Journal of Digital Ecosystem for Natural Sustainability (JoDENS)
Vol.3, No.2, Desember 2023, pp. 64~69
e-ISSN: 2798-6179

Evaluasi Keamanan Informasi di Lingkungan Rumah Sakit: Pendekatan Audit ISO 27001 di RS Rahman Rahim Sidoarjo

Mohammad Chevalier Daniswara [1]*, Daris Irfan Putrawanto[2], Mochammad Najib[3], Zharvi Achmadha[4], M. Chairuladanan S. I.[5], Siti Mukaromah[6]
[1,2,3,4,5,6]*Sistem Informasi, Universitas Pembangunan Nasional 'Veteran' Jawa Timur*
**Corresponding author E-mail: daniswaraasep@gmail.com*

Article Info

Article history:

Received 19-12-2023
Revised 20-12-2023
Accepted 22-12-2023

Keyword:

Audit, ISO 27001, Uji Kematangan

ABSTRACT

The development of technology and information systems has now grown rapidly and has penetrated various aspects of human life. Starting from education, government, health, to trade, technology has been implemented to help their business processes. One area that is important to protect from these risks is the health sector. The institutions responsible in this field are hospitals that provide health services to the community. Rahman Rahim Hospital is a type D general hospital located in Kebonagung Village, Sukodono District, Sidoarjo Regency. Rahman Rahim Hospital has implemented a Hospital Management Information System (SIMRS). This needs to receive more attention, considering that health assets are a vital component for maintaining the smooth operational processes of hospitals. Serious and continuous action in protecting health assets can increase the security of health assets in order to protect patient rights and maintain the integrity of hospitals. Information system audits are carried out using the ISO/IEC 27001 framework. Implementation of ISO/IEC 27001 protects all aspects of information security, namely confidentiality, integrity and availability. This results in a maturity level index of 2.46 which is at the Planned and Tracked level. The gap obtained from the average objective control calculation is 2.5.

I. PENDAHULUAN

Perkembangan teknologi dan sistem informasi saat ini telah berkembang pesat dan merambah ke berbagai aspek kehidupan manusia. Mulai dari pendidikan, pemerintahan, kesehatan, hingga perdagangan telah menerapkan teknologi untuk membantu proses bisnisnya. Perkembangan yang kian pesat ini juga diikuti dengan risiko terhadap keamanan yang menjadi bagian dalam teknologi dan sistem informasi [1]. Salah satu bidang yang penting untuk dilindungi dari adanya resiko tersebut adalah bidang kesehatan. Institusi yang yang bertanggung jawab dalam bidang ini salah satunya adalah rumah sakit yang menyediakan pelayanan kesehatan kepada masyarakat. Ketidakmampuan untuk menjaga keamanan aset dalam sebuah institusi pelayanan kesehatan memungkinkan orang yang tidak bertanggung jawab untuk mencuri atau mengganggu aktivitas yang berkaitan dengan aset kesehatan pasien dari institusi tersebut [2]. Hal ini perlu mendapat perhatian lebih, mengingat aset kesehatan merupakan komponen vital untuk menjaga kelancaran proses operasional dari Rumah Sakit. Adanya tindakan serius dan berkelanjutan dalam perlindungan aset kesehatan dapat meningkatkan keamanan terhadap aset kesehatan demi melindungi hak-hak pasien dan menjaga integritas Rumah Sakit.

Rumah sakit Rahman Rahim merupakan rumah sakit umum tipe D yang terletak di Desa Kebonagung, Kecamatan Sukodono, Kabupaten Sidoarjo. Rumah sakit Rahman Rahim telah menerapkan Sistem Informasi Manajemen Rumah Sakit (SIMRS) dalam beberapa proses bisnis yang telah ditetapkan sebelumnya oleh Peraturan Menteri Kesehatan Nomor 82 Tahun 2013. Penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) pada fasilitas kesehatan Rahman Rahim dilakukan dengan tujuan untuk mengolah dan mengintegrasikan seluruh tahapan pelayanan rumah sakit ke dalam suatu jaringan yang terkoordinasi. Hal ini mencakup pelaporan dan tata cara administrasi untuk memperoleh informasi yang akurat dan tepat waktu. SIMRS merupakan

bagian integral dari Sistem Informasi Kesehatan secara keseluruhan.

Proses bisnis yang dijalankan di rumah sakit Rahman Rahim dilakukan secara dinamis dengan menyesuaikan peraturan yang berlaku, baik dari pemerintah daerah dan pemerintah pusat. Alur proses bisnis yang dinamis ini juga selaras dengan tujuan bisnis rumah sakit Rahman Rahim. Sistem Informasi Manajemen Rumah Sakit (SIMRS) dituntut untuk dapat menyesuaikan dengan kebutuhan yang berlaku saat ini dan dapat mempengaruhi seluruh aspek proses bisnis.

Sistem Informasi Manajemen Rumah Sakit (SIMRS) di rumah sakit Rahman Rahim merupakan tanggung jawab penuh dari divisi IT rumah sakit. SIMRS disimpan pada sebuah ruang server yang memiliki akses yang sangat terbatas dan tidak semua pihak mendapatkan akses untuk masuk pada ruangan server sesuai dengan SOP yang berlaku. Walau dengan akses yang terbatas pada ruang server, masih ditemukan kasus kehilangan data dengan frekuensi yang cukup sering. Data yang disimpan pada NAS (*Network Attach Storage*) dapat diakses oleh lokal user dengan otorisasi *Create, Read, Update, Delete* (CRUD). Realita yang terjadi, pengguna yang memiliki otoritas kurang bertanggung jawab hingga mengakibatkan kehilangan data. Dalam kasus pencurian data belum pernah terjadi di rumah sakit Rahman Rahim. Kasus manipulasi data pernah terjadi dan ditemukan pada laporan hasil rumah sakit yang diubah oleh pihak luar yang mengatasnamakan RS Rahman Rahim. Sedangkan kasus virus komputer merupakan kasus yang sering terjadi. Hal ini dikarenakan lalu lintas pertukaran data melalui internet merupakan akses utama yang digunakan dalam proses pelayanan dan administratif.

Dari latar belakang diatas, perlu dilakukan audit sistem informasi pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) di rumah sakit Rahman Rahim Sidoarjo. Solusi yang dapat ditawarkan dalam menjawab masalah yang terjadi yaitu melakukan audit sistem informasi dengan menggunakan framework ISO/IEC 27001. Implementasi ISO/IEC 27001 bertujuan untuk melindungi semua aspek keamanan informasi, termasuk kerahasiaan, integritas, dan ketersediaan [3]. ISO 27001 mencakup 133 kontrol keamanan informasi, dan perusahaan dapat memilih kontrol mana yang paling relevan dengan kondisi di lapangan mereka [4]. Penelitian ini berfokus pada Klausul 16 yaitu tentang Manajemen Insiden Keamanan Informasi yang didalamnya terdapat 7 kontrol objek.

II. METODE

Pelaksanaan Audit Manajemen Keamanan Informasi dilakukan dengan beberapa tahapan yang harus dilalui dari proses awal hingga akhir penelitian agar menghasilkan hasil audit yang tepat sasaran. Tahapan dari penelitian ini dapat dilihat pada gambar berikut

A. Observasi dan Wawancara

Tahap observasi dalam audit keamanan IT di rumah sakit melibatkan pengamatan langsung terhadap infrastruktur teknologi yang digunakan, seperti sistem komputer, jaringan, dan perlengkapan keamanan fisik. Observasi ini juga mencakup penilaian terhadap implementasi kebijakan keamanan, tata kelola akses, serta pengawasan terhadap aktivitas pengguna. Sementara itu, tahap wawancara melibatkan interaksi langsung dengan personel kunci di rumah sakit, seperti petugas keamanan IT dan administrator sistem yang menggunakan teknologi tersebut. Wawancara ini bertujuan untuk memahami praktik keamanan yang diterapkan, kesadaran akan keamanan informasi, serta mendapatkan wawasan langsung mengenai tantangan keamanan yang mungkin dihadapi oleh rumah sakit dalam penggunaan teknologi informasi.

B. Pengumpulan Informasi

Tahap pengumpulan informasi adalah proses menghimpun berbagai referensi dan sumber daya terkait yang dapat dijadikan landasan untuk penelitian, mencakup literatur seperti buku, artikel jurnal ilmiah, dan sumber lainnya. Dalam konteks audit keamanan IT di rumah sakit, langkah ini mencakup pengumpulan referensi terkait regulasi keamanan informasi serta literatur tentang metode audit keamanan IT. Pemahaman mendalam terhadap literatur ini dapat membantu membangun dasar teoritis dan merancang strategi audit yang efektif untuk menilai keamanan sistem informasi di rumah sakit.

C. Perumusan Masalah

Perumusan masalah dilakukan dengan tujuan untuk mengidentifikasi masalah yang memerlukan penelitian lebih lanjut dan menetapkan batas-batas dalam proses penelitian untuk mencapai solusi yang tepat.

D. Penentuan Kontrol Objektif

Dalam langkah ini, ditentukan jenis dan prosedur metode penelitian, serta ditetapkan klausul yang akan digunakan sebagai kontrol objektif sesuai dengan pedoman standar ISO 27002:2013. Langkah ini sangat penting untuk mempersempit cakupan data yang akan dipelajari, sehingga penelitian menjadi lebih fokus dan terarah pada prinsip-prinsip keamanan informasi yang diatur dalam ISO 27002:2013.

E. Penusunan Pertanyaan

Dalam fase ini, pernyataan untuk setiap kontrol objektif yang tercantum dalam klausul konrol objektif disusun. Kemudian, tahap selanjutnya melibatkan pengembangan pertanyaan terkait. Kaitannya dengan ISO 27001 adalah bahwa langkah ini dapat terkait dengan proses penyusunan kebijakan dan prosedur keamanan informasi sesuai dengan standar ISO 27001, khususnya dalam konteks manajemen insiden keamanan informasi.

F. Penusunan Pernyataan

Dalam tahap ini, langkah yang diambil adalah merumuskan pernyataan terkait setiap tujuan kontrol yang tercantum dalam klausul control objektif dari dokumen panduan ISO 27001:2013. Fokusnya adalah pada Manajemen Insiden Keamanan Informasi, yang kemudian diteruskan ke tahap selanjutnya untuk merinci pertanyaan yang akan diajukan. Proses ini memungkinkan penyusunan pernyataan kontrol yang sesuai dengan standar keamanan ISO 27001:2013, sehingga dapat diintegrasikan dengan langkah-langkah audit keamanan IT di rumah sakit, memberikan panduan yang kokoh dan sesuai regulasi untuk mengevaluasi sistem informasi. Uji Kematangan

Setelah audit data selesai, dilakukan pengujian kematangan keamanan sistem, yang juga dikenal sebagai perhitungan tingkat kematangan dengan skala nilai dari 0 (nol) hingga 5 (lima).

III. HASIL DAN PEMBAHASAN

A. Audit Sistem Informasi

Dalam sistem informasi, kegiatan manusia dan teknologi bekerja sama untuk membantu operasional dan manajemen perusahaan. Dalam proses audit, data dikumpulkan dan diuji oleh pihak yang berwenang untuk memastikan bahwa informasi yang diaudit sesuai dengan persyaratan atau standar. Tujuan dari proses audit adalah untuk memberikan informasi tersebut kepada pihak yang membutuhkannya. Audit sistem informasi menghimpun dan mengevaluasi bukti yang ada untuk menentukan apakah sistem komputerisasi perusahaan telah memperoleh dan menerapkan sistem pengendalian dan data yang menjaga integritas serta memastikan bahwa sistem informasi berbasis komputer berfungsi dengan baik dan efisien [5].

B. Keamanan Informasi

Keamanan sistem informasi mencakup berbagai upaya untuk melindungi dan mencegah penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab atas operasi sistem untuk menjamin kelangsungan bisnis, mengurangi risiko bisnis, dan optimalisasi pengembalian investasi dan peluang bisnis. [6].

C. SIMRS (Sistem Informasi Manajemen Rumah Sakit)

Sistem Informasi Manajemen Rumah Sakit (SIMRS) adalah sebuah sistem informasi yang terintegrasi yang disiapkan untuk menangani keseluruhan proses manajemen rumah sakit, mulai dari pelayanan diagnosa dan tindakan untuk pasien, medical record, apotek, gudang farmasi, penagihan, database personalia, penggajian karyawan, proses akuntansi sampai dengan pengendalian oleh manajemen [7].

D. ISO 27001

ISO/IEC 27001 adalah metode untuk standar manajemen keamanan informasi yang dikeluarkan oleh International Organization for Standardization dan International Electrotechnical Commission. ISO 27001 memberikan pedoman yang sangat komprehensif untuk pengelolaan keamanan informasi di seluruh dunia [8].

E. Maturity Level

Penerapan keamanan informasi dapat dinilai sejauh mana melalui penggunaan model maturitas yang dapat dilhat pada Tabel 1, penentuan kontrol objektif pada Tabel 2, dan penyusunan pertanyaan pada Tabel 3. Model maturitas merupakan suatu pendekatan untuk menilai tingkat kemajuan proses manajemen, mencerminkan seberapa baik kemampuan manajemen dalam mengimplementasikan keamanan informasi [9].

Tabel 1. Skala Index Maturity

Skala	Index	Deskripsi
0.00-0.50	Not Performed	Proses tidak lengkap. Proses tidak dilaksanakan atau gagal mencapai keluaran yang ditentukan.
0.51-1.50	Performed Informally	Proses telah dilakukan dan berhasil mencapai tujuan.
1.51-2.50	Planned and Tracked	Telah dilaksanakan dan dilaksanakan dengan lebih tertib dan hasil yang dihasilkan telah ditetapkan, dikendalikan dan dipelihara dengan baik
2.51-3.50	Well Defined	Proses tersebut telah dilaksanakan sesuai aturan/proses yang ditetapkan dan mampu mencapai keluaran yang diharapkan.
3.51-4.50	Quantitatively Controlled	Proses tersebut telah dilaksanakan sesuai dengan aturan yang telah ditentukan untuk mencapai hasil yang diharapkan.
4.51-5.00	Continuously Improving	Optimalisasi proses-proses yang ada secara berkala dan berkesinambungan diperbaiki untuk mencapai tujuan yang diharapkan baik saat ini maupun di masa yang akan datang.

F. Penentuan Kontrol Objektif

Tabel 2. Kontrol Objektif

A.16.1 Manajemen Insiden dan Peningkatan Kemanan Informasi
16.1.1 Tanggung Jawab dan Prosedur
16.1.2 Melaporkan Kejadian Kemanan Informasi
16.1.3 Melaporkan Kelemahan Keamanan Informasi
16.1.4 Penilaian dan Keputusan tentang Peristiwa Keamanan Informasi
16.1.5 Menanggapi Insiden Keamanan Informasi
16.1.6 Belajar dari Insiden Keamanan Informasi

G. Penyusunan Pertanyaan

Tabel 3. Penyusunan Pertanyaan

No.	A.16.1 Manajemen Insiden Keamanan Sistem Informasi
1	Apa jabatan atau tugas dan fungsi Anda pada divisi yang ditempatkan?

2	Apa saja proses bisnis yang ditangani oleh divisi tersebut?
3	Bagaimana penerapan TI yang sudah berjalan selama ini?
4	Apakah terdapat kendala selama implementasi sistem informasi tersebut?
5	Apakah ada evaluasi secara berkala?
6	Apakah sudah dilakukan perlindungan pada keamanan data dan asset Perusahaan?

H. Penyusunan Pernyataan

Tabel 4. Penyusunan Pernyataan

A.16.1	**Manajemen Insiden dan Peningkatan Keamanan Sistem Informasi**				
16.1.1	Tanggung Jawab dan Prosedur				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Tanggung jawab dan prosedur manajemen untuk penanganan insiden keamanan informasi telah ditetapkan dan didokumentasikan.	1	✓		3
2	Tanggung jawab dan prosedur manajemen untuk penanganan insiden keamanan informasi telah dikomunikasikan kepada semua staf yang relevan.	1	✓		3
3	Tanggung jawab dan prosedur manajemen untuk penanganan insiden keamanan informasi telah ditinjau dan diperbarui secara berkala.	1		✓	1
16.1.2	Pelaporan Kejadian Keamanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Memiliki prosedur yang terdokumentasi untuk pelaporan insiden keamanan informasi.	1	✓		3
2	Menindaklanjuti semua insiden keamanan informasi sesuai dengan prosedur yang terdokumentasi.	1	✓		3
3	Mengumpulkan bukti sesegera mungkin setelah insiden terjadi.	1	✓		3
16.1.3	Pelaporan Kelemahan Keamanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Pelaporan masalah ke titik kontak secepat mungkin untuk mencegah insiden keamanan informasi	1	✓		4
2	Mekanisme Pelaporan yang mudah, dapat diakses dan tersedia	1	✓		2
3	Adanya panduan tertulis dan mudah diakses mengenai proses pelaporan masalah	1		✓	1
16.1.4	Penilaian dan Keputusan Pada Kejadian Keaman Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Pencatatan hasil evaluasi apakah peristiwa keamanan informasi telah dianalisis dengan cermat untuk menentukan klasifikasinya sebagai insiden keamanan informasi.	1		✓	1
2	Penilaian dan keputusan insiden keamanan informasi dilakukan oleh personil yang kompeten dan berwenang.	1	✓		3
3	Hasil penilaian dan keputusan insiden keamanan informasi dicatat secara rinci untuk referensi dan verifikasi di masa mendatang.	1	✓		3
16.1.5	Tanggapan Terhadap Insiden Keamanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Menyusun dan mendokumentasikan prosedur respon terhadap insiden keamanan informasi	1		✓	1
2	Tim respons insiden keamanan telah ditetapkan dan dijelaskan dalam prosedur yang terdokumentasi	1		✓	1
3	Insiden keamanan informasi dilaporkan secara tepat waktu sesuai dengan prosedur yang telah ditetapkan	1	✓		3
16.1.6	Pembelajaran dari Insiden Kemanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5

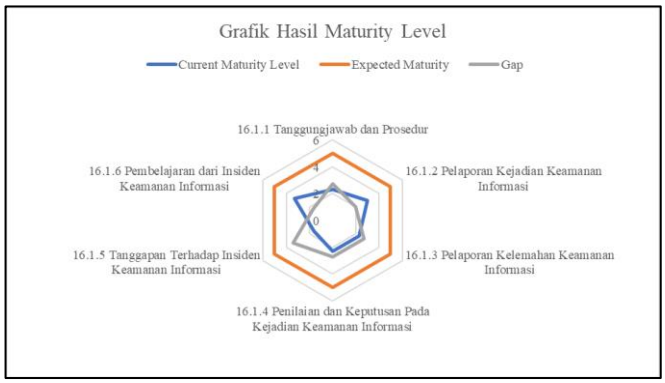
1	Analisis insiden keamanan informasi dilakukan secara menyeluruh untuk mengevaluasi penyebab dan dampaknya.	1	✓	3
2	Pengetahuan yang diperoleh dari analisis insiden keamanan informasi digunakan untuk menyusun rekomendasi perbaikan dan tindakan pencegahan.	1	✓	4
3	Hasil analisis insiden keamanan informasi diterapkan dalam pembaruan prosedur, kebijakan, atau kontrol keamanan informasi yang ada	1	✓	3

I. Tingkat Kematangan

Tabel dibawah ini menunjukkan tingkat kematangan tiap objek kontrol saat ini *(Current Maturity)* dan juga indeks kematangan menurut ISO 27001.

Tabel 5. Rangkuman Tingkat Kematangan

No	Objek Kontrol	Current Maturity	Expected Maturity	Gap	Index
1	Tanggungjawab dan Prosedur	2,3	5	2,7	Planned and Tracked
2	Pelaporan Kejadian Keamanan Informasi	3	5	2	Well Defined
3	Pelaporan Kelemahan Kemanan Informasi	2,3	5	2,7	Planned and Tracked
4	Penilaian dan Keputusan Pada Kejadian Keamanan Informasi	2,3	5	2,7	Planned and Tracked
5	Tanggapan Terhadap Insiden Keamanan Informasi	1,6	5	3,4	Planned and Tracked
6	Pembelajran dari Insiden Kemanan Informasi	3,3	5	1,7	Well Defined
	Rata-rata	**2,46**		**2,54**	**Planned and Tracked**



Gambar 1. Radar Chart Maturity Level

Berdasarkan dari hasil current maturity yang didapat setiap kontrol objektif ISO, teridentifikasi bahwa tingkat kematangan keamanan informasi relatif bervariasi di setiap domain. Rata-rata yang didapatkan dari current maturity yaitu senilai 2,46 yang menunjukkan bahwa perusahaan telah mencapai tingkat kematangan dengan kategori planned and tracked dari perhitungan skala yang digunakan. Perbedaan nilai setiap kontrol objektif yang berbeda dapat menunjukkan bahwa adanya variasi dalam penerapan keamanan informasi pada organisasi. Nilai tinggi kontrol objektif yang diperoleh seperti pada Tanggapan Terhadapan Insiden Keamanan Informasi menggambarkan tingkat kesiapan yang lebih baik daripada kontrol objektif lainnya. Oleh karena itu, hasil diatas memberikan gambaran secara umum tentang bagaimana keberhasilan organisasi dalam menerapkan dan melaksanakan kontrol keamanan informasi sesuai dengan standar ISO yang ada.

IV. KESIMPULAN

Berdasarkan dari penelitian yang telah dilakukan, kesimpulan dari penelitian ini adalah tingkat kematangan manajamen insiden keamanan informasi dan perbaikan di RS Rahman Rahim berada di angka 2,46 yang berarti berada pada index Planned and Tracked. Yang berarti Telah dilaksanakan dengan lebih tertib dan hasil yang dihasilkan telah ditetapkan, dikendalikan dan dipelihara dengan baik.

Gap yang diperoleh dari rata-rata perhitungan kontrol objektif yaitu sebesar 2,54. Dari nilai gap yang didapatkan menunjukkan bahwa manajemen insiden keamanan rumah sakit Rahman Rahim telah menerapkan manajemen keamanan informasi dengan baik

UCAPAN TERIMA KASIH

Kami ingin menyampaikan ucapan terima kasih yang tulus kepada Universitas Pembangunan Nasional "Veteran" Jawa Timur atas kesempatan berharga yang telah diberikan kepada kami untuk melakukan penelitian mengenai audit keamanan informasi di Rumah Sakit Rahman Rahim Sidoarjo. Serta rasa terima kasih kami juga disampaikan kepada pihak Rumah Sakit Rahman Rahim Sidoarjo atas kerjasama sebagai auditee dalam penelitian ini. Akhirnya, kami juga mengucapkan terima kasih kepada JoDENS atas

kesempatan yang diberikan untuk menerbitkan jurnal ini, semoga hasil penelitian ini dapat memberikan kontribusi yang berarti.

DAFTAR PUSTAKA

[1] S. Dwiasnati and R. R. Hidayat, "Penerapan Manajemen Risiko Menggunakan COSO: Enterprise Risk Management Framework Integrated Pada PT ALPHANET," *J. Tata Kelola dan Kerangka Kerja Teknol. Inf.*, vol. 8, no. 2, pp. 66–72, 2022, doi: 10.34010/jtk3ti.v8i2.7845.

[2] Amri Hairul, Haryada Alwi Awilo, Abdi Kairul, and Ikhwan Ali, "Manajemen Resiko Keamanan Aset Informasi Pada Puskesmas Pancur Batu Tuntungan," *J. Sains Dan Teknol.*, vol. 3, no. 1, pp. 141–150, 2023.

[3] A. A. Ipungkarti, "Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta," *J. Media Infotama*, vol. 19, no. 1, pp. 103–110, 2023, doi: 10.37676/jmi.v19i1.3481.

[4] M. Bakri and N. Irmayana, "Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar Iso 27001," *J. Tekno Kompak*, vol. 11, no. 2, p. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[5] D. Akbar, S. Mulia, W. Ningrum, and ..., "Audit Sistem Informasi Pengantaran Barang Pada PT Samudera Arkan Nusantara Menggunakan Framework COBIT 4.1," *... Nat. Sustain.*, vol. 2, no. 1, pp. 34–38, 2022, [Online]. Available: http://journal.uvers2.ac.id/index.php/jodens/article/view/74%0Ahttp://journal.uvers2.ac.id/index.php/jodens/article/download/74/52

[6] E. Riana, M. E. S. Sulistyawati, and O. P. Putra, "Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013," *J. Inf. Syst. Res.*, vol. 4, no. 2, pp. 632–640, 2023, doi: 10.47065/josh.v4i2.2552.

[7] R. Molly and M. Itaar, "Analisis Pemanfaatan Sistem Informasi Manajemen Rumah Sakit (SIMRS) Pada RRSUD DOK II Jayapura," *J. Softw. Eng. Ampera*, vol. 2, no. 2, pp. 95–101, 2021, doi: 10.51519/journalsea.v2i2.127.

[8] P. Februari and F. Fitria, "Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung," *POSITIF J. Sist. dan Teknol. Inf.*, vol. 5, no. 2, p. 97, 2019, doi: 10.31961/positif.v5i2.833.

[9] I. Mantra, A. Abd. Rahman, and H. Saragih, "Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education," *Int. J. Eng. Technol.*, vol. 9, no. 2, p. 429, 2020, doi: 10.14419/ijet.v9i2.30581.