ANALISIS RISIKO DAN PERANCANGAN KONTROL KEAMANAN INFORMASI PADA SISTEM INFORMASI MANAJEMEN RUMAH SAKIT MODUL ASET MENGGUNAKAN METODE OCTAVE ALLEGRO (STUDI KASUS: RUMAH SAKIT KHUSUS IBU DAN ANAK BANDUNG)

RISK ANALYSIS AND INFORMATION SECURITY CONTROL DESIGN IN HOSPITAL MANAGEMENT INFORMATION SYSTEM ASSET MODULE USING OCTAVE ALLEGRO METHOD (CASE STUDY: SPECIAL HOSPITAL FOR MOTHER AND CHILDREN OF BANDUNG)

Daffa Naufal Mauluddani, Dr. ir. Lukman Abdurrahman, MIS[2], Iqbal Santosa, S.Si, MTI.[3]
[1]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[2]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]daffanaufal@student.telkomuniversity.ac.id, [2]abdural@telkomuniversity.ac.id, [3]iqbals@telkomuniversity.ac.id.

ABSTRAK

Rumah Sakit Khusus Ibu dan Anak (RSKIA) Kota Bandung adalah rumah sakit milik pemerintah yang telah menggunakan Sistem Informasi Manajemen Rumah Sakit (SIMRS) sejak tahun 2014. Semenjak awal pengimplementasian Sistem Informasi Manajemen Rumah Sakit (SIMRS) belum melakukan pengukuran risiko dan manajemen risiko yang akan muncul pada SIMRS tersebut, kesadaran akan pentingnya keamanan sistem informasi beserta aset-asetnya bagi suatu perusahaan atau organisasi dan dampak yang mungkin timbul akibat kerusakan sistem informasi tampaknya masih belum mendapatkan perhatian bagi sebagaian besar di perusahaan. Penilaian risiko merupakan bagian dari manajemen risiko sistem informasi dan risiko atas ancaman tersebut harus dapat dikelola sehingga dampak atas risiko tersebut dapat diminimalisir. Pada penelitian ini metode Octave Allegro digunakan untuk menilai besar ancaman dari sebuah risiko serta menggunakan NIST SP 800-53 sebagai rekomendasi perancangan kontrol terhadap risiko yang ditimbulkan khususnya terkait dengan asset Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang dimiliki Rumah Sakit Khusus Ibu dan Anak Kota Bandung.

Kata Kunci: Sistem Informasi Manajemen Rumah Sakit, *OCTAVE Allegro,* NIST SP 800-53, RSKIA

ABSTRACT

The Special Hospital for Mother and Children (RSKIA) in Bandung City is a government-owned hospital that has been using the Hospital Management Information System (SIMRS) since 2014. Since the beginning of implementing the Hospital Management Information System (SIMRS), it has not carried out the measurement and risk management that will appears in the SIMRS, awareness of the importance of information systems and their assets for a company or organization and the impact that may arise due to damage to the information system has not yet received attention for most of the company. Risk assessment is part of information system risk management and the risk of these threats must have an impact so that the impact of these risks can be reduced. In this study, the Octave Allegro method is used to assess the threat of a risk and uses NIST SP 800-53 as a design recommendation for the risks posed, especially those related to the Hospital Management Information System (SIMRS) assets owned by the Special Hospital for Mother and Children in Bandung.

Keywords: Hospital Management Information System, OCTAVE Allegro, NIST SP 800-53, RSKIA

1. PENDAHULUAN

Penerapan teknologi informasi saat ini sudah menjadi kebutuhan dan tuntutan pada setiap instansi penyelenggara pelayanan publik salah satunya adalah dalam bidang kesehatan saat ini khususnya pada instansi rumah sakit merupakan suatu hal yang penting dan tidak dapat dipisahkan dari suatu proses bisnisnya. Namun, selama penggunaan dan implementasi teknologi tersebut tidak menutup kemungkinan dapat menimbulkan berbagai macam risiko yang dapat mengancam keberlangsungan proses bisnis dan tujuan pencapainnya. Salah satu langkah awal yang dilakukan di rumah sakit untuk mengelola risiko-risiko ini yakni melakukan upaya pengukuran terhadap risiko teknologi informasi (nilai risiko).

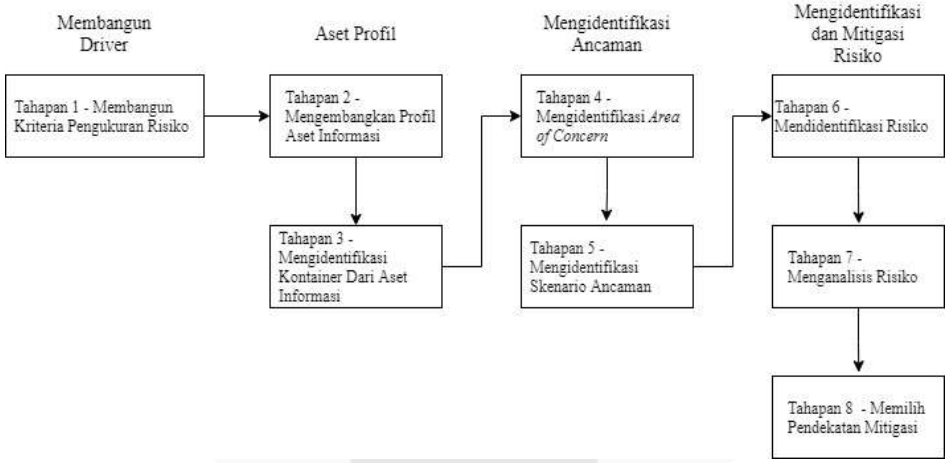
Rumah Sakit Khusus Ibu dan Anak Kota Bandung (RSKIA), merupakan sebuah instansi dalam bidang kesehatan yang pelayanannya disediakan oleh dokter (umum dan spesialis), perawat dan tenaga ahli kesehatan lainnya. Dalam menjalankan proses bisnisnya, RSKIA menggunakan sistem informasi yang ter-integrasi, akan tetapi rumah sakit belum pernah melakukan pengukuran risiko terhadap teknologi informasinya dan belum menerapkan manajemen risiko untuk meminimalisir risiko-risiko yang mungkin terjadi di masa yang akan datang.

Pengukuran terhadap sistem tersebut dimaksudkan agar berbagai risiko pada teknologi informasi di rumah sakit dapat diminimalisir dan diatasi. Selanjutnya, setelah dilakukan pengukuran maka akan diketahui dampak besarnya ancaman dan kerentanan dari setiap informasi data yang dinilai kritis, sehingga akan diterapkan kontrol yang tepat dengan memprioritaskan informasi risiko yang paling besar. Salah satu metode yang digunakan untuk menilai dan menganalisis risiko pada suatu teknologi informasi adalah menggunakan OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evaluation). Dengan begitu, RSKIA Kota Bandung dapat terus melakukan pengembangan terhadap manajemen sumber daya manusia dan melakukan peningkatan kualitas pelayanan kepada pasien.

Hasil analisis penilaian risiko keamanan informasi dan manajemen rumah sakit bagi RSKIA dapat digunakan untuk mengetahui risiko-risiko yang terjadi sehingga dapat dijadikan panduan untuk menyempurnakan penerapan sistem informasi secara keseluruhan.

2. METODE PENELITIAN OCTAVE ALLEGRO

OCTAVE Allegro merupakan metode yang kolaboratif yang disederhanakan dengan berfokus pada asset informasi. OCTAVE Allegro terdiri dari delapan tahapan dan empat fase :



Gambar 1 Langkah-Langkah OCTAVE Allegro
(Sumber: Caralli, Stevens, Young, & Wilson, 2007)

Tahapan 1 – Membangun Kriteria Pengukuran Risiko

Pada tahapan pertama, *organizational driver* yang akan digunakan untuk mengevaluasi akibat dari sebuah risiko terhadap misi dan tujuan bisnis perusahaan diidentifikasi. Kriteria pengukuran risiko digunakan untuk mengevaluasi akibat masing-masing area dan memprioritaskannya dan membuat ukuran kuantitatif pada *risk measurement criteria*.

Tahapan 2 – Mengembangkan Profil Aset Informasi

Membangun profil aset informasi atas aset-aset perusahaan. Profil merupakan merupakan representasi dari aset informasi yang menggambarkan fitur, kualitas, karakteristik dan nilai yang unik.

Tahapan 3 – Mengidentifikasi Kontainer dari Aset Informasi

Kontainer adalah tempat dimana aset informasi disimpan, dikirim, dan diproses, dalam tahapan ketiga

seluruh kontainer baik internal maupun eksternal diidentifikasi.

Tahapan 4 – Mengidentifikasi *Area of Concern*

Mengidentifikasi area perhatian tentang kondisi atau situasi yang dapat mengancam aset dan informasi kritis perusahaan.

Tahapan 5 – Mengidentifikasi kenario Ancaman

Mengindentifikasi area-area yang menjadi perhatian pada langkah sebelumnya, dengan memperjelas ancaman dengan mengidentifikasi *threat scenario* dengan melengkapi *information asset risk worksheet.*

Tahapan 6 – Mengidentifikasi Risiko

Menentukan bagaimana *threat scenario* yang telah dibuat pada *Information Asset Risk Worksheet* berdampak pada organisasi.

Tahapan 7 – Menganalisa Risiko

Pengukuran kuantitatif sederhana untuk organisasi yang terkena dampak dari *threat* dihitung. Nilai risiko relative didapatkan dengan cara mempertimbangkan sejauh mana konsekuensi atas dampak risiko terhadap berbagai *impact area*.

Tahapan 8 – Memilih Pendekatan Mitigasi

Dalam tahapan terakhir dari OCTAVE Allegro, organisasi menentukan risiko yang memerlukan mitigasi dan mengembangkan strategi untuk mengurangi risiko tersebut.

3. RUMAH SAKIT KHUSUS IBU DAN ANAK KOTA BANDUNG

Pada bab ini menjelaskan tentang visi – misi RSKIA Kota Bandung dan menjelaskan tentang Sistem Informasi Manajemen Rumah Sakit yang menjadi objek penelitian kali ini.

3.1 Visi, Misi dan Nilai RSKIA Kota Bandung

1. **Visi**

   Menjadi Rumah Sakit rujukan pelayanan kesehatan Ibu dan Anak yang Unggul, Mudah dan Nyaman.

2. **Misi**
   a. Menyelenggarakan pelayanan kesehatan yang lengkap, terpadu, unggul, dan bermutu kelas dunia
   b. Membangun kolaborasi dan jejaring dengan berbagai pihak
   c. Mengembangkan sumber daya manusia yang profesional, berakhlak mulian dan berdaya saing tinggi
3. **Nilai – nilai RSKIA**
   a. Ramah : Komunikasi yang baik dengan penuh kasih antara petugas dan pelanggan.
   b. Sigap : Cepat tanggap dalam memberikan pelayanan dan menyelesaikan tugas.
   c. Kreatif : Berinovasi dalam menciptakan sesuatu yang baru untuk memberikan pelayanan yang baik.
   d. Integritas : Komitmen untuk konsisten dalam memberikan pelayanan sesuai dengan nilai, etika dan norma yang berlaku
   e. Aman : Melaksanakan tugas secara profesional dengan mengutamakan keselamatan pasien, keselamatan kerja dan akunbilitas

3.2 Sistem Informasi Manajemen Rumah Sakit

SIMRS dapat didefinisikan sebagai sistem yang dapat mengintegrasikan seluruh network dari dalam dan luar rumah sakit. SIMRS juga dapat dimengerti sebagai aplikasi sistem *enterprise* pengelolaan dan membantu meningkatkan pelayanan rumah sakit. Informasi yang diintegrasikan berupa informasi mengenai sistem rekam medis elektronik, informasi laboratorium, farmasi, penagihan, pembuatan laporan, keperawatan, radiologi dan juga informasi mengenai asset rumah sakit . Adapun selain informasi yang sudah disebutkan, SIMRS juga mengintegrasikan informasi berupa penggajian karyawan, ruang inap pasien, dan juga proses akuntansi.

4. TAHAPAN DAN ANALISIS

Data yang telah diperoleh akan diolah dan dianalisis. Analisa terdiri dari analisis identifikasi aset dan analisis risiko menggunakan. Berikut ini adalah tahapan dari penilaian risiko dengan menggunakan metode OCTAVE Allegro :

4.1 Tahapan 1, Membangung Kriteria Pengukuran Risiko

Tahapan pertama adalah melakukan identifikasi terhadap *organizational drivers* yang akan digunakan untuk mengevaluasi akibat masing-masing area kedalam *Risk Measurement Criteria Worksheet* dan akan diprioritaskan dari sebuah risiko yang ada di SIMRS yang telah ditentukan berdasarkan hasil dari

wawancara dengan narasumber. Berikut adalah tabel kriteria pengukuran risiko.

Tabel 1 *Risk Measurement Criteria*

Allegro Worksheet 1	**RISK MEASUREMENT CRITERIA – REPUTASI DAN KEPERCAYAAN PELANGGAN**		
Impact Area	Low	Medium	High
Reputasi	Reputasi perusahaan terkena dampak minimal : kecil atau tidak ada usaha sama sekali untuk pemulihan	Reputasi perusahaan terkena dampak sedang dan dibutuhkan usaha yang cukup untuk pemulihan	Reputasi perusahaan terkena dampak besar dan dibutuhkan usaha yang besar untuk pemulihan
Kepercayaan Pelanggan	Kepercayaan pelanggan terhadap perusahaan tinggi karena tidak ada risiko dalam aset perusahaan	Kepercayaan pelanggan terhadap perusahaan cukup karena rendahnya risiko dalam aset perusahaan	Kepercayaan pelanggan terhadap perusahaan hampir tidak ada karena tingginya risiko dalam aset perusahaan

4.2 Tahapan 2, Mengembangkan Profil Aset informasi

Langkah ini terdiri dari delapan kegiatan, dimulai dengan mengidentifikasi informasi aset, kemudian melakukan penilaian risiko terstruktur pada aset kritis. Kegiatan tiga dan empat berkaitan dengan pengumpulan informasi tentang aset penting, diikuti dengan mendokumentasikan alasan pemilihan aset tersebut. Kegiatan lima dan enam terdiri dari menggambarkan aset informasi kritis, diikuti oleh identifikasi kepemilikan aset. Kegiatan tujuh adalah mengisi persyaratan keamanan untuk kerahasiaan, integritas, dan ketersediaan. Kegiatan delapan adalah mengidentifikasi persyaratan keamanan mana yang paling penting untuk aset.

Tabel 2 *Critical Information Asset Profile*

Allegro Worksheet 8a	**CRITICAL INFORMATION ASSET PROFILE**	
Critical Asset	**Rationale for Selection**	**Description**
What is the critical information asset?	*Why is this information asset important to the organization?*	*What is the agreed-upon description of this information asset?*
Data User	Memastikan bahwa user yang melakukan login kedalam SIMRS adalah user yang sah	Berisi tentang nama pegawai, NIP, username, password serta hak ases untuk menggunakan aplikasi SIMRS
Owner(s)		
Pengelola SIMRS		
Security Requirements		
What are the security requirements for this information asset?		

Confidentiality	Only authorized personnel can view this information asset, as follows:	Pengelola SIMRS
Integrity	Only authorized personnel can modify this information asset, as follows:	Pengelola SIMRS
Availability	This asset must be available for these personnel to do their jobs, as follows	Pegawai dan Pengelola SIMRS
	This asset must be available for 24 hours, 7 days/week.	
Most Important Security Requirement		
What is the most important security requirement for this information asset?		
[] Confidentiality	[V] Integrity	[] Availability

4.3 Tahapan 3, Mengidentifikasi Kontainer dari Aset Informasi

Tahapan ketiga adalah mengidentifikasi dari setiap aset kontainer yang merupakan tempat aset di simpan dan di proses, baik internal maupun eksternal. Di dalam kontainer ini terbagi menadi 3 kategori yaitu, *Technical* Sebuah perangkat keras, perangkat lunak atau sistem pada kontainer tersebut baik internal maupun eksternal, *Physical* Lokasi fisik atau dokumen dari kontainer tersebut disimpan baik internal maupun eksternal, dan *People* Pelaku yang memiliki kontrol terhadap aset informasi ini baik internal maupun eksternal.

Tabel 3 *Information Asset Risk Environment Map (Technical)*

Allegro Worksheet 9a - Data User	**INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)**
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Web server dan Database server (Perangkat keras yang digunakan sebagai tempat penyimpanan pusat data dari SIMRS)	Pengelola SIMRS
2. Jaringan Internal (LAN) (Jaringan nirkabel internal yang berfungsi untuk menghubungkan antara Database dengan Komputer dan Laptop)	Pengelola SIMRS
3. Komputer dan Laptop (Perangkat keras yang digunakan untuk mengakses aplikasi SIMRS)	Seksi Sarana dan Prasarana
EXTERNAL	

CONTAINER DESCRIPTION	OWNER(S)
1. Internet Service Provider	Vendor

Tabel 4 *Information Asset Risk Environment Map (Physical)*

Allegro Worksheet 9b - Data User	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	OWNER(S)
1. Form Registrasi User	Pengelola SIMRS

Tabel 5 Information Asset Risk Environment Map (People)

Allegro Worksheet 9c - Data User	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1. Staff pengelola SIMRS	Pengelola SIMRS

4.4 Tahapan 4, Mengidentifikasi Area Perhatian

Tahapan keempat adalah mengidentifikasi area perhatian tentang kondisi atau situasi yang dapat mengancam aset dan informasi kritis perusahaan, dengan melakukan *review* terhadap setiap container yang telah dibuat untuk melihat *Area of Concern* yang potensial dan mendokumentasikan bagaimana ancaman ini akan mempengaruhi *Security Requirements* yang telah ditetapkan untuk asset informasi

Tabel 6 *Area of Concern* pada Data User

No.	Area Of Concern - Data User
1	Adanya kesalahan dalam melakukan login
2	Data user dirubah oleh pihak yang tidak bertanggung jawab
3	Hilangnya data user
4	Pengguna yang tidak berwenang mencoba untuk masuk ke sistem

4.5 Tahapan 5, Mengidentifikasi Skenario Ancaman

Tahapan kelima adalah mengindentifikasi area-area yang menjadi perhatian pada langkah sebelumnya, dengan memperjelas ancaman dengan mengidentifikasi *threat scenario* dengan memberikan gambaran secara rinci terhadap *threat*, antara lain *actor, means, motives, outcome* dan *security requirement* serta menentukan *probability* dari *threat scenario* yang telah dibuat kedalam *information asset risk worksheet.*

Tabel 7 Mengidentifikasi Salah Satu Skenario Ancaman pada Data User

No	**Information Asset**	Data User
1	**Area of Concern**	Adanya kesalahan dalam melakukan login
	1- Actor	User
	2 - Means	User salah menginputkan username atau password

	3 - Motives	Tidak Disengaja
	4 - Outcome	[ ] Disclosure [ ] Modification [ ] Destruction [V] Interuption
	5 - Security Requirement	Melakukan validasi ulang
	6 - Probability	[ ] High [V] Medium [ ] Low

4.6 Tahapan 6, Mengidentifikasi Risiko

Tahapan keenam adalah menentukan bagaimana *threat scenario* yang telah dibuat pada *Information Asset Risk Worksheet* berdampak pada organisasi.

Tabel 8 Identifikasi RIsiko pada Data User

No	Area of Concern	7 - Consequence
1	Adanya kesalahan dalam melakukan login	User tidak bisa masuk ke dalam aplikasi SIMRS

4.7 Tahapan 7, Analisis Risiko

Tahapan ketujuh adalah mengevaluasi nilai kuantitatif organisasi yang terkena dampak dari risiko dengan cara mengukur skor risiko relatif terhadap setiap *Information Asset Worksheet.* Dengan melakukan *review* terhadap *risk measurement criteria* lalu dilanjutkan dengan menghitung nilai risiko relative yang dapat digunakan untuk menganalisis risiko dan membantu organisasi untuk menentukan strategi pendekatan mitigasi.

Tabel 9 *Priority Impact Area*

PRIORITY	IMPACT AREAS	Low (1)	Medium (2)	High (3)
5	Reputasi dan kepercayaan pelanggan	5	10	15
4	Keuangan	4	8	12
3	Produktivitas	3	6	9
1	Keselamatan dan kesehatan	1	2	3
2	Denda dan pinalti	2	4	6

Impact Area yang lebih prioritas akan memiliki nilai skor *priority* yang lebih besar. Perhitungan skor risiko ini dilakukan dengan mengalikan skor *priority* dengan *value*, setelah menghitung masing-masing *impact area*, kemudian semua skor dijumlahkan sehingga didapatkan skor risiko relative dan tahapan selanjutnya akan dilakukan pemilihan pendekatan mitigasi.

4.8 Tahapan 8, Memilih Pendekatan Mitigasi

Langkah terakhir dari proses OCTAVE Allegro adalah organisasi menentukan risiko yang akan dimitigasi berdasarkan risiko yang telah diidentifikasi dan dianalisa serta mengembangkan strategi mitigasi untuk risiko. Aktivitas pertama adalah melakukan klasifikasi pada setiap *area of concern* yang telah diidentifkasi dan dianalisis kedalam *Relative Risk Matrix* berdasarkan *Risk Score* (*Impact)* dan *Probability* kemudian hasilnya akan dilihat berdasarkan pool yang tertera dalam *Relative Risk Matrix* hal ini dilakukan untuk membantu dalam pengambilan keputusan terhadap mitigasi risiko tersebut.

Tabel 10 *Relative Risk Matrix*

RELATIVE RISK MATRIX			
Probability	***Risk Score (Impact)***		
	30 to 45	**16 to 29**	**0 to 15**
High	POOL 1	POOL 2	POOL 2
Medium	POOL 2	POOL 2	POOL 3
Low	POOL 3	POOL 3	POOL 4

Aktivitas kedua adalah menentukan pedekatan mitigasi yang sesuai berdasarkan penempatan kategori pada masing-masing pool.

Tabel 11 Pendekatan Mitigasi

Pool	***Mitigation Approach***
Pool 1	*Mitigate*
Pool 2	*Mitigate or Defer*
Pool 3	*Defer or Accept*
Pool 4	*Accept*

Aktivitas ketiga untuk semua *area of concern* yang telah diklasifikasi selanjutnya dibuatkan rencana mitigasi berdasarkan pendekatan mitigasi.

Tabel 12 Hasil Identifikasi dan Analisis Risiko dari semua *Area of Concern*

No	**Area of Concern**	**Probability**	**Risk Score (Impact)**	**POOL**	**Mitigation Approach**
1	Adanya kesalahan dalam melakukan login	Medium	15	Pool 3	Accept
2	Data user dirubah oleh pihak yang tidak bertanggung jawab	Medium	31	Pool 2	Mitigate
3	Hilangnya data user	Medium	39	Pool 2	Mitigate
4	Pengguna yang tidak berwenang mencoba untuk masuk ke sistem	Low	31	Pool 3	Defer
5	Adanya kesalahan dalam menginput data barang masuk	Medium	15	Pool 3	Accept
6	Pemalsuan data barang terhadap user	Low	31	Pool 3	Defer
7	Kerusakan pada data barang	High	39	Pool 1	Mitigate
8	Kesalahan dalam mencetak barcode	Low	15	Pool 4	Accept

9	Kerusakan data pada saat ingin mencetak barcode	High	31	Pool 1	Mitigate
10	Pemalsuan pada data barcode	Low	31	Pool 3	Defer

5. Kontrol dan Rekomendasi

5.1 Penetapan Kontrol

Kontrol risiko merupakan langkah-langkah yang dilakukan untuk mengendalikan sebuah risiko, sehingga dapat meminimalkan kejadian risiko yang berulang. NIST SP 800-53 merupakan standar yang berisi mengenai prosedur penilaian keamanan informasi yang komprehensif. Berikut pada Tabel 13 merupakan rekomendasi kontrol risiko :

Tabel 13 Penetapan Kontrol

No	Area of Concern	Rekomendasi	Deskripsi
1	Kerusakan pada data barang	*RA-5 Vulnerability Scanning* *CP-9 Information System Backup*	• Memindai kerentanan dalam sistem informasi dan aplikasi yang telah ditentukan oleh organisasi ketika terdapat kerentanan baru yang berpotensi mempengaruhi sistem atau aplikasi (RA-5) • Menggunakan alat dan teknik pemindaian kerentanan (RA-5) • Melakukan backup informasi tingkat sistem yang terdapat dalam sistem informasi (CP-9) • Melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan di lokasi penyimpanan (CP-9)
2	Kerusakan data pada saat ingin mencetak barcode		
3	Data user dirubah oleh pihak yang tidak bertanggung jawab		
4	Hilangnya data user		
5	Pemalsuan pada data barcode	*SI-4 Information System Monitoring*	• Sistem informasi mendeteksi serta melakukan pemantauan terhadap serangan yang potensial (logical attacks) sehingga dapat merubah isi data
6	Pemalsuan data barang terhadap user		
7	Pengguna yang tidak berwenang mencoba untuk masuk ke sistem	*IA-2 Identification and Authentication (Organizational Users)*	• Sistem informasi secara unik mengidentifikasi dan mengautentikasi pengguna organisasi (atau proses yang bertindak atas nama pengguna organisasi)

5.2 Aspek Rekomendasi

Setelah memberikan kontrol pada tahap diatas, selanjutnya memberikan rekomendasi untuk risiko yang belum mempunyai kontrol serta kontrol yang perlu diberikan peningkatan ke dalam 3 aspek, yaitu : *people, process* dan *technology.*

Tabel 14 Aspek Rekomendasi

No	Kontrol	Aspek	Rekomendasi
1	RA-5 *Vulnerability*	*People*	*Pelatihan Kemampuan SDM*

	Scanning	*Process*	*Pembahasan rancangan SPO Vulnerability Scanning*
		Technology	*Implementasi tools Vulnerability Scanning*
2	CP-9 *Information System Backup*	*Process*	1. Pembahasan revisi SPO *Backup Data* SIMRS 2. Pembahasan revisi SPO cara *Backup* data
3	SI-4 *Information System Monitoring*	*People*	*Pelatihan Kemampuan SDM*
		Process	*Pembahasan rancangan SPO Monitoring*
		Technology	*Implementasi fitur System Monitoring*
4	IA-2 *Identification and Authentication* (*Organizational Unit*)	*Process*	*Pembahasan rancangan SPO User SIMRS*

5.3 Rekomendasi Aspek *People*

Rekomendasi yang diberikan terhadap aspek *people* adalah melakukan pelatihan terhadap kemampuan dan kompetensi sumber daya manusia.

Tabel 15 Rekomendasi Aspek *People*

No	Kontrol	Judul Pelatihan	Deskripsi
1	RA-5 *Vulnerability Scanning*	Pelatihan menggunakan *tools Vulnerability Scanning*	Meningkatkan kemampuan dan kompetensi staff terhadap penggunaan *tools* maupun fitur *security* yang ada pada SIMRS
2	SI-4 *Information System Monitoring*	Pelatihan menggunakan fitur *System Monitoring*	

5.4 Rekomendasi Aspek *Process*

Rekomendasi yang diberikan terhadap aspek *process* adalah memberikan saran terhadap pembuatan SPO baru atau merevisi SPO yang sudah ada.

Tabel 16 Rekomendasi Aspek *Process*

No	Kontrol	Judul Pelatihan	Deskripsi
1	*RA-5 Vulnerability Scanning*	Pembahasan rancangan SPO *Vulnerability Scanning*	Membuat SPO baru tentang memindai dan memonitor kerentanan
2	*CP-9 Information System Backup*	1. Pembahasan revisi SPO *Backup Data* SIMRS 2. Pembahasan revisi SPO cara *Backup* data	Menambah isi dari SPO *backup data* SIMRS dan SPO cara *backup* data
3	*SI-4 Information System Monitoring*	Pembahasan rancangan SPO *Monitoring*	Membuat SPO baru tentang monitoring secara berkala
4	*IA-2 Identification and Authentication (Organizational Users*	Pembahasan rancangan SPO User SIMRS	Membuat SPO baru tentang hak akses user

5.5 Rekomendasi Aspek *Technology*

Rekomendasi yang diberikan terhadap aspek *technology* adalah pengajuan mengimplementasikan *tools vulnerability scanning* dan menambahkan fitur *Monitoring System* pada SIMRS Modul Aset.

Tabel 17 Rekomendasi Aspek *Technology*

No	Kontrol	Rekomendasi	Deskripsi
1	RA-5 *Vulnerability Scanning*	Implementasi Tools *Vulnerability Scanning*	Berfungsi sebagai pendeteksi celah keamanan
2	SI-4 *Information System Monitoring*	Menambahkan fitur *Monitoring System*	Berfungsi untuk melindungi data user dan data barcode

5.5.1 Komparasi *Tools : Vulnerability Scanning*

Komparasi *tools Vulnerability Scanning* berfungsi sebagai perbandingan antar *tools* yang direkomendasikan, terdapat tiga opsi yaitu, Qualys, Acunetix360, dan Intruder. Masing-masing opsi memiliki fitur yang berbeda. Selanjutnya akan dipilih sebagai rekomendasi kontrol dari RA-5 *Vulnerability Scanning* dan opsi yang dipilih dari kontrol tersebut adalah Qualys karena aplikasi yang berbasis layanan *cloud* sehingga tidak membutuhkan resource banyak dan terintegrasi terhadap *software development tools* untuk mengotomatiskan keamanan.

Tabel 18 Komparasi *Tools : Vulnerability Scanning*

Opsi	Fitur	Rekomendasi
Qualys	1. Terdapat 3 jenis scan yang disediakan yaitu : • Vulnerability checks • OWASP : *Web application security checks* • SCAP checks 2. Terintegrasi dengan Microsoft Azure, Amazon Web Service, dan Google Cloud serta *platform* CI/CD seperti Puppet, Jenkins, dan Bamboo 3. Menggunakan Six Sigma 4. Terdapat banyak fitur security didalam Qualys	Qualys karena aplikasi yang berbasis layanan *cloud* sehingga tidak membutuhkan resource banyak dan terintegrasi terhadap *software development tools* untuk mengotomatiskan keamanan
Acunetix 360	1. Memindai dan mendukung otomatis semua aplikasi web dan aplikasi web kompleks termasuk HTML5 dan JavaScript 2. Pemindai paling menyeluruh terhadap SQL injections, XSS, *misconfigurations, weak passwords* dan *exposed database* 3. Terintegrasi dengan layanan pihak ketiga seperti GitHub, GitLab, Azure, Jira Software, Bugzilla dan Mantis 4. Menggunakan teknologi Acusensor	
Intruder	1. Pemindaian terhadap *misconfigurations, missing*	

	patches, SQL Injenction dan cross-site scripting 2. Terintegrasi dengan pihak ketiga seperti Slack, Jira, Microsoft Teams, Zapier dan layanan Cloud 3. Otomatis IP dan DNS Tracking 4. Menggunakan *Two-Factor Authentication*	

5.5.2 Penambahan Fitur SIMRS : *System Monitoring*

System Monitoring berfungsi untuk memantau aktivitas user dalam menggunakan SIMRS Modul Aset. Berikut merupakan Tabel 19 yang berisikan fitur tambahan pada SIMRS Modul Aset : *System Monitoring*

Tabel 19 Penambahan Fitur SIMRS Modul Aset : *System Monitoring*

No	Fitur	Proses	Deskripsi
1	*User login*	Masuk kedalam aplikasi SIMRS dan menuju modul Aset	Mencatat informasi user (Nama dan NIP) ketika login kedalam SIMRS
2	*User logout*	Keluar dari aplikasi SIMRS	Mencatat informasi user (Nama dan NIP) ketika telah logout dari SIMRS
3	Alamat IP	Komputer/laptop yang digunakan oleh user	Mencatat alamat IP komputer ketika digunakan oleh user
4	Waktu *realtime*	User aktif menggunakan SIMRS	Mencatat waktu terhadap pemakaian SIMRS
5	Membuat, merubah dan menghapus data	Membuat data baru, merubah data, dan menghapus data	Mencatat kegiatan yang dilakukan oleh user

6. Penutup

6.1 Kesimpulan

Bedasarkan hasil penelitian dan analisis risiko yang dilakukan pada SIMRS Modul Aset, dapat disimpulkan :

1. Fase pertama dalam menganalisis risiko menggunakan metode OCTAVE Allegro adalah mengembangkan kriteria pengkuran risiko terdapat 5 *impact areas* yang menjadi indikator dalam penilian dan mitigasi risiko yang akan digunakan, yaitu *Reputation and Customer Confidence*, *Financial*, *Productivity*, *Safety and Health*, dan *Fines and Legal Pinalties*. Fase kedua membuat profil aset informasi dan mengidentifikasi informasi aset containner. Fase ketiga mengidentifikasi *area of concern* dan memperjelas ancaman dengan memberikan gambaran secara rinci terhadap *threat*, antara lain *actor*, *means*, *motives*, *outcome* dan *security requirement* serta menentukan *probability* dari *threat scenario* yang telah dibuat kedalam *information asset risk worksheet.* Fase keempat adalah mulai mengembangkan pendekatan mitigasi terhadap risiko yang telah diidentifikasi dan dianalisis.
2. Mitigasi risiko dilakukan berdasarkan hasil dari pool *Relative Risk Matrix* yang sudah didefinisikan sebelumnya. Terdapat dua jenis penanganan pada risiko yang diberikan, yaitu *mitigate* dan *defer*.

Risiko yang diberikan penanganan *mitigate* karena memiliki dampak level yang besar sehingga harus diberikan rekomendasi kontrol yang sesuai untuk mengurangi dampak yang terjadi dan risiko yang diberikan penanganan *defer* karena pihak RSKIA menagguhkan dampak dari risiko dikarenakan ingin melakukan evaluasi dan mengumpulkan informasi lainnya guna melakukan analisis tambahan.

3. Rekomendasi kontrol yang digunakan pada penelitian ini adalah berdasarkan NIST SP 800-53. Kontrol yang digunakan adalah RA-5 *Vulnerability Scanning,* CP-9 *Information System Backup,* SI-4 *Information System Monitoring,* IA-2 *Identification and Authentication (Organizational Users).*

6.2 Saran

Berikut saran yang dapat diberikan sebagai bahan pertimbangan untuk perbaikan dari penulis untuk penelitian selanjutnya terhadap SIMRS RSKIA adalah sebagai berikut :

1. Menjadikan analisis risiko ini sebagai referensi bahwa setiap aset informasi pasti memiliki potensi risiko serta pihak RSKIA menjadi lebih sadar akan kemungkinan risiko yang akan terjadi terhadap semua modul yang terdapat pada SIMRS.
2. Mengimplementasikan rekomendasi yang telah disarankan agar dampak serta kemungkinan terjadinya risiko dapat dapat diminimalisir.
3. Hasil analisis dapat dijadikan referensi terhadap penelitian selanjutnya ketika menggunakan atau menambahkan metode lain yang berkaitan agar penelitian selanjutnya cakupan terhadap manajemen risiko menjadi lebih luas.

Referensi

Alberts, C., & Stevens, J. (2010). Introduction to the eastern approach. *Pregnancy and Childbirth*, (August), 121–129.

Alberts, C. J., & Dorofee, A. J. (2001). *OCTAVE Criteria*, *Version 2.0*. (December), 116.

Agrawal, M., Campoe, A., & Pierce, E. (2014). *Information Security and IT Risk Management*.

Caralli, R. a R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. *Young*, (May), 1–113.

Cruz, S. T. (2007). Information security risk assessment. *Information Security Management Handbook*, *Sixth Edition*, pp. 243–250.

Hevner, Alan R., Salvatore T. March, Jinsoo Park, and Sudha Ram. "Design Science in Information Systems Research." MIS Quarterly 28, no. 1 (2004): 75-105.

Ikhsan, H., Jarti, N., Baja, J. T. U., Studi, P., Industri, T., & Allegro, O. (2019). *Analisis Risiko Keamanan Teknologi Informasi*. *2*(1), 31–41.

Informasi, T., & Padang, P. N. (2012). *PERBANDINGAN METODOLOGI EVALUASI RISIKO KEAMANAN INFORMASI OCTAVE-S DAN OCTAVE ALLEGRO*. 111–116.

Mamduh M, H. (2014). Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management. *Management Research Review*, 1–40.

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(1), 282–287.

NIST. (2013). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. *NIST SP-800-53 Ar4*, 400+.

Rachmaniah, M., & Mustafa, B. (2016). Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro. *Jurnal Pustakawan Indonesia*, *14*(1).

Saputra, R. R., Ambarwati, A., & Setiawan, E. (2020). Manajemen Risiko Teknologi Informasi Menggunakan Octave Allegro Pada Pt.Hd. *Jurnal Sains Dan Teknologi Industri*, *17*(1), 1.

Wulansari, A. (2013). *Universitas Indonesia Analisis Penilaian Risiko Keamanan Untuk Aset Informasi Pada Usaha Kecil Dan Menengah Bidang Program Studi Sistem Informasi Depok*. 1–8.

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security, Sixth Edition. In *Cengage Learning*.