Sistem Informasi pada Rumah Sakit Umum ' XYZ ' Menggunakan Kerangka Kerja COBIT 5," vol. 5.
[26] M. F. Cobit and D. S. S. Framework, "Audit keamanan sistem informasi pada rs mata dr.yap yogyakarta menggunakan framework cobit 5," vol. 1, no. September, 2017.
[27] T. Ç. Şahika Eroğlu, "Enterprise Information Systems within the Context of Information Security: A Risk Assessment for a Health Organization in Turkey," in Procedia Computer Science, 2016, p. 8.
[28] B. Barnes and T. Daim, "Information Security Maturity Model for Healthcare Organizations in the United States," IEEE Trans. Eng. Manag., vol. PP, pp. 1–12, 2021, doi: 10.1109/TEM.2021.3139836.
[29] J. Armas-aguirre, E. Fabrizzio, and P. Valencia, "Cybersecurity maturity model for the protection and privacy of personal health data," pp. 1–4, 2022, doi: 10.1109/ICALTER57193.2022.9964729.
[30] M. Lubis, "Information Systems Maturity Level Assessment using the HISMM Framework : Case Study of State Hospital in Jakarta," 2022 Int. Conf. Sci. Technol., no. 6, pp. 1–6, 2019, doi: 10.1109/ICOSTECH54296.2022.9829143.
[31] A. Aditya Rahman, P. Gusman Dharma, R. Mohamad Fatchur, A. Nala Freedrikson, B. Pranata Ari, and Y. Ruldeviyani, "Master data management maturity assessment: A case study of a Pasar Rebo Public Hospital," *2019 Int. Conf. Adv. Comput. Sci. Inf. Syst. ICACSIS 2019*, pp. 497–504, 2019, doi: 10.1109/ICACSIS47736.2019.8979656.
[32] M. H. Yarmohammadian, N. Tavakoli, a Shams, and F. Hatampour, "Evaluation of organizational maturity based on people capacity maturity model in medical record wards of Iranian hospitals," *J. Educ. Health Promot.*, vol. 3, no. June, pp. 54-9531.134743. eCollection 2014, 2014, doi: 10.4103/2277-9531.134743.
[33] H. Kwan, M. Riley, N. Prasad, and K. Robinson, "An investigation of the status and maturity of hospitals' health information governance in Victoria, Australia," *Heal. Inf. Manag. J.*, vol. 51, no. 2, pp. 89–97, 2022, doi: 10.1177/1833358320938309.
[34] P. A. H. Williams, B. Lovelock, T. Cabarrus, and M. Harvey, "Improving digital hospital transformation: Development of an outcomes-based infrastructure maturity assessment framework," *JMIR Med. Informatics*, vol. 7, no. 1, 2019, doi: 10.2196/12465.
[35] R. Kumar, M. T. Jamal Ansari, A. Baz, H. Alhakami, A. Agrawal, and R. A. Khan, "A multi-perspective benchmarking framework for estimating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods," *KSII Trans. Internet Inf. Syst.*, vol. 15, no. 1, pp. 240–263, 2021, doi: 10.3837/TIIS.2021.01.014