TUGAS AKHIR – KS09 1336

PEMBUATAN STANDAR OPERASIONAL PROSEDUR KONTROL AKSES *PHYSICAL* DAN *LOGICAL* PADA APLIKASI SISTEM INFORMASI RUMAH SAKIT (SIMRS) MENGGUNAKAN KERANGKA KERJA OCTAVE, FMEA DAN KONTROL ISO 27002:2013 (STUDI KASUS: INSTALASI PENGELOLA DATA ELEKTRONIK RUMAH SAKIT DOKTER MOEWARDI)

NIMAS NAWANGSIH
NRP 5213 100 100

Dosen Pembimbing:
Dr. Apol Pribadi S., S.T, M.T
Eko Wahyu Tyas D, S.Kom, MBA

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS09 1336

DEVELOPING STANDARD OPERATING PROCEDURE TO CONTROL PHYSICAL AND LOGICAL ACCESS FOR INFORMATION SYSTEM HOSPITAL APPLICATION (SIMRS) USING FRAMEWORK OF OCTAVE, FMEA AND CONTROL OF ISO 27002:2013 (STUDY CASE: ELECTRONIC DATA MANAGEMENT INSTALLATION OF DOKTER MOEWARDI HOSPITAL)

NIMAS NAWANGSIH
NRP 5213 100 100

Supervisor:
Dr. Apol Pribadi S., S.T, M.T
Eko Wahyu Tyas D, S.Kom, MBA

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Sepuluh Nopember Institute of Technology
Surabaya 2017

TUGAS AKHIR – KS 091336

PEMBUATAN STANDAR OPERASIONAL PROSEDUR KONTROL AKSES *PHYSICAL* DAN *LOGICAL* PADA APLIKASI SISTEM INFORMASI RUMAH SAKIT (SIMRS) MENGGUNAKAN KERANGKA KERJA OCTAVE, FMEA DAN KONTROL ISO 27002:2013 (STUDI KASUS: INSTALASI PENGELOLA DATA ELEKTRONIK RUMAH SAKIT DOKTER MOEWARDI)

NIMAS NAWANGSIH
NRP 5213 100 100

Dosen Pembimbing:
Dr. Apol Pribadi S., S.T, M.T
Eko Wahyu Tyas D, S.Kom, MBA

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS 091336

DEVELOPING STANDARD OPERATING PROCEDURE TO CONTROL PHYSICAL AND LOGICAL ACCESS FOR INFORMATION SYSTEM HOSPITAL APPLICATION (SIMRS) USING FRAMEWORK OF OCTAVE, FMEA AND CONTROL OF ISO 27002:2013 (STUDY CASE: ELECTRONIC DATA MANAGEMENT INSTALLATION OF DOKTER MOEWARDI HOSPITAL)

NIMAS NAWANGSIH
NRP 5213 100 100

Supervisor:
Dr. Apol Pribadi S., S.T, M.T
Eko Wahyu Tyas D, S.Kom, MBA

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Sepuluh Nopember Institute of Technology
Surabaya 2017

PEMBUATAN STANDAR OPERASIONAL PROSEDUR KONTROL AKSES *PHYSICAL* DAN *LOGICAL* PADA APLIKASI SISTEM INFORMASI RUMAH SAKIT (SIMRS) MENGGUNAKAN KERANGKA KERJA OCTAVE, FMEA DAN KONTROL ISO 27002:2013 (STUDI KASUS: INSTALASI PENGELOLA DATA ELEKTRONIK RUMAH SAKIT DOKTER MOEWARDI)

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

NIMAS NAWANGSIH
Nrp. 5213 100 100

Surabaya, Juli 2017
Kepala Jurusan Sistem Informasi

Dr.Ir.Aris Tjahyanto, M.Kom
NIP.19660310 199102 1 001

PEMBUATAN STANDAR OPERASIONAL PROSEDUR KONTROL AKSES *PHYSICAL* DAN *LOGICAL* PADA APLIKASI SISTEM INFORMASI RUMAH SAKIT (SIMRS) MENGGUNAKAN KERANGKA KERJA OCTAVE, FMEA DAN KONTROL ISO 27002:2013 (STUDI KASUS: INSTALASI PENGELOLA DATA ELEKTRONIK RUMAH SAKIT DOKTER MOEWARDI)

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Oleh :

NIMAS NAWANGSIH
Nrp. 5213 100 100

Disetujui Tim Penguji : Tanggal Ujian : 10 Juli 2017
Periode Wisuda : September 2017

1. **Dr. Apol Pribadi S, S.T, M.T** **(Pembimbing I)**
2. **Eko Wahyu Tyas, S.Kom, MBA** **(Pembimbing II)**
3. **Feby Artwodini M., S.Kom., M.T** **(Penguji I)**
4. **Sholiq, S.T., M.Kom., M.SA** **(Penguji II)**

Pembuatan Standar Operasional Prosedur Kontrol Akses *Physical* dan *Logical* pada Aplikasi Sistem Informasi Rumah Sakit (SIMRS) Menggunakan Kerangka Kerja OCTAVE, FMEA dan Kontrol ISO 27002:2013 (Studi Kasus: Instalasi Pengelola Data Elektronik Rumah Sakit Dokter Moewardi)

Nama Mahasiswa : Nimas Nawangsih
NRP : 5213 100 100
Jurusan : SISTEM INFORMASI FTIF-ITS
Dosen Pembimbing 1 : Dr. Apol Pribadi S, S.T, M.T
Dosen Pembimbing 2 : Eko Wahyu Tyas, S.Kom, MBA

ABSTRAK

Dalam rangka mencegah akses tidak sah pada data pasien dan data keuangan, Intalasi Pengelola Data Elektronik di Rumah Sakit Dokter Moewardi memisahkan data yang bersifat kritis dan sensitif tersebut dari internet. Sehingga data-data tersebut hanya dapat diakses melalui fasilitas TI yang ada didalam gedung Rumah Sakit. Hal tersebut menimbulkan tantangan baru bagi IPDE sebagai pihak yang bertugas untuk menjaga dan mengelola keamanan informasi seluruh aspek kontrol akses pada Aplikasi SIMRS yang meliputi kontrol akses physical dan logical. Selama ini IPDE belum memiliki acuan yang baku berdasarkan standar tertentu dalam mengelola akses physical dan logical pada Aplikasi SIMRS. Hal tersebut menimbulkan celah keamanan pada sistem sekaligus menjadi kelemahan ketika akan dilakukan audit sistem. Dengan demikian salah satu bentuk dukungan untuk menyelesaikan permasalahan tersebut adalah dengan membuat SOP yang dibakukan berdasarkan standar, yang dapat digunakan sebagai acuan proses pengelolaan keamanan akses physical dan logical pada Aplikasi SIMRS.

Penyusunan Standar Operasional Prosedur (SOP) mengenai kontrol akses physical dan logical pada Aplikasi SIMRS ini dibuat berdasarkan pendekatan analisis risiko pada aset informasi yang terkait dengan Aplikasi SIMRS menggunakan kerangka kerja OCTAVE dan FMEA. SOP dibuat berdasarkan rekomendasi mitigasi risiko menggunakan acuan standar dari ISO27002:2013. Dari dokumen SOP yang telah dihasilkan dilakukan verifikasi dan validasi untuk memastikan dokumen SOP tersebut telah tepat dan sesuai dengan kebutuhan dari IPDE.

Tugas akhir ini menghasilkan dokumen Standar Operasional Prosedur (SOP) kontrol akses physical dan logical menggunakan kerangka kerja OCTAVE, FMEA dan kontrol pada standar ISO 27002:2013 yang terverifikasi dan valid sehingga dapat membantu IPDE dalam mengelola keamanan akses physical dan logical pada Aplikasi SIMRS.

Kata Kunci: Standard Operating Procedure, Logical and Physical Access Control, Risiko, Manajemen Risiko, ISO27002:2013, Kontrol Akses

Developing Standard Operating Procedure to Control Physical and Logical Access for Information System Hospital Application (SIMRS) Using Framework of OCTAVE, FMEA and Control of ISO 27002:2013 (Study Case: Electronic Data Management Installation Of Dokter Moewardi Hospital)

Name	**: Nimas Nawangsih**
NRP	**: 5210 100 100**
Majority	**: SISTEM INFORMASI FTIF-ITS**
Supervisor	**: Dr. Apol Pribadi S, S.T, M.T**
	Eko Wahyu Tyas, S.Kom, MBA

ABSTRACT

In order to prevent unauthorized access to patient data and financial data, the Electronic Data Management Installation at Doctor Moewardi Hospital separates that critical and sensitive data from the internet. So that datas can only be accessed through existing IT facility inside hospital building. This poses a new challenge for IPDE as the party in charge of safeguarding and managing information security to protect all aspects of access control on the SIMRS Application which includes logical and physical access control. So far IPDE does not have a standard reference based on certain standards in managing logical and physical access on the SIMRS Application. This creates a security weakness when the system audit will be done. Thus one form of support to solve the problem is to create a standard SOP based on the standards that can be used by IPDE as a reference process of security of physical and logical access to the SIMRS Application.

The preparation of Standard Operating Procedures (SOP) on logical and physical access controls on the SIMRS Application is based on a risk approach on information assets associated with the SIMRS Application using the framework of

OCTAVE and FMEA. SOPs are made based on risk mitigation recommendations using ISO 27002: 2013 standard reference. From SOP documents that have been generated verification and validation to ensure the SOP document has been appropriate and in accordance with the needs of the IPDE.

This final project produces documents Standard Operating Procedure (SOP) for physical and logical access control using framework of OCTAVE, FMEA and control on the standard ISO 27002: 2013, which verified and valid so that it can help IPDE manage physical and logical access security on SIMRS applications.

Key Word: Standard Operating Procedure, Logical and Physical Access Security, Risiko, Manajemen Risiko,, ISO27002:2013

KATA PENGANTAR

Syukur Alhamdulillah terucap atas segala petunjuk, pertolongan, kasih sayang dan kekuatan yang diberikan oleh Allah SWT. Hanya karena ridho-Nya, peneliti dapat menyelesaikan laporan Tugas Akhir, dengan judul ***Pembuatan Standar Operasional Prosedur Kontrol Akses Physical dan Logical pada Aplikasi Sistem Informasi Rumah Sakit (SIMRS) Menggunakan Kerangka Kerja OCTAVE, FMEA dan Kontrol ISO 27002:2013 (Studi Kasus: Instalasi Pengelola Data Elektronik Rumah Sakit Dokter Moewardi).*** Tugas akhir ini dibuat dalam rangka menyelesaikan gelar sarjana di Jurusan Sistem Informasi Fakultas Teknologi Informasi Institut Teknologi Sepuluh Nopember Surabaya

Terima kasih tiada henti terucap untuk seluruh pihak yang sangat luar biasa dalam membantu proses penelitian ini, yaitu:

- Ibu dan Bapak peneliti yang telah membantu memotivasi, meyakinkan, membiayai dan selalu mendoakan sehingga penelitian dapat terselesaikan.
- dr. Satrio Budi Susilo, Sp.PD, M.Kes, selaku Kepala IPDE atas kerjasama, bantuan dan fasilitas terbaik untuk kebutuhan penelitian.
- Dr. Apol Pribadi, S.T, M.T, selaku dosen pembimbing 1 atas segala bimbingan, ilmu serta motivasi yang sangat bermanfaat untuk penulis.
- Eko Wahyu Tyas D, S.Kom, MBA, selaku dosen pembimbing 2 atas segala ilmu dan pengertian yang sebesar-besarnya terhadap penulis.
- Mbak Dina, Mbak Dipta, Mas Poggy, Pak Aris dan seluruh staf IPDE yang telah membantu dalam proses penelitian.
- Kepada Bu Feby Artwodini M., S.Kom., M.T dan Bapak Sholiq, S.T., M.Kom., M.SA sebagai dosen penguji

peneliti, terima kasih atas kritikan dan masukan yang bersifat membangun untuk peningkatan kualitas penelitian ini.

- Mbak Niken, Mas Dadang dan Tiara, selaku saudara peneliti yang sangat banyak membantu memotivasi, memberikan semangat dan selalu menjadi pelipur lara serta tempat dalam berbagi tawa dan kesedihan
- Nance dan Fiandi, selaku sahabat dekat peneliti yang selalu menguatkan dalam perjuangan menyelesaikan penelitian.
- Pak Hermanto, selaku admin MSI yang sangat informatif.
- Hanun, Tami, Dina, Natascha, Dinar, Ranti, Nini, Mbak Sandra, Aisyah, Wayan, Umi, Unsa, Nurita dan Tayomi selaku kawan seperjuangan yang selalu
- Ibu Mahendrawati, selaku dosen wali yang selalu membimbing dan memberikan dukungan serta motivasi yang berarti bagi peneliti.
- Teman-teman Lab MSI dan Lab RDIB.
- Teman-teman Beltranis dan Click.

Penulis menyadari bahwa masih banyak kekurangan pada tugas akhir ini, maka penulis mohon maaf atas segala kekurangan dan kekeliruan yang ada di dalam tugas akhir ini. Penulis membuka pintu selebar-lebarnya bagi pihak-pihak yang ingin memberikan kritik dan saran bagi penulis untuk menyempurnakan tugas akhir ini. Semoga tugas akhir ini dapat bermanfaat bagi seluruh pembaca.

Surabaya, 19 Juli 2017

Peneliti

DAFTAR ISI

DAFTAR GAMBA

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini membahas mengenai hal-hal yang mendasar dari penelitian tugas akhir. Hal-hal mendasar tersebut antara lain latar belakang, rumusan permasalahan, batasan masalah, tujuan, manfaat, relevansi dan sistematika dari penelitian tugas akhir. Uraian di bawah diharapkan dapat memberikan pemahaman terhadap gambaran secara umum dari penelitian tugas akhir ini.

1.1 Latar Belakang

Rumah Sakit Umum Daerah (RSUD) Dokter Moewardi merupakan salah satu rumah sakit kelas A milik pemerintah di daerah Surakarta. Rumah Sakit kelas A adalah rumah sakit yang mempunyai fasilitas dan kemampuan pelayanan medik spesialistik luas dan subpesialistik luas, sehingga rumah sakit jenis ini ditetapkan sebagai tempat pelayanan rujukan tertinggi *(top referral hospital)* atau disebut juga rumah sakit pusat. Rumah Sakit Dokter Moewardi memiliki visi untuk menjadi Rumah Sakit terkemuka berkelas dunia. Salah satu cara untuk mewujudkan visi tersebut adalah dengan meningkatkan mutu pelayanan rumah sakit dengan standar internasional, baik untuk pelayanan medis maupun pelayanan pendukung. Komitmen ini ditunjukkan dengan terakreditasinya rumah sakit dengan standar internasional ISO 9001 dari tahun 2007 hingga 2016 tentang kualitas manajemen sistem.

Salah satu upaya non-medis yang dapat dilakukan untuk meningkatkan mutu pelayanan adalah dengan menerapkan teknologi informasi untuk meningkatkan kualitas pengolahan informasi dalam rangka memberikan kontribusi untuk perawatan pasien yang lebih baik. Sistem informasi yang baik dapat mendukung alur kerja klinis dengan berbagai cara yang akan memberikan kontribusi untuk perawatan pasien yang lebih baik. Sistem informasi mempunyai tiga peranan penting dalam mendukung proses pelayanan kesehatan, yaitu:

mendukung proses dan operasi pelayanan kesehatan, mendukung pengambilan keputusan staf dan manajamen serta mendukung berbagai strategi untuk keunggulan kompetitif [1]. Rumah Sakit Dokter Moewardi telah menerapkan Sistem Informasi Rumah Sakit berbasis teknologi yang berbentuk Aplikasi Sistem Informasi Rumah Sakit (SIMRS) yang didasarkan pada PERMENKES RI nomor 82 tahun 2013 tentang SIMRS dan PERMENKES nomor 97 tahun 2015 tentang Peta Jalan SIK. Dalam rangka memastikan kualitas Aplikasi Sistem Informasi Rumah Saki, Rumah Sakit Dokter Moewardi membentuk badan atau bagian bernama Instalasi Pengelola Data Elektronik (IPDE). IPDE bertugas untuk merencanakan, mengelola dan mengevaluasi Sistem Informasi Manajemen Rumah Sakit. IPDE terdiri dari lima sub bagian yaitu bagian jaringan, data, program, hardware dan administrasi.

Salah satu aspek yang harus dilindungi untuk menjaga kualitas Aplikasi SIMRS adalah dengan menjaga keamanan data atau informasi yang ada di dalam Aplikasi SIMRS terutama yang berhubungan dengan data atau informasi pasien [2]. Berdasarkan penelitian yang dilakukan oleh Menteri Kesehatan pada tahun 2013 menunjukkan bahwa ke 6 (enam) komponen implementasi sistem informasi kesehatan, yaitu kebijakan, infrastruktur, aplikasi, standar, tata kelola, dan pengamanan data sebagian sudah tersedia, tetapi masih banyak memerlukan upaya penguatan, terutama pada aspek keamanan data [3]. Tujuan pengelolaan keamanan data adalah menjaga kerahasiaan, ketersediaan, dan integritas informasi (termasuk keaslian, akuntabilitas dan auditabilitas) [4]. Tujuan ini menjadi krusial ketika berhadapan dengan data kesehatan, karena kegagalan dalam menjaga keamanan informasi dapat menyebabkan kerugian, yang terburuk adalah membahayakan kehidupan pasien atau terungkapnya data rahasia tentang pasien [5].

Salah satu faktor yang dapat merusak keamanan informasi adalah akses yang tidak sah pada informasi. Akses adalah salah satu aspek keamanan yang paling sering dieksploitasi karena merupakan pintu gerbang ke aset kritis [6]. Akses adalah proses yang dilakukan oleh subyek ke sumber informasi dengan mekanisme identifikasi, authentikasi dan otorisasi [7]. Menurut penelitian yang dilakukan oleh Komisi Informasi dan Privasi Ontario mengenai akses tidak sah ke informasi kesehatan pribadi yang didasarkan pada analisis lebih dari 63.000 laporan dari 95 negara menunjukkan bahwa hubungan antara karyawan internal dan penyalahgunaan hak akses adalah 15% penyebab akses tidak sah tersebut adalah dari aspek pelanggaran organisasi dan 85% lainya berasal dari pelanggaran yang melibatkan elektronik (Information and Privacy Commissioner of Ontario, 2015). Hal tersebut patut diwaspadai oleh IPDE sebagai pihak yang bertugas menjaga keamanan Aplikasi SIMRS untuk lebih memperkuat kontrol aksesnya.

Dalam rangka mencegah akses tidak sah pada data atau informasi penting, IPDE telah melakukan berbagai upaya, yang salah satunya adalah memisahkan data penting seperti data pasien dan data keuangan yang ada didalam Aplikasi SIMRS dari internet, sehingga hanya dapat diakses lewat jaringan lokal Rumah Sakit saja. Hal tersebut menimbulkan tantangan baru bagi IPDE sebagai pihak yang bertugas menjaga keamanan informasi, untuk melindungi seluruh aspek kontrol akses Aplikasi SIMRS yang hanya dapat diakses didalam gedung Rumah Sakit. Selain aspek kontrol *logical* yang harus dijaga keamanan aksesnya, kontrol akses *physical* juga perlu dipertimbangkan mengingat data penting hanya dapat diakses di dalam area gedung Rumah Sakit saja. Dengan adanya tantangan tersebut, keamanan akses harus dapat dikelola dengan baik sehingga dapat memperkecil risiko yang menyebabkan terganggunya proses bisnis.

Menurut ISO 27002, kontrol akses adalah bagian dari sistem manajemen keamanan informasi yang merupakan bagian terintegrasi dari sebuah proses organisasi dan keseluruhan manajemen keamanan informasi dalam menjaga kerahasiaan *(confidentiality)*, keutuhannya *(integrity)* dan ketersediaannya *(availability)* informasi yang mengaplikasikan proses manajemen risiko untuk memberikan kepercayaan bagi organisasi bahwa risiko telah dikelola dengan cukup baik. Dimana dalam hal ini, akses merupakan gerbang utama menuju aset kritis. Akses yang tidak sah pada sebuah dapat dapat merusak keamanan data tersebut. Sehingga dalam menginisiasi sebuah keamanan informasi, perlu bagi sebuah organisasi untuk memastikan kontrol akses untuk menjaga keamanan data atau informasi. Pengelolaan risiko pada ketiga aspek keamanan informasi membutuhkan adanya sebuah kontrol dan aksi mitigasi terhadap risiko tesebut. Kontrol mitigasi pada risiko dapat dilakukan dengan membuat sebuah prosedur yang baik untuk memastikan tidak adanya risiko yang berulang kembali dan dapat menyebabkan terganggunya proses bisnis yang berjalan.

Dengan demikian, salah satu bentuk dukungan dalam menjaga kontrol akses yang dapat diimplementasikan pada Aplikasi Sistem Informasi Rumah Sakit milik RS Dokter Moewardi adalah dengan membuat sebuah prosedur yang terdokumentasi dengan baik dalam bentuk sebuah dokumen SOP *(Standard Operating Procedure)* mengenai kontrol akses agar risiko dari keamanan informasi dapat dikurangi atau dihindari. SOP berguna dalam mendefinisikan seluruh konsep, teknik, dan persyaratan dalam melakukan suatu proses yang dituliskan ke dalam suatu bentuk yang langsung dapat digunakan oleh pegawai yang bersangkutan dalam melaksanakan tugas proses bisnisnya. Selain itu, SOP juga berguna untuk mendefinisikan seluruh konsep, teknik dan persyaratan dalam melakukan suatu proses yang dituangkan ke dalam suatu bentuk yang lansung dapat digunakan oleh pegawai dalam melaksanakan proses bisnisnya. Suatu SOP juga sangat diperlukan untuk

menghilangkan variasi dalam penerapan kerja [8]. Dalam proses pendefinisian SOP diperlukan adanya standar yang nantinya akan menjadi acuann. Standar tersebut akan digunakan sebagai penentu kontrol apa saja yang harus ada dalam penyusunan dokumen SOP[8].

Pada penelitian ini SOP didasarkan pada pendekatan analisis risiko aset informasi yang terkait dengan Aplikasi SIMRS menggunakan kerangka kerja OCTAVE dan FMEA. Kemudian setiap risiko yang berhubungan dengan akses *physical* dan *logical* akan ditentukan aksi mitigasinya sesuai dengan acuan yang ada pada standar ISO 27002:2013. Hal tersebut menjadi masukan untuk pembuatan SOP kontrol akses *physical* dan *logical* pada Aplikasi SIMRS yang kemudian akan diverifikasi dan divalidasi untuk memastikan bahwa SOP telah sesuai dengan anjuran standar pada ISO 27002:2013 dan sesuai dengan kebutuhan IPDE sehingga dapat digunakan sebagai acuan dalam mengendalikan akses *physical* dan *logical* pada Aplikasi SIMRS.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang di atas, rumusan masalah yang menjadi fokus utama dalam tugas akhir ini adalah:

1. Apa hasil analisis risiko akses *physical* dan *logical* berdasarkan aset infromasi yang terkait dengan Aplikasi SIMRS di Rumah Sakit Dokter Moewardi ?
2. Bagaimana hasil pembuatan dokumen SOP kontrol akses *physical* dan *logical* pada Aplikasi SIMRS di Rumah Sakit Dokter Moewardi berdasarkan mitigasi risiko untuk pihak Instalasi Pengelola Data Elektronik?
3. Bagaimana hasil verifikasi dan validasi dokumen SOP kontrol akses *physical* dan *logical* pada Aplikasi SIMRS di Rumah Sakit Dokter Moewardi?

1.3 Batasan Masalah

Dari permasalahan yang disebutkan di atas, batasan masalah dalam tugas akhir ini adalah:

1. Penelitian ini bertujuan untuk menghasilkan dokumen tata kelola TI berupa kebijakan, prosedur, formulir dan instruksi kerja
2. Pembuatan SOP ditujukan kepada bagian Instalasi Pengelola Data Elektronik sebagai pihak penyedia layanan Aplikasi SIMRS
3. Justifikasi analisis risiko berdasarkan hasil wawancara dan diskusi dengan Kepala IPDE.
4. Kontrol akses untuk aspek *logical* menggunakan acuan klausul 9 *Access control* pada ISO 27002:2013.
5. Kontrol akses untuk aspek *physical* menggunakan acuan 11.1.1 *Physical security perimeter*, 11.1.2 *Physical entry controls*, 11.1.3 *Securing offices*, *rooms and facilities*, *11.1.5 Working in secure area*, 11.2.1 *Equipment siting and protection*, 11.2.3 *Cabling security,* 11.2.8 *Unattended user equipment* dan 11.2.9 *Clear desk and clear screen policy* pada ISO 27002:2013.

1.4 Tujuan

Dari rumusan masalah yang disebutkan sebelumnya, tujuan yang akan dicapai melalui tugas akhir ini adalah:

1. Mengetahui hasil analisis risiko akses *physical* dan *logical* pada Aplikasi SIMRS di Rumah Sakit Dokter Moewardi berdasarkan aset informasi yang terkait.
2. Mengetahui hasil pembuatan dokumen SOP kontrol akses *physical* dan *logical* pada Aplikasi SIMRS di Rumah Sakit Dokter Moewardi berdasarkan mitigasi risiko untuk pihak Instalasi Pengelola Data Elektronik.
3. Mengetahui hasil verifikasi dan validasi dokumen SOP kontrol akses *physical* dan *logical* Aplikasi SIMRS di Rumah Sakit Dokter Moewardi.

1.5 Manfaat

Melalui tugas akhir ini diharapkan dapat memberi manfaat yaitu:

A. Bagi pihak Instalasi Pengelola Data Elektronik (IPDE) Rumah Sakit Dokter Moewardi
    1. IPDE mengetahui hasil analisis risiko akses *physical* dan *logical* berdasarkan aset informasi yang terkait dengan Aplikasi SIMRS.
    2. Pihak IPDE memiliki dokumen SOP (*Standard Operating Procedure*) kontrol akses *physical* dan *logical* pada Aplikasi SIMRS berdasarkan hasil mitigasi risiko yang dapat digunakan sebagai acuan dalam mengamankan akses ke Aplikasi SIMRS.
    3. Pihak IPDE memiliki dokumen SOP keamanan akses Aplikasi SIMRS berdasarkan kontrol akses *physical* dan *logical* yang mengacu kontrol ISO/IEC 27002:2013 yang telah terverifikasi dan tervalidasi.

B. Bagi Akademis
    1. Memberikan kontribusi mengenai implementasi penggunaan kerangka kerja OCTAVE, FMEA dan standar ISO 27002 dalam pembuatan sebuah standar operasional prosedur.
    2. Memberikan kontribusi mengenai penyusunan dokumen SOP yang meliputi aspek akses *physical* sekaligus *logical* untuk suatu aplikasi.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibagi menjadi tujuh bab, yakni:

BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat, relevansi dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA
Bab ini menjelaskan penelitian terdahulu yang memiliki topik yang berkaitan dengan penelitian tugas akhir ini, definisi serta penjelasan dasar teori yang dijadikan referensi dalam pembuatan tugas akhir.

BAB III METODOLOGI
Bab ini menggambarkan urutan dan uraian pengerjaan penelitian tugas akhir. Bab ini secara terperinci menjelaskan bagaimana proses peneliti dalam membuat SOP.

BAB IV PERANCANGAN
Bab ini menjelaskan perancangan perangkat yang dilakukan oleh peneliti. Perancangan dibuat untuk menjelaskan dengan detail setiap tahapan pengerjaan penelitian tugas akhir yang telah dijelaskan pada BAB III.

BAB V IMPLEMENTASI
Bab ini menjelaskan hasil yang didapatkan dari proses pengumpulan data, yakni identifikasi aset kritis, kebutuhan keamanan, ancaman, praktik keamanan yang telah dilakukan dan kerentanan. Bab ini jugas menjelaskan mengenai penyusunan *risk register* (identifikasi risiko) dan perlakuan risiko, yakni pemetaan risiko dengan kontrol pada standar dan hasil rekomendasi mitigasi.

BAB VI HASIL DAN PEMBAHASAN
Bab ini menjelaskan tahap penyusunan SOP yang dihasilkan. Bab ini menjelaskan kebijakan, prosedur dan formulir yang dihasilkan serta hasil verifikasi dan validasi SOP.

BAB VII PENUTUP
Bab ini berisi tentang kesimpulan dari keseluruhan pengerjaan tugas akhir dan saran maupun rekomendasi terhadap penelitian tugas akhir ini untuk perbaikan ataupun penelitian lanjutan yang memiliki kesamaan dengan topik yang diangkat pada tugas akhir ini.

BAB II
TINJAUAN PUSTAKA

Pada bab ini dijelaskan mengenai penelitian sebelumnya dan dasar teori apa saja yang digunakan dalam penelitian tugas akhir.

2.1 Penelitian Sebelumnya

Tabel 2. 1 Penelitian Sebelumnya

Judul Penelitian: Pembuatan Dokumen SOP *(Standard Operating Procedure)* Keamanan Data yang Mengacu Pada Kontrol Kerangka Kerja COBIT 5 dan ISO27002:2013 (Studi Kasus : STIE Perbanas)	
Nama Peneliti	Aulia Nur Fatimah
Tahun Penelitian	2016
Hasil Penelitian	Penelitian ini menghasilkan dokumen kebijakan, SOP, instruksi kerja dan formulir. Penelitian ini menghasilkan SOP dengan menggunakan pendekatan analisis risiko berbasis aset untuk menggali kebutuhan keamanan data pada studi kasus. Dalam menganalisis risiko, peneliti menggunakan metode OCTAVE dan FMEA, sedangkan penilaian risiko didasarkan pada pendekatan *risk assessment* dan *risk treatment* ISO27001:2013. SOP dibuat berdasarkan hasil mitigasi risiko, dimana sebelumnya risiko dipetakan terlebih dahulu dengan kontrol pada standar yang digunakan.
Hubungan Penelitian dengan Tugas Akhir	Pembuatan SOP pada penelitian ini juga menggunakan pendekatan analisis risiko berbasis aset. Metode untuk identifikasi risiko sama, yaitu dengan menggunakan pendekatan metode OCTAVE. Penelitian ini juga membuat SOP yang didasarkan pada hasil mitigasi risiko, dimana sebelumya risiko dipetakan terlebih dahulu dengan kebutuhan kontrol pada standar. Secara umum metodologi penelitian yang akan

	dilakukan sama dengan metode penelitian ini dari tahap penggalian data hingga validasi SOP.
Judul Penelitian: : Pembuatan Standar Operasional Prosedur (SOP) Manajemen Akses Untuk Aplikasi E-Performance Bina Program Kota Surabaya Berdasarkan Kerangka Kerja ITIL V3 Dan ISO 27002	
Nama Peneliti	Wildan Radista Wicaksana
Tahun Penelitian	2016
Hasil Penelitian	Penelitian ini membuat SOP berdasarkan pendekatan analisis kesenjangan antara proses manajemen akses yang ada dengan kerangka kerja dan standar yang digunakan. Objek pada penelitian ini adalah manajemen akses pada Aplikasi E-Performance Bina Surabaya Kota Surabaya.
Hubungan Penelitian dengan Tugas Akhir	Penelitian ini dengan penelitian yang akan dilakukan memiliki objek penelitian yang sama yaitu akses pada suatu aplikasi dan menggunakan standar yang sama yaitu ISO 27002, sehingga secara umum kemungkinan SOP untuk kontrol akses *logical* yang akan dihasilkan memiliki kemiripan dengan SOP yang dihasilkan pada penelitian ini.
Judul Penelitian: : Pembuatan Standar Operating Procedure Keamanan Aset Informasi Berdasarkan Kendali Akses Dengan Menggunakan ISO/IEC:27002:2013 Pada Studi Kasus STIE Perbanas Surabaya.	
Nama Peneliti	Ardhana Yudi Saputra
Tahun Penelitian	2016
Hasil Penelitian	Penelitian ini menghasilkan dokumen kebijakan, SOP dan formulir yang berhubungan dengan kendali akses. Penmelitian ini membuat SOP dengan pendekatan analisis risiko berbasis aset. etode analisis risiko yang digunakan adalah OCTAVE dan FMEA. Penelitian ini terlebih dahulu mengidentifikasi kebutuhan keamanan infromasi pada studi kasus, kemudian barulah menggali risiko yang berkaitan dengan kendali akses.

Hubungan Penelitian dengan Tugas Akhir	Penelitian yang akan dilakukan merupakan perluasan lingkup dari penelitian ini. Dimana tidak hanya aspek kontrol akses *logical* saja, namun juga mempertimbangkan aspek *hardware* pada kontrol akses *physical* . Metode identifikasi risiko sama, yaitu menjalankan OCTAVE untuk mendapatkan kebutuhan keamanan dan ancaman yang ada pada studi kasus, kemudia berdasarkan kedua aspek tersebut barulah risiko-risiko terkait kendali akses digali.

2.2 Dasar Teori

Berikut merupakan dasar teori yang digunakan pada penelitian.

2.2.1 Aplikasi Sistem Informasi Rumah Sakit (SIMRS) Rumah Sakit Dokter Moewardi

Sistem Informasi Manajemen Rumah Sakit yang selanjutnya disingkat SIMRS adalah suatu sistem teknologi informasi komunikasi yang memproses dan mengintegrasikan seluruh alur proses pelayanan Rumah Sakit dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk memperoleh informasi secara tepat dan akurat, dan merupakan bagian dari Sistem Informasi Kesehatan [3].

Sistem informasi mempunyai 3 peranan penting dalam mendukung proses pelayanan kesehatan, yaitu:

- Mendukung proses dan operasi pelayanan kesehatan
- Mendukung pengambilan keputusan staf dan manajamen
- Mendukung berbagai strategi untuk keunggulan kompetitif [1].

Secara umum Aplikasi Sistem Informasi Rumah Sakit atau SIMRS pada Rumah Sakit Dokter Moewardi terdiri atas 10

Menu/modul utama, yaitu *Admission*, Transaksi, Farmasi, *Billing*, Penagihan, Jasa Pelayanan, *Inventory*, Rekam Medis, Information Eksekutif dan *Utility*.
Aplikasi SIMRS ini merupakan aplikasi untuk melayani pasien secara paripurna. Layanan pada aplikasi ini mulai dari pembayaran ke kasir oleh pasien, hasil diagnosa penyakit (rekam medik) hingga resep yang terhubung dengan bagian farmasi. Aplikasi ini memiliki tiga kategori user utama yaitu:

- Pegawai RS Dokter Moewardi
- Dokter spesialis
- Residen

Tujuan penting dari Aplikasi SIMRS adalah pertukaran data elektronik antar penyedia layanan kesehatan (dokter praktik, fasilitas primer dan rumah sakit) sehingga dapat menjamin ketersediaan informasi pasien secara komprehensif dan efisiensi pelayanan. Informasi pasien yang lengkap dapat membantu proses pelayanan pasien secara lebih baik [3]. Aplikasi SIMRS pada RS Dokter Moewardi dikembangkan oleh pihak ke-3 dan dikelola oleh Instalasi Pengelolaan Data Elektronik. Aplikasi ini terhubung dengan jaringan LAN pada gedung RS yang bertujuan untuk memitigasi kemungkinan kebocoran data yang disebabkan oleh internet mengingat data yang disimpan dan diolah oleh Aplikasi SIMRS adalah data sensitif yang berhubungan dengan data pasien, data keuangan dan data inventory milik gudang dan farmasi.

2.2.2 Aset Teknologi Informasi

Kata aset menurut Kamus Besar Bahasa Indonesia (KBBI) adalah sesuatu yang mempunyai nilai tukar, modal atau kekayaan. Istilah aset informasi mengacu pada elemen data aktual, catatan, file, sistem perangkat lunak, dan sebagainya. Sedangkan istiah aset TI mengacu pada sekumpulan aset yang lebih luas termasuk perangkat keras, media, elemen-elemen komunikasi, dan lingkungan TI yang sebenarnya dari perusahaan. Istiah umum asetmengacu pada baik aset informasi maupun aset TI [9]. Menurut penelitian sistem

informasi yang dilakukan oleh Jeanne Ross, Cynthia Mathis, dan Dale Goodhue ditemukan bahwa ada tiga jenis aset TI yang terpenting. Penemuan tersebut dinamakan dengan istilah *"The Three IT Assets",* yang mana ketiga aset tersebut adalah Sumber Daya Manusia, Teknologi, dan Relasi [10]. Relasi yang dimaksud adalah manajemen risiko dan tanggungjawab aset IT.

Pada penelitian ini akan definisi aset akan difokuskan pada Sumber Daya Manusia dan aset teknologi. Aset Sumber Daya Manusia yang dimaksudkan adalah seluruh pengguna Aplikasi SIMRS, sedangkan aset teknologi adalah seluruh infrastruktur teknologi informasi pendukung Aplikasi SIMRS, yaitu *hardware*, jaringan, dan data yang tersimpan serta tersistem secara terpusat di *server* Rumah Sakit.

2.2.3 Keamanan Informasi

Menurut ISO/IEC 27001:2005 tentang *information security management system* bahwa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis. Keamanan Informasi memiliki 3 aspek, aspek tersebut biasa disebut dengan *CIA Triad Model* yaitu:

- *Confidentiality* (kerahasiaan). Merupakan aspek yang menjamin bahwa informasi tidak diungkapkan kepada individu, program, atau proses yang tidak berhak. Beberapa informasi lebih sensitif dibandingkan informasi lainnya dan membutuhkan tingkat jaminan kerahasiaan yang lebih tinggi, sehingga mekanisme kontrol perlu berada di tempat yang tepat untuk mengatur siapa saja yang dapat mengakses suatu data dan aktifitas apa yang boleh dilakukan pada data [7].
- *Integrity* (integritas). Merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi.

Integritas adalah proses memastikan bahwa modifikasi pada data tidak dibuat oleh personel atau proses yang tidak sah dan menjaga konsistensi data secara internal dan eksternal, yaitu bahwa informasi internal konsisten di antara semua subentities dan bahwa informasi internal konsisten dengan dunia nyata atau situasi eksternal [6].

- *Availability* (ketersediaan). Merupakan aspek yang menjamin bahwa data akan tersedia saat dibutuhkan kapanpun dan dimanapun, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait [6].

Pada penelitian ini ketiga aspek keamanan informasi tersebut akan digunakan untuk penggalian kebutuhan keamanan dari objek penelitian yaitu Aplikasi Sistem Informasi Rumah Sakit (SIMRS), karena kontrol akses berfungsi untuk menjaga atau melindungi ketiga aspek keamanan informasi tersebut.

2.2.4 Kontrol Akses

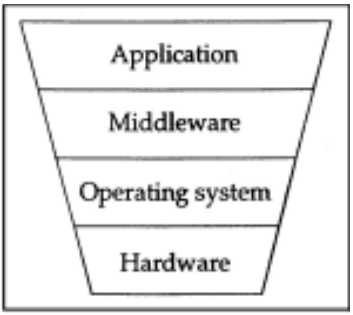
Dalam teknologi informasi, akses adalah aliran informasi antara subjek dan objek. Sebuah subjek merupakan entitas aktif yang meminta akses ke suatu objek atau data dalam suatu objek. Sebuah subjek dapat berupa pengguna, program, atau proses yang mengakses objek untuk menyelesaikan tugas. Sementara objek adalah entitas pasif yang berisi informasi atau fungsi yang dibutuhkan, yang dapat berupa komputer, database ataupun file program komputer [7].

Sedangkan Kontrol Akses sendiri adalah fitur keamanan informasi yang mengontrol bagaimana pengguna dan sistem berkomunikasi dan berinteraksi dengan sistem dan sumber daya lainnya. Fitur keamanan infromasi tersebut melindungi sistem dan sumber daya dari akses yang tidak sah dan dapat menjadi komponen yang ikut menentukan tingkat otorisasi setelah prosedur otentikasi telah berhasil diselesaikan [7]. Proses tersebut memberikan atau menyangkal permintaan khusus untuk memperoleh dan menggunakan informasi serta layanan pemrosesan informasi atau sumber daya untuk

memasukkan fasilitas fisik tertentu, seperti bangunan atau ditunjuk sumber ruangan yang berisi informasi. Mendampingi proses prosedur yang memantau akses. Tujuan dari kontrol akses adalah untuk mencegah akses tidak sah ke sistem TI [11]. Pengertian lain menyebutkan bahwa Kontrol Akses merupakan sebuah pusat kendali yang berfungsi untuk mengontrol pengguna (Orang, proses, mesin, dll) yang memiliki akses terhadap sumber daya yang ada di dalam sistem yang mana akses tersebut bias digunakan untuk membaca, memprogram dan kemudian dilakukan eksekusi, dan juga dapat berbagi data dengan pengguna yang lain [12].

2.2.4.1 Level Kontrol Akses

Menurut Ross Anderson, terdapat empat level kontrol akses dalam sebuah sistem [12]. Keempat level tresebut ditunjukkan dalam Gambar 2.1 dibawah, berikut deskripsi dari masing-masing level tersebut.



Gambar 2. 1 Level Kontrol Pada Sistem [12]

- Mekanisme kendali akses yang dapat dilihat oleh pengguna pada level aplikasi memiliki kebijakan keamanan yang sangat ketat dan komplek.
- Aplikasi dapat ditulis di atas middleware, seperti database sistem manajemen atau paket pembukuan

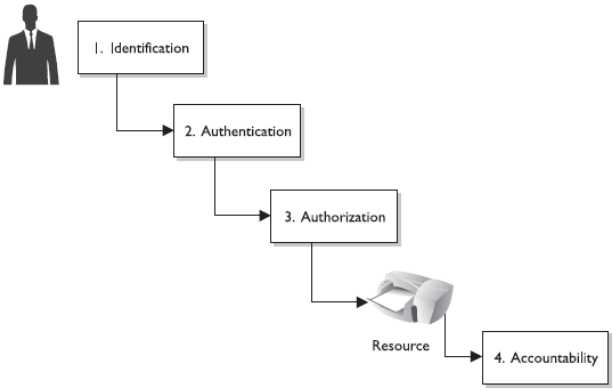
yang memaksa sistem harus diberi perlindungan khusus.

- Middleware akan menggunakan fasilitas yang disediakan oleh sistem operasi yang mendasarinya.
- Dan yang terakhir, sistem operasi kendali akses biasanya akan bergantung pada fitur perangkat keras yang disediakan oleh prosesor atau dengan manajemen memori yang dimiliki oleh perangkat keras tersebut.

Objek penelitian ini adalah Aplikasi Sistem Informasi Rumah Sakit (SIMRS), dimana dalam level kontrol akses pada sebuah sistem merupakan level paling atas atau pertama. Kontrol *logical* pada penelitian mencakup level aplikasi, *middleware* dan sistem operasi. Sedangkan kontrol *physical* mencakup hardware dan lokasi *hardware* berada atau disimpan.

2.2.4.2 Tahapan Proses Kontrol Akses

Menurut Shon Harris, terdapat empat tahapan dalam proses kontrol akses. Proses tersebut dimulai dengan tahap identifikasi, autentikasi, otorisasi dan yang terakhir adalah memastikan akuntabilitas dari akses [7]. Berikut digambarkan pada Gambar 2.2 penjelasan mengenai setiap tahapan pada kontrol akses.



Gambar 2. 2 Tahap Pada Proses Kontrol Akses [7]

a) Identifikasi *(Identification*). Identifikasi merupakan suatu aktivitas untuk memastikan bahwa subjek (user, program, atau proses) adalah entitas yang diklaimnya. Metode identifikasi dapat disediakan dengan menggunakan sejumlah nama pengguna, ID pengguna atau akun.
b) Autentikasi *(Authentication).* Autentifikasi adalah aktivitas memverifikasi informasi identitas. Metode untuk melakukan autentifikasi dapat berupa kata sandi, nomor identitas pribadi (PIN), biometrik dan lain sebagainya. Jika informasi identitas dan kata sandinya sesuai, barulah pengguna dapat dikonfirmasi.
c) Otorisasi *(Authorization).* Setelah pengguna berhasil diidentifikasi dengan tepat, sistem akan menentukan apakah akses yang dibutuhkan oleh pengguna tersebut telah mendapat hak akses dari sistem atau pihak manajemen. Sehingga otorisasi berkaitan dengan hak akses dan pembatasan akses.
d) Akuntabilitas *(Accountability).* Menurut kajian pustaka bahasa Indonesia akuntabilitas adalah

> pertanggungjawaban dari seseorang atau kelompok yang telah diberi amanat untuk menjalankan tugas tertentu kepada pihak pemberi amanat. Salah satu cara untuk menjaga akuntabilitas adalah dengan membuat log audit dan monitoring aktivitas subjek dengan objek. Akuntabilitas memberikan administrator kemampuan untuk melacak kegiatan apa pengguna dilakukan pada waktu tertentu. Hal Ini juga cara utama untuk melihat layanan apa yang digunakan dan bagaimana sumber daya sistem digunakan oleh pengguna individu. Akuntabilitas dilakukan dengan melakukan audit dan mengembangkan sistem untuk membuat dan menyimpan jejak audit [13].

Pada penelitian ini, tahapan dari kontrol akses tersebut akan menjadi dasar penggalian risiko keamanan pada akses Aplikasi Sistem Informasi Rumah Sakit (SIMRS) Rumah Sakit Dokter Moewardi.

2.2.4.3 Kategori Kontrol Akses

Terdapat tiga kategori dalam kontrol akses, berikut penjelasan untuk setiap kategori kontrol akses.

- Kontrol Akses Administratif

Kontrol administratif untuk akses lebih berorientasi ke manajemen atau pengelolaan. Contoh dari kontrol administratif adalah dokumen keamanan, manajemen risiko, keamanan personil dan pelatihan. Kontrol administratif dapat berbentuk kebijakan, prosedur, praktik perekrutan yang efektif, pemeriksaan latar belakang pra-kerja, klasifikasi data dan pelabelan, serta kesadaran keamanan. Kontrol administratif merupakan kontrol yang diupayakan oleh organisasi untuk mengekakkan hak akses ke sumber daya atau aset informasi [CITATION Ron01 \l 1057].

- Kontrol Akses *Logical*

Kontrol *logical* atau disebut juga kontrol teknis merupakan penggunaan teknologi perangkat lunak sebagai dasar untuk mengendalikan akses penggunaan data sensitif di seluruh struktur fisik dan melalui jaringan [6]. Teknologi tersebut digunakan untuk melakukan identifikasi, otentikasi, otorisasi, dan akuntabilitas. Perangkat lunak tersebut berfungsi untuk menegakkan hak akses pada sistem, program, proses, dan informasi. Kontrol akses *logical* dapat tertanam dalam sistem operasi, aplikasi, add-on paket keamanan, atau database dan manajemen sistem telekomunikasi [7]. Contoh dari kontrol akses *logical* adalah enkripsi dan protokol, pengamanan pada akses arsitektur jaringan, manajemen *passsword* (*Password Synchronization, Self-Service Password Reset, Legacy Single Sign-On, Password Hashing and Encryption, Password Aging, Limit Log on Attempts), Biometrics,* manajemen akun (*profile update, limited provisioning, secure dictionary) [7]*.

- Kontrol Akses *Physical*

Menurut ISO 27002, kontrol akses fisik merupakan bagian dari keamanan fisik dan lingkungan. Kontrol *physical* merupakan mekanisme untuk mengidentifikasi individu yang mencoba untuk memasuki fasilitas atau daerah yang dapat digunakan untuk mengakses informasi tertentu. Tujuan kontrol akses *physical* adalah untuk memastikan bahwa hanya individu yang memiliki hak akses yang dapat menggunakan fasilitas *hardware* dan memasuki daerah TI tertentu [7]. Contoh dari kontrol akses *physical* adalah keamanan kabel, *perimeter security,* memisahkan area kerja TI, penguncian ruangan TI, penguncian pelindung perangkat TI, pemisahan perangkat jaringan, memblokir *input-disk* eksternal, implementasi perangkat perlindungan yang mengurangi emisi listrik untuk menggagalkan upaya mengumpulkan informasi melalui gelombang udara, pengecekan identitas sebelum masuk area TI [7].

Penelitian ini bertujuan untuk menciptakan kontrol akses pada Aplikasi SIMRS dengan mempertimbangkan seluruh kategori

kontrol akses. Dalam kategori kontrol administrasi, penelitian ini bertujuan untuk membuat kebijakan dan prosedur untuk kontrol akses pada Aplikasi SIMRS, dimana kebijakan dan prosedur tersebut memuat atau meliputi kontrol *physical* dan *logical* pada Aplikasi Sistem Informasi Rumah Sakit (SIMRS).

2.2.5 Standar ISO 27002:2013

Standar ISO/IEC 27002 merupakan standar mengenai keamanan informasi. Standar ini memberikan panduan dalam perencaan dan implementasi suatu program untuk melindung aset-aset informasi, salah satunya adalah data di dalam aplikasi [14]. ISO/IEC 27002:2013 dikeluarkan oleh International Organization for Standardization (ISO) dan International Electronical Commision (IEC). ISO/IEC 27002 memiliki keterkaitan dengan ISO/IEC 27001, dimana dalam dokumen ISO/IEC 27001 berisikan kebutuhan mandatory dari sistem manajemen keamanan informasi sedangkan ISO/IEC 27002 melengkapinya dengan *code of practice* atau kontrol keamanan informasi untuk risiko keamanan pada kerahasian, keutuhan dan ketersediaan informasi. ISO/IEC 27002 memberikan *best practice* bagi organisasi dalam mengembangkan dan mengelola standard keamanan dan bagi manajemen untuk meningkatkan keamanan informasi dalam organisasi (IT Governance Institute & Office of Government Commerce, 2008). ISO/IEC 27002 memiliki 11 klausul utama kontrol yang masing masingnya terdiri dari kategori utama keamanan (*main security categories*) dan control. Kategori utama keamanan terdiri dari 14 area berdasarkan ISO27002:2013 yaitu:

a) *Security Policy* (Kebijakan Keamanan)
b) *Organizing Information Security* (Keamanan Informasi Organisasi)
c) *Human Resources Security* (Keamanan Sumber Daya Manusia)
d) *Asset Management* (Pengelolaan Aset)
e) *Access Control* (Kontrol Akses)
f) *Cryptography* (Kriptografi)

g) *Physical and Environmental Security* (Keamanan Fisik dan Lingkungan)
h) *Operations Security* (Keamanan Operasional)
i) *Communication Security* (Keamanan Komunikasi)
j) *System Acquisition, Development and Maintenance* (Akuisisi, Pengembangan dan Pengelolaan Sistem)
k) *Supplier Relationship* (Hubungan dengan *Supplier*)
l) *Information Security Incident Management* (Pengelolaan Insiden Keamanan Informasi)
m) *Information Security Aspects of Business Continuity Management* (Keamanan Informasi dari Aspek Pengelolaan Keberlangsungan Bisnis)
n) *Compliance* (Kepatuhan)

2.2.5.1 Kontrol Standar ISO 27002:2013

Kategori utama keamanan meiliki kontrol (*control*) dan pedoman pengimplementasian (*implementation guidance*). Kontrol merupakan pendefinisian dari pernyataan mengenai kontrol untuk menjawab kontrol objektif dari setiap kategori utama keamanan dan pedoman pengimplementasian menyediakan detail informasi untuk mendukung pengimplementasian kontrol. Berikut ini merupakan kontrol ISO27002:2013 yang digunakan dalam penelitian:

- Kontrol Standar Untuk Akses *Logical*

Tabel 2. 2 Kontrol *Logical* pada ISO 27002:2013

Klausul	Poin Utama	*Control Objective*	Penjelasan
9 Access control	*9.1 Business requirements of access control*	*9.1.1 Access control policy*	Kontrol untuk memastikan bahwa kebijakan kontrol akses telah dibentuk, didokumentasikan dan ditinjau berdasarkan kebutuhan keamanan bisnis dan informasi

Klausul	Poin Utama	*Control Objective*	Penjelasan
		9.1.2 Access to networks and network services	Kontrol untuk memastikan bahwa pengguna hanya telah disediakan akses ke jaringan dan ke layanan jaringan sesuai dengan izin yang telah ditetapkan oleh sistem untuk mereka gunakan.
	9.2 User access management	*9.2.1 User registration and de-registration*	Kontrol untuk memastikan bahwa proses registrasi dan de-registrasi pengguna formal telah diimplementasikan untuk memberikan hak akses yang tepat.
		9.2.2 User access provisioning	Kontrol untuk memastikan bahwa proses penyediaan hak akses resmi pengguna telah diimplementasikan untuk mencabut dan menetapkan hak akses pada seluruh jenis pengguna di semua sistem dan layanan.
		9.2.3 Management of privileged access rights	Kontrol untuk membatasi dan mengendalikan alokasi dan penggunaan hak akses istimewa.
		9.2.4 Management of secret authentication information of	Kontrol untuk memastikan bahwa alokasi informasi yang memiliki otentikasi rahasia telah

Klausul	Poin Utama	*Control Objective*	Penjelasan
		users	dikendalikan melalui proses manajemen resmi.
		9.2.5 Review of user access rights	Kontrol untuk memastikan bahwa pemilik aset telah meninjau hak akses penggunaan asetnya secara berkala
		9.2.6 Removal or adjustment of access rights	Kotrol untuk memastikan bahwa hak akses seluruh karyawan dan pengguna pihak eksternal pada akses informasi dan akses fasilitas pengolahan informasi telah dihapus setelah pemutusan hubungan kerja, kontrak atau perjanjian merela, atau disesuaikan dengan perubahan.
	9.3 User responsibilities	*9.3.1 Use of secret authentication information*	Kontrol untuk memastikan bahwa pengguna telah mengikuti cara-cara organisasi dalam menggunakan informasi yang harus memiliki otentikasi rahasia.
	9.4 System and application access control	*9.4.1 Information access restriction*	Kontrol untuk memastikan bahwa akses ke informasi dan fungsi sistem aplikasi telah dibatasi sesuai dengan kebijakan

Klausul	Poin Utama	*Control Objective*	Penjelasan
			kontrol akses.
		9.4.2 Secure log-on procedures	Kontrol untuk memastikan bahwa prosedur *log-on* aman ketika dibutuhkan oleh kebijakan kontrol akses, akses ke sistem dan akses ke aplikasi.
		9.4.3 Password management system	Kontrol untuk memastikan bahwa sistem manajemen password telah interaktif dan telah dipastikan kualitas passwordnya.
		9.4.4 Use of privileged utility programs	Kontrol untuk memastikan bahwa penggunaan dari utilitas program yang mungkin mampu menolak sistem dan aplikasi telah dibatasi dan dikontrol ketat.
		9.4.5 Access control to program source code	Kontrol untuk memastikan bahwa akses ke kode sumber program telah dibatasi.

- Kontrol Standar Untuk Akses *Physical*
  Kontrol untuk akses *physical* tergabung pada kalusul 11 yaitu mengenai keamanan fisik.

Tabel 2. 3 Kontrol *Physical* pada ISO27002:2013

Klausul	Poin Utama	*Control Objective*	Penjelasan
11 Physical and environmental	*11.1 Secure areas*	*11.1.1 Physical security*	Kontrol untuk memastikan bahwa perimeter atau

Klausul	Poin Utama	*Control Objective*	Penjelasan
security		*perimeter*	batasan keamanan telah didefinisikan dan digunakan untuk melindungi area yang berisi informasi dan pengolahan informasi fasilitas yang sensitif atau kritis.
		11.1.2 Physical entry controls	Kontrol untuk memastikan bahwa daerah telah dilindungi oleh kontrol masuk yang tepat sehingga dapat dipastikan bahwa hanya pihak yang berwenang yang diperbolehkan mengakses.
		11.1.3 Securing offices, rooms and facilities	Kontrol untuk memastikan bahwa keamanan fisik untuk kantor, kamar dan fasilitas telah dirancang dan diterapkan.
		11.1.5 Working in secure area	Kontrol untuk memastikan bahwa prosedur untuk bekerja di area aman telah dirancang dan diterapkan.
	11.2	*11.2.1*	Kontrol untuk

Klausul	Poin Utama	*Control Objective*	Penjelasan
	Equipment	*Equipment siting and protection*	memastikan bahwa peralatan telah diletakkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya ingkungan, serta kesempatan akses oleh pihak yang tidak sah.
		11.2.3 Cabling security	Kontrol untuk memastikan bahwa listrik dan telekomunikasi kabel pembawa data atau pendukung layanan informasi harus dilindungi dari penyadapan, gangguan atau kerusakan.
		11.2.8 Unattended user equipment	Kontrol untuk memastikan bahwa peralatan yang tidak diawasi memiliki perlindungan yang tepat.
		11.2.9 Clear desk and clear screen policy	Kontrol untuk memastikan bahwa kebijakan meja kerja bebas dari kertas yang berisi informasi rahasia dan media penyimpanan yang mudah

Klausul	Poin Utama	*Control Objective*	Penjelasan
			dipindahkan. Kebijakan layar yang bebas dari informasi rahasia pada fasilitas pengolahan informasi harus diadopsi.

2.2.6 Risiko

Menurut ISO/IEC *Guide* 73 dalam buku *"A Risk Management Standard"*, risiko adalah perpaduan antara probabilitas atau kemungkinan dari suatu kejadian yang tidak pasti dengan konsekuensinya, di mana konsekuensi tersebut dapat bernilai positif maupun negatif. Dari pendapat mengenai risiko tersebut, maka dapat disimpulkan bahwa risiko adalah bagian dari ketidakpastian suatu kejadian yang dapat memberikan dampak, baik negatif maupun positif dan akan berpengaruh terhadap kemampuan organisasi dalam mencapai tujuan organisasi [10].

2.2.7 Risiko Teknologi Informasi

Risiko teknologi informasi menurut ISACA (*Information Systems Audit and Control Association*) merupakan sebuah risiko bisnis yang berkaitan dengan aspek teknologi informasi yang tidak direncanakan dan dapat menimbulkan dampak pada perusahaan. Sehingga risiko TI perlu dianalisis dan dimitigasi untuk mencegah terhambatnya proses bisnis yang dapat menghambat kegiatan opersional perusahaan ataupun organisasi.

Risiko teknologi informasi, merupakan bagian dari risiko operasional karena sifatnya yang terkait dengan penggunaan aset teknologi informasi untuk mendukung operasional proses bisnis di dalam perusahaan. Risiko teknologi informasi antara lain mencakup risiko yang berasal dari internal seperti

kegagalan sistem, kegagalan jaringan *(network),* kerusakan *hardware*, kerusakan *software*, kehilangan data, virus, dan risiko lainnya yang berasal dari eksternal seperti bencana alam [10].

Risiko TI meningkat sebanding dengan perkembangan penggunaan teknologi informasi. Penggunaan TI yang meningkat mengakibatkan ketergantungan bagi organisasi maupun perusahaan yang mengadopsi TI pada proses bisnisnya, sehingga risiko yang ditimbulkan dari pengimplementasian TI tersebut pun meningkat. Risiko TI adalah sebuah kejadian yang tidak dapat direncanakan dan berdampak pada keagalan atau penyalahgunaan TI yang mengancam tujuan bisnis [15].

2.2.8 Keterkaitan antara Risiko Teknologi Informasi dan Kontrol Akses

Menurut ISRMC (*Information Systems Management Research Center*) dalam penelitiannya mengenai Operational Risk Framework, sebuah risiko TI yang berhubungan dalam bidang operasional disebut dengan risiko operasional. Dan risiko operasional adalah hal hal operasional yang mungkin terjadi dan berdampak pada informasi organisasi ataupun aset kritisnya [16]. Dimana risiko TI dalam bidang operasional tersebut erat hubungannya dengan ketiga aspek keamanan informasi yaitu kerahasiaan *(confidentiality),* keutuhan *(integrity)* dan ketersediaan *(availability).* ISRMC menggambarkan sebuah kerangka kerja Operational Risk Framework sebagai berikut.

Gambar 2. 3 Operational Risk Framework Model [16]

Dalam Operational Risk Framework dijelaskan bahwa sebuah risiko dilihat berdasarkan aset yang ada. Dimana risiko tersebut diidentifikasikan berdasarkan kategori kemanan informasi yaitu kerahasiaan *(confidentiality),* keutuhan *(integrity)* dan ketersediaan *(availability)* dari masing masing aset yang ada. Sementara, salah satu bagian dari keamanan informasi adalah kontrol akses. Kontrol akses bertujuan untuk mengatur akses dari subjek ke aset TI agar keamanan informasi dapat terlindungi atau terjaga. Karena salah satu aspek yang dapat merusak kerahasiaan *(confidentiality),* keutuhan *(integrity)* dan ketersediaan *(availability)* adalah akses tidak sah pada aset TI.

Sehingga pada penelitian ini, penggalian kebutuhan SOP kontrol akses pada Aplikasi SIMRS akan didasarkan dari risiko pada masing-masing aset TI yang berkaitan dengan Aplikasi SIMRS. Penelitian ini akan menggali terlebih dahulu kebutuhan keamanan informasi beserta ancamannya pada

setiap aset TI yang berkaitan dengan Aplikasi SIMRS. Kemudian dari kebutuhan keamanan dan ancamannya tadi berulah dilakukan penggalian risiko yang berhubungan dengan kontrol akses, yaitu yang berkaitan dengan aktivitas identifikasi, autentikasi, otorisasi dan akuntabilitas akes.

2.2.9 Manajemen Risiko

Menurut ISO 31000:2009 manajemen risiko adalah suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehinga dapat memperoleh hasil yang optimal. Proses manajemen risiko menurut ISO 31000:2009 meliputi lima kegiatan, yaitu komunikasi dan konsultasi, menentukan konteks, *assesment* risiko, perlakuan risiko, serta *monitoring* dan *review*. Sehingga dapat disimpulkan bahwa manajemen risiko adalah sebuah proses yang didalamnya terdapat aktifitas pengelolaan risiko untuk meminimalisir kerugian atau dampak bagi organisasi atau perusahaan [17] . Selain itu manajemen risiko juga dilakukan dengan tujuan sebagai tindakan perlindungan bagi seluruh aset TI dan untuk meminimalisir risiko maupun dampak dari risiko yang berkaitan dengan teknologi informasi/sistem informasi [15].

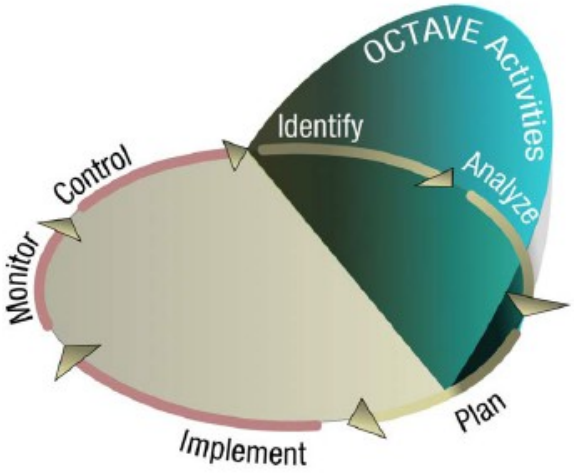
2.2.10 Manajemen Risiko Teknologi Informasi

Menurut National Institute Risk Technology (NIST) dalam publikasinya menyatakan, manajemen risiko teknologi informasi adalah suatu rangkaian proses yang meliputi penilaian risiko, mitigasi risiko dan evaluasi dari komponen TI sebuah organisasi atau perusahaan. Manajemen risiko TI merupakan bagian dari proses pengelolaan risiko TI di sebuah organisasi atau perusahaan yang melakukan proses pengelolaan risiko TI. Proses ini berupa identifikasi, penilaian dan mitigasi risiko yang terjadi di organisasi tersebut. Manajemen risiko TI juga dilakukan dengan tujuan sebagai tindakan perlindungan bagi seluruh aset TI dan untuk

meminimalisir risiko maupun dampak dari risiko yang berkaitan dengan teknologi informasi/sistem informasi.

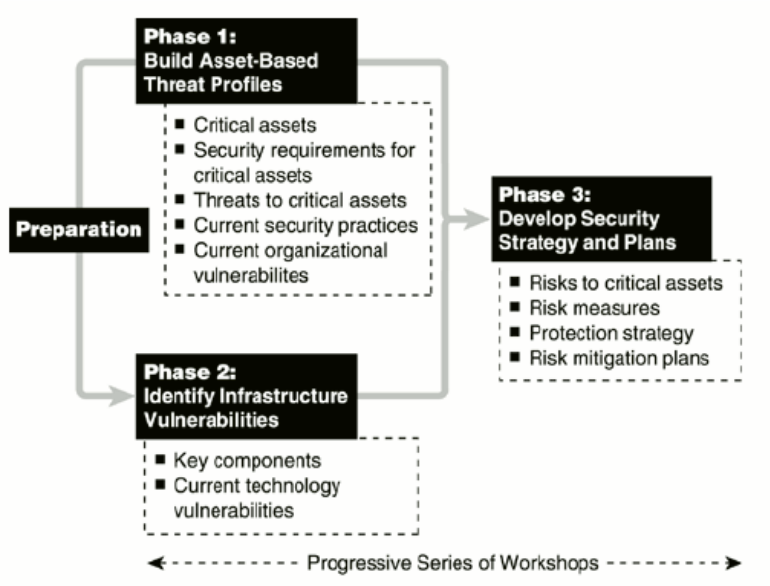
2.2.11 OCTAVE

OCTAVE *(Operationally Critical Threat, Asset, and Vulnerability Evaluation*) adalah *framework* untuk mengevaluasi risiko teknologi informasi yang mempertimbangkan dua isu utama yaitu pada aspek organisasi dan teknologi. Evaluasi risiko keamanan informasi merupakan bagian dari kegiatan organisasi untuk mengelola risiko keamanan informasi. Dalam siklus *plan-do-check-act* manajemen risiko teknologi informasi, OCTAVE berfungsi sebagai bagian dari perencanaan yaitu mengidentifikasi dan menganalisa risiko yang berkaitan dengan teknologi informasi pada organisasi khususnya aspek keamanan [18]. Hubungan antara manjemen teknologi informasi dengan evaluasi risiko pada *framework* OCTAVE dapat dilihat pada gambar dibawah.



Gambar 2. 4 Manajemen Risiko TI Pada OCTAVE [18]

OCTAVE menggunakan pendekatan tiga tahapan dalam menguji isu organisasi terhadap penyusunan masalah yang komprehensif dan berhubungan dengan kebutuhan keamanan sebuah organisasi. Berikut merupakan penjelasan dari masing masing tahapan dalam OCTAVE:



Gambar 2. 5 Tahap Pada Proses Kontrol Akses [18]

a. Tahap 1: Membangun Profil Aset Berbasis Ancaman [18].

Dua fungsi utama dari fase ini adalah mengumpulkan informasi dari berbagai level organisasi dan mendefinisikan profil ancaman untuk aset kritis. Tahap ini merupakan bagian dari *organisational view* yang melihat dari sisi internal organisasi, sehingga luaran dari tahapan ini adalah aset penting organisasi, kebutuhan keamanan organisasi, praktek keamanan terkini yang telah atau sedang dilakukan organisasi dan kelemahan kebijakan yang dimiliki organisasi saat ini.

a) Proses 1: Mengidentifikasi Pengetahuan Manajemen Senior. Mengumpulkan informasi mengenai aset penting, persyaratan keamanan, ancaman, dan kekuatan serta kerentanannya dari sisi manajemen.

b) Proses 2: Mengidentifikasi Pengetahuan Area Operasional. Mengumpulkan informasi mengenai aset penting, persyaratan keamanan, ancaman, dan kekuatan serta kerentanannya dari sisi operasional.
c) Proses 3: Mengidentifikasi Pengetahuan Karyawaan. Mengumpulkan informasi mengenai aset penting, persyaratan keamanan, ancaman, dan kekuatan serta kerentanannya dari karyawan umum dan karyawan TI dari bidang operasional yang dipilih.
d) Proses 4: Membuat Profil Ancaman. Memilih tiga hingga lima informasi aset kritis dan mendefinisikan profil ancaman untuk aset-aset tersebut.

b. Tahap 2: Identifikasi Infrastruktur *Vulnerabilities [18]*.

Tahapan ini akan melihat dari sisi teknologi yaitu melakukan evaluasi komponen kunci dari sistem pendukung aset penting untuk kerentanan infrastruktur teknologi yang dimiliki organisasi. Sehingga luaran dari tahapan ini adalah berupa komponen penting dalam aset kritis dan kelemahan infrastruktur TI yang ada saat ini.

a) Proses 5: Mengidentifikasi Komponen Kunci. Mengidentifikasi satuan komponen kunci yang merepresentasikan sistem yang mendukung atau memproses aset informasi kritis yang sudah teridentifikasi.
b) Proses 6: Mengevaluasi Komponen yang Dipilih. Mengevaluasi kelemahan komponen pendukung aset kritis yaitu infrastruktur TI yang ada saat ini.

c. Tahap 3 : Mengembangkan Strategi Keamanan dan Perencanaan [18].

Tahapan ini merupakan tahapan penilaian risiko terhadap aset kritis dan mitigasi risiko dengan melakukan pengembangan strategi keamanan dan perencanaannya. Sehingga luaran dari

tahapan ini adalah berupa analisis risiko, pengukuran tingkat risiko dan strategi proteksi.

a) Proses 7: Melakukan Analisis Risiko.
   Mengevaluasi kriteria dampak organisasi untuk membangun dasar umum dalam menentukan nilai dampak *(medium, high, or low)* karena ancaman terhadap aset kritis. Pada penelitian ini analisis risiko dilakukan dengan menggunakan pendekatan metode FMEA.
b) Proses 8: Mengembangkan Strategi Perlindungan.
   Mengembangkan strategi perlindungan yang fokus pada meningkatkan praktik keamanan organisasi seperti rencana mitigasi untuk mengurangi risiko penting pada aset kritis.

2.2.12 FMEA

FMEA (*Failure Modes and Effects Analysis*) adalah suatu prosedur terstruktur untuk mengidentifikasi akibat atau konsekuensi dari kegagalan sistem atau proses, serta mengurangi atau mengeliminasi peluang terjadinya kegagalan. FMEA merupakan metode yang dapat digunakan untuk mengurangi kerugian yang terjadi akibat kegagalan tersebut. Metode FMEA mampu mengidentifikasi tiga hal yaitu penyebab kegagalan dari sistem, desain produk, dan proses, efek dari kegagalan dan tingkatan kritikal efek dari suatu kegagalan.

Metode FMEA memiliki langkah-langkah terstruktur. Langkah langkah dalam FMEA tesebut adalah sebagai berikut :

1. Mengidentifikasi komponen komponen dan fungsi yang terkait
2. Mengidentifikasi mode kegagalan (*failure modes)*
3. Mengidentifikasi dampak dari mode kegagalan (*failure mode)*

4. Menentukan nilai keparahan (*severity)* dari kegagalan
5. Mengidentifikasi penyebab dari kegagalan
6. Menentukan nilai frekuensi sering terjadinya (*occurence)* kegagalan
7. Mengidentifikasi kontrol yang diperlukan
8. Menentukan nilai keefektifan kontrol yang sedang berjalan (*detection)*
9. Melakukan kalkulasi nilai RPN (*risk priority number)*
10. Menentukan tindakan untuk mengurangi kegagalan

Untuk dapat menggunakan FMEA sebagai alat untuk melakukan penilaian risiko dan menghasilkan keluaran yang akurat, maka terlebih dahulu ada beberapa hal yang perlu dilakukan penentuan nilai, yaitu severity, occurence dan detection. Berikut adalah pembahasan dari ketiganya.

2.2.12.1 Penentuan Nilai Dampak (*Severity* = S)

Pengukuran nilai dampak akan dilihat dari seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek aspek penting dalam organisasi. Dalam menentukan penilaian tingkat dampak, perlu dibuat parameter untuk setiap nilainya. Berikut merupakan penjelasan dari masing masing nilai dampak.

Tabel 2. 4 Tabel Nilai Parameter *Severity*

Dampak	Dampak dari Efek	Ranking
Akibat Berbahaya	Melukai Pelanggan atau Karyawan	10
Akibat Serius	Aktivitas yang illegal	9
Akibat Ekstrim	Mengubah Produk atau Jasa menjadi tidak layak digunakan	8
Akibat Major	Menyebabkan ketidakpuasan pelanggan secara ekstrim	7
Akibat Signifikan	Menghasilkan kerusakan parsial secara moderat	6

Dampak	Dampak dari Efek	Ranking
Akibat Moderat	Menyebabkan penurunan kinerja dan mengakibatkan keluhan	5
Akibat Minor	Menyebabkan sedikit kerugian	4
Akibat Ringan	Menyebabkan gangguan kecil yang dapat diatasi tanpa kehilangan sesuatu	3
Akibat Sangat Ringan	Tanpa disadari: terjadi gangguan kecil pada kinerja	2
Tidak Ada Akibat	Tanpa disadari dan tidak mempengaruhi kinerja	1

2.2.12.2 Penentuan Nilai Kemungkinan (*Occurence* = O)

Nilai kemungkinan atau *occurence* merupakaan pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat menghasilkan kegagalan. Pada tabel dibawah, terdapat penjelasan nilai kemungkinan dan kemungkinan terjadinya risiko.

Tabel 2. 5 Tabel Nilai Parameter *Occurence*

Kemungkinan Kegagalan	Kemungkinan Terjadi	Ranking
Very High: Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya	10
Very High: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari	9
High: Kegagalan terjadi berulang kali	Satu kali dalam seminggu	8
High: Kegagalan sering terjadi	Satu kali dalam sebulan	7
Moderatly High : Kegagalan terjadi saat	Satu kali setiap 3 bulan	6

Kemungkinan Kegagalan	Kemungkinan Terjadi	Ranking
waktu tertentu		
Moderate : Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low : Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relative kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relative kecil dan sangat jarang	Satu kali dalam 3 - 6 tahun	2
Remote: Kegagalan tiak pernah terjadi	Satu kali dalam 6 - 50 tahun	1

2.2.12.3 Petunjuk Pemberian Skor Deteksi (Detection = D)

Pengkuruan nilai deteksi merupakan penilaian terhadap kemampuan organisasi dalam melakukan kontrol dan kendali terhadap terjadinya suatu gangguan atau kegagalan yang akan terjadi. Berikut adalah penjelasan nilai deteksi dan metode deteksi terhadap risiko.

Tabel 2. 6 Tabel Nilai Parameter *Detection*

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode detensi	10
Sangat Kecil	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi	9
Kecil	Metode deteksi tidak terbukti untuk mendeteksi tepat waktu	8
Sangat Rendah	Metode deteksi tidak andal dalam mendeteksi tepat waktu	7

Deteksi	Kriteria Deteksi	Ranking
Rendah	Metode deteksi memiliki tingkat efektifitas yang rendah	6
Sedang	Metode deteksi memiliki tingkat efektifitas yang rata-rata	5
Cukup Tinggi	Metode deteksi memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan	4
Tinggi	Metode deteksi memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan	3
Sangat Tinggi	Metode deteksi sangat efektif untuk dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	2
Hampir Pasti	Metode deteksi hampir pasti dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	1

2.2.12.4 Penentuan Level Risiko (RPN)

Setelah melakukan penetuan nilai dampak (*severity*), nilai kemungkinan (*occurence*) dan nilai deteksi (*detection*) selanjutnya adalah melakukan kalkulasi nilai prioritasi risiko *(Risk Priority Number)* yang didapatkan dari formulasi berikut:

$$\mathbf{RPN = S \times O \times D}$$

RPN : *Risk Priority Number*, perhitungan nilai risiko
S : *Severity*, nilai dampak
O : *Occurrence*, niai kemungkinan

D: *Detection*, nilai deteksi

Penentuan kriteria penerimaan risiko didasarkan pada hasil penilaian risiko, dimana setelah ditentukan nilai RPN dari masing-masing risiko, selanjutnya ditentukan level risiko berdasarkan skala RPN. Hasil dari penghitungan berfungsi sebagai petunjuk kepada IPDE agar mengetahui risiko mana yang perlu menjadi prioritas. Berikut ini adalah skala penentuan nilai RPN berdasarkan pada metode FMEA.

Tabel 2. 7 Tabel Skala Penentuan Nilai RPN

Level Risiko	Skala Nilai RPN
Very High	>= 200
High	>=120 - < 200
Medium	>=80 - < 120
Low	>=20 - < 80
Very Low	0 - < 20

2.2.13 SOP

Tata kelola TI diartikan sebagai pengaturan yang dilaksanakan secara terpadu dan tidak terpisahkan dengan sumber daya organisasi. Menurut Weill dan Ross, Tata kelola TI adalah pengaturan pengaturan yang terkait dengan pengambilan keputusan. Pengaturan dijalankan untuk mendorong tercapainya perilaku pemakaian teknologi informasi yang mendukung tercapainya tujuan organisasi. Tata kelola TI memiliki struktur hirarki dokumen.

SOP (*Standard Operating Procedure*) merupakan dokumen proses yang menjelaskan secara terperinci mengenai bagaimana cara melakukan sesuatu dalam sebuh kegiatan operasional [19]. SOP adalah kumpulan dari intruksi mengenai aktifitas yang didokumentasikan secara berulang pada sebuah organisasi. SOP digunakan untuk menjaga konsistensi kegiatan

operasional serta sebagai tolak ukur keberhasilan suatu kegiatan operasional [8]. Dengan menyusun SOP, organisasi dapat mendefinisikan tujuan dari kegiatan operasionalnya, dan seluruh komponen terkait seperti alat atau data terkait operasional, aktifitas terkait kegiatan operasional maupun aktor yang terlibat dalam kegiatan operasional tersebut. Salah satu manfaat dari implementasi SOP yaitu meminimalkan variasi pelaksanaan suatu kegiatan operasional, dan juga untuk menjaga konsistensi dalam meningkatkan kualitas dari suatu operasional, bahkan apabila terjadi pergantian aktor dalam kegiatan operasional tersebut, kegiatan masih dapat berjalan karena telah memiliki suatu standard proses yang jelas [19]. Standard dokumen SOP harus disusun dengan ringkas namun telah memuat seluruh aktifitas secara berurutan dengan format yang mudah dimengerti. Berikut adalah beberapa kriteria penulisan SOP yang baik menurut Akyar [19].

1. Spesifik dan Lengkap
   Sebuah SOP disusun dengan menspesifikasikan seluruh aktifitas yang terkait dalam proses, termasuk memasukan seluruh unsur terkait proses tersebut yaitu melibatkan seluruh aktifitas, aktor hingga data yang terkait dalam kegiatan operasional. Dokumen SOP juga harus mencantumkan keterangkan lengkap mengenai nomor SOP, versi SOP, judul SOP serta status SOP.
2. Dapat Dipahami
   Sebuah SOP disusun dengan jelas dan spesifik dengan menggunakan bahasa formal dan format penulisan yang baik untuk mudah dipahami.
3. Dapat Diaplikasikan
   Sebuah SOP disusun dengan beracuan pada dokumen terkait yang ada pada organisasi sehingga dapat diaplikasikan pada proses operasional yang sesungguhnya. Dokumen terkait yang dapat menjadi acuan dari pembuatan SOP adalah seperti kebijakan pendukung SOP hingga dokumen teknis lainnya.

4. Dapat Diaudit
   Sebuah SOP disusun dengan lengkap dan spesifik untuk memudahkan proses audit internal dalam organisasi. Dimana sebuah SOP merupakan proses yang periodic sehingga harus dapat diaudit untuk memastikan penjelasan alur proses yang ada didalamnya masih sesuai dengan kondisi organisasi.
5. Dapat Diubah
   Sebuah SOP disusun dengan mengikuti kondisi organisasi dan harus mampu menyesuaikan perubahan kegiatan operasional yang terjadi pada proses operasional yang terkait.

Dalam penyusunan dokumen SOP tidak terdapat suatu format baku yang dapat dijadikan acuan, hal ini dikarenakan SOP merupakan dokumen internal yang kebiijakan pembuatannya disesuaikan oleh masing masing organisasi, begitu pula dengan penyunan format dari dokumen SOP tersebut. Namun sebuah SOP juga memiliki kriteria yang harus dipenuhi untuk memastikan bahwa dokumen yang disusun mudah dimengerti secara spesifik, efisien serta mudah diaplikasikan dalam organisas.

2.2.14 Format Dokumen SOP

Menurut Tjipto Atmoko, terdapat beberapa jenis format dalam pembuatan SOP, yang pertama adalah Langkah sederhana (simple steps), yang kedua adalah Tahapan berurutan (Hierarchical steps), yang ketiga adalah Grafik (graphic), dan yang terakhir adalah Diagram alir (flowcharts). Terdapat empat faktor yang dapat dijadikan dasar dalam penentuan format penysunan Standard Operating Procedure (SOP) yang akan dipakai oleh suatu organisasi yaitu :

- Banyaknya keputusan yang akan dibuat dalam suatu prosedur.

- Banyaknya langkah dan sub langkah yang diperlukan dalam suatu prosedur.
- Siapa yang akan dijadikan target sebagai pelaksana Standard Operating Procedure (SOP).
- Tujuan yang ingin dicapai dalam pembuatan Standard Operating Procedure (SOP) ini.

Ada 4 jenis format umum Standard Operating Procedure (SOP), diantaranya adalah sebagai berikut :

a. Langkah sederhana (simple steps)
   Simple steps dapat digunakan jika prosedur yang akan disusun hanya memuat sedikit kegiatan dan memerlukan sedikit keputusan yang bersifat sederhana. Format SOP ini dapat digunakan dalam situasi dimana hanya ada beberapa orang yang akan melaksanakan prosedur yang telah disusun.
b. Tahapan berurutan (Hierarchical steps)
   Format ini merupakan pengembangan dari simple steps. Digunakan jika prosedur yang disusun panjang, lebih dari 10 langkah dan membutuhkan informasi yang lebih detail, akan tetapi hanya memerlukan sedikit pengambilan keputusan.
c. Grafik (graphic)
   Format grafik ini bertujuan untuk memudahkan dalam memahami prosedur yang ada dan biasanya ditujukan untuk pelaksanaan eksternal organisasi (pemohon).
d. Diagram alir (flowcharts)
   Flowcharts merupakan format yang biasa digunakan, jika dalam Standard Operating Procedure (SOP) diperlukan pengambilan keputusan yang banyak (kompleks) dan membutuhkan opsi jawaban (alternative jawaban) seperti : jawaban “ya” atau “tidak”, “lengkap” atau “tidak”, “benar” atau “salah”, dsb. Simbol-simbol tersebut memiliki fungsi yang bersifat khas (teknis dan khusus) yang pada dasarnya dikembangkan dari simbol

dasar flowcharts (basic symbols of flowcharts) yang terdiri dari 4 simbol, yaitu:

1. Simbol kapsul/terminator, untuk mendeskripsikan kegiatan mulai dan berakhir.
2. Simbol kotak/process, untuk mendeskripsikan proses atau kegiatan eksekusi.
3. Simbol belah ketupat/decision, untuk mendeskripsikan kegiatan pengambilan keputusan.
4. Simbol anak panah/arrow, untuk mendeskripsikan arah kegiatan (alur proses kegiatan).
5. Simbol segi lima/off-page connector, untuk mendeskripsikan hubungan antar simbol yang berbeda halaman.

Format *Standard Operating Procedure* (SOP) dalam bentuk flowcharts terdiri dari 2 jenis yaitu :

1. Linear flowcharts (diagram alir linier)
   Ciri utama dari format linear flowcharts ini adalah unsur kegiatan yang disatukan, yaitu : unsur kegiatan atau unsur pelaksanaannya dan menuliskan rumusan kegiatan secara singkat didalam simbol yang dipakai.
2. Branching flowcharts (diagram alir bercabang)
   Format Branching Flowcharts memiliki ciri utama dipisahkannya unsur pelaksana dalam kolom-kolom yang terpisah dari kolom kegiatan dan menggambarkan prosedur kegiatan dalam bentuk simbol yang dihubungkan secara bercabang-cabang.

Format penyusunan dokumen SOP akan digunakan untuk memudahkan dalam penyusunan SOP dan juga sebagai acuan pembuatan dokumen SOP akses kontrol Aplikasi SIMRS Rumah Sakit Dokter Moewardi. Berikut merupakan panduan format umum penyusunan SOP Administrasi Pemerintah yang dikeluarkan oleh Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi

RI melalui PERMENPAN Nomor 35 Tahun 2012 yang harus memenuhi unsur dokumentasi dan unsur prosedur.

1. Unsur Dokumentasi

Unsur dokumentasi merupakan unsur yang terkait dengan proses pendokumentasian SOP sebagai sebuah dokumen. Unsur dokumentasi yaitu halaman judul, keputusan pimpinan terkait, dan deskripsi singkat penggunaan dokumen.

a) Halaman Judul (*Cover*)
Halaman judul merupakan halaman yang menjadi sampul dari dokumen SOP dan harus mampu memberikan informasi mengenai isi dokumen. Sehingga dalam halam judul beberapa hal yang harus ada adalah judul SOP, instansi/satuan kerja, tahun pembuatan dan keterangan informasi lain sesuai persetujuan organisasi terkait.

b) Daftar Isi Dokumen SOP
Daftar isi digunakan untuk mempercepat pencarian informasi dan menulis perubahan atau revisi dari bagian tertentu pada SOP.

c) Deskripsi Penggunaan Dokumen
Dalam diskripsi singkat penggunaan dokumen, perlu dijelaskan mengenai ruang lingkup yang membahas mengenai tujuan disusunya prosedur, tingkasan mengenai prosedur yang disusun dan definisi kata yang terkait didalam dokumen SOP.

2. Unsur Prosedur

Unsur proedur merupakan bagian identitas dan bagian alur prosedur atau *flowchart*. Berikut adalah masing masing penjelasannya.

a) Bagian Identitas

Bagian identitas dalam dokumen SOP berisikan logo dan nama instanasi terkait, nomor SOP, tanggal pembuatan, tanggal revisi, tanggal efektif, pengesahan dokumen, judul SOP, dasar hukum dan identitas lainnya sesuai dengan kebijakan dan persetujuan organisasi terkait.

KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI DEPUTI BIDANG TATALAKSANA ASISTEN DEPUTI PENGEMBANGAN SISTEM DAN PROSEDUR PEMERINTAHAN	NOMOR SOP	: K/PAN-RB/D.IV/4/001/2011
	TGL. PEMBUATAN	: 6 Juli 2011
	TGL. REVISI	:
	TGL. EFEKTIF	: 8 Agustus 2011
	DISAHKAN OLEH	: Asisten Deputi Pengembangan Sistem dan Prosedur Pemerintahan Nama NIP
	NAMA SOP	: PEMBUATAN LAPORAN KONSINYERING

DASAR HUKUM:	KUALIFIKASI PELAKSANA:
1. Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2009 tentang Pembentukan dan Organisasi Kementerian Negara 2. Peraturan Presiden Republik Indonesia Nomor 24 Tahun 2010 tentang Kedudukan, Tugas, dan Fungsi Kementerian Negara serta Susunan Organisasi, Tugas, dan Fungsi Eselon I Kementerian Negara 3. Peraturan Menteri Negara PAN dan RB Nomor 12 Tahun 2010 tentang Organisasi Dan Tata Kerja Kementerian PAN dan RB	1. Memiliki kemampuan pengolahan data sederhana 2. Mengetahui tugas dan fungsi Sistem dan Prosedur Pemerintahan 3. Mengetahui tugas dan fungsi mekanisme pembuatan laporan
KETERKAITAN:	**PERALATAN/PERLENGKAPAN:**
1. SOP Pelaksanaan Konsinyering 2. SOP Pendokumentasian Laporan Konsinyering 3. SOP Pencairan Anggaran Konsinyering	1. Lembar Kerja / Rencana Kerja dan Anggaran 2. Term of Refference 3. Komputer/Printer/Scanner 4. Jaringan internet
PERINGATAN:	**PENCATATAN DAN PENDATAAN:**
Apabila Laporan Konsinyering terlambat dibuat maka pelaksanaan kegiatan Konsinyering berikutnya akan tertunda.	- Di simpan sebagai data elektronik dan manual

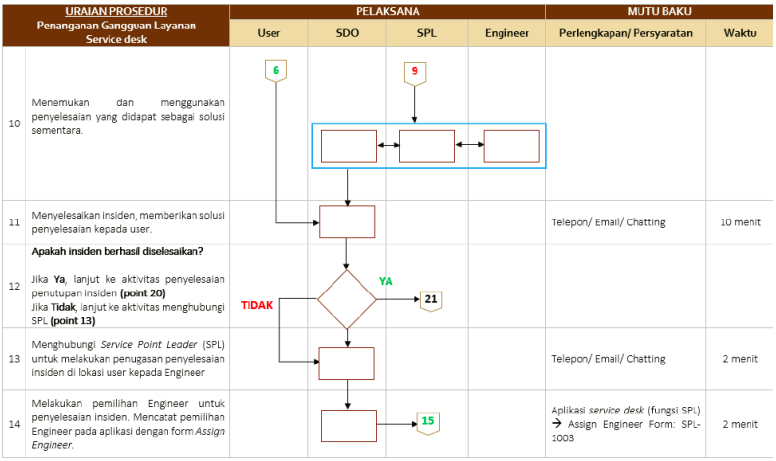
Gambar 2. 6 Contoh Bagian Identitas Prosedur [20]

b) Alur Prosedur

Bagian alur prosedur merupakan bagian yang berisikan penjelasan langkah langkah prosedur kegiatan beserta mutu baku dan keterangan yang diperlukan. Alur prosedur dibentuk dalam sebuah *flowchart* yang menjelaskan langkah dari kegiatan secara berurutan dan sistemastis. Bagan alur atau *flowchart* adalah salah satu unsur dari sebuah prosedur. *Flowchart* merupakan bagian yang berisi penjelasan langkah langkah sebuah prosedur atau kegiatan beserta standard baku dan keterangan yang diperlukan.

Berikut merupakan contoh bagian *flowchart* yang sistematis dan memenuhi standard isi bagan alur yang terdiri dari nomor

kegiata, uraian kegiatan yang berisi langkah-langkah (prosedur), pelaksana yang merupakan pelaku kegiatan, mutu baku yang berisi kelengkapan, waktu, output dan keterangan.

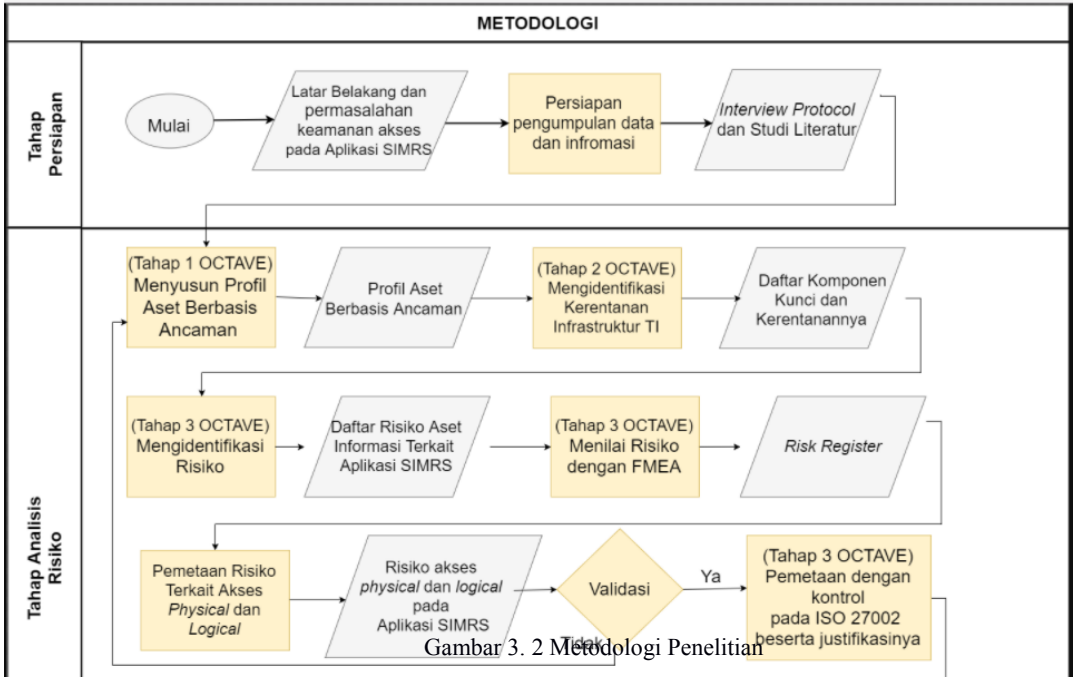


Gambar 2. 7 Contoh Bagan Alut Prosedur [20]

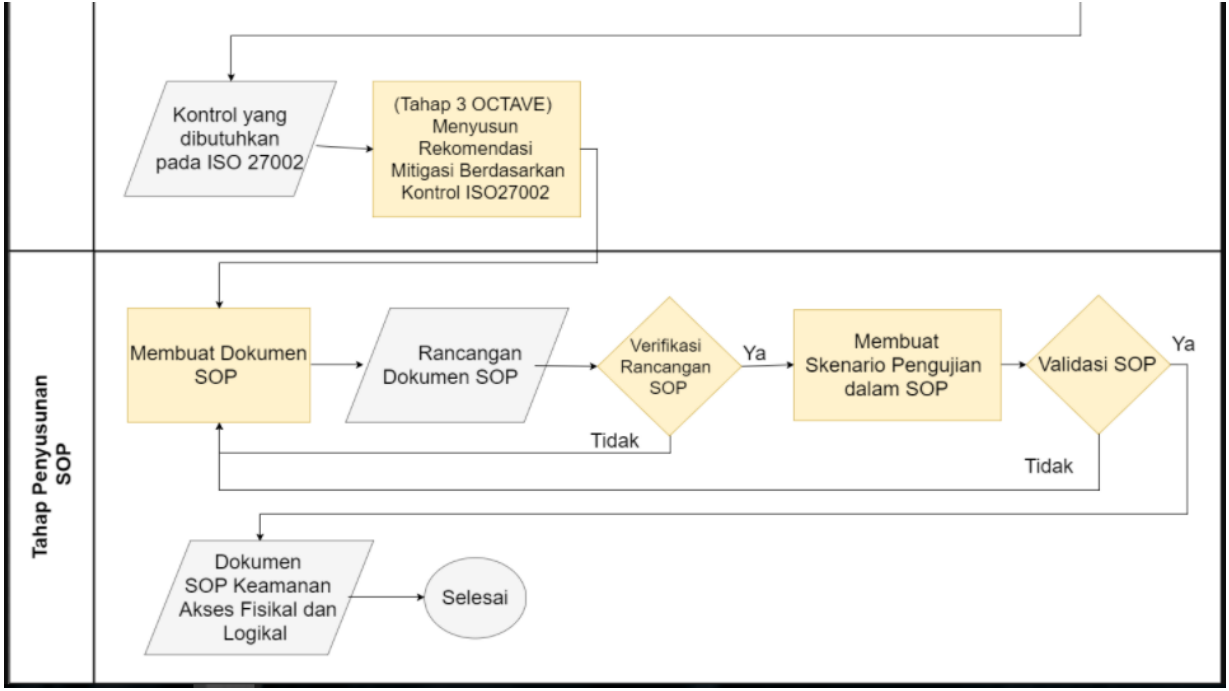
Berdasarkan penjabaran diatas maka dalam penyusunan dokumen SOP terhadap penelitian ini akan digunakan dengan bagan alur untuk menggambarkan alur prosedur yang ada dan disesuaikan pula berdasarkan kriteria dan sturktur atau format yang telah dijelaskan. Dokumen SOP yang akan disusun yaitu dokumen SOP untuk keamanan aset informasi pada kontrol akses *physical* dan *logical*pada Rumah Sakit Dokter Moewardi akan digunakan sebagai prosedur yang telah distandarisasi.

BAB III
METODE PENELITIAN

Gambar 3. 1 Metodologi Penelitian



Gambar 3. 2 Metodologi Penelitian


Kontrol yang dibutuhkan pada ISO 27002
(Tahap 3 OCTAVE) Menyusun Rekomendasi Mitigasi Berdasarkan Kontrol ISO27002
Tahap Penyusunan SOP
Membuat Dokumen SOP
Rancangan Dokumen SOP
Verifikasi Rancangan SOP
Ya
Tidak
Membuat Skenario Pengujian dalam SOP
Validasi SOP
Ya
Tidak
Dokumen SOP Keamanan Akses Fisikal dan Logikal
Selesai

3.1 Tahap Persiapan

Tahap persiapan merupakan langkah awal untuk memulai penyusunan tugas akhir. Masukan dalam tahapan ini adalah permasalahan mengenai keamanan akses *physical* dan *logical* yang ada pada Aplikasi SIMRS. Dimana masukan dari permasalahan yang ada datang dari permintaan manajemen Rumah Sakit Dokter Moewardi, untuk meninjau permasalahan keamanan akses *physical* dan *logical* yang ada di Aplikasi SIMRS. Dalam tahap persiapan dilakukan proses pengumpulan data dan informasi, dimana hasil luaran dari proses tersebut adalah berupa hasil studi literatur dan *interview protocol* yang digunakan sebagai media penggalian risiko keamanan informasi lebih lanjut.

Penyusunan *Interview protocol* didasarkan pada metode OCTAVE yaitu dengan menggali aset kritis, ancaman, kebutuhan keamanan, kerentanan teknologi, kelemahan organisasi dan praktik saat ini yang sudah dilakukan untuk mengamankan akses ke Aplikasi SIMRS yang berhubungan proses identifikasi, autentikasi dan otorisasi. Penggalian informasi dilakukan kepada pihak manajemen Rumah Sakit Dokter Moewardi yaitu kepada Kepala Bagian Perencanaan, Kepala Instalasi Pengelola Data Elektronik dan Database Administrator Aplikasi SIMRS.

3.2 Tahap Analisis Risiko

Tahap analisis risiko dilakukan dengan mengacu pada kerangka kerja OCTAVE dimana penilaian risiko dibantu menggunakan kerangka kerja FMEA. Tahap pada OCTAVE tersebut adalah:

3.2.1 Fase 1 - Membangun Profil Aset Berbasis Ancaman

Fase 1 OCTAVE ini dilakukan dengan mengidentifikasi Aset Kritis, Kebutuhan Keamanan untuk Aset Kritis, Ancaman untuk Aset Kritis, Praktik Keamanan yang telah Dilakukan dan Kelemahan Organisasi. Output yang dihasilkan dari fase ini adalah profil aset berbasis ancaman yaitu berupa tabel aset

kritis, tabel kebutuhan keamanan untuk aset kritis, ancaman untuk aset kritis, praktik keamanan yang sekarang dilakukan dan kelemahan organiisasi.

3.2.2 Fase 2 - Mengidentifikasi kerentanan Infrastruktur TI

Fase 2 OCTAVE ini dilakukan dengan mengidentifikasi komponen utama dari aset kritis dan kerentanan teknologi dari komponen utama. Fase ini dilakukan berdsarkan *Technological View* dari aset kritis. Output fase ini adalah tabel komponen utama dari aset kritis dan tabel kerentanan teknologi yang dimiliki komponen utama tersebut.

3.2.3 Fase 3 - Membangun Perencanaan dan Strategi Keamanan

Pada fase ini dilakukan identifikasi terhadap risiko aset informasi terkait dengan Aplikasi SIMRS terlebih dahulu, kemudian dilakukan penilaian risiko untuk mengetahui tingkat urgensi risiko. Kemudian dilakukan pemetaan risiko yang terkait dengan akses *physical* dan *logical*. Seletah itu dilakukan pemetaan risiko dengan kontrol pada ISO 27002:2013. Pemetaan ini dilakukan dengan tujuan untuk menentukan tujuan kontrol ISO 27002:2013 yang dibutuhkan dalam melakukan mitigasi terhadap risiko. Dalam pemetaan kontrol dengan kerangka kerja ISO 27002:2013 terdapat 2 klausul. Dimana klausul yang digunakan untuk kontrol akses *logical* adalah klausul *9 Access control* yang terdiri dari 4 poin utama yaitu *9.1 Business requirements of access control, 9.2 User access management, 9.3 User responsibilities* dan *9.4 System and application access control.* Sehingga total *Control Objective* yang akan menjadi pertimbangan pada kontrol akses *logical* ada 14 *Control Objective.*

Klausul yang akan digunakan untuk kontrol akses *physical* terdapat pada klausul *11 Physical and environmental security.*

Dimana klausul ini akan dipilih lagi yang berhubungan dengan keamanan akses. Meliputi 2 poin utama yaitu *11.1 Secure areas* dan *11.2 Equipment.* Terdapat 8 *Control Objective* pada kontrol akses *physical* yaitu *11.1.1 Physical security perimeter, 11.1.2 Physical entry controls, 11.1.3 Securing offices, rooms and facilities, 11.2.1 Equipment siting and protection, 11.2.3 Cabling security, 11.2.8 Unattended user equipment dan 11.2.9 Clear desk and clear screen policy.*

Langkah selanjutnya adalah membuat tindakan rekomendasi mitigasi risiko. Rekomendasi mitigasi risiko yang dihasilkan akan didasarkan pada kontrol objektif dan petunjuk pelaksanaan pada *Control Objective* ISO 27002:2013. Selain itu, rekomendasi risiko juga didasarkan identifikasi praktik keamanan yang telah diimplementasikan risiko, hal ini berfungsi untuk memastikan tidak ada redundansi tindakan mitigasi risiko dalam mengelola risiko yang muncul. Dalam rekomendasi mitigasi risiko akan didefinisikan input untuk membuat dokumen *Standard Operating Procedure* (SOP) Kontrol akses pada Aplikasi SIMRS berdasarkan kontrol akses *logical* dan kontrol akses *physical* .

3.3 Tahap Penyusunan SOP

Tahap penyususnan SOP merupakan tahap akhir dari penelitian, luaran dari tahap ini adalah dokumen SOP keamanan aset informasi pada kontrol akses *physical* dan *logical* yang telah terverifikasi dan tervalidasi.

3.3.1 Pembuatan SOP

Berdasarkan kontrol yang dibutuhkan untuk melakukan mitigasi terhadap risiko yang ada akan dilakukan perancangan dokumen SOP yang akan disesuaikan dengan konten dokumen yang sudah divalidasi oleh pihak manajemen Rumah Sakit Dokter Moewardi. Proses selanjutnya adalah verifikasi kepada pemilih risiko untuk menentukan apakah menurut pemilih risiko SOP sudah sesuai dengan kebutuhan kontrol mitigasi risiko.

3.3.2 Pembuatan Skenario Prosedur Dalam SOP

Pada proses ini akan dilakukan pembuatan tahapan pengujian prosedur dalam SOP. Dalam hal ini, skenarioisasi pengujian dibutuhkan untuk memastikan bahwa prosedur yang dikembangkan sesuai dengan kondisi rumah sakit dan dapat diimplementasikan dengan baik. Skenario pengujian akan berisikan seluruh prosedur yang ada, proses pengujiannya, keterangan pihak yang berhubungan dengan prosedur SOP dan hasil dari pengujian serta status untuk menunjukan penerimaan atau ketepatan prosedur. Apabila terdapat kesalahan dalam prosedur maka akan dilakukan kembali perbaikan pada prosedur. Namun jika seluruh prosedur telah sesuai maka akan dilanjutkan pada proses selanjutnya yaitu validasi dokumen SOP.

3.3.3 Verifikasi SOP

Verifikasi bertujuan untuk memastikan produk yang dibuat telah sesuai dengan standar yang telah ditentukan yaitu ISO 27002:2013. Oleh karena itu verifikasi dilakukan dengan melakukan pemetaan keterkaitan antara kontrol pada ISO 27002 dengan aktivitas pada SOP yang dihasilkan.

3.3.4 Validasi SOP

Validasi SOP dilakukan dengan menanyakan langsung dan diskusi hasil SOP yang dibuat dengan pihak-pihak yang terkait dengan SOP tersebut. Setelah dilakukan diskusi maka kemudian peneliti akan merubah SOP atau menyesuaikan SOP berdasarkan rekomendasi pihak terkait namun dengan tetap memperhatikan batasan-batasan yang dianjurkan pada ISO 27002:2013. Validasi dilakukan untuk memastikan dokumen SOP dapat berjalan sesuai dengan kondisi yang ada pada rumah sakit dan untuk menemukan ketidaksesuaian dan kekurangan SOP sehingga dapat dibenahi sesuai dengan kondisi yang ada. Metode yang digunakan adalah dengan pengujian SOP yaitu simulasi SOP dengan pelaksanan SOP.

BAB IV
PERANCANGAN

Bab ini menjelaskan tentang perancangan konseptual dalam pengerjaan tugas akhir ini, yaitu perancangan secara detail dari setiap tahapan pengerjaan yang telah dijerlaskan pada Bab III.

4.1 Subjek dan Objek Penelitian

Menurut Arikunto, subjek penelitian adalah subjek yang diteliti oleh peneliti [21]. Menurut penjelasan tersebut, dapat diketahui bahwa subjek penelitian dapat berupa individu, organisasi, atau hal-hal yang dapat dijadikan sebagai sumber penggalian data informasi penelitian. Pada tugas akhir ini yang menjadi subjek penelitian adalah Instalasi Pengelola Data Elektronik (IPDE), lembaga yang memiliki tanggung jawab untuk menjaga dan mengelola keamanan akses pada Aplikasi SIMRS.

Selanjutnya, objek penelitian adalah sesuatu hal yang menjadi perhatian dalam sebuah penelitian [21]. Dari penjelasan tersebut, dapat diketahui bahwa objek penelitian adalah variabel dalam sebuah penelitian. Objek dari penelitian tugas akhir ini adalah keamanan akses pada Aplikasi SIMRS. Objek tersebut akan digunakan untuk proses penggalian risiko keamanan akses berdasarkan kontrol akses *physical* dan *logical* pada setiap aset yang dimiliki oleh Aplikasi SIMRS.

1.1.1 Rumah Sakit Dokter Moewardi

- **Profil Singkat**

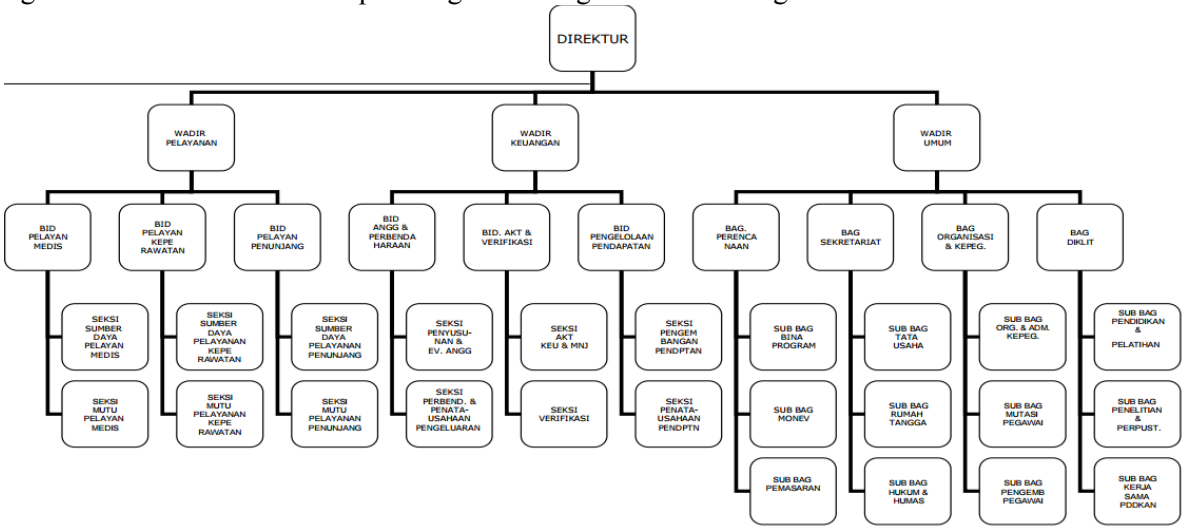
  Rumah Sakit Umum Daerah Dokter Moewardi Surakarta adalah rumah sakit negeri kelas A. Rumah sakit ini mampu memberikan pelayanan kedokteran spesialis dan subspesialis luas oleh pemerintah ditetapkan sebagai rujukan tertinggi atau disebut pula

sebagai rumah sakit pusat. Visi Rumah Sakit Dokter Moewardi adalah "Menjadi Rumah Sakit Terkemuka Berkelas Dunia". Misi Rumah Sakit ini adalah "Menyediakan pelayanan kesehatan berbasis pada keuanggulan sumbaer daya manusia, kecanggihan dan kecukupan alat serta profesionalisme manajemen pelayanan" dan "Menyediakan wahana pendidikan danpelatihan kesehatan unggul berbasis pada perkembangan ilmu pengetahuan dan teknologi kesehatan yang bersinergi dengan mutu pelayanan". Rumah Sakit ini telah terakreditasi ISO 9001:2008 sejak tahun 2007 dan ISO 22000:2005 sejak tahun 2014.

Pada tahun 2015 Rumah Sakit ini memiliki 2.065 tenaga kerja yang terdiri dari tenaga medis yang terdiri dari dokter umum dan spesialis; paramedis perawatan; paramedis non-perawatan yang terdiri dari kefarmasian, kesehatan masyarakat, gizi, ketrampilan fisik dan ketrampilan medis; dan non medis. Rumah sakit ini memiliki 676 kamar inap dan terdiri dari pelayanan Instalasi Gawat Darurat, Instalasi Rawat Jalan, Poliklinik Spesialis dan Sub-spesialis.

- **Struktur Organisasi**

  Funsional bisnis dalam Rumah Sakit Dokter Moewardi secara umum digambarkan dalam sebuah struktur organisasi, susunan fungsional tersebut terdiri dari Direktur yang dibantu oleh tiga Wakil Direktur dan 10 Kepala Bagian/Bidang serta 24 sub bagian/seksi.



Gambar 4. 1 Struktur Organisasi Rumah Sakit Dokter Moewardi

Berikut adalah keterangan bagan struktur organisasi Rumah Sakit Dokter Moewardi Surakarta:

1. Direktur
2. Wakil Direktur Pelayanan
3. Wakil Direktur Keuangan
4. Wakil Direktur Umum
5. Bidang Pelayanan Medis, membawahkan :
   a) Seksi Sumber Daya Pelayanan Medis
   b) Seksi Mutu Pelayanan Medis
6. Bidang Pelayanan Keperawatan, membawahkan :
   a) Seksi Sumber Daya Pelayanan Keperawatan
   b) Seksi Mutu Pelayanan Keperawatan
7. Bidang Pelayanan penunjang, membawahkan :
   a) Seksi Sumber Daya Pelayanan Penunjang
   b) Seksi Mutu Pelayanan Penunjang
8. Bidang Anggaran & Perbendaharaan, membawahkan;
   a) Seksi Penyusunan dan Evaluasi Anggaran
   b) Seksi Perbendaharaan & Penata Usahaan Pengeluaran
9. Bidang Akuntansi & Verifikasi, membawahkan;
   a) Seksi Akuntansi Keuangan dan Manajemen
   b) Seksi Verifikasi
10. Bidang Pengelolaan Pendapatan, membawahkan;
    a) Seksi Pengembangan Pendapatan
    b) Seksi Penatausahaan Pendapatan
11. Bagian Perencanaan, membawahkan;
    a) Sub Bagian Bina Program
    b) Sub Bagian Monitoring dan evaluasi
    c) Sub Bagian Pemasaran

Subjek penelitian ini adalah Instalasi Pengelola Data Elektronik (IPDE) yang dalah struktur fungsional merupakan tanggungjawab Wakil Direktur Umum dan berada dibawah Bagian Perencanaan. Wakil Direktur Umum, mempunyai tugas mengkoordinasikan perumusan kebijakan teknis, pelaksanaan dan pelayanan administrasi dan teknis di bidang perencanaan program dan monitoring evaluasi, kesekretariatan, organisasi

dan kepegawaian, dan pendidikan dan pelatihan. Bagian-bagian yang secara struktur organisatoris berada di bawah Wakil Direktur Umum mempunyai Tugas sebagai berikut :

1. Bagian Perencanaan, mempunyai tugas melaksanakan penyiapan perumusan kebijakan teknis, pelaksanaan dan pelayanan administrasi dan teknis di bidang bina program, monitoring dan evaluasi, dan pemasaran.
2. Bagian Sekretariat, mempunyai tugas melaksanakan penyiapan perumusan kebijakan teknis, pelaksanaan dan pelayanan administrasi dan teknis di bidang tata usaha, rumah tangga, dan hukum dan hubungan masyarakat.
3. Bagian Organisasi Dan Kepegawaian, mempunyai tugas melaksanakan penyiapan perumusan kebijakan teknis, pelaksanaan dan pelayanan administrasi dan teknis di bidang organisasi dan administrasi pegawai, mutasi pegawai dan pengembangan pegawai.
4. Bagian Pendidikan Dan Penelitian, mempunyai tugas melaksanakan penyiapan perumusan kebijakan teknis, pelaksanaan dan pelayanan administrasi dan teknis di bidang pendidikan dan pelatihan, penelitian dan perpustakaan, dan kerjasama pendidikan.

1.1.1.1 Instalasi Pengelola Data Elektronik

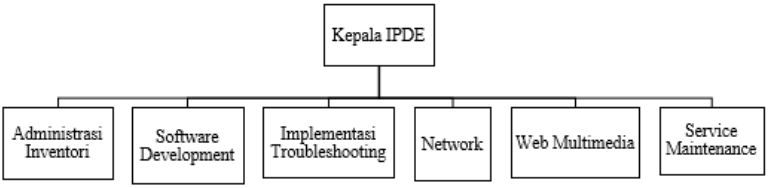
Instalasi Pengelola Data Elektronik pada Rumah Sakit Dokter Moewardi dikepalai oleh R. Satrio Budi Susilo, dr., Sp. PD., M.Kes. Instalasi ini bertugas untuk melakukan perencanaan, pengelolaan dan evaluasi Sistem Informasi Manajemen Rumah Sakit dalam rangka untuk mendukung pelayanan. IPDE berkoordinasi dengan kepala bagian pelayanan penunjang untuk menunjang pelayanan medis dengan implementasi teknologi infomasi.

Jenis pelayanan yang dilakukan oleh IPDE antara lain:

- Penyedia aplikasi Sistem Informasi Rumah Sakit
- Mengelola SIMRS baik pembaharuan, perubahan atau penambahan

- Mengelola Instalasi, servis dan *maintenance* pada *hardware*
- Mengalola jaringan SIMRS
- Menyiapkan dan menjaga kelangsungan Web RS

Berikut dibawah merupakan gambaran struktur organisasi dari IPDE:



Gambar 4. 2 Struktur Organisasi Instalasi Pengelola Data Elektronik

Berikut dibawah merupakan tugas pokok dan fungsi dari masing-masing sub-bagian pada IPDE

Tabel 4. 1 Tugas Pokok dan Fungsi Instalasi Pengelola Data Elektronik

No	Nama Jabatan	Uraian Tugas
1.	Kepala Instalasi	1. Memfasilitasi penyelenggaraan pendukung pelayanan kesehatan dalam bidang pengelolaan data elektronik dan teknologi informasi sesuai dengan standar yang sudah ditetapkan melalui pengelolaan sumber daya yang tersedia secara efektif, efisien dan produktif. 2. Menyusun rencana dan program kerja. 3. Mengelola dan memberdayakan semua sumber daya di Instalasi dalam rangka untuk mningkatkan mutu pelayanan dan cakupan pelayanan. 4. Memenuhi target, sasaran dan tujuan sesuai rencana kerja.

		5. Mengembangakan dan memajukan kemampuan instalasi dalam pelayanan pengelolaan data elektronik dan teknologi informasi. 6. Menyusun, melaksanakan dan mengevaluasi standar pelayanan atau dukungan pelayanan yang berlaku di Internal Instalasi. 7. Melakukan evaluasi terhadap pelaksanaan kegiatan. 8. Mengatasi masalah yang menghambat pelayanan atau dukungan pelayanan serta penyelenggaraan tugas instalasi. 9. Menjamin tersedianya fasilitas secara proporsional sesuai kebutuhan pelayanan atau dukungan pelayanan. 10. Melaporkan secara lisan atau tertulis tugas dan kegiatan kepada Kepala Bagian Perencanaan.
2.	Pengembangan Software	1. Bertanggungjawab atas operasional/pemeliharaan perangkat lunak (software) komputer, keamanan data dan backup data. 2. Melakukan instalasi dan pengaturan perangkat lunak (software) agar bisa digunakan dengan lancar oleh user. 3. Melakukan pemeliharaan perangkat lunak yang telah selesai dibuat dan melakukan perubahan atau penambahan sesuai dengan kebutuhan user. 4. Mengembangkan software yang sesuai dengan kebutuhan RSDM. 5. Melaksanakan tugas lain yang diberikan oleh pimpinan.
3.	Web dan Multimedia	1. Mendesain dan memelihara website RSDM.

		2. Mengembangkan aplikasi multimedia sesuai kebutuhan. 3. Melaksanakan tugas lain yang diberikan oleh pimpinan.
4.	Servis dan Pemeliharaan	1. Bertanggungjawab menangani : instalasi komputer baru, servis komputer dan pemeliharaan komputer. 2. Melaksanakan tugas lain yang diberikan oleh pimpinan
5.	Implementasi dan Troubleshooting	1. Melakukan supervisi terhadap implementasi aplikasi baru. 2. Menjawab dan mengelola permasalahan pelanggan. 3. Melaksanakan tugas lain yang diberikan oleh pimpinan.
6.	Jaringan	1. Bertanggungjawab untuk merancang, memasang kabel, memasang koneksi terhadap jaringan baik internet dan intranet. 2. Mengelola, memelihara dan memastikan koneksi jaringan berjalan lancar dan aman. 3. Melaksanakan tugas lain yang diberikan oleh pimpinan.
7.	Administrasi dan Inventori	1. Menyusun laporan, arsip, surat menyurat dan desai pemeliharaan 2. Bertanggungjawab terhadap inventaris perangkat keras/lunak IPDE 3. Melaksanakan tugas lain yang diperintahkan oleh atasan.

4.2 Persiapan Penggalian Data

Pengumpulan data yang dilakukan dalam penelitian bertujuan untuk mengidentifikasi dan menganalisa risiko yang berkaitan dengan keamanan akses pada aplikasi Sistem Informasi Rumah Sakit. Dalam melakukan pengumpulan data dilakukan

wawancara dengan sumber informasi yang dibutuhkan dan observasi proses yang ada saat ini.

4.2.1 Wawancara

Wawancara dilakukan untuk melakukan penggalian data secara langsung ke narasumber yang dituju. Sebelum melakukan wawancara, maka diperlukan pembuatan *interview protocol*. Hal ini dilakukan sebagai acuan dalam penggalian data kepada nasumber agar data dan informasi yang didapatkan sesuai dengan yang dibutuhkan.

Tabel 4. 2 Proses dan Pengumpulan Data

Nama Proses	Pengumpulan Data dan Informassi
Teknik	Wawancara Wawancara sebuah kegiatan penggalian informasi melalui percakapan secara langsung kepada pihak yang berkaitan dengan objek penelitian. Wawancara umumnya menggunakan format Tanya jawab yang terencana. Dalam penelitian ini, jenis wawancara yang digunakan adalah wawancara terstruktur, yaitu dengan mempersiapkan pertanyaan .
Objek	Keamanan akses berdasarkan kontrol akses *physical* dan *logical* pada aset aplikasi Sistem Informasi Rumah Sakit.
Kebutuhan proses	*Interview protocol*
Strategi pelaksanaan	Untuk mengumpulkan data melalui wawancara perlu dirumuskan strategi pelaksanaan agar pada saat wawancara berlangsung tidak ditemui hambatan. Strategi tersebut dapat berupa urutan tahapan yang akan dilakukan untuk memperisapkan wawancara. Tahapan wawancara tresebut adalah sebagai berikut : • Menetapkan tujuan wawancara • Membuat Interview Protocol • Menentukan narasumber

4.2.1.1 Tujuan Wawancara

Tujuan wawancara ditetapkan untuk menjadi acuan dalam perumusan pertanyaan wawancara, sehingga proses penggalian data dapat berjalan sesuai dengan tujuan yang diinginkan dan mendapatkan data serta informasi yang dibutukan dalam penelitian.

Tabel 4. 3 Tujuan Wawancara

No	Narasumber	Tujuan Wawancara
1	Kepala Bagian Perencanaan	• Memahami alur koordinasi terkait Aplikasi SIMRS • Mengetahui aset kritis terkait SIMRS • Mengetahui ancaman yang pernah terjadi • Mengetahui kebutuhan keamanan pada masing-masing aset
2	Kepala Instalasi Pengelola Data Elektronik	• Mengetahui alur koordinasi kerja IPDE • Mengetahui aset kritis terkait SIMRS • Mengetahui ancaman yang pernah terjadi • Mengetahui kebutuhan keamanan pada masing-masing aset • Mengetahui praktik keamanan terkini
3	Database Administrator	• Mengetahui alur koordinasi kerja IPDE • Mengetahui aset kritis terkait SIMRS • Mengetahui ancaman yang pernah terjadi • Mengetahui kebutuhan keamanan pada masing-masing aset Mengetahui praktik keamanan terkini

4.2.1.2 Menentukan Narasumber

Penentuan narasumber dilakukan untuk memudahkan proses pengumpulan data. Dalam penetapan pihak narasumber, yang harus diperahtikan adalah kapasitas objek dalam kewenangannya memberi informasi yang valid, dan apakah pertanyaan yang dirumuskan relevan dengan pengetahuan pihak narasumber. Berikut adalah profil narasumber dalam penelitian.

Tabel 4. 4 Narasumber Wawancara

Nama	Jabatan
Drs. Wido	Kepala Bagian Perencanaan
R.Satrio Budi Susilo, dr., Sp.PD., M.Kes	Kepala Instalasi Pengelola Data Elektronik (IPDE)
Aris Andriyanto, S.Kom	Staff Pengolahan Data Elektronik/ Database Administrator

4.2.2 Observasi

Observasi langsung dilakukan untuk mengamati objek penelitian secara langsung di lapangan. Metode observasi ini bertujuan untuk mendapatkan informasi mengenai kondisi nyata yang terjadi pada kontrol akses Aplikasi SIMRS. Dengan adanya metode ini penulis dapat mempelajari proses kerja yang tidak bisa didapatkan melalui komunikasi, sehingga penulis dapat melakukan pencatatan terhadap hasil pengamatan tersebut.

4.3 Perancangan Analisis Risiko Berdasarkan OCTAVE

Berikut adalah perancangan identifikasi risiko berdasarkan OCTAVE.

4.3.1 Perancangan Profil Aset Berbasis Ancaman dan Kerentanan TI

Profil aset berbasis ancaman dan kerentanan TI ini disusun dengan menggunakan acuan metode OCTAVE *(Operationally Critical Threat, Asset, and Vulnerability Evaluation*). Penyusunan Profil Aset ini didasarkan pada data hasil

interview protocol pada pihak Wakil Direktur Umum, Kepala Bagian Perencanaan dan Kepala IPDE. Profil aset ini akan disusun dengan mempertimbangkan *organizational view* dan *technologycal view* dari aplikasi Sistem Informasi Rumah Sakit (SIMRS) milik Rumah Sakit Dokter Moewardi. Menurut OCTAVE profil aset tersebut disusun berdasarkan:

- Identifikasi Aset Kritis
- Identifikasi Kebutuhan Keamanan Aset Kritis
- Identifikasi Ancaman Aset Kritis
- Identifikasi Praktik Kemanan yang Telah Diterapkan
- Identifikasi Kelemahan Organisasi
- Identifikasi Kompone Kunci
- Identifikasi Kerentanan Infrastruktur TI

4.3.2 Perancangan *Risk Register*

Berdasarkan informasi yang didapat dari penggalian data pada profil aset berbasis ancaman dan kerentanan TI yang sudah didapatkan dari masing-masing aset kritis pada aplikasi SIMRS, kemudian dilakukan penggalian risiko yang difokuskan pada akses *physical* dan *logical* dari proses identifikasi, autentikasi dan otorisasi. Setelah dilakukan identifikasi risiko kemudian dilakukan penilaian risiko dengan menggunakan metode FMEA untuk mengetahui kategori risiko apakah termasuk risiko dengan kategori *very high, high, medium, low* atau *very low.* Pengkategorian risiko diperlukan untuk mengetahui jenis kategori risiko pada masing-masing risiko kontrol akses yang didapatkan.

4.3.3 Pemetaan Risiko dengan Kontrol ISO27002:2013

Setiap risiko yang telah diperolah dari tahap identifikasi risiko akan ditentukan kontrolnya berdasarkan acuan standar pada ISO/IEC 27002:2013. Pemetaan ini dilakukan dengan tujuan untuk menentukan tujuan kontrol berdasarkan acuan ISO27002:2013 yang dibutuhkan dalam melakukan mitigasi terhadap risiko.

Tabel 4. 5 Perencanaan Pemetaan risiko dengan kontrol

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Jenis Risiko	Pemilik Risiko	Risiko	Potensi Penyebab kegagalan	Kontrol pada ISO27002:2013		Justifikasi
							Kontrol	*Control Objective*	

Setelah pemetaan kontrol dengan ISO27002:2013 dilakukan, risiko-risiko dengan pemilik adalah IPDE akan dibuat daftar rekomendasi mitigasi risiko. Hal tersebut dikarenakan fokus pada penelitian ini adalah pembuatan SOP yang ditujukan untuk pihak IPDE sebagai pihak penyedia layanan aplikasi SIMRS agar dapat menjadi panduan dalam proses mengamankan akses aplikasi. Hasil rekomendasi mitigasi risiko inilah yang akan menjadi bahan pertimbangan untuk usulan perancangan prosedur.

4.3.4 Rekomendasi Mitigasi Risiko

Risiko-risiko milik IPDE yang sudah ditentukan kontrolnya pada standar ISO27002:2013 kemudian ditentukan tindakan rekomendasi mitigasinya sesuai dengan petunjuk pelaksanaan pada standar. Rekomendai mitigasi risiko ini juga mempertimbangkan praktik kontrol yang sudah diterapkan sehingga dapat menjadi pertimbangan untuk prosedur yang perlu dihasilkan. Luaran yang didapatkan dari penentuan mitigasi risiko adalah identifikasi sebuah prosedur yang diperlukan untuk memastikan risiko tidak berulang. Berikut ini adalah tabel rekomendasi mitigasi risiko.

Tabel 4. 6 Perencanaan tabe rekomendasi risiko

Kategori Aset Informasi Kritis	Aset Informasi Kritis	ID Risiko	Jenis Risiko	Risiko	Tindakan Mitigasi Risiko Berdasarkan ISO27002:2013			Rekomendai Mitigasi Risiko	Prosedur yang dihasilkan
					Kontrol	*Control Objective*	Petunjuk Pelaksanaan berdasarkan kontrol		

4.5 Perancangan SOP

Dalam menyusun dokumen SOP, tidak terdapat suatu format baku yang dapat menjadi acuan, hal tersebut dikarenakan SOP merupakan dokumen internal yang kebiijakan pembuatannya disesuaikan dengan kebutuhan masing masing organisasi, begitu pula dengan penyunan format dari dokumen SOP tersebut. Format langkah-langkah dalam SOP penelitian ini dibuat dalam bentuk *flowchart* untuk memudahkan penggambaran alur aktivitas.

Perancangan format SOP akan dikembangkan mengacu pada peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia mengenai pedoman penyusunan standar operasional prosedur nomor 35 tahun 2012. Berdasarkan panduan tersebut, berikut penjelasan struktur dan konten yang akan dimasukkan dalam dokumen SOP penelitian.

Tabel 4. 7 Perancangan SOP

Struktur Bab	Sub-Bab	Deskripsi
Pendahuluan	Tujuan	Penjelasan mengenai tujuan dari pembuatan dokumen Standar Operasional Prosedur keamanan akses pada aplikasi SIMRS.
	Ruang Lingkup	Penjelasan mengenai ruang lingkup dokumen SOP yang dibuat.
	Overview kontrol akses	Berisi penjelasan singkat mengenai kontrol akses logikla dan *physical* , beserta proses

Struktur Bab	Sub-Bab	Deskripsi
		identifikasi, autentikasi, otorisasi dan akuntabilitas.
	Hasil Identifikias Risiko	Berisikan penjelasan dan hasil dari identifikasi risiko akses *physical* dan *logical* aplikasi SIMRS yang pemiliknya merupakan pihak IPDE.
Prosedur	Definisi	Merupakan pendefinisian tujuan, ruang lingkup, referensi kontrol dan pendefinisian istilah lain yang terkait dalam prosedur yang dibuat.
	SOP	Penjelasan mengenai langkah-langkah dalam menjalankan suatu proses. Prosedur dalam penelitian ini digambarkan dengan *flowchart.*
	Formulir	Semua formulir yang diperlukan untuk menjalankan prosedur akan dijelaskan cara penggunaannya.

4.6 Perancangan Pengujian SOP

Pengujian SOP dilakukan melalui dua cara yakni verifikasi dan validasi.

4.6.1 Verifikasi

Verifikasi bertujuan untuk memastikan produk yang dibuat telah sesuai dengan standar yang telah ditentukan yaitu ISO 27002:2013. Oleh karena itu verifikasi dilakukan dengan melakukan pemetaan keterkaitan antara kontrol pada ISO 27002 dengan aktivitas pada SOP yang dihasilkan.

4.6.2 Validasi

Validasi merupakan tahap pengujian untuk memastikan bahwa dokumen SOP yang dibuat telah sesuai dengan kebutuhan dan

kondisi nyata yang ada di Rumah Sakit Dokter Moewardi. Validasi dilakukan dengan dua tahap. Pada tahap awal validasi dilakukan konfirmasi melalui diskusi dengan pihak IPDE setelah itu dilakukan simulasi aktivitas-aktivitas pada SOP beserta pengisian formulir untuk memastikan bahwa SOP sudah sesuai dengan kondisi nyata yang ada di IPDE.

- Konfirmasi

Konfirmasi adalah aktivitas memastikan kebenaran mengenai suatu data dan informasi yang dimiliki. Konfirmasi yang dilakukan adalah *expert review* berupa diskusi dengan pihak internal IPDE.

Tabel 4. 8 Perancangan Konfirmasi

Konfirmasi	Uraian
Tujuan	Mengkonfirmasi dokumen *Standard Operating Procedure* kontrol akses Aplikasi SIMRS untuk memastikan tentang kebenaran dari informasi yang termuat dalam dokumen SOP telah sesuai dengan kebutuhan Instalasi Pengelola Data Elektronik (IPDE).
Metode	Wawancara dengan IPDE sebagai pihak yang memiliki kewenangan dalam mengelola keamanan akses aplikasi SIMRS.
Sasaran	*Key User (*pihak yang memiliki kedudukan penting dalam bagian IPDE dan memiliki kewenangan untuk mendefinisikan kebutuhan keamanan akses aplikasi SIMRS) yaitu Kepala IPDE.
Tahap Pengujian	• Penulis menyerahkan dokumen SOP kepada pihak IPDE dan menjelaskan isi dokumen dengan detil. • Pihak IPDE melakukan review dokumen SOP. • Penulis mengadakan wawancara secara langsung setelah pihak IPDE selesai mereview dokumen. Pertanyaan yang dilontarkan terkait struktur SOP, konten SOP, serta istilah yang digunakan dalam SOP. • Pihak IPDE memberikan review dan revisi dokumen jika ada.

	• Penulis melakukan pembenahan dokumen SOP sesuai saran dari pihak IPDE. • Penulis menyerahkan ulang hasil revisi pada pihak IPDE. • Pihak IPDE menyetujui dokumen SOP yang telah diperbaiki.

- Simulasi

Simulasi adalah aktivitas memastikan kesesuaian data dan informasi yang dimiliki dengan cara melakukan sebuat pengujian atau simulasi. Simulasi SOP dilakukan oleh semua pihak yan terkait dengan SOP dengan melakukan seluruh aktivitas yang ada pada SOP hingga mengisi formulir-formulir untuk pendokumentasian aktivitas.

Tabel 4. 9 Tabel Perancangan Simulasi

Simulasi	Uraian
Tujuan	Simulasi dilakukan untuk memastikan dokumen SOP dapat berjalan sesuai dengan kondisi yang ada pada IPDE dan untuk menemukan ketidaksesuaian dan kekurangan SOP sehingga dapat dibenahi sesuai kondisi yang ada.
Metode	Simulasi SOP dengan pelaksana SOP yaitu pihak internal IPDE.
Sasaran	Pelaksana SOP, yakni pegawai internal IPDE.
Tahap Pengujian	• Peneliti menyerahkan dokumen SOP yang telah diperbaiki pada tahap verifikasi dan konfrmasi. • Peneliti memberikan arahan penggunaan dokumen SOP dan menjelaskan beberapa skenario yang akan diuji. • Pelaksana mensimulasikan SOP, termasuk mengisi form-form yang tersedia. • Setelah simulasi selesai, peneliti meminta *feedback* dan *review* dari pelaksana. • Peneliti melakukan perbaikan dokumen jika terdapat ketidaksesuaian pada proses simulasi. • Setelah selesai, dokumen SOP dapat dinyatakan valid dan dapat diterapkan.

Halaman ini sengaja dikosongkan.

BAB V
IMPLEMENTASI

Bab ini menjelaskan tentang hasil implementasi yang telah didapatkan dari proses perancangan pada bab IV yang telah dipaparkan sebelumnya.

5.1 Proses Pengumpulan Data

Pengumpulan data yang dilakukan dalam penelitian bertujuan untuk mengidentifikasi risiko yang berkaitan dengan kontrol akses yang bersifat *logical* maupun *physical* pada akses ke Aplikasi SIMRS Rumah Sakit Dokter Moewardi. Pengumpulan data dilakukan dengan wawancara menggunakan *interview protocol* kepada tiga narasumber yaitu Kepala Bagian Perencanaan, Kepala IPDE dan Staff Pengolahan Data Elektronik. Hasil dan rincian dari wawancara dapat dilihat pada Lampiran A. Berikut adalah hasil identifikasi risiko yang dapat ditarik dari hasil wawancara mengenai keamanan informasi pada Aplikasi SIMRS.

5.2 Proses Analisis Risiko berdasarkan OCTAVE

Penggalian analisis risiko dilakukan dari hasil wawancara yang telah dilakukan sebelumnya. Proses analisis risiko dilakukan berdasarkan metode OCTAVE, yaitu:

Tabel 5. 1 Fase Penelitian OCTAVE

Fase	Output
Fase 1 – Membangun Aset Berbasis Profil Ancaman	Daftar Aset Kritis
	Daftar Kebutuhan Keamanan untuk Aset Kritis
	Daftar Ancaman untuk Aset Kritis
	Daftar Praktik Keamanan yang telah Dilakukan
	Daftar Kelemahan Organisasi
Fase 2 – Mengidentifikasi	Daftar Komponen Utama
	Daftar Kerentanan Teknologi

kelemahan	
Fase 3 – Membangun Perencanaan dan Strategi Keamanan	Daftar Risiko untuk Aset Kritis
	Pengukuran Risiko
	Strategi Proteksi
	Rencana-Rencana Penguranga Mitigasi Risiko

5.2.1 Fase 1 - Membangun Profil Aset Berbasis Ancaman

Pada fase ini akan dilakukan identifikai aset dan ancaman berbasis aset degan menggunakan informasi yang didapat dari senior manajemen, bagian operasional dan karyawan. Hal ini diperlukan agar nantinya didapatkan suatu profil aset yang lengkap dari sisi manajemen maupun dari sisi teknis. Diharapkan nantinya analisis ini dapat melihat aset mana yang dianggap kritis dan apa saja langkah proteksi yang saat ini telah dilakukan. Selain itu organisasi nantinya juga dapat melihat apakah masing-masing aset kritis telah memiliki tingkat keamanan sesuai dengan kebutuhanya.

Output yang dihasilkan dari fase ini nantinya adalah tabel aset kritis, tabel kebutuhan keamanan untuk aset kritis, ancaman untuk aset kritis, praktik keamanan yang sekarang dilakukan dan kelemahan organiisasi.

Untuk dapat membangun profil ancaman berbasis aset terlebih dahulu organisasi perlu mengidentifikasi aset kritis TI. Aset Kritis ini merupakan suatu barang yang memberikan nilai (value) tinggi untuk organisasi dalam melakukan proses bisnisnya. Selain itu, identifikasi aset kritis juga dilihat dari apabila tanpa adanya aset ini, proses bisnis pada Aplikasi SIMRS yang ada di RS Dokter Moewardi tidak dapat berjalan dengan lancar dan dalam kondisi normal.

5.2.1.1 Identifikasi Aset Informasi Terkait Aplikasi SIMRS

Penentuan aset infromasi ini didapat dari hasil observasi langsung dan wawancara dengan ketiga narasumber yaitu pihak manajemen yang berkaitan langsung dengan Aplikasi SIMRS yaitu Kepala Bagian Perencanaan, pihak operasional yaitu Kepala IPDE dan staff dari IPDE yang merupakan salah satu admin *database* pada Aplikasi SIMRS yang dapat dilihat pada Lampiran A. Hasil identifikasi ini kemudian dipaparkan kepada narasumber yaitu Kepala IPDE untuk divalidasi agar peneliti dapat memastikan bahwa hasil yang didapat sudah sesuai dengan kondisi yang ada saat ini.

Tabel 5. 2 Daftar Aset Informasi Terkait Aplikasi SIMRS

Kategori Aset	Deskripsi
Manusia	Manusia pada Aplikasi SIMRS Rumah Sakit Dokter Moewardi menurut fungsional bisnis serta hak aksesnya pada Aplikasi SIMRS dikategorikan menjadi 3 level, yaitu: • Admin Admin pada Aplikasi SIMRS merupakan pihak Instalasi Pengelola Data Elektronik (IPDE) yang mempunyai wewenang untuk mengelola hak akses serta melakukan perubahan pada aplikasi. Pihak yang dapat mengakses panel admin antara lain adalah programer, database administrator dan bagian troubleshooting. Admin berhak mengubah, menambah atau menghapus hak akses user berdasarkan surat terkait permintaan hak akses dan keputusan Kepala IPDE sendiri. • Supervisor Supervisor pada Aplikasi SIMRS berisi pihak eksekutif Rumah Sakit Dokter Moewardi seperti Kepala Bagian, Kepala Instalasi, Direktur, Wakil Direktur, Kepala Bangsal, Kelapa Poli dan lain-lain. Supervisor merupakan pihak yang bertugas

	melakukan monitoring kinerja serta pihak yang bertugas menentukan keputusan berdasarkan hasil analisis data pada Aplikasi SIMRS. • User User pada Aplikasi SIMRS dapat dikategorikan menjadi 3 yaitu dokter spesialis, non-dokter dan residen (mahasiswa kedokteran). User berfungsi untuk memodifikasi, menambah, membaca atau menghapus data pada Aplikasi SIMRS sesuai dengan role hak aksesnya. Masing-masing user tersebut memiliki prosedur atau alur yang berbeda dalam mengajukan perubahan ataupun pengajuan hak akses pada Aplikasi SIMRS.
Hardware	Berdasarkan hasil wawancara dengan Kepala dan Staff pada Instalasi Pengelola Data Elektronik, *hardware* atau perangkat keras yang berkaitan dengan objek penelitian yaitu Aplikasi SIMRS adalah server, *Personal Computer* (PC) dan *Uninterruptible Power Supply* (UPS). Berikut dibawah penjelasan masing-masing perangkat keras tersebut. • Server Server berfungsi sebagai tempat menyimpan data-data yang ada pada Aplikasi SIMRS. Server tersebut berada didalam ruang server khusus yang telah memiliki kunci yang menggunakan *barcode,* prosedur akses masuk, formulir akses masuk dan acuan serta peralatan keamanan fisik. • Personal Computer (PC) Saat ini, pengguna Aplikasi SIMRS hanya dapat mengakses aplikasi lewat PC yang ada didalam Rumah Sakit yang terhubung dengan jaringan LAN. PC ini terdapat dibeberapa tempat seperti bangsal, poli ataupun kantor unit. PC ini memiliki perlindungan fisik berupa kunci almari

	tempat CPU diletakkan. Terdapat beberapa PC yang digunakan untuk beberapa pengguna. Terdapat sekitar 600 PC yang dimiliki oleh Rumah Sakit. • Uninterruptible Power Supply (UPC) UPS merupakan alat yang berfungsi sebagai penyedia sumber listrik cadangan apabila sumber listrik utama mati atau mengalami gangguan. UPS saat ini akan otomatis menyala dalam waktu 3-4 detik setelah sumber listrik utama mati atau mengalami gangguan. UPS saat ini mampu menyediakan sumber listrik cadangan selama 3-4 jam. • CCTV CCTV digunakan untuk memantau aktifitas yang ada di dalam gedung Rumah Sakit. CCTV dikelola oleh bagian pusat keamanan RSDM dan telah dilakukan monitoring terus-menerus. Data yang tersimpan dalam CCTV juga telah di simpan dan dibackup. • Printer Printer digunakan untuk mencetak hasil dokumen dari elektronik ke dokumen non-elektronik. Printer secara tidak langsung berhubungan dengan Aplikasi SIMRS. • Telepon Telepon pada RSDM digunakan sebagai media telekomunikasi yang paling sering digunakan. Pada IPDE sendiri telepon digunakan untuk membantu permasalahan user terkait IT ataupun Aplikasi SIMRS sendiri
Software	Software atau perangkat lunak yang terkait Aplikasi SIMRS selain aplikasi itu sendiri adalah *Operating System* yang terdapat pada PC untuk mengakses aplikasi. • Aplikasi SIMRS Aplikasi SIMRS pada Rumah Sakit Dokter

	Moewardi memiliki beberapa modul antara lain modul admission, transaksi, farmasi, billing, penagihan, jasa pelayanan, inventory, rekam medis, informasi eksekutif dan utility. Setiap user ataupun supervisor memiliki *interface* modul yang berbeda-beda tergantung pada role hak aksesnya. Saat ini Aplikasi SIMRS telah memiliki prosedur penambahan, perubahan dan penghapusan hak akses. Aplikasi ini juga telah memiliki beberapa kebijakan terkait keamanan dan penggunaan. • Operating System (OS) OS yang telah digunakan pada PC untuk mengakses Aplikasi SIMRS saat ini adalah windows, dimana pada OS telah diinstall antivirus yang terhubung dengan jaringan dan secara rutin dipantau oleh petugas IPDE.
Jaringan	Saat ini Aplikasi SIMRS diakses lewat jaringan *Local Area Network* (LAN) Rumah Sakit. Berdasarkan hasil wawancara komponen jaringan terkait dengan Aplikasi SIMRS Rumah Sakit Dokter Moewardi antara lain microtic, switch ethernet, kabel LAN dan fiber optic. Berikut penjelasan dari masing-masing komponen jaringan. • Microtic Microtic merupkan suatu alat yang dipasang pada komputer sehingga komputer tersebut dapat menjadi pengendali lali-lintas data antar jaringan atau router. • Switch Switch merupakan alat yang berfungsi untuk menerima, mentransmisikan, memperkuat dan membagi sinyal data dari router dengan komputer maupun komputer dengan komputer. • Kabel UTP Kabel UTP digunakan sebagai kabel untuk jaringan *Local Area Network* (LAN) pada

	sistem jaringan komputer. Kabel ini berfungsi untuk menghubungkan antar perangkat keras dalam satu jaringan agar dapat mentransmisikan data. • Fiber Optic Saat ini, kabel fiber optic digunakan sebagai *backbone* pada perangkat server di Rumah Sakit Dokter Moewardi. Kabel fiber optic berfungsi sebagai alat untuk menstransmisikan data, namun berbeda dengan kabel UTP, fiber optic lebih aman dan lebih cepat dalam mentransmisikan data. • Bandwith Bandwith berfungsi sebagai salah satu kunci kecepatan jaringan pada RSDM. Saat ini bandwith yang dimilii oleh RSDM adalah dengan kecepatan 20 Mb
Data	Kategori data pada Aplikasi SIMRS didasarkan pada modul-modul yang ada pada aplikasi. Aplikasi SIMRS memilki beberapa modul antara lain modul admission, transaksi, farmasi, billing, penagihan, jasa pelayanan, inventory, rekam medis, informasi eksekutif dan utility. Sehingga berdasarkan fungsi dari masing-masing modul tersebut peneliti mengkategorikan data pada Aplikasi SIMRS sebagai berikut: • Data Keuangan Data keuangan merupakan data-data yang berhubungan dengan billing, pendapatan, penagihan dan transaksi. Data ini membutuhkan keakuratan perhitungan dan waktu karena merupakan tujuan akhir dari seluruh organisasi yaitu mendapatkan keuntungan berupa finansial. • Data Rekam Medis Data rekam medis berisi catatan seperti identitas pasien, hasil pemeriksaan, pengobatan yang telah diberikan, serta tindakan dan pelayanan lain yang telah diberikan kepada pasien. Data ini

	memerlukan kerahasiaan dan keakuratan tinggi karena berhubungan dengan keselamatan pasien itu sendiri. • Data Inventory Data inventory berhubungan dengan data persediaan baik farmasi maupun non-farmasi dalam gudang Rumah Sakit. Data ini memerlukan keakuratan antara jumlah sebenarnya pada gudang dengan perhitungan pada sistem aplikasi.

Hasil identifikasi aset informasi yang terkait dengan Aplikasi SIMRS ini kemudian akan digunakan untuk analisa kembali pada proses penelitian selanjutnya yaitu menentukan aset informasi kritis pada Aplikasi SIMRS.

5.2.1.2 Identifikasi Aset Informasi Kritis

Penentuan aset kritis dilakukan melalui pengumpulan informasi berdasarkan sudut pandang ketiga narasumber yang dapat dilihat pada Lampiran A. Selain itu justifikasi penentuan aset kritis ini juga dilakukan dengan cara melakukan observasi secara langsung dan diskusi dengan pihak yang terkait. Dari wawancara, observasi dan diskusi yang dilakukan kemudian dipaparkan kepada narasumber yaitu Kepala IPDE untuk kemudian divalidasi. Hal tersebut dilakukan untuk memastikan agar hasil yang didapat sudah sesuai dengan kondisi yang ada saat ini.

Tabel 5. 3 Daftar Aset Informasi Kritis

Kategori Aset	Aset Kritis	Alasan / Sebab
Manusia	User	Diperlukan sebagai pihak yang bertugas untuk menambah atau mengentrIkan data sehingga data-data tersebut dapat diolah untuk menjadi laporan kepada pihak eksekutif atau direksi.
	Supervisor	Diperlukan untuk memonitoring kinerja dan menganalisis data yang terekam pada aplikasi

Kategori Aset	Aset Kritis	Alasan / Sebab
		untuk selanjutnya membuat tindakan berupa keputusan-keputusan oleh pihak eksekutif.
	Admin	Admin pada Aplikasi SIMRS berfungsi sebagai pengelola keamanan sekaligus pihak yang bertugas menjaga keberlangsungan aplikasi.
Hardware	Server	Server diperlukan untuk menyimpan seluruh data dan transaksi yang terdapat pada Aplikasi SIMRS
	PC	PC diperlukan untuk mengakses Aplikasi SIMRS didalam gedung Rumah Sakit, dan saat ini PC merupakan satu-satunya alat yang dapat digunakan untuk mengakses Aplikasi SIMRS.
Software	Aplikasi SIMRS	Aplikasi SIMRS diperlukan untuk memberikan pelayanan administrasi dan pelayanan kesehatan ke pasien. Aplikasi ini juga diperlukan sebagai sumber data yang akan digunakan untuk analisa keputusan pihak eksekutif atau direksi.
	OS	OS diperlukan sebagai penghubung antara perangkat keras dengan pengguna dan sekaligus menjadi software yang mewadahi Aplikasi SIMRS.
Jaringan	Microtic	Microtic diperlukan agar suatu komputer dapat menjadi pengatur lalulintas transmisi data atau komputer router
	Switch	Switch diperlukan untuk

Kategori Aset	Aset Kritis	Alasan / Sebab
		distribusi penyebaran dari satu kabel UTP ke banyak kabel UTP, agar seluruh PC dalam gedung terhubung dengan server.
	Kabel UTP	Kabel UTP diperlukan untuk pendistribusian data dari server ke seluruh PC yang ada digedung dan sebaliknya.
	Fiber Optic	Kabel fiber optic diperlukan untuk menjadi *backbone* transmisi data pada server.
Data	Data Keuangan	Data keuangan diperlukan agar Rumah Sakit dapat mengetahui laba dan rugi yang berguna untuk dasar pengambilan keputusan, pengamatan serta pengendalian kegiatan Rumah Sakit oleh direksi.
	Data Rekam Medis	Data rekam medis diperlukan untuk mengetahui identitas atau kebutuhan pasien dalam pelayanan kesehatan.
	Data Inventory	Data inventory diperlukan untuk mengetahui persediaan barang yang ada digudang Rumah Sakit baik barang farmasi maupun non-farmasi.

5.2.1.3 Identifikasi Kebutuhan Keamanan

Kebutuhan keamanan merupakan bentuk perlindungan terhadap ancaman yang mungkin terjadi dalam upaya untuk memastikan keberlangsungan proses bisnis pada Aplikasi SIMRS atau meminimalisir risiko bisnis. Sedangkan aspek keamanan informasi yaitu terdiri dari kerahasisaan (*confidentiaityl*), integritas (*integrity*) dan ketersediaan (*availability*). Aspek keamanan informasi tersebut akan

menjadi kategori dalam mengidentifikasi kebutuhan keamanan aset kritis. Justifikasi kebutuhan keamanan aset kritis ini dilakukan dengan cara melakukan wawancara yang dapat dilihat pada Lampiran A serta observasi secara langsung dan diskusi dengan pihak yang terkait. Kemudian hasil tersebut dipaparkan kepada narasumber yaitu Kepala IPDE untuk kemudian divalidasi. Hal ini dilakukan untuk memastikan hasil yang didapat sudah sesuai dengan kondisi yang ada saat ini. Berikut adalah daftar kebutuhan keamanan aset kritis yang terkait dengan Aplikasi SIMRS.

Tabel 5. 4 Daftar Kebutuhan Keamanan Aset Kritis

Aset	Aspek Keamanan	Kebutuhan Keamanan	Narasumber
User, Supervisor	*Confidentiality*	Menjaga kerahasiaan *username* dan *password* miliknya sendiri	Kepala IPDE
	Integrity	Menggunakan akun login milik sendiri	Kepala IPDE
		Menjaga session loginnya	Database Administrator
		Mengganti *password*nya secara rutin	Database Administrator
		Mengganti *password*nya secara rutin	Database Administrator
Admin	*Confidentiality*	Menjaga kerahasiaan *username* dan *password* miliknya sendiri	Kepala IPDE
	Integrity	Memahami dan menjalankan tata kelola TI yang ada	Kepala IPDE
	Availability	Tersedia pada jam	Kepala IPDE

Aset	Aspek Keamanan	Kebutuhan Keamanan	Narasumber
		kerja	
Server	*Confidentiality*	Lokasi server hanya diketahui oleh pihak berkepentingan	Kepala Bagian Perencanaan
	Integrity	Kunci ruang server hanya dimiliki oleh pihak berwenang	Database Administrator
		Terdapat pembatasan hak akses masuk ruang server	Database Administrator
		Ruang server harus selalu dalam keadaan terkunci	Database Administrator
		Terdapat prosedur akses masuk ke ruang server	Kepala IPDE
		Terdapat log/catatan akses masuk ruang server	Kepala IPDE
		Konfigurasi dilakukan dengan benar	Kepala IPDE
	Availability	Dapat diakses 24 jam dalam 7 hari	Kepala IPDE
		Terdapat sumber listrik cadangan	Kepala IPDE
		Terdapat pemeliharaan rutin	Kepala IPDE
		Terdapat perlindungan keamanan fisik dan lingkungan server	Kepala IPDE
PC	*Confidentiality*	Bersih dari catatan informasi rahasia	Kepala IPDE
	Integrity	Hanya dapat diakses oleh orang	Kepala IPDE

Aset	Aspek Keamanan	Kebutuhan Keamanan	Narasumber
		yang berhak	
	Availability	PC tidak boleh diakses oleh pihak yang tidak berwenang yang dapat merusak	Kepala IPDE
		Dapat diakses 24 jam selama 7 hari	Kepala IPDE
		Terdapat perlindungan keamanan fisik dan lingkungan pada PC	Kepala IPDE
		Adanya sumber listrik cadangan	Kepala IPDE
		Selalu terhubung dengan jaringan	Database Administrator
		Terdapat monitoring dan pemeliharaan rutin	Database Administrator
Aplikasi SIMRS	*Confidentiality*	Kerahasiaan informasi pada Aplikasi SIMRS terjamin	Kepala IPDE
	Integrity	Terdapat sistem login	Kepala IPDE
		Terdapat pembatasan hak akses	Kepala IPDE
	Availability	Dapat diakses 24 jam selama 7 hari	Kepala Bagian Perencanaan
		Terdapat pengecekan rutin untuk memastikan keamanan aplikasi	Kepala IPDE
OS	*Integrity*	Terdapat sistem login	Kepala IPDE
	Availability	Terdapat antivirus	Kepala IPDE

Aset	Aspek Keamanan	Kebutuhan Keamanan	Narasumber
		Berfungsi dengan baik selama 24 jam dalam 7 hari.	Kepala IPDE
Microtic	*Confidentiality*	PC router hanya diketahui oleh orang yang berkepentingan	Database Administrator
		PC router hanya dapat diakses oleh pihak yang berwenang	Database Administrator
	Integrity	Konfigurasi microtic dilakukan dengan tepat	Kepala IPDE
		Terdapat monitoring log	Database Administrator
		Tidak dimodifikasi oleh pihak yang tidak berwenang	Database Administrator
		Terdapat pembatasan hak akses	Kepala IPDE
		Terdapat perlindungan dari netcut/virus/ports/ scanner/attacker	Kepala Bagian Perencanaan
	Availability	Terdapat monitoring dan pemeliharaan rutin	Kepala IPDE
		Mengupdate OS microtic secara berkala	Kepala IPDE
Switch	*Integrity*	Tidak dimodifikasi oleh pihak yang tidak berwenang	Kepala IPDE
		Memiliki konfigurasi yang tepat	Kepala IPDE

Aset	Aspek Keamanan	Kebutuhan Keamanan	Narasumber
	Availability	Dapat berfungsi dengan baik selama 24 jam dalam 7 hari	Kepala IPDE
		Terdapat perlindungan keamanan fisik pada switch	Kepala IPDE
		Terdapat monitoring dan pemeliharaan secara rutin	Kepala IPDE
		Terdapat perlindungan fisik dari pencurian	Kepala IPDE
Kabel UTP, Fiber Optic	*Integrity*	Tidak dimodifikasi oleh pihak yang tidak berwenang	Database Administrator
		Memiliki konfigurasi yang tepat	Database Administrator
		Terdapat pelabelan pada kabel	Database Administrator
	Availability	Terdapat perlindungan fisik pada kabel	Kepala IPDE
		Terdapat pengecekan dan pemeliharaan rutin pada fisik kabel	Kepala IPDE
		Dapat berfungsi dengan baik selama 24 jam dalam 7 hari	Kepala IPDE
Data Keuangan, Data Rekam Medis,	*Confidentiality*	Hanya dapat diketahui/dibaca oleh pihak yang berwenang	Database Administrator
		Tidak dipublikasikan	Kepala Bagian

Aset	Aspek Keamanan	Kebutuhan Keamanan	Narasumber
Data Inventory		tanpa ijin direksi atau disalahgunakan	Perencanaan
	Integrity	Data harus lengkap dan akurat	Kepala Bagian Perencanaan
		Hanya dapat diubah oleh orang yang berhak	Database Administrator
		Selalu di-*update*	Kepala Bagian Perencanaan
		Tidak terdapat data yang redundan	Database Administrator
		Tidak terdapat data yang salah perhitungan	Database Administrator
	Availability	Adanya *backup* data secara rutin	Database Administrator
		Selalu tersedia ketika dibutuhkan	Kepala Bagian Perencanaan

5.2.1.4 Identifikasi Ancaman

Ancaman aset kritis merupakan hal yang mungkin terjadi dan pernah terjadi pada aset dan mengakibatkan terganggung proses bisnis pada Aplikasi SIMRS. Identifikasi ancaman pada aset kritis dikategorikan kedalam ancaman dari lingkungan, ancaman dari manusia dan ancaman dari infrastruktur. Daftar Ancaman berikut ini didapatkan dari hasil wawancara kepada narasumber. Berikut adalah daftar ancaman aset kritis pada Aplikasi SIMRS.

Tabel 5. 5 Daftar Ancaman Aset Kritis

Ancaman dari Lingkungan	
1.	Gempa bumi
2.	Tsunami dan badai
3.	Banjir
4.	Kebakaran
5.	Kerusakan pada bangunan
6.	Perubahan regulasi
7.	Kegagalan sumber daya listrik
8.	Petir
Ancaman dari Manusia	
9.	Kesalahan input data
10.	Penipuan identitas
11.	Pencurian data
12.	Pencurian peralatan
13.	Modifikasi data/konfigurasi secara ilegal
14.	Sharing Password
15.	Sharing kartu akses/ID
16.	Sabotase jaringan
17.	Kelalaian/ketidakdisiplinan pegawai
18.	Penurunan loyalitas pegawai
Ancaman Infrastruktur	
a. Hardware	
19.	Kerusakan pad Hardware
20.	Kesalahan konfigurasi Hardware
21.	Hilangnya peralatan hardware
b. Software	

22.	Bug pada software
23.	Serangan virus/worm
24.	Kesalahan konfigurasi Sistem
25.	Pembobolan sistem
c. Jaringan	
26.	Gangguan pada microtic
27.	Kerusakan kabel
28.	Hilangnya komponen

5.2.1.5 Identifikasi Praktik Keamanan yang Telah Dilakukan Organisasi

Berikut ini merupakan daftar praktik keamanan yang telah dilakukan oleh Rumah Sakit Dokter Moewardi khusunya IPDE dalam memastikan keamanan teknologi informasi dapat mendukung berjalannya proses bisnis Aplikasi SIMRS.

Tabel 5. 6 Daftar Praktik Keamanan Terkini

Praktik Keamanan Organisasi	Pihak yang Bertanggung jawab
Adanya sistem backup otomatis pada server setiap hari pukul setengah 3 pagi	IPDE
Adanya antivirus yang terhubung dengan jaringan dan diupdate secara berkala	IPDE
Adanya update patch dan firewall secara berkala	IPDE
Telah dipasang pendingin pada ruang server untuk mengurangi terjadinya overheat	IPDE
Telah ada prosedur mengenai monitoring suhu dan kelembapan ruangan	IPDE
Adanya camera CCTV yang bekerja selama 24 jam	Pusat Keamanan RSDM
Switch telah diletakkan di tempat yang sulit dijangkau sehingga tidak mudah dimodifikasi secara ilegal	IPDE
Adanya fire extinguisher untuk memadamkan api saat terjadi kebakaran	IPDE
Adanya UPS sebagai sumber listrik cadangan	PIC UPS Pusat
Terdapat bagian servis dan pemeliharaan yang telah melakukan pemeliharaan perangkat IT secara rutin	IPDE
Adanya teknologi barcode ID untuk akses masuk ruang server	IPDE
Telah dilakukan pelatihan mengenai keamanan infromasi kepada user	IPDE
Terdapat pendataan kebutuhan hak akses sesuai dengan kebutuhan fungsional	Bagian Organisasi dan Kepegawaian

Praktik Keamanan Organisasi	Pihak yang Bertanggung jawab
bisnis user	
Terdapat Kartu ID sebagai identitas untuk masuk lokasi TI maupun mengakses peralatan TI	IPDE
Telah terdapat protocol UPS untuk otomatis menyala 3-4 detik setelah sumber listrik utama mati	PIC UPS Pusat
Terdapat kebijakan mengenai Keamanan Informasi Data Elektronik	IPDE
Pada PC operator tidak dapat menginstall aplikasi dari luar	IPDE
Terdapat formulir log buku tamu akses masuk ruang server	IPDE
Terdapat pembatasan modul untuk setiap user pada Aplikasi SIMRS	IPDE
Terdapat pembatasan operasi/modifikasi untuk setiap user	IPDE
Monitoring jaringan selalu dilakukan selama jam kerja	IPDE
Terdapat log akses user pada Aplikasi SIMRS	IPDE
Terdpat pendataan inventaris peralatan IT	IPDE
Terdapat bagian troubleshooting dan implementasi yang dapat dihubungi selama jam kerja jika user mengalami kesulitan terkait permasalahan IT	IPDE
CPU operator diletakkan pada almari yang memiliki kunci	IPDE Operator
Telah dilakukan pengecekan dan pemeliharaan rutin pada UPS	PIC UPS Pusat
Adanya anggota satuan keamanan yang berkeliling selama 24 jam penuh	Pusat Keamanan RSDM

5.2.1.6 Identifikasi Kelemahan Organisasi

Justifikasi kelemahan organisasi didapat dari hasil wawancara yang dapat dilihat pada Lampiran A serta observasi langsung yang dilakukan oleh peneliti. Berikut adalah hasil identifikasi kelemahan organisasi pada Aplikasi SIMRS di Rumah Sakit Dokter Moewardi.

Tabel 5. 7 Daftar Kelemahan Organisasi

No	Kelemahan Organisasi
1.	Belum ada kebijakan yang mengatur mengenai keamanan password
2.	Belum ada penentuan strong password
3.	Kesadaran user akan pentingnya menjaga keamanan passswordnya masih rendah
4.	Kepatuhan user pada anjuran keamanan hak akses masih rendah
5.	Belum ada mirroring database
6.	Tidak adanya evaluasi setelah dilakukan pelatihan mengenai keamanan informasi
7.	Tata kelola TI belum lengkap dan belum sepenuhnya dijalankan
8.	Pemantauan status hak akses belum sepernuhnya dijalankan
9.	Belum ada prosedur untuk penonaktifan akun/hak akses
10.	Pengelolaan terhadap akun nonaktif belum dilakukan
11.	Sistem belum dapat melacak dan mencatat aktivitas user secara terperinci

5.2.2 Fase 2 - Mengidentifikasi kerentanan Infrastruktur TI

Pada fase ini akan dilakukan identifiksai kelemahan infrastruktur dengan menggunakan informasi yang didapat dari senior manajemen, bagian operasional dan karywan. Pada fase ini akan dilakukan evaluasi terhadap komponen utama dari sistem yang bersifat mendukung aset kritis, setelah didapat komponen utama maka dari itu akan ditinjau kelemahannya. Output yang dihasilkan dari fase ini nantinya adalah tabel komponen utama dan tabel kerentanan teknologi.

Komponen utama merupakan suatu komponen yang mana berkaitan dan berperan penting pada suatu aset.

5.2.2.1 Identifikasi Komponen Kunci

Komponen kunci merupakan unsur kunci yang dalam penerapannya mendukung proses bisnis utama dari Aplikasi SIMRS. Komponen operasional kunci dari infrastruktur teknologi informasi yang mempengaruhi kinerja dari Aplikasi SIMRS (server, PC dan perangkat jaringan) diidentifikasi kelemahannya baik dari sisi teknologi dan konfigurasi, yang dapat menimbulkan akses keamanan oleh yang tidak berhak.

Tabel 2. 8 Tabel Daftar Komponen Utama

Server	
System of Interest	Server penyimpan data pada Aplikasi SIMRS
Komponen Utama	
• Processor • RAM • Harddisk	
Personal Computer	
System of Interest	PC milik operator dan admin pada Aplikasi SIMRS
Komponen Utama	
• CPU • Monitor • Keyboard • Mouse	
Aplikasi SIMRS	
System of Interest	Aplikasi Sistem Informasi Rumah sakit milik RS Dokter Moewardi
Komponen Utama	
• Sumber kode program • User • Jaringan • Sistem Operasi	
Microtic	
System of Interest	Microtic pada komputer router pusat

Komponen Utama	
• RouterBoard • PC	
Switch	
System of Interest	Switch penghubung jaringan pada RS Dokter Moewardi
Komponen Utama	
• Port Ethernet • Kabel LAN	

5.2.2.2 Identifikasi Kerentanan Teknologi

Setelah dilakukan identifikasi komponen utama, maka akan dilakukan identifikasi ancaman untuk masing-masing komponen utama. Hal ini dilakukan untuk dapat melihat kerentanan teknologi yang ada. Ancaman yang menyerang komponen utama tentunya juga akan mengancam aset kritis, oleh karena itu hal ini dapat membantuk dalam melihat keseluruhan ancaman yang dapat mengganggu aset kritis.

Tabel 5. 8 Daftar Kerentanan Teknologi Aset Kritis

Server	
System of Interest	Server penyimpan data pada Aplikasi SIMRS
Komponen Utama	**Kemungkinan Kerentanan**
• Processor • RAM • Harddisk	• Serangan *Denial of Service* (DoS) • RAM mengalami kelebihan memori • Kinerja Procesor menurun akibat terlalu banyak kapasitas data • Tempat penyimpanan *(Harddisk)* penuh • Server mengalami *overheat* • Sistem *backup* otomatis mengalami gangguan
Personal Computer	
System of Interest	PC milik operator dan admin pada Aplikasi SIMRS
Komponen Utama	**Kemungkinan Kerentanan**
• CPU	• Monitor, Keyboard ataupun mouse

• Monitor • Keyboard • Mouse	mengalami kerusakan karena pemakaian berlebih • Monitor, Keyboard ataupun mouse mengalami kerusakan akibat benturan • Monitor, Keyboard ataupun mouse mengalami konsleting akibat terkena air • CPU mengalami *overheat*
Aplikasi SIMRS	
System of Interest	Aplikasi Sistem Informasi Rumah sakit milik RS Dokter Moewardi
Komponen Utama	**Kemungkinan Kerentanan**
• Sumber kode program • Jaringan • Sistem Operasi	• *Password Cracking* dengan *Brute-force* yaitu sebuah teknik di mana akan dicobakan semua kemungkinan kata kunci *(password)* untuk bisa ditebak untuk akses ke dalam sebuah sistem. • Terdapat *bugs* pada aplikasi • *Buffer Overflow* yaitu kondisi saat aplikasi mencoba memasukkan lebih banyak data ke buffer daripada yang dapat ditahan • Exploitasi *session login*
Microtic	
System of Interest	Microtic pada komputer router pusat
Komponen Utama	**Kemungkinan Kerentanan**
• RouterBoard • PC	• *IP Scanning*, yaitu metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network korban • Terdapat *rootkit* yaitu alat untuk menghilangkan jejak apabila telah dilakukan penyusupan. • Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman listrik • *Routerboard* mengalami kerusakan • Terjadi *routing loop,* yaitu looping

	pada jaringan sehingga komputer client tidak dapat mengakses tujuannya • Terjadi kesalahan konfigurasi pada microtic • IP *spoofing*
Switch	
System of Interest	Switch penghubung jaringan pada RS Dokter Moewardi
Komponen Utama	**Kemungkinan Kerentanan**
• Port Ethernet • Kabel LAN	• Terjadi kesalahan konfigurasi pada switch dan kabel LAN • Port switch rusak • Switch hang akibat fluktuatif arus • Kabel LAN putus akibat hewan pengerat • *Overheat* pada switch • Terjasi *looping* pada switch • Kerusakan pada konektor ethernet • Switch mengalami konsleting akibat air

5.2.3 Fase 3 - Membangun Perencanaan dan Strategi Keamanan

Fase ini dilakukan dengan tujuan untuk melakukan evaluasi risiko dari aset kritis berdasarkan output yang telah didapatkan dari fase 1 dan fase 2. Dari tahap I dan II diperoleh profil ancaman dan kelemahan infrastruktur sistem jaringan informasi. Pada tahap III ditindaklanjuti dengan merangkum kegiatan sebelumnya menjadi bentuk profil risiko dengan tingkat ukuran risiko (secara kualitatif) yang dikaitkan dengan dampaknya bagi organisasi.

5.2.3.1 Risiko Keamanan Aset Informasi terkait Aplikasi SIMRS

Dalam penelitian ini, risiko dititik beratkan pada risiko-risiko yang berhubungan dengan akses tidak sah pada aset informasi

yang terkait dengan Aplikasi SIMRS baik akses yang bersifat *logical* maupun *physical* . Untuk mendapatkan risiko-risiko tersebut, peneliti terlebih dahulu mengidentifikasi seluruh kemungkinan risiko keamanan aset informasi yang terkait dengan Aplikasi SIMRS. Hasil identifikasi risiko keamanan aset informasi terkait dengan Aplikasi SIMRS dapat dilihat pada Lampiran B.

Tabel 5. 9 Daftar Risiko Aset Infromasi Terkait Aplikasi SIMRS

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan
Manusia	User, Supervisor ,Admin	R01	Manipulasi data	R01.1	Pencurian *username* dan *password* pada user
				R01.2	Exploitasi *session login*
Hardwar e	Server	R02	Kerusakan pada server	R02.1	Gempa Bumi
				R02.2	Badai dan Petir
				R02.3	Banjir
				R02.4	Kebakaran
				R02.5	Kebocoran dan Kerusakan Bangunan
		R03	Server berhenti	R03.1	Kerusakan pada UPS
				R03.2	Listrik Mati
		R05	Kinerja server melambat	R05.1	RAM mengalami kelebihan memori
				R05.2	Kinerja Procesor menurun akibat terlalu banyak kapasitas data
				R05.3	Tempat penyimpanan (*Harddisk)* penuh
				R05.4	Server mengalami *overheat*
		R06	Server Down	R06.1	Serangan *Denial of Service* (DoS), SQL-Injection, Sniffing
				R06.2	Overload Request
		R07	Akses tidak	R07.1	Pihak luar yang masuk ke

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan
					ruang server secara ilegal
			sah ke ruang server	R07.2	Kurangnya evaluasi hak akses pada peralatan dan lokasi fasilitas pengolahan data elektronik.
				R07.3	Kelalaian petugas yang meninggalkan ruang server dalam keadaan tidak terkunci
	PC	R08	Kerusakan PC	R08.1	Gempa Bumi
				R08.2	Badai dan Petir
				R08.3	Banjir
				R08.4	Kebakaran
				R08.5	Kebocoran dan Kerusakan Bangunan
				R08.6	Monitor, Keyboard ataupun mouse mengalami kerusakan karena pemakaian berlebih
				R08.7	Kesalahan konfigurasi
		R09	PC tidak dapat menyala	R09.1	Kerusakan pada UPS
				R09.2	Listrik Mati
		R10	Kinerja PC melambat	R10.1	CPU mengalami overheat
				R10.2	RAM mengalami kelebihan memori
				R10.3	Kinerja Procesor menurun akibat terlalu banyak kapasitas data
		R11	PC tidak dapat terhubung dengan jaringan	R11.1	Port ethernet pada PC rusak
		R12	Akses tidak sah ke PC	R12.1	Kelalaian petugas yang meninggalkan ruangan/lokasi PC dalam keadaan tidak terkunci
				R12.2	Kelalaian pengguna yang meninggalkan PC dalam keadaan menyala/ tidak terkunci.
		R13	Komponen PC hilang	R12.3	Pencurian pada komponen PC
Software	Aplikasi SIMRS	R14	Aplikasi tidak dapat diakses	R14.1	Terdapat *bug* pada aplikasi
				R14.2	Gangguan pada jaringan
				R14.3	Listrik mati
				R14.4	Server down

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan
		R15	Aplikasi diakses oleh pihak tidak berwenang	R15.1	Exploitasi akun pegawai yang sudah pindah atau pensiun
				R15.2	*Sharing password* pada user
				R15.3	Kesalahan pemberian hak akses pada user
				R15.4	Kurangnya evaluasi dan monitoring pada hak akses
		R16	User tidak dapat login	R16.1	User lupa *password*
				R16.2	Kesalahan dalam pemberian hak akses
	OS	R17	Terserang virus	R17.1	Antivirus tidak update
				R17.2	Terdapat bug pada antivirus sehingga tidak dapat berjalan
				R17.3	Kesalahan konfigurasi pada antivirus/firewall
		R18	Terserang *worm* atau *Trojan Horse*	R18.1	Terdapat file yang terjangkit *worm* atau *Trojan Horse* lewat usb
				R18.2	Membuka atau mendownload file yang terjangkit *worm* atau *Trojan Horse*
Jaringan	Microtic	R19	Kerusakan pada microtic	R19.1	Kerusakan *routerboard*
				R19.2	Kesalahan konfigurasi
				R19.3	Terjadi *routing loop*
				R19.4	Gempa Bumi
				R19.5	Badai dan Petir
				R19.6	Banjir
				R19.7	Kebakaran

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan
	Switch	R20	Kerusakan pada switch	R20.1	Gempa Bumi
				R20.2	Badai dan Petir
				R20.3	Banjir
				R20.4	Kebakaran
		R21	Penurunan kinerja pada switch	R21.1	*Overheat* pada switch
				R21.2	Kerusakan pada konektor ethernet
				R21.3	Port switch rusak
				R21.4	Terjadi kesalahan konfigurasi
		R22	Kehilangan switch	R22.1	Pencurian switch
	Kabel UTP, Fiber Optic	R23	Kerusakan pada kabel	R23.1	Digigit hewan pengerat
				R23.2	Lapisan pelindung kabel mengelupas/ lepas
				R23.3	Kabel berkarat/usang
				R23.4	Kurangnya kontrol pengamanan kabel
		R24	Modifikasi ilegal pada konfigurasi kabel	R24.1	Kabel UTP dipindah demi kepentingan pribadi
				R24.2	Kabel UTP dicabut secara ilegal
		R25	Kabel hilang	R25.1	Pencurian pada kabel
				R25.2	Kelalaian pegawai
Data	Data keuangan, Data Rekam Medis, Data Inventoy	R26	Kegagalan backup data	R26.1	Kapasitas media penyimpanan overload
				R26.2	Terdapat gangguan jaringan pada sistem back up data otomatis
		R27	Pencurian data	R27.1	Terjadi Packet Sniffing pada jaringan untuk mencuri data
				R27.2	Terjadi social engineering pada user maupun admin
				R27.3	Loyalitas pegawai menururn
		R28	Data tidak valid	R28.1	Kesalahan input oleh user
				R28.2	Kesalahan perhitungan pada sistem maupun user
		R29	Kehilangan	R29.1	Virus

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan
			data	R29.2	Kelalaian user
				R29.3	Sistem back up gagal
				R29.4	Rusaknya media penyimpanan

5.2.3.2 Pengukuran Risiko Keamanan Aset Informasi terkait Aplikasi SIMRS

Berdasarkan pengukuran risiko dengan metode FMEA terdapat 1 risiko dengan kategori *Very Low,* 45 risiko dengan kategori *Low,* 14 risiko dengan kategori *Medium*, 21 risiko dengan kategori *High* dan 4 risiko dengan kategori *Very High.* Untuk detail dari penilaian risiko dapat dilihat pda Tabel C. Pengukuran risiko ini diperlukan untuk mengetahui jenis kategori masing-masing risiko.

Pengukuran risiko digunakan untuk mengetahui jenis kategori risiko pada masing-masing risiko kontrol akses *physical* dan *logical,* sehingga pihak IPDE mengetahui tingkat urgensi risiko kontrol akses yang akan dimitigasi apakah risiko tersebut termasuk kategori *Very High, High, Medium, Low atau Very Low.* Sehingga dalam penyusunan SOP dapat diketahui SOP mana yang memitigasi risiko dengan kategori risiko paling tinggi atau paling rendah.

5.2.3.2.1 Pemetaan Risiko Kontrol Akses *Logical*

Setelah mengidentifikasi keseluruhan risiko keamanan aset infromasi pada Aplikasi SIMRS, kemudian dilakukan pemetaan untuk mengetahui risiko-risiko apa saja yang berhubungan dengan akses tidak sah sehingga dapat diketahui tindakan kontrol akses apa saja yang perlu diterapkan. Berikut adalah hasil risiko kontrol akses *logical* pada aset kritis yang terkait dengan Aplikasi SIMRS.

Tabel 5. 10 Risiko Akses *Logical*

Aset	ID	Potensi Mode Kegagalan	ID Penyebab	Potensi Penyebab Kegagalan	Nilai RPN	Kategori
Aplikasi SIMRS	R15	Aplikasi diakses oleh pihak tidak berwenang	R15.1	Exploitasi akun pegawai yang sudah pindah atau pensiun	224	*Very High*
			R15.3	Kesalahan pemberian hak akses pada user Aplikasi SIMRS	160	*High*
			R15.4	Kurangnya evaluasi dan monitoring pada hak akses Aplikasi SIMRS	343	*Very High*
			R15.2	*Sharing password* pada user	336	*Very high*
Data	R01	Manipulasi data	R01.1	Pencurian *username* dan *password* pada user	96	*Medium*
			R01.2	Exploitasi *session login*	144	*High*

5.2.3.2.2 Pemetaan Risiko Kontrol Akses *Physical*

Berikut adalah hasil risiko kontrol akses *logical* pada aset kritis yang terkait dengan Aplikasi SIMRS.

Tabel 5. 11 Risiko Akses *Physical*

Aset	ID	Potensi Mode Kegagalan	ID Penyebab	Potensi Penyebab Kegagalan	Nilai RPN	Kategori
Server	R07	Akses tidak sah ke ruang server	R07.1	Pihak luar yang masuk ke ruang server secara ilegal	81	*Low*
			R07.2	Kurangnya evaluasi hak akses pada peralatan dan lokasi fasilitas pengolahan data elektronik.	108	*High*
			R07.3	Kelalaian petugas yang meninggalkan ruang server dalam keadaan tidak terkunci	160	*High*
PC	R12	Akses tidak sah ke PC	R12.1	Kelalaian pengguna yang meninggalkan PC dalam keadaan menyala/ tidak terkunci.	140	*High*
Data	R27	Pencurian data	R27.2	Penulisan *username* dan *password* pada lokasi yang mudah dilihat	82	*Medium*

5.2.3.3 Rencana Mitigasi Risiko

Tahap perlakuan risiko merupakan tahap dalam menentukan tindakan mitigasi risiko yang tepat. Tahap perlakuan risiko dilakukan dengan melakukan pemetaan risiko terhadap masing masing kontrol yang dibutuhkan dalam ISO27002:2013 serta menganalisis rekomendasi mitigasi risiko.

Tujuan dari pemetaan risiko kedalam ISO27002:2013 adalah untuk memastikan bahwa perlakuan risiko telah tepat dan sesuai dengan *control objective*. Selain pemetaan risiko dan kontrol pada kerangka kerja, dilakukan pula justifikasi kebutuhan kontrol. Justifikasi kebutuhan kontrol tersebut memiliki fungsi untuk memastikan bahwa kontrol yang ada sesuai dengan risiko yang akan dimitigasi.

Setelah melakukan pemetaan risiko dengan ISO27002:2013, selanjutnya akan ditentukan rekomendasi mitigasi risiko berdasarkan kontrol yang telah ditentukan. Rekomendasi mitigasi risiko yang telah dipetakan sesuai dengan risiko dan kebutuhan kontrolnya nantinya akan mendefinisikan usulan-usulan perbaikan dalam kontrol akses Aplikasi SIMRS pada Rumah Sakit Dokter Moewardi dan juga sebagai input untuk membuat dokumen *Standard Operating Procedure* (SOP) Kontrol Akses Aplikasi SIMRS.

5.2.3.3.1 Pemetaan Risiko dengan Kontrol ISO 27002:2013

Berikut merupakan hasil pemetaan risiko dengan kontrol yang ada pada ISO 27002:2013 beserta justifikasinya.

Tabel 5. 12 Tabel Pemetaan Risiko dengan Kontrol ISO27002

ID	Potensial Penyebab Kegagalan	Control Objective ISO27002	Justifikasi
Risiko Akses *Logical*			
R15.1	Exploitasi akun pegawai yang sudah pindah atau pensiun	*9.2.6 Removal or adjustment of access rights*	Kontrol untuk memastikan bahwa hak akses seluruh karyawan dan

ID	Potensial Penyebab Kegagalan	Control Objective ISO27002	Justifikasi
			pengguna pihak eksternal pada akses informasi dan akses fasilitas pengolahan informasi telah dihapus setelah pemutusan hubungan kerja, kontrak atau perjanjian merela, atau disesuaikan dengan perubahan.
R15.3	Kesalahan pemberian hak akses pada user Aplikasi SIMRS	*9.1.1 Access control policy*	Kontrol untuk memastikan bahwa kebijakan kontrol akses telah dibentuk, didokumentasikan dan ditinjau berdasarkan kebutuhan keamanan bisnis dan informasi
		9.2.1 User registration and de-registration	Kontrol untuk memastikan bahwa proses registrasi dan de-registrasi pengguna formal telah diimplementasikan untuk memberikan hak akses yang tepat.
		9.2.2 User access provisioning	Kontrol untuk memastikan bahwa proses penyediaan hak akses resmi pengguna telah diimplementasikan untuk mencabut dan menetapkan hak

ID	Potensial Penyebab Kegagalan	Control Objective ISO27002	Justifikasi
			akses pada seluruh jenis pengguna di semua sistem dan layanan.
		9.4.1 Information access restriction	Kontrol untuk memastikan bahwa akses ke informasi dan fungsi sistem aplikasi telah dibatasi sesuai dengan kebijakan kontrol akses.
R15.4	Kurangnya evaluasi dan monitoring pada hak akses Aplikasi SIMRS	*9.2.5 Review of user access rights*	Kontrol untuk memastikan bahwa pemilik aset telah meninjau hak akses penggunaan asetnya secara berkala
R15.2	*Sharing password* pada user Aplikasi SIMRS	*9.3.1 Use of secret authentication information*	Kontrol untuk memastikan bahwa pengguna telah mengikuti cara-cara organisasi dalam menggunakan informasi yang harus memiliki otentikasi rahasia.
R01.1	Pencurian *username* dan *password* pada user	*9.3.1 Use of secret authentication information*	Kontrol untuk memastikan bahwa sistem manajemen password telah interaktif dan telah dipastikan kualitas passwordnya.
R01.2	Exploitasi *session login*	*9.3.1 Use of secret authentication*	Kontrol untuk memastikan bahwa prosedur *log-on* aman

ID	Potensial Penyebab Kegagalan	Control Objective ISO27002	Justifikasi
		information	ketika dibutuhkan oleh kebijakan kontrol akses, akses ke sistem dan akses ke aplikasi.
Risiko Akses *Physical*			
R07.1	Pihak luar yang masuk ke ruang server secara ilegal	*11.1.2 Physical entry controls* *11.1.2 Physical entry controls*	Kontrol untuk memastikan bahwa daerah telah dilindungi oleh kontrol masuk yang tepat sehingga dapat dipastikan bahwa hanya pihak yang berwenang yang diperbolehkan mengakses
R07.2	Kurangnya evaluasi hak akses pada peralatan dan lokasi fasilitas pengolahan data elektronik.		
R07.3	Kelalaian petugas yang meninggalkan ruang server dalam keadaan tidak terkunci	*11.1.5 Working In Secure Area*	Kontrol untuk memastikan bahwa prosedur untuk bekerja di area aman telah dirancang dan diterapkan.
R12.1	Kelalaian pengguna yang meninggalkan PC dalam keadaan menyala/ tidak terkunci.	*11.2.8 Unattended user equipment*	Kontrol untuk memastikan bahwa peralatan yang tidak diawasi memiliki perlindungan yang tepat.
R27.2	Penulisan *username* dan *password* pada lokasi yang mudah dilihat	*11.2.9 Clear desk and clear screen policy*	Kontrol untuk memastikan bahwa kebijakan meja kerja bebas dari kertas yang berisi informasi rahasia dan media

ID	Potensial Penyebab Kegagalan	Control Objective ISO27002	Justifikasi
			penyimpanan yang mudah dipindahkan. Kebijakan layar yang bebas dari informasi rahasia pada fasilitas pengolahan informasi harus diadopsi.

5.2.3.3.2 Rekomendasi Mitigasi Risiko

Rekomendasi mitigasi risiko yang dihasilkan akan didasarkan pada kontrol objektif dan petunjuk pelaksanaan *control objective* yang telah ditentukan padaISO27002:2013. Selain itu, rekomendasi risiko juga didasarkan pada identifikasi praktik keamanan yang telah diimplementasikan, hal ini berfungsi untuk menyesuakian tindakan mitigasi risiko dalam mengelola risiko yang muncul. Dalam rekomendasi mitigasi risiko akan didefinisikan input untuk membuat dokumen SOP Kontrol Akses Aplikasi SIMRS dan juga usulan-usulan perbaikan dalam meningkatkan keamanan akses. Pemetaan rekomendasi mitigasi risiko dari kontrol objektif ISO27002:2013 dapat dilihat pada Lampiran C.

BAB VI
HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan mengenai hasil dari pengolahan data yang telah didapatkan dari bab sebelumnya. Luaran dari bab ini berupa pembahasan produk penelitian.

6.1 Dokumen SOP yang Ada Saat Ini

Berikut merupakan daftar dokumen yang terkait dengan kontrol akses *physical* dan *logical* yang telah ada di Rumah Sakit Dokter Moewardi saat ini.

Tabel 6. 1 Tabel Dokumen saaat ini

No	Nama Dokumen	Keterangan
1	Kebijakan Keamanan Informasi Data Elektronik di Lingkungan RSUD Dr. Moewardi	Kebijakan ini terdiri dari pengendalian fisik, akses dan pengelolaan gangguan keamanan informasi. Pada pengendalian fisik memiliki lingkup pengamanan area dan perangkat. Pengendalian akses memilkik lingkup persyaratan untuk pengendalian akses, pengelolaan akses pengguna, tanggung jawab pengguna, pengendalian akses jaringan dan pengendalian akses ke Aplikasi dan Sistem Informasi. Sementara pengendalian pengelolaan gangguan keamanan informasi terdiri dari pelaporan kejadian dan kelemahan keamanan informasi dan pengelolaan gangguan keamanan informasi dan perbikan. Namun kebijakan ini tidak mengacu kepada standar tertentu dan hanya dibuat berdasarkan pengetahuan dari karyawan IPDE. Kebijakan ini belum seluruhnya memiliki tindak lanjut berupa prosedur untuk memenuhi peraturan dalam kebijakan. Sehingga evaluasi kepatuhan terhadap kebijakan sulit untuk dilakukan.
2.	Prosedur	Prosedur ini dapat dikatakan sebagai

	permintaan, perubahan dan penonaktifan *username* dan *password* masuk ke sistem informasi. *(RSDM/SPO. A/IPDE/015)*	prosedur untuk kontrol akses *Logical.* Namun prosedur ini tidak mempunyai acuan dan tidak berisi aktivitas-aktivitas yang berurutan, melainkan hanya berisi pernyataan mengenai aktor terkait saja. Sehingga apabila terjadi pergantian pegawai/ pelaksana tidak dapat diaplikasikan karena bukan berupa instruksi. Selain itu untuk keperluan audit sistem, prosedur tersebut tidak memiliki suatu dokumentasi kontrol pada pelasanaan prosedur berupa formulir log atau formulir aktivitas dan tidak mengacu atau menenuhi suatu standar tertentu sehingga akan mengakibatkan buruknya penilaian audit dan kesulitan dalam mengetahui kepatuhan proses dengan prosedur yang ada.
3.	Prosedur Akses ke Ruang Server. *(RSDM/SPO. A/IPDE/016)*	Prosedur ini dapat dikatakan sebagai salah satu prosedur kontrol akses *Physical.* Prosedur ini berisi mengenai pernyataan aktor terkait dan beberapa peraturan terkait dengan akses masuk ke ruang server. Prosedur ini tidak disajikan dalam bentuk instruksi aktivitas secara berurutan sehingga apabila terjadi pergantian pegawai akan sulit diaplikasikan sebagai media petunjuk pelasanaan suatu proses. Selain itu prosedur ini belum mengacu pada standar tertentu sehingga sulit dilakukan evaluasi atau audit mengenai kepatuhan prosedur dengan acuan. Prosedur ini dilengkapi dengan formulir akses masuk ruang server (buku tamu), namun formulir buku tamu tersebut hanya wajib diisi oleh pengunjung tanpa melewati persetujuan resmi dari Kepala IPDE. Sehingga apabila terjadi kerusakan/ pencurian masih sulit dilakukan pelacakan karena petugas maupun pegawai tidak diwajibkan mengisi formulir tersebut. Selain itu prosedur tidak memuat dengan detail

		keperluan akses masuk pengunjung sehingga sulit untuk dievaluasi.

6.2 SOP yang Dihasilkan Berdasarkan Rekomendasi Mitigasi Risiko

Berdasarkan hasil rekomendasi mitigasi risiko, didefinisikan beberapa prosedur yang dapat dihasilkan dalam penelitian. Berikut ini adalah prosedur yang dihasilkan dalam penelitian.

Tabel 6. 2 Tabel SOP yang Dihasilkan

Potensial Penyebab Kegagalan	Kontrol pada ISO27002	Prosedur ID	Prosedur Nama
R15.3 Kesalahan pemberian hak akses pada user Aplikasi SIMRS	9.2.1 *User registration and de-registration*	**SP01**	**SOP Pembuatan dan Perubahan Hak Akses Akun Aplikasi SIMRS**
	9.2.2 User access provisioning		
	9.4.1 Information access restriction		
R15.4 Kurangnya evaluasi dan monitoring pada hak akses Aplikasi SIMRS	*9.2.5 Review of user access rights*	**SP02**	**SOP Peninjauan Hak Akses pada Akun Aplikasi SIMRS**
R15.1 Exploitasi akun pegawai yang sudah pindah atau pensiun	*9.2.6 Removal or adjustment of access rights*	**SP03**	**SOP Penghapusan pada Hak Akses Akun Aplikasi SIMRS**
R15.2 *Sharing password* pada user Aplikasi SIMRS	*9.3.1 Use of Secret Authentication Information*	**SP04**	**SOP Pemeliharaan Keamanan Akses Pada Aplikasi SIMRS**
R01.1 Pencurian *username* dan *password* pada	*9.3.1 Use of Secret Authentication Information*		

Potensial Penyebab	Kontrol pada ISO27002	Prosedur ID	Prosedur Nama
user			
R01.2 Exploitasi *session login*	*9.3.1 Use of Secret Authentication Information*		
R07.1 Pihak luar yang masuk ke ruang server secara ilegal	*11.1.2 Physical entry controls*	**SP05**	**SOP Akses Server Aplikasi SIMRS**
R07.2 Kurangnya evaluasi dan pembatasan hak akses pada akses peralatan dan ruangan server	*11.1.2 Physical entry controls*		
R07.3 Kelalaian petugas yang meninggalkan ruang server dalam keadaan tidak terkunci	*11.1.5 Working In Secure Area*		
R12.1 Kelalaian pengguna yang meninggalkan PC dalam keadaan menyala/ tidak terkunci.	*11.2.8 Unattended user equipment*	**SP06**	**SOP Pemantauan Akses Komputer**
R27.2 Penulisan *username* dan *password* pada lokasi yang mudah dilihat	*11.2.9 Clear desk and clear screen policy*		

6.3 Perancangan Struktur dan Isi SOP

Pada sub-bab ini akan dijelaskan mengenai perancangan SOP yang akan dibuat. Perancangan SOP ini mengacu pada manajemen akses, penulis menggunakan panduan SOP menurut Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan. Namun, dalam perancangan struktur dan isi SOP tidak keseluruhan struktur konten akan mengacu pada standar tersebut karena akan disesuaikan dengan kebutuhan. Pada SOP ini, model prosedur akan dijabarkan dalam bentuk *flowchart* karena terdapat banyak aktivitas dan keputusan yang terkait. Hasil keseluruhan dokumen SOP akan dilampirkan pada buku produk SOP manajemen akses. Sedangkan dalam penyusunan aktivitas dalam prosedur digunakanlah relevansi kontrol dan aktivitas pada masing-masing prosedur. Struktur dokumen SOP yang akan disusun ini akan dihasilkan ke dalam sebuah buku produk yang akan diberikan kepada pihak Instalasi Pengelola Data Elektronik sebagai rekomendasi pengamanan kontrol akses *physical* dan *logical* pada Aplikasi SIMRS.

Adapun struktur atau konten yang akan dimasukkan ke dalam kerangka dokumen *Standard Operating Procedure* (SOP) kontrol akses logika dan *physical* pada Aplikasi SIMRS adalah sebagai berikut.

Tabel 6. 3 Hasil Perancangan Struktur dan Isi SOP

Stuktur Bab	Sub-Bab	Konten
Pendahuluan	Rincian	Berisi pengesahan, deskripsi dokumen dan riwayat revisi.
	Tujuan	Berisi informasi mengenai tujuan umum pembuatan SOP
	Risiko Kontrol Akses pada Aplikasi SIMRS	Tabel risiko dan penyebabnya

Stuktur Bab	Sub-Bab	Konten
	Pemetaan risiko, kontrol dan SOP	Tabel penyebab risiko, kontrol pada ISO27002 dan SOP yang dihasilkan berdasarkan risiko dan kontrol tersebut
	Ruang Lingkup Konten SOP	Berisi Keterkaitan antara SOP dengan kebijakan, formulir dan Instruksi kerja
	Overview Kontrol Akses	Aspek kontrol akses *logical* dan *physical*
SP01 - Prosedur Penanganan Permintaan Hak Akses Aplikasi SIMRS	Tujuan	Deskripsi umum dan infromasi prosedur
	Ruang Lingkup	
	Definisi	Definisi isilah baru yang digunakan dalam prosedur
	Alur Manajemen Eskalasi	Alur manajemen eskalasi keputusan dan penanganan sesuai kebutuhan prosedur
	Rincian Prosedur	Sub-prosedur Pembuatan akun baru
		Sub-prosedur perubahan hak akses lama
	Bagan Alur Prosedur	Tabel bagan alur SOP
SP02 - Prosedur Pemantauan Hak Akses pada Akun Aplikasi SIMRS	Tujuan	Deskripsi umum dan infromasi prosedur
	Ruang Lingkup	
	Definisi	Definisi isilah baru yang digunakan dalam prosedur
	Alur Manajemen Eskalasi	Alur manajemen eskalasi keputusan

Stuktur Bab	Sub-Bab	Konten
		dan penanganan sesuai kebutuhan prosedur
	Rincian Prosedur	Berisi rincian aktivitas pada prosedur
	Bagan Alur Prosedur	Tabel bagan alur SOP
SP03 - Prosedur Penghapusan Hak Akses pada Akun Aplikasi SIMRS	Tujuan	Deskripsi umum dan infromasi prosedur
	Ruang Lingkup	
	Definisi	Definisi isilah baru yang digunakan dalam prosedur
	Alur Manajemen Eskalasi	Alur manajemen eskalasi keputusan dan penanganan sesuai kebutuhan prosedur
	Rincian Prosedur	Berisi rincian aktivitas pada prosedur
	Bagan Alur Prosedur	Tabel bagan alur SOP
SP04 - Prosedur Pemeliharaan Keamanan Akses pada Akun Aplikasi SIMRS	Tujuan	Deskripsi umum dan infromasi prosedur
	Ruang Lingkup	
	Definisi	Definisi isilah baru yang digunakan dalam prosedur
	Alur Manajemen Eskalasi	Alur manajemen eskalasi keputusan dan penanganan sesuai kebutuhan prosedur
	Rincian Prosedur	Berisi rincian aktivitas pada prosedur
	Bagan Alur Prosedur	Tabel bagan alur

Stuktur Bab	Sub-Bab	Konten
		SOP
SP05 - Prosedur Akses Server Aplikasi SIMRS	Tujuan	Deskripsi umum dan infromasi prosedur
	Ruang Lingkup	
	Definisi	Definisi isilah baru yang digunakan dalam prosedur
	Alur Manajemen Eskalasi	Alur manajemen eskalasi keputusan dan penanganan sesuai kebutuhan prosedur
	Rincian Prosedur	Berisi rincian aktivitas pada prosedur
	Bagan Alur Prosedur	Tabel bagan alur SOP
SP06 - Prosedur Pemantauan Keamanan Akses Komputer	Tujuan	Deskripsi umum dan infromasi prosedur
	Ruang Lingkup	
	Definisi	Definisi isilah baru yang digunakan dalam prosedur
	Alur Manajemen Eskalasi	Alur manajemen eskalasi keputusan dan penanganan sesuai kebutuhan prosedur
	Rincian Prosedur	Berisi rincian aktivitas pada prosedur
	Bagan Alur Prosedur	Tabel bagan alur SOP

6.3 Hasil Perancangan SOP

Pada sub-bab ini akan dijelaskan mengenai hasil akhir dari perencanaan dan perancangan SOP yang telah diinisasi berdasarkan dari sub-bab sebelumnya. Berikut menampilkan pemetaan dari perancangan SOP dengan formulir dan instruksi yang digunakan pada setiap prosedur.

Tabel 6. 4 Konten SOP

No Dokumen	Nama Dokumen Sop	No Dokumen	Dokumen Terkait
SP01	**SOP Pembuatan dan Perubahan Hak Akses Akun Aplikasi SIMRS**	KJ01	Kebijakan Pengendalian Hak Akses Sistem Informasi
		FM01	Formulir Permintaan Akun Baru
		FM02	Formulir Permintaan Perubahan Akses
		FM04	Formulir Log Perekaman Permintaan Hak Akses
		IK01	Instruksi Kerja Penambahan Akun dan Hak Akses
		IK02	Instruksi Kerja Penghapusan Hak Akses Akun
SP02	**SOP Peninjauan Hak Akses pada Aplikasi SIMRS**	KJ01	Kebijakan Pengendalian Hak Akses Sistem Informasi
		FM06	Formulir Pemantauan dan Evaluasi Hak Akses
SP03	**SOP Penghapusan**	KJ01	Kebijakan Pengendalian Hak

No Dokumen	Nama Dokumen Sop	No Dokumen	Dokumen Terkait
	Hak Akses pada Aplikasi SIMRS		Akses Sistem Informasi
		FM03	Formulir Penghapusan Hak Akses
		FM04	Formulir Log Perekaman Permintaan Hak Akses
		IK02	Instruksi Kerja Penghapusan Hak Akses Akun
SP04	**SOP Pemeliharaan Keamanan Akses pada Akun Aplikasi SIMRS**	KJ02	Kebijakan Ketentuan Pengguna
		FM07	Formulir Log Permasalahan Hak Akses
SP05	**SOP Akses Server Aplikasi SIMRS**	KJ03	Kebijakan Pengendalian Akses Fisik Fasilitas Teknologi Informasi
		FM08	Formulir Log Akses Server
		FM09	Formulir Permintaan Akses Server Pengunjung
SP06	**SOP Pemantauan Keamanan Akses Komputer**	KJ03	Kebijakan Pengendalian Akses Fisik Fasilitas Teknologi Informasi
		FM10	Formulir Pemantauan Keamanan Akses Komputer

6.3.1 Kebijakan

Menurut PER/35/M.PAN/06/2012 agar SOP dapat bersifat mengikat untuk seluruh pegawai dan dapat dilaksanakan dengan penuh komitmen, maka suatu SOP harus memiliki landasan hukum yang jelas dari pihak direksi. Landasan hukum tersebut dapat berupa kebijakan yang disahkan oleh pihak direksi untuk dilaksanakan dalam bentuk prosedur-prosedur yang memenuhi kebijakan tersebut. Kebijakan yang dibuat pada penelitian ini mengacu pada ISO27002:2013 sebagai usulan kebijakan kontrol akses kepada Rumah Sakit Dokter Moewardi. Contoh salah satu bentuk kebijakan yang telah dibuat dapat dilihat pada Lampiran D. Berikut adalah penjelasan dari masing-masing kebijakan yang dibuat.

6.3.1.1 Kebijakan Pengendalian Akses Sistem Informasi

Kebijakan ini dibuat berdasarkan panduan umum pada kontrol obyektif 9.1.1 *Access control policy,* 9.2.1 *User registration and de-registration, 9.2.2 User access provisioning, 9.4.1 Information access restriction, 9.2.5 Review of user access right* dan *9.2.6 Removal or adjustment of access rights* yang adan di ISO27002:2013. Kebijakan ini terdiri dari 3 peraturan yaitu mengenai pengelolaan hak akses pengguna sistem informasi, pengalolaan hak akses sementara dan persyaratan akun pengguan.

6.3.1.2 Kebijakan Ketentuan Pengguna Sistem Informasi

Kebijakan ini dibuat berdasarkan panduan umum pada kontrol obyektif 9.3.1 *Use of secret authentication information* yang ada di ISO27002:2013. Kebijakan ini berisi mengenai peraturan untuk melindungi informasi authentikasi pribadi bagi seluruh pengguna sistem informasi yang ada di Rumah Sakit Dokter Moewardi.

6.3.1.3 Kebijakan Pengendalian Akses Fisik Fasilitas Teknologi Informasi

Kebijakan ini dibuat berdasarkan panduan umum pada kontrol obyektif *11.1.2 Physical entry controls, 11.1.5 Working in*

secure area, 11.2.8 *Unattended user equipment* dan 11.2.9 *Clear desk and clear screen policy.* Kebijakan ini berisi 2 peraturan yaitu, peraturan pengelolaan keamanan akses fasilitas TI dan peraturan untuk melindungi akses fasilitas perangkat TI.

6.3.2 Prosedur

Terdapat 6 prosedur yang dihasilkan dalam penelitian ini. Prosedur ini dibuat sebagai pelaksanaan kebijakan yang telah dibuat sebelumnya. Contoh dari salah satu Prosedur yang telah dihasilkan dalam penelitian ini dapat dilihat pada Lampiran E. Berikut adalah penjelasan mengenai prosedur-prosedur yang dihasilkan.

6.3.2.1 Prosedur Pembuatan dan Perubahan Hak Akses Akun Aplikasi SIMRS (SP01)

Prosedur ini terdiri dari 2 sub-prosedur yaitu sub-prosedur pembuatan akun baru dan sub-prosedur perubahan akses lama. Prosedur ini dibuat sebagai tindakan untuk mitigasi risiko R16.2 yaitu kesalahan pemberian hak akses pada user Aplikasi SIMRS. Dimana kontrol pada ISO27002:2013 yang dianggap sesuai untuk mengurangi risiko tersebut adalah kontrol 9.2.1 *User registration and de-registration, 9.2.2 User access provisioning* dan *9.4.1 Information access restriction,* sehingga prosedur ini dibuat dengan menggunakan acuan kontrol-kontrol tersebut. Prosedur ini merupakan bentuk pelaksanaan dari kebijakan pengendalian akses sistem informasi (KJ01) yang telah dibuat sebelumnya.

6.3.2.2 Prosedur Peninjauan Hak Akses pada Aplikasi SIMRS (SP02)

Prosedur ini dibuat sebagai tindakan untuk memitigasi risiko R16.3 yaitu kurangnya evaluasi dan monitoring pada hak akses Aplikasi SIMRS. Dimana kontrol pada ISO27002:2013 yang dianggap sesuai untuk mengurangi risiko tersebut adalah kontrol *9.2.5 Review of user access rights*, sehingga prosedur ini dibuat dengan menggunakan acuan yang ada didalam

kontrol tersebut. Prosedur ini merupakan bentuk pelaksanaan dari kebijakan pengendalian akses sistem informasi (KJ01) yang telah dibuat sebelumnya.

6.3.2.3 Prosedur Penghapusan Hak Akses Pada Aplikasi SIMRS (SP03)

Prosedur ini dibuat sebagai tindakan untuk memitigasi risiko R16.1 yaitu eksploitasi akun pegawai yang sudah pindah atau pensiun. Dimana kontrol pada ISO27002:2013 yang dianggap sesuai untuk mengurangi risiko tersebut adalah kontrol *9.2.6 Removal or adjustment of access rights*, sehingga prosedur ini dibuat dengan menggunakan acuan yang ada didalam kontrol tersebut. Prosedur ini merupakan bentuk pelaksanaan dari kebijakan pengendalian akses sistem informasi (KJ01) yang telah dibuat sebelumnya.

6.3.2.4 Prosedur Pemeliharaan Keamanan Akses Pada Akun Aplikasi SIMRS (SP04)

Prosedur ini dibuat sebagai tindakan untuk memitigasi risiko R16.4 yaitu *Sharing password* pada user Aplikasi SIMRS, risiko R28.1 yaitu terjadi *social engineering* pada user maupun admin, risiko R02.1 yaitu pencurian *username* dan *password* pada user, dan risiko R02.2 yaitu exploitasi *session login.* Dimana kontrol pada ISO27002:2013 yang dianggap sesuai untuk mengurangi risiko tersebut adalah kontrol *9.3.1 Use of Secret Authentication Information*, sehingga prosedur ini dibuat dengan menggunakan acuan yang ada didalam kontrol tersebut. Prosedur ini merupakan bentuk pelaksanaan dari kebijakan ketentuan sistem informasi (KJ02) yang telah dibuat sebelumnya.

6.3.2.5 Prosedur Pemeliharaan Keamanan Akses Pada Akun Aplikasi SIMRS (SP05)

Prosedur ini dibuat sebagai tindakan untuk memitigasi risiko R08.1 yaitu pihak luar yang masuk ke ruang server secara ilegal dan risiko R08.3 yaitu kelalaian petugas yang meninggalkan ruang server dalam keadaan tidak terkunci.

Dimana kontrol pada ISO27002:2013 yang dianggap sesuai untuk mengurangi risiko tersebut adalah kontrol *11.1.2 Physical entry controls* dan kontrol *11.1.5 Working In Secure Area*, sehingga prosedur ini dibuat dengan menggunakan acuan yang ada didalam kontrol tersebut. Prosedur ini merupakan bentuk pelaksanaan dari kebijakan pengendalian akses fisik fasilitas teknologi informasi (KJ03) yang telah dibuat sebelumnya.

6.3.2.6 Prosedur Pemantauan Keamanan Akses Komputer (SP06)

Prosedur ini dibuat sebagai tindakan untuk memitigasi risiko R13.2 yaitu kelalaian pengguna yang meninggalkan PC dalam keadaan menyala/ tidak terkunci dan risiko R02.2 yaitu penulisan *username* dan *password* pada lokasi yang mudah dilihat. Dimana kontrol pada ISO27002:2013 yang dianggap sesuai untuk mengurangi risiko tersebut adalah kontrol *11.2.8 Unattended user equipment* dan kontrol *11.2.9 Clear desk and clear screen policy,* sehingga prosedur ini dibuat dengan menggunakan acuan yang ada didalam kontrol tersebut. Prosedur ini merupakan bentuk pelaksanaan dari kebijakan pengendalian akses fisik fasilitas teknologi informasi (KJ03) yang telah dibuat sebelumnya.

6.3.3 Formulir

Dalam mendukung pelaksanaan prosedur, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Contoh dari bentuk formlir yang dihasilkan dalam penelitian ini dapat dilihat pada Lampiran F. Berikut adalah formulir-formulir yang dibutuhkan untuk mendukung pelaksanaan setiap prosedur.

6.3.3.1 Formulir Permintaan Akun Baru

Formulir ini diisi oleh pengguna yang ingin meminta akses ke Aplikasi SIMRS. Formulir ini merupakan pendokumentasian dari prosedur SP01 sub-prosedur pembuatan akses baru. Pelaksanaan formulir ini akan menyebabkan perubahan pada

format surat permintaan hak akses yang ada saat ini. Surat permintaan hak akses saat ini berisikan informasi password dan username yan ingin diajukan oleh pengguna, sementara untuk formulir ini surat permintaan hak akses hanya perlu mencantumkan permintaan username dari pengguna. Hal ini dikarenakan apabila surat permintaan hak akses saat ini terus diterapkan maka dapat menimbulkan celah keamanan pada kontrol akses.

6.3.3.2 Formulir Permintaan Perubahan Akses

Formulir ini merupakan pendokumentasian dari prosedur SP01 sub-prosedur perubahan hak akses lama. Formulir ini diisi oleh pengguna yang ingin meminta akses ke Aplikasi SIMRS. Perubahan yang dilakukan oleh formulir ini adalah pengguna harus menyertakan alasan perubahan hak akses.

6.3.3.3 Formulir Penghapusan Hak Akses

Formulir ini merupakan pendokumentasian dari prosedur SP03. Formulir ini diisi oleh admin Aplikasi SIMRS. Masukan dari formulir ini ada 2, yaitu surat permintaan penghapusan akses atau hasil dari peninjauan hak akses (SP02) yang telah dilakukan oleh admin.

6.3.3.4 Formulir Log Perekaman Permintaan Hak Akses

Formulir ini merupakan pendokumentasian dari prosedur SP01 dan SP03. Formulir ini diisi oleh petugas administrasi untuk menyimpan catatan mengenai perubahan penting pada hak akses yang merupakan anjuran dari kontrol ISO27002:2013. Formulir ini mendokumentasikan permintaan penambahan, prubahan dan penghapusan hak akses pada akun Aplikasi SIMRS.

6.3.3.5 Formulir Verifikasi dan Pemberian Akses

Formulir ini merupakan pendokumentasian dari prosedur SP01 dan SP03. Formulir ini mendokumentasikan pembatasan hak akses sesuai dengan kebutuhan proses bisnis dari pengguna sesuai dengan anjuran yang ada pada ISO27002:2013.

6.3.3.6 Formulir Pemantauan dan Evaluasi Hak Akses

Formulir ini merupakan pendokumentasian dari prosedur SP02. Formulir ini mendokumentasikan proses review hak akses user pada Aplikasi SIMRS yang dilakukan secara berkala sesuai dengan panduan pada kontrol ISO27002:2013.

6.3.3.7 Formulir Log Permasalahan Hak Akses

Formulir ini merupakan pendokumentasian dari prosedur SP04. Formulir ini mendokumentasikan pelaporan permasalahan ataupun insiden terkait dengan hak akses pada Aplikasi SIMRS.

6.3.3.8 Formulir Log Akses Server

Formulir ini merupakan pendokumentasian dari prosedur SP05. Formulir ini nantinya akan diletakkan didalam ruang server dan seluruh personil yang memasuki ruang server diwajibkan untuk mengisi formulir ini.

6.3.3.8 Formulir Permintaan Akses Server Pengunjung

Formulir ini merupakan pendokumentasian dari prosedur SP05. Formulir ini diisi oleh pengunjung yang ingin mengakses server untuk keperluan tertentu. Pengunjung yang dimaksud adalah pegawai maupun pihak luar yang bukan petugas Instalasi Pengelola Data Elektronik.

6.3.3.10 Formulir Pemantauan Keamanan Akses Komputer

Formulir ini merupakan pendokumentasian dari prosedur SP06. Formulir ini diisi oleh petugas hardware dan petugas jaringan Instalasi Pengelola Data Elektronik setiap 1 bulan sekali bersamaan dengan pemantauan hardware untuk proses pemeliharaan yang ada saat ini.

6.3.4 Instruksi Kerja

Dalam mendukung pelaksanaan SOP, dibutuhkan beberapa instruksi kerja yang berfungsi sebagai media transfer pengetahuan apabila terjadi pergantian petugas.

6.3.4.1 Instruksi Kerja Penambahan Akun dan Hak Akses

Instruksi ini dijalankan oleh admin sebagai petunjuk teknis pelaksanaan penambahan akun dan penambahan hak akses pada Aplikasi SIMRS. Instruksi ini terdiri dari instruksi penambahan akun baru dan instruksi penambahan hak akses baru. Instruksi ini membutuhkan formulir verifikasi dan pemberian akses (FM05) yang telah disetujui oleh Kepala Instalasi Pengelola Data Elektronik sebagai panduan pemberian hak akses.

6.3.4.2 Instruksi Kerja Penghapusan Hak Akses Akun

Instruksi memberikan manual panduan tentang cara penghapusan hak akses sebagian maupun penghapusan akun secara keseluruhan. Instruksi ini akan dijalankan oleh admin pada Aplikasi SIMRS untuk pembatasan hak akses.

6.4 Hasil Pengujian SOP

Pengujian SOP dilakukan dengan verifikasi dan validasi. Verifikasi dilakukan dengan wawancara untuk memastikan kesesuian antara prosedur yang dihasilkan dengan kebutuhan. Sementara validasi dilakukan dengan cara mensimulasikan SOP untuk mengetahui ketepatan prosedur ketika diimplementasikan dalam kasus yang nyata.

6.4.1 Hasil Verifikasi

Verifikasi dilakukan untuk memastikan bahwa SOP yang dibuat telah sesuai dengan kontrol standar yang telah dipilih. Berdasarkan hasil verifikasi yang dapat dilihat pada Lampiran F dapat diketahui pemenuhan SOP dengan kontrol yang ada pada ISO 27002:2013. Berdasarkan kontrol pada ISO 27002:2013 yang ditentukan diawal diketahui bahwa penelitian ini menyusun SOP debgan menggunakan acuan 12 kontrol obyektif pada ISO 27002:2013. Pada kontrol akses *Physical* didapatkan 2 SOP yang mengacu pada 4 kontrol obyektif klausul 11 ISO 27002:2013 dan kontrol akses *Logical* didapatkan 4 SOP yang mengacu 7 kontrol Obyektif pada

kalusul 9 ISO 27002:2013. Kontrol obyektif yang dipenuhi SOP pada penelitian ini yaitu:

1. *9.1.1 Access control policy*
2. *9.2.1 User registration and de-registration*
3. *9.2.2 User access provisioning*
4. *9.2.5 Review of user access rights*
5. *9.2.6 Removal or adjustment of access rights*
6. *9.3.1 Use of secret authentication information*
7. *9.4.1 Information access restriction*
8. *11.1.2 Physical entry controls*
9. *11.1.5 Working In Secure Area*
10. *11.2.8 Unattended user equipment*
11. *11.2.9 Clear desk and clear screen policy*

6.4.2 Hasil Validasi

Validasi SOP dilakukan dengan dua tahap. Tahap awal adalah konformasi dengan cara wawancara pada Kepala IPDE dan Staff IPDE yang terkait. Dari hasil validasi awal dibutuhkan beberapa revisi dokumen SOP, yaitu :

1. Perubahan pada Prosedur Pembuatan Akun Baru

Sebelum dilakukan perubahan, aktor yang diharuskan mengisi formulir Permintaan Akun Baru adalah petugas Administrasi IPDE. Namun setelah diverifikasi surat permintaan yang ada saat ini tidak memuat detail dari identitas pemohon sehingga Petugas Administrasi harus menghubungi pemohon lebih lanjut. Sehingga skenario diubah menjadi aktor yang diwajibkan mengisi formulir Permintaan Akun Baru adalah user tersebut sendiri.

No	Uraian Prosedur	Pela	
		User	Petugas Administrasi
1.Proses Penerimaan Permintaan Akses Baru			
1.	Mengirimkan surat permintaan username dan password ke Instalasi PDE		
2.	Menerima surat permintaan username dan password		
3.	Mencatat permintaan akses baru dalam Formulir Pembuatan Akses Baru (FM02)		

Gambar 6. 1 Skenario sebelum perubahan

Setelah dilakukan perubahan maka peneliti menambahkan formulir yang akan diisi oleh user.

No	Uraian Prosedur	Pela	
		User	Petugas Administrasi
1. Proses Pengajuan Permintaan Akun Baru			
1.	Membuat surat permohonan pembuatan akun baru Aplikasi SIMRS yang disetujui oleh Kepala Unit terkait		
2.	Mengisi Formulir Permintaan Akun Baru (FM01)		
3.	Menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran ke petugas Administrasi Instalasi PDE		

Gambar 6. 2 Skenario setelah perubahan

2. Perubahan pada Formulir Verifikasi dan Pemberian Akses

Sebelum perubahan, kolom pemberian akses diisi dengan Beban Akses Saat ini dan Permintaaan Beban Akses. Namun setelah dilakukan verifikasi dengan admin, kalimat tersebut dirasa membingungkan, sehingga diubah menjadi Grup dan Akses Unit Saat ini dan Grup dan Akses Unit yang diajukan. Grup disini berisi modul-modul layanan hak akses.

INFORMASI AKUN SAAT INI		
Username		
Beban Akses Saat ini	**Level User**	**Wewenang**
	☐ Super User ☐ Admin ☐ Operator	☐ Administrator ☐ Membaca ☐ Menambah ☐ Menghapus
PERUBAHAN YANG DIAJUKAN		
Username		
Permintaan Beban Akses	**Level User**	**Wewenang**
	☐ Super User ☐ Admin ☐ Operator	☐ Administrator ☐ Membaca ☐ Menambah ☐ Menghapus

Gambar 6. 3 Formulir Verifikasi dan pemberian Akses sebelum perubahan

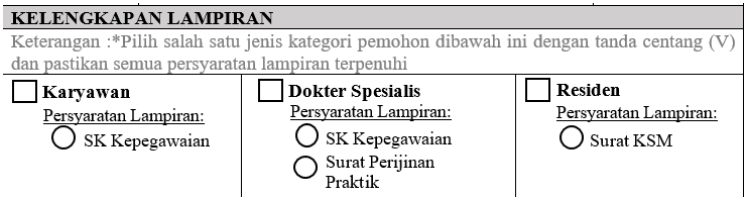
Setelah dilakukan perubahan maka kalimat diubah menjadi Grup dan Akses unit saat ini.

INFORMASI AKUN SAAT INI *		
*Isi jika jenis pemberian akses *Perubahan Akses*		
Grup dan Akses Unit Saat ini	**Level User**	**Wewenang**
(Modul akses dan unit sesuai acuan role hak akses)	☐ Administrator ☐ Supervisor ☐ User Operator	☐ Administrator ☐ Membaca ☐ Menambah ☐ Menghapus
HAK AKSES YANG DIAJUKAN		
Grup dan Akses Unit yang Diajukan	**Level User**	**Wewenang**
(Modul akses dan unit sesuai acuan role hak akses)	☐ Administrator ☐ Supervisor ☐ User Operator	☐ Administrator ☐ Membaca ☐ Menambah ☐ Menghapus

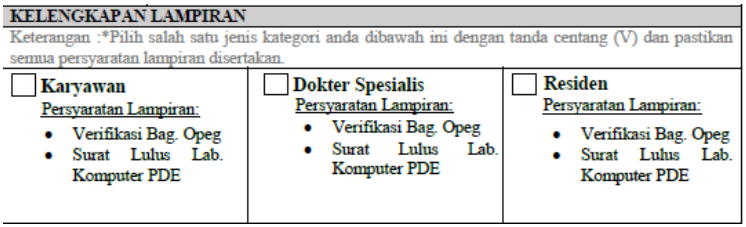
Gambar 6. 4 Formulir Verifikasi dan pemberian Akses setelah perubahan

3. Perubahan pada Formulir Permintaan Akun Baru dan Formulir Perubahan Akses

Sebelum perubahan, persyaratan lampiran pada formulir ini memerlukan fotokopi SK Kepegawaian dari Bagian Organisasi dan Kepegawaian yang disesuaikan dengan proses validasi kebenaran data kepegawaian saat ini. Namun setelah melakukan validasi dengan Kepala IPDE, lampiran SK Kepegawaian dirasa tidak perlu ditangani oleh IPDE karena hal tersebut merupakan tanggungjawab Bagian Organisasi dan Kepegawaian, sehingga persyaratan lampiran diubah menjadi verifikasi Bagian Organisasi dan Kepegawaian, dimana verifikasi tersebut adalah berupa surat disposisi dan Surat Lulus Laboratorium Komputer PDE. Surat ini diperlukan untuk memastikan bahwa pengguna mengerti cara mengoperasikan komputer.



Gambar 6. 5 Formulir Perubahan Akses sebelum dilakukan perubahan



Gambar 6. 6 Formulir Perubahan Akses setelah dilakukan perubahan

4. Perubahan pada Formulir Log Pemasalahan Hak Akses

Sebelum dirubah, kolom saluran berisi “telepon/ email / offline”. Namun setelah dilakukan verifikasi, proses saat ini

tidak pernah menggunakan email, sehingga saluran hanya diisi "telepon / offline"

5. Perubahan pada Formulir Pemantauan dan Evaluasi Hak Akses

Sebelum dirubah, keterangan mengharuskan jangka waktu pemantauan dan evaluasi dilakukan setiap 1 tahun sekali sesuai dengan anjuran Kepala IPDE. Namun setelah dilakukan verifikasi dengan Admin Apikasi, maka jangka waktu diubah menjadi 1 bulan sekali, hal ini dikarenakan pergantian residen biasanya 3 bulan, sehingga jangka waktu 1 tahun terlalu lama.

Validasi SOP selanjutnya dilakukan dengan mensimulasikan beberapa aktivitas operasional yang benar-benar terjadi. Validasi yang dilakukan tidak mencakup semua prosedur karena keterbatasan sumber daya pendukung. Berikut adalah pemetaan antara masing-masing prosedur dan skenario simulasinya.

Tabel 6. 5 Hasil Validasi dengan Simulasi

No	SOP	Skenario	Tanggal	Keterangan
1	SOP Penanganan Permintaan Hak Akses Aplikasi SIMRS	Mencoba mensimulasikan dengan masukan salah satu surat permintaan pembuatan akun baru	16 Juni 2017	Dilakukan dengan baik
2	SOP Peninjauan Hak Akses pada Akun Aplikasi SIMRS	Mensimulasikan dengan masukan kasus akun yang redundan	16 Juni 2017	Dilakukan dengan baik
3	SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS	Mensimulasikan dengan menindaklanjuti masukan kasus akun yang redundan dari peninjauan	16 Juni 2017	Dilakukan dengan baik

4	SOP Pemeliharaan Keamanan Akses pada Akun Aplikasi SIMRS	Mensimulasikan dengan masukan salah satu user merasa tidak pernah melakukan suatu transaksi namun transaksi tersebut tercatat pada sistem dengan akunnya.	16 juni 2017	Dilakukan dengan baik
5.	SOP Akses Server Aplikasi SIMRS	Mensimulasikan dengan masukan peneliti sebagai mahasiswa ingin meminta ijin untuk mengakses ruang server untuk keperluan penelitian tugas akhir	16 juni 2017	Dilakukan sebatas verifikasi ketersesuaian prosedur dan formulir karena keterbatasan waktu.
6.	SOP Pemantauan Keamanan Akses Komputer	Mensimulasikan pemantauan keamanan akses komputer yang ada didalam Ruang IPDE	1 Juli 2017	Dilakukan dengan baik

Halaman ini sengaja dikosongkan

BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

7.1 Kesimpulan

Kesimpulan yang dibuat adalah jawaban dari perumusan masalah yang telah didefinisikan sebelumnya dan berdasarkan hasil penelitian yang telah dilakukan. Kesimpulan yang didapat dari tahap identifikasi risiko hingga perancangan dan validasi dokumen produk adalah :

1. **Hasil identifikasi risiko akses *physical* dan *logical* pada aset infromasi yang terkait dengan Aplikasi SIMRS di Rumah Sakit Dokter Moewardi**

Berdasarkan metode analisis risiko OCTAVE dengan mengidentifikasi Aset Informasi tekait dengan Aplikasi SIMRS maka didapat 29 risiko keamanan aset informasi. Risiko tersebut kemudian dipetakan sehingga didapatkan hasil pemetaan 11 risiko akses, yaitu 6 risiko akses *logical* dan 5 risiko kontrol akses *physical* . Risiko tersebut didapat dari total risiko aset informasi terkait dengan Aplikasi SIMRS yaitu sebanyak 29 risiko. Berikut dibawah adalah risiko-risiko akses *logical* dan *physical* tersebut, yakni :

Tabel 7. 1 Risiko Kontrol Akses *Logical* dan *Physical* pada Aplikasi SIMRS

Kategori Aset Kritis	Aset Kritis	Risiko		Penyebab		Nilai RPN	Kategori
		ID	Nama	ID	Nama		
Risiko Akses *Logical*							
Software	Aplikasi SIMRS	R16	Aplikasi diakses oleh pihak tidak berwenang	R16.1	Eksploitasi akun pegawai yang sudah pindah atau pensiun	252	*Very High*
Software	Aplikasi SIMRS	R16	Aplikasi diakses oleh pihak tidak berwenang	R16.2	Kesalahan pemberian hak akses pada user Aplikasi SIMRS	216	*Very High*
Software	Aplikasi SIMRS	R16	Aplikasi diakses oleh pihak tidak berwenang	R16.3	Kurangnya evaluasi dan monitoring pada hak akses Aplikasi SIMRS	441	*Very High*
Software	Aplikasi SIMRS	R16	Aplikasi diakses oleh pihak tidak berwenang	R16.4	*Sharing password* pada user Aplikasi SIMRS	*405*	*Very High*
Software	Data	R02	Manipulasi data	R02.1	Pencurian *username* dan *password* pada user	100	*Medium*
Software	Data	R02	Manipulasi data	R02.2	Exploitasi *session login*	140	*High*
Risiko Akses *Physical*							
Hardware	Server	R08	Akses tidak sah ke ruang server	R08.1	Pihak luar yang masuk ke ruang server secara ilegal	45	Low

Hardware	Server	R08	Akses tidak sah ke ruang server	R08.2	Kurangnya evaluasi hak akses pada peralatan dan ruangan server	135	*High*
Hardware	Server	R08	Akses tidak sah ke ruang server	R08.3	Kelalaian petugas yang meninggalkan ruang server dalam keadaan tidak terkunci	180	*High*
Hardware	PC	R13	Akses tidak sah ke PC	R13.2	Kelalaian pengguna yang meninggalkan PC dalam keadaan menyala/tidak terkunci	196	*High*
Software	Data	R02	Manipulasi Data	R02.2	Penulisan username dan password pada lokasi yang mudah dilihat	108	*Medium*

2. **Hasil pembuatan dokumen SOP kontrol akses *physical* dan *logical* pada Aplikasi SIMRS di Rumah Sakit Dokter Moewardi berdasarkan mitigasi risiko untuk pihak Instalasi Pengelola Data Elektronik.**

   Berdasarkan hasil identifikasi risiko dan rekomendasi mitigasi risiko dengan kontrol pada ISO 27002:2013, didapatkan usulan pembuatan **3 Kebijakan** yaitu 1)Kebijakan Pengendalian Hak Akses Sistem Informasi 2)Kebijakan Ketentuan Pengguna 3)Kebijakan Pengendalian Akses Fisik Fasilitas Teknologi Informasi dan **6 SOP** yaitu 1)SOP Penanganan Permintaan Hak Akses Aplikasi SIMRS dengan dua sub-prosedur yaitu sub-prosedur Pembuatan Akun Baru dan sub-prosedur Perubahan Hak Akses Lama 2)SOP Peninjauan Hak Akses pada Akun Aplikasi SIMRS 3)SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS 4)SOP Pemeliharaan Keamanan Akses pada Akun Aplikasi SIMRS 5)SOP Akses Server Aplikasi SIMRS dan 6)SOP Pemantauan Keamanan Akses Komputer.

   Selain 3 Kebijakan dan 6 Prosedur tersebut, dihasilkan juga beberapa instrument pendukung dokumen SOP berupa instruksi kerja dan formulir untuk melengkapi dokumen SOP tersebut. Formulir tersebut antara lain yaitu 1)Formulir Permintaan Akun Baru 2)Formulir Permintaan Perubahan Akses 3)Formulir Penghapusan Hak Akses 4)Formulir Log Perekaman Hak Akses 5)Formulir Verifikasi dan Pemberian Akses 6)Formulir Pemantauan dan Evaluasi Hak Akses 7)Formulir Log Permasalahan Hak Akses 8)Formulir Log Akses Server 9)Formulir Permintaan Akses Server Pengunjung dan 10)Formulir Pemantauan Keamanan Akses Komputer. Instruksi Kerja yang dihasilkan antara lain 1)Instruksi

Kerja Penambahan Akun dan Hak Akses 2)Instruksi Kerja Penghapusan Hak Akses Akun

3. **Hasil verifikasi dan validasi dokumen SOP kontrol akses pada Aplikasi SIMRS di Rumah Sakit Dokter Moewardi.**

- Verifikasi

Dari kontrol pada ISO 27002:2013 yang ditentukan diawal diketahui bahwa penelitian ini menyusun SOP dengan menggunakan acuan 12 kontrol obyektif pada ISO 27002:2013. Pada kontrol akses Physical didapatkan 2 SOP yang mengacu pada 4 kontrol obyektif klausul 11 ISO 27002:2013 dan kontrol akses *Logical* didapatkan 4 SOP yang mengacu 7 kontrol Obyektif pada kalusul 9 ISO 27002:2013. Kontrol obyektif yang dipenuhi SOP pada penelitian ini yaitu:

1. *9.1.1 Access control policy*
2. *9.2.1 User registration and de-registration*
3. *9.2.2 User access provisioning*
4. *9.2.5 Review of user access rights*
5. *9.2.6 Removal or adjustment of access rights*
6. *9.3.1 Use of secret authentication information*
7. *9.4.1 Information access restriction*
8. *11.1.2 Physical entry controls*
9. *11.1.5 Working In Secure Area*
10. *11.2.8 Unattended user equipment*
11. *11.2.9 Clear desk and clear screen policy*

- Validasi

Pada proses validasi tahap awal dilakukan diskusi mengenai dokumen SOP yang dihasilkan sebelum disimulasikan oleh pihak yang berkepentingan. Terdapat beberapa perubahan dari dokumen awal yang sudah dibuat seperti perubahan aktor pengisi formulir dan waktu pelasanaan pelaporan.

7.2 Saran

Saran yang dapat peneliti sampaikan terkait dengan pengerjaan tugas akhir ini meliputi dua hal, yaitu saran untuk pihak Instalasi Pengelola Data Elektronik RSUD Dr. Moewardi dan saran untuk penelitian selanjutnya.

Saran yang dapat diberikan untuk pihak Instalasi Pengelola Data Elektronik RSUD Dr. Moewardi adalah :

1. Penulis menyarankan agar dokumen SOP yang telah diuji bisa benar-benar diterapkan dengan baik. Hal pertama yang dapat dilakukan oleh Instalasi Pengelola Data Elektronik RSUD Dr. Moewardi adalah melakukan rencana penerapan dan melakukan sosialisasi pada seluruh pihak yang terkait pada seluruh pelaksanan SOP.
2. Usulan formulir log diimplementasikan dengan baik untuk mengelola catatan pemeliharaan hak akses.

Saran yang dapat penulis berikan untuk penelitian selanjutnya adalah :

1. Penelitian ini sebatas pembuatan dokumen SOP hingga proses pengujian tanpa memantau pengimplementasian SOP tersebut dan pengaruhnya bagi proses bisnis organisasi. Untuk penelitian selanjutnya, dapat dilakukan pengujian dan evaluasi keefektifan dokumen SOP ini terhadap peningkatan kontrol akses *physical* dan *logical* aset informasi terkait dengan Aplikasi SIMRS.
2. Penelitian ini hanya mengacu pada beberapa kontrol objektif ISO27002:2013 dan tidak secara keseluruhan memenuhi salah satu domain atau klausul pada kerangka kerja tesebut, sehingga dalam penelitian selanjutnya dianjurkan untuk melengkapi objektif pada salah satu domain atau klausul pada kerangka

kerja sehingga kontrol dalam penyusunan SOP lebih menyeluruh dan patuh.

DAFTAR PUSTAKA

[1] E. Hariana, Y. G. Sanjaya, and A. R. Rahmawati, "PENGGUNAAN SISTEM INFORMASI MANAJEMEN RUMAHSAKIT (SIMRS) DI DIY," *Semin. Nasionla Sist. Inf. Indones.*, 2013.

[2] Menteri Kesehatan Republik Indonesia, "Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit," *Peratur. Menteri Kesehat. Republik Indones. Nomor 82 Tahun 2013 tentang Sist. Inf. Manaj. Rumah Sakit*, pp. 1–37, 2013.

[3] MENTERI KESEHATAN REPUBLIK INDONESIA, "PETA JALAN SISTEM INFORMASI KESEHATAN TAHUN 2015-2019," 2015.

[4] M. E. Whitman and H. J. Mattord, "Principles of information security," *Course Technol.*, pp. 1–617, 2012.

[5] T. Ngqondi, "The ISO / IEC 27002 and ISO / IEC 27799 Information Security Management Standards : A Comparative Analysis from a Healthcare Perspective Tembisa G . Ngqondi Magister Technologiae School of Information and Communication Technology Faculty of Engineering ," *Geneva*, 2009.

[6] R. Krutz and R. Vines, *The CISSP prep Guide: Mastering the ten domains of Computer Security*. 2001.

[7] S. Harris, *All in one CISSP*. 2013.

[8] J. Gough and M. Hamrell, "Standard Operating Procedures (SOPs): How to Write Them to Be Effective Tools," *Drug Inf. J.*, vol. 44, no. 4, pp. 463–468, 2010.

[9] D. Innike, C. H. Bekti, and M. A. Hanim,

"PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS DI DIVISI TI PT. BANK XYZ SURABAYA," no. September, 2014.

[10] T. A. Megawati, H. M. Astuti, and A. Herdiyanti, "Pengelolaan Risiko Aset Teknologi Informasi Pada Perusahaan Properti Pt Xyz , Tangerang Berdasarkan," no. September, 2014.

[11] W. S. Maurice and N. S. Peter, "Physical and Logical Access Security," *George Mason University*, 2016. [Online]. Available: https://universitypolicy.gmu.edu/policies/physical-and-logical-access-security/. [Accessed: 13-Apr-2017].

[12] R. Anderson, "Access Control," *Secur. Eng. A Guid. to Build. Dependable Distrib. Syst.*, no. Access Control, pp. 51–71, 2011.

[13] M. Gregg and D. Kim, "The Role Authentication, Authorization and Accountability Play in a Secure Organization," 2005. [Online]. Available: http://flylib.com/books/en/1.35.1.25/1/.

[14] W. R. Wicaksana, A. Herdiyanti, and T. D. Susanto, "Pembuatan Standar Operasional Prosedur (SOP) Manajemen Akses Untuk Aplikasi E-Performance Bina Program Kota Surabaya Berdasarkan Kerangka Kerja ITIL V3 Dan ISO," vol. 6, no. 1, pp. 101–116, 2016.

[15] G. Westerman and R. Hunter, "IT Risk : Turning Business Threats into Competitive Advantage," no. June, 2007.

[16] ISMRC, "Information Security Handbook," 2009. .

[17] A. Novia, R. Yanuar, F. A. W, and D. J. Dwi, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)," 2015.

[18] C. Alberts and A. Dorofee, "Introduction to the

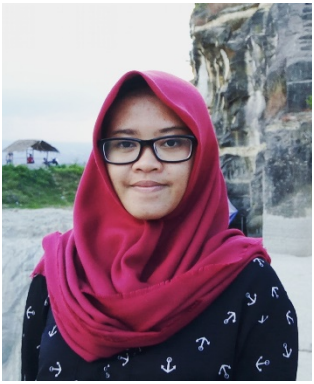
OCTAVE Approach," ... , *PA, Carnegie Mellon ...*, no. August, pp. 1–37, 2003.

[19] I. Akyar, "Standard Operating Procedure (What Are Thry Good For?)," *InTech*, 2012. [Online]. Available: Isin Akyar (2012). Standard Operating Procedures (What Are They Good For ?), Latest Research into Quality Control, Dr. Mohammad Saber Fallah Nezhad (Ed.), InTech, Dhttps://www.intechopen.com/books/latest-research-into-quality-control/standard-operating-pr. [Accessed: 13-Apr-2017].

[20] Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi RI, "Pedoman penyusunan standar operasional prosedur administrasi pemerintahan," p. 63, 2012.

[21] M. Arikunto, "Pengertian Subyek dan Objek Penelitian," *Scribd*. [Online]. Available: https://id.scribd.com/doc/149548027/Pengertian-Objek-penelitian. [Accessed: 29-Mar-2017].

BIODATA PENULIS



Penulis bernama lengkap Nimas Nawangsih, dilahirkan di Karanganyar pada tanggal 4 Januari 1995. Penulis telah menempuh pendidikan formal di SDN 4 Jaten, tamat SMP di SMPN 1 Karanganyar, tamat SMA di SMAN 1 Karanganyar, dan kemudian masuk perguruan tinggi negeri ITS Surabaya pada jurusan Sistem Informasi (SI), Fakultas Teknologi Informasi pada tahun 2013. Pengalaman yang didapatkan penulis selama melakukan studi di ITS selain dibidang akademik yakni berkecimpung dibeberapa organisasi kemahasiswaan, salah satunya adalah menjadi pengurus di UKM Cinematography of ITS selama 3 Tahun. Penulis pernah menjalani kerja praktik di Bank Indonesia Pusat pada Departemen Pengelolaan Sistem Informasi selama kurang lebih 1,5 bulan pada tahun 2016. Pengalaman yang didapatkan penulis selama bekerja praktik yaitu membuat Dokumen Manajemen Risiko untuk Sistem BI-RTGS dalam rangka membantu perusahaan melaksanakan *Financial Sector Assessment Program* (FSAP).

Pada pengerjaan Tugas Akhir, penulis mengambil bidang minat Manajemen Sistem Informasi dengan topik Manajemen Risiko TI, Tata Kelola TI dan Keamanan Aset Informasi, yakni mengenai pembuatan dokumen *Standard Operating Procedure* (SOP) Kontrol Akses *Physical* dan *Logical* pada

Aplikasi Sistem Informasi Rumah Sakit (SIMRS) Menggunakan Kerangka Kerja OCTAVE, FMEA dan Kontrol ISO 27002:2013 (Studi Kasus: Instalasi Pengelola Data Elektronik Rumah Sakit Dokter Moewardi)**.** **U**ntuk menghubungi penulis, dapat melalui email : nimasnaw@gmail.com

LAMPIRAN A – HASIL INTERVIEW PROTOCOL

Wawancara dengan Kepala Bagian Perencanaan

A. INFORMASI PELAKSANAAN INTERVIEW

Hari/ Tanggal	Kamis/ 2 Mei 2017
Pukul	14:30
Lokasi	Ruang Kerja Bagian Perencanaan

B. PROFIL NARASUMBER

Nama	Drs. Wido
Jabatan	Kepala Bagian Perencanaan
Lama Bekerja	5 Tahun

C. PERTANYAAN INTERVIEW PROTOCOL

NO	URAIAN
	Informasi Umum
	Pertanyaan:
	Apa peran dan tanggungjawab anda sebagai Kepala Bagian Perencanaan pada Aplikasi SIMRS?
	Jawaban:
	Untuk dengan Aplikasi SIMRS yaitu mengkoordinasikan kebutuhan IPDE dengan pihak/unit terkait.
	Pertanyaan:
	Apa fungsi dari Aplikasi SIMRS?
	Jawaban:
	Mempermudah pekerjaan, mempercepat pekerjaan, menjamin keakuratan data, aman dan nyaman. Yang paling penting adalah kecepatan dan ketepatan, karena utamanya Aplikasi SIMRS itu dibuat untuk melayani pasien, pasien merupakan orang yang sedang sakit, sehingga butuh pelayanan yang cepat dan tepat.

	Pertanyaan:
	Bagaimana alur koordinasi Bagian Perencanaan dengan Wakil Direktur Umum terkait Aplikasi SIMRS?
	Jawaban:
	Bagian Perencanaan dengan Wadir Umum merupakan jalur komando, artinya saya menunggu perintah dari Wadir untuk kemudian saya tindaklanjuti dan laksanakan.
	Pertanyaan:
	Bagaimana alur koordinasi Bagian Perencanaan dengan IPDE terkait dengan Aplikasi SIMRS?
	Jawaban:
	Bagian perencanaan dengan IPDE merupakan jalur koordinasi, artinya IPDE secara struktural langsung dibawah Wadir Umum namun ada alur koordinasi dengan Bagian Perencanaan. Ada dua jenis alur koordinasi yaitu *top-down* dan *bottom-up*, untuk masalah Aplikasi SIMRS sendiri bersifat *bottom-up* karena yang ahli adalah pihak IPDE sendiri sehingga jika terdapat pengembangan atau perubahan maka pihak IPDE akan mempresentasikan rencananya ke bagian/unit terkait dan didampingi oleh Bagian Perencanaan. Misalkan ada pengembangan di sistem billing aplikasi, maka akan dipresentasikan dengan Bagian Anggaran dan Perbendaharaa serta Pengelolaan Pendapatan. Terkait dengan kebijakan biasanya pihak IPDE mengusulkan sendiri karena yang ahli dalam bidang IT adalah IPDE nya sendiri, kemudian akan langsung ke direktur untuk disetujui dan ditandatangani. Karena Direktur, Wadir ataupun Bagian Perencanaan tidak ada yang mengerti atau paham betul mengenai IT.
	Informasi Kondisi Keamanan Terkini Berdasarkan Metode OCTAVE
	Pertanyaan:
	Menurut anda, apa saja aset kritis Rumah Sakit yang berkaitan dengan Aplikasi SIMRS?
	Jawaban:

		Data dan hardware, terutama di server harus benar-benar teramankan. Karena data yang diserver itu berhubungan dengan data pasien. Data pasien itu sangat rahasia, sudah ada peraturan-peraturan mulai dari mentri, provinsi sampai dinas terkait dengan kerahasiaan data pasien. Untuk jaringan jangan sampai terdapat hacker karena dapat membahayakan. Selama ini sudah ada kontrol oleh IPDE pada server dan ruang server, dan tidak semua pegawai mengetahui dimana ruang server tersebut. Untuk data sendiri di Aplikasi SIMRS ada banyak macamnya. Untuk data pasien merupakan tanggung jawab Bagian Rekam Medis, data keuangan seperti billing dapat terbagi-bagi, bisa masuk di Bagian Anggaran dan Perbendaharaan atau bisa masuk di Bagian Pengelolaan Pendapatan.
	7.	**Pertanyaan:**
		Apa saja ancaman yang pernah terjadi pada Aplikasi SIMRS?
		Jawaban:
		Selama ini yang sering terjadi adalah kedisiplinan terkait hak akses user aplikasinya, masih sering terjadi satu akun dibagi-bagi entah karena lupa *password*nya sendiri atau alasan lain, namun sering sekali terjadi *sharing username* dan *password*. IPDE sering mendapati ada satu akun digunakan bersamaan oleh beberapa orang, terutama oleh residen, karena residen masih mahasiswa sehingga sering sekali menggunakan cara-cara yang tidak patuh. Ancaman lain yang bahaya yaitu pembajakan tenaga ahli. Karena programmer di IPDE dapat dikatakan sudah ahli dan mereka bukan PNS, hanya pegawai kontrak. Selama ini yang membuat atau mengembangkan Aplikasi SIMRS adalah programmer-programmer yang bersifat kontrak tersebut, sehingga jika kontraknya sudah habis lalu ditawari harga yang mahal bisa saja karya yang sudah dibuat dari RSDM dibajak untuk disalahgunakan.

		Pertanyaan:
		Apa kebutuhan keamanan masing-masing aset yang sudah disebutkan diatas?
		Jawaban:
		Yang utama adalah server. Server itu tidak boleh sembarangan orang tau dan harus selalu dikunci supaya aman. Data-data terutama data pasien supaya tetap terjaga kerahasiaannya dan tidak disalahgunakan oleh pihak manapun tanpa seijin pihak direksi terutama ibu direktur. Karena ancamannya adalah nama baik RS Dokter Moewardi. Terutama dalam menjaga keamanan data pasien, karena jika sampai disalahgunakan maka akan berakibat pasien tidak percaya lagi dan tidak mau berobat ke Rumah Sakit Dokter Moewardi lagi nanti. Untuk software diharapkan sudah ada pengendaliannya. Selama ini faktor ketersediaan sangat penting, karena kembali lagi tujuan utama aplikasi SIMRS adalah melayani pasien atau orang sakit, sehingga butuh pelayanan yang cepat, untuk itu Aplikasi SIMRS harus selalu tersedia dan data-datanya harus tepat atau akurat.
	8.	**Pertanyaan:**
		Apa harapan anda terkait keamanan pada Aplikasi SIMRS?
		Jawaban:
		Harapan saya pada aplikasi SIMRS agar aplikasi ini tidak bisa dihacker, tidak bisa dicuri datanya, tidak boleh dirusak atau disalahgunakan. Lalu untuk user-usernya lebih disiplin terutama untuk masalah hak akses.

Wawancara dengan Kepala Instalasi Pengelola Data Elektronik

A. INFORMASI PELAKSANAAN INTERVIEW

Hari/ Tanggal	Kamis/ 27 April 2017
Pukul	08:00
Lokasi	Ruang Kerja Kepala IPDE

B. PROFIL NARASUMBER

Nama	R. Satrio Budi S, dr., Sp.PD., M.Kes
Jabatan	Kepala IPDE
Lama Bekerja	2 Tahun

C. PERTANYAAN INTERVIEW PROTOCOL

NO	URAIAN
	Informasi Umum
	Pertanyaan:
	Apa peran dan tanggungjawab anda sebagai Kepala IPDE pada Aplikasi SIMRS?
	Jawaban:
	Mengawasi, memonitoring komplain user dan membuat keputusan.
	Pertanyaan:
	Apa fungsi dari Aplikasi SIMRS?
	Jawaban:
	Terdapat beberapa modul pada Aplikasi SIMRS, setiap modul memiliki fungsi masing-masing. Diantaranya ada modul rekam medis yang berfungsi untuk pendataan pasien, resep, perawatannya dll. Didalam modul rekam medis ini terbagi lagi menjadi rawat jalan, rawat inap atau gawat darurat. Selain itu terdapat modul-modul lain seperti pengadaaan, gudang (terdiri dari farmasi dan non-farmasi), farmasi dan billing yang semua punya fungsi

	masing-masing sesuai bagiannya.
Informasi Instalasi Pengelola Data Elektronik	
	Pertanyaan:
	Apa peran dan tanggungjawab dari masing-masing sub-bagian pada IPDE terkait dengan Aplikasi SIMRS?
	Jawaban:
	IPDE terbagi menjadi beberapa divisi, antara lain divisi Application Development, divisi Jaringan (lokal dan wide), divisi Hardware Maintenance, divisi Administrasi, divisi Troubleshooting dan Implementasi.
	Pertanyaan:
	Bagaimana alur koordinasi internal IPDE dalam melaksanakan peran dan tanggungjawabnya terkait dengan Aplikasi SIMRS?
	Jawaban:
	Tergantung kasusnya, apakah yang bermasalah adalah jaringan, software atau hardware-nya karena ada bagiannya sendiri-sendiri. Tapi selama ini setiap pagi kita di internal IPDE sendiri selalu mengadakan rapat rutin untuk membahas koordinasi tersebut.
	Pertanyaan:
	Bagaimana alur koordinasi eksternal IPDE dengan Bagian Perencanaan dan Wakil Direktur Umum terkait dengan Aplikasi SIMRS?
	Jawaban:
	IPDE sendiri tepat berada dibawah Kasi Monev, namun hal yang dibahas dengan Kasi Monev bukanlah hal yang berhubungan dengan IT. Kemudian kita (IPDE) berkoordinasi dengan Bagian Perencanaan dan jika dilihat dari struktur organisasi semua instalasi pada RSDM langsung dibawah Wadir, IPDE sendiri berada dibawah Wadir Umum. Tapi untuk permasalahan tertentu biasanya langsung ke Direktur.
Informasi Kondisi Keamanan Terkini Berdasarkan Metode OCTAVE	
Obyektif 1: Menggali aset kritis TI terkait Aplikasi SIMRS	

		Pertanyaan:
		Dimana saja data penting pada Aplikasi SIMRS tersebut disimpan?
		Jawaban:
		Untuk Aplikasi SIMRS berada di satu server, namun jika data-data seperti BPJS atau Website berbeda,mereka memiliki servernya masing-masing.
	7.	**Pertanyaan:**
		Apa saja *hardware* yang dapat digunakan untuk mengoperasikan Aplikasi SIMRS?
		Jawaban:
		Untuk Aplkasi SIMRS sendiri hanya PC. Namun untuk aplikasi lain seperti pemantauan kerja dapat dijalankan melalui Android.
		Pertanyaan:
		Diamana saja *hardware* tersebut berada?
		Jawaban:
		Semua unit dan bangsal. Bisa di kasir atau poli.
		Pertanyaan:
		Siapa saja yang boleh menggunakan *hardware* tersebut?
		Jawaban:
		Komputer tersebut disediakan untuk operator supaya bisa mengentrikan data. Operatornya ini dapat berupa dokter spesialis untuk entri di rekam medis, bisa juga bagian kasir untuk entri di billing.
	10.	**Pertanyaan:**
		Bagaimana cara memastikan bahwa orang tersebut memang orang yang berhak memasuki lokasi TI dan mengakses *hardware* atau server?
		Jawaban:
		Selama ini akses masuk ruang server sudah ada SPO-nya, sudah terdapat penjelasan mengenai siapa saja yang boleh masuk. Kunci ruang server sendiri bukan kunci biasa tetapi menggunakan *barcode scanner* pada ID sehingga hanya orang-orang tertentu yan dapat membuaknya. Untuk PC sendiri saat ini PC berada diruang terbuka sehingga belum ada kontrol untuk akses masuknya. Selama ini satu PC dapat digunakan untuk beberapa operator untuk

		kasus PC yang berada di poli, sehingga tidak semua PC untuk satu orang seperti yang ada dikantor.
	11.	**Pertanyaan:**
		Siapa saja yang bertanggungjawab memastikan bahwa lokasi dan perangkat *hardware/*server hanya diakses oleh orang yang berhak?
		Jawaban:
		Untuk PC di level end-user adalah masing-masing operatornya. Jadi masing-masing operator ketika pertama kali masuk sudah dibekali pelatihan bahwa ini komputer untuk operator tersebut dan sudah dijelaskan peraturan-peraturan mengenai pemeliharaan dan keamanan serta dampaknya.
	12.	**Pertanyaan:**
		Menurut anda, apa saja *software* yang berkaitan dengan Aplikasi SIMRS?
		Jawaban:
		Antivirus, OS, terdapat Website namun berbeda dengan aplikasi.
	13.	**Pertanyaan:**
		Apa saja perangkat jaringan yang berkaitan untuk akses Aplikasi SIMRS?
		Jawaban:
		Untuk jaringan wide selama ini terdapat provider dan bandwith yang dirasa penting, untuk bandwith Rumah Sakit ini memiliki kapasitas 20 Mb. Untuk jaringan lokal yang utama adalah server, switch, microtic, ethernet, UPS, Kabel LAN, fiber optic untuk backbone server. Untuk UPS sendiri sudah memiliki protocol agar kematian jaringan tidak boleh lebih dari 30 menit. Selain itu juga terdapat wifi untuk residen agar dapat mengakses jurnal.
	Obyektif 2: Menggali ancaman dan kebutuhan keamanan aset kritis	
	14.	**Pertanyaan:**
		Apa saja ancaman yang mungkin atau pernah terjadi pada masing-masing aset diatas?
		Jawaban:
		Tikus sering merusak kabel jaringan. Switch yang dicolokan sembarangan khususnya oleh residen.

		Pengamanan *password* kurang ketat dan yang sering terjadi adalah menggunakan satu akun untuk login beberapa orang sehingga tidak sesuai dengan hak akes dan jika terjadi masalah maka yang disalahkan adalah pemilik akunnya padahal yang melakukan kesalahan bukan orang tersebut. Selain itu sudah terdapat pelatihan untuk user tentang pemeliharaan dan menjaga keamanan loginnya sendiri namun dari IPDE sendiri belum ada evaluasi setelah melakukan pelatihan tersebut.
	15.	**Pertanyaan:**
		Apakah dampak dari masing-masing ancaman (yang telah disebutkan sebelumnya) terhadap keberlangsungan Aplikasi SIMRS?
		Jawaban:
		Hanya menganggu. Namun selama ini yang crusial adalah listrik, namun selama ini sudah terdapat protocol bahwa down tidak boleh lebih dari 1 jam.
	16.	**Pertanyaan:**
		Kebutuhan keamanan seperti apa yang dibutuhkan berdasarkan masing-masing ancaman yang telah disebutkan sebelumnya?
		Jawaban:
		Saat ini untuk listrik sudah tersedia UPS sebagai sumber listrik cadangan. Saat ini sedang mengusahakan jalur switch tanpa listrik sehingga jika listrik mati masih akan menyimpan baterai. Operator seharusnya dikontrol rutin dan untuk aplikasi dapat diakses 24 jam. Aman dari kebakaran, banjir, log user yang mengahapus data, karena selama ini log hanya dapat mencatat siapa yang online dan kapan sehingga belum detail.
Obyektif 3: Menggali praktik keamanan terkini pada Aplikasi SIMRS		
	17.	**Pertanyaan:**
		Teknologi apa sajakah yang telah diterapkan untuk membatasi hak akses pada Aplikasi SIMRS?
		Jawaban:
		Interface sesuai dengan hak akses yang diberikan.
	18.	**Pertanyaan:**

		Apakah terdapat kebijakan mengenai kewajiban user untuk mengamankan *password* miliknya sendiri?
		Jawaban:
		Hanya secara verbal sudah dijelaskan penting dan dampaknya saat pelatihan, namun belum ada tindakan evaluasi dari kami.
	19.	**Pertanyaan:**
		Bagaimana cara memastikan kualitas keamanan *password* pada Aplikasi SIMRS saat ini?
		Jawaban:
		Belum ada
	20.	**Pertanyaan:**
		Bagaimana proses registrasi pada Aplikasi SIMRS saat ini? • Permintaan akses dari user • Verifikasi permintaan • Pemberian hak akses
		Jawaban:
		Tergantung siapa usernya, disini ada beberapa operator. Misalkan untuk dokter spesialis harus mengajukan surat ke Bagian Organisasi dan Kepegawaian serta lampiran surat lulus ujian praktik. Untuk residenberbeda lagi. Macamnya tergantung pihak yang bersangkutan. Untuk sistem verifikasi dan permberian hak akses biasanya saya yang memberi keputusan.
	21.	**Pertanyaan:**
		Bagaimana proses pengelolaan hak akses saat ini? • Pemantauan status identitas akses • Penghapusan dan pembatasan hak akses
		Jawaban:6
		Belum ada
Obyektif 4: Menggali kelemahan organisasi dan kerentanan teknologi		
	22.	**Pertanyaan:**
		Menurut anda apa saja kerentanan teknologi yang saat ini sudah diterapkan untuk menjaga keamanan Aplikasi SIMRS?
		Jawaban:
		Yang paling rentan adalah jaringan

23.	**Pertanyaan:**
	Menurut anda apa saja kelemahan organisasi dalam menjaga keamanan Aplikasi SIMRS?
	Jawaban:
	User masih sering membagi akses login, tidak merubah *password default* dan tidak ada pemantauan user akses.

Wawancara dengan Staff Pengolahan Data Elektronik

A. INFORMASI PELAKSANAAN INTERVIEW

Hari/ Tanggal	Kamis/ 27 April 2017
Pukul	09:00
Lokasi	Ruang Kerja IPDE

B. PROFIL NARASUMBER

Nama	Aris Andriyanto, S.Kom
Jabatan	Staff Pengolahan Data Elektronik/ Database Administrator
Lama Bekerja	7 Tahun

C. PERTANYAAN INTERVIEW PROTOCOL

NO	URAIAN
	Informasi Umum
1.	**Pertanyaan:**
	Apa peran dan tanggungjawab anda pada Aplikasi SIMRS?
	Jawaban:
	Memastikan semua aplikasi di Rumah Sakit berjalan dengan baik.
2.	**Pertanyaan:**
	Apa fungsi dari Aplikasi SIMRS?
	Jawaban:
	Membantu meringankan kerja dan keakuratan data.
	Informasi Kondisi Keamanan Terkini Berdasarkan Metode OCTAVE
	Obyektif 1: Menggali aset kritis TI terkait Aplikasi SIMRS
3.	**Pertanyaan:**
	Menurut anda apa saja aset kritis terkait Aplikasi SIMRS?
	Jawaban:

		Semua penting yang dari mulai hardware ada PC, CPU dan server. Jaringan ada switch dan komponen-komponen jaringan lainya.
	Obyektif 2: Menggali ancaman dan kebutuhan keamanan aset kritis	
	4.	**Pertanyaan:**
		Apa saja ancaman yang mungkin atau pernah terjadi pada masing-masing aset diatas?
		Jawaban:
		Kalau di jaringan pernah terjadi blocking/looping dan software penjumlahan dikasir pernah trouble jadi angka yang diinputkan dengan perhitungan tidak sesuai kemudian kabel jaringan putus akibat tikus dan overload sehingga kinerjanya melambat. Kalau software mungkin hanya masalah virus. Hardware misalnya rusak atau terbakar. Untuk data sendiri mungkin hanya masalah redudansi saja ya.
	5.	**Pertanyaan:**
		Kebutuhan keamanan seperti apa yang dibutuhkan pada Aplikasi SIMRS?
		Jawaban:
		Kalau selama transaksi pada aplikasi seperti menghapus atau menambah data itu belum bisa dilacak.
	Obyektif 3: Menggali praktik keamanan terkini pada Aplikasi SIMRS	
	6.	**Pertanyaan:**
		Teknologi apa sajakah yang telah diterapkan untuk membatasi hak akses pada Aplikasi SIMRS?
		Jawaban:
		Modul tiap pengguna dibatasi sesuai dengan kebutuhan berdasarkan surat dari Bagian Organisasi dan Kepegawaian.
	7.	**Pertanyaan:**
		Apakah terdapat kebijakan mengenai kewajiban user untuk mengamankan *password* miliknya sendiri?

		Jawaban:
		Belum ada, yang ada hanya kebijakan tentang username harus unik namun untuk keamanan login sendiri sudah ada pelatihan diawal bahwa satu akun untuk satu orang, harus mengganti password secara rutin, anjuran untuk segera logout aplikasi jika sudah selesai digunakan dan sebagainya, namun seringnya kenyataan dilapangan berbeda.
	8.	**Pertanyaan:**
		Bagaimana cara memastikan kualitas keamanan *password* pada Aplikasi SIMRS saat ini?
		Jawaban:
		Belum ada, hanya jika user bermasalah dengan akun atau passwordnya bisa laingsung telfon ke IPDE
	9.	**Pertanyaan:**
		Bagaimana proses registrasi pada Aplikasi SIMRS saat ini? • Permintaan akses dari user • Verifikasi permintaan • Pemberian hak akses
		Jawaban:
		Dapat dibedakan terdapat dua operator, yaitu operator biasa dan dokter spesialis. Operator meminta surat untuk hak akses dari unit yang bersangkutan ditujukan kepada kepala IPDE. Jika dokter spesialis maka butuh surat dari Bagian Organisasi dan Kepegawaian untuk memastikan bahwa memang benar pegawai RSDM dan lampiran surat yang menyatakan bahwa dokter spesialis tersebut sudah lulus ujian praktik serta boleh melakukan praktik dengan tandatangan direktur. Kemudian surat dari Bagian Organisasi dan Kepegawaian tersebut akan langsung ke IPDE. Namun jika bukan dokter spesialis hanya cukup surat dari Bagian Organisasi dan Kepegawaian dengan melengkapi jabatan dan keperluan pada Aplikasi SIMRS yang ingin

		diberikan hak akses. Kemudian ada hak akses untuk residen atau mahasiswa dokter spesialis, untuk mahasiswa tersebut langsung diawasi oleh KSM, sehingga hanya memerlukan surat dari KSM dan ditujukan ke Kepala IPDE. Dari IPDE sendiri, surat masuk akan diterima oleh bagian administrasi lalu diserahkan ke Kepala IPDE. Kemudian segala keputusan ada di Kepala IPDE. Setelah itu biasanya langsung ada tindaklanjuti untuk ditugaskan ke siapa, karena disini terdapat beberapa pegawai yang diberi login admin, sehingga bisa langsung menambah user dan hak akses baru. Yang bisa jadi admin selain saya ada beberapa programmer yang bisa, mbak Dina (troubleshooting dan implementasi) dan bagian jaringan juga bisa.
	10.	**Pertanyaan:**
		Bagaimana proses pengelolaan hak akses saat ini? • Pemantauan status identitas akses • Penghapusan dan pembatasan hak akses
		Jawaban:
		Untuk pemantauan sendiri belum ada caranya ya, kalau penghapusan dan pembatasan hak akses sesuai dengan surat Bagian Oranisasi dan Kepegawaian tadi. Namun yang terjadi Bagian Orpeg hanya menambah hak akses terus, sehingga jika ada akun yang dirasa sudah lama tidak aktif biasanya kita tanyakan ke Orpeg sendiri apakah akun ini masih aktif atau tidak karena jika masih dipertahankan padahal orangnya sudah pindah atau pensiun selain bahaya di keamanan juga memakan memori.
	Obyektif 4: Menggali kelemahan organisasi dan kerentanan teknologi	
	11.	**Pertanyaan:**
		Menurut anda apa saja kerentanan teknologi yang saat ini sudah diterapkan untuk menjaga keamanan Aplikasi SIMRS?
		Jawaban:

		Jaringan itu banyak sekali kerentanan karena yang paling sering terjadi trouble. Untuk data sendiri di server sudah ada ID untuk masuk keruangan menggunakan barcode. Sistem backup server sudah otomatis baik di internal ataupun eksternal setiap hari kira-kira jam setengah 3 pagi. Kemudian UPS saat ini kapasitanys hanya 3-4 jam saja kurang ya kalau menurut saya. UPS saat ini akan otomatis menyala sekirtar 3 atau 4 detik setelah listrik PLN mati. Kalau antivirus sudah terhubung oleh jaringan jadi sekali pindai langsung semua komputer dan nanti ada laporannya apa saja virus, malware dan lainya.
12.		**Pertanyaan:**
		Menurut anda apa saja kelemahan organisasi dalam menjaga keamanan Aplikasi SIMRS?
		Jawaban:
		Belum ada kebijakan untuk password dan yang paling sering adalah user masih sering berbagi *password.*

LAMPIRAN B – *RISK REGISTER*

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
Manusia	User, Supervisor ,Admin	R01	Manipulasi data	R01.1	Pencurian *username* dan *password* pada user	8	- Menimbulkan kerentanan terhadap akses tidak sah yang dapat merusak keamanan data khusunya faktor kerahasiaan dan keakuratan data. - Menurunnya tingkat kepercayaan pengguna	2	Terdapat kebijakan dan pelatihan untuk melindungi keamanan informasi, hanya dapat diakses di gedug RS dan petugas keamanan yang beroperasi selama 24 jam	6	96	Medium	IPDE
				R01.2	Exploitasi *session login*	8	- Menimbulkan kerentanan terhadap akses tidak sah yang dapat merusak keamanan data khusunya faktor kerahasiaan dan keakuratan data. - Menurunnya tingkat kepercayaan pengguna	3	Terdapat anjuran untuk me-logout akun yang sudah tidak di	6	144	High	IPDE
Hardware	Server	R02	Kerusakan pada server	R02.1	Gempa Bumi	10	- Kerusakan permanen pada fisik server sehingga server tidak dapat berfungsi.	2	Server berada pada ruangan khusus	7	140	High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
							- Terhentinya proses bisnis Aplikasi SIMRS - Menyebabkan kerentanan kehilangan data - Menyebabkan kerugian finansial						
				R02.2	Badai dan Petir	9	- Menimbulkan konsleting pada server akibat tersambar petir sehingga server dapat rusak. - Terhentinya proses bisnis Aplikasi SIMRS - Menyebabkan kerentanan kehilangan data - Menyebabkan kerugian finansial	2	Terdapat penangkal petir pada bangunan	2	36	Low	IPDE
				R02.3	Banjir	9	- Air dapat menyebabkan kerusakan dan konsleting pada server sehingga data yang tersimpan dapat hilang. - Terganggunya proses bisnis Aplikasi SIMRS - Menyebabkan kerusakan server - Menyebabkan kerugian finansial	4	Server berada pada ruangan khusus yang tinggi	6	216	Very High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
							- Menurunnya citra Rumah Sakit						
				R02.4	Kebakaran	8	- Dapat meyebabkan kerusakan permanen pada fisik server yang menyebabkan kerugian finansial dan kehilangan data. - Menyebabkan kerugian finansial - Menurunnya citra Rumah Sakit	2	- Terdapat Fire Extinguisher pada setiap ruangan di RS - Terdapat petunjuk keselamatan kerja dan penggunaan Fire Extinguisher pada setiap runangan di RS - Terdapat pelatihan keselamatan kerja pada semua pegawai RS	3	48	Low	IPDE
				R02.5	Kebocoran dan Kerusakan Bangunan	6	Menyebabkan kerugian finansial untuk perbaikan dan dapat menyebabkan terganggunya kinerja server	3	Server berada pada ruangan khusus	7	126	High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
							atau dampak paling parah adalah kerusakan permanen pada server sehingga server tidak dapat berfungsi.						
		R03	Server berhenti	R03.1	Kerusakan pada UPS	9	UPS merupakan satu-satunya sumber listrik cadangan apabila sumber listrik utama mengalami kerusakan, sehingga kerusakan UPS dapat menyebabkan terhentinya seluruh proses bisnis Aplikasi SIMS.	3	Telah dilakukan pemeliharaan dan pengecekan rutin oleh PIC UPS	5	135	High	PIC UPS pusat
				R03.2	Listrik Mati	10	- Menyebabkan terhentinya seluruh proses bisnis Rumah Sakit yang melibatkan Aplikasi SIMRS, sehingga dapat menimbulkan keluhan dan terhambatnya proses pelayanan pada RS. - Terhentinya proses bisnis Aplikasi SIMRS	5	Terdapat UPS otomatis	2	100	Medium	IPDE
		R05	Kinerja server melambat	R05.1	RAM mengalami kelebihan memori	5	Menyebabkan gangguan pada kinerja server sehingga berdampak pada penurunan kecepatan respon kinerja Aplikasi SIMRS .	4	Terdapat pemeliharaan dan pengecekan rutin pada komponen server	3	60	Low	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
				R05.2	Kinerja Procesor menurun akibat terlalu banyak kapasitas data	5	Menyebabkan gangguan pada kinerja server sehingga berdampak pada penurunan kecepatan respon kinerja Aplikasi SIMRS .	4	Terdapat pemeliharaan dan pengecekan rutin pada komponen server	3	60	Low	IPDE
				R05.3	Tempat penyimpanan (*Harddisk)* penuh	10	Menyebabkan fungsi server sebagai media penyimpanan data tidak dapat berungsi dengan baik dan dapat menimbulkan ancaman kehilangan data-data penting yang ada pada Aplikasi SIMRS.	3	Terdapat pemeliharaan dan pengecekan rutin pada komponen server	2	60	Low	IPDE
				R05.4	Server mengalami *overheat*	5	Menyebabkan penuruan kinerja pada server namun tidak signifikan, namun jika terus dibiarkan dapat memicu kebakaran dan kerusakan pada server	3	Rerdapat AC pada ruang server	2	30	Low	IPDE
		R06	Server Down	R06.1	Serangan *Denial of Service* (DoS), SQL-Injection, Sniffing	9	- Menyebabkan penurunan respon server untuk memproses data yang ada pada Aplikasi SIMRS, dalam kasus yang parah dapat menyebabkan kehilangan data yang belum ter-back up	2	Adanya Monitoring lalulintas jaringan selama jam kerja	5	90	Medium	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
							- Terhambatnya proses bisnis Aplikasi SIMRS - Menurunnya tingkat kepercayaan pengguna						
				R06.2	Overload Request	7	- Terganggunya kinerja server dalam memproses data sehingga menimbulkan kelambatan pada proses pelayanan pasien yang memerlukan Apliaksi SIMRS. - Menurunnya tingkat kepuasan pengguna	4	Adanya Monitoring lalulintas jaringan selama jam kerja	5	140	High	IPDE
		R07	Akses tidak sah ke ruang server	R07.1	Pihak luar yang masuk ke ruang server secara ilegal	9	Menimbulkan kerentanan terhadap akses data tidak sah yang dapat merusak keamanan data, modifikasi pada pengaturan server, dan dapat menimbulkan kerusakan atau pencurian server.	3	Terdapat prosedur akses ruang server.	3	81	Medium	IPDE
				R07.2	Kurangnya evaluasi hak akses pada peralatan dan lokasi fasilitas pengolahan data elektronik.	9	Menimbulkan kerentanan terhadap akses data tidak sah yang dapat merusak keamanan data, modifikasi pada pengaturan server, dan dapat menimbulkan kerusakan atau pencurian	4	Terdapat penguncian ruang server dengan teknologi card reader.	3	108	High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
							server.						
				R07.3	Kelalaian petugas yang meninggalkan ruang server dalam keadaan tidak terkunci	8	Menimbulkan kerentanan terhadap akses data tidak sah yang dapat merusak keamanan data, modifikasi pada pengaturan server, dan dapat menimbulkan kerusakan atau pencurian server.	5	Terdapat pembatasan hak akses pada pemilik kunci ruang server	4	160	High	IPDE
	PC	R08	Kerusakan PC	R08.1	Gempa Bumi	5	- Dapat menyebabkan kerusakan permanen pada PC sehingga selain dapat menyebabkan kerugian finansial. - Terganggunya proses bisnis Aplikasi SIMRS	2	Terdapat perlindungan pada PC dan bangunan	7	70	Low	IPDE
				R08.2	Badai dan Petir	6	Petir dapat membuat keruskan pada PC berupa konsleting ataupun kebakaran. Sehingga menimbulkan kerugian finansial untuk proses perbaikan.	2	Terdapat penangkal petir pada bangunan	4	48	Low	IPDE
				R08.3	Banjir	6	- Menyebabkan kerugian finansial - Terganggunya proses bisnis Aplikasi SIMRS	2	Lantai lokasi bangunan tinggi	8	96	Medium	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
				R08.4	Kebakaran	10	- Menyebabkan kerugian finansial untuk biaya perbaikan atau pergantian - Menganggu proses pelayanan - Penurunan citra Rumah Sakit	2	- Terdapat Fire Extinguisher pada setiap ruangan di RS - Terdapat petunjuk keselamatan kerja dan penggunaan Fire Extinguisher pada setiap runangan di RS - Terdapat pelatihan keselamatan kerja pada semua pegawai RS	3	60	Low	IPDE
				R08.5	Kebocoran dan Kerusakan Bangunan	6	Menyebabkan kerugian finansial untuk biaya perbaikan atau pergantian	3	Terdapat perlindungan pada bangunan	4	72	Low	IPDE
				R08.6	Monitor, Keyboard ataupun mouse mengalami kerusakan karena	4	- Menyebabkan kerugian finansial - Penurunan kinerja proses bisnis dan pelayanan	3	Adanya pemeliharaan dan pengecekan rutin pada	5	60	Low	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
					pemakaian berlebih				perangkat jaringan				
				R08.7	Kesalahan konfigurasi	4	- Menyebabkan penurunan kinerja - Menurunkan tingkat kepuasan dan kepercayaan pengguna	5	Terdapat pegawai bagian *hardware* dan *troubleshooting* yang ahli	3	60	Low	IPDE
		R09	PC tidak dapat menyala	R09.1	Kerusakan pada UPS	8	Gangguan pada kinerja pelayanan sehingga proses bisnis terhambat	3	Telah dilakukan pemeliharaan dan pengecekan rutin oleh PIC UPS	4	96	Medium	IPDE
				R09.2	Listrik Mati	7	Gangguan pada kinerja pelayanan sehingga proses bisnis terhambat	3	Terdapat UPS otomatis	3	63	Low	PIC UPS pusat
		R10	Kinerja PC melambat	R10.1	CPU mengalami overheat	2 2	Gangguan pada kinerja pelayanan sehingga proses bisnis terhambat	3	Terdapat AC pada ruang kerja	4	24	Low	IPDE
				R10.2	RAM mengalami kelebihan memori	4	Penurunan kinerja proses pelayanan akibat waktu respon lambat	3	Terdapat pemeliharaan dan pengecekan rutin pada komponen PC	5	60	Low	IPDE
				R10.3	Kinerja Procesor menurun akibat terlalu banyak kapasitas data	3	Penurunan kinerja proses pelayanan akibat waktu respon lambat	3	Terdapat pemeliharaan dan pengecekan rutin pada	5	45	Low	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
									komponen PC				
		R11	PC tidak dapat terhubung dengan jaringan	R11.1	Port ethernet pada PC rusak	4	- Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja - Menimbulkan ketidakpuasan oleh user dan pasien	3	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	6	72	Low	IPDE
		R12	Akses tidak sah ke PC	R12.1	Kelalaian petugas yang meninggalkan ruangan/lokasi PC dalam keadaan tidak terkunci	6	Rentan terhadap kehilangan dan penyalahgunaan data	3	Terdapat kamera CCTV yang dipantau 24 jam.	5	90	Medium	Satuan Keamanan pusat
				R12.2	Kelalaian pengguna yang meninggalkan PC dalam keadaan menyala/ tidak terkunci.	7	Rentan terhadap kehilangan dan penyalahgunaan data	5	Terdapat kamera CCTV yang dipantau 24 jam.	4	140	High	User
		R13	Komponen PC hilang	R12.3	Pencurian pada komponen PC	4	Kerugian finansial	2	Adanya Camera CCTV yang bekerja 24 jam	3	24	Low	Satuan Keamanan pusat
Software	Aplikasi SIMRS	R14	Aplikasi tidak dapat diakses	R14.1	Terdapat *bug* pada aplikasi	7	- Gangguan pada kinerja pelayanan sehingga proses bisnis terhambat - Menimbulkan ketidapuasan pengguna	4	Terdapat pegawai bagian pengembangan *software* yang handal	4	112	Medium	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
							- Menurunkan tingkat kepercayaan pengguna						
				R14.2	Gangguan pada jaringan	7	- Terhentinya proses bisnis pada Aplikasi SIMRS - Menimbulkan ketidapuasan pengguna - Menurunkan tingkat kepercayaan pengguna	5	Adanya Monitoring lalulintas jaringan selama jam kerja	4	140	High	IPDE
				R14.3	Listrik mati	7	- Terhentinya proses bisnis pada Aplikasi SIMRS - Menimbulkan ketidapuasan pengguna - Menurunkan tingkat kepercayaan pengguna Penurunan citra Rumah Sakit	4	Terdapat UPS otomatis	3	84	Medium	IPDE
				R14.4	Server down	7	- Terhentinya proses bisnis pada Aplikasi SIMRS - Menimbulkan ketidapuasan pengguna - Menurunkan tingkat kepercayaan pengguna Penurunan citra Rumah Sakit	4	Adanya Monitoring lalulintas jaringan selama jam kerja	3	84	Medium	IPDE
		R15	Aplikasi diakses oleh pihak tidak	R15.1	Exploitasi akun pegawai yang sudah pindah atau	8	- Menimbulkan kerentanan terhadap akses tidak sah sehingga mengancam	4	Terdapat pendataan terhadap status	7	224	Very High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
			berwenang		pensiun		ketersediaan, kerahasiaan dan keakuratan data - Menyebabkan penurunan tingkat kepercayaan pengguna		keaktifan kerja pegawai				
				R15.2	*Sharing password* pada user	8	- Menimbulkan kerentanan terhadap akses tidak sah sehingga mengancam ketersediaan, kerahasiaan dan keakuratan data - Menyebabkan penurunan tingkat kepercayaan pengguna	6	Terdapat kebijakan dan pelatihan mengenai keamanan informasi	7	336	Very High	User
				R15.3	Kesalahan pemberian hak akses pada user	8	- Menimbulkan kerentanan terhadap akses tidak sah sehingga mengancam ketersediaan, kerahasiaan dan keakuratan data - Menyebabkan penurunan tingkat kepercayaan pengguna - Menimbulkan komplain ekstrim	4	Terdapat prosedur pengajuan surat untuk hak akses	5	160	High	IPDE
				R15.4	Kurangnya evaluasi dan monitoring pada hak akses	8	- Menimbulkan kerentanan terhadap akses tidak sah sehingga mengancam ketersediaan, kerahasiaan dan keakuratan data	7	Terdapat pendataan terhadap status keaktifan kerja pegawai	7	343	Very High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
							- Menyebabkan penurunan tingkat kepercayaan pengguna - Menimbulkan komplain ekstrim						
		R16	User tidak dapat login	R16.1	User lupa *password*	3	Menghambat proses pelayanan	5	Terdapat bagian *troubleshooting* yang ahli	5	75	Low	User
				R16.2	Kesalahan dalam pemberian hak akses	4	Menghambat proses pelayanan	3	Terdapat prosedur pemberian hak akses	5	60	Low	IPDE
	OS	R17	Terserang virus	R17.1	Antivirus tidak update	8	Menimbulkan kerentanan terjangkit virus yang dapat menyebabkan kehilangan data dan kerusakan pada sistem	2	Adanya antivirus dan diupdate secara berkala	3	48	Low	IPDE
				R17.2	Terdapat bug pada antivirus sehingga tidak dapat berjalan	7	Menimbulkan kerentanan terjangkit virus yang dapat menyebabkan kehilangan data dan kerusakan pada sistem	2	Adanya antivirus dan diupdate secara berkala	3	42	Low	IPDE
				R17.3	Kesalahan konfigurasi pada antivirus/firewall	7	Menimbulkan kerentanan terjangkit virus yang dapat menyebabkan kehilangan data dan kerusakan pada sistem	2	Adanya update patch dan firewall secara berkala	3	42	Low	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
		R18	Terserang *worm* atau *Trojan Horse*	R18.1	Terdapat file yang terjangkit *worm* atau *Trojan Horse* lewat usb	6	- Menimbulkan kerentanan kehilangan data - Menimbulkan kerentanan kerusakan sistem dan jaringan - Menganggu proses bisnis Aplikasi SIMRS	5	Adanya update patch dan firewall secara berkala	4	120	High	IPDE
				R18.2	Membuka atau mendownload file yang terjangkit *worm* atau *Trojan Horse*	6	- Menimbulkan kerentanan kehilangan data - Menimbulkan kerentanan kerusakan sistem dan jaringan - Menganggu proses bisnis Aplikasi SIMRS	6	Adanya update patch dan firewall secara berkala	4	144	High	IPDE
Jaringan	Microtic	R19	Kerusakan pada microtic	R19.1	Kerusakan *routerboard*	8	- Kerugian finansial akbiat biaya perbaikan - Jaringan mati sehingga proses bisnis Aplikasi SIMRS tidak dapat berjalan - Menyebabkan keluhan pelanggan akibat terganggunya proses pelayanan	2	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	4	64	Low	IPDE
				R19.2	Kesalahan konfigurasi	7	- Menimbulkan gangguan pada akses jaringan sehingga menganggu	2	- Adanya pemeliharaan dan	4	56	Low	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
							kinerja Aplikasi SIMRS - Menyebabkan keluhan pelanggan akibat terganggunya proses pelayanan		pengecekan rutin pada perangkat jaringan - Memiliki tenaga ahli jaringan yang mengerti bidangnya dengan baik				
				R19.3	Terjadi *routing loop*	7	- Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja Aplikasi SIMRS - Menyebabkan keluhan pelanggan akibat terganggunya proses pelayanan	5	- Adanya monitoring lalulintas jaringan selama jam kerja - Memiliki tenaga ahli jaringan yang mengerti bidangnya dengan baik	5	170	High	IPDE
				R19.4	Gempa Bumi	10	- Kerugian finansial akbiat biaya perbaikan atau membeli baru - Menyebabkan mati jaringan pada seluruh area	2	Terdapat perlindungan pada bangunan	5	100	Medium	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
							RS sehingga proses bisnis Aplikasi SIMRS terhenti						
				R19.5	Badai dan Petir	10	- Menyebabkan mati jaringan pada seluruh area RS sehingga proses bisnis Aplikasi SIMRS terhenti - Kerugian finansial akbiat biaya perbaikan atau membeli baru	2	- Terdapat perlindungan bangunan untuk menghindari badai - Terdapat penangkal petir	3	60	Low	IPDE
				R19.6	Banjir	10	- Kerugian finansial akbiat biaya perbaikan atau membeli baru - Menyebabkan mati jaringan pada seluruh area RS sehingga proses bisnis Aplikasi SIMRS terhenti	3	Menaikan lantai bangunan di tempat penyimpanan PC microtic	5	150	High	IPDE
				R19.7	Kebakaran	10	- Kerugian finansial akbiat biaya perbaikan atau membeli baru - Menyebabkan mati jaringan pada seluruh area RS sehingga proses bisnis Aplikasi SIMRS terhenti - Menurunnya citra Rumah Sakit	3	- Terdapat Fire Extinguisher pada setiap ruangan di RS - Terdapat petunjuk keselamatan kerja dan	3	90	Medium	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
									penggunaan Fire Extinguisher pada setiap runangan di RS - Terdapat pelatihan keselamatan kerja pada semua pegawai RS				
	Switch	R20	Kerusakan pada switch	R20.1	Gempa Bumi	9	- Kerugian finansial akibat keperluan biaya untuk perbaikan atau membeli baru - Terganggunya proses bisnis Aplikasi SIMRS akibat terhentinya jaringan pada sebagian lokasi RS	2	Terdapat perlindungan pada bangunan	4	72	Low	IPDE
				R20.2	Badai dan Petir	9	- Kerugian finansial akibat keperluan biaya untuk perbaikan atau membeli baru - Terganggunya proses bisnis Aplikasi SIMRS akibat terhentinya jaringan	2	Terdapat penangkal petir pada bangunan	3	54	Low	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
							pada sebagian lokasi RS						
				R20.3	Banjir	9	- Kerugian finansial akibat keperluan biaya untuk perbaikan atau membeli baru - Terganggunya proses bisnis Aplikasi SIMRS akibat terhentinya jaringan pada sebagian lokasi RS - Menurunnya citra RS	2	Switch digantung pada lokasi tinggi yang sulit dijangkau manusia	4	72	Low	IPDE
				R20.4	Kebakaran	9	- Kerugian finansial akibat keperluan biaya untuk perbaikan atau membeli baru - Terganggunya proses bisnis Aplikasi SIMRS akibat terhentinya jaringan pada sebagian lokasi RS - Menurunnya citra RS	3	- Terdapat Fire Extinguisher pada setiap ruangan di RS - Terdapat petunjuk keselamatan kerja dan penggunaan Fire Extinguisher pada setiap runangan di RS - Terdapat pelatihan keselamatan	3	81	Medium	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
									kerja pada semua pegawai RS				
		R21	Penurunan kinerja pada switch	R21.1	*Overheat* pada switch	4	- Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja Aplikasi SIMRS - Menimbulkan keluhan pada pelanggan akbibat melambatnya pelayanan - Lama-kelamaan dapat menyebabkan kerusakan pada switch atau memicu kebakaran	3	Terdapat AC pada setiap ruangan	4	48	Low	IPDE
				R21.2	Kerusakan pada konektor ethernet	3	- Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja Aplikasi SIMRS - Menimbulkan keluhan pada pelanggan akbibat melambatnya pelayanan	3	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	3	27	Low	IPDE
				R21.3	Port switch rusak	3	Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja Aplikasi SIMRS	3	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	3	27	Low	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
				R21.4	Terjadi kesalahan konfigurasi	2	Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja Aplikasi SIMRS	3	Terdapat pegawai bagian *hardware* dan *troubleshooting* yang ahli	3	18	Very Low	IPDE
		R22	Kehilangan switch	R22.1	Pencurian switch	4	- Menimbulkan kerugian finansial - Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja Aplikasi SIMRS	2	- Adanya Camera CCTV yang bekerja 24 jam - Adanya satuan petugas keamanan yang bekerja 24 jam - Adanya penguncian ruangan yang ditinggalkan tanpa pengawasan - Switch digantung di tempat tinggi yang sulit dijangkau manusia	3	24	Low	Satuan keamanan pusat

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
	Kabel UTP, Fiber Optic	R23	Kerusakan pada kabel	R23.1	Digigit hewan pengerat	2	- Kerugian finansial akibat perbaikan - Menimbulkan gangguan pada jaringan	4	Terdapat pelapis atau pelindung pada kabel	4	32	Low	IPDE
				R23.2	Lapisan pelindung kabel mengelupas/ lepas	1	Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja	3	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	4	12	Very Low	IPDE
				R23.3	Kabel berkarat/usang	1	Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja	3	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	3	9	Very Low	IPDE
				R23.4	Kurangnya kontrol pengamanan kabel	2	Menimbulkan gangguan pada akses jaringan sehingga menganggu kinerja	3	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	3	18	Very Low	IPDE
		R24	Modifikasi ilegal pada konfigurasi kabel	R24.1	Kabel UTP dipindah demi kepentingan pribadi	5	- Menimbulkan kerentanan akses tidak sah ke sistem - Menimbulkan kerentanan kehilangan dan kerusakan pada kabel	5	Adanya pemeliharaan dan pengecekan rutin pada perangkat	7	175	High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
									jaringan				
				R24.2	Kabel UTP dicabut secara ilegal	5	- Menimbulkan kerentanan akses tidak sah ke sistem - Menimbulkan kerentanan kehilangan dan kerusakan pada kabel	5	Adanya pemeliharaan dan pengecekan rutin pada perangkat jaringan	7	175	High	IPDE
		R25	Kabel hilang	R25.1	Pencurian pada kabel	4	- Kerugian finansial - Menyebabkan gangguan pada sebagian kecil jaringan	1	Adanya Camera CCTV yang bekerja 24 jam	4	16	Very Low	Satuan Keamanan Pusat
				R25.2	Kelalaian pegawai	3	- Kerugian finansial - Menyebabkan gangguan pada sebagian kecil jaringan	1	Adanya Camera CCTV yang bekerja 24 jam	4	12	Very Low	IPDE
Data	Data keuangan, Data Rekam Medis, Data Inventoy	R26	Kegagalan backup data	R26.1	Kapasitas media penyimpanan overload	9	- Rentan terhadap kehilangan data - Mengganggu proses bisnis Aplikasi SIMRS - Penurunan citra Rumah Sakit - Menimbulkan keluhan ekstrim	4	Terdapat pemeliharaan dan pengecekan rutin pada komponen server	4	144	High	IPDE
				R26.2	Terdapat gangguan jaringan pada sistem back up data otomatis	9	- Rentan terhadap kehilangan data - Mengganggu proses bisnis Aplikasi SIMRS	5	Adanya Monitoring lalulintas jaringan selama	5	225	Very High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
							- Penurunan citra Rumah Sakit Menimbulkan keluhan ekstrim		jam kerja				
		R27	Pencurian data	R27.1	Terjadi Packet Sniffing pada jaringan untuk mencuri data	9	- Dapat merusak kerahasiaan, keakuratan dan ketersediaan data - Penurunan citra Rumah Sakit	3	Adanya Monitoring lalulintas jaringan selama jam kerja	4	108	High	IPDE
				R27.2	Terjadi social engineering pada user maupun admin	7	- Dapat merusak kerahasiaan, keakuratan dan ketersediaan data - Penurunan citra rumah sakit - Dapat menyebabkan akses tidak sah pada sistem untuk pengerusakan	4	Telah dilakukan pelatihan mengenai kewaspadaan keamanan informasi	4	112	Medium	IPDE
				R27.3	Loyalitas pegawai menururn	7	- Dapat merusak kerahasiaan, keakuratan dan ketersediaan data - Penurunan citra Rumah Sakit	3	Terdapat kebijakan mengenai keamanan informasi data elektronik	4	84	Medium	IPDE
		R28	Data tidak valid	R28.1	Kesalahan input oleh user	7	- Merusak keakuratan data - Dapat menyebabkan komplain eksrim	5	Terdapat prosedur entri data pada sistem	4	140	High	Organisasi

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	SEV	Potensi Dampak Kegagalan	OCC	Proses Kontrol Saat Ini	DET	RPN	Level	Pemilik Risiko
									infromasi				
				R28.2	Kesalahan perhitungan pada sistem maupun user	7	- Merusak keakuratan data - Dapat menyebabkan komplain eksrim	3	Terdapat pegawai bagian pengembangan *software* yang handal	3	63	Low	IPDE
		R29	Kehilangan data	R29.1	Virus	6	- Menurunnya kepercayaan pelanggan - Penurunan citra rumah sakit - Terhambatnya proses bisnis Aplikasi SIMRS	5	Terdapat antivirus yang terhubung dengan jaringan	4	120	High	IPDE
				R29.2	Kelalaian user	6	- Merusak keakuratan data - Dapat menyebabkan komplain ekstrim - Menurunnya tingkat kepercayaan pelanggan	4	Terdapat back up data secara otomatis	4	96	Medium	Organisasi
				R29.3	Sistem back up gagal	9	- Menurunnya kepercayaan pelanggan - Penurunan citra rumah sakit - Terhambatnya proses bisnis Aplikasi SIMRS - Dapat menyebabkan komplain ekstrim	4	Terdapat sistem backup otomatis setiap hari dan juga sistem backup secara manual yang dilakukan oleh petugas	4	144	High	IPDE

Kategori Aset	Aset Kritis	ID *Risk*	Potensi Mode Kegagalan	ID Penye-bab	Potensi Penyebab Kegagalan	S E V	Potensi Dampak Kegagalan	O C C	Proses Kontrol Saat Ini	D E T	RPN	Level	Pemilik Risiko
				R29.4	Rusaknya media penyimpanan	9	- Menurunnya kepercayaan pelanggan - Penurunan citra rumah sakit - Terhambatnya proses bisnis Aplikasi SIMRS - Dapat menyebabkan komplain ekstrim	4	Terdapat pemeliharaan dan pengecekan rutin pada komponen server	4	144	High	IPDE

LAMPIRAN C – REKOMENDASI MITIGASI RISIKO

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
Risiko Kontrol Akses *Logical*						
R16	Aplikasi diakses oleh pihak tidak berwenang	Exploitasi akun pegawai yang sudah pindah atau pensiun	***9.2.6 Removal or adjustment of access rights*** Kotrol untuk memastikan bahwa hak akses seluruh karyawan dan pengguna pihak	• Segera menghapus atau menangguhkan hak akses terhadap fasilitas (fisik) dan layanan (logis) sistem informasi kepada pengguna yang telah diberhentikan. • Memiliki dokumentasi/ catatan terhadap penghapusan hak akses ke informasi	• Terdapat pendataan mengenai keaktifan/ status kepegawaian oleh Bagian Organisasi dan Kepegawaian	• IPDE membuat prosedur formal untuk penagguhan atau penghapusan hak akses terhadap karyawan yang telah diberhentikan pada Aplikasi SIMRS. • IPDE membuat prosedur formal

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			eksternal pada akses informasi dan akses fasilitas pengolahan informasi telah dihapus setelah pemutusan hubungan kerja, kontrak atau perjanjian mereka, atau disesuaikan dengan	aset maupun fasilitas pemrosesan sistem informasi.		untuk penghapusan hak akses ke fasilitas pengolahan informasi kepada pegawai yang telah diberhentikan. • IPDE membuat dokumentasi/ catatan terhadap penghapusan hak akses ke informasi aset maupun fasilitas pemrosesan

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			perubahan.			sistem informasi • Membuat kebijakan mengenai hak akses Aplikasi SIMRS maupun hak akses ke fasilitas fisik pengolahan informasi untuk segera menghapus hak akses pegawai yang telah berhenti.
		Kesalahan pemberian	***9.1.1 Access control***	• Terdapat aturan	• Terdapat	• IPDE membuat

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
		hak akses pada user Aplikasi SIMRS	***policy*** Kontrol untuk memastikan bahwa kebijakan kontrol akses telah dibentuk, didokumentasikan dan ditinjau berdasarkan kebutuhan keamanan bisnis dan informasi	kontrol akses yang sesuai, hak akses dan batasan peran pengguna pada setiap aset organisasi sesuai dengan kepentingan risiko yang dimiliki. • Terdapat kontrol akses yang bersifat logis dan fisik pada aset. • Memiliki kebijakan mengenai persyaratan keamanan aplikasi bisnis. • Memiliki kebijakan untuk penyebaran	pemberian hak akses kepada pengguna sesuai dengan peran dan kebutuhan bisnisnya. • Memiliki kebijakan mengenai persyaratan keamanan aplikasi bisnis. • Memiliki persyaratan permintaan akses formal untuk otorisasi. • Terdapat	SOP untuk kontrol akses logis pada Aplikasi SIMRS • IPDE membuat SOP untuk kontrol akses fisik pada fasilitas pengolahan informasi dan media penyimpanan informasi elektronik. • Membuat kebijakan mengenai

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				informasi dan otorisasi, seperti prinsip kebutuhan untuk mengetahui tingkat keamanan informasi dan klasifikasinya. • Memiliki konsistensi antara kebijakan hak akses dengan klasifikasi informasi sistem dan jaringan. • Terdapat pembatasan peran kontrol akses, seperti permintaan akses, otorisasi akses, administrasi akses. • Memiliki	prosedur untuk permintaan hak akses, penghapusan dan perubahan hak akses pada Aplikasi SIMRS.	persyaratan keamanan informasi • Membuat kebijakan untuk penyebaran informasi dan otorisasi, seperti prinsip kebutuhan untuk mengetahui tingkat keamanan informasi dan klasifikasinya. • IPDE membuat aturan/

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				persyaratan permintaan akses formal untuk otorisasi. • Memiliki persyaratan *review* hak akses secara berkala. • Memiliki persyaratan penghapusan hak akses. • Memiliki perngarsipan catatan semua kejadian penting mengenai penggunaan dan pengelolaan identitas dan informasi otentikasi rahasia.		persyaratan pembatasan peran kontrol akses, seperti permintaan akses, otorisasi akses, administrasi akses. • IPDE membuat aturan/ persyaratan *review* hak akses secara berkala. • IPDE membuat prosedur formal untuk manajemen akses

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				• Memiliki prosedur formal untuk manajemen akses pengguna, tanggung jawab pengguna dan kontrol akses sistem dan aplikasi.		pengguna, tanggung jawab pengguna dan kontrol akses sistem dan aplikasi. • IPDE membuat perngarsipan catatan semua kejadian penting mengenai penggunaan dan pengelolaan identitas dan informasi otentikasi rahasia.
			9.2.1 User registration	• Terdapat ID yang	• Setiap pengguna	• Membuat

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			and de-registration Kontrol untuk memastikan bahwa proses registrasi dan de-registrasi pengguna formal telah diimplementasikan untuk memberikan hak akses yang tepat.	unik untuk setiap pengguna, agar tindakan setiap penguna mudah dimonitoring. • Penggunaan sebuah ID secara bersama *(sharing ID)* hanya boleh diijinkan di tempat yang diperlukan untuk bisnis atau operasional dengan alasan yang telah disetujui dan didokumentasikan. • Segera menonaktifkan atau menghapus ID	Aplikasi SIMRS memiliki ID unik yang berbeda dengan ID pengguna lain. • Terdapat kebijakan dan peringatan untuk tidak melakukan *sharing akun* pada Aplikasi SIMRS. • Terdapat prosedur formal untuk pengguna meminta hak akses ke Aplikasi SIMRS.	kebijakan mengenai hak akses Aplikasi SIMRS untuk menyediakan ID yang unik untuk setiap pengguna agar mudah dimonitoring. • Membuat kebijakan ketentuan pengguna untuk Aplikasi SIMRS agar penggunaan sebuah ID secara bersama *(sharing ID)* hanya boleh diijinkan di

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				pengguna dari pengguna yang telah meninggalkan organisasi. • Secara berkala mengidentifikasi dan menghapus atau menonaktifkan ID pengguna yang berlebihan atau tidak perlu. • Memastikan tidak ada redudansi ID antar pengguna. • Terdapat prosedur menetapkan atau mencabut ID pengguna. • Terdapat prosedur	• Sistem akan secara otomatis memperingatkan jika suatu ID baru yang akan dibuat memiliki kesamaan dengan ID lain yang sudah ada.	tempat yang diperlukan untuk bisnis atau operasional dengan alasan yang telah disetujui dan didokumentasikan. • Membuat kebijakan untuk memastikan bahwa tidak ada redudansi ID antar pengguna. • IPDE membuat prosedur formal untuk menetapkan atau

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				untuk menyediakan atau mencabut hak akses ke user ID.		mencabut ID pengguna. • IPDE membuat prosedur formal untuk menyediakan, merubah maupun menghapus hak akses suatu ID ke Aplikasi SIMRS. • IPDE membuat prosedur formal untuk secara berkala mengidentifikasi dan menghapus atau menonaktifkan

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
						ID pengguna yang berlebihan atau tidak perlu.
			9.2.2 User access provisioning Kontrol untuk memastikan bahwa proses penyediaan hak akses resmi pengguna telah diimplementasikan untuk	• Terdapat proses otorisasi resmi dari pemilik sistem informasi/ layanan kepada pengguna ataupun persetujuan terpisah dari pihak manajemen terkait hak akses. • Terdapat proses verifikasi bahwa tingkat akses yang diberikan sesuai dengan kebijakan akses dan konsisten	• Terdapat prosedur / alur formal untuk pengguna meminta hak akses pada Aplikasi SIMRS. • Terdapat pemberian hak akses sesuai dengan kebutuhan bisnis pegawai. • Terdapat proses verifikasi tingkat	• IPDE meninjau hak akses pada Aplikasi SIMRS secara berkala**.** • IPDE memasukan ketentuan hak akses dan sanksi pelanggarannya pada pada kontrak kerja pengguna. • IPDE membuat prosedur untuk memblokir hak

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			mencabut dan menetapkan hak akses pada seluruh jenis pengguna di semua sistem dan layanan.	dengan persyaratan lain seperti pemisahan tugas. • Terdapat kontrol untuk memastikan bahwa hak akses tidak diaktifkan oleh penyedia layanan sebelum prosedur otorisasi selesai. • Memiliki catatan mengenai hak akses yang diberikan kepada user ID untuk mengakses sistem informasi. • Segera mengadaptasi hak akses pengguna	akses pengguna oleh Kepala IPDE.	akses pengguna yang telah meninggalkan organisasi. • IPDE membuat prosedur untuk mengenai mengadaptasi hak akses pengguna yang telah memiliki perubahan peran atau pekerjaan. • IPDE membuat catatan mengenai hak akses yang diberikan kepada user ID untuk mengakses sistem

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				yang telah memiliki perubahan peran atau pekerjaan. • Segera memblokir hak akses pengguna yang telah meninggalkan organisasi. • Meninjau hak akses secara berkala. • Memberikan atau menetapkan peran akses berdasarkan kebutuhan bisnis. • Memasukan ketentuan hak akses dan sanksi pelanggarannya pada pada kontrak kerja		informasi. • Membuat kebijakan/ aturan untuk memastikan bahwa hak akses tidak diaktifkan oleh penyedia layanan sebelum prosedur otorisasi selesai.

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				pengguna.		
			9.4.1 Information access restriction Kontrol untuk memastikan bahwa akses ke informasi dan fungsi sistem aplikasi telah dibatasi sesuai dengan	• Terdapat pembatasan menu/ interface untuk mengendalikan akses terhadap fungsi sistem aplikasi. • Terdapat pengendalian data untuk diakses oleh pengguna tertentu. • Mengendalikan hak akses pengguna seperti membaca, menulis, menghapus dan mengeksekusi. • Terdapat	• Sistem memiliki pembatasan menu/ interface sesuai dengan hak akses pengguna. • Terdapat pengendalian data untuk diakses oleh pengguna tertentu. • Terdapat pengendalian hak akses pengguna	• IPDE membuat prosedur formal untuk mengendalikan pembatasan menu/ interface sesuai dengan hak akses pengguna. • IPDE membuat prosedur formal untuk mengendalikan hak akses pengguna seperti

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			kebijakan kontrol akses.	pengendalian hak akses dari aplikasi lain. • Terdapat pengendalian terhadap informasi yang terkandung dalam output. • Memiliki kontrol akses fisik atau logis untuk isolasi aplikasi sensitif, aplikasi data atau sistem.	seperti membaca, menulis, menghapus dan mengeksekusi oleh database administrator.	membaca, menulis, menghapus dan mengeksekusi oleh database administrator. • IPDE membuat aturan/ persyaratan untuk mengendalikan informasi yang terkandung dalam output. • IPDE membuat kontrol akses fisik atau logis untuk isolasi aplikasi sensitif, aplikasi data atau

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
						sistem.
		Kurangnya evaluasi dan monitoring	***9.2.5 Review of user access***	• Terdapat peninjauan ulang terhadap hak	• Terdapat pendataan	• IPDE membuat prosedur

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
		pada hak akses Aplikasi SIMRS	***rights*** Kontrol untuk memastikan bahwa pemilik aset telah meninjau hak akses penggunaan asetnya secara berkala	akses pengguna secara berkala, terutama setelah ada perubahan seperti promosi, penurunan pangkat atau pemutusan hubungan kerja. • Memiliki catatan terhadap perubahan akun dan ditinjau secara berkala, terutama akun yang memiliki hak istimewa. • Memastikan bahwa tidak ada hak akses ilegal (tidak sah).	mengenai status kepegawaian oleh Bagian Organisasi dan Kepegawaian	mengenai peninjauan ulang terhadap hak akses pengguna pada Aplikasi SIMRS. • IPDE melakukan *review* terhadap hak akses pengguna pada Aplikasi SIMRS secara rutin dan berkala. • IPDE membuat pendataan/ pencatatan mengenai histori perubahan hak akses pada

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
						Aplikasi SIMRS (penambahan, modifikasi dan penghapusan). • IPDE harus melakukan pengecekan rutin untuk memastikan bahwa status kepegawaian dan hak akses sudah sesuai. • IPDE harus memastikan bahwa tidak ada satupun hak akses ilegal ataupun *redundan*.

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
						• IPDE harus memastikan bahwa tidak ada penggunaan akun bersama oleh beberapa pengguna Aplikasi SIMRS. • IPDE memberikan peringatan atau sanksi bagi pengguna yang ketahuan melanggar hak akses pada Aplikasi SIMRS.

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
		Sharing password pada user Aplikasi SIMRS	***9.3.1 Use of secret authentication information*** Kontrol untuk memastikan bahwa pengguna telah mengikuti cara-cara organisasi dalam menggunakan informasi yang harus	• Terdapat saran atau anjuran kepada pengguna untuk merahasiakan informasi rahasia / autentikasi kepada pihak luar atau pihak yang tidak berwenang. • Terdapat saran atau anjuran kepada pengguna untuk menghindari penyimpanan catatan (seperti diatas kertas, file perangkat lunak atau perangkat	• Terdapat pelatihan mengenai kewaspadaan keamanan informasi untuk para pengguna Aplikasi SIMRS. • Terdpat kebijakan mengenai keamanan informasi data elektronik	• IPDE membuat aturan / kebijakan penggunaan autentikasi pada akun Aplikasi SIMRS, agar pengguna tidak diperbolehkan untuk melakukan *sharing* informasi autenttikasi. • IPDE membuat aturan/ kebijakan agar pengguna

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
R28	Pencurian data	Terjadi social engineering pada user maupun admin	memiliki otentikasi rahasia.	genggan) mengenai autentikasi rahasia milik pribadi. • Mengubah informasi authentikasi rahasia pada keadaan tertentu sesuai evaluasi risiko. • Memiliki kriteria kualitas *password.*	• Terdapat pelatihan mengenai kewaspadaan keamanan informasi bagi para pengguna Aplikasi SIMRS.	tidak diperbolehkan untuk menyimpan informasi autentikasi pada tempat yang dapat dilihat oleh pengguna lain (kertas, *mobile device*). • IPDE membuat aturan mengenai standar minimum untuk kualitas *password user* pada Aplikasi

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
						SIMRS. • IPDE membuat anjuran kepada pengguna untuk tidak memberikan informasi apapun kepada pihak luar mengenai Aplikasi SIMRS dan authentikasinya untuk menghindari *social engineering* pada

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
						user. • IPDE membuat aturan/ kebijakan mengenai batas kadaluarsa suatu *password.*
R02	Manipulasi data	Pencurian *username* dan *password* pada user Aplikasi SIMRS	***9.4.3 Password management system*** Kontrol untuk memastikan bahwa sistem manajemen password telah	• Terdapat penggunaan ID dan kata kunci individual untuk menjaga akuntabilitas. • Memiliki sistem yang memungkinkan pengguna untuk memilih dan mengubah *password* mereka sendiri. • Memiliki sistem	• Terdpat kebijakan mengenai keamanan informasi data elektronik • Sistem memiliki menu untuk memungkinkan pengguna memilih dan mengubah	• IPDE membuat sistem ataupun persyaratan yang memaksa pengguna mengubah kata sandi *default* yang diberikan padat saat pertama masuk. • IPDE membuat standar minimum

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			interaktif dan telah dipastikan kualitas passwordnya.	yang memaksa pengguna mengubah kata sandi *default* yang diberikan padat saat pertama masuk. • Memiliki kriteria pilihan kata kunci yang berkualitas. • Terdapat penyimpanan catatan *password* yang sebelumnya digunakan untuk mencegah penggunaan ulang *password* tersebut. • Tidak menampilkan kata sandi di layar	*password* mereka sendiri. • Memiliki ID unik untuk setiap pengguna • Terdapat pemberian *password* default kepada setiap pengguna ketika pertama kali log-on • Sistem telah menyembunyikan kata sandi di layar saat proses masuk	untuk kualitas *password* pada Aplikasi SIMRS. • IPDE menyediakan sistem yang menyimpan catatan histori *password* pengguna, agar *password* yang sama tidak digunakan oleh satu pengguna selama lebih dari satu kali. • Menyimpan file kata sandi secara terpisah dari data

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				saat proses masuk. • Menyimpan file kata sandi secara terpisah dari data sistem aplikasi. • Menyimpan dan mengirimkan kata sandi dalam bentuk yang dilindungi seperti enkripsi. • Menegakkan perubahan *password default* dan perubahan *password* secara masal pada periode tertentu sesuai dengan kebutuhan.		sistem aplikasi • IPDE membuat aturan/kebijakan untuk menegakkan perubahan *password default* dan perubahan *password* secara masal pada periode tertentu sesuai dengan kebutuhan.

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
		Exploitasi *session login*	***9.4.2 Secure log-on procedures*** Kontrol untuk memastikan bahwa prosedur log-on aman ketika dibutuhkan oleh kebijakan kontrol akses, akses ke sistem dan akses ke aplikasi.	• Memiliki prosedur untuk masuk ke sistem atau aplikasi untuk meminimalkan peluang akses tidak sah. • Terdapat persyaratan log-on yang aman bagi pengguna dengan menampilkan seminimal mungkin infromasi authentikasi pada saat log-on. • Mengenkripsi kata sandi selama sesi log-on melalui jaringan untuk	• Sistem telah menyembunyikan kata sandi di layar selama proses log-on	• IPDE membuat aturan/ kebijakan mengenai persyaratan log-on yang aman bagi pengguna Aplikasi SIMRS. • IPDE meng-enkripsi kata sandi selama sesi log-on melalui jaringan untuk menhindari program *sniffer.* • IPDE membuat prosedur untuk masuk ke sistem atau aplikasi

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				menghindari program sniffer.		untuk meminimalkan peluang akses tidak sah
Risiko Kontrol Akses *Physical*						
			11.1.2 Physical entry controls Kontrol untuk memastikan bahwa daerah telah dilindungi oleh kontrol masuk yang tepat sehingga	• Terdapat kontrol akses masuk yang sesuai pada lokasi yang mengandung informasi sensitif atau fasilitas pengolahan informasi yang kritis. • Memiliki catatan mengenai tanggal dan waktu masuk pengunjung ke lokasi yang mengandung	• Terdapat penguncian menggunakan teknologi bar code pada pintu ruang server. • Terdapat formulir masuk area ruang server. • Terdapat kartu identitas ID	• Membuat prosedur akses masuk ruang server. • Membuat catatan mengenai tanggal dan waktu masuk pengunjung ke lokasi yang mengandung informasi sensitif atau fasilitas pengolahan

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			dapat dipastikan bahwa hanya pihak yang berwenang yang diperbolehkan mengakses.	informasi sensitif atau fasilitas pengolahan informasi yang kritis. • Terdapat pengawasan pada pengunjung yang akan masuk ke lokasi IT kecuali akses mereka telah disetujui sebelumnya. • Terdapat sarana untuk mengautentikasi identitas pengunjung. • Terdapat instruksi mengenai persyaratan	untuk mengauthentikasi pengguna yang ingin akses lokasi IT. • Terdapat pembatasan untuk pengguna yang dapat dan diperbolehkan akses PC dan lokasi server.	informasi yang kritis. • Membuat kebijakan untuk melakukan pengawasan terhadap pengunjung yang akan masuk ke lokasi IT kecuali akses mereka telah disetujui sebelumnya. • Membuat dan memberikan akses yang spesifik untuk pengguna sesuai dengan tujuan

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				keamanan daerah dan prosedur darurat. • Memberikan akses yang spesifik untuk pengguna sesuai dengan tujuan yang telah disahkan. • Terdapat kontrol akses ke area dimana informasi rahasia diproses atau disimpan harus dibatasi, seperti mekanisme otentikasi. • Memiliki buku log fisik atau jejak audit elektronik untuk semua akses dan		yang telah disahkan. • Memantau buku log akses secara berkala. • Terdapat instruksi untuk semua karyawan, kontraktor dan pihak luar agar mengenakan beberapa bentuk identikasi yang terlihat. • Membuat instruksi untuk segera memberitahu petugas

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				diperlihara serta dipantau dengan aman. • Terdapat instruksi untuk semua karyawan, kontraktor dan pihak luar agar mengenakan beberapa bentuk identikasi yang terlihat. • Terdapat instruksi untuk segera memberitahu petugas keamanan jika melihat pengunjung tanpa identitas yang jelas.		keamanan jika melihat pengunjung tanpa identitas yang jelas. • Melakukan *review* hak akses ke area TI, serta meninjau dan memperbaharui secara berkala, dan mencabut hak akses bila diperlukan. • Membuat batasan akses area atau fasilitas pemrosesan informasi rahasia

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				• Terdapat batasan akses area atau fasilitas pemrosesan informasi rahasia yang jelas untuk personel layanan pendukung pihak luar, akses tersebut harus diotorisasi dan dipantau dengan jelas. • Hak akses ke area TI harus ditinjau dan diperbaharui secara berkala, dan dicabut bila diperlukan.		yang jelas untuk personel layanan pendukung pihak luar.
			11.1.5 Working in secure area	• Menghindari pekerjaan tanpa	• Terdapat pengawasan	• Membuat aturan/ kebijakan agar

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			Kontrol untuk memastikan bahwa prosedur untuk bekerja di area aman telah dirancang dan diterapkan.	pengawasan di daerah yang memiliki informasi kritis dan sensitif. • Lokasi atau area yang memiliki informasi kritis dan sensitif yang kosong harus dikunci secara fisik dan ditinjau secara berkala. • Terdapat persyaratan untuk melarang peralatan perekam fotografi, video, audio atau lainnya, seperti kamera di perangkat mobile kecuali telah	CCTV pada jalur keluar-masuk ruangan yang diawasi oleh petugas keamanan. • Terdapat beberapa personil satuan petugas keamanan yang melakukan monitoring keamanan ke ruangan-ruangan. • Memiliki almari	selalu meninggalkan peralatan IT dan ruangan IT dalam keadaan terkunci. • Membuat aturan/ kebijakan untuk melarang peralatan perekam fotografi, video, audio atau lainnya, seperti kamera di perangkat mobile kecuali telah memiliki ijin yang sah.

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				memiliki ijin yang sah.	pelindung CPU yang memiliki kunci.	
			11.2.8 Unattended user equipment Kontrol untuk memastikan bahwa peralatan yang tidak diawasi memiliki perlindungan yang tepat.	• Terdapat persyaratan dan prosedur keamanan untuk melindungi peralatan tanpa pengawasan, serta tanggung jawab mereka untuk menerapkan perlindungan. • Terdapat persyaratan pada pengguna untuk menghentikan sesi aktif saat selesai, kecuali jika dijamin dengan mekanisme	• Terdapat kebijakan mengenai pengendalian fisik untuk mengamankan area dan perangkat pengolahan informasi elektronik.	• Membuat persyaratan keamanan untuk melindungi peralatan tanpa pengawasan, serta tanggung jawab mereka untuk menerapkan perlindungan • Membuat persyaratan pada pengguna untuk

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
				penguncian otomatis seperti *screensaver* yang dilindungi dengan kata sandi. • Terdapat persyaratan kepada pengguna untuk log-off dari aplikasi atau layanan jaringan bila tidak lagi dibutuhkan. • Terdapat pengamanan pada komputer atau perangkat mobile dari pengguna tidak sah dengan kunci seperti *password.*		menghentikan sesi aktif saat selesai, kecuali jika dijamin dengan mekanisme penguncian otomatis seperti *screensaver* yang dilindungi dengan kata sandi. • Membuat persyaratan kepada pengguna untuk log-off dari aplikasi atau layanan jaringan bila tidak lagi

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
						dibutuhkan. • Membuat pengamanan pada komputer atau perangkat mobile dari pengguna tidak sah dengan kunci seperti *password.*
			11.2.9 Clear desk and clear screen policy Kontrol untuk memastikan bahwa kebijakan	• Memiliki kebijakan mengenai ruang kerja dan layar kerja yang berbas dari informasi rahasia • Informasi bisnis yang kritis dan sensitif, misal di atas	• Terdapat pelatihan mengenai kewaspadaan keamanan informasi pada pengguna.	• Membuat kebijakan mengenai ruang kerja dan layar kerja yang bebas dari informasi rahasia. • Membuat

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			meja kerja bebas dari kertas yang berisi informasi rahasia dan media penyimpanan yang mudah dipindahkan. Kebijakan layar yang bebas dari informasi rahasia pada fasilitas pengolahan informasi	kertas atau media penyimpanan elektronik harus selalu terkunci bila tidak dibutuhkan, terutama saat kantor sedang dalam keadaan kosong. • Komputer dan terminal harus dibiarkan mati atau dilindungi dengan penguncian layar serta keyboard saat tidak digunakan. • Penggunaan mesin fotokopi dan teknologi reproduksi lainya yang tidak sah		kebijakan untuk melindungi informasi bisnis yang kritis dan sensitif, misal di atas kertas atau media penyimpanan elektronik harus selalu terkunci bila tidak dibutuhkan, terutama saat kantor sedang dalam keadaan kosong. • Komputer dan terminal harus

Risiko			Tindakan mitigasi berdasarkan ISO/IEC:27002:2013		Praktik Keamanan Terkini	Rekomendasi Mitigasi
ID	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	*Control Objective*	Petunjuk pelaksanaan berdasarkan kontrol ISO27002:2013		
			harus diadopsi.	seperti scanner atau kamera digital harus dicegah. • Media yang berisi informasi sensitif atau rahasia harus segera dihapus dari printer.		dibiarkan mati atau dilindungi dengan penguncian layar serta keyboard saat tidak digunakan

LAMPIRAN D – KEBIJAKAN

1. Kebijakan Pengendalian Hak Akses Sistem Informasi

KJ01 - KEBIJAKAN PENGENDALIAN HAK AKSES SISTEM INFORMASI

KEBIJAKAN PENGENDALIAN HAK AKSES SISTEM INFORMASI DI LINGKUNGAN RSUD Dr. MOEWARDI

1. TUJUAN

   Pengendalian akses bertujuan untuk memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang ke sistem informasi untuk menjaga keamanan informasi pada sistem informasi.

2. RUANG LINGKUP
   1. Pengelolaan Hak Akses Pengguna Sistem Informasi
   2. Pengelolaan Hak Akses Sementara
   3. Persyaratan Akun Pengguna

3. REFERENSI

   ISO 27002:2013 - 9.1.1 *Access control policy*

   ISO 27002:2013 - 9.2.1 *User registration and de-registration*

   ISO 27002:2013 - *9.2.2 User access provisioning*

   ISO 27002:2013 - *9.4.1 Information access restriction*

   ISO 27002:2013 - *9.2.5 Review of user access rights*

   ISO 27002:2013 - *9.2.6 Removal or adjustment of access rights*

4. KEBIJAKAN
   1. Pengelolaan Hak Akses Pengguna Sistem Informasi
      a. Hak akses pada setiap sistem informasi harus dibedakan sesuai dengan peran dan fungsi dari masing-masing pengguna.
      b. Pemberian hak akses pada sistem informasi harus dibatasi berdasarkan kebutuhan proses bisnis pengguna dan harus disetujui oleh Kepala IPDE.
      c. Pemberian hak akses sistem informasi dengan tingkatan tinggi (root, super user atau administrator) hanya diberikan kepada karyawan yang

benar-benar kompeten, terpercaya dan mendapat persetujuan dari Kepala IPDE.

d. Hak akses hanya boleh diberikan setelah prosedur resmi permintaan hak akses telah dipenuhi dan diselesaikan oleh pengguna.
e. Setiap proses pengelolaan baik penghapusan maupun pemberian hak akses harus didokumentasikan.
f. Dilakukan peninjauan ulang pada hak akses sistem informasi secara berkala.
g. Hak akses yang sudah diberikan tidak boleh digunakan maupun dipinjamkan kepada orang lain tanpa adanya ijin dan pemberitahuan perubahan hak akses baru.

2. Pengelolaan Hak Akses Sementara
   a. Pegawai magang, residen dan pihak ketiga RSUD Dr. Moewardi yang ingin mengakses sistem informasi harus memenuhi prosedur permintaan akses yang telah ditetapkan.
   b. Pemberian hak akses sementara harus dibatasi waktunya sesuai dengan kebutuhan proses bisnis pengguna tersebut.
   c. Segera menonaktifkan hak akses sementara ketika mencapai batas waktu yang diizinkan.
   d. Hak akses sementara harus ditinjau ulang secara berkala.
   e. Setiap kegiatan yang dilakukan pihak ketiga harus di dimonitoring.

3. Persyaratan Akun Pengguna
   a. Menyediakan akun yang unik untuk setiap pengguna yang ingin terhubung ke sistem informasi agar tindakan setiap penguna mudah dimonitoring.
   b. Memastikan tidak ada redudansi akun dan hak akses pengguna.
   c. Memberikan peringatan agar user segera mengganti *password* default yang telah diberikan pertama kali.
   d. Penyedia layanan sistem informasi menentukan kriteria kualitas minimum *passsword* untuk masuk ke sistem informasi.
   e. Penyedia layanan sistem informasi menentukan jangka waktu maksimal untuk merubah *password*.

LAMPIRAN E – PROSEDUR

1. SP01-Standar Operasional Prosedur Penanganan Permintaan Hak Akses Aplikasi SIMRS.

SP01/KJ01-STANDAR OPERASIONAL PROSEDUR PENANGANAN PERMINTAAN HAK AKSES APLIKASI SIMRS

RUMAH SAKIT UMUM DAERAH Dr.MOEWARDI 	Nomor SOP	**SP01**
	Nama SOP	**SOP Penanganan Permintaan Hak Akses Aplikasi SIMRS**
	Tanggal Pembuatan	/ /
	Nomor Revisi	/ /
	Tanggal Berlaku	/ /
	Disahkan oleh	(_____)

DESKRIPSI SOP	**KUALIFIKASI DAN DAFTAR PELAKSANA**
Prosedur ini berfungsi untuk memastikan bahwa pemberian hak akses telah terkontrol dengan baik dan memastikan seluruh akses telah terautorisasi serta memiliki sebuah *log* aktivitas yang dapat dimonitor dengan baik. Tujuan dari SOP ini adalah memberikan panduan secara efektif dan efisien dalam menyelesaikan permintaan pembuatan akun baru maupun perubahan akun lama pada Aplikasi SIMRS.	DAFTAR PELAKSANA - User - Petugas Administrasi - Admin - Kepala Instalasi PDE KUALIFIKASI PELAKSANA - Memiliki kemampuan pemahaman proses bisnis yang baik - Memiliki akses dalam pembuatan akses Aplikasi SIMRS - Memiliki pemahaman dan pengetahuan yang cukup dibidang pengelolaan hak akses Aplikasi SIMRS
KETERKAITAN	
KJ01-Kebijakan Pengendalian Hak Akses Sistem Informasi	
REFERENSI	**PERLENGKAPAN / PERSYARATAN**
- ISO 27002:2013 - 9.2.1 *User registration and de-registration* - ISO 27002:2013 - *9.2.2 User access provisioning* - ISO 27002:2013 - *9.4.1 Information access restriction*	- Formulir Permintaan Akun Baru (FM01) - Formulir Permintaan Perubahan Akses (FM02) - Formulir Log Perekaman Permintaan Hak Akses (FM04) - Formulir Verifikasi dan Pemberian Hak Akses (FM05) - Instruksi Kerja Penambahan Akun dan Hak Akses (IK01) - Instruksi Kerja Penghapusan Hak Akses (IK02)
PERINGATAN	
Jika SOP ini tidak dijalankan dapat mengakibatkan **Risiko R15.3** yaitu **Kesalahan pemberian hak akses pada user Aplikasi SIMRS** yang memiliki nilai RPN *(Risk Prriority Number)* 160 dan termasuk dalam kategori risiko "*High*".	

A. TUJUAN

Tujuan dari SOP ini adalah untuk menstandarkan proses pembuatan akun baru dan proses perubahan akun lama pada Aplikasi SIMRS yang mengacu pada kontrol ISO27002, serta untuk meminimalisir risiko kesalahan dalam pemberian hak akses. Selain itu, dengan adanya prosedur ini dapat memberikan kemudahan bagi Instalasi PDE dalam melakukan rekapan informasi mengenai permintaan pembuatan maupun perubahan hak akses yang ada pada akun Aplikasi SIMRS.

B. RUANG LINGKUP

Prosedur terdiri dari dua sub-prosedur yaitu prosedur pembuatan akun baru dan sub-prosedur perubahan hak akses lama

C. DEFINISI

Admin adalah pegawai Instalasi PDE yang diberi wewenang untuk melakukan ekseskusi pengelolaan hak akses seperti menambah, mengubah dan menghapus hak akses pada akun Aplikasi SIMRS. Pegawai Tersebut adalah Programmer dan petugas *Implementasi* dan *troubleshooting*.

D. ALUR MANAJEMEN ESKALASI

Eskalasi manajemen akses dibutuhkan apabila level tertentu tidak dapat menangani pengelolaan akses sehingga peranan level diatasnya dapat menangani permasalahan tersebut. Hal ini dapat dilaksanakan oleh pihak manajerial yang memiliki pengetahuan dan wewenang dalam melakukan penanganan manajemen akses. Semakin tinggi level pelaksana maka dapat berperan penting dalam pengambilan keputusan terkait manajemen akses.

Level	Pelaksana	Deskripsi Pekerjaan
Level 1	Petugas Administrasi	- Menerima surat masuk - Mencatat surat masuk - Menyimpan dan mengarsipkan surat dan berkas
Level 2	Admin	- Melaksanakan eksekusi pembuatan akun baru dan perubahan hak akses lama pada Aplikasi SIMRS
Level 3	Kepala Instalasi PDE	- Membuat keputusan mengenai pemberian hak akses user - Melakukan verifikasi kebutuhan hak akses user
Level 4	Kepala Bagian Perencanaan	Menjadi pengambil keputusan permasalahan diluar wewenang Kepala Instalasi PDE dan melakukan pengawasan
Level 5	Wakil Direktur Umum	Menjadi pengambil keputusan permasalahan diluar wewenang Kepala Bagian Perencanaan dan melakukan pengawasan
Level 6	Direktur	Menjadi pengambil keputusan tertinggi dan melakukan pengawasan

E. RINCIAN PROSEDUR

A) SUB-PROSEDUR PEMBUATAN AKUN BARU

1. Proses Pengajuan Permintaan Akun Baru

   1.1 User membuat surat permohonan pembuatan akun baru Aplikasi SIMRS yang disetujui oleh Kepala Unit terkait.
   1.2 User mengisi Formulir Permintaan Akun Baru (FM01).
   1.3 User menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran ke petugas Administrasi Instalasi PDE.

2. Proses Penerimaan Permintaan Akun Baru

   2.1 Petugas Administrasi menerima surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran.
   2.2 Petugas Administrasi mencatat permintaan akun baru Aplikasi SIMRS pada Formulir Log Perekaman Hak Akses (FM04).
   2.3 Petugas Administrasi menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran ke Admin.

1. Proses Verifikasi Permintaan Akun Baru

   3.1 Admin menerima surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran.
   3.2 Admin PDE mengisi Formulir Verifikasi dan Pemberian Akses (FM05) dengan melihat data *role* user dan hak akses sistem .
   3.3 Admin PDE menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) , persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05) ke Kepala Instalasi PDE untuk meminta persetujuan.
   3.4 Kepala Instalasi PDE memberikan keputusan persetujuan dan menyerahkan kembali kepada Admin

2. Proses Pemberian Hak Akses

   4.1 Admin menerima surat permohonan, Formulir Permintaan Akun Baru (FM01), persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05).
   4.2 Admin menjalankan Instruksi Kerja Penambahan Akun dan Hak Akses (IK01) dengan acuan Formulir Permintaan Akun Baru (FM01) dan Formulir Verifikasi dan Pemberian Akses (FM05).
   4.3 Admin mengecek permintaan *username*
   - Jika *username* yang diajukan sudah digunakan oleh user lain, maka Admin memberikan informasi kepada user via telepon atau email. Kemudian lakukan aktivitas 4.4.
   - Jika *username* yang diajukan belum digunakan oleh user lain maka lakukan aktivitas 4.4.

   4.4 Admin menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) , persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05) kepada petugas Administrasi.

3. Proses Penyelesaian Pembuatan Akun Baru

   5.1 Petugas Administrasi menerima surat permohonan, Formulir Permintaan Akun Baru (FM01) , persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05).
   5.2 Petugas Administrasi memperbaharui status permintaan pada Formulir Log Perekaman Hak Akses (FM04).

B) SUB-PROSEDUR PERUBAHAN HAK AKSES LAMA

1. Proses Pengajuan Permintaan Perubahan Hak Akses

   1.1 User membuat surat permohonan perubahan hak akses Aplikasi SIMRS yang disetujui oleh Kepala Unit terkait.
   1.2 User mengisi Formulir Perubahan Akses (FM02).
   1.3 User menyerahkan surat permohonan, Formulir Perubahan Akses (FM02) dan persyaratan lampiran ke petugas Administrasi Instalasi PDE.

2. Proses Penerimaan Permintaan Perubahan Hak Akses

   2.1 Petugas Administrasi menerima surat permohonan, Formulir Perubahan Akses (FM02) dan persyaratan lampiran.
   2.2 Petugas Administrasi mencatat permintaan akun baru Aplikasi SIMRS pada Formulir Log Perekaman Hak Akses (FM04).
   2.3 Petugas Administrasi menyerahkan surat permohonan, Formulir Perubahan Akses (FM02) dan persyaratan lampiran ke Admin.

3. Proses Verifikasi Permintaan Akun Baru

   3.1 Admin menerima surat permohonan, Formulir Perubahan Akses (FM02) dan persyaratan lampiran.
   3.2 Admin PDE mengisi Formulir Verifikasi dan Pemberian Akses (FM05) dengan melihat data *role* user dan hak akses sistem .
   3.3 Admin PDE menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) , persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05) ke Kepala Instalasi PDE untuk meminta persetujuan.
   3.4 Kepala Instalasi PDE memberikan keputusan persetujuan dan menyerahkan kembali kepada Admin

4. Proses Pemberian Hak Akses

   4.1 Admin menerima surat permohonan, Formulir Perubahan Akses (FM02), persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05).
   4.2 Admin menjalankan Instruksi Kerja Penambahan Akun dan Hak Akses (IK01) dan Instruksi Kerja Penghapusan Hak Akses (IK02) sesuai dengan acuan Formulir Verifikasi dan Pemberian Akses (FM05) yang telah verifikasi sesuai kebutuhan pekerjaan user.
   4.3 Admin menyerahkan surat permohonan, Formulir Perubahan Akses (FM02), persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05) kepada petugas Administrasi.

5. Proses Penyelesaian Pembuatan Akun Baru

   5.1 Petugas Administrasi menerima surat permohonan, Formulir Perubahan Akses (FM02), persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05)
   5.2 Petugas Administrasi memperbaharui status permintaan pada Formulir Log Perekaman Hak Akses (FM04)

F. BAGAN ALUR PROSEDUR

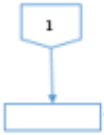
SP01-STANDAR OPERASIONAL PROSEDUR PENANGANAN PERMINTAAN HAK AKSES APLIKASI SIMRS

A) SUB-PROSEDUR PEMBUATAN AKUN BARU (1/4)

No	Uraian Prosedur	Pelaksana				Dokumen Terkait
		User	Petugas Administrasi	Admin	Kepala Instalasi PDE	
1. Proses Pengajuan Permintaan Akun Baru						
1.	Membuat surat permohonan pembuatan akun baru Aplikasi SIMRS yang disetujui oleh Kepala Unit terkait					
2.	Mengisi Formulir Permintaan Akun Baru (FM01)					• Formulir Permintaan Akun Baru (FM01)
3.	Menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran ke petugas Administrasi Instalasi PDE					• Surat permohonan • Formulir Permintaan Akun Baru (FM01) • Persyaratan lampiran
2. Proses Penerimaan Permintaan Akun Baru						
4.	Menerima surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran					• Surat permohonan • Formulir Permintaan Akun Baru (FM01) • Persyaratan lampiran
5.	Mencatat permintaan akun baru Aplikasi SIMRS pada Formulir Log Perekaman Hak Akses (FM04)					• Formulir Log Perekaman Hak Akses (FM04)

SP01 STANDAR OPERASIONAL PROSEDUR PENANGANAN PERMINTAAN HAK AKSES APLIKASI SIMRS

A) SUB-PROSEDUR PEMBUATAN AKUN BARU (2/4)

No	Uraian Prosedur	Pelaksana				Dokumen Terkait
		User	Petugas Administrasi	Admin	Kepala Instalasi PDE	
6.	Menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran ke Admin					• Surat permohonan • Formulir Permintaan Akun Baru (FM01) • Persyaratan lampiran • Formulir Log Perekaman Hak Akses (FM04)
3. Proses Verifikasi Permintaan Akun Baru						
7.	Menerima surat permohonan, Formulir Permintaan Akun Baru (FM01) dan persyaratan lampiran					• Surat permohonan • Formulir Permintaan Akun Baru (FM01) • Persyaratan lampiran
8.	Mengisi Formulir Verifikasi dan Pemberian Akses (FM05) dengan melihat data *role* user dan hak akses sistem					• Formulir Verifikasi dan Pemberian Akses (FM05) • Data *role* user dan hak akses sistem
9.	Menyerahkan surat permohonan, Formulir Permintaan Akun Baru (FM01) , persyaratan lampiran dan Formulir Verifikasi dan Pemberian Akses (FM05) ke Kepala Instalasi PDE					• Surat permohonan • Formulir Permintaan Akun Baru (FM01) • Persyaratan lampiran • Formulir Verifikasi dan Pemberian Akses (FM05)

LAMPIRAN F – FORMULIR

Berikut merupakan contoh dari salah satu Formulir yang dihasilkan dalam penelitian yaitu FM03- Formulir Penghapusan Hak Akses

FM03-FORMULIR PENGHAPUSAN HAK AKSES

	RUMAH SAKIT UMUM DAERAH Dr. MOEWARDI INSTALASI PENGELOLA DATA ELEKTRONIK	
	FM03	NOMOR FORMULIR : [Diisi oleh petugas]
	FORMULIR PENGHAPUSAN HAK AKSES	
Tanggal	_____/_____/_____ [ex: 04/01/2017]	
Sumber Penghapusan Hak Akses	☐ Hasil Pemantauan Admin	
	☐ Permintaan Nomor Surat Permintaan Penghapusan : [mengisi nomor surat permintaan dari unit]	
IDENTITAS PENGGUNA		
Username	[mengisi username saat ini]	
Nama Lengkap	[mengisi nama lengkap]	
NIP	[mengisi nomor NIP]	
Bagian/Unit	[mengisi bagian/unit]	
Jabatan	[mengisi jabatan]	
PENGHAPUSAN AKUN		
Keterangan :*Pilih salah satu jenis kategori anda dibawah ini dengan tanda centang (V).		
Jenis User Operator: ☐ Direksi ☐ Dokter Spesialis ☐ Pegawai ☐ Residen		Alasan: ☐ Mengundurkan Diri ☐ Diberhentikan ☐ Pensiun ☐ Purna Tugas ☐ Meninggal Dunia ☐ Lainnya____

KESESUAIAN SOP DENGAN KONTROL OBYEKTIF PADA ISO27002:2013

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
1	*9.1.1 Access control policy*	Kontrol untuk memastikan bahwa kebijakan kontrol akses telah dibentuk, didokumentasikan dan ditinjau berdasarkan kebutuhan keamanan bisnis dan informasi	- Mempertimbangkan kontrol akses *physical* dan *logical* secara bersama-sama	Digunakan dalam penelitian karena pembuatan SOP ini melibatkan kontrol akses *physical* dan *logical* dari Aplikasi SIMRS
			- Menentukan kontrol, hak akses dan batasan peran pengguna	- Termasuk dalam aktivitas no. 3.2 prosedur SPO Sub-Prosedur A - Termasuk dalam aktivitas no. 3.2 prosedur SP01 Sub-Prosedur B - Termasuk dalam aktivitas no. 2.2 dan 2.3 prosedur SP05
			- Pemisahan permintaan akses, otorisasi dan administrasi akses	Terdokumentasi pada FM01 Formulir Permintaan Akun Baru, FM02 Formulir Permintaan Perubahan Akses dan FM05 Formulir Verifikasi

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
				dan Pemberian Akses
			- Memiliki persyaratan untuk otorisasi formal permintaan akses	Termasuk dalam prosedur SP01 yaitu SOP Penanganan Permintaan Hak Akses Aplikasi SIMRS
			- Peninjauan hak akes secara berkala	Termasuk dalam prosedur SP02 yaitu SOP Pemantauan Hak Akses pada Akun Aplikasi SIMRS
			- Memiliki persyaratan penghapusan hak akses	Termasuk dalam prosedur SP03 yaitu SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS
			- Pengarsipan catatan kejadian penting mengenai penggunaan dan pengelolaan identitas pengguna dan informasi otentikasi	Terdokumentasi pada FM06 Formulir Pemantauan Dan Evaluasi Hak Akses
			- Memiliki peraturan	Tidak digunakan dalam

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
			perundang-undangan yang relevan dan kewajiban kontraktual mengenai pembatasan akses terhadap data atau layanan	penelitian
			- Manajemen hak akses yang terhubung untuk mengenali segala jenis tipe koneksi	Tidak digunakan dalam penelitian
2	9.2.1 *User registration and de-registration*	Kontrol untuk memastikan bahwa proses registrasi dan de-registrasi pengguna formal telah diimplementasikan untuk memberikan hak akses yang tepat.	- Penggunaan ID unik untuk setiap pengguna	Termasuk dalam aktivitas no. 4.3 prosedur SP01 Sub-Prosedur A
			- Memberikan hak akses sesuai dengan kebutuhan bisnis pengguna	- Termasuk dalam aktivitas no. 3.2 prosedur SPO1 Sub-Prosedur A - Termasuk dalam aktivitas no. 3.2 prosedur SP01 Sub-Prosedur B - Termasuk dalam aktivitas no. 2.2 dan 2.3 prosedur

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
				SP05
			- Perijinan penggunaan ID bersama *(shared ID)* harus didokumentasikan beserta alasannya	Tidak digunakan dalam penelitian
			- Segera menonaktifkan atau menghapus ID pengguna yang telah meninggalkan organisasi	Termasuk dalam prosedur SP03 yaitu SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS
			- Secara berkala mengidentifikasi dan menghapus/menonaktifkan ID pengguna yang redundan dan tidak perlu	- Termasuk dalam prosedur SP02 yaitu SOP Pemantauan Hak Akses pada Akun Aplikasi SIMRS - Termasuk dalam prosedur SP03 yaitu SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS
			- Memastikan tidak ada ID pengguna yang redundan	Termasuk dalam aktivitas no. 4.3 prosedur SP01Sub-Prosedur A

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
3	*9.2.2 User access provisioning*	Kontrol untuk memastikan bahwa proses penyediaan hak akses resmi pengguna telah diimplementasikan untuk mencabut dan menetapkan hak akses pada seluruh jenis pengguna di semua sistem dan layanan.	- Memastikan proses otorisasi hanya dilakukan oleh pihak penyedia layanan yang resmi	Termasuk dalam prosedur SP01 yaitu SOP Penanganan Permintaan Hak Akses Aplikasi SIMRS
			- Memisahkan persetujuan hak akses dari manajemen	Tidak digunakan dalam penelitian
			- Memverifikasi bahwa tingkat akses sesuai dengan kebutuhan dan konsisten dengan persyaratan lain	- Termasuk dalam aktivitas no. 3.2 prosedur SPO1 Sub-Prosedur A - Termasuk dalam aktivitas no. 3.2 prosedur SP01 Sub-Prosedur B - Termasuk dalam aktivitas no. 2.2 dan 2.3 prosedur SP05
			- Memastikan hak akses tidak diaktifkan sebelum prosedur otorisasi selesai	Termasuk dalam aktivitas no. 4.1 dan 4.2 prosedur SP01 Sub-Prosedur A dan B
			- Memelihara catatan hak akses	Terdokumentasi pada FM04 Formulir Log Perekaman Permintaan Hak Akses

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
			- Segera menyesuaikan perubahan hak akses apabila terjadi perubahan peran dan menghapus pengguna yang telah meninggalkan organisasi	- Termasuk dalam prosedur SP02 yaitu SOP Pemantauan Hak Akses pada Akun Aplikasi SIMRS - Termasuk dalam prosedur SP03 yaitu SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS
			- Meninjau hak akses secara berkala	Termasuk dalam prosedur SP02 yaitu SOP Pemantauan Hak Akses pada Akun Aplikasi SIMRS
			- Mencantumkan perjanjian hak akses dan sanksi pelanggarannya pada kontrak kerja	Tidak digunakan dalam penelitian
4	*9.2.5 Review of user access rights*	Kontrol untuk memastikan bahwa pemilik aset telah meninjau hak akses penggunaan asetnya	- Meninjau ulang hak akses secara berkala	Termasuk dalam prosedur SP02 yaitu SOP Pemantauan Hak Akses pada Akun Aplikasi SIMRS
			- Segera menyesuaikan	- Termasuk dalam prosedur

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
		secara berkala	apabila terdapat perubahan setelah promosi, penurunan pangkat atau pensiun	SP02 yaitu SOP Pemantauan Hak Akses pada Akun Aplikasi SIMRS - Termasuk dalam prosedur SP03 yaitu SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS
			- Otorisasi hak istimewa harus ditinjau lebih sering	Tidak digunakan dalam penelitian
			- Memeriksa alokasi hak istimewa secara berkala	Tidak digunakan dalam penelitian
			- Mencatat setiap perubahan pada hak akses untuk ditinjau secara berkala	Terdokumentasi dalam formulir FM04 Formulir Log Perekaman Permintaan Hak Akses
5	*9.2.6 Removal or adjustment of access rights*	Kontrol untuk memastikan bahwa hak akses seluruh karyawan dan pengguna pihak	- Mencabut seluruh hak akses terhadap fasilitas pengolah informasi dan aset terkait setelah pengguna diberhentikan	Termasuk dalam prosedur SP03 yaitu SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
		eksternal pada akses informasi dan akses fasilitas pengolahan informasi telah dihapus setelah pemutusan hubungan kerja, kontrak atau perjanjian merela, atau disesuaikan dengan perubahan.	- Mencatat dan mendokumentasikan alasan penghentian hak akses	Terdokumentasi dalam FM03 Formulir Penghapusan Hak Akses
			- Memastikan semua kryawan untuk tidak berbagi informasi dengan pengguna yang telah diberhentikan	Termasuk dalam prosedur SP03 yaitu SOP Penghapusan Hak Akses pada Akun Aplikasi SIMRS
			- Memastikan seluruh dokumentasi yang mengidentifikasi akses pengguna harus menyertakan informasi penghapusan/pemberhentian	Tidak digunakan dalam penelitian
6	*9.3.1 Use of Secret Authentication Information*	Kontrol untuk memastikan bahwa pengguna telah mengikuti cara-cara organisasi dalam	- Pengguna disarankan untuk merahasiakan informasi authentikasi	Termasuk dalam aktivitas no. 2 prosedur SP04
			- Menghindari	Termasuk dalam aktivitas no. 3 prosedur SP04

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
		menggunakan informasi yang harus memiliki otentikasi rahasia.	penyimpanan catatan otentikasi rahasia	
			- Mengganti informasi authentikasi secara berkala	Termasuk dalam aktivitas no. 4 prosedur SP04
			- Memiliki kriteria atau persyaratan strong password	Tidak digunakan dalam penelitian
7	*9.4.1 Information access restriction*	Kontrol untuk memastikan bahwa akses ke informasi dan fungsi sistem aplikasi telah dibatasi sesuai dengan kebijakan kontrol akses.	- Hanya menyediakan menu yang dibutuhkan	-Termasuk dalam aktivitas no. 4.2 prosedur SPO1 Sub-Prosedur A Termasuk dalam aktivitas no. 4.2 prosedur SP01 Sub-Prosedur B
			- Mengendalikan data yang dapat diakses oleh user tertentu	Tidak digunakan dalam penelitian
			- Mengendalikan hak akses user seperti membaca, menulis, menghapus dan mengeksekusi	-Termasuk dalam aktivitas no. 3.2 prosedur SPO1 Sub-Prosedur A -Termasuk dalam aktivitas no.

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
				3.2 prosedur SP01 Sub-Prosedur B
			- Mengendalikan hak akses dari aplikasi lain	Tidak digunakan dalam penelitian
			- Membatasi informasi yang terkandung dalam output	Tidak digunakan dalam penelitian
			- Menyediakan kontrol akses fisik atau logis untuk isolasi aplikasi sensitif, aplikasi data, atau sistem	Digunakan dalam penelitian karena pembuatan SOP ini melibatkan kontrol akses *physical* dan *logical* dari Aplikasi SIMRS
8	*11.1.2 Physical entry controls*	Kontrol untuk memastikan bahwa daerah telah dilindungi oleh kontrol masuk yang tepat sehingga dapat dipastikan bahwa hanya pihak yang berwenang yang	- Mencatat tanggal dan waktu masuk dan	Terdokumentasi dalam FM08 Formulir Log Akses Server
			- Semua pengunjung harus diawasi dan didampingi	Termasuk dalam aktivitas no. 3.1 SP05
			- Pengunjung diberi akses yang spesifik dan tujuan yang sah	Termasuk dalam aktivitas no. 2.2 dan 2.3 prosedur SP05
			- Identitas pengunjung	Termasukt dalam aktivitas no.

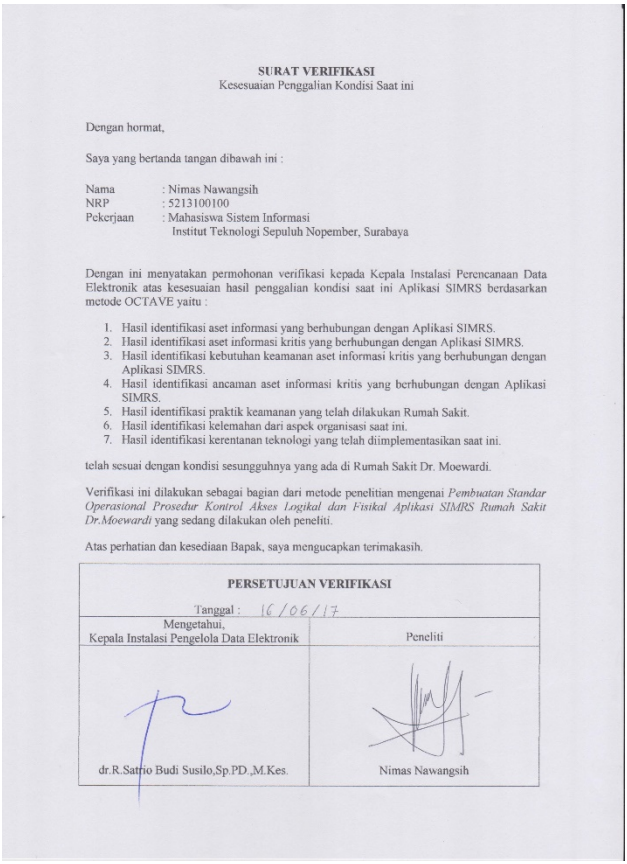
No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
		diperbolehkan mengakses.	harus diauthentikasi	2.2 prosedur SP05
			- Akses ke area informasi pengolahan dan penyimpanan informasi haris dibatasi.	Termasuk dalam aktivitas no. 3.3 prosedur SP05
			- Fisik buku log atau jejak audit elektronik untuk semua akses harus dipantau	Terdokumentasi pada FM08 Formulir Log Akses Server
			- Semua karyawan, kontrkator dan pihak luar harus mengenakan betuk identitas yang jelas.	Termasuk dalam aktivitas no.3 prosedur SP06
			- Personil layanan pendukung harus diberi akses terbatas	Tidak digunakan dalam penelitian
			- Hak akses ke area aman harus ditinjau dan diperbaharui secara berkala dan dicabut bila diperlukan	Termasukt dalam aktivitas no. 2.2 prosedur SP05

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
9	*11.1.5 Working in secure areas*	Kontrol untuk memastikan bahwa prosedur untuk bekerja di area yang aman telah dirancang dan diterapkan.	- Area aman yang kosong harus dikunci secara fisik dan ditinjau secara berkala	- Termasuk dalam aktivitas no 4.2 prosedur SP05 - Termasuk dalam aktivitas no. 7 prosedur SP06
			- Menghindari pekerjaan tanpa pengawasan di area aman	Tidak digunakan dalam penelitian namun selama ini sudah ada kamera pengawas CCTV di setiap ruangan
			- Peralatan perekam fotografi, video, audio atau lainnya, seperti kamera di perangkat mobile dilarang, kecuali telah mendapat izin resmi.	Termasuk dalam KJ03 Kebijakan Pengendalian Akses Fisik Fasilitas Teknologi Informasi
10	*11.2.8 Unattended user equipment*	Kontrol untuk memastikan bahwa peralatan yang tidak diawasi memiliki perlindungan yang tepat.	- Pengguna disarankan untuk menghentikan sesi aktif saat selesai menggunakan	Termasuk dalam aktivitas no. 6 prosedur SP04
			- Pengguna disarankan	Termasuk dalam aktivitas no. 6 prosedur SP04

No	Kontrol ISO 27002:2013	Kontrol Obyektif	Deskripsi Aktivitas Kontrol	Keterkaitan dengan SOP
			untuk log-off dari aplikasi/layanan jaringan bila tidak dibutuhkan	
			- Mengamankan komputer denngan kunci atau kontrol yang setara	Termasuk dalam aktivitas no. 7 prosedur SP06
11	*11.2.9 Clear desk and clear screen policy*	Kontrol untuk memastikan bahwa kebijakan meja kerja bebas dari kertas yang berisi informasi rahasia dan media penyimpanan yang mudah dipindahkan. Kebijakan layar yang bebas dari informasi rahasia pada fasilitas pengolahan informasi harus diadopsi.	- Melindungi informasi bisnis yang kritis dan sensitif	Termasuk dalam aktivitas no.4 prosedur SPO06
			- Komputer dan terminal harus dibiarkan mati /dilindungi dengan mekanisme penguncian	- Termasuk dalam aktivitas no. 6 prosedur SP06 - Termasuk dalam aktivitas no. 7 prosedur SP06

LAMPIRAN H– HASIL VALIDASI

Berikut adalah Surat Validasi berupa konfirmasi yang telah disetujuai oleh Kepala Instalasi Pengelola Data Elektronik Rumah Sakit Dokter Moewardi



SURAT VERIFIKASI
Kesesuaian Penggalian Kondisi Saat ini

Dengan hormat,

Saya yang bertanda tangan dibawah ini :

Nama : Nimas Nawangsih
NRP : 5213100100
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember, Surabaya

Dengan ini menyatakan permohonan verifikasi kepada Kepala Instalasi Perencanaan Data Elektronik atas kesesuaian hasil penggalian kondisi saat ini Aplikasi SIMRS berdasarkan metode OCTAVE yaitu :

1. Hasil identifikasi aset informasi yang berhubungan dengan Aplikasi SIMRS.
2. Hasil identifikasi aset informasi kritis yang berhubungan dengan Aplikasi SIMRS.
3. Hasil identifikasi kebutuhan keamanan aset informasi kritis yang berhubungan dengan Aplikasi SIMRS.
4. Hasil identifikasi ancaman aset informasi kritis yang berhubungan dengan Aplikasi SIMRS.
5. Hasil identifikasi praktik keamanan yang telah dilakukan Rumah Sakit.
6. Hasil identifikasi kelemahan dari aspek organisasi saat ini.
7. Hasil identifikasi kerentanan teknologi yang telah diimplementasikan saat ini.

telah sesuai dengan kondisi sesungguhnya yang ada di Rumah Sakit Dr. Moewardi.

Verifikasi ini dilakukan sebagai bagian dari metode penelitian mengenai *Pembuatan Standar Operasional Prosedur Kontrol Akses Logikal dan Fisikal Aplikasi SIMRS Rumah Sakit Dr.Moewardi* yang sedang dilakukan oleh peneliti.

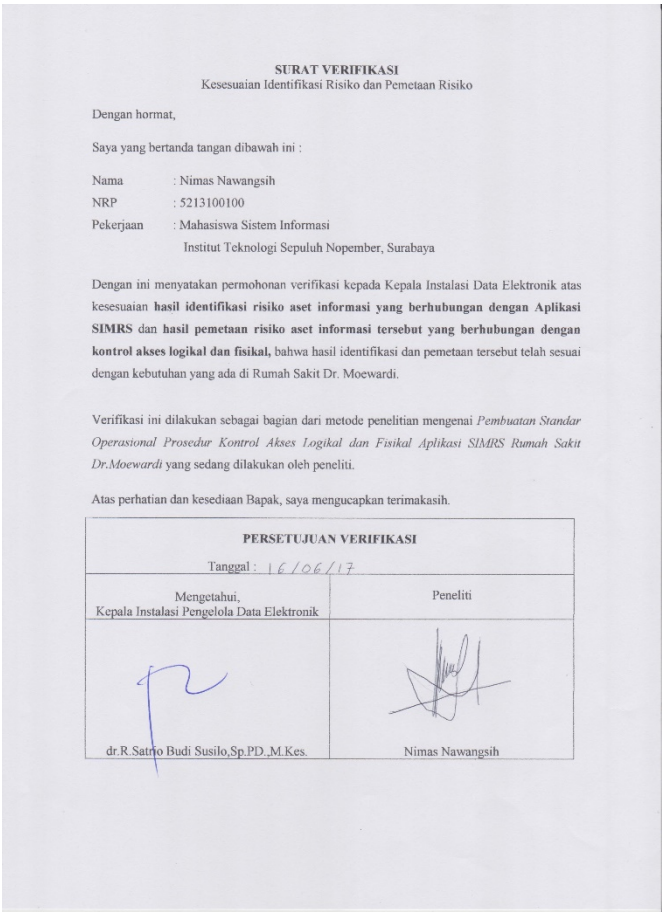
Atas perhatian dan kesediaan Bapak, saya mengucapkan terimakasih.

PERSETUJUAN VERIFIKASI

Tanggal : 16/06/17

Mengetahui, Kepala Instalasi Pengelola Data Elektronik	Peneliti
dr.R.Satrio Budi Susilo,Sp.PD.,M.Kes.	Nimas Nawangsih

Lampiran J. 1 Konfirmasi Penggalian Kondisi Saat Ini



SURAT VERIFIKASI
Kesesuaian Identifikasi Risiko dan Pemetaan Risiko

Dengan hormat,

Saya yang bertanda tangan dibawah ini :

Nama : Nimas Nawangsih
NRP : 5213100100
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember, Surabaya

Dengan ini menyatakan permohonan verifikasi kepada Kepala Instalasi Data Elektronik atas kesesuaian **hasil identifikasi risiko aset informasi yang berhubungan dengan Aplikasi SIMRS** dan **hasil pemetaan risiko aset informasi tersebut yang berhubungan dengan kontrol akses logikal dan fisikal,** bahwa hasil identifikasi dan pemetaan tersebut telah sesuai dengan kebutuhan yang ada di Rumah Sakit Dr. Moewardi.

Verifikasi ini dilakukan sebagai bagian dari metode penelitian mengenai *Pembuatan Standar Operasional Prosedur Kontrol Akses Logikal dan Fisikal Aplikasi SIMRS Rumah Sakit Dr.Moewardi* yang sedang dilakukan oleh peneliti.

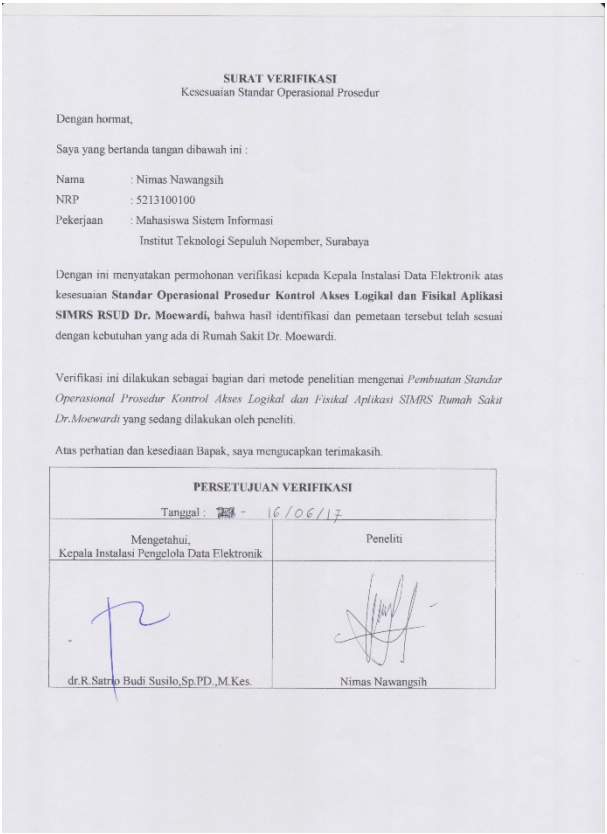
Atas perhatian dan kesediaan Bapak, saya mengucapkan terimakasih.

PERSETUJUAN VERIFIKASI

Tanggal : 16/06/17

Mengetahui, Kepala Instalasi Pengelola Data Elektronik	Peneliti
dr.R.Satrio Budi Susilo,Sp.PD.,M.Kes.	Nimas Nawangsih

Lampiran J. 2 Konfirmasi Penggalian Risiko dan Pemetaan Risiko Akses *Logical* dan *Physical*



SURAT VERIFIKASI
Kesesuaian Standar Operasional Prosedur

Dengan hormat,

Saya yang bertanda tangan dibawah ini :

Nama : Nimas Nawangsih
NRP : 5213100100
Pekerjaan : Mahasiswa Sistem Informasi
Institut Teknologi Sepuluh Nopember, Surabaya

Dengan ini menyatakan permohonan verifikasi kepada Kepala Instalasi Data Elektronik atas kesesuaian **Standar Operasional Prosedur Kontrol Akses Logikal dan Fisikal Aplikasi SIMRS RSUD Dr. Moewardi,** bahwa hasil identifikasi dan pemetaan tersebut telah sesuai dengan kebutuhan yang ada di Rumah Sakit Dr. Moewardi.

Verifikasi ini dilakukan sebagai bagian dari metode penelitian mengenai *Pembuatan Standar Operasional Prosedur Kontrol Akses Logikal dan Fisikal Aplikasi SIMRS Rumah Sakit Dr.Moewardi* yang sedang dilakukan oleh peneliti.

Atas perhatian dan kesediaan Bapak, saya mengucapkan terimakasih.

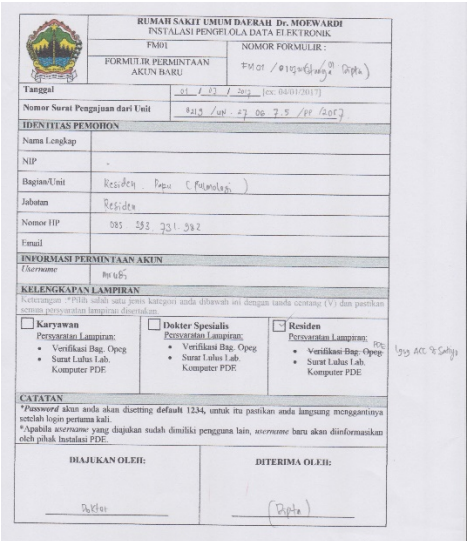
PERSETUJUAN VERIFIKASI

Tanggal : 16/06/17

Mengetahui, Kepala Instalasi Pengelola Data Elektronik	Peneliti
dr.R.Satrio Budi Susilo,Sp.PD.,M.Kes.	Nimas Nawangsih

Lampiran J. 3 Validasi Kesesuaian Hasil SOP yang Dihasilkan Dalam Penelitian

Berikut dibawah adalah hasil pengisian SOP yang dilakukan untuk keperluan validasi SOP.



RUMAH SAKIT UMUM DAERAH Dr. MOEWARDI
INSTALASI PENGELOLA DATA ELEKTRONIK

FM01 — FORMULIR PERMINTAAN AKUN BARU — NOMOR FORMULIR :

Tanggal : 01 / 02 / 2017 [ex: 04/01/2017]
Nomor Surat Pengajuan dari Unit : 0213 / UN. 27.06.7.5 / PP / 2017

IDENTITAS PEMOHON

Nama Lengkap	
NIP	-
Bagian/Unit	Residen Prog. Ilmu Kedokteran Forensik
Jabatan	Residen
Nomor HP	085 293 231 382
Email	

INFORMASI PERMINTAAN AKUN

Username	mygbs

KELENGKAPAN LAMPIRAN

Keterangan : *Pilih salah satu jenis kategori anda dibawah ini dengan tanda centang (V) dan pastikan semua persyaratan lampiran disertakan.

Karyawan	Dokter Spesialis	Residen
Persyaratan Lampiran:	Persyaratan Lampiran:	Persyaratan Lampiran:
• Verifikasi Bag. Opeg • Surat Lulus Lab. Komputer PDF	• Verifikasi Bag. Opeg • Surat Lulus Lab. Komputer PDF	• ~~Verifikasi Bag. Opeg~~ • Surat Lulus Lab. Komputer PDF

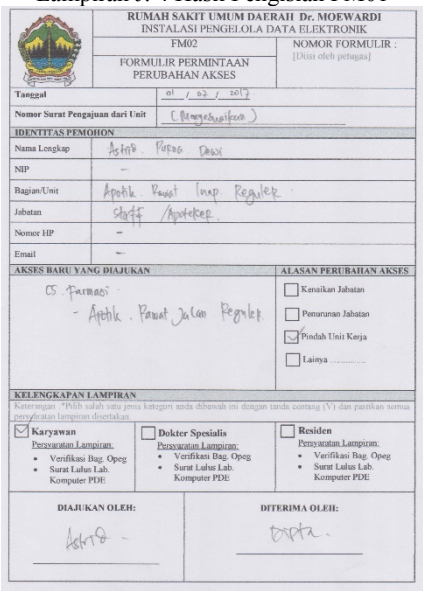
tgl ACC & Selesai

CATATAN

*Password akun anda akan disetting **default** 1234, untuk itu pastikan anda langsung menggantinya setelah login pertama kali.
*Apabila *username* yang diajukan sudah dimiliki pengguna lain, *username* baru akan diinformasikan oleh pihak Instalasi PDE.

DIAJUKAN OLEH:	DITERIMA OLEH:
Dokter	(Dipta)

Lampiran J. 4 Hasil Pengisian FM01



RUMAH SAKIT UMUM DAERAH Dr. MOEWARDI
INSTALASI PENGELOLA DATA ELEKTRONIK

FM02 — FORMULIR PERMINTAAN PERUBAHAN AKSES — NOMOR FORMULIR : [Diisi oleh petugas]

Tanggal : 01 / 02 / 2017
Nomor Surat Pengajuan dari Unit : (Manajemen Risiko)

IDENTITAS PEMOHON

Nama Lengkap	Astrid Puspa Dewi
NIP	-
Bagian/Unit	Apotik Pasat Jalan Reguler
Jabatan	Staff / Apotekep
Nomor HP	-
Email	-

AKSES BARU YANG DIAJUKAN	ALASAN PERUBAHAN AKSES
CS Farmasi - Apotik Pasat Jalan Reguler	☐ Kenaikan Jabatan ☐ Penurunan Jabatan ☑ Pindah Unit Kerja ☐ Lainya .....

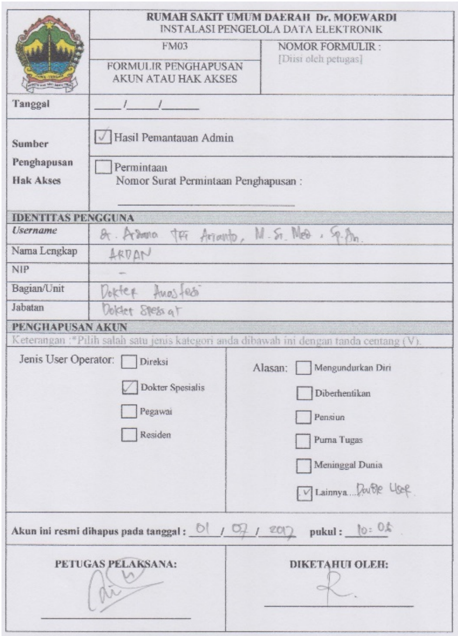
KELENGKAPAN LAMPIRAN

Keterangan : *Pilih salah satu jenis kategori anda dibawah ini dengan tanda centang (V) dan pastikan semua persyaratan lampiran disertakan.

☑ Karyawan	☐ Dokter Spesialis	☐ Residen
Persyaratan Lampiran:	Persyaratan Lampiran:	Persyaratan Lampiran:
• Verifikasi Bag. Opeg • Surat Lulus Lab. Komputer PDF	• Verifikasi Bag. Opeg • Surat Lulus Lab. Komputer PDF	• Verifikasi Bag. Opeg • Surat Lulus Lab. Komputer PDF

DIAJUKAN OLEH:	DITERIMA OLEH:
Astrid	Dipta

Lampiran J. 5 Hasil Pengisian FM02



	RUMAH SAKIT UMUM DAERAH Dr. MOEWARDI INSTALASI PENGELOLA DATA ELEKTRONIK	
	FM03 FORMULIR PENGHAPUSAN AKUN ATAU HAK AKSES	NOMOR FORMULIR : [Diisi oleh petugas]
Tanggal	____/____/____	
Sumber Penghapusan Hak Akses	☑ Hasil Pemantauan Admin	
	☐ Permintaan Nomor Surat Permintaan Penghapusan : ____________	

IDENTITAS PENGGUNA

Username	dr. Ardana Tri Arianto, M.Si. Med, Sp.An.
Nama Lengkap	ARDAN
NIP	–
Bagian/Unit	Dokter Anastesi
Jabatan	Dokter Spesialis

PENGHAPUSAN AKUN

Keterangan :*Pilih salah satu jenis kategori anda dibawah ini dengan tanda centang (V).

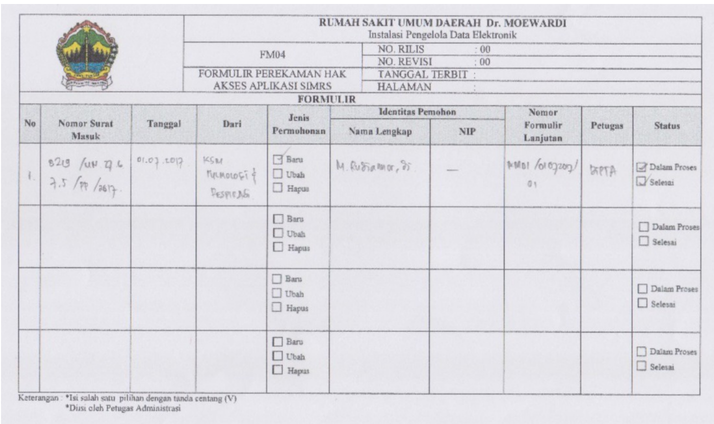
Jenis User Operator: ☐ Direksi ☑ Dokter Spesialis ☐ Pegawai ☐ Residen

Alasan: ☐ Mengundurkan Diri ☐ Diberhentikan ☐ Pensiun ☐ Purna Tugas ☐ Meninggal Dunia ☑ Lainnya... Double User

Akun ini resmi dihapus pada tanggal : 01 / 07 / 2017 **pukul :** 10:05

PETUGAS PELAKSANA:	**DIKETAHUI OLEH:**
[signature]	[signature]

Lampiran J. 6 Hasil Pengisian FM03



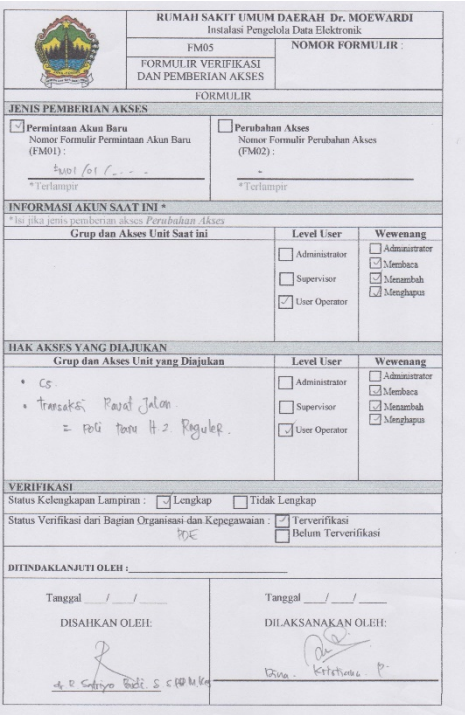
	RUMAH SAKIT UMUM DAERAH Dr. MOEWARDI Instalasi Pengelola Data Elektronik	
	FM04	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PEREKAMAN HAK AKSES APLIKASI SIMRS	TANGGAL TERBIT : HALAMAN :

FORMULIR

No	Nomor Surat Masuk	Tanggal	Dari	Jenis Permohonan	Identitas Pemohon: Nama Lengkap	Identitas Pemohon: NIP	Nomor Formulir Lanjutan	Petugas	Status
1.	8213 /UM.02.6 7.5/TT/2017	01.07.2017	KSM Pulmonologi & Respirasi	☑ Baru ☐ Ubah ☐ Hapus	M. Rudiamor, dr.	–	FM01/01072017/01	IPDE	☑ Dalam Proses ☑ Selesai
				☐ Baru ☐ Ubah ☐ Hapus					☐ Dalam Proses ☐ Selesai
				☐ Baru ☐ Ubah ☐ Hapus					☐ Dalam Proses ☐ Selesai
				☐ Baru ☐ Ubah ☐ Hapus					☐ Dalam Proses ☐ Selesai

Keterangan : *Isi salah satu pilihan dengan tanda centang (V)
*Diisi oleh Petugas Administrasi

Lampiran J. 7 Hasil Pengisian FM04



RUMAH SAKIT UMUM DAERAH Dr. MOEWARDI
Instalasi Pengelola Data Elektronik

FM05 | NOMOR FORMULIR :

FORMULIR VERIFIKASI DAN PEMBERIAN AKSES

FORMULIR

JENIS PEMBERIAN AKSES

☑ **Permintaan Akun Baru**
Nomor Formulir Permintaan Akun Baru (FM01) : tmd1/01/...
*Terlampir

☐ **Perubahan Akses**
Nomor Formulir Perubahan Akses (FM02) : -
*Terlampir

INFORMASI AKUN SAAT INI *
*Isi jika jenis pemberian akses *Perubahan Akses*

Grup dan Akses Unit Saat ini	Level User	Wewenang
	☐ Administrator ☐ Supervisor ☑ User Operator	☐ Administrator ☑ Membaca ☑ Menambah ☑ Menghapus

HAK AKSES YANG DIAJUKAN

Grup dan Akses Unit yang Diajukan	Level User	Wewenang
• CS • Transaksi Rawat Jalan = Poli Umum H2 Reguler.	☐ Administrator ☐ Supervisor ☑ User Operator	☐ Administrator ☑ Membaca ☑ Menambah ☑ Menghapus

VERIFIKASI

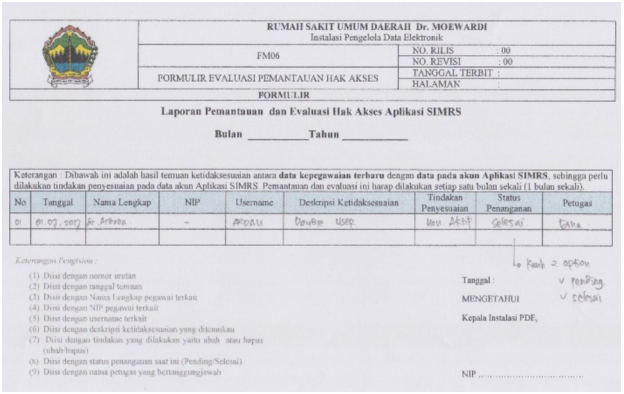
Status Kelengkapan Lampiran : ☑ Lengkap ☐ Tidak Lengkap

Status Verifikasi dari Bagian Organisasi dan Kepegawaian : ☑ Terverifikasi ☐ Belum Terverifikasi
PDE

DITINDAKLANJUTI OLEH : _____

Tanggal ___/___/____	Tanggal ___/___/____
DISAHKAN OLEH:	DILAKSANAKAN OLEH:
dr. R. Satrio Budi. S. SpBUK	Dina. Kepala Instalasi PDE

Lampiran J. 8 Hasil Pengisian FM05



RUMAH SAKIT UMUM DAERAH Dr. MOEWARDI
Instalasi Pengelola Data Elektronik

FM06 | NO. KILIS : 00 | NO. REVISI : 00 | TANGGAL TERBIT : | HALAMAN :

FORMULIR EVALUASI PEMANTAUAN HAK AKSES

FORMULIR

Laporan Pemantauan dan Evaluasi Hak Akses Aplikasi SIMRS

Bulan _____ **Tahun** _____

Keterangan : Dibawah ini adalah hasil temuan ketidaksesuaian antara **data kepegawaian terbaru** dengan **data pada akun Aplikasi SIMRS**, sehingga perlu dilakukan tindakan penyesuaian pada data akun Aplikasi SIMRS. Pemantauan dan evaluasi ini harap dilakukan setiap satu bulan sekali (1 bulan sekali).

No	Tanggal	Nama Lengkap	NIP	Username	Deskripsi Ketidaksesuaian	Tindakan Penyesuaian	Status Penanganan	Petugas
01	01.02.2017	dr Antoni	-	Antoni	Duplikat User	Non Aktif	Selesai	Dina

Isi pada 2 option

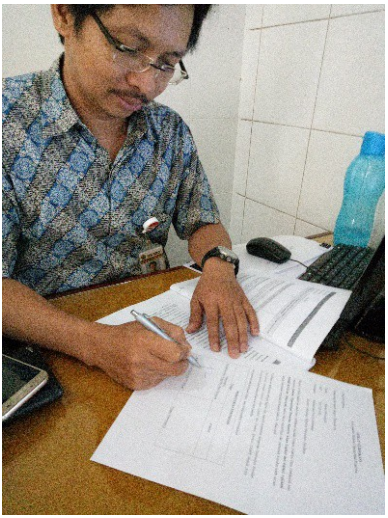
Keterangan Pengisian :
(1) Diisi dengan nomor urutan
(2) Diisi dengan tanggal temuan
(3) Diisi dengan Nama Lengkap pegawai terkait
(4) Diisi dengan NIP pegawai terkait
(5) Diisi dengan username terkait
(6) Diisi dengan deskripsi ketidaksesuaian yang ditemukan
(7) Diisi dengan tindakan yang dilakukan yaitu nhib atau hapus (nhib/hapus)
(8) Diisi dengan status penanganan saat ini (Pending/Selesai)
(9) Diisi dengan nama petugas yang bertanggungjawab

Tanggal : v pending / v selesai
MENGETAHUI
Kepala Instalasi PDE,

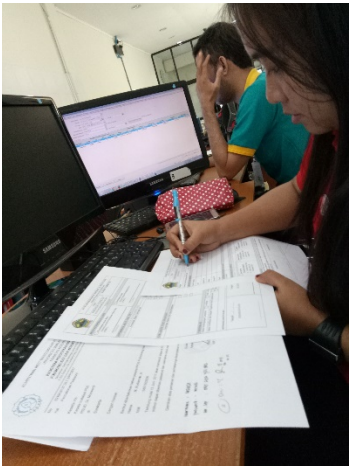
NIP .....

Lampiran J. 9 Hasil Pengisian FM06

LAMPIRAN I – DOKUMENTASI PENELITIAN



Gambar Dokumentasi . 1 Proses Validasi SOP oleh Kepala Instalasi Pengelola Data Elektronik



Gambar Dokumentasi . 2 Proses Simulasi SOP oleh salah satu admin Aplikasi SIMRS