ANALISIS RISIKO DAN PERANCANGAN KONTROL KEAMANAN INFORMASI PADA SISTEM INFORMASI MANAJEMEN RUMAH SAKIT MODUL BILLING 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 BILLING MODULE USING OCTAVE ALLEGRO METHOD (CASE STUDY: SPECIAL HOSPITAL FOR MOTHER AND CHILDREN OF BANDUNG)

Raden Ichsan Achmad Falach[1], Dr. ir. Lukman Abdurrahman, MIS[2], Iqbal Santoso, 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]ichsanachfal@student.telkomuniversity.ac.id, [2]abdural@telkomuniversity.ac.id,
[3]iqbals@telkomuniversity.ac.id.

ABSTRAK

Pada tugas akhir ini dijelaskan bahwa Rumah Sakit Khusus Ibu dan Anak (RSKIA) kota Bandung adalah rumah sakit yang dimiliki oleh pemerintah yang sudah menggunakan atau mengimplementasikan Sistem Informasi Manajemen Rumah Sakit (SIMRS) dari tahun 2014. Keamanan sistem informasi dan aset aset adalah hal yang paling penting pada sebuah organisasi atau perusahaan. Maka dari itu dilakukannya penilaian analisis risiko merupakan cara agar risiko yang ada pada sistem informasi rumah sakit dapat ditangani atau diminimalisir. Agar Rumah Sakit Khusus Ibu dan Anak (RSKIA) kota Bandung dapat terus meningkatkan kualitas pelayanan maka dilakukan analisis manajemen risiko keamanan informasi menggunakan metode OCTAVE Allegro untuk menilai besar nya risiko atau suatu ancaman. dan dari risiko yang didapat, akan diberikannya kontrol menggunakan NIST.SP.800-53.

Kata Kunci : Manajemen Risiko, OCTAVE Allegro, RSKIA, SIMRS, Rumah Sakit, NIST.SP.800-53

ABSTRACT

In this final project, it will be explained that the Special Hospital for mothers and children (RSKIA) in the city of Bandung is a hospital owned by the government that has used or implemented the Hospital Management Information System (SIMRS) from 2014. Security of information systems and asset assets is a matter of the most important in an organization or company. Therefore doing a risk analysis assessment is a way so that the risks that exist in the hospital information system can be handled or minimized. In order for the Special Hospital for Women and Children (RSKIA) in Bandung to continue to improve the quality of services, an information security risk management analysis is carried out using the OCTAVE Allegro *method to assess the size of a risk or a threat. and from the risks obtained, control will be given using NIST.SP.800-53.*

Keywords : Risk Management,OCTAVE Allegro, RSKIA, SIMRS, Hospital, NIST.SP.800-53

1. Pendahuluan

Penggunaan teknologi informasi dalam bidang kesehatan tepatnya pada instansi rumah sakit merupakan suatu hal yang sangat penting dan tidak dapat dipisahkan dari suatu proses bisnisnya. Akan tetapi, dalam penggunaan dan implementasi teknologi tersebut dapat memungkinkan adanya timbul berbagai risiko yang dapat mengancam proses bisnis dan tujuannya. Pengelolaan terhadap munculnya berbagai risiko ini adalah hal yang sangat perlu diperhatikan. Salah satu langkah awal yang dapat dilakukan di rumah sakit untuk mengelola risiko-risiko ini adalah melakukan pengukuran terhadap risiko teknologi informasi atau nilai risiko. Diperoleh regulasi dari peraturan Mentri Kesehatan (PERMENKES) Republik Indonesia No 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit yang menetapkan setiap rumah sakit melakukan, melaksanakan pengelolaan dan meningkatkan pengembangan SIMRS.

Rumah Sakit Khusus Ibu dan Anak Bandung (RSKIA), adalah sebuah instansi perawatan kesehatan yang pelayanannya disediakan oleh dokter (umum dan spesialis), perawat dan tenaga ahli kesehatan lainnya. Dalam menjalankan proses bisnisnya, RSKIA ini menggunakan sistem informasi terkomputerisasi, akan tetapi rumah sakit belum pernah melakukan pengukuran risiko terhadap teknologi informasinya dan belum menerapkan manajemen risiko. Untuk meminimalisisasi risiko-risiko yang mungkin terjadi pada masa yang akan datang, RSKIA Bandung perlu melakukan pengukuran terhadap sistem tersebut.

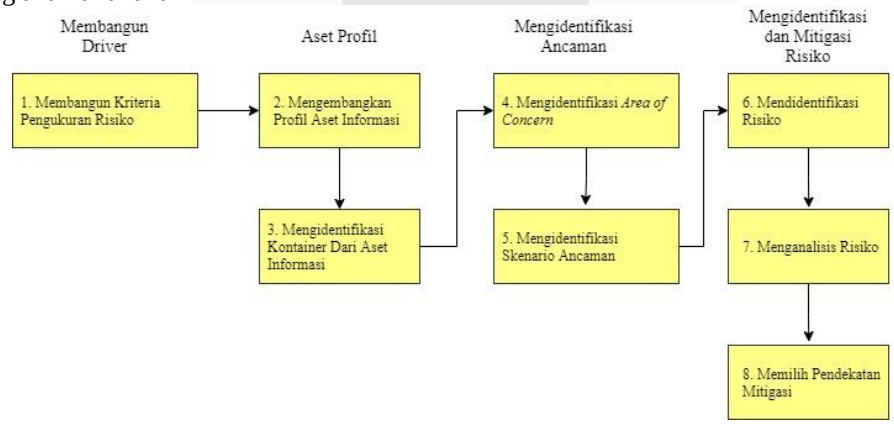
Pengukuran dilakukan agar berbagai risiko pada teknologi informasi rumah sakit dapat diminimilisir dan bisa teratasi. Setelah dilakukannya pengukuran maka kita akan mengetahui besarnya ancaman dari informasi data yang dinilai kritis, sehingga dapat diterapkan kontrol yang tepat dengan memprioritaskan informasi risiko yang paling kritis. Maka dengan begitu, RSKIA Bandung dapat terus melakukan pengembangan terhadap manajemen sumber daya manusia (MSDM) dan dapat terus melakukan peningkatan kualitas pelayanannya terhadap pasien.

Dalam penelitian ini diharapkan pihak RSKIA Kota Bandung dapat lebih bijak dalam mengelola informasi, termasuk didalamnya tentang "Keamanan Informasi". Informasi merupakan aset yang berharga untuk sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha, Oleh karena itu perlindungan terhadap informasi merupakan hal yang sangat mutlak harus diperhatikan secara *detail* oleh jajaran pemilik, manajemen, dan karyawan perusahaan yang bersangkutan. Keamanan informasi yang di maksud menyangkut kebijakan, prosedur, proses dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga dapat menyebabkan terjadinya kerugian bagi kelangsungan hidup suatu perusahaan atau organisasi. Evaluasi yang dilakukan pada RSKIA Bandung ini yang merujuk pada delapan area yang mencakup uji data, infrastruktur, hardware, software, jaringan, aplikasi, dan juga karyawan. Evaluasi terhadap sistem informasi manajeman rumah sakit (SIMRS) dapat diukur dengan metode Octave Allegro.

Pada penelitian ini, diharapkan dapat memperoleh hasil analisis penilaian risiko SIMRS bagi RSKIA yang dapat digunakan untuk mengetahui banyak nya risiko yang terjadi sehingga dapat dijadikan panduan untuk menyempurnakan penerapan sistem informasi secara keseluruhan. Lalu, penelitian juga dapat memberikan solusi dan risiko yang telah ditentukan untuk mengurangi terjadinya kerugian terhadap bidang teknologi informasi yang memungkinkan terjadi di RSKIA. Penelitian ini juga dapat dijadikan sebagai acuan untuk penelitian selanjutnya yang berkaitan dengan manajemen risiko SIMRS.

2. Metode Penelitian Octave Allegro

Pada saat menerapkan manajemen risiko, suatu perusahaan atau organisasi harus melakukan beberapa tahapan. Metode ini terdiri dari delapan tahapan, tiap tahap dirinci lagi menjadi beberapa aktivitaspenilaian risiko yang akan dilakukan



Gambar 1 Langkah Octave Allegro (Sumber : Caralli et al., 2007)

2.1 Tahapan 1 – Membangun Kriteria Pengukuran Risiko

Di dalam langkah ini terdapat dua aktivitas di awali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting

2.2 Tahapan 2 – Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi asset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi asset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk confidentiality, integrity dan availaibility. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi

2.3 Tahapan 3 – Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap container dari aaset informasi

2.4 Tahapan 4 – Mengidentifikasi *Area of Concern*

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi

2.5 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.*

2.6 Tahapan 6 – Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan

2.7 Tahapan 7 – Menganalisa Risiko

Aktivitas satu dimulai dengan melakukan review risk measurement criteria dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko

2.8 Tahapan 8 – Memilih Pendekatan Mitigasi

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasaarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi itu

3. Rumah Sakit Ibu dan Anak Kota Bandung (RSKIA)

Dijelaskan mengenai visi dan misi RSKIA Kota Bandung dan menjelaskan tentang Sistem Informasi Manejemen Rumah Sakit yang menjadi objek penelitian kali ini.

3.1 Visi, Misi dan Nilai RSKIA Kota Bandung

Mewujudkan Kota Bandung yang unggul, Nyaman, Sejahtera, dan Agamis, dengan misi membangun masyarakat yang humanis, agamis, dan berdaya saing. Pemerintah Kota Bandung dengan berlandaskan nilai nilai agama, dan budaya, berkomitmen memberikan kemudahan serta menjamin terselenggaranya pelayanan pendidikan, kesehatan, dan sosial yang bermutu, adil, dan merata.

3.2 Nilai Nilai RSKIA

Ramah, Sigap, Kreatif, Integritas, Aman.

3.3 Sistem Informasi Manajemen Rumah Sakit (SIMRS)

SIMRS dapat didefinisikan sebagai sistem yang dapat mengintegrasikan aliran dari suatu informasi dari dalam dan luar rumah sakit. SIMRS juga dapat dimengerti sebagai aplikasi sistem *enterprise* pengelolaan dan membantu meningkatkan pelayanan rumah sakit.

4. Tahapan dan Analisis

Data yang sudah di dapat akan diolah dan dianalisis. Identifikasi aset dan analisis risiko menggunakan metode Octave Allegro :

4.1 Tahapan 1 - Kriteria Pengukuran Risiko

Pada langkah ini, kita melalukan analisis untuk mengevaluasi akibat masing-masing area dan memprioritaskannya dari risiko yang ada pada SIMRS. Kriteria risiko dapat dlihat pada tabel berikut,

Tabel 1 Kriteria Penilaian Risiko

Allegro Worksheet 1	Kriteria Penilaian Risiko - Reputasi dan Kepercayaan Pelanggan		
Impact Area	Low	Medium	High
Reputasi	Reputasi perusahaan terkena dampak minimal : kecil atau tidak ada usahan sama sekali untuk pemulihan	Reputasi perusahaan rusak. Tidak lebih dari IDR50jt untuk biaya pemulihan dalam waktu 3 bulan	Reputasi perusahaan rusak parah. Lebih dari IDR50jt untuk biaya pemulihan dalam waktu 6 bulan
Kepercayaan Pelanggan	Kepercayaan pelanggan terhadap perusahaan tinggi karena tidak ada risiko dalam aset perusahaan	Kepercayaan pelanggan terhadap perusahaan rendah terhadap risiko dalam aset perusahaan	Kepercayaan pelanggan tidak ada terhadap perusahaan karena risiko yang ditimbulkan akan aset perusahaan

4.2 Tahapan 2 - Membangun profil aset informasi

Tahapan kedua adalah membangun profil aset informasi atas asset apa saja yang ada di perusahaan, profil setiap asset dikerjakaan dalam satu lembar kerja dan akan di identifikasi atau dicatat dalam *Critical Information Asset People Worksheet* yang disediakan oleh Octave Allegro yang dapat dilihat pada tabel berikut,

Tabel 2 *Critical Information Asset Profil*

Allegro Worksheet 8a	**CRITICAL INFORMATION ASSET PROFILE**	
Critical Asset *What is the critical information asset?*	**Rationale for Selection** *Why is this information asset important to the organization?*	**Description** *What is the agreed-upon description of this information asset?*
Data User	Dikarenakan user harus melakukan login terlebih dahulu untuk mengakses aplikasi SIMRS	Berisi tentang username , password dan hak akses untuk mengakses 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	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 dan Aset Informasi

Tahapan ketiga adalah mengidentifikasi setiap kontainer yang di simpan dan di proses, baik internal maupun eksternal. Di dalam container ini terbagi menjadi 3 kategori. yaitu *Technical, Physical, dan People* yang dapat dilihat pada tabel berikut,

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

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 (Phy)*

Allegro Worksheet 9a – 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 (Peo)*

Allegro Worksheet 9a – 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 ini berisikan tentang mengidentifikasi area perhatian kondisi atau situasi yang dapat mengancam asset informasi suatu perusahaan, dengan cara mengelompokkan aktivitas-aktivitas sebagai berikut yang dapat dilihat pada tabel dibawah,

Tabel 6 *Area Of Concern*

No.	Area Of Concern – Data User
1	Kesalahan dalam melakukan login
2	Penyalahgunaan hak akses user
3	Kerusakan pada data user

4.5 Tahapan 5 - Mengidentifikasi Skenario Ancaman

Pada tahapan ini yang kita lakukan adalah mengidentifikasi area yang menjadi perhatian pada langkah sebelumnya dengan cara memperjelas ancaman dengan melakukan identifikasi threat scenario dengan memeberikan 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 yang dapat dilihat pada tabel berikut,

Tabel 7 *Identifikasi Data Ancaman*

No	**Information Asset**	Data User
1	**Area of Concern**	Kesalahan dalam melakukan login
	(1) Actor	User
	(2) Means	Adanya kesalahan user dalam menginputkan username dan password
	(3) Motives	Tidak disengaja
	(4) Outcome	[] Disclosure [] Modification [] Destruction [V] Interuption
	(5) Security Requirement	Melakukan validasi pada data yang di inputkan
	(6) Probability	[] High [] Medium [V] Low

4.6 Tahapan 6 - Mengidentifikasi Risiko

Pada tahapan ini kita menentukan bagaimana *threat scenario* yang telah dibuat pada *Information Asset Risk Worksheet* berdampak pada organisasi yang dapat dilihat pada tabel berikut,

Tabel 8 Identifikasi Risiko

No	Area of Concern	7 – Consequences
1	Kesalahan dalam melakukan login	User tidak dapat masuk ke dalam aplikasi SIMRS

4.7 Tahapan 7 - Analisis Risiko

Pada tahapan ini adalah suatu organisasi yang terkena dampak dari risiko dengan cara mengukur jumlah/skor risiko relative terhadap setiap *Information Asset Worksheet* yang dapat dilihat pada tabel berikut,

Tabel 9 *Priority Impact*

PRIORITY	*IMPACT AREAS*	*LOW*	*MEDIUM*	*HIGH*
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

4.8 Tahapan 8 - Memilih Pendekatan Mitigasi

Pada langkah terakhir ini menurut OCTAVE ALLEGRO adalah menentukan risiko yang akan dimitigasi dari risiko yang telah diidentifikasi dan dianalisa lalu mengembangkan strategi mitigasi untuk risiko yang dapat dilihat pada tabel berikut,

Tabel 10 *Relative Risk Matrix*

RELATIVE RISK MATRIX			
Probability	***Relative 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

Kemudian menentukan pedekatan mitigasi yang sesuai berdasarkan penempatan kategori pada masing-masing pool yang dapat dilihat pada tabel berikut,

Tabel 11 Pendekatan Mitigasi

POOL	*MITIGATION APPROACH*
Pool 1	*Mitigate*
Pool 2	*Mitigate or Defer*
Pool 3	*Defer or Accept*
Pool 4	*Accept*

Lalu untuk semua *Area Of Concern* yang telah diklasifikasikan selanjutnya membuat rencana mitigasi berdasarkan dengan pendekatan mitigasi yang dapat dilihat pada tabel berikut,

Tabel 12 Mitigasi Risiko

NO	*AREA OF CONCERN*	*PROBABILITY*	*RELATIVE RISK SCORE*	POOL	*MITIGATION APPROACH*
1	Kesalahan dalam melakukan login	*Low*	15	Pool 4	*Accept*
2	Penyalahgunaan hak akses user	*High*	31	Pool 1	*Mitigate*
3	Kerusakan data user	*High*	35	Pool 1	*Mitigate*
4	Kesalahan dalam penginputan jumlah biaya pada rincian tindakan/pelayanan	*Medium*	28	Pool 2	*Defer*
5	Kesalahan notifikasi data obat pada rincian tindakan/pelayanan	*High*	32	Pool 1	*Mitigate*
6	Data jumlah biaya tindakan/pelayanan dapat di modifikasi atau di hapus	*High*	39	Pool 1	*Mitigate*
7	Kesalahan dalam penginputan data invoice pasien	*High*	32	Pool 1	*Mitigate*
8	Kerusakan pada data invoice	*High*	35	Pool 1	*Mitigate*
9	Kesalahan dalam mencetak invoice	*Medium*	27	Pool 2	*Defer*

5. Kontrol dan Rekomendasi

Kontrol ditetapkan untuk mengontrol sebuah risiko agar dapat meminimalisir terjadinya risiko yang berulang. NIST SP 800-53 merupakan kontrol yang digunakan pada penelitian ini yang dapat dilihat pada tabel berikut,

Tabel 13 Tabel kontrol dan rekomendasi

No	Area of Concern	Rekomendasi	Deskripsi
1	Kerusakan pada data user	*RA-5 Vulnerability Scanning,*	Melakukan pemindaian kerentanan dalam sistem informasi dan aplikasi yang telah ditentukan oleh organisasi ketika terdapat kerentanan baru yang

2	Kerusakan pada data invoice		dapat berpotensi mempengaruhi sistem atau aplikasi.
3	Kesalahan dalam penginputan jumlah biaya pada rincian tindakan/pelayanan	*SI-10 Information Input Validation*	Melakukan kembali validitas informasi dengan bantuan sistem informasi
4	Kesalahan notifikasi data obat pada rincian tindakan/pelayanan		
5	Kesalahan dalam penginputan data invoice pasien		
6	Kesalahan dalam mencetak invoice		
7	Penyalahgunaan hak akses user	*IA-2 Identification and Authentication (Organizational Users)*	Melakukan identifikasi dan autentifikasi pada user
8	Data jumlah biaya tindakan/pelayanan dapat di modifikasi atau di hapus	*SI-4 Information System Monitoring*	Melakukan pemantauan terhadap serangan yang dapat memodifikasi data

5.1 Aspek Rekomendasi

Setelah melakukan penetapan kontrol rekomendasi, Lalu kita bagi rekomendasi ke dalam 3 aspek rekomendasi. Ada aspek *people*, *Process* dan *technology*. Kontrol pada SIMRS modul billing dapat dilihat pada tabel berikut,

Tabel 14 Aspek Rekomendasi

No	Rekomendasi	Aspek		
		People	*Process*	*Technology*
1	RA-5 *Vulnerability Scanning*	Melakukan peningkatan keterampilan SDM	Melakukan penyusunan SPO *Vulnerability Scanning*	Mengimplementasikan Tools *Vulnerability Scanning*
2	*SI-10 Information Input Validation*	-	Melakukan Penyusunan SPO penginputan data	-

3	*IA-2 Identification and Authentication (Organizational Users)*	Melakukan peningkatan keterampilan SDM	Melakukan penyusunan SPO *Scanning Barcode*	Mengimplementasikan fitur *QR Code*
4	*SI-4 Information System Monitoring*	-	Melakukan penyusunan SPO monitoring user SIMRS	-

5.2 Rekomendasi Aspek People

Pada perancangan rekomendasi aspek *people*, akan dilakukannya pelatihan kemampuan dan peningkatan SDM. Rekomendasi aspek people dapat dilihat pada tabel berikut,

Tabel 15 Rekomendasi Aspek *People*

Kontrol	Judul Pelatihan	Deskripsi
RA-5 *Vulnerability Scanning*	Pelatihan penggunaan *tools vulnerability scanning*	Meningkatkan kompetensi pada staff dengan cara penerapan penggunaan *tools vulnerability scanning* pada SIMRS
IA-2 Identification and Authentication (Organizational Users)	Pelatihan penggunaan fitur QR Code	Meningkatkan kompetensi pada staff dengan cara penerapan penggunaan fitur *QR Code* pada SIMRS

5.3 Rekomendasi Aspek Process

Pada perancangan rekomendasi aspek *Process*, akan dilakukannya pengajuan pembuatan Standar Prosedur Operasional dan melakukan revisi Standar Prosedur Operasional yang sudah berjalan. Rekomendasi aspek process dapat dilihat pada tabel berikut,

Tabel 16 Rekomendasi Aspek *Process*

Kontrol	Rekomendasi	Deskripsi
RA-5 *Vulnerability Scanning*	Melakukan penyusunan SPO *Vulnerability Scanning*	Membuat SPO tentang penggunaan *monitoring* kerentanan
SI-10 *Information Input Validation*	Melakukan penyusunan SPO Penginputan Data	Membuat SPO tentang penginputan data
IA-2 Identification and Authentication (Organizational Users)	Melakukan penyusunan SPO *Scanning Barcode*	Membuat SPO tentang penggunaan *Scanning Barcode*
SI-4 *Information System Monitoring*	Melakukan penyusunan SPO monitoring user SIMRS	Membuat SPO tentang monitoring user SIMRS

5.4 Rekomendasi Aspek Technology

Pada perancangan rekomendasi aspek *Technology*, akan dilakukannya pengajuan implementasi tools *vulnerability scanning*. Rekomendasi aspek technology dapat dilihat pada tabel berikut,

Tabel 17 Rekomendasi Aspek *Technology*

Kontrol	Rekomendasi	Deskripsi
RA-5 *Vulnerability Scanning*	Implementasi dengan Tools *Vulnerability Scanning*,	Aplikasi yang berfungsi sebagai pendeteksi celah kemanan
IA-2 Identification and Authentication (Organizational Users	Penambahan fitur *Scanning Barcode*	Berfungsi sebagai otorisasi pengguna

5.5 Komparasi Tools: Vulnerability Scanning

Komparasi tools vulnerability scanning berfungsi sebagai perbandingan antar tools yang akan direkomendasikan. Berikut adalah tabel perbandingan fitur tools vulnerability scanning yang tersedia, ada empat opsi yaitu *Angry IP Scanner*, *SolarWinds*, *PRTG Network Monitor*, *Acunetix*. Masing masing opsi memiliki fitur yang berbeda, Lalu akan dipilih sebagai rekomendasi untuk kontrol RA-5 *Vulnerability Scanning.* Dan opsi yang dipilih untuk kontrol tersebut adalah Acunetix dikarenakan tools ini dapat memberikan solusi dari kelemahan yang ditemukan dan mengelola *traceability* dari setiap *vulnerabilities* . Hasil komparasi tools dapat dilihat pada tabel berikut,

Tabel 18 Komparasi *Tools*

Opsi	Fitur	Rekomendasi
Angry IP Scanner	1. Laporan pemindaian terdiri dari informasi seperti nama host, NetBIOS (Sistem Input / Output Dasar Jaringan), alamat MAC, nama komputer, informasi grup kerja, dll. 2. Pembuatan laporan dalam format CSV, Txt dan / atau XML. 3. Pemindaian Multi-utas yang merupakan utas pemindaian terpisah untuk setiap alamat IP individu, membantu meningkatkan proses pemindaian.	Acunetix, karena tools ini dapat memberikan solusi dari kelemahan yang ditemukan dan mengelola *traceability* dari setiap *vulnerabilities* tersebut
SolarWinds	1. Pemindai Perangkat Jaringan akan secara otomatis menemukan dan memindai perangkat jaringan. Anda akan dapat memetakan topologi jaringan. 2. Memberikan metrik kesalahan, ketersediaan, dan kinerja untuk perangkat di jaringan. - Monitor Kinerja Jaringan menyediakan dasbor yang dapat disesuaikan untuk menampilkan informasi tersebut. 3. Monitor Kinerja Jaringan akan memberikan akar penyebab lebih cepat melalui peringatan jaringan cerdas, ketergantungan & topologi. 4. Melakukan analisis hop-by-hop cloud dan aplikasi & layanan lokal.	
PRTG Network Monitor	1. PRTG Network Monitor akan memberi tahu Anda tentang bandwidth yang digunakan perangkat dan aplikasi Anda untuk mengidentifikasi sumber kemacetan. 2. Dengan bantuan sensor PRTG yang dikonfigurasi secara individual dan kueri SQL, Anda dapat memantau kumpulan data tertentu dari database Anda. 3. Memberikan statistik terperinci untuk setiap aplikasi di jaringan Anda. Anda akan dapat memantau dan mengelola semua layanan komputasi Anda secara terpusat dari mana saja.	

	4. Memiliki lebih banyak fitur dan fungsi untuk Server, Pemantauan, Pemantauan LAN, SNMP, dll.	
Acunetix	1. Teknologi Acusensor 2. Industri yang paling canggih dan mendalam dalam SQL injection dan pengujian Cross site scripting. 3. Mendukung HTML5 penuh dengan Acunetix DeepScan Teknologi 4. Aplikasi scanning komprehensif baik untuk Halaman Single dan situs berbasis JavaScript 5. Mendukung Mobile web site 6. Dapat mendeteksi kerentanan Blind XSS dengan layanan AcuMonitor 7. Dapat mendeteksi otomatis kerentanan XSS berbasis DOM 8. Alat pengujian penetrasi Canggih, seperti HTTP Editor dan HTTP Fuzzer 9. Fasilitas pelaporan ekstensif termasuk laporan kepatuhan PCI 10. Multi-berulir dan petir scanner cepat merangkak ratusan ribu halaman dengan mudah.	

5.6 Penambahan Fitur SIMRS : QR Code

Berikut merupakan tabel yang berisikan fitur tambahan pada SIMRS Modul Billing : *QR Code* , yang dapat dilihat pada tabel V-7

Tabel 19 Penambahan Fitur SIMRS

No	Penambahan Fitur	Proses	Deskripsi
1	*Reader*	Melakukan pemindaian barcode akun pengguna	Membaca data dalam bentuk barcode
2	*Decoder*	Melakukan penerimaan kode barcode dan merubahnya menjadi data yang dapat dibaca oleh sistem computer	Menerjemahkan data barcode

6. Penutup

6.1 Kesimpulan

Berdasarkan penelitian yang sudah dilakukan pada SIMRS Modul Billing, berikut merupakan kesimpulan yang dapat diambil :

1. Fase pertama dalam menganalisis ririko menggunakan metode OCTAVE Allegro adalah dengan mengembangkan kriteria pengukuran risiko terdapat 5 impact areas yang menjadi indicator dalam penilaian dan mitigasi risiko yang akan digunakan, yaitu *Reputation and Customer Confidence*, *Financial*, *Productivity*, *Safe and Health*, dan *Fines and Legal Penalties*. Fase kedua membuat profil aset informasi dan mengidentifikasi informasi aset kontainer. Fase ketiga mengidentifikasi *area of concern* dan memperjelas ancaman dengan memberikan gambaran secara detail 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 memulai 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. Ada dua jenis penanganan pada risiko yang diberikan yaitu *mitigate* dan *defer*. Risiko yang diberikan penanganan mitigasi dikarenakan memiliki dampak level yang besar sehingga harus diberikan rekomendasi kontrol yang sesuai agar dapat mengurangi dampak yang terjadi dan risiko yang diberikan penanganan *defer* karena pihak RSKIA menangguhkan dampak risiko dikarenakan ingin melakukan evaluasi dan mengumpulkan informasi lainnya agar guna melakukan analisis tambahan

3. Kontrol dan rekomendasi yang digunakan pada penelitian ini adalah NIST.SP.800-53. Dan kontrol yang digunakan adalah RA-5 *Vulnerability Scanning*, SI-10 *Information Input Validation*, IA-2 *Identification and Authentication (Organizational Users)*, SI-4 *Information System Monitoring*
4. Roadmap berfungsi sebagai acuan waktu dalam menerapkan rekomendasi kontrol yang telah dibuat sebelumnya. Terdapat 3 aspek *people*, *process*, dan *technology*.

6.2 Saran

Saran bagi RSKIA kota Bandung terkait penelitian ini adalah:

1. Meningkatkan kesadaran terhadap risiko yang mungkin atau bahkan akan terjadi pada semua modul yang terdapat pada SIMRS
2. Memberikan rekomendasi yang sudah disarankan agar dampak kemungkinan terjadinya suatu risiko dapat dicegah atau diminimalisir
3. Hasil penelitian ini dapat dijadikan referensi terhadap peneliti selanjutnya agar penelitian selanjutnya menjadi lebih luas

Referensi

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. http://www.sei.cmu.edu/publications/pubweb.html

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.

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. https://doi.org/10.29207/resti.v2i1.96

Rachmaniah, M., & Mustafa, B. (2015). 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. https://doi.org/10.24014/sitekin.v16i2.7457

Setyawan D. (2016). Analisis Implementasi Pemanfaatan Sistem Informasi Manajemen Rumah Sakit (Simrs) Pada Rsud Kardinah Tegal. *Indonesian Journal on Computer and Information Technology*, *1*(2), 54–61. http://ejournal.bsi.ac.id/ejurnal/index.php/ijcit/article/view/1503

Security and Privacy Controls for Federal Information Systems and Organizations. (2013). https://doi.org/10.6028/NIST.SP.800-53r4

St, R. F., Adhitya, R., & St, N. (2020). *ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO PADA DINAS KOMUNIKASI DAN INFORMATIKA*. *7*(2), 7003–7008.

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, *2*(2), 8. https://doi.org/10.24014/coreit.v2i2.2356

Tobing, J. J. L., & Puspa, A. K. (2015). Analisis Manajemen Resiko untuk Evaluasi Aset Menggunakan Metode Octave Allegro. *EXPERT: Jurnal Manajemen Sistem Informasi Dan Teknologi*, *5*(1). https://doi.org/10.36448/jmsit.v5i1.719

Wijaya, R. A. P., & Arif Rahman Hakim. (2020). Perancangan Perangkat Audit Internal Untuk Sistem Keamanan Informasi Pada Organisasi Xyz Developing Internal Audit Tool for Information Security System. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *7*(3), 435–442. https://doi.org/10.25126/jtiik.202071940