e-ISBN 978-623-93343-4-5
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 15 September 2021

Analisis dan Manajemen Risiko Keamanan Informasi pada Rumah Sakit Menggunakan Metode Octave Allegro (Studi Kasus: Rumah Sakit Umum Daerah Cengkareng)

Jesica Wijaya [1], Anggi Megafitri [2], Khusnul Khotimah[3], Ria Astriratma, S.Kom., M.Cs.[4]
S1 Sistem Informasi / Fakultas Ilmu Komputer Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
Jl. RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Daerah Khusus Ibukota Jakarta 12450
jesicaw@upnvj.ac.id[1], anggim@upnvj.ac.id [2], khusnulkhotimah@upnvj.ac.id[3], astriratma@upnvj.ac.id[4]

Abstrak. Keamanan informasi adalah satu hal yang begitu penting untuk suatu perusahaan ataupun organisasi lain. karena keamanan informasi memiliki tujuan untuk menjaga suatu kerahasiaan, ketersediaan, dan integritas yang ada dalam suatu perusahaan ataupun organisasi tersebut. Apabila suatu keamanan informasi yang tidak dirawat dengan baik dan benar yang akan menimbulkan suatu permasalahan dan ancaman yang tidak terduga untuk perusahaan atau organisasi tersebut. Penelitian ini dilakukan untuk menganalisis dan mengetahui keadaan keamanan sistem informasi sebuah Rumah Sakit Umum Daerah (RSUD) Cengkareng. RSUD Cengkareng ini dalam pengelolaan informasinya belum pernah melakukan pengukuran risiko dan juga belum menerapkan manajemen risiko. Untuk menganalisis permasalahan yang kemungkinan terjadi pada RSUD Cengkareng, penelitian ini menggunakan metode Octave Allegro. RSUD Cengkareng mendapatkan rekomendasi kontrol berupa saran pembuatan sebuah simulasi visual untuk memudahkan stafnya dalam memahami pentingnya aset informasi, potensi ancaman dan risiko, serta konsekuensinya.

Kata Kunci: Keamanan Informasi, RSUD Cengkareng, Manajemen Risiko, Octave Allegro.

1 Pendahuluan

Penerapan manajemen risiko dan pengukuran risiko keamanan informasi saat ini dapat membantu perusahaan menetapkan prosedur untuk menghindari ancaman sekaligus melindungi masa depan suatu perusahaan dari berbagai ancaman keamanan informasi. Dalam implementasi yang dilakukan, terdapat beberapa risiko yang dihadapi sebuah instansi rumah sakit dalam melakukan pengukuran terhadap risiko atau nilai risiko. Rumah Sakit Umum Daerah (RSUD) Cengkareng yang berdiri pada tahun 1999 dan memiliki akreditasi B di bawah naungan Pemerintah. Saat ini pengelolaan proses bisnis pada RSUD Cengkareng belum menerapkan manajemen risiko dengan pengukuran risiko. Oleh karena itu untuk meminimalisir banyaknya risiko yang mungkin terjadi, maka RSUD Cengkareng perlu melakukan pengukuran keamanan informasi.

Pentingnya manajemen risiko diharapkan dapat memperoleh rekomendasi panduan untuk menyempurnakan penerapan keamanan informasi serta memiliki solusi pada risiko yang dihadapi secara keseluruhan untuk mengurangi kerugian pada RSUD Cengkareng. Cakupan yang akan diteliti dan difokuskan hanya pada prosedur-prosedur yang ada pada RSUD Cengkareng, proses dan aktivitas guna menjaga informasi dari risiko-risiko yang mungkin terjadi. Evaluasi yang dilakukan pada RSUD Cengkareng merujuk pada delapan area yang mencangkup uji data, infrastruktur, perangkat keras, perangkat lunak, jaringan, aplikasi, dan juga staf.

2 Landasan Teori

2.1 Informasi

Informasi merupakan sekelompok data dan fakta yang diproses menjadi suatu yang bermanfaat serta bernilai sehingga dapat dijadikan dasar untuk untuk mengambil suatu keputusan. Informasi dapat menjadi sumber pengetahuan bagi masyarakat karena dapat menyediakan sebuah peristiwa dan kondisi dalam masyarakat.

Informasi merupakan sesuatu yang diolah dengan cara tertentu sehingga menghasilkan arti bagi penerima berdasarkan sekumpulan data dan fakta yang tersedia [1]. Informasi juga dapat mempengaruhi masyarakat, saat ini masyarakat sering terpengaruh melalui media massa yang beredar.

2.2 Manajemen Risiko

Manajemen risiko secara luas diartikan sebagai sebuah proses yang bertujuan untuk mengukur atau menilai suatu teknologi informasi untuk memperoleh sebuah keseimbangan untuk meminimalkan berbagai kerentanan dan kerugian. Manajemen risiko merupakan suatu sistem pengawasan dan perlindungan aset atau harta milik suatu perusahaan atau perorangan yang memungkinkan akan menimbulkan kerugian dikarenakan terjadinya suatu risiko yang merugikan pemilik aset tersebut [2].

2.3 Keamanan Informasi

Keamanan infomasi merupakan suatu cover yang melindungi informasi, termasuk perangkat sistem yang digunakan dalam kelangsungan pekerjaan untuk meminimalisir terjadinya kerusakan yang disebabkan karena adanya ancaman [3]. Keamanan informasi memiliki beberapa aspek yang diantaranya terdapat *privacy, identification, authentication, authorization, dan accountability.*

Keamanan informasi sangat dibutuhkan untuk memproteksi informasi yang ada dari ancaman untuk memperkecil kerugian suatu organisasi atau perusahaan. Untuk meningkatkan sistem pengendalian yang ada baik internal maupun eksternal perusahaan dalam membantu kegiatan guna mencapai tujuan.

2.4 Octave Allegro

Octave atau dikenal sebagai *Operationally Critical Threat, Asset, and Vulnerability Evaluation* merupakan sekumpulan komponen yang bersifat komprehensif dan sistematis dari konteks berbasis evaluasi risiko pada suatu keamanan informasi. Metode octave allegro dirancang untuk memungkinkan penilaian secara luas risiko dengan tujuan menghasilkan hasil yang lebih akurat tanpa pengetahuan penilaian risiko yang luas [4].

Metode Octave Allegro menggunakan delapan tahapan untuk melakukan penilaian risiko keamanan informasi yang diantaranya adalah sebagai berikut:

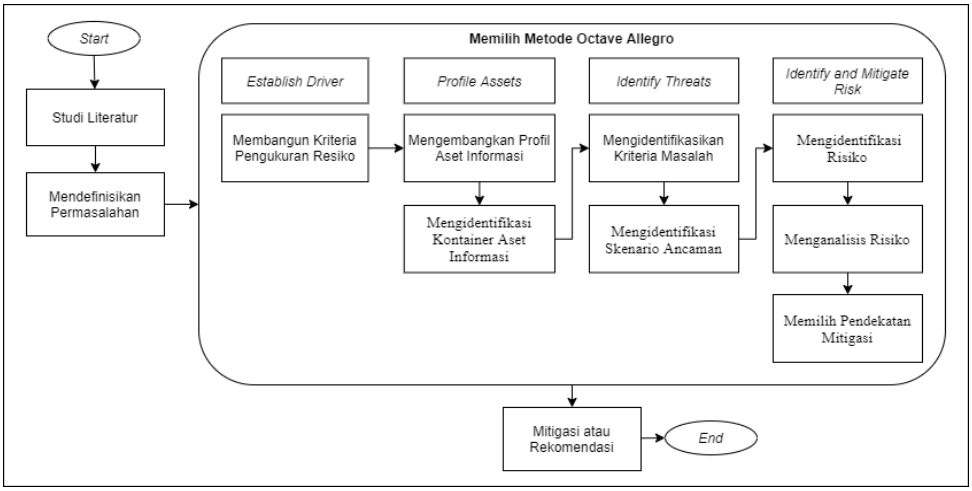
1. Membangun Kriteria Pengukuran Risiko yaitu bekerja untuk membangun penggerak organisasi yang berfungsi sebagai bahan evaluasi dari dampak risiko pada tujuan bisnis dalam mengenali *impact area* di ruang lingkup manajemen risiko.
2. Mengembangkan Profil Aset Informasi, terdiri dari banyak aktivitas yang dijalankan, yaitu diantaranya identifikasi aset informasi, penilaian risiko terstruktur, mengumpulkan informasi aset, membuat dokumentasi pemilihan aset, membuat deskripsi aset, mengisi keamanan untuk kerahasiaan, integritas, dan ketersediaan serta mengidentifikasi kebutuhan keamanan untuk aset informasi.
3. Mengidentifikasi Kontainer Aset Informasi yaitu memperhatikan poin penting dari aset informasi yang akan dijaga.
4. Mengidentifikasi Area Masalah yaitu merupakan sebuah aktivitas dalam mengembangkan profil risiko dari sebuah aset informasi.
5. Mengidentifikasi Skenario Ancaman yaitu melakukan identifikasi terhadap skenario ancaman tambahan.

6. Mengidentifikasi Risiko yaitu melakukan identifikasi terhadap risiko yang mungkin terjadi dan telah didokumentasikan pada *information asset risk worksheet.*
7. Menganalisis Risiko terdiri dari aktivitas dalam melakukan peninjauan kriteria pengukuran risiko serta menghitung nilai risiko *relative* yang dapat dimanfaatkan sebagai bahan menganalisis risiko dan dapat memutuskan strategi terbaik dalam menghadapi risiko.
8. Memilih Pendekatan Mitigasi yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risiko kemudian melakukan pendekatan serta mitigasi untuk setiap risiko dengan melihat pada kondisi yang terjadi saat ini pada suatu organisasi.

3 Metode Penelitian

3.1 Tahap Penelitian

Penelitian yang berlangsung pada RSUD Cengkareng saat ini terdapat beberapa tahapan. Berikut tahapan penelitian yang kami lakukan dapat dilihat dari gambar tahap penelitian di bawah ini.



Gambar. 1. Tahap Penelitian

Penelitian pada Rumah Sakit Umum Daerah Cengkareng dimulai dengan melakukan studi literatur, lalu kami melakukan perumusan atau mengidentifikasi masalah terkait risiko keamanan informasi yang dapat terjadi pada Rumah Sakit Umum Daerah Cengkareng. Setelah merumuskan masalah, kami menganalisis masalah tersebut menggunakan metode Octave Allegro. Kajian data yang didapatkan melalui proses survei lapangan pada pihak pegawai RSUD Cengkareng. Pengumpulan data bertujuan untuk menguatkan informasi yang dibutuhkan pada identifikasi risiko keamanan informasi agar proses penelitian bisa berjalan dengan maksimal. Setelah mendapatkan hasil dari penelitian menggunakan metode Octave Allegro, kami memberikan beberapa mitigasi atau rekomendasi untuk meminimalisir masalah tersebut.

3.2 Pengumpulan Data

3.2.1 Studi Literatur

Studi literatur merupakan salah satu tahapan yang cukup penting dalam penelitian yang akan dilakukan, karena dapat dikatakan sebagai proses awal dari sebuah penelitian. Studi literatur merupakan kegiatan membaca, mencatat, dan mengolah sekumpulan data pustaka yang dapat berguna sebagai bahan dari sebuah penelitian. Teknik studi literatur digunakan untuk mengungkapkan sekumpulan teori-teori relevan yang dapat mendukung penelitian yang akan dilakukan.

3.3 Pendefinisian Permasalahan

Pendefinisian permasalahan membantu peneliti agar menyatakan tujuan dari penelitian dan dapat memberikan rekomendasi sesuai dengan permasalahan yang di dapat. Permasalahan yang di dapat berdasarkan studi literatur menjelaskan bahwa RSUD Cengkareng belum adanya sebuah pengukuran risiko dan penerapan manajemen risiko. Oleh karena itu dibutuhkan sebuah manajemen risiko keamanan informasi yang dapat membantu RSUD Cengkareng dalam mengurangi serta mengantisipasi ancaman yang mungkin terjadi di masa depan.

3.4 Mitigasi atau Rekomendasi

Hasil dari penelitian ini berupa rancangan mitigasi atau rekomendasi yang dapat menjadi panduan atau saran dalam penerapan manajemen risiko keamanan informasi yang dapat membantu RSUD Cengkareng dalam mengurangi serta mengantisipasi ancaman yang mungkin terjadi di masa depan.

4 Hasil dan Pembahasan

4.1 Kriteria Pengukuran Risiko

Berdasarkan analisis penulis pada tahap kriteria pengukuran risiko untuk menentukan dampak *area* dan memberikan skala utama pada dampak *area* yang ditemukan. 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. Hasil yang didapat pada kriteria pengukuran risiko oleh analisa penulis terdapat pada tabel. 1 sebagai berikut:

Tabel. 1. Kriteria Pengukuran Risiko 1

Allegro Worksheet	***Risk Measurement Criteria Reputation And Customer Confidence***
Priority	***Impact Area***
2	*Reputation and Customer Confidence*
3	*Financial*
4	*Productivity*
1	*Safety and Health*
5	*Fines and Lawsuits*

4.2 Membangun Profil Aset Informasi

Berdasarkan analisis penulis pada tahap membangun profil aset informasi dilakukan proses pembangunan profil aset informasi atas aset apa saja yang dimiliki RSUD Cengkareng. Hasil analisis yang didapatkan oleh penulis terdapat pada tabel. 2 sebagai berikut:

Tabel. 2. Membangun Profil Aset Informasi

Allegro Worksheet	***Critical Information Asset Profile***	
Critical Asset	Apa aset informasi penting?	Data *User*
Rationable for Selection	Mengapa informasi tersebut menjadi aset bagi organisasi?	*User* harus melakukan *login* terlebih dahulu untuk mengakses informasi yang terdapat dalam aplikasi RSUD Cengkareng.
Description	Apa deskripsi yang disepakati dari aset informasi ini?	Berisi tentang *username*, *password*, dan hak akses untuk mengakses aplikasi RSUD Cengkareng.
Owner(s)		Bidang Pengelolaan RSUD Cengkareng.
Security Requirements	Apa persyaratan keamanan untuk aset informasi?	
Confidentiality	Hanya staf berwenang yang dapat melihat aset informasi berikut.	Pengelola Sistem Informasi RSUD Cengkareng.
Integrity	Hanya staf berwenang yang dapat melihat aset informasi berikut.	Pengelola Sistem Informasi RSUD Cengkareng.
Availability	Aset ini harus tersedia bagi staf untuk melakukan pekerjaan mereka. Aset ini harus tersedia selama 24 jam, 7 hari/minggu.	Pengelola Sarana dan Prasarana RSUD Cengkareng.
Most Important Security Requirement		
Apa persyaratan keamanan terpenting untuk aset informasi ?		
Kerahasiaan [ ]	Integritas [V]	Ketersediaan [ ]

4.3 Identifikasi Kontainer dan Aset Informasi

Berdasarkan analisis penulis pada tahap identifikasi kontainer dan aset informasi, perlu dilakukan identifikasi pada setiap kontainer yang akan disimpan dan diproses, baik secara *internal* maupun *eksternal*. Berdasarkan hasil analisis yang didapat oleh penulis pada tabel.3 tersebut dibagi menjadi 3 kategori, yaitu *Technical, Physical*, dan *People* yang dapat dilihat sebagai berikut:

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

Kategori	***Description***	***Owner***
Internal	*Web Server dan Database server*	Pengelola Sistem Informasi RSUD Cengkareng

	Komputer dan Laptop	Pengelola Sarana dan Prasarana RSUD Cengkareng
	Jaringan Internal (LAN)	Pengelola Sistem Informasi RSUD Cengkareng
Eksternal	*Internet Service Provider* (ISP)	Vendor

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

Kategori	*Description*	*Owner*
Internal	*Form Registrasi User*	Pengelola Sistem Informasi RSUD Cengkareng

Tabel. 5. *Information Asset Risk Environment (People)*

Kategori	*Description*	*Owner*
Internal	Staf Pengelola Sistem Informasi RSUD Cengkareng	Pengelola Sistem Informasi RSUD Cengkareng

4.4 Identifikasi Area Masalah

Berdasarkan analisis penulis pada tahap identifikasi area masalah harus dilakukan pengidentifikasian area masalah pada suatu keadaan atau status yang dapat merusak semua aset informasi rumah sakit, dengan cara mengelompokkan aktivitas-aktivitas tersebut. Hasil analisis dari pengidentifikasian area masalah oleh penulis terdapat pada tabel. 6 sebagai berikut:

Tabel. 6. *Mengidentifikasi Area Masalah*

No.	*Area Of Concern* - Data *User*
1	Pemanfaatan celah dalam mengakses keamanan sistem informasi oleh pihak luar maupun dalam yang tidak diketahui identitasnya.
2	Penyalahgunaan hak akses terhadap data *user*.
3	Adanya kerusakan pada data user yang terdapat dalam *database* rumah sakit.
4	Kehilangan data *user* karena tidak melakukan *backup* data.
5	Pemalsuan informasi data terhadap data *user*.
6	Kesalahan dalam menginput data *user* ke dalam sistem rumah sakit.
7	Kebocoran data permintaan *user*.
8	Penyebaran hak akses terhadap data permintaan layanan yang sedang dalam proses.

4.5 Identifikasi Skenario Ancaman

Berdasarkan analisis penulis pada tahap identifikasi skenario ancaman yaitu mengidentifikasi area yang akan menjadi pusat perhatian untuk tahap sebelumnya dengan cara mempertajam ancaman dengan mengadakan identifikasi *threat scenario* dengan membuat gambaran secara terperinci pada *information assets* dari *threat scenario* yang telah ditentukan dalam *information asset risk* yang ada. Hasil analisis tersebut terdapat pada tabel. 7 sebagai berikut:

Tabel. 7. Mengidentifikasi Skenario Ancaman

Information Asset	**Data *User***
Area of Concern	Pemanfaatan celah dalam mengakses keamanan sistem informasi oleh pihak luar maupun dalam yang tidak diketahui identitasnya.
1. *Actor*	*User*
2. *Means*	Pemanfaatan celah keamanan dari *server*, *database* ataupun modul oleh pihak luar maupun dalam.
3. *Motives*	Dengan sengaja ataupun tidak sengaja.
4. *Outcome*	[v] *Disclosure* [v] *Modification* [v] *Destruction* [v] *Interuption*
5. *Security Requirement*	Meningkatkan tingkat keamanan dari *software*, *hardware*, dan jaringan. Dilakukannya pemantauan secara berkala terhadap keamanan sistem informasi pada RSUD Cengkareng.
6. *Probability*	[v] *High* [v] *Medium* [v] *Low*

4.6 Identifikasi Risiko

Berdasarkan analisis penulis pada tahap identifikasi risiko merupakan penentuan pada *threat scenario* yang telah ada pada *Information Asset Risk Worksheet* yang berdampak pada RSUD Cengkareng yang dapat dilihat pada tabel. 8 sebagai berikut:

Tabel. 8. Mengidentifikasi Risiko

No	*Area Of Concern*	*Consequences*
1	Pemanfaatan celah dalam mengakses keamanan sistem informasi oleh pihak luar maupun dalam yang tidak diketahui identitasnya.	Informasi yang dapat dimodifikasi karena adanya celah keamanan dapat menyebabkan informasi tersebut tidak benar adanya atau rusak sehingga mengganggu kerja sistem informasi rumah sakit yang sedang berjalan.
2	Penyalahgunaan hak akses terhadap data *user*.	Adanya ancaman terhadap keamanan data *user* yang dapat menyebabkan tersebarnya data *critical asset* yang ada pada

		rumah sakit dan mengganggu proses berjalannya bisnis, serta adanya ancaman pemalsuan informasi pada data *user*.
3	Adanya kerusakan pada data user yang terdapat dalam *database* rumah sakit.	Kerusakan data *user* pada *database* rumah sakit menyebabkan terganggunya integritas data-data penting yang terdapat pada rumah sakit.
4	Kehilangan data *user* karena tidak melakukan *backup* data.	Proses bisnis pada rumah sakit terganggu dan dapat mengalami kerugian besar akibat hilangnya data-data penting rumah sakit.
5	Pemalsuan informasi data terhadap data *user*.	Informasi palsu pada data *user* dapat menyebabkan kurangnya kepercayaan pengguna terhadap manajemen rumah sakit.
6	Kesalahan dalam menginput data *user* ke dalam sistem rumah sakit.	Kesalahan data yang diinput dapat menyebabkan kerugian bagi pengguna serta dapat mengganggu kerja sistem.
7	Kebocoran data permintaan *user*.	Data permintaan user yang mengalami kebocoran dapat menyebabkan penyalahgunaan oleh pihak yang tidak bertanggung jawab sehingga dapat merugikan baik pengguna maupun pihak rumah sakit.
8	Penyebaran hak akses terhadap data permintaan layanan yang sedang dalam proses.	Penyebaran hak akses menyebabkan layanan yang sedang dalam proses mengalami gangguan dan memperlambat kerja sistem yang ada.

4.7 Analisis Risiko

Berdasarkan analisis penulis pada tahap analisis risiko dilakukan *review risk measurement criteria* dimana mengukur dampak yang ada pada risiko dengan cara menakar jumlah/nilai risiko relatif. Dalam menghitung skor dampak area dan skor risiko relatif pada setiap risiko aset informasi dapat dilakukan dengan perkalian pada prioritas dampak area. Terdapat 3 kategori pada *impact area* dengan metode octave allegro, yaitu: Low=1, Medium=2, High=3. Hasil dari penentuan skor *impact area* dapat dilihat pada tabel. 9 sebagai berikut:

Tabel. 9. Penentuan Skor *Impact Area*

Impact Area	*Priority*	*Score Impact Area*		
		Low (n = (1))	*Medium* (n = (2))	*High* (n = (3))
Reputation and Customer Confidence	2	2	4	6
Financial	3	3	6	9
Productivity	4	4	8	12
Safety and Health	1	1	2	3
Fines and Lawsuits	5	5	10	15

Pada tabel. 9 dapat ditentukan untuk menghitung skor *Risk Relative Matrix* yang berguna untuk mendapatkan hasil analisis risiko. Hasil analisis risiko yang didapat dapat dilihat pada tabel. 10.

Tabel 10. Analisis Risiko

Area of Concern	***Risk***			
Pemanfaatan celah dalam mengakses keamanan sistem informasi oleh pihak luar maupun dalam yang tidak diketahui identitasnya.	***Consequences***	Informasi yang dapat dimodifikasi karena adanya celah keamanan dapat menyebabkan informasi tersebut tidak benar adanya atau rusak sehingga mengganggu kerja sistem informasi rumah sakit yang sedang berjalan.		
	Severity	***Impact Area***	***Value***	***Score***
		Reputation and Customer Confidence	*High*	6
		Financial	*Medium*	6
		Productivity	*Medium*	8
		Safety and Health	*Medium*	2
		Fines and Lawsuits	*High*	15
		Relative Risk Score		**37**
Penyalahgunaan hak akses terhadap data *user*.	***Consequences***	Adanya ancaman terhadap keamanan data *user* yang dapat menyebabkan tersebarnya data *critical asset* yang ada pada rumah sakit dan mengganggu proses berjalannya bisnis, serta adanya ancaman pemalsuan informasi pada data *user*.		
	Severity	***Impact Area***	***Value***	***Score***
		Reputation and Customer Confidence	*High*	6
		Financial	*Low*	3
		Productivity	*Medium*	8
		Safety and Health	*Medium*	2
		Fines and Lawsuits	*Medium*	10
		Relative Risk Score		**29**
Pemalsuan informasi data terhadap data *user*.	***Consequences***	Kerusakan data *user* pada *database* rumah sakit menyebabkan terganggunya integritas data-data penting yang terdapat pada rumah sakit.		
	Severity	***Impact Area***	***Value***	***Score***
		Reputation and Customer Confidence	*High*	6
		Financial	*High*	9
		Productivity	*Medium*	8
		Safety and Health	*Medium*	2
		Fines and Lawsuits	*High*	15
		Relative Risk Score		**40**

<table>
<tr><td rowspan="8">Kehilangan data user karena tidak melakukan backup data.</td><td>Consequences</td><td colspan="3">Proses bisnis pada rumah sakit terganggu dan dapat mengalami kerugian besar akibat hilangnya data-data penting rumah sakit.</td></tr>
<tr><td rowspan="7">Severity</td><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td>Reputation and Customer Confidence</td><td>Medium</td><td>4</td></tr>
<tr><td>Financial</td><td>High</td><td>9</td></tr>
<tr><td>Productivity</td><td>High</td><td>12</td></tr>
<tr><td>Safety and Health</td><td>High</td><td>3</td></tr>
<tr><td>Fines and Lawsuits</td><td>High</td><td>15</td></tr>
<tr><td colspan="2">Relative Risk Score</td><td>43</td></tr>
<tr><td rowspan="8">Adanya kerusakan pada data user yang terdapat dalam database rumah sakit.</td><td>Consequences</td><td colspan="3">Informasi palsu pada data user dapat menyebabkan kurangnya kepercayaan pengguna terhadap manajemen rumah sakit.</td></tr>
<tr><td rowspan="7">Severity</td><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td>Reputation and Customer Confidence</td><td>High</td><td>6</td></tr>
<tr><td>Financial</td><td>High</td><td>9</td></tr>
<tr><td>Productivity</td><td>High</td><td>12</td></tr>
<tr><td>Safety and Health</td><td>Medium</td><td>2</td></tr>
<tr><td>Fines and Lawsuits</td><td>High</td><td>15</td></tr>
<tr><td colspan="2">Relative Risk Score</td><td>44</td></tr>
<tr><td rowspan="8">Kesalahan dalam menginput data user kedalam sistem rumah sakit.</td><td>Consequences</td><td colspan="3">Kesalahan data yang diinput dapat menyebabkan kerugian bagi pengguna serta dapat mengganggu kerja sistem.</td></tr>
<tr><td rowspan="7">Severity</td><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td>Reputation and Customer Confidence</td><td>Low</td><td>2</td></tr>
<tr><td>Financial</td><td>Low</td><td>3</td></tr>
<tr><td>Productivity</td><td>Low</td><td>4</td></tr>
<tr><td>Safety and Health</td><td>Low</td><td>1</td></tr>
<tr><td>Fines and Lawsuits</td><td>Low</td><td>5</td></tr>
<tr><td colspan="2">Relative Risk Score</td><td>15</td></tr>
<tr><td rowspan="3">Kebocoran data permintaan user.</td><td>Consequences</td><td colspan="3">Data permintaan user yang mengalami kebocoran dapat menyebabkan penyalahgunaan oleh pihak yang tidak bertanggung jawab sehingga dapat merugikan baik pengguna maupun pihak rumah sakit.</td></tr>
<tr><td rowspan="2">Severity</td><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td>Reputation and Customer Confidence</td><td>High</td><td>6</td></tr>
</table>

		Financial	*Medium*	6
		Productivity	*Medium*	8
		Safety and Health	*Low*	1
		Fines and Lawsuits	*High*	15
		Relative Risk Score		**36**
Penyebaran hak akses terhadap data permintaan layanan yang sedang dalam proses.	***Consequences***	Penyebaran hak akses menyebabkan layanan yang sedang dalam proses mengalami gangguan dan memperlambat kerja sistem yang ada.		
	Severity	***Impact Area***	***Value***	***Score***
		Reputation and Customer Confidence	*Medium*	4
		Financial	*Low*	3
		Productivity	*Medium*	8
		Safety and Health	*Low*	1
		Fines and Lawsuits	*Medium*	10
		Relative Risk Score		**26**

4.8 Pendekatan Mitigasi

Berdasarkan analisis penulis pada tahap akhir ini menggunakan pendekatan mitigasi yang akan menentukan semua risiko yang telah diidentifikasi berdasarkan *relative risk score*. Menurut penulis pendekatan mitigasi ini sangat mendukung dalam pengambilan keputusan status rekomendasi setiap risiko tersebut. Kemudian berdasarkan *risk relative matrix* pada tabel.11 maka dapat disimpulkan *mitigation approach* pada setiap *area of concern* yang dapat dilihat pada tabel. 12.

Tabel. 11. *Risk Relative Matrix*

Risk Relative Matrix		
Risk Score	***POOL***	***Mitigation Approach***
30-45	1	*Mitigate*
16-29	2	*Defer*
0-15	3	*Accept*

Tabel. 12. Mitigasi

No	*Area Of Concern*	*Risk Relative Matrix*	POOL	*Mitigation Approach*

1	Pemanfaatan celah dalam mengakses keamanan sistem informasi oleh pihak luar maupun dalam yang tidak diketahui identitasnya.	37	1	*Mitigate*
2	Penyalahgunaan hak akses terhadap data *user*.	29	2	*Defer*
3	Pemalsuan informasi data terhadap data *user*.	40	1	*Mitigate*
4	Kehilangan data *user* karena tidak melakukan *backup* data.	43	1	*Mitigate*
5	Adanya kerusakan pada data *user* yang terdapat dalam *database* rumah sakit.	44	1	*Mitigate*
6	Kesalahan dalam menginput data *user* kedalam sistem rumah sakit.	15	3	*Accept*
7	Kebocoran data permintaan *user*.	36	1	*Mitigate*
8	Penyebaran hak akses terhadap data permintaan layanan yang sedang dalam proses.	26	2	*Defer*

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 [6]. Berikut kontrol dan rekomendasi berdasarkan NIST SP 800-53 dapat dilihat pada tabel. 13.

Tabel. 13. Kontrol dan Rekomendasi

No	*Area of Concern*	Rekomendasi	Deskripsi
1	Pemanfaatan celah dalam mengakses keamanan sistem informasi oleh pihak luar maupun dalam yang tidak diketahui identitasnya.	RA-3 *Risk Assessment.*	Mengidentifikasi dan mendokumentasikan ancaman dan kerentanan dalam sistem baik internal maupun eksternal.
2	Penyalahgunaan hak akses terhadap data *user*.	PE-2 *Physical Access Control.*	Melakukan pengecekan dan pengawasan terhadap data *user.*
3	Pemalsuan informasi data terhadap data *user*.	AC-4 *Information Flow Enforcement.*	Melakukan pengawasan dan peninjauan terkait informasi pada data *user*.
4	Kehilangan data *user* karena tidak melakukan *backup* data.	CP-2 *Contingency Plan* CP-9 *Information System Backup*	● Mengupayakan rencana cadangan sebagai *alternative* terhadap ancaman dan kerentanan risiko. ● Melakukan *backup* informasi serta melindungi kerahasiaan, integritas, dan ketersediaan informasi cadangan.
5	Adanya kerusakan pada data *user* yang terdapat dalam *database* rumah sakit.		

6	Kesalahan dalam menginput data *user* kedalam sistem rumah sakit.	IR-4 *Incident Handling*	Melakukan pemeriksaan ulang validitas input informasi terhadap data *user*.
7	Kebocoran data permintaan *user*.	IA-2 *Identification and Authentication (Organizational Users)*.	Melakukan penggantian *username* dan *password* pada *user*.
8	Penyebaran hak akses terhadap data permintaan layanan yang sedang dalam proses.		

5 Kesimpulan dan Saran

Pada penelitian ini memberikan sebuah mitigasi risiko berdasarkan *pool relative risk matrix* dengan menggunakan metode Octave Allegro. Metode Octave Allegro merupakan salah satu metode manajemen informasi yang dapat direkomendasikan untuk perusahaan yang fokus dalam *finansial planner* dan kesiapan informasi yang penting untuk mendukung perusahaan dalam mencapai tujuannya.

Analisis risiko yang diberikan penanganan mitigasi atau rekomendasi dikarenakan mempunyai tingkat *level* yang luas yang besar kemudian diberikannya rekomendasi control supaya dapat meminimalisir dampak yang mungkin akan terjadi. Dampak area pada metode Octave Allegro adalah *reputation and customer confidence, financial. productivity, safety and health, fines and lawsuits*. Pada hasil identifikasi risiko terdapat 8 area yang difokuskan serta memiliki hasil mitigasi pada risiko tersebut.

Rekomendasi untuk RSUD Cengkareng adalah untuk menjadi simulasi gambaran visual untuk memudahkan pihak rumah sakit dalam mengerti pentingnya aset informasi yang ada serta ancaman dan risikonya. RSUD Cengkareng juga harus mengulas kembali keamanan sistem informasinya secara berperiode agar tidak terjadi sebuah masalah. Prosedur Manajemen Risiko Keamanan Informasi RSUD Cengkareng ini dibuat berdasarkan hasil analisis risiko dan rekomendasi kebijakan yang ada sesuai dengan yang tertera pada metode Octave Allegro.

RSUD Cengkareng memiliki beberapa identifikasi risiko, masalah risiko yang tinggi berdasarkan perhitungan *relative risk matrix* yaitu adanya kerusakan pada data *user* yang terdapat dalam *database* rumah sakit, maka dari itu, untuk meminimalisir risiko tersebut, perlunya perbaikan dengan mendokumentasikan sistem, arsipkan salinan asli data *user*, memiliki cadangan file yang sudah diuji dan diverifikasi, dan mempunyai rencana dalam memulihkan data *user* jika terjadi masalah, serta menggunakan antivirus.

Referensi

[1] E. Y. Anggraeni, E. Risanto, Y. Basuki, D. Nofianto, A. A. C, and A. Offset, *Pengantar Sistem Informasi*. Penerbit Andi.
[2] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.
[3] D. R. Windirya, H. Tanuwijaya, and E. Sutomo, "AUDIT KEAMANAN SISTEM INFORMASI PADA INSTALASI SISTEM INFORMASI MANAJEMEN RSUD BANGIL BERDASARKAN ISO 27002 Danastri," *Sist. Inf.*, vol. 3, no. 1, pp. 1–206, 2013.
[4] B. Supradono, "Manajemen risiko keamanan informasi dengan menggunakan metode octave (operationally critical threat, asset, and vulnerability evaluation)," *Media Elektr.*, vol. 2, no. 1, pp. 4–8, 2009.
[5] J. Sanjaya, "Analisis Risk Assessment Terhadap Perusahaan It Octave Allegro Framework."
[6] NIST SP800-53, "Security and privacy controls for federal information systems and organizations," *NIST Spec. Publ.*, vol. 800, p. 53, 2013.