

**Hak Cipta Dilindungi Undang-Undang**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

**PENGGUNAAN METODE FMEA DALAM PENILAIAN
MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI
RUMAH SAKIT**

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:



SETIA NINGSIH SAPUTRI

11950325023



UIN SUSKA RIAU

UIN SUSKA RIAU

**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2024**

LEMBAR PERSETUJUAN

**PENGUNAAN METODE FMEA DALAM PENILAIAN
MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI
RUMAH SAKIT**

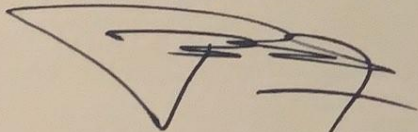
TUGAS AKHIR

Oleh:

SETIA NINGSIH SAPUTRI
11950325023

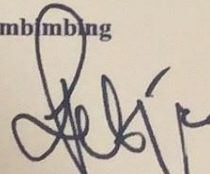
Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 10 Juni 2024

Ketua Program Studi



Eki Saputra, S.Kom., M.Kom.
NIP. 198307162014011008

Pembimbing



Febi Nur salisah, S.Kom., M.Kom.
NIP. 199002222023212038

LEMBAR PENGESAHAN

**PENGUNAAN METODE FMEA DALAM PENILAIAN
MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI
RUMAH SAKIT**

TUGAS AKHIR

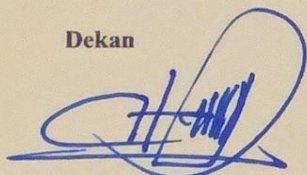
Oleh:

SETIA NINGSIH SAPUTRI
11950325023

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 30 April 2024

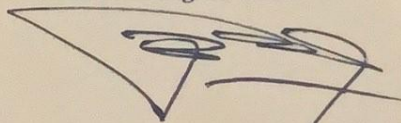
Pekanbaru, 30 April 2024
Mengesahkan,

Dekan



Dr. Hartono, M.Pd.
NIP. 196403011992031003

Ketua Program Studi



Eki Saputra, S.Kom., M.Kom.
NIP. 198307162011011008

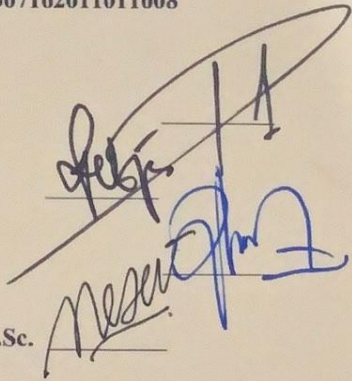
DEWAN PENGUJI:

Ketua : Syaifullah, SE., M.Sc.

Sekretaris : Febi Nursalisah, S.Kom., M.Kom.

Anggota 1 : Idria Maita, S.Kom., M.Sc.

Anggota 2 : Nesdi Evrilyan Rozanda, S.Kom., M.Sc.





- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Lampiran Surat :

Nomor : Nomor 25/2021

Tanggal : 10 September 2021

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama : SETIA MINGSIH SAPUTRI

NIM : 11950325023

Tempat/ Tgl. Lahir : HARAPAN JAYA

Fakultas/Pascasarjana : SAINS DAN TEKNOLOGI

Prodi : SISTEM INFORMASI

Judul Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya*:

PENGGUHAMAN METODE FMEA DALAM PENILAIAN
MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI
RUMAH SAKIT

Menyatakan dengan sebenar-benarnya bahwa :

1. Penulisan Disertasi/Tesis/Skripsi/Karya Ilmiah lainnya* dengan judul sebagaimana tersebut di atas adalah hasil pemikiran dan penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernya.
3. Oleh karena itu Disertasi/Tesis/Skripsi/Karya Ilmiah lainnya* saya ini, saya nyatakan bebas dari plagiat.
4. Apa bila dikemudian hari terbukti terdapat plagiat dalam penulisan Disertasi/Tesis/Skripsi/(Karya Ilmiah lainnya)* saya tersebut, maka saya bersedia menerima sanksi sesuai peraturan peraturan perundang-undangan.

Demikian Surat Pernyataan ini saya buat dengan penuh kesadaran dan tanpa paksaan dari pihak manapun juga.

Pekanbaru, 13 Juni 2024

yang membuat pernyataan



Setia Mingsih Saputri
 SETIA MINGSIH SAPUTRI
 NIM : 11950325023

*pilih salah satu sesuai jenis karya tulis

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 30 April 2024

Yang membuat pernyataan,

SETIA NINGSIH SAPUTRI

NIM. 11950325023



UIN SUSKA RIAU

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dengan menyebut nama Allah yang maha pengasih lagi maha penyayang

Assalamu 'alaikum Warahmatullahi Wabarakaatuh

Alhamdulillah Rabbil 'Alamin, segala puji bagi Allah *Subhanahu Wa Ta'ala* sebagai bentuk rasa syukur atas segala nikmat yang telah diberikan tanpa ada kekurangan sedikitpun. *Shalawat* beserta salam tak lupa pula kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Semoga kita semua selalu senantiasa mendapat syafa'at-Nya di dunia maupun di akhirat, *Aamiin Ya Rabbal'alaamiin*. Peneliti persembahkan karya kecil ini sebagai salah satu hadiah istimewa bentuk bakti, rasa terima kasih, dan hormatku kepada orang tuaku tercinta, yaitu Ayah dan Bunda.

Ayah dan Bunda tersayang, terima kasih atas setiap perjuangan, doa, bimbingan, dukungan, serta segala kebaikan yang kalian berikan kepada peneliti, dan selalu ada saat keadaan tersulit sekalipun. Terima kasih untuk segala pengorbanan yang kalian lakukan. Sampai kapanpun tiada rasa dan cara yang dapat membalas semuanya. Peneliti akan selalu mendoakan yang terbaik untuk Ayah dan Bunda agar bahagia dunia dan akhirat, serta diberikan tempat istimewa di sisi-Nya kelak sehingga kita bisa berkumpul kembali bersama-sama di Jannah-Nya. Terima kasih juga peneliti ucapkan kepada Adik, Kakek, dan Nenek yang sangat peneliti cintai. Terima kasih untuk segala waktu berharga yang telah dilalui bersama, doa, dan dukungan yang tiada hentinya.

Terima kasih kepada Fery Ardiansyah yang telah menemani, memberikan motivasi, dan semangat kepada peneliti. Terima kasih juga kepada teman-teman seperjuangan, yaitu Siti Wardani, Aisyah, Fajarul Amrie, Habibi Arbiansyah, Oak, Lydia, Aura, Asri, Maisarah Assa'diah, Ella, Dinda Sinaga, dan masih banyak lagi teman-teman yang telah memberikan dukungan, bantuan, inspirasi serta motivasi untuk terus maju kepada peneliti dalam pembuatan Tugas Akhir ini. Tak lupa peneliti ucapkan terima kasih kepada Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah mewariskan ilmu yang bermanfaat kepada peneliti untuk menyelesaikan studi di Program Studi Sistem Informasi ini. Semoga kita semua selalu diberikan kemudahan, rahmat, serta karunia-Nya. *Aamiin*.

Wassalamu 'alaikum Warahmatullahi Wabarakaatuh



KATA PENGANTAR

Alhamdulillah Rabbil 'Alamin, segala puji dan syukur kita ucapkan atas kehadiran Allah *Subhanahu Wa Ta'ala* atas segala rahmat dan karunia-Nya sehingga Laporan Tugas Akhir ini dapat penulis selesaikan. *Shalawat* beserta salam selalu turunkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam*, beserta keluarga dan para sahabatnya dengan lafaz *Allahumma Sholli'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Jasa beliau yang telah membawa manusia merasakan nikmatnya Islam seperti sekarang ini. Laporan Tugas Akhir ini disusun sebagai salah satu syarat memperoleh gelar Sarjana Komputer pada Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau. Selama penyusunan Laporan Tugas Akhir, penulis memperoleh banyak bantuan dari berbagai pihak, untuk itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang terlibat dan telah bersedia meluangkan waktunya untuk membantu penulis dalam menyelesaikan Laporan Tugas Akhir ini. Untuk itu, penulis ingin memberikan ucapan terima kasih kepada:

1. Bapak Prof. Dr. Hairunas, M.Ag sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Hartono, M.Pd sebagai Dekan Fakultas Sains dan Teknologi.
3. Bapak Eki Saputra, S.Kom., M.Kom sebagai Ketua Program Studi Sistem Informasi.
4. Ibu Siti Monalisa, ST., M.Kom sebagai Sekretaris Program Studi Sistem Informasi.
5. Bapak Tengku Khairil Ahsyar, S.Kom., M.Kom sebagai Kepala Laboratorium Program Studi Sistem Informasi.
6. Ibu Febi Nur Salisah, S.Kom., M.Kom sebagai Pembimbing Tugas Akhir peneliti yang telah memberikan bimbingan dan semangat dalam menyelesaikan Tugas Akhir ini.
7. Bapak Syaifullah, SE., M.Sc sebagai Ketua Sidang Tugas Akhir peneliti yang telah berkenan memberikan saran dan masukan yang berguna untuk penelitian ini.
8. Ibu Idria Maita, S.Kom., M.Sc sebagai Penguji I peneliti yang berkenan memberikan saran dan masukan yang berguna untuk penelitian ini.
9. Bapak Nesdi Evrilyan Rozanda, S.Kom., M.Sc sebagai Penguji II peneliti yang berkenan memberikan saran dan masukan yang berguna untuk penelitian ini.
10. Seluruh Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

banyak memberikan ilmunya kepada peneliti. Semoga ilmu yang diberikan dapat peneliti amalkan dan menjadi amal *jariah*.

1. Seluruh Pegawai dan Staff Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau yang telah membantu dan mempermudah proses administrasi selama perkuliahan ini.
2. Orang tua tercinta Ayahanda Iwan Munthe dan Ibunda Irawati yang selalu menjadi penyemangat peneliti sebagai sandaran terkuat dari kerasnya dunia yang tiada hentinya selalu memberikan kasih sayang, doa, dan motivasi dengan penuh keikhlasan yang tak terhingga kepada peneliti. Terima kasih sudah berjuang untuk kehidupan peneliti.
3. Kakek Misman, Nenek Malem, Atuk Rusli Munthe, dan Nenek Nurma yang selalu menjadi penyemangat peneliti sebagai sandaran terkuat dari kerasnya dunia yang tiada hentinya selalu memberikan kasih sayang, doa, dan motivasi dengan penuh keikhlasan yang tak terhingga kepada peneliti. Terima kasih sudah berjuang untuk kehidupan peneliti.
14. Kedua Adik peneliti, yaitu Della Kurniawati dan Adisti Humairah. Terima kasih atas segala doa dan motivasi yang kalian berikan kepada peneliti.
15. Seluruh pihak yang tidak dapat disebutkan satu persatu yang terlibat dalam perjuangan penyelesaian pendidikan Strata 1 (S1) yang telah memberikan bantuan, dukungan, dan semangat kepada peneliti, baik dalam pengumpulan data maupun penyusunan Tugas Akhir ini.

Semoga segala doa dan dorongan yang telah diberikan selama ini menjadi amal kebajikan dan mendapat balasan setimpal dari Allah *Subhanahu Wa Ta'ala*. Peneliti menyadari bahwa penulisan Tugas Akhir ini masih terdapat banyak kekurangan dan jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangat diharapkan demi kesempurnaan Tugas Akhir ini dan semoga laporan ini bermanfaat bagi kita semua. Akhir kata peneliti ucapkan terima kasih.

Pekanbaru, 10 Juni 2024

Peneliti,

UIN SUSKA RIAU

SETIA NINGSIH SAPUTRI
NIM. 11950325023

Jurnal INOVTEK Polbeng

Seri Informatika

ISSN: 2527 - 9866
Akreditasi Kemristekdikti
No. 36/E/KPT/2019
Peningkat Sinta 3

Vol. 4 No. 2 (2019) - Vol. 9 No. 1 (2024)

Home About User Home Search Current Archives Announcements Journal Template Accreditation Certificate

Home > Vol 8, No 2 (2023)

Jurnal Inovtek Polbeng Seri Informatika

Journal Inovasi dan Teknologi (Inovtek) Polbeng Seri Informatika (ISI) Politeknik Negeri Bengkalis is an informatics journal based on scientific research. This journal is expected to be a forum for all academics, researchers, and practitioners to disseminate research results. Inovtek Journal Polbeng - Informatics Series publishes manuscripts relating to Web and Mobile Computing, Image processing, Intelligent Systems, Information Systems, Databases, DSS, IT project management, Geographical Information Systems, Information Technology, Computer Network and Security, Wireless Sensor Networks, and others.

ISI is an open-access journal. Readers may read, download, copy, distribute, print, search, or link to the full texts of these articles without any charge. All submitted papers are peer-reviewed before being accepted for publication. The authors who intend to submit manuscripts to ISI should follow the norms described in the guidelines.

Each volume in a year is published in electronic form with a different number. The publication with the number 1 in June and number 2 in November. The language used in this journal is Bahasa Indonesia and English.

ISI has been ACCREDITED in SINTA 3A by Directorate General of Strengthening Research and Development-Ministry of Research, Technology and Higher Education-Republic of Indonesia in 2019 for Volume 4 Number 2 to Volume 9 Number 1 with No 36/E/KPT/2019.

Journal title	: Inovtek Polbeng Seri Informatika
Initials	: ISI
Frequency	: 2 issues per year
DOI	: Prefix 10.35314 by Crossref
ISSN	: 2527-9866
Accreditation	: SINTA 3A SK. No. 36/E/KPT/2019
Editor-in-chief	: Agus Tedyyana
Managing Editor	: Jaroji
Publisher	: P3M Politeknik Negeri Bengkalis
Citation Analysis	: Google Scholar, Crossref

ANNOUNCEMENTS

No announcements have been published.

More Announcements...

VOL 8, NO 2 (2023)

Jurnal Inovasi dan Teknologi Seri Informatika (Jurnal Inovtek Seri Informatika) merupakan jurnal informatika berbasis penelitian ilmiah. Jurnal Inovtek Seri Informatika terbit 2 kali dalam setahun. Secara berkala Jurnal Inovtek Seri Informatika terbit setiap bulan Juni dan November.

TABLE OF CONTENTS

FRONT MATTER

Cover dan Daftar Isi
Editor Editor

PDF (Bahasa
Indonesia)
i - vi

ARTICLES



AUTHOR GUIDELINES

REVIEWER GUIDELINES

FOCUS & SCOPE

EDITORIAL TEAM

PEER REVIEWERS

PUBLICATION ETHICS

COPYRIGHT TRANSFER AGREEMENT

CONTACT US

JOURNAL HISTORY

INDEXING

REGISTER FOR NEW REVIEWER

User

You are logged in as...

setianingsih_313

- » My Journals
- » My Profile
- » Log Out

Tools



Current Issue

ATOH 2.0

PEE 2.0

PEE 3.0

**Pusat Penelitian dan Pengabdian Kepada Masyarakat
Politeknik Negeri Bengkalis**

Jl. Bathin alam, Sungai Alam Bengkalis-Riau 28711

SURAT KETERANGAN PENERIMAAN NASKAH JURNAL

Nomor: 009/ISI/Vol IX.1/2024

Dewan editor Jurnal INOVTEK Polbeng Seri Informatika telah menerima artikel berikut:

Penulis : Setia Ningsih Saputri, Febi Nur Salisah, Idria Maita, Nesdi Evrilyan
Rozanda

Judul : Penggunaan Metode FMEA dalam Penilaian Manajemen Risiko
Keamanan Sistem Informasi Rumah Sakit

Asal Instansi : Universitas Islam Negeri Sultan Syarif Kasim Riau

Menyatakan bahwa artikel tersebut telah memenuhi kriteria Penulisan Jurnal INOVTEK Polbeng Seri Informatika Politeknik Negeri Bengkalis dan akan diterbitkan pada Volume 9 Nomor 1 Tahun 2024. Demikian surat keterangan ini dibuat untuk digunakan sebagaimana mestinya

Bengkalis, 18 Maret 2024

Ketua Dewan Editor



Agus Tedyyana

Penggunaan Metode FMEA dalam Penilaian Manajemen Risiko Keamanan Sistem Informasi Rumah Sakit

Setia Ningsih Saputri¹, Febi Nur Salisah², Idria Maita³, Nesdi Evrilyan Rozanda⁴

Universitas Islam Negeri Sultan Syarif Kasim Riau, Jl. HR. Soebrantas No. 155 Km. 15, Panam
 Email: ningsihsetya313@gmail.com¹, febinursalisah@uin-suska.ac.id², idria@uin-suska.ac.id³,
 nesdi.rozanda@uin-suska.ac.id⁴

Abstract –In the healthcare industry, where hospitals are involved, information system security risk management is crucial for preventing and mitigating information system failures that could impede the attainment of organizational objectives. One such failure could be damage to the hospital service system, which could cause operational disruptions. In the execution of risk management and assessment, one notable method is the Failure Mode and Effect Analysis (FMEA). This study specifically examines the risks associated with the information system of a health sector industry, RSUD Indah Bagan Batu, called SIMRS Khanza. This research not only provides a comprehensive picture of possible security risks, but also risk categorization with RPN that can prioritize appropriate mitigation so that SIMRS Khanza can protect patient data, doctors, medicines and other staff from potential threats, which all This data has a big influence on the hospital service process. Risk assessment using the FMEA method which includes; business process flow, risk brainstorming, calculation of severity, occurrence and detection values, resulting in an RPN value of 34 risks in the information system used with 5 RPN level categories: three fall under the very high category (500–504), five in the high category (120–180), six in the medium category (84–108), four go into the extremely low group (8–15), while 17 fall into the low category (20–72).

Keywords – FMEA, Information Security System, Risk Management, RPN, Hospital.

Intisari –Manajemen risiko keamanan sistem informasi sangat penting dalam sektor kesehatan seperti Rumah Sakit untuk melindungi dan memperkecil setiap kegagalan sistem informasi yang berpotensi menghambat pencapaian tujuan perusahaan, seperti kerusakan pada sistem pelayanan Rumah Sakit yang digunakan, yang dapat mengganggu operasional Rumah Sakit. FMEA (*Failure Mode and Effect Analysis*) adalah salah satu metode yang digunakan dalam penilaian dan pengelolaan risiko. Penelitian ini menganalisa risiko pada sistem informasi yang digunakan RSUD Indah Bagan Batu, yaitu SIMRS Khanza. Penelitian ini tidak hanya memberikan gambaran lengkap tentang ancaman keamanan yang mungkin terjadi, tetapi pengkategorian risiko dengan RPN dapat memprioritaskan mitigasi yang tepat. Dengan demikian, data SIMRS Khanza dapat dilindungi dari ancaman terhadap pasien, dokter, obat-obatan, dan staf lainnya. Semua data ini berdampak signifikan pada proses pelayanan rumah sakit. Penilaian risiko menggunakan metode FMEA yang meliputi; alur proses bisnis, risiko *brainstorming*, perhitungan nilai *severity*, *occurrence*, dan *detection*, sehingga menghasilkan nilai RPN sebanyak 34 risiko pada sistem informasi yang digunakan, dengan 5 kategori *level RPN* yaitu 3 kategori *very high* dengan rentang 500-504, 5 kategori *high* dengan rentang 120-180, 6 kategori *moderate* dengan rentang 84-108, 17 kategori *low* dengan rentang 20-72 dan 4 kategori *very low* dengan rentang 8-15.

Kata Kunci – FMEA, Keamanan Sistem Informasi, Manajemen Risiko, RPN, Rumah Sakit

1. Ularang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.
 a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

I. PENDAHULUAN

Di era kontemporer seperti ini, kebutuhan akan teknologi informasi untuk membantu bisnis menjalankan proses bisnisnya dengan cepat dan efisien semakin meningkat. Dengan teknologi informasi yang sesuai dengan kebutuhan pengguna, organisasi dapat mencapai visi, misi, dan tujuannya[1]. Dalam suatu bisnis, teknologi informasi menjadi aset yang paling penting pada suatu organisasi, sehingga penggunaan TI ini tidak hanya memiliki keuntungan, tetapi juga memiliki risiko, yang pada akhirnya dapat merugikan organisasi [2], [3]. Untuk menjamin ketersediaan data yang tepat dan dapat dipercaya oleh lingkungan internal maupun eksternal, teknologi informasi yang mengandung banyak data penting harus dilindungi keamanannya[4]. Organisasi yang menggunakan teknologi informasi harus memiliki kemampuan untuk melakukan manajemen risiko serta memastikan bahwa sistem informasi mereka berjalan lancar dan tidak mengganggu operasi perusahaan yang dapat menimbulkan kerugian[5].

Analisis dan pengendalian risiko yang ada di sebuah perusahaan atau organisasi dikenal sebagai manajemen risiko. Manajemen risiko bertujuan untuk melindungi dan mengurangi semua kegagalan yang mungkin terjadi pada perusahaan dari tingkat risiko yang paling tinggi, yang dapat menghambat pencapaian tujuan perusahaan[6]. Manajemen Risiko memiliki tiga proses tahapan utama yaitu mengidentifikasi risiko, evaluasi & pengukuran risiko dan pengelolaan risiko[7]. Risiko yang biasa terjadi terhadap data dan keamanan teknologi informasi meliputi: (1) Kerusakan *hardware* dan *software*, (2) *Malware*, (3) *Virus computer*, (4) *Spam, scams, and phishing*, dan (5) *Human error*[8]. Dalam lingkup keamanan sistem informasi mencakup pula 3 hal, yaitu: kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).

Metode *Failure Mode and Effect Analysis* (FMEA) adalah salah satu metode yang mendukung yang dapat digunakan untuk mengatasi masalah manajemen risiko keamanan sistem informasi ini yang berguna sebagai sarana untuk melaksanakan penilaian dan pengelolaan risiko. *Failure Mode and Effect Analysis* (FMEA) memungkinkan analisis dan identifikasi kemungkinan kegagalan yang menghasilkan daftar prioritas risiko, sehingga membantu memprioritaskan penyelesaian masalah yang paling penting [4], [8]. Salah satu tujuan dari metode *Failure Mode and Effect Analysis* (FMEA) adalah pengambilan tindakan untuk meminimalkan kegagalan, dimulai dengan konsekuensi yang paling signifikan. Adapun prosedur pembuatan FMEA, yaitu: (1) *Identify* Proses Bisnis, (2) *Brainstorming* Risiko, (3) Mengidentifikasi potensi kegagalan berdasarkan tingkat *Severity* (S), *Occurrence* (O) and *Detection* (D) dan (4) Menghitung *Risk Priority Number* (RPN) = $S \times O \times D$ [10]. FMEA membantu mengidentifikasi dan menilai mode, penyebab, dan efek dari kegagalan sistem sebelum terjadi. Untuk setiap kegagalan, hasil analisis dan penilaian ini akan menghasilkan tingkatan yang sesuai dengan tingkat risiko dan kemungkinan[11].

Studi terkait sebelumnya mengenai manajemen risiko keamanan sistem informasi menggunakan FMEA telah banyak dilakukan seperti yang telah dilakukan oleh [8], [9], [10], [11], dan [12]. Dalam penelitian yang dilakukan oleh [9], ditemukan 23 kemungkinan kegagalan untuk aset keamanan sistem informasi, termasuk 11 kemungkinan kegagalan *hardware*, 4 kemungkinan kegagalan *software*, 2 kemungkinan kegagalan *data*, 2 kemungkinan kegagalan sumber daya manusia, dan 5 kemungkinan kegagalan *network*. Hasil dari pengkategorian risiko sistem informasi Dinas Komunikasi dan Informasi Kabupaten Sambas menggunakan metode FMEA menunjukkan bahwa satu risiko kategori tinggi, empat risiko kategori sedang, tujuh risiko kategori rendah, dan sebelas risiko kategori sangat rendah. Penelitian yang dilakukan oleh [10] pada SIMAK UIN Raden Fatah Palembang terdapat enam kategori nilai telah dihitung menggunakan rumus RPN, yaitu satu nilai berkategori *very high*, tiga nilai berkategori *high*, empat nilai berkategori *moderate*, tiga nilai berkategori *low*, enam nilai berkategori *very low* dan satu nilai berkategori hampir tidak ada kegagalan. Lalu pada penelitian yang dilakukan oleh [11] pada Sistem Informasi RSIA Eria Bunda dengan tujuan

1. Uraian yang mengungkap sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



penelitian untuk mengetahui tingkat risiko sistem informasi dan menawarkan solusi untuk RSIA Eria Bunda. Hasil penelitian menunjukkan bahwa satu aktivitas termasuk kategori tinggi, enam aktivitas termasuk kategori sedang, dan sembilan belas aktivitas termasuk kategori rendah. Adapun juga penelitian yang dilakukan oleh [12] pada Sistem Informasi Karoline dari hasil prioritas risiko yang telah ditentukan maka peringkat risiko berdasarkan catatan proses nilai RPN, yaitu *cybercrime* (RPN = 216) sebagai *level very high*, kegagalan *system* (RPN = 160) sebagai *level high*, *human failure* (RPN = 112) sebagai *level medium* dan kerusakan komputer (RPN = 70) sebagai *level low*. Dan penelitian yang dilakukan oleh [13] pada Sistem Informasi Rocketic.id setelah dilakukan identifikasi risiko, selanjutnya melakukan analisis risiko. Dalam menganalisis risiko, diperlukan adanya penghitungan *Risk Priority Number* (RPN). *Level* RPN didapatkan berdasarkan perkalian dari *Severity* (S), *Occurrence* (O) dan *Detection* (O). Adapun hasil pengkategorian prioritas risiko pada Sistem Informasi Rocketic.id terdapat 3 pada kategori *very high*, 1 pada kategori *high*, 2 kategori *medium*, 3 kategori *low* dan 3 pada kategori *very low*.

Pada penelitian yang saya teliti di RSUD Indah Bagan Batu, mereka juga salah satu instansi yang telah menerapkan teknologi informasi dalam menjalankan bisnisnya. RSUD Indah Bagan Batu memiliki sistem informasi yang bernama Sistem Informasi Manajemen Rumah Sakit (SIMRS) Khanza. SIMRS Khanza adalah teknologi informasi yang dirancang untuk meningkatkan pelayanan Rumah Sakit. Ini bekerja dengan mengelola informasi yang berkaitan dengan data pasien dan laporan kegiatan Rumah Sakit. Dengan sistem informasi ini, tenaga kesehatan dapat bekerja dengan lebih efisien dan produktif, seperti yang mereka lakukan sebelumnya secara manual, tetapi dengan adanya sistem informasi ini, mereka menjadi lebih modern dan sistematis, yang berarti lebih banyak waktu yang dihabiskan untuk merawat pasien. Dalam pengimplementasian SIMRS Khanza ini, untuk meningkatkan pengetahuan *user* tentang cara mengaplikasikan, mengelola, dan menggunakan sistem dengan benar, evaluasi sistem dan *user* harus dilakukan.

Berdasarkan hasil observasi dan wawancara, SIMRS Khanza yang digunakan RSUD Indah Bagan Batu ini memiliki beberapa masalah yang sering terjadi seperti rusaknya *hardisk* yang disebabkan oleh listrik yang tidak stabil mengakibatkan hilangnya *data* pasien, lalu *server down* yang penyebabnya masih belum diketahui sampai sekarang dan belum adanya pendokumentasian terkait penanganan dan pencegahan risiko tersebut. Selain itu, masalah utama yang dihadapi RSUD ini termasuk kekurangan kebijakan keamanan informasi, yang disebabkan oleh kurangnya pelatihan staf tentang keamanan sistem informasi. Akibatnya, SIMRS Khanza berada di bawah risiko dan ancaman yang signifikan karena kerentanan sistem yang tidak ditangani dengan tepat, yang menghambat proses pelayanan di RSUD Indah Bagan Batu. Hal ini disebabkan oleh RSUD Indah Bagan Batu belum melakukan identifikasi risiko serta ancaman yang terjadi terhadap SIMRS Khanza. Sehingga dalam proses pengembangan sistem informasi ini sangat penting melakukan evaluasi sistem menurut persepsi *user* karena untuk meningkatkan pelayanan dan kepuasan *user*. Rumah sakit juga harus bertanggung jawab untuk melindungi data agar tidak hilang atau disalahgunakan oleh individu yang tidak bertanggung jawab.

Oleh karena itu, proses penilaian risiko dari penggunaan Sistem Informasi Manajemen Rumah Sakit (SIMRS) Khanza RSUD Indah Bagan Batu dilakukan dalam penelitian ini demi memperkuat dan melindungi keamanan sistem informasi tersebut. Dalam menilai risiko, penting untuk mempertimbangkan kemungkinan suatu peristiwa terjadi dan dampak yang akan ditimbulkannya[14]. Metode *Failure Mode and Effect* (FMEA) digunakan untuk mengidentifikasi risiko dan ancaman pada sistem informasi ini berdasarkan masalah yang telah dijelaskan. Karena dengan metode *Failure Mode and Effect* (FMEA) terdapat cara untuk dapat langsung menentukan apa prioritas risiko pada sistem informasi tersebut, yaitu hasilnya akan didapat dengan cara perhitungan *Risk Priority Number* (RPN) sehingga pihak rumah sakit dapat

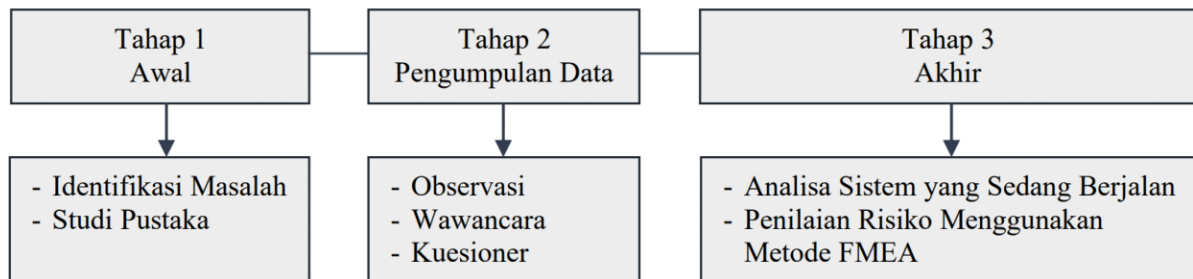
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



mengurangi risiko terhadap pasien dan operasi rumah sakit dengan dapatnya titik kegagalan atau risiko pada sistem informasi yang digunakan.

II. SIGNIFIKANSI STUDI

Dengan menggunakan pendekatan kualitatif, setelah studi lapangan awal, kerangka konseptual untuk penelitian kualitatif dibuat. Kerangka konseptual ini membantu peneliti memahami fenomena dan mendapatkan pemahaman yang lebih baik tentang masalah yang sedang diteliti[15]. Wawancara, observasi, kuesioner, dan penelitian pustaka adalah semua sumber data yang dihasilkan, termasuk data primer dan sekunder. Berikut dibawah ini Gambar 1. menunjukkan Metode Penelitian beserta penjelasannya:



Gambar 1. Metode Penelitian

A. Studi Literatur

Tahapan studi literatur ini dilakukannya pemeriksaan literatur tentang subjek penelitian ini. Sumber literatur dapat berupa buku, artikel, dan penelitian sebelumnya mengenai manajemen risiko keamanan sistem informasi dengan metode FMEA.

1. Manajemen Risiko

Jika bisnis ingin berjalan, manajemen harus belajar mengambil lebih banyak risiko dan menerima kegagalan daripada hanya mengontrol atau mengurangi risiko yang ada. Manajemen risiko adalah proses analisis dan pengendalian yang digunakan untuk menemukan dan mengendalikan risiko yang ada pada suatu organisasi. Manajemen risiko memungkinkan organisasi untuk mengurangi risiko yang dapat memiliki konsekuensi yang signifikan bagi organisasi sehingga dengan adanya proses manajemen risiko dapat membantu organisasi dalam membuat keputusan yang lebih baik dan meningkatkan efisiensi kinerja[16]. Risiko dan cara terbaik untuk menguranginya berkorelasi dengan tingkat keuntungan perusahaan atau organisasi[17]. Salah satu proses dalam manajemen risiko yang dapat dilakukan ialah penilaian risiko (*risk assessment*).

2. Keamanan Sistem Informasi

Menurut Whitman dan Mattord (2012) dalam [18], Keamanan Sistem Informasi merupakan melindungi *confidentiality*, *integrity*, dan *availability* pada aset informasi selama penyimpanan, pengolahan, dan transmisi. Ini dapat dicapai melalui pelaksanaan undang-undang, kesadaran, pelatihan, dan penggunaan teknologi. Keamanan sistem informasi mencakup perlindungan elemen-elemen berikut[19]:

a. Confidentiality (Kerahasiaan)

Elemen yang menjaga kerahasiaan data atau informasi termasuk memastikan bahwa hanya pihak yang berwenang yang dapat melihatnya dan memastikan bahwa pengiriman, penerimaan, dan penyimpanan data aman.

b. Integrity (Integritas)

1. Ujaran menguap sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.
 a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

Elemen yang memastikan bahwa tidak adanya perubahan data tanpa izin pihak yang berwenang, menjaga integritas dan keakuratan informasi, serta menerapkan prosedur untuk menjaga integritas informasi.

c. *Availability* (Ketersediaan)

Elemen yang memastikan bahwa data dapat diakses saat dibutuhkan dan hanya orang yang berhak dapat menggunakan informasi dan perangkat yang terkait.

Hak Cipta Dilindungi

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

3. *Metode Failure Mode and Effect Analysis (FMEA)*

FMEA adalah teknik rekayasa analisis terstruktur yang populer di industri mengenai kemungkinan kegagalan dalam menetapkan, mengidentifikasi, dan menghilangkan masalah, kegagalan, *error*, dan lainnya dari sistem, desain, proses, atau jasa sebelum mencapai konsumen[20][21]. Hasil akhir yang diperoleh dari proses FMEA yaitu dengan *Risk Priority Number* (RPN), yang juga dikenal sebagai poin risiko prioritas. Skor RPN dihitung dengan perkalian antara tiga peringkat, yaitu *Severity*, *Occurance*, dan *Detection* (SOD).

B. *Tahapan Pengumpulan Data Penelitian*

1. *Observasi*

Observasi merupakan kegiatan pengamatan langsung ke lapangan dengan tujuan untuk memperkuat kebenaran data. Selama kegiatan observasi, proses bisnis saat ini di SIMRS *Khanza* diamati secara langsung.

2. *Wawancara*

Wawancara merupakan salah satu tahapan dari pengumpulan data melalui tanya jawab bersama pihak yang relevan, yaitu dengan salah satu *staff* RSUD Indah Bagan Batu. Tahap ini dilakukan bertujuan untuk mengetahui risiko serta permasalahan yang pernah dialami.

3. *Kuesioner*

Pada tahapan ini dilakukan dengan menyebarkan kuisisioner atau lembar kerja pengambilan data berupa angket yang digunakan untuk mengumpulkan data. Fokus dari kuisisioner ini adalah untuk mengevaluasi potensi bahaya yang terkait dengan penggunaan teknologi informasi di organisasi tempat penelitian ini. Responden kuisisioner penelitian ini dibuat dengan menggunakan *RACI Chart*. *RACI* adalah *Responsible*, *Accountable*, *Consulted*, *Informed* (RACI). *RACI Matrix* memiliki kemampuan untuk mengelola penugasan sumber daya untuk setiap pekerjaan proyek. Selain itu, *RACI* digunakan untuk mengidentifikasi hubungan antara tugas dan peran, tanggung jawab, dan tingkat otoritas yang terkait dengan setiap aktivitas proyek. Dengan menentukan siapa yang menerima informasi, seberapa sering, dan pada tingkat detail apa, *RACI* berfungsi sebagai dasar untuk rencana komunikasi[22].

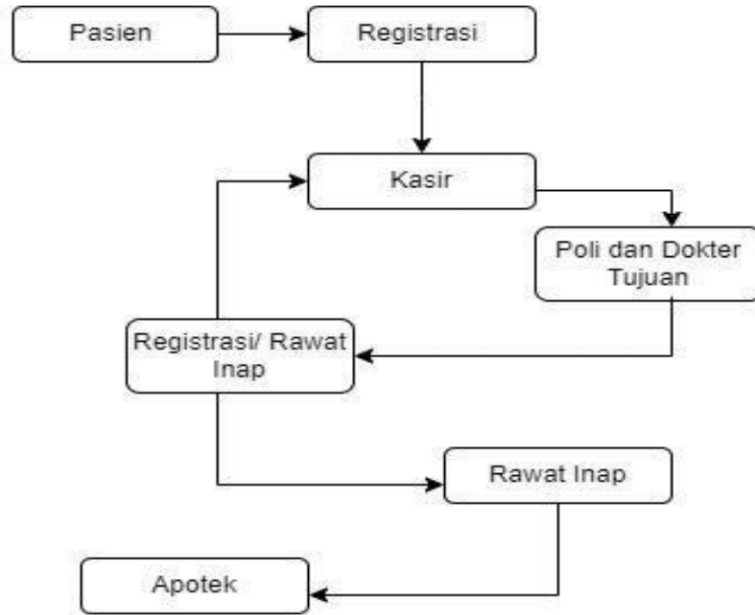
III. HASIL DAN PEMBAHASAN

A. *Analisa Sistem yang Sedang Berjalan*

Pada tahap ini dilakukannya peninjauan setiap proses bisnis pada SIMRS *Khanza* bertujuan untuk mengetahui dan menganalisa proses bisnis mana yang memiliki potensi kegagalan yang ada di RSUD Indah Bagan Batu. Adapun proses bisnis pada RSUD Indah Bagan Batu antara lain sebagai berikut:

1. *Proses Bisnis Instansi*

Gambar 2. menunjukkan Proses Bisnis Instansi RSUD Indah Bagan Batu:



Gambar 2. Proses Bisnis Instansi

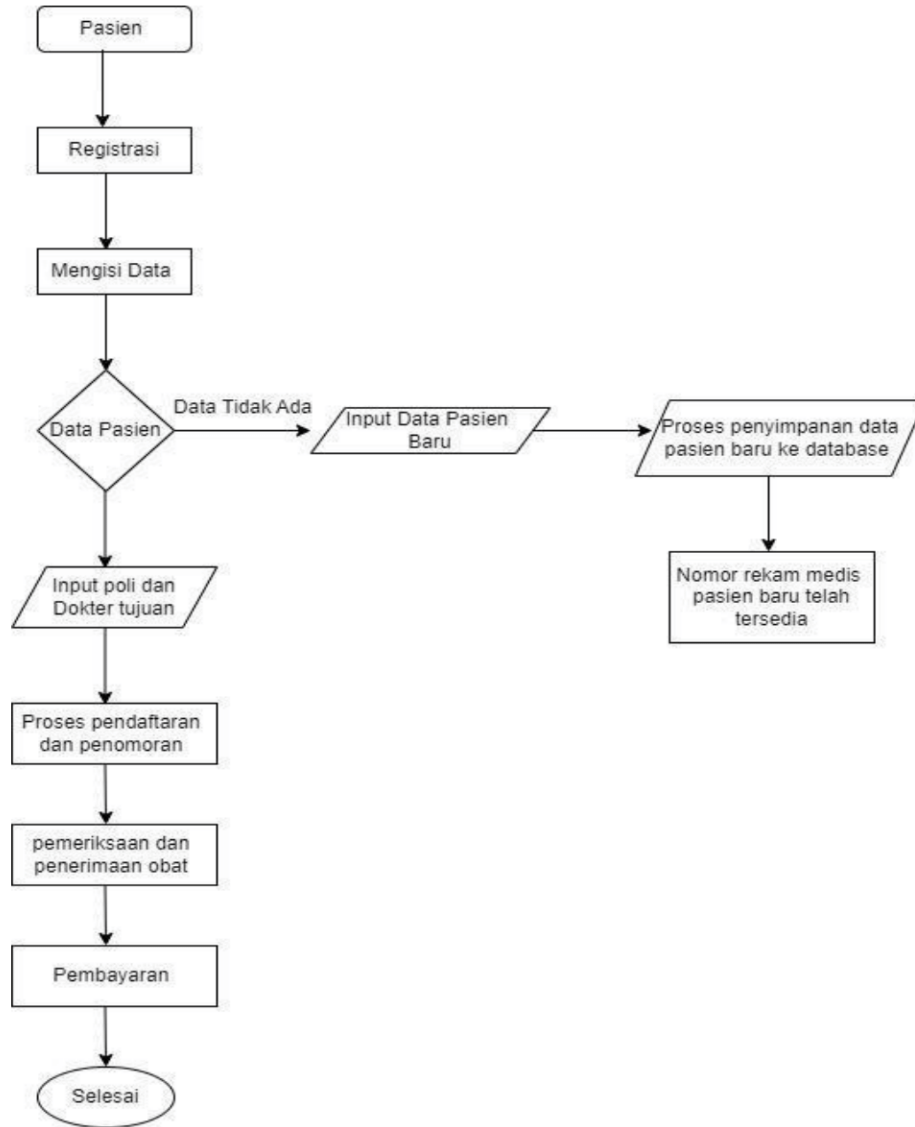
Adapun berikut dibawah ini penjelasan gambar alur diatas:

1. Penerimaan Data Pasien: Tahap awal proses termasuk menambahkan pasien baru ke sistem informasi rumah sakit.
2. Penyimpanan dan Pengelolaan Data: Metode untuk menyimpan dan mengawasi data pasien di sistem informasi, termasuk mengatur akses dan menggunakan teknologi keamanan.
3. Akses dan Penggunaan Data: Bagaimana karyawan rumah sakit mengakses dan menggunakan data pasien untuk memberikan perawatan yang tepat kepada pasien.
4. Pemantauan dan Audit: Proses pemantauan dan audit terhadap aktivitas yang berkaitan dengan penggunaan sistem informasi untuk mengidentifikasi potensi risiko keamanan atau penyalahgunaan.
5. Tindakan Perbaikan dan Mitigasi: Kerentanan atau masalah keamanan diatasi dengan perbaikan teknis, pelatihan karyawan, dan perubahan kebijakan.
6. Evaluasi Kinerja: Proses untuk mengevaluasi seberapa efektif prosedur mitigasi risiko yang diterapkan dan memastikan bahwa sistem informasi beroperasi sesuai dengan persyaratan keamanan yang ditetapkan.

2. *Proses Bisnis Sistem Informasi*

Gambar 3. menunjukkan Proses Bisnis SIMRS *Khanza*:

UIN SUSKA RIAU



Gambar 3. Proses Bisnis SIMRS Khanza

Adapun berikut dibawah ini penjelasan gambar alur diatas:

1. Pendaftaran Pasien: Proses ini mencakup registrasi pasien baru yang datang ke RSUD Indah Bagan Batu. Pada tahap ini, data pribadi seperti nama, alamat, dan informasi lainnya dimasukkan ke dalam sistem RSUD, yang memungkinkan RSUD mendapatkan informasi yang diperlukan untuk memberikan layanan medis kepada pasien.
2. Pemeriksaan Pasien: Pasien akan menjalani pemeriksaan oleh petugas medis setelah registrasi. Diagnosis awal, pemeriksaan fisik, dan mungkin pemeriksaan tambahan seperti tes darah atau *rontgen* adalah semua bagian dari proses ini.
3. Pengobatan dan Tindakan Medis: Pasien akan diberikan perawatan dan tindakan medis yang sesuai berdasarkan hasil pemeriksaan. Ini dapat termasuk pemberian obat, terapi fisik, atau prosedur medis lainnya.
4. Pencatatan Data Medis: Sistem SIMRS Khanza menyimpan catatan rinci tentang semua prosedur medis dan tindakan medis yang dilakukan terhadap pasien. Catatan ini mencakup diagnosis, resep obat, hasil tes laboratorium, dan catatan lainnya yang berkaitan dengan perawatan pasien.
5. Pembayaran dan Administrasi: Pasien akan membayar untuk layanan medis yang diberikan setelah perawatan selesai. Pengelolaan data keuangan, penagihan asuransi, dan pencatatan administratif lainnya adalah bagian dari proses administrasi juga.

1. Uraian yang menguraikan sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



6. Tindak Lanjut dan Pemantauan: RSUD Indah Bagan Batu akan memantau perkembangan kondisi pasien setelah perawatan. Ini dapat mencakup kunjungan ulang, pemeriksaan rutin, atau konsultasi lanjutan dengan dokter.

Proses bisnis SIMRS Khanza di RSUD Indah Bagan Batu dirancang untuk memastikan bahwa setiap langkah dalam pengelolaan informasi kesehatan dilakukan secara efisien, terdokumentasi dengan baik, dan sesuai standar prosedur medis yang berlaku. RSUD dapat meningkatkan efisiensi layanan kesehatan yang diberikan kepada pasien dan memastikan bahwa data medis pasien dikelola dengan baik dan aman.

B. Pemetaan RACI Chart

Untuk membantu memilih partisipan penelitian, RACI Chart menawarkan susunan jabatan sebagai pedoman. RACI Chart membantu peneliti mengidentifikasi responden. Responden yang dipilih diwakili dengan tabel:

- a. *Responsibility*, yaitu orang yang secara langsung melakukan pekerjaan atau yang bertanggung jawab atas kegiatan.
- b. *Accountability*, yaitu individu yang memiliki otoritas untuk membuat keputusan akhir.
- c. *Consult*, yaitu individu yang menawarkan saran atau masukan juga yang membantu proses pekerjaan.
- d. *Informed*, yaitu orang yang mendapatkan informasi mengenai hasil keputusan.

Perhitungan responden didasarkan pada RACI Chart yang menunjukkan peran *key stakeholder* yang terkait secara langsung dengan proses pengelolaan TI. Proses-proses ini akan disampaikan oleh departemen TI di RSUD Indah Bagan Batu. Selain itu, Pemimpin bertanggung jawab atas pelaksanaan proses TI; oleh karena itu, mereka adalah responden pada penelitian ini dalam peran penanggung jawab atau *accountable*.

TABEL I
RACI CHART

Tugas atau peran	Tim IT	User Rumah sakit	Esellon III	Esellon II
Infrastruktur sistem jaringan, server, dan database pada Rumah Sakit Umum Indah dibangun, diawasi, dioperasikan, dan dipelihara.	R	C	A	I
Mengawasi, menjalankan dan mengevaluasi kegiatan operasi IT	C	R	A	I
Membuat keputusan, mendapatkan persetujuan, dan bertanggung jawab atas seluruh karyawan Rumah Sakit Umum Indah	C	I	R	A
Memberi solusi bisnis Rumah Sakit Umum Indah	C	I	R	A
Memberi saran/rekomendasi untuk perbaikan	C	R	A	I

C. Penilaian Risiko Menggunakan Metode FMEA

1. Identify Process

Hak Cipta Dilindungi Undang-Undang. 1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber: a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah. b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau. 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



1) *Daftar Aset Komponen TI*

Berikut pada Tabel II. Daftar Aset Komponen TI yang dimiliki oleh RSUD Indragiri Siantan dalam mendukung berjalannya teknologi informasi yang digunakan:

TABEL III
DAFTAR ASET KOMPONEN TI

Kategori	Keterangan	Asset
Hardware	PC server	HPE Proliant DL20 Gen10
Software	KHANZA Sistem Operasi	Admin, user (pegawai)
Jaringan	LAN Kabel jaringan	Indihome dengan kapasitas 150Mbps. Fiber Optik (mencangkup seluruh gedung RSUD Indragiri Siantan) UTP CAT 6
Data	Data pasien Data administrasi Data pegawai	Identitas pasien: Nama pasien, alamat, jenis penyakit Pengelola keuangan, pemasaran dan manajemen pelayanan Data dokter umum/spesialis, tenaga kerja kebidanan, tenaga kerja kefarmasian, tenaga kerja teknologi dan informasi
People	Admin	Seluruh kegiatan sistem dapat diakses oleh admin, mulai dari input, edit, tambah data user, hapus data, mengelola hak akses.

2. *Brainstorming Risiko*

Brainstorming risiko dilakukan untuk menentukan kegagalan sistem yang mungkin terjadi. Berikut merupakan tahapan *brainstorming* risiko:

1) *Menentukan Kekuatan dan Kelemahan Instansi*

Tujuan dari prosedur ini adalah untuk menemukan peluang bahaya. Berikut dibawah menunjukkan Tabel III. Kekuatan dan Kelemahan Instansi:

TABEL III
KEKUATAN DAN KELEMAHAN INSTANSI

Kekuatan Instansi	Kelemahan Instansi
Lokasi Rumah Sakit yang strategis	Sistem untuk membuat keputusan beroperasi secara central
Adanya hak untuk mengakses ruangan server	Sedikitnya tenaga kerja teknologi
Dilengkapi kamera CCTV	Komputer yang memenuhi standar ISO
Ada petugas yang bertanggung jawab untuk menjaga keamanan	Kurangnya <i>human resource</i> di bidang teknologi

Nantinya, hasil dari tabel analisis kekuatan dan kelemahan instansi dan sistem di atas dapat digunakan sebagai referensi untuk proses pembuatan kuisisioner untuk menentukan kontrol proses yang tepat dalam memberikan nilai deteksi.

2) *Effect Analysis*

Tujuan proses ini guna untuk mengetahui potensi ancaman dan dampak dari ancaman tersebut. Berikut dapat dilihat pada Tabel IV. *Effect Analysis*:

Hak Cipta: ...
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumpukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



TABEL IV
EFFECT ANALYSIS

Risiko	Potensi Efek
Kebakaran <i>server</i>	Baik kinerja maupun operasional terhenti dan kerugian finansial
<i>Server down</i>	Baik kinerja maupun operasional terhenti dan kerugian hambat
Kerusakan <i>server</i>	Tidak dapat mengakses <i>server</i>
Kerusakan tidak dapat digunakan	Baik kinerja maupun kegiatan operasional terhenti dan kerugian hambat
Kegagalan jaringan	Baik kinerja maupun kegiatan operasional terhenti dan kerugian hambat
Kerusakan perangkat jaringan	Baik kinerja maupun kegiatan operasional dan kerugian hambat
Kegagalan <i>software</i>	Baik kinerja maupun kegiatan operasional terhenti dan kerugian hambat
Kegagalan sistem	Baik kinerja maupun kegiatan operasional terhenti
Kegagalan manusia	Profesional kinerja pelayanan terhadap pasien rumah sakit tidak maksimal
Falsifikasi atau penyalahgunaan hak akses	Reputasi instansi

D. Menentukan Hasil RPN dari Perhitungan *Severity*, *Occurrence* dan *Detection*

Pada tahap ini, proses yang dilakukan ialah menentukan nilai-nilai risiko yang terjadi di RSU Indah Bagan Batu. Nilai-nilai risiko terdiri dari nilai *severity*, *occurrence*, dan *detection* diperoleh dari kuisioner yang telah diisi berdasarkan RACI Chart. Nilai-nilai ini digunakan sebagai referensi untuk menentukan risiko tertinggi.

1. Menghitung Nilai RPN

Pada tahap ini dilakukan perhitungan *Risk Priority Number* (RPN). Nilai *severity*, *occurrence*, dan *detection* dilakukan untuk melakukan perhitungan ini. Nilai RPN adalah skor potensial dari risiko yang telah diidentifikasi. Berikut dibawah menunjukkan Tabel V. Hasil RPN:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.
 a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



TABEL V
HASIL RPN

Code	Process Function (category)	Critical Assets	Potential Failure Modes (process defects)	Potential Effects of Failure	S E V	Potential Causes of Failure	O C C	Current Process Controls	D E T	R P N	Lvl
HW 01	Hardware	Server	Kebakaran server	Baik kinerja maupun kegiatan operasional terhenti	9	Server overheating	2	Dilakukannya pengecekan ruangan server rutin tiap hari	2	36	Low
HW 02			Kebakaran server	Kerugian finansial	9	Hubungan arus pendek (power failure)	1	Pengecekan infrastruktur TI yang rusak	5	45	Low
HW 03			Server Overheat	Baik kinerja maupun kegiatan operasional terhambat	6	Tidak berfungsinya AC pada ruangan server	3	Dilakukannya pengecekan ruangan server rutin tiap hari	2	36	Low
HW 04			Server Down	Baik kinerja maupun kegiatan operasional terhambat	5	Serangan DDOS atau terlalu banyak unit yang mengakses server secara bersamaan	3	Pengecekan infrastruktur TI yang rusak	3	45	Low
HW 05			Kerusakan server	Server tidak dapat digunakan	6	Maintenance dan control yang tidak rutin	5	Pengecekan infrastruktur TI yang rusak	3	90	Moderate
HW 06		Kerusakan server	Kerugian finansial	4	Bencana alam seperti mengalami kerusakan bangunan (server berada dilantai bawah)	1	Pengecekan infrastruktur TI yang rusak	3	12	Very Low	
HW 07		Komputer/PC	Kerusakan komputer	Baik kinerja maupun kegiatan operasional terhambat	7	Adanya serangan virus	3	Adanya antivirus setiap PC	4	84	Moderate
HW 08			Komputer tidak dapat digunakan	Baik kinerja maupun kegiatan operasional terhambat	7	Kesalahan dalam konfigurasi komputer	4	Pengecekan infrastruktur TI yang rusak	5	140	High
HW 09			Komputer tidak dapat digunakan	Baik kinerja maupun kegiatan operasional terhambat	7	Lisensi software yang digunakan sudah melebihi batas waktu	7	Pengecekan infrastruktur TI yang rusak	3	147	High
HW 10			Komputer tidak dapat digunakan	Kerugian finansial	5	Bencana alam (kebakaran, banjir, petir)	1	Pengecekan infrastruktur TI yang rusak dan mematikan perangkat sebelum pulang	3	15	Very Low
HW 11	Perangkat komputer out of dated		Baik kinerja maupun kegiatan operasional terhambat	6	Usangnya teknologi yang digunakan	3	Monitoring perangkat sekali dalam setahun	4	72	Low	
HW12	Perangkat jaringan	Hilangnya komputer/PC	Kerugian finansial	7	Pencurian	2	Pengawasan dan pemantauan akses dan mengunci	2	28	Low	

1. Urut-urutan mengungkap sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebarkan sumber:
 a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



1. Urut-urutan menguap sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebarkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

HW1 3		Akses informasi PC secara ilegal	Mencuri informasi yang merusak reputasi instansi	7	Penjaga hak akses lemah dan atau komputer tidak diberi <i>password</i>	3	Memberikan <i>password</i> masing-masing PC pegawai dan memantau pergerakan yang dicurigakan dari CCTV	4	50	Low	
HW1 4		Kegagalan jaringan	Baik kinerja maupun kegiatan operasional terhambat	7	Kerusakan pada infrastruktur jaringan seperti <i>switch/hub, router, access point</i>	4	Pengecekan infrastruktur TI yang rusak	3	500	Very High	
HW1 5		Kegagalan jaringan	Baik kinerja maupun kegiatan operasional terhambat	6	Manipulasi konfigurasi jaringan	3	Pengecekan infrastruktur TI yang rusak	3	54	Low	
HW1 6		Kerusakan perangkat jaringan	Baik kinerja maupun kegiatan operasional terhambat	7	Bencana alam (<i>force of nature</i>) dan atau hewan	1	Pengecekan infrastruktur TI yang rusak	3	21	Low	
HW1 7		Hilangnya komponen perangkat jaringan	Baik kinerja maupun kegiatan operasional terhambat	7	Pencurian	2	Pengawasan dan pemantauan akses ruangan serta keberadaan CCTV	2	28	Low	
HW1 8		Kerusakan <i>printer/scanner</i>	Tidak dapat mencetak dan melakukan <i>scan</i> data	6	<i>Maintenance</i> dan control yang tidak rutin	3	Pengecekan infrastruktur TI yang rusak	3	54	Low	
SW0 1	<i>Software</i>	Sistem	Kegagalan sistem	Baik pelayanan ataupun kegiatan operasional terhambat/terhenti	9	Sistem masih terdapat <i>error</i>	7	<i>Maintenance</i> sistem dilakukan oleh pusat	8	504	Very High
SW0 2		Antivirus, SO, Ms. Office	Kegagalan <i>software</i>	Baik pelayanan ataupun kegiatan operasional terhambat/terhenti	6	Lisensi <i>software</i> yang digunakan sudah melebihi batas waktu	4	Pengecekan infrastruktur TI yang rusak	3	72	Low
SW0 3		Serangan <i>virus</i>	Baik kinerja maupun kegiatan operasional terhambat	1	Antivirus tidak mampu mendeteksi dan mencegah <i>virus</i> yang masuk	5	Melakukan <i>update</i> antivirus	4	20	Low	
PP01	<i>People</i>	Admin, user, dan masyarakat	Kegagalan manusia (<i>human failure</i>)	Profesionalitas kinerja	6	Kesalahan dalam penginputan data dan penggunaan perangkat sistem	4	Pelatihan sekali dalam setahun dan adanya SOP	4	96	Moderate
P P0 2		Kegagalan manusia (<i>human failure</i>)	Pelayanan terhadap pengunjung rumah sakit tidak maksimal	6	SDM kurang kompeten	3	Pelatihan sekali dalam setahun	6	108	Moderate	



1. Urut-urutan mengurutkan atau seurutkan karya tulis ini tanpa mencantumkan dan menyederukan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

P			Pemalsuan atau penyalahgunaan hak akses	Reputasi internal	8	Terdapat kerjasama dengan pihak luar untuk pemalsuan tanda tangan yang tercatat pada sistem	1	Tidak adanya hak akses edit ataupun hapus dalam Tingkat provinsi	8	64	Low
P03											
DA01	Data	Data	Penuhnya kapasitas	Tidak dapat menyimpan data	8	Kurangnya pengontrolan kapasitas memori <i>server</i> dan <i>storage</i> yang telah terpakai	2	Pengecekan terhadap infrastruktur TI	3	48	Low
DA02			Tersebar nya informasi	Kerahasiaan data	5	Penyebaran informasi rahasia oleh pegawai (berbagi <i>password</i>)	2	Adanya aliran data (bertingkat) dalam akses data	7	70	Low
DA03			Pembobolan data/informasi	Kerahasiaan data	9	Kegagalan <i>software</i> , jaringan	1	Adanya aliran data (bertingkat) dalam akses data	1	9	Very Low
DA04			Tidak coocknya data pada system dengan data fisik	Integritas data	4	Kesalahan operator/pegawai yang meng- <i>input</i> data	1	Validasi dan verifikasi dokumen	2	8	Very Low
DA05			Data hilang	Integritas dan ketersediaan data	7	Kegagalan <i>software</i> , jaringan	4	Pengecekan terhadap infrastruktur TI	3	84	Moderate
DA06			<i>Cybercrime (hacker attack)</i>	Kerahasiaan, integritas, ataupun ketersediaan data terancam	6	Kurangnya keamanan pada system (<i>firewall</i>)	6	Penggunaan VPN sebagai proteksi jaringan	5	180	High
NT01	Network	Internet, intranet	Koneksi jaringan putus	Sistem tidak dapat diakses	8	Kegagalan jaringan	5	Pengecekan infrastruktur TI yang rusak	3	120	High
NT02			Koneksi jaringan putus	Sistem tidak dapat diakses	8	Rusaknya perangkat jaringan dan atau mati lampu	5	Pengecekan infrastruktur TI yang rusak	3	120	High
NT03			Konektifitas jaringan menurun	System <i>error</i> , <i>backup failure</i> , <i>data corrupt</i>	7	Kegagalan jaringan	4	Pengecekan infrastruktur TI yang rusak	3	84	Moderate
NT04			Adanya kesalahan peng-alamatan IP	Tidak ada koneksi jaringan	8	<i>Human error</i>	2	Pengecekan infrastruktur TI yang rusak	3	48	Low

Setelah dilakukan perhitungan, terdapat 34 risiko yang terdapat pada sistem informasi yang digunakan. Dari 34 RPN yang dihasilkan terdapat 5 kategori *level* RPN yaitu 2 kategori *very high* dengan rentang 500-504, 5 kategori *high* dengan rentang 120-180, 6 kategori *moderate* dengan rentang 84-108, 17 kategori *low* dengan rentang 20-72 dan 4 kategori *very low* dengan rentang 8-15.

IV. KESIMPULAN

Ada dasar yang kuat untuk meningkatkan kebijakan keamanan informasi setelah penemuan kerentanan sistem yang signifikan dan ancaman keamanan yang potensial. Kerentanan yang diidentifikasi harus diperbaiki dengan menerapkan kebijakan baru yang lebih ketat dan



menyeluruh, seperti pengaturan akses yang lebih ketat dan pembaruan sistem yang lebih rutin. Dengan menggunakan metode FMEA, penelitian ini berhasil mencapai tujuannya untuk mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan pada SIMRS Khanza sistem informasi yang digunakan RSUD Indah Bagan Batu. Penelitian ini menemukan 34 risiko pada SIMRS *Khanza* yang diidentifikasi berdasarkan hasil evaluasi melalui tahapan proses FMEA dan konsekuensi setiap lembar kuesioner berdasarkan tingkat keparahannya. Tahapan dalam penilaian risiko tersebut meliputi; alur proses bisnis, risiko *brainstorming*, penilaian tingkat *severity*, *occurrence*, dan *detection*, lalu ketiga tingkatan ini dikalikan maka menghasilkan *Risk Priority Number* (RPN). Dari 34 RPN yang dihasilkan terdapat 5 kategori *level* RPN yaitu dengan 2 kategori *level very high*, 5 kategori *level high*, 6 kategori *level moderate*, 17 kategori *level low* dan 4 kategori *level very low*. Dengan mengidentifikasi 34 risiko keamanan yang berpotensi terjadi ini, penelitian ini memberikan pemahaman yang lebih baik tentang ancaman yang dihadapi oleh sistem informasi RSUD Indah Bagan Batu. RSUD Indah Bagan Batu belum pernah melakukan analisis manajemen risiko sebelumnya. Oleh karena itu, penelitian ini adalah satu-satunya penelitian awal yang menerapkan manajemen risiko keamanan sistem informasi di RSUD Indah Bagan Batu. Penelitian ini akan membantu RSUD memperbaiki kesalahan yang mungkin terjadi dan meningkatkan kinerjanya secara keseluruhan. Karena jika tidak dilakukan manajemen risiko pada sistem informasi yang digunakan, masalah ini akan menjadi sangat serius yang akan mengakibatkan terhambatnya proses pelayanan pada rumah sakit karena segala model pelayan pada rumah sakit ada pada sistem informasi ini.

Untuk penelitian yang akan datang bisa dilakukannya mitigasi atau pengukuran risiko terhadap penerapan sistem informasi ini agar keamanan pada SIMRS *Khanza* semakin terjaga dan penerapan manajemen risiko ini dapat meminimalisir dampak kerugian baik bagi rumah sakit maupun pengunjung/*user*. Selain itu, penelitian ini memberikan dasar yang kokoh bagi RSUD Indah Bagan Batu untuk mengembangkan kebijakan dan praktik manajemen risiko sistem informasi yang lembaga. Praktik terbaik dalam manajemen risiko sistem informasi, seperti pengujian keamanan rutin dan pemantauan sistem yang teratur, sangat penting untuk memastikan bahwa RSUD Indah Bagan Batu dapat menemukan dan mengatasi ancaman keamanan dengan cepat dan efektif di masa depan.

REFERENSI

- [1] F. A. Anshori, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)".
- [2] M. P. Wibawa and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Policy Service PT. Asuransi Sinar Mas Menggunakan Framework COBIT 5," *JATISI J. Tek. Inform. Dan Sist. Inf.*, vol. 7, no. 3, pp. 466–479, Dec. 2020, doi: 10.35957/jatisi.v7i3.409.
- [3] M. M. Sine and E. Maria, "Analisis Manajemen Risiko pada Penerapan Sistem Informasi Pembangunan Daerah (SIPD) Menggunakan IEC/ISO 31010:2019," *Build. Inform. Technol. Sci. BITS*, vol. 4, no. 1, Jun. 2022, doi: 10.47065/bits.v4i1.1531.
- [4] M. S. Hardani and K. Ramli, "Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30," *JURIKOM J. Ris. Komput.*, vol. 9, no. 3, Art. no. 3, Jun. 2022, doi: 10.30865/jurikom.v9i3.4181.
- [5] K. P. Ningsih, U. Tunnisa, and N. Erviana, "Manajemen Resiko Redesign Sistem Penjajaran Rekam Medis dengan Metode Failure Mode and Effect Analysis (FMEA)," 2020.
- [6] B. A. Nugraha, A. R. Perdanakusuma, and A. Rachmadi, "Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 4, no. 1, Art. no. 1, Feb. 2020.
- [7] "A Fog-based Cyber Security Risk Management System using Bayesian Games," *Commun. Appl. Electron.*, vol. 7, no. 35, 2021.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

- [8] "IT Risk Management," School of Information Systems. Accessed: Jan. 28, 2024. [Online]. Available: <https://sis.binus.ac.id/2019/04/08/it-risk-management/>
- [9] T. Tutik, N. Mutiah, and I. Rusi, "ANALISIS DAN MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN KONTROL ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas)," *Coding J. Komput. Dan Apl.*, vol. 10, no. 02, pp. 249–261, Oct. 2022, doi: 10.26418/coding.v10i02.55082.
- [10] Y. Ramayani, "Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)," *INOVTEK Polbeng - Seri Inform.*, vol. 7, no. 2, p. 289, Nov. 2022, doi: 10.35314/isi.v7i2.2631.
- [11] P. Hanifah and J. S Suroso, "Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA," *J. Komput. Terap.*, vol. 6, no. 2, pp. 210–221, Nov. 2020, doi: 10.35143/jkt.v6i2.3728.
- [12] M. Megawati, O. Okfalisa, and M. Alkarim, "Security risk assessment of online fish quarantine information system using FMEA," presented at the PROCEEDINGS OF 8TH INTERNATIONAL CONFERENCE ON ADVANCED MATERIALS ENGINEERING & TECHNOLOGY (ICAMET 2020), Langkawi, Malaysia, 2021, p. 020098. doi: 10.1063/5.0053584.
- [13] M. S. A. Setiawan, E. M. Safitri, M. A. T. Taufiqurahman, and M. A. Pratama, "Analisis Manajemen Risiko Keamanan Sistem Informasi Rocketic.id menggunakan Metode OCTAVE dan FMEA," *JUSTIN J. Sist. Dan Teknol. Inf.*, vol. 11, no. 3, pp. 504–514, Jul. 2023, doi: 10.26418/justin.v11i3.66628.
- [14] K. Ganguly and G. Kumar, "Supply chain risk assessment: a fuzzy AHP approach," *Oper. Supply Chain Manag. Int. J.*, vol. 12, no. 1, pp. 1–13, 2019.
- [15] M. Firmansyah, M. Masrun, and I. D. K. Y. S, "ESENSI PERBEDAAN METODE KUALITATIF DAN KUANTITATIF," *Elastisitas J. Ekon. Pembang.*, vol. 3, no. 2, Art. no. 2, Sep. 2021.
- [16] R. Bisma, "Manajemen Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan," *JIEET J. Inf. Eng. Educ. Technol.*, vol. 6, no. 2, Art. no. 2, Dec. 2022, doi: 10.26740/jieet.v6n2.p73-79.
- [17] "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office | JATISI (Jurnal Teknik Informatika dan Sistem Informasi)," Dec. 2020, Accessed: Feb. 01, 2024. [Online]. Available: <https://jurnal.mdp.ac.id/index.php/jatisi/article/view/525>
- [18] E. Supristiowadi and Y. G. Sucahyo, "Manajemen Risiko Keamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan," *Indones. Treas. Rev. J. Perbendaharaan Keuang. Negara Dan Kebijakan. Publik*, vol. 3, no. 1, Art. no. 1, Mar. 2018, doi: 10.33105/itrev.v3i1.20.
- [19] C. Chazar, "STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005," 2015.
- [20] E. Bartolomé and P. Benítez, "Failure mode and effect analysis (FMEA) to improve collaborative project-based learning: Case study of a Study and Research Path in mechanical engineering," *Int. J. Mech. Eng. Educ.*, vol. 50, no. 2, pp. 291–325, Apr. 2022, doi: 10.1177/0306419021999046.
- [21] B. N. Siswanto, E. F. Lubis, F. Azka, and P. N. K. P. Maharani, "Analisis Risiko Operasional dengan Metode Failure Mode and Effect Analysis (FMEA) di Gudang PT Hade Bogatama Nusantara," *J. Manaj. Logist. DAN Transp.*, vol. 8, no. 3, Art. no. 3, Dec. 2022.
- [22] R. D. P. Suhandi and D. Pratami, "RACI Matrix Design for Managing Stakeholders in Project Case Study of PT. XYZ," *Int. J. Innov. Enterp. Syst.*, vol. 5, no. 02, Art. no. 02, Jul. 2021, doi: 10.25124/ijies.v5i02.134.

1. Uraian mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LAMPIRAN A

SERTIFIKAT TERAKREDITASI JURNAL

SERTIFIKAT

Direktorat Jenderal Penguatan Riset dan Pengembangan,
Kementerian Riset, Teknologi dan Pendidikan Tinggi




Kutipan dari Keputusan Direktur Jenderal Penguatan Riset dan Pengembangan
Kementerian Riset, Teknologi dan Pendidikan Tinggi Republik Indonesia
Nomor: 36/E/KPT/2019, 13 Desember 2019
Peringkat Akreditasi Jurnal Ilmiah Periode VII Tahun 2019
Nama Jurnal Ilmiah
Jurnal Inovtek Polbeng Seri Informatika
E-ISSN: 25279866
Penerbit: P3M Politeknik Negeri Bengkalis
Ditetapkan Sebagai Jurnal Ilmiah

TERAKREDITASI PERINGKAT 3

Akreditasi Berlaku Selama 5 (lima) Tahun, Yaitu
Volume 4 Nomor 2 Tahun 2019 sampai Volume 9 Nomor 1 Tahun 2024
Peringkat 3 Desember 2019

Direktur Jenderal Penguatan Riset dan Pengembangan



Muhammad Dimiyati
NIP. 195912171984021001








LAMPIRAN B

KUESIONER LEMBAR KERJA FMEA

Code	Process Function (Category)	Critical assets	Potential failure modes (process defects)	Potential effect(s) of failure	S E V	Potential cause(s) of failure	O C C	Current process controls	D E T
HW01	Hardware	server	Kebakaran server	Kegiatan operasional ataupun kinerja terhambat	9	Server mengalami Overheat	2	Melakukan pengecekan ruangan server setiap hari	2
HW02			Kebakaran server	Kerugian finansial	9	Hubungan arus pendek (power failure)	1	Melakukan pengecekan terhadap infrastruktur TI yang rusak	5
HW03			Server overheat	Kegiatan operasional ataupun kinerja terhambat	6	Tidak berfungsinya AC pada ruangan server	3	Melakukan pengecekan ruangan server setiap hari	2
HW04			Server down	Kegiatan operasional ataupun kinerja terhambat	5	Terlalu banyaknya unit yang mengakses server pada waktu bersamaan ataupun serangan DOS	3	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
HW05			Kerusakan server	Server tidak dapat digunakan	6	Tidak adanya proses controlling dan maintenance secara Rutin	5	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
HW06			Kerusakan server	Kerugian finansial	4	Bencana alam seperti runtuhan bangunan (server terletak di lantai bawah)	1	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
HW07		Komputer/ PC	Kerusakan komputer	Kegiatan operasional ataupun kinerja terhambat	7	Adanya serangan virus	3	Adanya antivirus setiap PC	4
HW08			Komputer tidak dapat digunakan	Kegiatan operasional ataupun kinerja terhambat	7	Kesalahan dalam konfigurasi Komputer	4	Melakukan pengecekan terhadap infrastruktur TI yang rusak	5
HW09			Komputer tidak dapat digunakan	Kegiatan operasional ataupun kinerja terhambat	7	Lisensi software yang digunakan sudah melebihi batas waktu	7	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
HW10			Komputer tidak dapat digunakan	Kerugian finansial	5	Bencana alam (kebakaran, banjir, petir)	1	Melakukan pengecekan terhadap infrastruktur TI yang rusak, mematikan perangkat sebelum pulang	3
HW11			Perangkat komputer out of dated	Kegiatan operasional ataupun kinerja terhambat	6	Usangnya teknologi yang digunakan	3	Monitoring perangkat sekali dalam setahun	4
HW12			Hilangnya komponen PC	Kerugian finansial	7	Pencurian	2	Pembatasan dan pengawasan hak akses ruangan, mengunci ruangan dan ada CCTV	2
HW13			Akses informasi PC secara ilegal	Mencuri informasi yang merusak reputasi instansi	7	Penjagaan hak akses lemah dan atau komputer tidak diberi password	3	Memberikan password masing-masing PC pegawai dan memantau pergerakan yang mencurigakan dari CCTV	4
HW14		Perangkat jaringan	Kegagalan jaringan	Kegiatan operasional ataupun kinerja terhambat	7	Kerusakan pada infrastruktur jaringan seperti switch/hub, router, access point.	4	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
HW15			Kegagalan jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Manipulasi konfigurasi jaringan	3	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
HW16			Kerusakan perangkat jaringan	Kegiatan operasional ataupun kinerja terhambat	7	Bencana alam (force of nature) dan atau hewan	1	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
HW17			Hilangnya komponen perangkat jaringan	Kegiatan operasional ataupun kinerja terhambat	7	Pencurian	2	Pembatasan dan pengawasan hak akses ruangan dan adanya CCTV	2
HW18		Printer/ scanner	Kerusakan printer/scanner	Tidak dapat mencetak dan melakukan scan data	6	Maintenance dan kontrol yang tidak rutin	3	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3

- Hak Cipta Dilindungi Undang-Undang**
- Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
 - Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



HW19			Kerusakan <i>printer/scanner</i>	<i>printer</i>	Tidak dapat mencetak dan scan data	6	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir (<i>force of nature</i>)	1	Melakukan pengecekan terhadap infrastruktur TI yang rusak, mematikan perangkat sebelum pulang	3
HW20			Hilangnya <i>printer/scanner</i>	<i>printer</i>	Kerugian finansial	8	Pencurian	2	Pembatasan dan pengawasan hak akses ruangan dan adanya CCTV	2
SW01	<i>Software</i>	sistem khanza	Kegagalan sistem		Kegiatan operasional ataupun pelayanan terhambat atau terhenti	9	Sistem masih terdapat <i>error</i>	7	<i>Maintenance</i> sistem dilakukan oleh pusat	8
SW02		Antivirus, SO, Ms.Office	Kegagalan <i>software</i>		Kegiatan operasional ataupun pelayanan terhambat atau terhenti	6	Lisensi <i>software</i> yang digunakan sudah melebihi batas waktu	4	Melakukan pengecekan infrastruktur TI yang rusak	13
SW03			Serangan <i>Virus</i>		Kegiatan operasional ataupun kinerja terhambat	1	Antivirus tidak mampu mendeteksi dan mencegah <i>virus</i> yang masuk	5	Melakukan <i>update</i> antivirus	4
PP01	<i>People</i>	user, pasien	Kegagalan manusia (<i>human failure</i>)		Profesionalitas kinerja	6	Kesalahan dalam penginputan data dan penggunaan perangkat sistem	4	Pelatihan sekali dalam setahun dan adanya SOP	4
PP02			Kegagalan manusia (<i>human failure</i>)		Pelayanan terhadap pengunjung tidak maksimal	6	SDM kurang kompeten	3	Pelatihan sekali dalam setahun	6
PP03			Pemalsuan atau penyalahgunaan hak akses		Reputasi <i>internal</i>	8	Adanya kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	1	Tidak adanya hak akses edit ataupun hapus dalam tingkat provinsi	8
DA01	Data	Data	Penuhnya kapasitas		Tidak dapat menyimpan data	8	Kurangnya pengontrolan kapasitas memori <i>server</i> dan <i>storage</i> yang telah terpakai	2	Melakukan pengecekan terhadap infrastruktur TI	3
DA02			Tersebarnya informasi rahasia		Kerahasiaan data	5	Penyalahgunaan hak akses	2	Adanya aliran data (beringkat) dalam akses data	7
DA03			Pembobolan data/informasi		Kerahasiaan data	9	Penyebaran informasi rahasia oleh pegawai (berbagi <i>password</i>)	1	Adanya aliran data (beringkat) dalam akses data	1
DA04			Tidak cocoknya data pada sistem dengan data fisik		Integritas data	4	Kesalahan operator/pegawai yang menginputkan data	1	Validasi dan verifikasi dokumen	2
DA05			Data hilang		Integritas dan ketersediaan data	7	Kegagalan <i>software</i> , jaringan	4	Melakukan pengecekan terhadap infrastruktur TI	3
DA06			<i>Cyber crime (hacker attack)</i>		Kerahasiaan, integritas ataupun ketersediaan data terancam	6	Kurangnya keamanan pada sistem (<i>firewall</i>)	6	Penggunaan VPN sebagai proteksi jaringan	5
NT01	<i>Network</i>	<i>Internet, intranet</i>	Koneksi jaringan putus		Sistem tidak dapat diakses	8	Kegagalan jaringan	5	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
NT02			Koneksi jaringan putus		Sistem tidak dapat diakses	8	Rusaknya perangkat jaringan dan atau mati lampu	5	Melakukan pengecekan terhadap infrastruktur TI yang rusak, menunggu lampu hidup kembali	3
NT03			Konektifitas jaringan menurun		Sistem <i>error, backup failure, data corrupt</i>	7	Kegagalan jaringan	4	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3
NT04			Adanya kesalahan pengalamatan IP		Tidak ada koneksi jaringan	8	<i>Human error</i>	2	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.

LAMPIRAN C

DOKUMENTASI KEGIATAN



© Hak c

arif Kasim Riau

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



Sultan Syarif Kasim Riau

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.



DAFTAR RIWAYAT HIDUP

Nama lengkap penulis Setia Ningsih Saputri lahir pada tanggal 10 Oktober 2001 di Harapan Jaya, Kabupaten Rokan Hilir, Provinsi Riau. Penulis adalah anak dari Bapak Iwan Munthe dan Ibu Irawati, yang merupakan anak pertama dari tiga bersaudara. Penulis bertempat tinggal di Jalan Harapan Jaya, Kecamatan Bagan Sinembah Raya, Kabupaten Rokan Hilir, Provinsi Riau. Penulis menempuh pendidikan dimulai dari SD N 037 Boltrem Jaya sampai tahun 2013, selanjutnya penulis meneruskan pendidikannya di SMP N 9 Salean pada tahun 2013 sampai 2016. Setamatnya Sekolah Menengah Pertama, penulis melanjutkan pendidikan di SMA N 3 Bagan Sinembah Raya dengan jurusan Ilmu Pengetahuan Alam di bangku sekolah, dan penulis melanjutkan pendidikan Strata Satu (S1) di Universitas Islam Negeri Sultan Syarif Kasim Riau pada Fakultas Sains dan Teknologi tepatnya pada Program Studi Sistem Informasi tahun 2019. Selama perkuliahan penulis aktif dalam mengikuti berbagai seminar-seminar yang diadakan dikampus maupun diluar kampus. Penulis juga pernah mengikuti Kuliah Kerja Nyata di Desa Buana Bhakti, Kecamatan Kerinci Kanan pada tahun 2022. Pada penelitian Tugas Akhir ini, penulis mengambil topik Manajemen Risiko dengan judul penelitian Tugas Akhir “Penggunaan Metode FMEA dalam Penilaian Manajemen Risiko Keamanan Sistem Informasi Rumah Sakit”.

Hak Cipta Dilindungi Undang-Undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar UIN Suska Riau.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin UIN Suska Riau.