Analisis Risiko Jaringan Komputer untuk Meningkatkan Kualitas Keamanan pada Jaringan Komputer Rumah Sakit Universitas Muhammadiyah Semarang

Akhmad Fathurohman[1]✉, Riza Setiawan[2], Faris Eka Darmawan[3]
[1-3]Universitas Muhammadiyah Semarang, Indonesia

✉Corresponding Author: akhmadfathur@unimus.ac.id

ABSTRAK

Upaya peningkatan meningkatkan kualitas keamanan pada jaringan komputer Rumah Sakit Universitas Muhammadiyah Semarang (RS Unimus) sangat penting karena berbagai risiko yang dapat mengancam keamanan dan integritas data yang sangat sensitif, terlebih rumah sakit merupakan fasilitas layanan umum kesehatan yang harus terus meningkatkan kepercayaan masyarakat. Jaringan komputer sangat penting untuk kelancaran teknologi informasi yang diterapkan di rumah sakit. Dengan jaringan yang baik, informasi medis dapat diakses dengan cepat, sehingga pasien dapat menerima pelayanan kesehatan dengan tepat dan cepat. RS Unimus mengimplementasikan dan mengembangkan teknologi informasi yang didukung dengan jaringan komputer dalam mengembangkan sistem informasi manajemen rumah sakit (SIMRS) RS Unimus terintegrasi. Metode yang digunakan adalah metode analisis Risiko (*Risk Analysis*) sesuai dengan standar keamanan jaringan ISO 27001:2022 *Information Security Management Systems Risk Analysis.* Hasil analisis risiko jaringan komputer di RS Unimus menunjukkan berbagai tantangan dan potensi ancaman yang dapat memengaruhi operasional dan keamanan sistem informasi. Simpulan dari hasil identifikasi risiko utama, yaitu: (1) Data hilang, (2) Serangan dan gangguan siber (3) Mati listrik (4) Kegagalan booting komputer; (5) Kegagalan penginputan data; (6) Jaringan lambat; dan (7) Kerusakan hardware. Dampak dari risiko tersebut dapat beragam, mulai dari gangguan layanan hingga kerugian finansial dan reputasi RS Unimus. Beberapa langkah strategi mitigasi risiko yang disarankan: (1) Peningkatan keamanan sistem yaitu menggunakan firewall, antivirus, dan prosedur keamanan lainnya untuk melindungi data dan sistem dari ancaman eksternal; (2) Rutin melakukan backup data sehingga dipastikan data tetap aman dan pemulihan cepat; (3) Pelatihan staf mengenai peningkatan kemamuan TIK dan keamanan informasi; (4) Penyediaan infrastruktur cadangan agar sumber daya cadangan dapat menjaga kelangsungan operasional saat terjadi gangguan. Selanjutnya dirancang langkah-langkah mitigasi yang efektif, RS Unimus dapat menjaga ketersediaan dan kinerja sistem informasi mereka, serta melindungi data pasien dengan lebih baik.

Kata Kunci: risiko, jaringan komputer, rumah sakit

A. Pendahuluan

Rumah sakit sekarang ini mau tidak mau harus memiliki unit manajemen Teknologi Informasi dan Komunikasi (TIK), karena sudah menjadi kebutuhan karena seluruh system dan aplikasi membutuhkan layanan teknologi informasi. RS Unimus telah memiliki unit pengelola TIK yang mengelola infra struktur jaringan computer, pusat data (*Data Center*), SIMRS yang melingkupi seluruh manajemen di rumah sakit. Faktor yang sangat penting untuk diperhatikan dalam penyelenggaraan tata kelola TIK adalah keamanan informasi karena jika informasi sebagai salah satu objek utama dalam tata kelola TIK mengalami permasalahan dalam keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

Keamanan informasi menjadi sangat penting bagi instansi atau organisasi karena bukan hanya informasi internal instansi atau organisasi saja yang harus diperhatikan, tetapi informasi

pelanggan juga harus diperhatikan dan dipertimbangkan. Informasi pelanggan yang tidak aman dapat berisiko besar bagi pelanggan itu sendiri, seperti kebocoran data pribadi yang dapat digunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penting bagi organisasi untuk mengimplementasikan sistem keamanan informasi yang baik dan teratur agar informasi pelanggan tetap aman dan tidak dapat diakses oleh pihak yang tidak berwenang. Keamanan informasi menjadi sangat penting bagi instansi atau organisasi karena bukan hanya informasi internal instansi atau organisasi saja yang harus diperhatikan, tetapi informasi pelanggan juga harus diperhatikan dan dipertimbangkan terlebih bagi fasilitas layanan kesehtan (*Fasyankes*) seperti Rumah Sakit.[1]

Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi telah mengatur tentang sistem manajeman pengamanan informasi dengan menetapkan batasan istilah yang digunakan dalam pengaturannya. Dengan peraturan ini menjadi hal yang sangat penting bagi RS Unimus untuk berupaya meningkatkan keterjaminan keamanan informasi sehingga kualitas layanan informasi terjamin yang menyangkut informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) data dan informasi dengan memanfaatkan teknologiinformasi terutama pemanfaatan SIMRS. Kondisi saat ini IT RS Unimus yang berada pada satu bidang di bawah Manager Umum yang memiliki peran mengatur dan mengelola kebutuhan system informasi dan teknologi informasi untuk mendukung seluruh manajemen rumah sakit.[2]

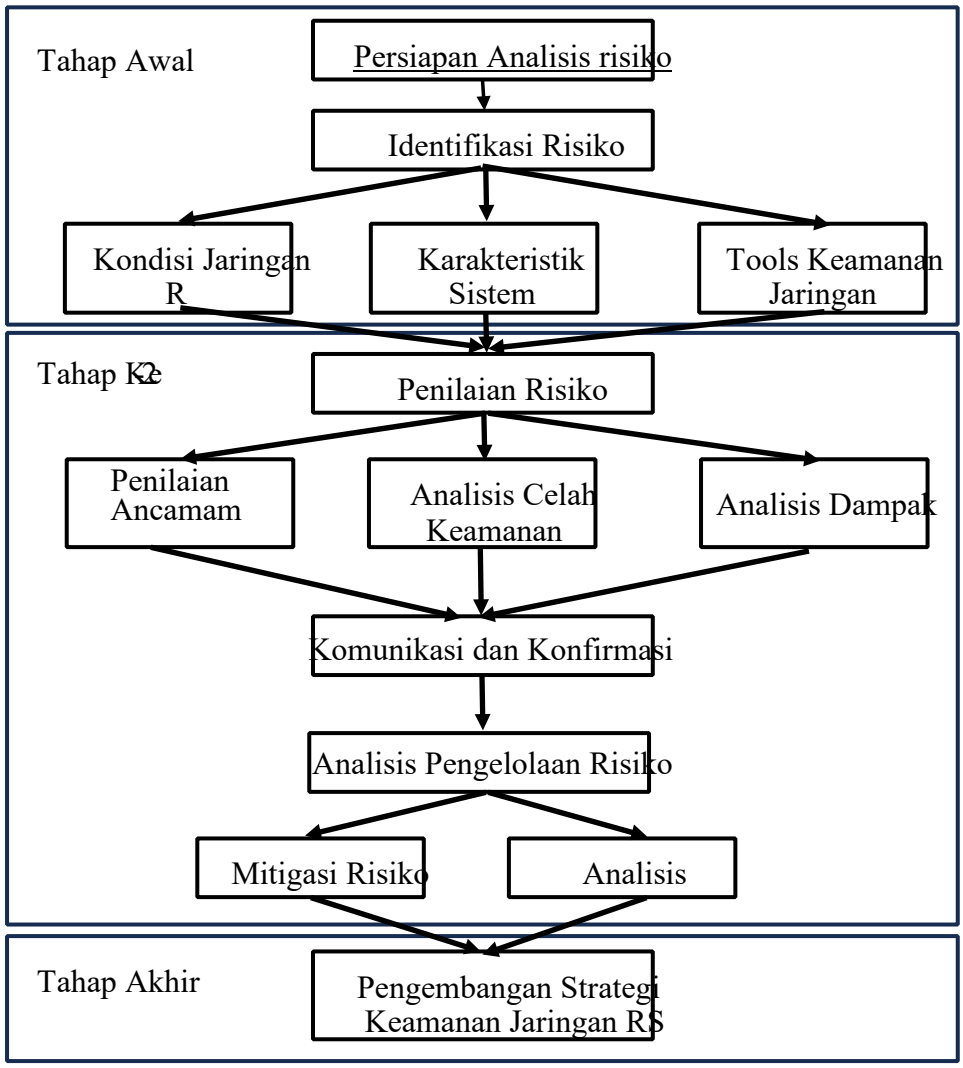
International Organization for Standardization (ISO) dan *International Electrotechnical Commission* (IEC). Mengeluarkan Standar internasional manajemen Teknologi informasi dan mengeluarkan panduan yang terdiri dari spesifikasi, pedoman, dan praktik terbaik untuk berbagai produk, layanan, dan proses. ISO/IEC standar dirancang untuk memastikan bahwa produk dan layanan aman, andal, dan berkualitas tinggi, serta kompatibel satu sama lain.[3] Mereka juga membantu memastikan bahwa produk dan layanan konsisten dan berkualitas tinggi, di mana saja mereka diproduksi atau digunakan. Terkait keamanan Informasi diterbitkan ISO 27001 yang memuat referensi untuk menentukan dan menerapkan kontrol untuk penanganan risiko keamanan informasi pada sistem manajemen keamanan informasi (*Information Security Management System* /ISMS) berdasarkan ISO/IEC 27001. Kontrol khusus organisasi atau lingkungan selain yang termasuk dalam dokumen ini dapat ditentukan melalui penilaian risiko jika diperlukan. ISO yang digunakan terbaru yaitu ISO 27002:2022 mencakup satu set referensi kontrol keamanan informasi umum, termasuk panduan implementasi.[4] Dokumen ini dirancang untuk membantu organisasi dalam memilih, menerapkan, dan memelihara Sistem Manajemen Keamanan Informasi (SMKI). Standar ini digunakan sebagai panduan yang lebih spesifik dari kerangka kerja ISO 27001 untuk memilih kontrol keamanan yang sesuai dengan organisasi masing-masing.[2]

B. Perumusan Masalah

Perumusan masalah dalam penelitian ini, yaotu : (1) apas risiko yang mungkin terjadi dalam pengelolaan jaringan computer di RS Unimus, (2) bagaiman Pengelolaan risiko sehingga risiko dapat antisipasi sedini mungkin, sehingg akualitas layanan jaringan computer semakin baik, dan (3) bagaimana pemantauan dan evaluasi nya pelaksanaan manajemen risiko sehingga semua risiko dapat dikendalikan dengan baik.

C. Metode Penelitian

Metode dalam penelitian ini adalah *risk analysys* dengan langkah-langkah untuk meningkatkan kualitas keamanan pada jaringan komputer RS Unimus melibatkan dengan tahapa penting sebagai berikut.

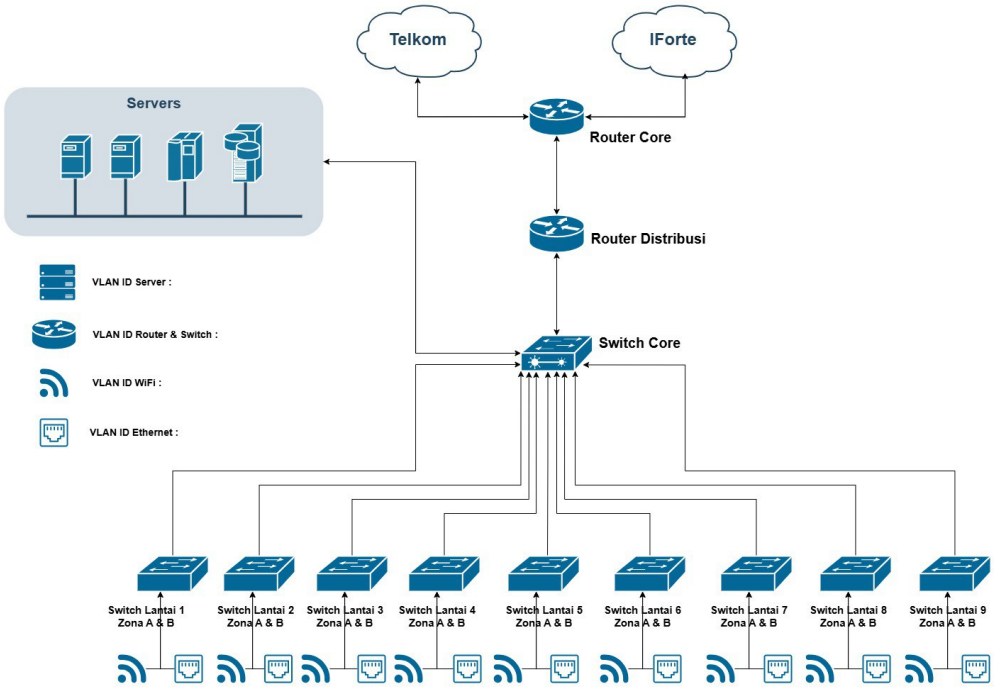


Gambar 1. Langkah-langkah penelitian

Tahap awal meiluti persiapan anlisis risiko, identifikasi resiku terhadap kondisi jaringan Komputer RS Unimus, Kondisi Sistem yang digunakan di RS Unimus dan peralatan keamanan jaringan yang digunakan. Tahap kedua penilaian risiko yang meliputi penilianan terhadap ancamanbari dari dalam maupun daru luar RS Unimus, analisis celah keamanan, dan analisis dampak, selanjutnya hasil analisis dikomunikasikan dan dikonfirmasi terhadap manajemen IT di RS Unimus yang selanjutnya dilakukan pe ngelolaan risiko melalui mitigasi risiko dan analisis permasalahan yang dihadapinya. Pada Tahap akhir dilakukan pengembangan strategi keamanan jaringan RS Unimus.

D. Hasil dan Pembahasan

Kondisi jaringan RS Unimus telah di desain dan diimple,entasikan secara baik sesuai dengan standar pengelolana jaringan komputer menggunakan topologi hierarchical seperti disajikan dalam gambar berikut.



Gambar 2. Topologi jaringan komputer RS Unimus Tahun 2024

Dari gambar 2. Sesuai dengan hasil pengamatan langsung dan penjelasan kepala bagian IT RS Unimus, terlihat bahwa jaringan komputer unimus terhubung ke jaringan internet melalui dua provider, yaitu PT Telkom Indonesia dan PT iForte Solusi Infotek. Selanjutnya dikendalikan menggunakan router utama (*Core Router*) Mikrotik dan router distribusi untuk membagi jaringan ke setiap gedung dan bagian manajemen di RS. Tersedia juga pusat dengan berbagai server yang sangat memadai untuk sistem informasi rumah sakit dan berbagai aplikasi pendukung kapasitas manajemen RS Unimus.

Berikut adalah tabel yang merangkum hasil analisis risiko jaringan komputer di rumah sakit berdasarkan penerapan standar ISO 27001:2022. Tabel ini mencakup kategori aset, ancaman yang diidentifikasi, dan tindakan mitigasi yang direkomendasikan.

Tabel 1. Kategori Aset dan Ancaman

Kategori Aset	Ancaman	Tingkat Risiko	Tindakan Mitigasi
Hardware	Kerusakan fisik (misalnya, kebakaran, banjir)	Tinggi	Pemeliharaan rutin, asuransi aset, dan penggunaan UPS

Kategori Aset	Ancaman	Tingkat Risiko	Tindakan Mitigasi
	Pencurian perangkat	Sedang	Pemasangan sistem keamanan fisik dan CCTV
Software	Serangan siber seperti malware (virus, ransomware)	Tinggi	Penggunaan antivirus dan firewall, pembaruan sistem
	Bug atau kesalahan dalam aplikasi	Sedang	Pengujian perangkat lunak secara berkala
Network	Gangguan konektivitas (jaringan *down*)	Tinggi	Redundansi jaringan dan pemantauan lalu lintas
	Penyadapan informasi	Tinggi	Enkripsi data dan penggunaan VPN
Data dan Informasi	Kebocoran data	Sangat Tinggi	Kebijakan kontrol akses yang ketat dan enkripsi data
	Kehilangan data	Tinggi	Backup data secara berkala
People	Kesalahan manusia (input data yang salah)	Sedang	Pelatihan rutin untuk karyawan
	Penyalahgunaan hak akses	Sangat Tinggi	Audit akses secara berkala dan pengawasan ketat

Pada kategori aset dikelompokkan elemen-elemen penting dalam infrastruktur teknologi informasi rumah sakit, selanjutnya pada ancaman disebutkan potensi risiko yang dapat mempengaruhi keamanan informasi. Pada tingkat risiko diindikasikan seberapa besar dampak yang mungkin terjadi jika ancaman tersebut terealisasi. Selanjutnya pada tindakan mitigasi diberikan hasil analisis yang menghasilkan rekomendasi langkah-langkah untuk mengurangi atau mengelola risiko yang teridentifikasi.

Analisis risiko jaringan komputer di RS Unimus menggunakan standar ISO 27001:2022 yaitu mengidentifikasi, mengevaluasi, dan mengelola risiko yang terkait dengan keamanan informasi.

Sesuai dengan fungsinya bahwa ISO 27001:2022 adalah standar internasional yang memberikan kerangka kerja untuk manajemen keamanan informasi (ISMS). Standar ini membantu organisasi, termasuk rumah sakit, dalam melindungi data sensitif dan memastikan kontinuitas layanan.

Identifikasi risiko yang berhasil diinentifikasi diantaranya adalah: (1) Risiko data hilang, yaitu kegagalan dalam sistem backup atau pemulihan data dapat menyebabkan kehilangan informasi penting. (2) Serangan siber: Ancaman dari malware, ransomware, atau peretasan yang dapat mengakses data pasien. (3) Kegagalan sistem, meliputi masalah perangkat keras atau perangkat lunak yang dapat menghentikan operasional SIMRS. (4) Kesalahan manusia, yang sering terjadi di RS Unimus adalah kesalahan pada penginputan data yang tidak akurat atau penyalahgunaan akses oleh pengguna.(5) koneksi jaringan yang tidak stabil, terkait dengan pengaturan banwidth untuk pengguna dan kesalahan sambungan jaringan fisik yang dapat mengganggu akses ke sistem informasi dan memperlambat pelayanan.

Rekomendasi mitigasi dari hasil identifikasi dan analisis analisis risiko jaringan komputer di RS Unimus disajikan pada tabel berdasarkan analisis menggunakan ISO 27001:2022 nsebagai berikut.

Tabel 2. Mitigasi Risiko yang Dapat Diterapkan

ID Risiko	Deskripsi Risiko	Dampak	Mitigasi yang Diterapkan	Status
R1	Data hilang akibat kegagalan backup	Kehilangan informasi penting	- Backup data secara rutin - Penyimpanan cadangan di lokasi terpisah	Dalam Proses
R2	Serangan siber (malware, ransomware)	Kebocoran data dan kerusakan sistem	- Pemasangan firewall dan antivirus - Pelatihan keamanan untuk staf	Aktif
R3	Kegagalan perangkat keras	Gangguan operasional	- Pemeliharaan rutin perangkat keras - Pengadaan perangkat cadangan	Dalam Proses
R4	Penyalahgunaan hak akses oleh pengguna	Kebocoran informasi sensitif	- Kontrol akses yang ketat - Audit akses secara berkala	Aktif
R5	Jaringan lambat atau terputus	Keterlambatan layanan	- Peningkatan infrastruktur jaringan - Pemantauan kinerja jaringan	Dalam Proses
R6	Kesalahan manusia dalam penginputan data	Data tidak akurat	- Pelatihan penggunaan SIMRS untuk staf - Prosedur verifikasi data	Aktif
R7	Kerusakan hardware	Gangguan pada sistem informasi	- Penyediaan ruang server khusus - Instalasi UPS untuk perlindungan	Dalam Proses

Tabel di atas memberikan gambaran mengenai risiko yang ada, dampaknya, serta langkah-langkah mitigasi yang telah diterapkan di rumah sakit untuk menjaga keamanan dan kelangsungan operasional jaringan komputer.

Dari tabel tersebut dapat dijelaskan hal-hal yang direkomendasikan adalah:

1. **Backup Data**: Melakukan backup secara rutin untuk mencegah kehilangan data penting.
2. **Keamanan Sistem**: Menggunakan firewall dan antivirus untuk melindungi sistem dari serangan siber yang senantiasa di chek secara rutin keberfungsiannya dalam mengantisipasi setiap serangan yang masuk.
3. **Pemeliharaan Rutin**: Menjadwalkan pemeliharaan perangkat keras untuk mencegah kerusakan.
4. **Kontrol Akses**: Mengimplementasikan kontrol akses yang ketat untuk mencegah penyalahgunaan hak akses, pengecekan secara berkala terhadap akun akun pengguna dan disarankan rutin penggantian password.
5. **Peningkatan Infrastruktur**: Memperbaiki dan meningkatkan infrastruktur jaringan untuk memastikan ketersediaan layanan sesuai kebutuhan pada setiap unit manajemen di RS Unimus.
6. **Pelatihan Staf**: Memberikan pelatihan kepada staf tentang pengoperasian sistem dan keamanan informasi, sehingga menjadi budaya pengamanan siber yang dimulai dari setiap pengguna.
7. **Ruang Server Khusus**: Meningkatkan ruang server yang lebih aman dan terlindungi

untuk mengurangi risiko kerusakan, dan akses yang terkontrol dengan baik.

Peningkatan Keamanan Sistem menjadi hal yang sangat penting dengan langkah-langkah keamanan diantaranya: (1) Implementasi kontrol akses yang ketat untuk melindungi data sensitif, (2) penggunaan *firewall* dan antivirus untuk melindungi dari serangan siber, (3) pelatihan staf dengan menyediakan pelatihan reguler mengenai keamanan informasi dan penggunaan SIMRS, (4) prosedur *backup* data dengan melakukan backup data secara rutin dan menyimpannya di lokasi terpisah untuk pemulihan cepat, dan (5) audit dan evaluasi secara berkala dengan melakukan audit keamanan secara berkala untuk mengevaluasi efektivitas kontrol yang diterapkan.

Dengan menerapkan ISO 27001:2022, rumah sakit dapat mengidentifikasi dan mengelola risiko jaringan komputer secara efektif, sehingga meningkatkan keamanan informasi dan kualitas pelayanan kesehatan kepada pasien. Penerapan langkah-langkah mitigasi yang tepat akan membantu meminimalkan dampak dari potensi ancaman terhadap sistem informasi rumah sakit.

Analisis risiko menggunakan standar ISO 27001 memberikan gambaran komprehensif mengenai potensi ancaman terhadap jaringan komputer di rumah sakit. Dengan menerapkan tindakan mitigasi yang tepat, rumah sakit dapat meningkatkan keamanan sistem informasi dan melindungi data pasien secara efektif. Pelaksanaan di rumah sakit seluruh risiko yang tinggi telah dilakukan mitigasi dan telah menggunakan Standar operasional prosedur yang sesuai.

E. Simpulan

Hasil analisis risiko jaringan komputer di RS Unimus menunjukkan berbagai tantangan dan potensi ancaman yang dapat mempengaruhi operasional dan keamanan sistem informasi. Berikut adalah simpulan dari analisis risiko yang dilakukan, melalui identifikasi risiko utama, yaitu: (1) Data hilang, risiko ini muncul akibat kegagalan dalam proses backup dan pemulihan data setelah kehilangan informasi;(2) Serangan dan gangguan siber yang dapat mengganggu pada sistem, data, kelambatan jaringan. (3) Mati listrik, perangkat tidak bisa beroperasi yang dapat mengganggu operasional SIMRS; (4) Kegagalan booting komputer: Masalah ini dapat menghalangi akses staf ke SIMRS; (5) Kegagalan penginputan data: Mengakibatkan informasi yang tidak akurat dalam sistem; (6) Jaringan lambat, dapat menyebabkan gangguan akses dan penggunaan SIMRS, memengaruhi efisiensi operasional; (7) Kerusakan hardware: Dapat mengganggu ketersediaan perangkat dan kinerja system. Dampak dari risiko-risiko tersebut dapat beragam, mulai dari gangguan layanan hingga kerugian finansial dan reputasi RS Unimus. Dengan mengidentifikasi risiko-risiko ini selanjutnya dirancang langkah-langkah mitigasi yang efektif, RS Unimus dapat menjaga ketersediaan dan kinerja sistem informasi mereka, serta melindungi data pasien dengan lebih baik.Beberapa langkah strategi mitigasi risiko yang disarankan meliputi: (1) Peningkatan keamanan sistem: Menggunakan *firewall*, antivirus, dan prosedur keamanan lainnya untuk melindungi data dan sistem dari ancaman eksternal; (2) Rutin melakukan backup data sehingga dipastikan data tetap aman dan dapat dipulihkan jika terjadi kehilangan; (3) Pelatihan untuk meningkatkan pengetahuan staf mengenai pengoperasian SIMRS dan keamanan informasi; (4) Penyediaan infrastruktur cadangan:

Memastikan adanya sumber daya cadangan untuk menjaga kelangsungan operasional saat terjadi gangguan.

F. Acknowledgment

Penulis menyampaikan ucapan terima kasih kepada Rektor Universitas Muhammadiyah Semarang atas biaya penelitian internal tahun 2024, dan direktur RS Unimus yang telah memberikan kesempatan untuk penelitian ini.

Daftar Pustaka

[1] Aginsa, A., Edward, I. Y. M., & Shalannanda, W. (2016, August). Enhanced information security management system framework design using ISO 27001 and zachman framework-A study case of XYZ company. In 2016 2nd International Conference on Wireless and Telematics (ICWT) (pp. 62-66). IEEE.

[2] Watkins, S. (2022). ISO/IEC 27001: 2022: An introduction to information security and the ISMS standard.

[3] Malatji, M. (2023, January). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In 2023 International conference on cyber management and engineering (CyMaEn) (pp. 117-122). IEEE.

[4] Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi

[5] Pramanik, S., Samanta, D., Vinay, M., & Guha, A. (Eds.). (2022). Cyber Security and Network Security. John Wiley & Sons

[6] Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd international conference on cyber security and cloud computing (pp. 307-311). IEEE.

[7] Gouveia, F., Silva, V., Lopes, J., Moreira, R. S., Torres, J. M., & Simas Guerreiro, M. (2024). Automated identification of building features with deep learning for risk analysis. SN Applied Sciences, 6(9), 466. doi:https://doi.org/10.1007/s42452-024-06070-2

[8] Marchand-Niño, W., Ortiz-Morales, E., Vega-Ventocilla, E., & Olivera-Ruiz, G. (2024). Modelo de integración de técnicas y herramientas de OSINT con los controles de seguridad de la ISO/IEC 27001:2022. [OSINT Techniques and Tools Integration Model with ISO/IEC 27001:2022 Security Controls] Revista Ibérica De Sistemas e Tecnologias De Informação, , 167-180. Retrieved from https://www.proquest.com/scholarly-journals/modelo-de-integración-técnicas-y-herramientas/docview/3132647464/se-2

[9] Grigaliūnas, Š., Schmidt, M., Brūzgienė, R., Smyrli, P., Andreou, S., & Lopata, A. (2024). Holistic information security management and compliance framework. Electronics, 13(19), 3955. doi:https://doi.org/10.3390/electronics13193955