Desain Kerangka Kerja Manajemen Risiko Keamanan Informasi Berdasarkan Kajian *Risk Profiling* pada Sektor Kesehatan

Amalia Fitri Kurnia Dewi [1],Yohan Suryanto[2]
Departemen Teknik Elektro, Fakultas Teknik,
Universitas Indonesia
Depok, (021)7867222
amalia.fitri01@ui.ac.id

Diterima: 21 April 2022. Disetujui: 27 Mei 2022. Dipublikasikan: 2 Juni 2022.

Abstract - The healthcare sector is currently becoming one of the paramount targets for cyberattacks. The utilization of information technology in the healthcare sector triggers the emergence of its varied vulnerabilities. Information security risk management is considered one of obligatory jobs for healthcare sector organizations. This study aims at constructing an information security risk management framework in the healthcare sector based on a study of its existing risk profile. This research employed qualitative method. Based on risk profiling results, the healthcare sector had two critical assets, namely electronic health records and Internet of Medical Things. These assets had high sensitivity, however, had numerous vulnerabilities that were prone to exploitations. In order to overcome this, an information security risk management framework consisting of four stages is proposed, namely Risk Profiling, Risk Level Assessment, Risk Treatment, and Monitoring. Risk Profiling is a vital stage in the risk management process. This stage is performed to produce an overview of the information security risk profile resulted from critical assets owned by the organization and the condition of cyberspace in the information security in the healthcare sector. The proposed framework is cyclical as the risk profile in the healthcare sector is dynamic. Thus, monitoring changes in the organization's risk profile is imperative. The proposed framework design was tested in Puskesmas XYZ which is kind of health care facility agencies. The resul of the testing is there are seven risks in the information security contex. There are three High Level riskd and four Medium Level risks. All the risks are reduced by applying some controls. The result of the evaluation of proposed framework state that it has described the sequence of security risk management stage, all activities in information security risk management are includes, and the proposed fra,ework can be applied to health care facilities.

Keywords: risk profiling, information security risk management, framework, healthcare sector

Abstrak*--Saat ini, sektor kesehatan merupakan salah satu sektor yang menjadi target utama serangan siber. Penggunaan teknologi informasi pada sektor kesehatan menyebabkan munculnya berbagai kerentanan dalam sektor kesehatan. Pengelolaan risiko keamanan informasi merupakan salah satu hal yang harus dilakukan oleh organisasi sektor kesehatan. Penelitian ini bertujuan untuk menghasilkan kerangka kerja manajemen risiko keamanan informasi pada sektor kesehatan berdasarkan kajian terhadap profil risiko yang ada pada sektor kesehatan. Penelitian dilakukan dengan metode kualitatif. Berdasarkan hasil *risk profiling*, sektor kesehatan mempunyai dua aset kritikal, yaitu *electronic health record* dan *Internet of Medical Things*. Aset tersebut mempunyai sensitivitas yang tinggi namun mempunyai berbagai kerentanan yang rawan dieksploitasi. Untuk mengatasi hal tersebut, diajukan kerangka kerja manajemen risiko keamanan informasi yang terdiri atas empat tahap, yaitu *Risk Profiling*, Pengukuran Level Risiko, Perlakuan Risiko, dan Pemantauan. *Risk Profiling* merupakan tahap yang penting dalam proses manajemen risiko. Tahap tersebut menghasilkan gambaran profil risiko keamanan informasi berdasarkan aset kritikal yang dimiliki organisasi dan kondisi ruang siber dalam konteks keamanan informasi di sektor kesehatan. Kerangka yang diajukan bersifat siklis karena profil risiko pada sektor kesehatan sifatnya dinamis. Usulan desain kerangka kerja diuji coba pada Puskesmas XYZ yang merupakan salah satu instansi fasilitas pelayanan kesehatan. Pada hasil uji coba tersebut, terdapat tujuh risiko yang terdiri atas 3 risiko level Tinggi dan 4 risiko level Sedang. Perlakuan terhadap seluruh risiko tersebut adalah dikurangi dengan penerapan kontrol. Hasil evaluasi terhadap usulan kerangka kerja menyatakan bahwa usulan desain kerangka kerja telah menggambarkan urutan tahapan manajamen risiko keamanan informasi, mencakup seluruh aktivitas untuk melakukan manajemen risiko keamanan informasi, dan dapat diaplikasikan pada instansi fasilitas pelayanan kesehatan.

***Kata kunci: risk profiling,* manajemen risiko keamanan informasi, kerangka kerja, sektor kesehatan**

I. PENDAHULUAN

Sektor kesehatan merupakan salah satu sektor yang saat ini menjadi salah satu target utama serangan siber. Perkembangan perangkat medis yang saling terkoneksi mengakibatkan berbagai kejadian *security breach* yang dapat membahayakan kesehatan dan keselamatan pasien [1]. Selain itu, terdapat unsur penting pada sektor kesehatan yaitu data rekamedis pasien atau *electronic health record*. Data rekamedis pasien merupakan catatan yang dibuat berdasarkan hasil diagnosis pasien yang mengandung sosial demografi pasien, keluarga, laporan hasil pemeriksaan laboratorium, catatan klinik, dan lain sebagainya [2].

Pada tahun 2021, berdasarkan laporan yang dikeluarkan oleh *IBM Security*, sektor kesehatan merupakan sektor yang mengalami kerugian tertinggi akibat adanya *data breach*, yaitu sebesar 9,23 juta USD [3]. Jumlah ini mengalami peningkatan sebanyak 29,5% bila dibandingkan dengan kerugian yang dialami pada tahun 2020 [3].

Sejak adanya pandemi COVID-19, serangan pada sektor kesehatan mengalami peningkatan. Berdasarkan laporan yang dikeluarkan oleh *Mandiant Lab Threat*, sektor kesehatan menduduki peringkat ketiga sebagai sektor yang menjadi target serangan siber pada tahun 2020 [4]. Posisi tersebut meningkat drastis karena pada tahun 2019 sektor kesehatan menempati peringkat kedelapan. Selain itu, berdasarkan laporan *McAfee Lab Threat* periode Q2 tahun 2021, sektor kesehatan juga menempati lima besar sektor dengan serangan tertinggi [5]. Selain itu, adanya kegiatan *cyber espionage* yang menargetkan sektor kesehatan dengan tujuan mendapatkan data dan informasi terkait pengendalian dan vaksinasi COVID-19 [4].

Meningkatnya penggunaan teknologi informasi pada sektor kesehatan juga menyebabkan meningkatnya kerentanan sektor kesehatan akan adanya serangan siber [6]. Akan tetapi, berbagai organisasi yang bergerak di bidang kesehatan sering kekurangan sumber daya untuk dapat memberikan perlindungan terhadap aset sehingga apabila terjadi serangan siber akan menimbulkan dampak yang signifikan dan kerugian yang besar [6].

Seluruh organisasi dan institusi yang bergerak di sektor kesehatan perlu meningkatkan kesadaran bahwa sektor kesehatan merupakan salah satu sektor yang rentan terhadap serangan siber. Sektor kesehatan juga perlu melakukan penilaian terhadap risiko yang ada pada konteks serangan siber, terutama selama masa pandemi COVID-19 [6]. Pentingnya melakukan penilaian terhadap risiko tersebut agar risiko yang ada dapat dikelola sehingga tidak menimbulkan dampak yang merugikan dan membahayakan keselamatan pasien.

Manajemen risiko keamanan informasi merupakan salah satu elemen penting yang harus dilakukan untuk menunjang keamanan siber pada sektor kesehatan. Manajemen risiko merupakan keseluruhan program yang bertujuan untuk melakukan identifikasi terhadap kerentanan dan ancaman yang dapat mengeksploitasi kerentanan tersebut, serta melakukan penilaian terhadap dampak buruk pada organisasi [7]. Manajemen risiko merupakan panduan bagi organisasi untuk mengurangi peluang terjadinya risiko yang tidak diharapkan [7].

Saat ini, terdapat berbagai kerangka kerja manajemen risiko yang dikeluarkan oleh berbagai organisasi internasional dan asosiasi profesional. Beberapa kerangka kerja tersebut antara lain ISO/IEC 31000:2018, ISO/IEC 27005:2018, OCTAVE Allegro, NIST SP 800-30 *Revision* 1, dan lain sebagainya. Setiap kerangka kerja tersebut mempunyai pendekatan yang cukup berbeda sehingga dibutuhkan analisis untuk menentukan kerangka kerja mana yang paling tepat untuk diterapkan di instansi atau sektor tertentu..

Berbagai penelitian juga dilakukan untuk mengajukan kerangka kerja manajemen risiko dengan berbagai pendekatan baru atau objek tertentu serta pengembangan dari kerangka kerja yang sudah ada. Berdasarkan penelitian yang dilakukan oleh Prajanti et.al., dilakukan penelitian terkait kerangka kerja untuk memberikan peringkat terhadap aset informasi yang kritis pada proses penilaian risiko keamanan informasi dengan menggunakan metode OCTAVE Allegro dan *Decision Support System* [8]. Kombinasi OCTAVE Allegro dan metode untuk melakukan pengambilan keputusan *(decision support system)* yang terdiri atas *Simple Additive Weighting* (SAW) dan *Analytic Hierarchy Process* (AHP) menghasilkan input yang lebih baik untuk menentukan prioritas risiko dan menghindari adanya kesalahan dalam menentukan sumber daya untuk melindungi aset informasi kritis [8].

Penelitian terkait manajemen risiko juga dilakukan untuk mengajukan kerangka kerja yang digunakan oleh penyedia layanan maupun layanan konsumen [9]. Pada kerangka kerja yang diajukan, terdapat dua komponen kunci yang digunakan, yaitu *Threat Model* dan *Risk Model* [9]. Kedua komponen

kunci tersebut dirancang agar sesuai untuk fitur khusus pada layanan *online* dan *environment* pada ruang siber.

Berdasarkan penelitian yang dilakukan oleh Joshi et.al., dilakukan penelitian mengenai penyusunan kerangka kerja manajemen risiko keamanan informasi pada jaringan universitas untuk menghindari terjadinya *data breach* [10]. Pada kerangka kerja yang diajukan, terdapat tiga fase untuk mengurangi risiko *data breach*. Fase pertama adalah penilaian terhadap ancaman dan kerentanan untuk mengidentifikasi titik kelemahan lingkungan pendidikan, fase kedua adalah penentuan fokus utama pada risiko yang mempunyai level tinggi dan penyusunan rencana perbaikan yang *actionable*, dan fase ketiga adalah pemantauan seluruh persyaratan telah dilakukan sesuai dengan manajemen kerentanan [10].

Penelitian untuk menyusun kerangka kerja penilaian risiko pada perangkat medis dilakukan oleh Yaqoob et.al. [1]. Kerangka kerja yang diajukan adalah ISSP *(Integrated Security, Safety, and Privacy) Risk Assessment Framework*. Kerangka kerja tersebut diajukan sebagai metode yang sistematis untuk menentukan level risiko suatu perangkat medis dan kontrol keamanan yang diperlukan [1]. Pada ISSP *Risk Assessment Framework*, terdapat sembilan tahap yang harus dilakukan untuk menganalisis risiko suatu perangkat medis, yaitu (1) *Device Characterization*, (2) *Identification of Vulnerabilities, Threats, and Hazards*, (3) *Control Analysis*, (4) *Vulnerability/Threat Likelihood Determination*, (5) *Hazard Likelihood Determination*, (6) *Impact Valuation*, (7) *Risk Determination*, (8) *Controls*, dan (9) *Monitoring and Patch Management* [1]. Kerangka kerja yang diajukan diuji coba untuk melakukan penilaian risiko pada perangkat pompa infus. Berdasarkan hasil perbandingan, kerangka kerja yang diajukan menyediakan pendekatan yang lebih terpadu untuk menentukan risiko yang ada pada suatu perangkat medis [1].

Penelitian untuk menyusun kerangka kerja manajemen risiko keamanan informasi dilakukan oleh Baehaki [11]. Pada penelitian tersebut, dilakukan perancangan kerangka kerja manajemen risiko keamanan informasi yang sederhana namun memenuhi prinsip manajemen risiko [11]. Dalam penyusunan kerangka kerja tersebut, dilakukan integrasi antara ISO 27005 yang berupa standar, NIST SP 800-39 yang merupakan pedoman, OCTAVE Allegro yang berupa metodologi, dan COBIT yang merupakan kerangka kerja [11]. Kerangka kerja yang diajukan terdiri atas empat tahap, yaitu identifikasi, pengukuran, administrasi, dan pemantauan [11]. Kemudian, kerangka kerja tersebut diuji coba pada Pusat Pendidikan dan Pelatihan Badan XYZ [11].

Penelitian yang dilakukan oleh Lee mengajukan desain kerangka kerja manajemen risiko keamanan siber, mengkaji proses penilaian risiko siber, dan memberikan ilustrasi mengenai peningkatan performa keamanan siber yang berkelanjutan dengan memperhatikan hasil analisis *cost benefit*. Kerangka kerja manajemen risiko keamanan siber yang diajukan terdiri atas empat layer, yaitu *Cyber Ecosystem Layer, Cyber Infrastructure Layer, Cyber Risk Asseessment Layer*, dan *Cyber Performance Layer* [12]. Berdasarkan hasil manajemen risiko tersebut, dilakukan *cost benefit analysis* untuk menentukan teknologi yang menjadi prioritas organisasi untuk menunjang peningkatan keamanan siber [12].

Meningkatnya serangan siber terhadap sektor kesehatan akan berdampak pada keselamatan jiwa pasien sehingga diperlukan kerangka kerja manajemen risiko yang mempertimbangkan dampak terkait keselamatan jiwa pasien [1]. Berbagai kerangka kerja manajemen risiko yang ada saat ini dibuat untuk organisasi secara umum tanpa memperhatikan karakteristik yang ada pada sektor tertentu, termasuk pada sektor kesehatan. Oleh sebab itu, diperlukan kerangka kerja manajemen risiko yang sesuai untuk sektor kesehatan berdasarkan karakteristik pada sektor tersebut.

Berdasarkan hasil evaluasi Indeks KAMI yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN) pada tahun 2018/2019, tingkat kesiapan pengaman informasi pada sektor kesehatan dinilai Tidak Layak [13]. Instansi sektor kesehatan yang mendapat kategori Baik hanya sebesar 5%. Sementara itu, persentase instansi dengan kategori Tidak Layak sebesar 67% dan sebesar 26% mendapat kategori Perlu Perbaikan [13]. Pada hasil evaluasi tersebut, tiga area hasil evaluasi yang mempunyai nilai paling rendah adalah area pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, dan tata kelola keamanan informasi [13].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk membuat desain kerangka kerja manajemen risiko yang sesuai untuk sektor kesehatan. Kerangka kerja tersebut dibuat berdasarkan profil risiko yang ada pada sektor

kesehatan dengan melakukan *risk profiling* sebagai tahap awal. Desain kerangka kerja yang diajukan mencakup keseluruhan tahapan yang diperlukan untuk melakukan manajemen risiko keamanan informasi pada sektor kesehatan. Tujuan diusulkannya kerangka kerja manajemen risiko keamanan informasi untuk sektor kesehatan adalah agar instansi yang bergerak di bidang kesehatan, terutama fasilitas pelayanan kesehatan dapat melakukan *self—assessment* berkaitan dengan manajemen risiko keamanan informasi.

II. METODE PENELITIAN

Metode penelitian yang dilakukan pada penelitian ini adalah metode kualitatif. Metode penelitian ini dilakukan pada kondisi alamiah atau natural *setting* serta proses pengumpulan dan analisis data bersifat kualitatif [14]. Objek pada penelitian ini adalah instansi pada sektor kesehatan, namun dilakukan pembatasan terhadap objek penelitian, yaitu berfokus pada fasilitas pelayanan kesehatan. Berikut ini adalah tahapan penelitian yang dilakukan:

1) Studi pendahuluan dan *risk profiling*

Pada tahap ini, dilakukan studi literatur dari berbagai sumber seperti buku, jurnal, artikel *proceeding*, standar, dan peraturan lain yang berkaitan dengan risiko keamanan informasi serta keadaan dan karakteristik sektor kesehatan, terutama pada fasilitas pelayanan kesehatan *(Fasyankes)*.

2) Pemetaan tahapan pada kerangka kerja

Kerangka kerja yang dijadikan sebagai acuan terhadap desain yang diajukan adala ISO/IEC 27005:2018[15] , NIST SP 800-30 Rev 1 [16], *ISSP Risk Assessment Framework for Medical Device* [1], dan teori *Security Risk Management* oleh Wheeler [7]. Seluruh tahapn yang ada pada empat kerangka kerja acuan tersebut dipetakan ke dalam lima aktivitas kegiatan untuk mempermudah analisis, yaitu aktivitas kegiatan Identifikasi, Pengukuran, Perlakuan, Administrasi, dan Pemantauan. Pemetaan aktivitas kegiatan tersebut merujuk pada penelitian yang dilakukan oleh Baehaki [11].

3) Penyusunan desain kerangka kerja yang diajukan

Berdasarkan analisis terhadap hasil *risk profiling* dan pemetaan aktivitas kegiatan pada kerangka kerja acuan, disusun desain kerangka kerja untuk sektor kesehatan berdasarkan karakteristik sektor kesehatan dan integrasi setiap tahapan pada kerangka kerja acuan. Integrasi tersebut dilakukan agar usulan kerangka kerja dapat menggambarkan urutan tahapan manajemen risiko keamanan informasi serta tahapan yang ada mencakup seluruh aktivitas yang diperlukan dalam manajemen risiko keamanan informasi.

4) Penerapan desain kerangka kerja dan evaluasi

Usulan kerangka kerja manajemen risiko keamanan informasi diuji coba pada fasilitas pelayanan kesehatan berupa Puskesmas XYZ. Pada uji coba tersebut, dilakukan penyusunan dokumen manajemen risiko keamanan informasi berdasarkan desain kerangka kerja yang diajukan serta evaluasi usulan kerangka kerja.

III. HASIL DAN PEMBAHASAN

Bab ini berisi hasil *Risk Profiling* pada sektor kesehatan, dengan fokus instansi yang merupakan fasilitas layanan kesehatan dan, usulan desain kerangka kerja manajemen risiko keamanan informasi, dan pembahasan.

A. *Hasil Risk Profiling pada Sektor Kesehatan*

Berdasarkan Wheeler, risiko dalam konteks keamanan informasi didefinisikan sebagai kemungkinan frekuensi dan dampak yang akan terjadi apabila terjadi *event* yang menyebabkan hilangnya kerahasiaan, integritas, ketersediaan, atau akuntabilitas [7]. *Risk profiling* dilakukan untuk mengetahui bagaimana profil risiko pada sektor kesehatan berdasarkan sensitivitas aset yang ada pada sektor tersebut. Terdapat beberapa aspek yang dapat dipertimbangkan dalam menentukan profil risiko, seperti kerugian finansial, hukum, reputasi, atau peraturan yang dilanggar apabila terjadi *cyber attack* pada sektor kesehatan [7].

1) Aset

Penggunaan teknologi informasi pada sektor kesehatan mempunyai tujuan dalam rangka peningkatan, pemeliharaan, dan pemulihan kesehatan dan kesejahteraan individu atau populasi dengan memastikan adanya keberlanjutan pada sistem kesehatan [17]. Adanya penggunaan teknologi informasi menghasilkan dua aset yang mempunyai nilai sensitivitas sangat tinggi dan sifatnya kritikal pada sektor ini, yaitu *electronic health record* (EHR) dan perangkat medis yang saling terhubung. Berdasarkan hasil penelitian yang dilakukan oleh Tarikere et.al., terdapat dua komponen pada sektor kesehatan yang menyebabkan sektor ini rentan terhadap serangan siber, yaitu *electronic health record* dan penggunaan perangkat medis yang sifatnya IoMT [18]. Dua komponen tersebut juga merupakan aset utama yang ada pada sektor kesehatan

Meningkatnya kebutuhan akan layanan kesehatan dan berkembangnya teknologi memicu berbagai organisasi sektor kesehatan melakukan transformasi digital untuk menunjang berbagai layanan kesehatan dan proses bisnis yang dilakukan organisasi . Transformasi digital dilakukan dengan mengubah sistem yang digunakan, yaitu sistem yang semula bersifat *paper-based* berubah menjadi *computer-based* [19]. Adanya transformasi tersebut menyebabkan organisasi sektor kesehatan menggunakan teknologi yang ada untuk melakukan pengumpulan, penyimpanan, dan pengaksesan informasi kesehatan pribadi melalui media elektronik[19].

Health record atau rekamedis pasien merupakan informasi yang bersifat privat, namun apabila dianalisis akan memberikan manfaat bagi pasien dan masyarakat pada umumnya [2]. Saat ini, data rekamedis tersebut disimpan dalam bentuk digital, dikenal sebagai *electronic health records* (EHR). Berdasarkkan *ISO Committee Draft Technical Recommendation 20514*, EHR didefinisikan sebagai tempat penyimpanan informasi mengenai pasien atau subjek yang menerima perawatan medis [2]. Informasi tersebut dapat diproses, ditransmisikan, dan disimpan dengan aman menggunakan komputer serta dapat diakses oleh pihak yang mempunyai wewenang [2].

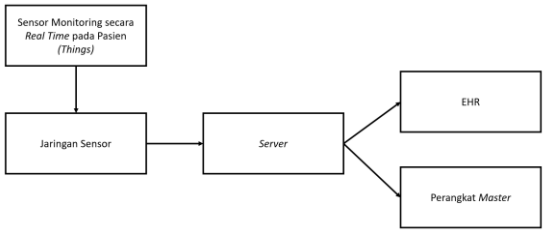
Perangkat medis yang banyak digunakan pada sektor kesehatan saat ini bersifat *portable* dan saling terhubung melalui jaringan [20]. Menurut *World Health Organization*, perangkat medis didefinisikan sebagai instrumen, mesin, artikel, atau alat bantu yang penggunaannya dapat membantu proses diagnosis, perawatan, pemantauan, dan pencegahan suatu penyakit [20]. Perangkat tersebut dapat berupa *software, hardware,* atau gabungan antara *software* dan *hardware* [20].

Saat ini, berkembang pula perangkat medis yang saling terkoneksi atau disebut *Internet of Medical Things* (IoMT). IoMT adalah perangkat medis yang tersambung ke jaringan untuk berbagi data terkait kondisi kesehatan atau organ pengguna agar informasi tersebut dapat ditindak lanjuti [18]. IoMT digunakan untuk berbagai keperluan, kesehatan seperti pemantauan, pemberian diagnosis, alat bantu dalam melakukan terapi pada pasien, dan pendukung proses penanganan pasien [21]. IoMT banyak digunakan sebagai perangkat yang menyediakan pengukuran diagnosis secara *real-time,* meningkatkan perawatan, dan menghubungkan pasien dengan penyedia layanan kesehatan saat pasien mengalami waktu krisis [18].

Konsep IoMT adalah membuat koneksi antara peralatan medis yang dapat dimonitor dan dikendalikan dari jarak jauh melalui jaringan internet. Peralatan tersebut disambungkan ke jaringan dengan menggunakan sensor yang tertanam dan selalu aktif *(pervasive connectivity)* [13]. Penggunaan IoMT dapat mempermudah dalam perawatan pasien karena seluruh data pasien dapat diperbarui dan dapat diakses *real-time*.

Terdapat tiga bagian pada IoMT, yaitu *Master*, *Server*, dan *Things* [13] [22]. *Master* adalah para tenaga kesehatan yang mempunyai hak untuk menggunakan perangkat medis dan perangkat TI seperti *smartphone, personal computer,* atau *tablet* untuk melakukan perawatan kepada pasien. *Server* adalah bagina sentral dari keseluruhan sistem perawatan kesehatan yang bertanggung jawab dalam pengelolaan *data base*, analisis data, dan lain sebagainya. *Things* adalah perangkat yang dihubungkan pada pasien atau sumber daya manusia lain untuk memantau keadaan fisik melalui sensor. Ketika sensor tersebut menerima suatu data, maka data tersebut akan dikirimkan melalui jaringan agar dapat disampaikan kepada *Master*.

Gambar 1 merupakan diagram mekanisme IoMT.



Gambar 1. Ilustrasi Mekanisme Pengelolaan Informasi pada IoMT

2) Attack Vector

Berdasarkan hasil penelitian yang dilakukan oleh Khan et.al., terdapat tujuh *attack vector* yang dapat memicu terjadinya serangan siber pada perangkat medis [20] *Attack vector* tersebut antara lain (1) kerentanan yang ada pada *software, firmware,* atau *hardware* karena proses pengembangan yang tidak mempertimbangkan prinsip keamanan, (2) penggunaan protokol komunikasi dengan *channel* yang rentan, (3) berbagai penggunaan aplikasi pada *smartphone* yang terkoneksi dengan *personal computer*, (4) proses

transmisi data dari sensor atau aplikasi dilakukan dengan mekanisme yang tidak aman, (5) penyimpanan data yang tidak sesuai dengan mekanisme pengamanan, (6) proses transmisi data ke *cloud storage* yang tidak memenuhi standar keamanan, dan (7) penyimpanan data pada *cloud storage* yang tidak mempertimbangkan prinsip keamanan

3) Serangan Siber

Muthuppalaniappan et.al. menyatakan bahwa penyedia layanan kesehatan saat ini menjadi target serangan siber dengan berbagai variasi serangan yang kompleks dan terkoordinasi [6] Terlebih lagi sejak adanya pandemi COVID-19, kebutuhan akan layanan kesehatan, perangkat medis, dan industri sektor kesehatan mengalami peningkatan yang signifikan sehingga menjadi target utama para *attacker* [6].

Tabel I adalah rangkuman dari berbagai literatur yang melakukan identifikasi terhadap serangan siber pada sektor kesehatan.

TABEL I. DENTIFIKASI SERANGAN PADA SEKTOR KESEHATAN

Peneliti	**Serangan Siber yang Diidentifikasi**	**Keterangan**
Thomasian et.al.[21]	Serangan pada perangkat medis (IoMT)	*Remote unauthorized user, DoS, information leak attack*
Bhosale et.al.[23]	*Physical Attack*	*DoS, Malicious software, social engineering*
	Software Attack	*Phishing attack, worm, spamming, dan Cross Site Scripting (XSS)*
	Network Attack	*Formjacking, browser extension, online converters*
	Encryption Attack	*Man in the middle attack, cryptographic attack*
Thamer et.al. [24]	*Ransomware attack*	*Email phishing, Remote Desktop Protocol, exploit kit, Watering Hole Attacks, removable media* dan *serial bus, pirated software, Microsoft Office Macros,* dan *botnets*
Khan et.al. [20]		*DDOS Attack, malicious domains, malicious websites, malware, ransomware, spam email, malicious social media messaging, business email compromise, mobile threats,* dan *browsing applications*
Muthuppalaniappan et.al. [6]		*Ransomware, data breach, state-sponsored cyber-attack* yang menargetkan pengembang vaksin COVID-19, *malicious site* yang mencuri *password* staf WHO
Yaqoob et.al. [25]		*Firmware modification attack, eavesdropping, sniffing, information disclosure, man in the middle attack, unauthorized access and spoofing, replay attack, tampering and modification attack,DoS, depletion,* dan *jamming attack, side channel attack, ransomware,*

4) Profil Risiko

Sensitivitas aset untuk menggambarkan profil risiko kesehatan dilakukan melalui berbagai perspektif. Berdasarkan hasil penelitian yang dilakukan oleh Deshanta et.al., perspektif bisnis dengan metris dampak finansial, reputasi, level kritis, ukuran organisasi, dan tipe organisasi dapat digunakan untuk melakukan analisis untuk menghasilkan profil risiko pada sektor kesehatan [26].

Organisasi pada sektor kesehatan akan mengalami dampak finansial yang paling tinggi apabila mengalami serangan siber. Berdasarkan IBM, kerugian finansial yang disebabkan adanya *data breach* pada sektor kesehatan mencapai 9,23 juta USD [3].

EHR mempunyai kerentanan yang tinggi karena mempunyai nilai informasi yang sangat tinggi sehingga menjadi target para pelaku *cybercrime* [2]. Adanya EHR juga memicu terekspos nya informasi kesehatan pribadi terhadap berbagai serangan keamanan baru [19].

Perangkat medis yang banyak digunakan pada sektor kesehatan juga rentan terhadap serangan. Salah satu penyebabnya adalah pengembangan perangkat medis tidak didesain dengan mempertimbangkan aspek keamanan siber karena tidak terpikirkan bahwa perangkat medis dapat diretas [1]. Berdasarkan laporan FDA yang dikutip oleh Yaqoob et.al., terdapat laporan bahwa selama sepuluh tahun terakhir, terdapat lebih dari 1,5 juta perangkat medis telah dieksploitasi oleh para

attacker karena adanya kerentanan pada *software* yang digunakan.

Adanya ketergantungan yang tinggi antara perangkat medis dengan teknologi informasi akan berdampak pada keselamatan pasien apabila terjadi serangan siber seperti *Denial of Service (DoS)*, *tampering attack*, atau *ransomware attack* [1]. Penelitian yang dilakukan oleh Thomasian et.al. menyatakan bahwa perangkat medis yang saat ini saling terkoneksi satu sama lain, dikenal sebagai IoMT, mempunyai risiko dalam konteks keamanan siber yang dapat mengancam keselamatan pasien [21].

Berdasarkan *Cisco Security and Cybersecurity Ventures* yang dikutip oleh Lee, organisasi sektor kesehatan terutama rumah sakit merupakan jenis organisasi yang lebih rentan terhadap adanya serangan siber bila dibandingkan dengan organisasi lain yang bergerak di sektor kesehatan [19]. Hal tersebut disebabkan karena penggunaan sistem yang sudah ketinggalan zaman, kurangnya personil yang berpengalaman terkait keamanan siber, data yang disimpan oleh rumah sakit berupa EHR merupakan data yang mempunyai nilai sangat tinggi, dan adanya insentif yang memang disediakan untuk membayar uang tebusan terhadap data pasien [19].

Beberapa insiden siber pada sektor kesehatan menyebabkan organisasi pada sektor ini tidak dapat memberikan layanan kesehatan sebagaimana mestinya. Kerugian finansial yang ditimbulkan sangat besar karena organisasi harus mengeluarkan biaya untuk membayar tebusan apabila serangan tersebut berupa *Ransomware attack*, mengganti biaya perawatan pasien yang terkena dampak serangan siber, dan biaya perbaikan sistem [17]. Kerugian juga berupa hilangnya reputasi organisasi sehingga kepercayaan masyarakat untuk menggunakan layanan organisasi akan mengalami penurunan [17]. Bahkan, korban yang merupakan pasien atau keluarga pasien dapat menuntut organisasi sektor kesehatan apabila insiden yang terjadi menyebabkan *data breach* [17].

B. *Desain Kerangka Kerja Manajemen Risiko Keamanan Informasi pada Sektor Kesehatan*

Berdasarkan hasil analisis terhadap profil risiko keamanan informasi sektor kesehatan, terdapat dua jenis aset kritikal, yaitu EHR dan IoMT. Kedua aset tersebut juga merupakan salah satu karakteristik pada sektor kesehatan. Oleh sebab itu, pada usulan desain yang diajukan, dibuat kategorisasi aset menjadi tiga jenis, yaitu EHR, IoMT atau perangkat medis yang terkoneksi jaringan, dan aset pendukung lain yang digunakan untuk menunjang proses bisnis pada sektor kesehatan.

Berikut ini adalah pemetaan aktivitas kegiatan pada masing-masing kerangka kerja manajemen risiko keamanan informasi yang menjadi acuan.

1) Aktivitas Kegiatan Identifikasi

Tabel II adalah pemetaan aktivitas kegiatan Identifikasi pada masing-masing kerangka kerja acuan.

TABEL II. PEMETAAN AKTIVITAS KEGIATAN IDENTIFIKASI

ISO/IEC 27005:2018 [15]	**NIST SP 800-30 Rev 1** [16]	**ISSP** [1]	**Wheeler** [7]
Penetapan Konteks Identifikasi aset, ancaman, kontrol yang ada, kerentanan	Tujuan, ruang lingkup, asumsi dan konstrain, sumber informasi, penedekatan Sumber ancaman, peristiwa ancaman, kerentanan, kondisi predisposisi	Karakteristik pernagkat medis, kerentanan ancaman, bahaya, dan kontrol	Profil sumber daya dan sensitivitas, *threat*, *vulnerability*, dan risiko

2) Aktivitas Kegiatan Pengukuran

Tabel III pemetaan aktivitas kegiatan Pengukuran pada kerangka kerja acuan.

TABEL III. PEMETAAN AKTIVITAS KEGIATAN PENGUKURAN

ISO/IEC 27005:2018 [15]	**NIST SP 800-30 Rev 1** [16]	**ISSP** [1]	**Wheeler** [7]
Pengukuran konsekuensi, dampak, dan level risiko	Level dampak, frekuensi, dan risiko	*Vulnerability/threat likelihood*, *hazard likelihood*, dan *impact valuation*	Estimasi *severity*, frekuensi, dan *risk exposure*

3) Aktivitas Kegiatan Perlakuan

Tabel IV adalah pemetaan aktivitas kegiatan Perlakuan terhadap risiko yang sudah diidentifikasi pada kerangka kerja acuan.

TABEL IV. PEMETAAN AKTIVITAS KEGIATAN PERLAKUAN

ISO/IEC 27005:2018 [15]	**NIST SP 800-30 Rev 1** [16]	**ISSP** [1]	**Wheeler** [7]
Modification, retention, avoidance, dan *sharing*	-	Kelas I, II, dan III mempunyai masing-masing perlakuan	*Accept, avoid, transfer,* dan *mitigate*

4) Aktivitas Kegiatan Administrasi

Tabel V pemetaan aktivitas kegiatan yang berkaitan dengan Administrasi pada setiap kerangka kerja yang menjadi acuan pada penyusunan desain.

TABEL V. PEMETAAN AKTIVITAS KEGIATAN ADMINISTRASI

ISO/IEC 27005:2018 [15]	**NIST SP 800-30 Rev 1**[16]	**ISSP** [1]	**Wheeler** [7]
Risk evaluation dan komunikasi	Komunikasi dan penyebaran informasi	Kontrol berdasarkan FDA	Penyusunan dokumen *risk decision,* implementasi rencana mitigasi, dan validasi

5) Aktivitas Kegiatan Pemantauan

Tabel VI pemetaan aktivitas kegiatan Pemantauan pada kerangka kerja acuan.

TABEL VI. PEMETAAN AKTIVITAS KEGIATAN PEMANTAUAN

ISO/IEC 27005:2018 [15]	**NIST SP 800-30 Rev 1** [16]	**ISSP** [1]	**Wheeler** [7]
Faktor risiko dan peningkatan manajemen risiko	Faktor risiko dan pembaharuan nilai risiko	Monitoring perangkat dan *patch management*	*Tracking* perubahan *risk profile*

Berdasarkan hasil pemetaan aktivitas kegiatan pada empat kerangka kerja acuan, diketahui bahwa terdapat tahapan yang harus ada pada proses manajemen risiko keamanan informasi, yaitu:

1) Tahap pendahuluan untuk menentukan tujuan dan ruang lingkup kegiatan.
2) Tahap identifikasi aset, kerentanan, ancaman, dan kontrol yang sudah ada.
3) Tahap pengukuran level risiko.
4) Tahap untuk menentukan bagaimana risiko yang sudah diidentifikasi dan diukur akan diperlakukan.
5) Tahap administrasi berupa penyusunan dokumen rencana tindak lanjut dan pemilihan kontrol.
6) Tahap pemantauan karena kegiatan manajemen risiko keamanan informasi bersifat siklis.

Hasil analisis terhadap profil risiko di sektor kesehatan, terdapat dua aset yang merupakan karakteristik sektor kesehatan, yaitu pengelolaan terhadap EHR atau rekamedis pasien dan penggunaan perangkat medis yang saling terhubung atau IoMT. Usulan desain membagi aset menjadi tiga jenis, yaitu aset berupa EHR, aset berupa perangkat medis atau IoMT, dan aset pendukung seperti jaringan, ruang *server*, dan lain sebagainya.

Desain kerangka kerja manajemen risiko keamanan informasi yang diajukan digambarkan pada Gambar 2.

1) Risk Profiling

Risk Profiling merupakan tahap awal yang dilakukan untuk menentukan profil risiko organisasi yang bergerak di sektor kesehatan. Tahap ini dilakukan untuk mengetahui bagaimana profil risiko yang ada pada organisasi sehingga dapat menjadi *input* dalam melakukan manajemen risiko keamanan informasi.

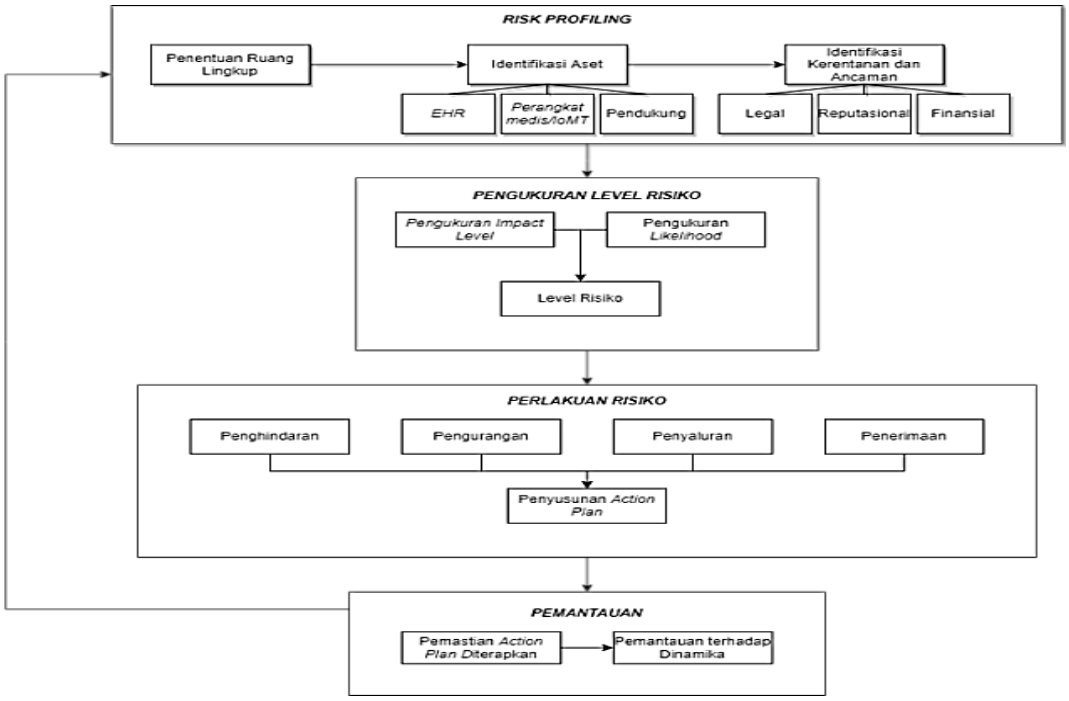
Risk Profiling terdiri atas tiga tahap, yaitu:

a. Identifikasi ruang lingkup

Identifikasi ruang lingkup dilakukan untuk menentukan cakupan manajemen risiko keamanan informasi pada organisasi. Pada tahap ini, dilakukan penentuan pihak yang terlibat dalam melakukan manajemen risiko keamanan informasi, apa saja yang akan menjadi objek manajemen risiko.

b. Identifikasi Aset

Pada kerangka kerja ini, terdapat tiga jenis aset yang ada pada sektor kesehatan, yaitu aset informasi yang berupa *electronic medical record* atau catatan rekamedis, aset berupa perangkat medis yang yang saling terhubung, dan aset pendukung atau *containment*. Aset pendukung dapat berupa perangkat keras, perangkat lunak, perangkat jaringan, sumber daya manusia, berbagai prosedur, dan lain sebagainya.



Gambar 2. Usulan Desain Kerangka Kerja Keamanan Informasi pada Sektor Kesehatan

c. Identifikasi kerentanan dan ancaman serta kontrol yang sudah ada

Setelah melakukan identifikasi terhadap aset yang dimiliki oleh organisasi, maka dilakukan identifikasi terhadap kerentanan dan ancaman pada aset tersebut. Risiko merupakan kombinasi antara kerentanan dan ancaman terhadap suatu aset yang dimiliki oleh organisasi. Kerentanan dan ancaman yang diidentifikasi juga berdasarkan analisis terhadap aspek finansial, legal, atau reputasional [7] apabila suatu ancaman tersebut mengeksploitasi kerentanan pada aset organisasi.

2) Pengukuran Level Risiko

Pada kerangka kerja yang diajukan, pengukuran level risiko disusun berdasarkan [16] dengan penyesuaian agar dapat mempermudah melakukan pengukuran level risiko pada sektor kesehatan. Terdapat lima skala yang digunakan untuk menentukan level risiko secara semi-kuantitatif.

Penilaian risiko dilakukan berdasarkan level dampak *(impact level)* yang diakibatkan bila suatu ancaman terjadi dan frekuensi terjadinya ancaman tersebut *(likelihood)*.

Tabel VII skala dampak yang akan diakibatkan bila risiko terjadi.

TABEL VII. SKALA DAMPAK

Nilai	Deskripsi	Keterangan
10	Sangat Tinggi	Mengakibatkan berbagai dampak yang sangat buruk bagi organisasi seperti membahayakan keselamatan jiwa pasien dan SDM, menyebabkan kerugian finansial yang besar, hilangnya reputasi, dan terhentinya proses bisnis fasilitas pelayanankesehatan untuk waktu yang lama.
8	Tinggi	Mengakibatkan dampak yang buruk bagi organisasi seperti membahayakan keselamatan jiwa pasien dan SDM, menyebabkan kerugian finansial yang besar, hilangnya reputasi, atau terhentinya proses bisnis fasilitas pelayanankesehatan untuk waktu yang lama.
5	Sedang	Mengakibatkan dampak serius bagi organisasi seperti menyebabkan cedera pasien dan SDM, menyebabkan kerugian finansial yang signifikan, berkurangnya reputasi, atau terhentinya proses bisnis fasilitas pelayanankesehatan dalam jangka waktu tertentu

Nilai	Deskripsi	Keterangan
2	Rendah	Mengakibatkan dampak yang kecil bagi organisasi seperti menyebabkan kerugian finansial yang kecil, atau menyebabkan kerusakan ringan pada aset fasilitas pelayanankesehatan
0	Sangat Rendah	Dampak yang ditimbulkan oleh suatu ancaman dapat diabaikan oleh fasilitas pelayanankesehatan karena sangat kecil.

Tabel VIII adalah skala kemungkinan terjadinya suatu risiko.

TABEL VIII. SKALA KEMUNGKINAN ATAU FREKUENSI

Nilai	Deskripsi	Keterangan
10	Sangat Tinggi	Risiko sangat sering terjadi, bahkan mencapai lebih dari 10 kali dalam setahun
8	Tinggi	Risiko sering terjadi, dalam satu tahun biasanya terjadi antara 6-10 kali
5	Sedang	Risiko beberapa kali terjadi, dalam satu tahun maksimal 5 kali terjadi
2	Rendah	Risiko jarang terjadi, dalam setahun maksimal satu kali terjadi
0	Sangat Rendah	Risiko sangat jarang terjadi, setiap tahun tidak selalu terjadi namun ada kemungkinan terjadi satu kali dalam beberapa tahun

Berdasarkan level dampak dan level kemungkinan terjadinya suatu risiko, dilakukan penilaian untuk mengetahui level risiko tersebut. Level risiko diperoleh dari perpaduan antara *impact level* dan *likelihood level* yang sudah ditentukan pada proses sebelumnya. Berikut ini adalah tabel perpaduan *impact level* dan *likelihood* yang menghasilkan level risiko.

Likelihood Level	*Impact Level*				
	Sangat Rendah	*Rendah*	*Sedang*	*Tinggi*	*Sangat Tinggi*
Sangat Tinggi	*Sangat Rendah*	*Rendah*	*Sedang*	*Tinggi*	*Sangat Tinggi*
Tinggi	*Sangat Rendah*	*Rendah*	*Sedang*	*Tinggi*	*Sangat Tinggi*
Sedang	*Sangat Rendah*	*Rendah*	*Sedang*	*Sedang*	*Tinggi*
Rendah	*Sangat Rendah*	*Rendah*	*Rendah*	*Rendah*	*Sedang*
Sangat Rendah	*Sangat Rendah*	*Sangat Rendah*	*Sangat Rendah*	*Rendah*	*Rendah*

Gambar 3. Perpaduan *Impact Level* dan *Likelihood Level* (sumber: NIST SP 800-30 Revision 1)

Setelah mengetahui kombinasi antara level dampak dan level kemungkinan dari suatu risiko, maka akan diperoleh level risiko yang terdiri atas lima skala. Tabel IX merupakan penjelasan masing-masing level risiko.

TABEL IX. SKALA LEVEL RISIKO

Nilai	Deskripsi	Keterangan
10	Risiko Sangat Tinggi	Mengakibatkan berbagai dampak yang sangat buruk bagi aset organisasi, seperti membahayakan keselamatan pasien dan SDM, merugikan pihak lain secara luas bahkan merugikan negara, hilangnya reputasi, dan lain sebagainya.
8	Risiko Tinggi	Mengakibatkan dampak yang buruk bagi aset organisasi dan merugikan berbagai pihak secara luas.
5	Risiko Sedang	Mengakibatkan dampak buruk yang merugikan dan serius pada proses operasional organisasi, aset, pihak lain, bahkan negara.
2	Risiko Rendah	Dampak yang ditimbulkan menyebabkan kerugian yang terbatas pada organisasi.
0	Risiko Sangat Rendah	Dampak yang ditimbulkan menyebabkan kerugian yang sangat kecil, bahkan dapat diabaikan.

3) Penanganan

Setelah level risiko diketahui, maka dapat diputuskan bagaimana organisasi akan memperlakukan risiko tersebut sesuai dengan levelnya. Pada kerangka kerja yang diajukan ini, terdapat empat jenis perlakuan terhadap risiko, yaitu menghindari, mengurangi, menyalurkan, dan menerima. Keempat pilihan untuk memperlakukan risiko yang diajukan mengacu pada tahapan *risk treatment* pada ISO/IEC 27005:2018 dan Wheeler [7], [15].

a. Penghindaran

Apabila level risiko berdasarkan hasil penilaian berada pada level yang tinggi atau sangat tinggi namun sumber daya yang diperlukan untuk menerapkan kontrol terhadap risiko tersebut terlalu besar, maka organisasi dapat memilih untuk menghindari risiko tersebut. Dengan demikian, risiko tersebut hampir dapat dipastikan tidak akan pernah terjadi.

b. Pengurangan

Apabila suatu risiko berada pada level yang sedang, tinggi, atau sangat tinggi namun tidak mungkin untuk menghindari risiko tersebut, maka organisasi dapat memilih untuk mengurangi nilai risiko tersebut ke level yang dapat diterima. Pengurangan risiko tersebut dapat dilakukan dengan menerapkan kontrol yang tepat dengan mempertimbangkan sumber daya yang diperlukan.

c. Penyaluran

Selain mengurangi risiko dengan kontrol tertentu, organisasi juga dapat membagi atau menyalurkan risiko dengan pihak lain agar lebih efektif. Dengan demikian, risiko yang ada akan ditanggung bersama dengan pihak lain tersebut, seperti asuransi atau subkontraktor.

d. Penerimaan

Organisasi dapat menerima risiko tanpa perlu melakukan apapun terhadap risiko tersebut karena level risiko berada pada level yang rendah atau sangat rendah, sehingga dapat diterima bahkan diabaikan oleh organisasi

Setelah menentukan bagaimana masing-masing risiko akan diperlakukan, perlu dilakukan pemetaan untuk melaksanakan pengelolaan risiko tersebut. Apabila risiko yang ada harus dihindari, dikurangi, atau disalurkan, maka organisasi perlu menyusun *Action Plan*. *Action Plan* adalah dokumen yang berisi daftar risiko serta tindakan yang *actionable* terhadap risiko tersebut dengan tujuan menjadi panduan bagi organisasi untuk menentukan tindakan apa saja yang perlu dilakukan dalam menangani risiko yang ada. Terdapat tiga hal yang harus ada pada dokumen *Action Plan*, yaitu *Person in Charge* yang bertanggung jawab untuk melakukan kontrol, *due date* atau batas waktu yang ditetapkan untuk menerapkan kontrol yang dipilih, dan perhitungan efektivitas kontrol yang dipilih dalam mengelola risiko yang ada. *Action Plan* disusun berdasarkan prioritas dan keadaan sumber daya organisasi agar tindak lanjut dalam manajemen risiko benar-benar dilakukan sehingga proses manajemen risiko dapat dilakukan dengan maksimal.

4) Pemantauan

Seluruh *output* yang dihasilkan dalam proses manajemen risiko perlu dipantau. Selain itu, dunia siber merupakan dunia yang dinamis dan selalu mengalami perubahan sewaktu-waktu. Dengan demikian, perlu dilakukan pemantauan secara berkala untuk memastikan bahwa risiko yang ada sudah dikelola dengan maksimal serta mengetahui apakah terdapat risiko baru bagi organisasi.

Pemantauan dilakukan untuk memastikan bahwa seluruh tindakan yang diperlukan dalam melakukan manajemen risiko benar-benar dilaksanakan dengan baik oleh seluruh pihak yang terlibat. Pemantauan juga dilakukan agar kontrol yang sudah ditetapkan dijalankan dengan baik.

Selain itu, pemantauan juga dilakukan untuk memperbarui profil risiko organisasi dalam konteks keamanan siber. Mengacu pada ISO/IEC 27005:2018, berikut ini adalah beberapa hal yang menyebabkan perlu dilakukannya pemantauan [15]:

a. Adanya aset baru atau modifikasi nilai aset milik organisasi dalam konteks keamanan siber.
b. Adanya ancaman baru pada sektor kesehatan yang akan membahayakan organisasi.
c. Adanya kerentanan baru pada sistem yang digunakan oleh organisasi sehingga apabila kerentanan tersebut dieksploitasi, akan menimbulkan kejadian yang merugikan.
d. Adanya *threat vector* baru pada sektor kesehatan.

Berdasarkan Wheeler, pemantauan dilakukan untuk mempertimbangkan apakah ada perubahan sumber daya yang signifikan, perubahan *threat landscape*, perubahan fokus bisnis organisasi, perubahan peraturan atau persyaratan legal, kelemahan baru yang terdeteksi, dan jangka waktu untuk melakukan manajemen risiko sudah habis. Berdasarkan pertimbangan terhadap hasil pemantauan tersebut, ditentukan apakah harus dilakukan manajemen risiko kembali pada organisasi.

Tabel X adalah hasil pemetaan setiap tahapan pada usulan desain kerangka kerja manajemen risiko keamanan informasi terhadap aktivitas kegiatan.

TABELX. TABEL HASIL PEMETAAN AKTIVITAS KEGIATAN TERHADAP USULAN KERANGKA KERJA

Aktivitas Kegiatan	Tahapan pada Usulan	Sub-tahapan	Output	Referensi
Identifikasi	*Risk Profiling*	Penentuan Ruang Lingkup	Tujuan kegiatan manajemen risiko keamanan informasi, pihak yang terlibat dalam kegiatan, sumber data yang akan digunakan, dan selera risiko	ISO/IEC 27005 [15], NIST SP 800-30 Rev 1 [16]
		Identifikasi Aset	Daftar aset TI yang sudah dikategorisasikan berdasarkan jenis	Yaqoob et.al. [1]
		Identifikasi Kerentanan	Daftar kerentanan pada setiap aset	ISO/IEC 27005 [15], Wheeler [7], Yaqoob et.al. [1], NIST SP 800-30 Rev 1 [16]
		Identifikasi Ancaman	Daftar ancaman yang dapat mengeksploitasi kerentanan pada setiap aset	ISO/IEC 27005 [15], Yaqoob et.a.l. [1], NIST SP 800-30 Rev 1[16]
		Identifikasi Kontrol yang Ada	Daftar kontrol yang sudah ada untuk setiap aset	ISO/IEC 27005 [15], Yaqoob et.al. [1]
Pengukuran	Pengukuran secara semi-kuantitatif	Level dampak	Skala level dampak	NIST SP 800-30 Rev 1[16]
		Level frekuensi	Skala level frekuensi	
		Level risiko	Skala level risiko	
Perlakuan	Pilihan memperlakukan risiko	Penghindaran	Pemilihan bagaimana risiko akan diperlakukan dilakukan berdasarkan selera risiko yang sudah ditentukan pada tahap Penentuan Ruang Lingkup	ISO/IEC 27005 [15], Wheeler [7]
		Pengurangan		
		Penyaluran		
		Penerimaan		
Administrasi	*Action Plan*	Prioritas kontrol	Kontrol baru yang dipilih sesuai prioritas	ISO/IEC 27005[15]
		Person in Charce	Pihak yang bertanggung jawab untuk melaksanakan setiap kontrol	Peltier [27]
		Due Date	Batas waktu pelaksanaan kontrol	
Pemantauan	Pemantauan	Pelaksanaan *Action Plan*	Pengawasan terhadap kesesuaian pelaksanaan *Actiion Plan*	Wheeler [7]
		Perubahan *threat landscape* dan dinamika organisasi	Pemantauan terhadap perubahan keadaan keamanan siber dan perubahan pada organisasi	ISO/IEC 27005 [15], Wheeler [7], NIST SP 800-30 Rev 1[16]

C. Pembahasan

Berdasarkan hasil penelitian yang dilakukan, tahap risk profiling merupakan tahap yang penting untuk dilakukan untuk mengetahui bagaimana profil risiko pada sektor kesehatan dalam konteks keamanan siber. Diawali dengan melakukan analisis terhadap aset apa saja yang penting bagi sektor kesehatan, penyusunan profil risiko keamanan pada sektor kesehatan dapat dilakukan dengan mempertimbangkan beberapa faktor, diantaranya aspek finansial, legal, dan reputasional [7].

Berdasarkan hasil *risk profiling*, sektor kesehatan mempunyai dua aset yang sifatnya kritikal yaitu *electronic health record* dan perangkat medis yang saling terhubung *(Internet of Medical Things).* Dua aset tersebut merupakan aset yang penting namun mempunyai berbagai kerentanan dalam konteks keamanan siber. Apabila kerentanan pada aset tersebut dieksploitasi, akan menimbulkan dampak yang merugikan organisasi sektor kesehatan terhadap aspek finansial, reputasi organisasi, keselamatan nyawa, maupun aspek legal atau hukum yang berlaku.

Pada kerangka kerja manajemen risiko keamanan informasi yang diajukan, *risk profiling* adalah tahap pertama yang dilakukan. Hal tersebut disebabkan karena profil risiko keamanan sangat

dibutuhkan oleh organisasi dalam tahap manajemen risiko keamanan informasi karena profil risiko tersebut berisi data terkait aset atau sumber daya organisasi yang sifatnya kritikal serta terdapat informasi mengenai sensitivitas dan kerentanan aset tersebut dalam konteks keamanan informasi [7]. Dengan melakukan *risk profiling* pada tahap awal, organisasi dapat mengetahui bagaimana keadaan kondisi aset atau sumber daya yang dimiliki serta risiko terhadap aset tersebut dalam konteks keamanan siber.

Pada desain kerangka kerja yang diajukan, tahap pertama yang dilakukan adalah Penentuan Ruang Lingkup. Tahap ini mengacu pada ISO/IEC 27005:2018 dan NIST SP 800-30 Rev 1 agar selama dilakukan manajemen risiko keaman informasi dapat fokus pada ruang lingkup yang sudah ditentukan di awal.

Pada tahap identifikasi aset, pada usulan kerangka kerja dibuat kategorisasi aset yang menjadi salah satu karakteristik sektor kesehatan, terutama fasilitas layanan kesehatan. Karakteristik tersebut adalah hampir setiap fasilitas layanan kesehatan melakukan pengelolaan terhadap data pribadi pasien atau rekam medis pasien, bahkan sebagian besar fasilitas layanan kesehatan mengelola data tersebut secara elektronik.

Tahapan Pengukuran Risiko dilakukan berdasarkan acuan kerangka kerja NIST SP 800-30 Rev 1. Pada acuan tersebut, salah satu pendekatan yang dapat digunakan untuk mengukur level risiko adalah pendekatan semi-kuantitatif. Pendekatan semi-kuantitatif yang digunakan dalam melakukan pengukuran risiko dapat memberikan manfaat baik secara kuantitatif maupun kualitatif [16]. Untuk mempermudah personil pada fasilitas layanan kesehatan melakukan pengukura risiko, maka level dampak disesuaikan dengan karakteristik yang ada pada fasilitas layanan kesehatan, yaitu berkaitan dengan kerugian finansial, hilangnya reputasi fasilitas pelayanan kesehatan, terhentinya operasional fasilitas layanan kesehatan, dan pelannggraran terhadap aturan yang berlaku bagi fasilitas layanan kesehatan.

Apabila risiko sudah diidentifikasi, maka ditentukan bagaimana risiko tersebut akan diperlakukan. Usulan kerangka kerja dalam memperlakukan risiko merujuk pada ISO/IEC 27005:2018 dan Wheeler. Pada kerangka kerja tersebut, terdapat empat kategori yang dapat dipilih untuk memperlakukan risiko, yaitu dihindari, dikurangi, disalurkan, atau diterima. Pemilihan perlakuan tersebut didasarkan pada selera risiko yang sudah ditentukan pada tahap Penentuan Ruang Lingkup.

Penyusunan *Action Plan* ditambahkan pada usulan kerangka kerja agar hasil kegiatan menajemen risiko keamanan informasi dapat segera ditindak lanjuti oleh instansi fasilitas pelayanan kesehatan.

Berikut ini adalah tabel perbandingan kerangka kerja yang menjadi acuan dengan usulan kerangka kerja manajemen risiko.

Usulan kerangka kerja sudah diuji coba pada fasilitas pelayanan kesehatan yaitu Puskesmas XYZ. Uji coba dibatasi sampai pada tahap 3, yaitu perlakuan risiko dengan *output* berupa dokumen manajemen risiko keamanan informasi. Tabel XI adalah hasil uji coba usulan kerangka kerja pada Puskesmas XYZ:

1) *Risk Profiling*

Berikut ini adalah hasil pada tahap *risk profiling* keadaan Puskesmas XYZ dalam konteks keamanan siber.

a. Penentuan ruang lingkup

Ruang lingkup yang ditentukan meliputi tujuan kegiatan, partisipan, sumber data, dan selera risiko. Yjuan kegiatan manajemen risiko keamana informasi aldalah untuk mengethaui risiko yang berkaitan dengan keamanan informasi pada proses bisnis Puskesmas XYZ. Apabila risiko yang ada sudah diketahui, maka dapat dikelola sesuai dengan sumber daya yang dimiliki. Partisipan kegiatan ini adalah staf Tata Usaha dan perwakilan tenaga kesehatan yang juga terlibat dalam pengelolaan data rekkamedis pasien. Sumber data yang digunakan adalah data historis Puskesmas XYZ dan hasil *focus group discussion* para partisipan kegiatan. Selera risiko yang diterima adalah risiko dengan level sangat rendah. Risiko dengan level rendah, sedang, dan tinggi akan dikurangi atau disalurkan. Risiko dengan level sangat tinggi akan dihindari, namun bila tidak dapat dihindari maka akan dikurangi atau disalurkan.

b. Identifikasi aset

Berdasarkan hasil analisis, diketahui bahwa puskesmas tersebut melakukan pengelolaan terhadap aset data rekam medis pasien menggunakan dua cara, yaitu melalui aplikasi Sistem Informasi Puskesmas (SIMPUS) yang terhubung ke Dinas Kesehatan Daerah dan melakukan *input* data secara manual ke komputer.

TABEL XI. TABEL PERBANDINGAN KERANGKA KERJA

Faktor Pembanding	**ISO/IEC 27005:2018**	**NIST SP 800-30 Rev 1**	**ISSP *Assessment Framework***	***Security Risk Management***	**Usulan Kerangka Kerja**
Tahapan penentuan ruang lingkup	Ada	Ada	-	-	Ada
Pembagian Jenis Aset	Primer dan sekunder	-	Kategorisasi aset berdasarkan *software, user interface*, dan sumber energi	-	EHR, Perangkat Medis/IoMT, dan Pendukung
Pendekatan Pengukuran Risiko	Kualitatif	Kuantitatif, Semi-kuantitatif, dan kualitati	Kuantitatif	Kualitatif	Semi-kuantitatif
Pilihan untuk Memperlakukan Risiko	Ada	Tidak Ada	Tidak Ada	Ada	Ada
Prioritas Risiko	Ada	Tidak Ada	Tidak Ada	Tidak Ada	Ada
Dokumen *Action Plan*	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Ada
Analisis terkait *Residual Risk*	Ada	Tidak Ada	Tidak Ada	Tidak Ada	Ada
Sifat kerangka kerja	Siklis	Siklis	Siklis	Siklis	Siklis

Puskesmas XYZ tidak mempunyai aset berupa perangkat medis yang terkoneksi dengan jaringan atau IoMT. Aset pendukung yang dimiliki oleh Puskesmas yaitu laptop atau komputer yang digunakan untuk operasional dan jaringan internal.

c. Identifikasi kerentanan dan ancaman

Aset data rekamedis yang di-*input* manual mempunyai kerentanan tidak dienkripsi dan tidak diberi *password* serta tidak ada mekanisme *back up* data yang sesuai dengan prosedur. Aset tersebut mempunyai ancaman berupa adanya penyalahgunaan oleh pihak yang tidak sah dan hilangnya data karena kesalahan teknis atau serangan *malware*. Kontrol yang sudah berjalan adalah proses *back up* data dilakukan dengan cara menyalin data tersebut secara manual ke dalam buku arsip.

Aplikasi SIMPUS mempunyai kerentanan berupa kurangnya *patch update* terkait keamanan aplikasi dan belum pernah dilakukan penilaian kerentanan terhadap aplikasi tersebut. Ancaman yang ada pada aplikasi tersebut adalah serangan *malware* atau peretasan serta aplikasi tidak dapat diakses *(down)* apabila *load* akses meningkat. Saat ini, belum ada kontrol yang diterapkan pada aplikasi tersebut.

Aset berupa komputer atau laptop untuk operasional mempunyai kerentanan tidak ada kebijakan akses kontrol sehingga ada ancaman berupa penyalahgunaan oleh pihak yang tidak sah. Belum ada kontrol yang diterapkan pada aset tersebut.

Kerentanan pada aset jaringan internal adalah tidak dilakukannya pemeliharaan dan perawatan secara rutin dan menyeluruh. Ancaman pada aset tersebut adalah adanya kesalahan dalam konfigurasi jaringan dan adanya serangan *malware* atau peretasan. Belum ada kontrol yang diterapkan untuk risiko pada aset ini.

2) Pengukuran Level Risiko

Berdasarkan hasil penilaian dari tujuh risiko yang ada, terdapat tiga risiko level tinggi dan empat risiko level sedang. Risiko yang mempunyai level tinggi adalah hilangnya data karena kesalahan teknis atau serangan *malware* pada data rekamedis yang di-*input* secara manual ke komputer, aplikasi SIMPUS yang *down* sehingga tidak dapat diakses, dan kesalahan pada konfigurasi jaringan internal

Puskesmas. Risiko dengan level sedang yaitu penyalahgunaan data rekamedis yang di-*input* manual oleh pihak yang tidak sah, adanya serangan *malware* atau peretasan pada aplikasi SIMPUS, penyalahgunaan komputer atau laptop operasional oleh pihak yang tidak sah, dan adanya serangan *malware* atau peretasan pada jaringan internal.

3) Perlakuan Risiko

Sesuai dengan selera risiko yang sudah ditentukan, maka tujuh risiko yang sudah diidentifikasi akan dikurangi dengan menerapkan kontrol tertentu. Kontrol tersebut dimuat dalam Tabel XII.

TABELXII. TABEL *ACTION PLAN* PADA PUSKESMAS XYZ

Risiko	**Kontrol**	***PIC***	***Due Date***
Hilangnya data rekamedis karena kesalahan teknis atau serangan *malware*	Prosedur *back up* terhadap data dalam kurun waktu yang teratur	Staf TU	Juni 2022
Aplikasi SIMPUS *down* sehingga tidak dapat diakses	Dilakukan *patch management* terhadap aplikasi secara berkala	Staf TU	Juli 2022
Kesalahan pada konfigurasi jaringan internal	Dilakukan pemantauan dan audit secara teratur terhadap layanan jaringan internal yang diberikan oleh *supplier*	Staf TU dan teknisi jaringan	Juni 2022
Penyalahgunaan data rekamedis oleh pihak tidak sah	Pemberian *password* pada data rekamedis dan disimpan dalam bentuk terenkripsi	Staf TU dan tenaga kesehatan	Juni 2022
Adanya serangan *malware* atau peretasan pada aplikasi SIMPUS	Pemasangan *antivirus* dan *firewall*, dilakukan *back up* secara teratur terhadap data di SIMPUS	Staf TU	Juli 2022
Penyalahgunaan perangkat komputer atau laptop operasional oleh pihak yang tidak sah	Pemberian kredensial (*username* dan *password)* pada setiap komputer atau laptop	Staf TU	Juni 2022
Adanya serangan *malware* atau peretasan pada jaringan internal	Penggunaan *firewall*, mekanisme deteksi *malicious website* dengan *blacklisting* atau *whitelisting*	Staf TU	Januari 2023

Pada uji coba tersebut, dilakukan evaluasi terhadap usulan kerangka kerja manajemen risiko keamanan informasi. Evaluasi dilakukan dengan menggunakan kuesioner yang diberikan kepada responden di Puskesmas XYZ. Berdasarkan kuesioner tersebut, dinyatakan bahwa usulan kerangka kerja sudah menggambarkan urutan tahapan manajemen risiko keamanan informasi, telah mencakup seluruh aktivitas yang diperlukan untuk melakukan manajemen risiko keamanan informasi, dan dapat diaplikasikan pada instansi fasilitas pelayanan kesehatan.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa sektor kesehatan mempunyai dua aset utama yang sangat penting namun rentan terhadap serangan siber, yaitu *electronic health record* atau rekamedis kesehatan dan perangkat medis yang terhubung dengan jaringan. Berdasarkan hasil *risk profiling*, dapat disimpulkan bahwa sektor kesehatan merupakan salah satu sektor yang rentan terhadap adanya serangan siber, bahkan menjadi target utama serangan.

Kerangka kerja manajemen risiko keamanan informasi yang diajukan pada penelitian ini dibuat berdasarkan profil risiko tersebut. Karena dunia siber merupakan ranah yang sangat dinamis dan selalu mengalami perubahan, maka kerangka kerja yang diajukan bersifat siklis dan perlu dilakukan dalam jangka waktu tertentu. Tahap pertama yang dilakukan pada kerangka yang diajukan adalah *Risk Profiling* agar organisasi pada sektor kesehatan mengetahui profil risiko organisasi mereka. Dengan memahami profil risiko tersebut, maka dapat dilakukan pengelolaan terhadap risiko yang ada agar tidak menyebabkan dampak yang merugikan organisasi. Selain itu, mengetahui profil risiko pada sektor kesehatan secara umum juga merupakan bagian dari pemantauan, sebagai bahan masukan pada tahap *Risk Profiling* berikutnya.

Kerangka kerja yang diajukan terdiri atas empat tahap, yaitu *Risk Profiling*, Pengukuran Level Risiko dengan pendekatan semi-kuantitatif, Perlakukan Risiko, dan Pemantauan. Masing-masing tahap saling berkaitan satu sama lain karena *output* yang dihasilkan pada satu tahap menjadi *input* bagi tahap selanjutnya. Selain itu, kerangka kerja yang diajukan sifatnya siklis sehingga *Risk Profiling* perlu dilakukan baik secara umum dalam sektor kesehatan maupun secara khusus pada organisasi untuk mengantisipasi perubahan yang terjadi dalam konteks keamanan siber.

Berdasarkan hasil evaluasi, kerangka kerja yang diajukan sudah menggambarkan urutan tahapn yang ada pada kegiatan manajemen risiko keamanan informasi. Usulan tersebut juga sudah mencakup keseluruhan aktivitas yang diperlukan pada kegiatan manajemen risiko keamanan informasi dan dapat diterapkan pada instansi sektor kesehatan.

Penelitian lebih lanjut perlu dilakukan untuk melakukan uji coba usulan kerangka kerja manajemen risiko keamanan informasi yang diajukan pada fasilitas layanan kesehatan lain seperti klinik dan rumah sakit.

REFERENSI

[1] T. Yaqoob, H. Abbas, and N. Shafqat, "Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 6, pp. 1752–1761, Jun. 2020, doi: 10.1109/JBHI.2019.2952906.

[2] A. Umejiaku and T. Dang, "Visualising Developing Nations Health Records: Opportunities, Challenges and Research Agenda," Jun. 2021. doi: 10.1145/3468784.3471607.

[3] IBM Security, "Cost of a Data Breach Report 2021," 2021.

[4] FireEye and Mandiant, "M-Trends 2021 Fireeye Mandiant Service Special Report," 2021.

[5] McAfee, "McAfee Labs Threat Report 06.2021," 2021.

[6] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," *International Journal for Quality in Health Care*, vol. 33, no. 1, 2021, doi: 10.1093/intqhc/mzaa117.

[7] E. Wheeler, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Waltham USA: Elsevier Inc., 2011.

[8] A. D. Prajanti and K. Ramli, "A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods."

[9] J. Meszaros and A. Buchalcevova, "Introducing OSSF: A framework for online service cybersecurity risk management," *Computers and Security*, vol. 65, pp. 300–313, Mar. 2017, doi: 10.1016/j.cose.2016.12.008.

[10] C. Joshi and U. K. Singh, "Information security risks management framework – A step towards mitigating security risks in university network," *Journal of Information Security and Applications*, vol. 35, pp. 128–137, Aug. 2017, doi: 10.1016/j.jisa.2017.06.006.

[11] I. Baehaki, "Desain Kerangka Kerja Manajemen Risiko Keamanan Informasi Berdasarkan Integrasi ISO/IEC 27005:2018, NIST SP 800-39, OCTAVE Allegro, dan COBIT 2019 (Studi Penerapan Awal di Pusat Pendidikan dan Pelatihan Badan XYZ)," Universitas Indonesia, Jakarta, 2020.

[12] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," *Business Horizons*, vol. 64, no. 5, pp. 659–671, Sep. 2021, doi: 10.1016/j.bushor.2021.02.022.

[13] Direktorat Proteksi Infrastruktur Informasi Kritikal Nasional BSSN, "Buku Putih Keamanan SIber Sektor Kesehatan," Jakarta, 2020.

[14] Sugiyono, *Metode Penelitian Kuantitatif Kualitatif dan R&D*, 3rd ed. Bandung: Alfabeta, 2021.

[15] *ISO/IEC 27005: Information technology - Security techniques - Information security risk management*. 2018.

[16] National Institute of Standards and Technology, *NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments*. U.S., 2012.

[17] H. Alami, M. P. Gagnon, M. A. Ag Ahmed, and J. P. Fortin, "Digital health: Cybersecurity is a value creation lever, not only a source of expenditure," *Health Policy and Technology*, vol. 8, no. 4, pp. 319–321, Dec. 2019, doi: 10.1016/j.hlpt.2019.09.002.

[18] S. Tarikere, I. Donner, and D. Woods, "Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G," *Business Horizons*, vol. 64, no. 6, pp. 799–807, Nov. 2021, doi: 10.1016/j.bushor.2021.07.015.

[19] I. Lee, "An analysis of data breaches in the U.S. healthcare industry: diversity, trends, and risk profiling," *Information Security Journal*, 2021, doi: 10.1080/19393555.2021.2017522.

[20] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic," 2020.

[21] N. M. Thomasian and E. Y. Adashi, "Cybersecurity in the Internet of Medical Things," *Health Policy and Technology*, vol. 10, no. 3, Sep. 2021, doi: 10.1016/j.hlpt.2021.100549.

[22] D. v Dimitrov, "Medical Internet of Things and Big Data in Healthcare," *Healthc Inform Res*, vol. 22, no. 3, pp. 156–163, Jul. 2016, doi: 10.4258/hir.2016.22.3.156.

[23] K. S. Bhosale, M. Nenova, and G. Iliev, "A study of cyber attacks: In the healthcare sector," 2021. doi: 10.1109/Lighting49406.2021.9598947.

[24] N. Thamer and R. Alubady, "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research," in *1st Babylon International Conference on Information Technology and Science 2021, BICITS 2021*, 2021, pp. 210–216. doi: 10.1109/BICITS51482.2021.9509877.

[25] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 3723–3768, Oct. 2019, doi: 10.1109/COMST.2019.2914094.

[26] P. Deshanta Ibnugraha, L. E. Nugroho, and P. I. Santosa, "Metrics analysis of risk profile: A perspective on business aspects," in *2018 International Conference on Information and Communications Technology, ICOIACT 2018*, Apr. 2018, vol. 2018-January, pp. 275–279. doi: 10.1109/ICOIACT.2018.8350675.

[27] T. R. Peltier, *Information Security Risk Analysis Third Edition*, 3rd ed. Florida: Auerbach Publications Tayor & Francis Group, 2010.