JURNAL ILMIAH BETRIK
Besemah Teknologi Informasi dan Komputer
ISSN : 2339 - 1871
Editor Office : LPPM Sekolah Tinggi Teknologi Pagar Alam, Jln. Masik Siagim No. 75 Simpang Mbacang, Pagar Alam, SUM-SEL, Indonesia
Phone : +62 852-7901-1390.
Email : betrik@sttpagaralam.ac.id | admin.jurnal@sttpagaralam.ac.id
Website : https://ejournal.sttpagaralam.ac.id/index.php/betrik/index

ANALISIS MANAJEMEN RESIKO SISTEM INFORMASI ELEKRONIK PUSKESMAS (SIEPUS) PADA PUSKESMAS XYZ MENGGUNAKAN ISO 31000

Nur Ayuwulantari[1], Egy Septian[2] , Tata Sutabri[3]
Program Studi Magister Tehnik Informatika Universitas Bina Darma
Jalan A.Yani , Kota Palembang 3551
Sur-el : wulantarinurayu@gmail.com[1] ,egy.septian@gmail.com[2] , tata.sutabri@gmail.com[3]

Abstrak*:* Puskesmas semakin mengandalkan Sistem Informasi Elektronik (SIEPUS) untuk mengoptimalkan pengelolaan data dan pelayanan kesehatan. Namun, dengan semakin kompleksnya SIEPUS yang digunakan, risiko-risiko terkait keamanan dan integritas data juga semakin meningkat. Puskesmas XYZ sebagai salah satu pusat pelayanan Kesehatan yang menggunakan SIEPUS menghadapi tantangan dan manajemen resikko yang berhubungan dengan keamanan dan sistem yang terintegritas. Risiko-risiko ini mencakup kebocoran data, gangguan sistem, dan ketidakpatuhan terhadap peraturan dan standar keamanan data kesehatan. Tujuan dari penelitian untuk menganalisis manajemen risiko SIEPUS pada Puskesmas XYZ dengan menggunakan ISO 31000 menggunakan metode pengumpulan data kuantitatif dengan teknik pengumpulan data Studi literatur, observasi dan kuisioner. Hasil dari analisis yaitu terdapat 3 risiko dalam level low, 6 risiko dalam level medium dan 3 risiko dalam level high.

Kata Kunci : SIEPUS, Manajemen Risiko, ISO 31000

***Abstract** : Puskesmas increasingly rely on Electronic Information Systems (SIEPUS) to optimize data management and health services. However, with the increasing complexity of SIEPUS used, risks related to data security and integrity also increase. Puskesmas XYZ as one of the health institutions that uses SIEPUS faces challenges in managing risks related to security and system integrity. These risks include data leakage, system disruption, and non-compliance with health data security regulations and standards. The purpose of the study was to analyze SIEPUS risk management at Puskesmas XYZ using ISO 31000 using quantitative data collection methods with data collection techniques Literature study, observation and questionnaire. The result of the analysis is that there are 3 risks in the low level, 6 risks in the medium level and 3 risks in the high level.*

***Keywords** : SIEPUS, Risk Management, ISO 31000*

1. PENDAHULUAN

Puskesmas merupakan salah satu instansi pemerintah yang bergerak dibidang pelayanan kesehatan masyarakat di tingkat kecamatan. Peran puskesmas sangatlah penting dalam menopang kinerja dari instansi kesehatan diatasnya seperti rumah sakit, sebagai upaya

pencegahan dan penanggulangan kesehatan masyaraka[1]]. Puskesmas semakin mengandalkan Sistem Informasi Elektronik (SIEPUS) untuk mengoptimalkan pengelolaan data dan pelayanan kesehatan. Namun, dengan semakin kompleksnya SIEPUS yang digunakan, risiko-risiko terkait keamanan dan integritas data juga semakin meningkat. Oleh karena itu, manajemen risiko menjadi krusial dalam memastikan keberlangsungan dan keamanan operasional SIEPUS di Puskesmas.

Puskesmas XYZ sebagai salah satu lembaga kesehatan yang menggunakan SIEPUS menghadapi tantangan dalam mengelola risiko-risiko yang terkait dengan keamanan dan integritas sistem. Risiko-risiko tersebut meliputi kebocoran data, gangguan sistem, serta ketidakpatuhan terhadap regulasi dan standar keamanan data kesehatan.

Manajemen risiko adalah aktivitas terorganisasi yang dilakukan untuk mengarahkan dan mengelola organisasi dalam rangka menangani risiko[2]. Dalam konteks ini, risiko dapat diartikan sebagai kemungkinan terjadinya peristiwa yang mengakibatkan dampak negatif pada keberlangsungan operasional, reputasi, atau tujuan yang diinginkan suatu entitas. Pendekatan manajemen risiko melibatkan proses yang terstruktur, mulai dari identifikasi risiko yang potensial, penilaian terhadap tingkat dampak dan probabilitas terjadinya risiko, hingga pengembangan strategi mitigasi untuk mengurangi atau menghilangkan risiko yang ada. Manajemen risiko juga mencakup proses monitoring dan pengendalian terhadap implementasi strategi mitigasi yang telah ditetapkan, serta evaluasi secara berkala terhadap efektivitasnya. Dengan demikian, manajemen risiko menjadi suatu pendekatan yang penting bagi organisasi dalam menghadapi ketidakpastian dan kompleksitas lingkungan operasionalnya, sehingga dapat meningkatkan kemampuan adaptasi dan menjaga keberlangsungan usaha secara efektif.

ISO 31000 merupakan standart yang di publikasikan oleh ISO yang mengatur pengelolaan risiko[3], Puskesmas XYZ diharapkan dapat memperkuat kapabilitasnya dalam mengelola risiko-risiko yang terkait dengan SIEPUS, sehingga dapat meningkatkan keandalan dan keamanan layanan kesehatan yang disediakan.

Penelitian ini bertujuan dan berfokus pada analisis manajemen risiko yang terkait dengan SIEPUS di Puskesmas XYZ. Analisis akan meliputi identifikasi risiko, evaluasi risiko, serta pengembangan strategi mitigasi berdasarkan kerangka kerja ISO 31000.

2. METODE PENELITIAN

Dalam identifikasi masalah, penulis menggunakan metide pengumpulan data kuantitatif dengan teknik pengumpulan data adalah sebagai berikut :

1. Studi Literatur

Studi literatur adalah cara yang dipakai untuk menghimpun data-data atau sumber-sumber yang berhubungan dengan topik yang diangkat dalam suatu penelitian[4].

2. Observasi

Penulis melakukan pengamatan pada objek yang akan di teliti

3. Kuesioner

Kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawab[5]..

4. ISO 31000

ISO 31000 merupakan standart yang di publikasikan oleh ISO yang mengatur pengelolaan risiko. ISO 31000-2009 memberikan panduan, kerangka kerja, dan proses untuk mengatur risiko. Standart ini dapat digunakan oleh berbagai organisasi untuk membantu meningkatkan kemungkinan (likehood) di dalam proses mencapai tujuan, meningkatkan performa di dalam mengidentifikasi peluang (opportunity) dan ancaman (threat) serta dilakukan untuk memanfaatkan sumber daya yang ada dalam menangani risiko (risk treatment)[6].

3. TINJAUAN PUSTAKA

1. Puskesmas

Puskesmas disepakati sebagai suatu unit pelayanan kesehatan yang Memberikan pelayanan kuratif dan preventif secara terpadu, menyeluruh dan mudah dijangkau, dalam wilayah kerja kecamatan atau sebagian kecamatan di kota madya. 2007). Pengertian Puskesmas menurut Pedoman Kerja Puskesmas DEPKES-RI adalah suatu kesatuan organisasi kesehatan fungsional yang merupakan pusat pengembangan kesehatan masyarakat yang juga membina peran serta masyarakat disamping memberikan pelayanan secara menyeluruh dan

terpadu kepada masyarakat di wilayah kerjanya dalam bentuk kegiatan pokok[7].

2. Manajemen Risiko

manajemen risiko merupakan suatu usaha untuk mengetahui, menganalisis, serta mengendalikan risiko dalam setiap kegiatan perusahaan dengan tujuan untuk memperoleh efektivitas dan efisiensi yang lebih tinggi. Manajemen risiko adalah suatu pendekatan yang mengadopsi sistem yang konsisten untuk mengelola semua risiko yang dihadapi oleh perusahaan[8].

3. Elektronik Puskesmas

Elektronik Puskesmas Merupakan aplikasi untuk layanan kesehatan yang dikembangkan untuk memberikan pelayanan dasar kepada masyarakat. Dengan Elektronik Puskesmas (e-Puskesmas), pencatatan dan pendataan pasien dilakukan secara elektronik dan memudahkan Dinas Kesehatan dalam memonitor data kesehatan masyarakat. Aplikasi Elektronik Puskesmas (e-Puskesmas) merupakan wujud dari penerapan teknologi informasi dan komunikasi yang mampu memberikan kontribusi yang sangat besar dalam memberikan pelayanan yang prima kepada pasien[9].

4. ISO 31000

ISO 31000 merupa kanpa nduan penerapan risiko ya ng terdiri a ta s tiga elemen, ya itu: kerangka kerja(framework), prinsip (principle)dan proses (process). SO 31000 menyediakan kerangka kerja ,prinsipdan proses manajemen risiko yang bisa diguna kan sebagai arsitektur manajemen risiko dan menjamin penerapan manajemen risiko yang efektif dalam organisasi[10].

Langkah-langkah dalam ISO 31000

A. Rumus yang di gunakan

Untuk menghitung hasil kuisioner yang telah di kumpulkan dari para responden penulis menggunakan rumus likert. Rumus ini digunakan untuk mengetahui hasil persentasi dari setiap jawaban responden:

% = F/N.100 (1)

Keterangan :

% = Indeks

F = Frekuensi pada kuisioner

N = Jumlah Skor max (Total responden x Skor tertinggi)

B. Identifikasi Risiko

Merupakan proses sistematis untuk mengenali, menggambarkan, dan memahami potensi terjadinya suatu peristiwa yang dapat memengaruhi pencapaian tujuan organisasi. Tahapan dalam mengidentifikasi risiko adalah :

1. Mengidentifikasi Teknologi informasi dalam organisasi.
2. Menganalisis kemungkinan risiko yang akan muncul dalam teknologi informasi tersebut.
3. Mengidentifikasi dampak dari risiko

C. Analisis Risiko

Analisis risiko bertujuan untuk memahami secara lebih mendalam tentang potensi dampak dan kemungkinan terjadinya risiko yang telah diidentifikasi. Analisis risiko menggabungkan informasi tentang kemungkinan terjadinya risiko dengan dampak yang mungkin timbul jika risiko tersebut terwujud.

Tabel 1 Likehood

Likehood			
Bobot Penilaian	**Kriteria**	**Tingkat Kejadian**	**Frekuensi**
1	Rare	Hampir Tidak terjadi	>2Tahum
2	Unlikely	Jarang	1-2 Tahun
3	Possible	Kadang-kadang terjadi	7-12 Bulan
4	Likely	Sering terjadi	4-6 Bulan
5	Certain	Hampir sering terjadi	1-3 Bulan

Tabel likehood digunakan dalam analisis risiko untuk mengevaluasi seberapa mungkin suatu peristiwa atau risiko tertentu akan terjadi.

Tabel 2 Impact

Impact		
Ratting	Kriteria	**Keterangan**
1	Insignifican	Tidak mengganggu/menggagalkan aktivitas bisnis perusahaan
2	Minor	Aktivitas perusahaan sedikit terhambat namun aktivitas inti perusahaan tidak terganggu.
3	Moderate	Risiko yang terjadi mulai mengganggu pada proses bisnis sehingga sebagian jalannya aktivitas perusahaan terhambat

4	Major	Risiko yang terjadi mulai mengganggu aktivitas bisnis perusahaan sehingga Menghambat hampir seluruh aktivitas perusahaan
5	Insignificant	Aktivitas perusahaan berhenti karena proses bisnis mengalami gangguan total

Tabel Impact adalah alat yang digunakan dalam analisis risiko untuk mengevaluasi tingkat dampak atau konsekuensi yang mungkin terjadi jika suatu risiko atau peristiwa tertentu terwujud.

D. EVALUASI RISIKO

Evaluasi risiko adalah proses penilaian yang sistematis dan terstruktur terhadap risiko yang diidentifikasi dalam konteks organisasi. Tujuan dari evaluasi risiko adalah untuk memahami dengan lebih baik potensi dampak dari risiko-risiko yang dihadapi oleh organisasi dan tingkat kemungkinan terjadinya, sehingga organisasi dapat mengambil langkah-langkah yang sesuai untuk mengelola risiko tersebut.

Tabel 3 Matriks Risiko

Likehood						
	Certain	5	Medium	Medium	Hight	Hight	Hight
	Likely	4	Medium	Medium	Medium	Hight	Hight
	Possible	3	Low	Medium	Medium	Hight	Hight
	Unlikely	2	Low	Low	Medium	Medium	Medium
	Rare	1	Low	Low	Low	Medium	Medium
			1	2	3	4	5
	Impact		Insignificant	Minor	Moderate	Major	Catasthropic

4. HASIL DAN PEMBAHASAN

1. Identifikasi Risiko

Pada tahap identifikasi risiko pada Puskesmas XYZ, tim manajemen secara sistematis mengevaluasi lingkungan operasionalnya untuk mengidentifikasi potensi kejadian yang dapat mengganggu aktivitas dalam unit rekam medis

Tabel 4 Identifikasi Risiko

ID	Skenario Risiko	Kategori Risiko
S01	Adanya kesalahan input informasi oleh staff TI	Human Error
S02	Adanya kerusakan hardware	Information
S03	Terjadi Hang pada komputer	Information
S04	Database corrupt / Tidak dapat melihat data yang tersimpan sebelumnya	Information
S05	Sistem tidak dapat menghandle dikarenakan banyak nya data saat volume pasien meningkat	Infrastructure
S06	Terjadinya mati listrik dan jaringan yang lambat	Infrastructure
S07	Adanya bug pada software	Software
S08	Tidak bisa mengoperasikan SIEPUS	Software
S09	*Crush System*	Software
S10	Adanya kebakaran	Acts of nature
S11	Adanya gempa	Acts of nature
S12	Adanya gangguan virus	Logical Attack

2. Analisis Risiko

Setelah melakukan identifikasi risiko, tahap selanjutnya adalah melakukan analisis risiko. melakukan evaluasi mendalam terhadap setiap risiko yang teridentifikasi. Hal ini melibatkan penilaian terhadap dampak potensial dari masing-masing risiko terhadap tujuan operasional dan kesejahteraan pasien, serta probabilitas terjadinya.

Tabel 5 Analisis Risiko

ID	Skenario Risiko	*%likehood*	*Likehood*	*%impact*	*Impact*
S01	Adanya kesalahan input informasi oleh staff TI	32 %	2	40%	3
S02	Adanya kerusakan hardware	55 %	3	68%	4
S03	Terjadi Hang pada komputer	50 %	3	62%	4

S04	Database corrupt / Tidak dapat melihat data yang tersimpan sebelumnya	30 %	2	37%	3
S05	Sistem tidak dapat menghandle dikarenakan banyaknya data saat volume pasien meningkat	36 %	2	45%	3
S06	Terjadinya mati listrik dan jaringan yang lambat	44 %	3	55%	3
S07	Adanya bug pada software	40 %	3	50%	3
S08	Tidak bisa mengoperasikan SIEPUS	38 %	2	47%	3
S09	*Crush System*	30 %	2	37%	2
S10	Adanya kebakaran	15 %	1	18%	1
S11	Adanya gempa	17 %	1	21%	1
S12	Adanya gangguan virus	50 %	3	62%	4

3. Evaluasi Risiko

Pada tahap terakhir yaitu evaluasi risiko yang bertujuan untuk melakukan penilaian mendalam terhadap risiko-risiko yang telah diidentifikasi dan dianalisis sebelumnya. Hasil dari evalusi risiko akan di bagi menjadi 3 level yaitu high, medium, dan low dan tahan sebelumnya akan disesuaikan dengan matriks risiko

Tabel 6 matriks Risiko

Likehood						
	Certain	5	*Medium*	*Medium*	*Hight*	*Hight*	*Hight*
	Likely	4	*Medium*	*Medium*	*Medium*	*Hight*	*Hight*
	Possible	3	*Low*	*Medium*	S07,S06	S02,S03,S12	*Hight*
	Unlikely	2	*Low*	S09	S01,S05,S04,S08	*Medium*	*Medium*
	Rare	1	S10,S11	*Low*	*Low*	*Medium*	*Medium*
			1	2	3	4	5
	Impact		*Insignificant*	*Minor*	*Moderate*	*Major*	*Catasthropic*

Setelah melakukan evaluasi risiko dan memasukkan hasil evaluasi kedalam matriks risiko berdasarkan likehood dan impact selanjutnya adalah pengelolaan risiko. Padah tahap ini penulis memberikan saran pengelolaan risiko terhadap SIEPUS untuk setiap kemungkinan risiko yang ada. Strategi pengelolaan risiko dapat mencakup tindakan preventif, seperti meningkatkan keamanan infrastruktur, tindakan mitigasi untuk mengurangi kemungkinan terjadinya risiko, pemindahan risiko melalui asuransi atau kontrak, atau penerimaan risiko jika risiko tersebut tidak dapat dihindari sepenuhnya. Usulan ini didasarkan pada evaluasi dampak dan probabilitas risiko serta mengacu pada tujuan dan kebutuhan organisasi.

Tabel 8 Usulan Pengelolaan risiko

Skenario Risiko	*Risk Level*	*Risk Treatment*
Adanya kerusakan hardware	*High*	1. Rutin melakukan pemeliharaan preventif terhadap perangkat keras 2. Menyediakan sumber daya pendidikan tentang cara menggunakan perangkat keras dengan benar untuk meminimalkan risiko kerusakan.
Terjadi Hang pada komputer	*High*	1. Lakukan pemeliharaan rutin dan pembersihan perangkat keras 2. Perbarui dan optimalkan sistem operasi serta perangkat lunak aplikasi secara teratur.

Adanya gangguan virus	*High*	1. Pastikan setiap komputer dilengkapi dengan program antivirus dan anti-malware yang terkini. 2. Perbarui definisi virus secara berkala untuk melindungi sistem dari ancaman terbaru.
Terjadinya mati listrik dan jaringan yang lambat	*Medium*	Pasang perangkat UPS (Uninterruptible Power Supply) untuk memberikan daya cadangan kepada perangkat kritis seperti server dan perangkat jaringan selama pemadaman listrik.
Adanya bug pada software	*Medium*	Perbarui perangkat lunak secara teratur untuk mengintegrasikan perbaikan bug dan pembaruan keamanan terbaru.
Adanya kesalahan input informasi oleh staff TI	*Medium*	Lakukan Pelatihan pada staf dan Lakukan Double-check dan peer review untuk meninimalisir kesalahan dalam input data
Sistem tidak dapat menghandle dikarenakan banyak nya data saat volume pasien meningkat	*Medium*	1. Pastikan sistem memiliki kemampuan untuk disesuaikan dengan peningkatan volume data dengan mudah. 2. Lakukan optimasi perangkat keras dan perangkat lunak sistem untuk meningkatkan kinerja dan kecepatan pemrosesan data.
Database corrupt / Tidak dapat melihat data yang tersimpan sebelumnya	*Medium*	Buat dan simpan backup data secara teratur, termasuk backup lengkap dan backup berkala dari data yang baru saja dimasukkan.dan Lakukan perawatan rutin pada database, termasuk pembersihan dan perbaikan indeks, perbaikan kerentanan keamanan, dan optimasi kinerja.
Tidak bisa mengoperasikan SIEPUS	*Medium*	Lakukan Pelatihan pada staf cara mengoperasikan SIEPUS dengan baik dan benar
Crush System	*Low*	Pasang komponen sistem yang redundan, seperti server ganda atau koneksi jaringan ganda, untuk meningkatkan ketersediaan sistem.
Adanya kebakaran	*Low*	Pasang sistem deteksi kebakaran yang

		efektif di seluruh bangunan atau area yang berpotensi terkena dampak kebakaran.
Adanya gempa	*Low*	Pastikan bangunan dan fasilitas dipasang dengan desain dan teknik konstruksi yang tahan gempa sesuai dengan standar bangunan yang berlaku.

Dapat dilihat pada tabel usulan pengelolaan risiko bahwa risiko dengan level high risk butuh penangana oleh divisi IT dalam pengelolaan risiko yang tersebut. Dengan adanya usulan tersebut maka likakukan penulisan pelaporan untuk deserahkan pada pihak puskesmas yang meliputi laporan terkait kemungkinan risiko yang berpotensi menghambat aktivitas dalam SIEPUS.

5. KESIMPULAN

Berdasarkan penelitian yang telah di lakukan dalam manajemen risiko terhadap SIEPUS pada Puskesmas XYZ maka dapat diambil kesimpulan yaitu :

1. Dari hasil identifikasi risiko pada SIEPUS terdapat 12 Risiko dengan kategori risiko 1 risiko dengan kategori (Human Error), 3 risiko dengan kategori (Information), 2 risiko dengan kategori (Infrastructure), 3 risiko dengan kategori (software), 2 risiko dengan kategori (Acts of nature) dan 1 risiko dengan kategori (Logical attack)
2. Hasil analisa terdapat 3 risiko dengan level rendah (Crush System, Adanya kebakaran,Adanya gempa), 6 risiko dengan level sedang (Terjadinya mati listrik dan jaringan yang lambat, Adanya bug pada software, data yang di input tidak sesuai, Adanya kesalahan input informasi oleh staff TI, Sistem tidak dapat menghandle dikarenakan banyak nya data saat volume pasien meningkat, Database corrupt / Tidak dapat melihat data yang tersimpan sebelumnya, Tidak bisa mengoperasikan SIEPUS)dan 3 risiko dengan level tinggi (Adanya kerusakan hardware, Terjadi Hang pada komputer, Adanya gangguan virus)

6. SARAN

Peneliti Telah melakukan analisis manajemen risiko pada SIEPUS menggunakan ISO 31000, dan dengan hasil yang didapat tentunya terdapat banyak kekurang sehinggan saran yang bisa penulis sarankan adalah Dalam melakukan konteks kriteria, diharapkan dapat dianalisis secara menyeluruh, baik dari konteks eksternal maupun internal, agar mengetahui seberapa besar kontribusi stakeholder dalam menjalankan SIEPUS.

Daftar Pustaka

[1] A. Syukron dan N. Hasan, "Perancangan Sistem Informasi Rawat Jalan Berbasis Web Pada Puskesmas Winong," *Bianglala Inform.*, vol. 3, no. 1, Art. no. 1, Nov 2015, doi: 10.31294/bi.v3i1.574.

[2] M. B. A. Sajjad, S. D. Kalista, M. Zidan, dan J. Christian, "ANALISIS MANAJEMEN RISIKO BISNIS," *J. Akunt. Univ. JEMBER*, vol. 18, no. 1, hlm. 51–61, Jul 2020, doi: 10.19184/jauj.v18i1.18123.

[3] F. M. Hutabarat dan A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, Art. no. 1, Feb 2020, doi: 10.33557/binakomputer.v2i1.792.

[4] F. Estikhamah dan A. Rumintang, "Studi Literatur Tentang Pengaruh Demand Bus Antar Kota Terhadap Kualitas Udara di Area Terminal," *J. Tek. Sipil*, vol. 1, no. 1, hlm. 36–41, Mei 2020, doi: 10.31284/j.jts.2020.v1i1.904.

[5] T. Titah dan T. Sutabri, "Analisis Kualitas Layanan Shopee menggunakan pendekatan E-ServQual dan Potential Gain in Customer Value(PGCV)," *Jupit. J. Penelit. Ilmu Dan Teknol. Komput.*, vol. 15, no. 2, Art. no. 2, Nov 2023, doi: 10.5281/zenodo.10075026.

[6] L. E. Hutagalung, "ANALISA MANAJEMEN RISIKO SISTEM INFORMASI MANAJEMEN RUMAH SAKIT (SIMRS) PADA RUMAH SAKIT XYZ MENGGUNAKAN ISO 31000," *TeIKa*, vol. 12, no. 01, Art. no. 01, Mei 2022, doi: 10.36342/teika.v12i01.2820.

[7] T. Radito, "ANALISIS PENGARUH KUALITAS PELAYANAN DAN FASILITAS KESEHATAN TERHADAP KEPUASAN PASIEN PUSKESMAS," *J. ILMU Manaj.*, vol. 11, no. 2, Art. no. 2, Apr 2014, doi: 10.21831/jim.v11i2.11753.

[8] Y. N. Qintharah, "Perancangan Penerapan Manajemen Risiko," *JRAK J. Ris. Akunt. Dan Komputerisasi Akunt.*, vol. 10, no. 1, hlm. 67–86, Feb 2019, doi: 10.33558/jrak.v10i1.1645.

[9] H. Adrianti dan H. Usman, "Pengaruh Faktor End User Computing Satisfaction (EUCS) Terhadap Manfaat Nyata Pengguna Sistem Informasi Elektronik (E-Puskesmas) di Puskesmas Sawah Besar Jakarta," *Indones. Health Inf. Manag. J. INOHIM*, vol. 6, no. 2, Art. no. 2, 2018, doi: 10.47007/inohim.v6i2.21.

[10] I. Setiawan, A. R. Sekarini, R. Waluyo, dan F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," *MATRIK J. Manaj. Tek. Inform. Dan Rekayasa Komput.*, vol. 20, no. 2, Art. no. 2, Mei 2021, doi: 10.30812/matrik.v20i2.1093.