Terbit online pada laman web jurnal : **http://jurnal.iaii.or.id**

JURNAL RESTI

(Rekayasa Sistem dan Teknologi Informasi)

Vol. 2 No. 1 (2018) 282 – 287 ISSN : 2580-0760 (media online)

Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)

Nurhafifah Matondang[a], Ika Nurlaili Isnainiyah[b], Anita Muliawati[c]

[a]Manajemen Informatika, Fakultas Ilmu Komputer, UPN "Veteran" Jakarta, nurhafifahmatondang@yahoo.com

[b]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jakarta, nurlailika@gmail.com

[c]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jakarta, anitamuliawati2013@yahoo.com

Abstract

This paper describes the implementation of OCTAVE Allegro method to evaluate several aspects related to information security risks of the information technology applied in a health institution. The evaluation was conducted at RSUD XYZ and referred to five impact areas: reputation and customer confidence, finance, productivity, security and health, and also penalties and punishment. The results show that the impact area of reputation and customer confidence has the highest risk assessment result among other areas. The overall result and discussion presented in this paper certainly does not violate the code of ethics for RSUD XYZ.

Keywords: information security, OCTAVE Allegro, risk management, hospital

Abstrak

Paper ini membahas mengenai penerapan metode *OCTAVE Allegro* untuk melakukan evaluasi risiko-risiko keamanan informasi pada instansi kesehatan yang telah menerapkan teknologi informasi. Evaluasi dilakukan pada RSUD XYZ dan merujuk pada lima area yaitu: reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dan kesehatan, serta denda dan penalti. Hasil penelitian menunjukkan bahwa reputasi dan kepercayaan pelanggan memberikan hasil penilaian risiko paling tinggi. Keseluruhan penyajian dan pembahasan yang ada dalam penelitian ini dipastikan tidak melanggar kode etik bagi RSUD XYZ.

Kata kunci: keamanan informasi, *OCTAVE Allegro*, manajemen resiko, rumah sakit

1. Pendahuluan

Penggunaan teknologi informasi dalam bidang kesehatan khususnya pada instansi rumah sakit merupakan suatu hal penting dan tidak dapat dipisahkan dari proses bisnisnya. Akan tetapi, selama penggunaan dan implementasi teknologi informasi tersebut dapat dimungkinkan timbulnya berbagai risiko yang dapat mengancam keberlangsungan proses bisnis. Pengelolaan terhadap kemungkinan munculnya berbagai risiko ini merupakan hal yang perlu diperhatikan. Salah satu langkah awal rumah sakit dalam mengelola risiko-risiko ini yakni melakukan upaya pengukuran terhadap risiko teknologi informasi (penilaian risiko).

Rumah Sakit Umum Daerah XYZ merupakan sebuah instansi perawatan kesehatan yang pelayanannya disediakan oleh dokter spesialis, perawat, dan tenaga ahli kesehatan lainnya. Dalam menjalankan proses bisnisnya, Rumah Sakit Umum Daerah ini menggunakan sistem informasi terkomputerisasi, namun rumah sakit belum pernah melakukan pengukuran risiko terhadap teknologi informasinya dan belum menerapkan manajemen risiko. Untuk meminimalisir risiko-risiko yang mungkin terjadi di masa mendatang, Rumah Sakit Umum Daerah XYZ perlu melakukan pengukuran atau evaluasi terhadap sistem tersebut.

Pengukuran dimaksudkan agar berbagai risiko pada teknologi informasi rumah sakit dapat diminimalisir dan diatasi. Lalu setelah dilakukan pengukuran maka dapat diketahui besarnya ancaman dan kerentanan dari setiap informasi data yang dinilai kritis, sehingga dapat diterapkan kontrol yang tepat dengan memprioritaskan informasi yang paling berharga bagi perusahaan serta resiko dan ancaman yang paling besar. Dengan begitu, Rumah Sakit Umum Daerah XYZ dapat terus melakukan pengembangan manajemen sumber daya manusia dan peningkatan kualitas pelayanan kepada pasien.

Diterima Redaksi : 25-11-2017 | Selesai Revisi : 22-12-2017 | Diterbitkan Online : 16-04-2018

Dalam penelitian ini, diangkat suatu rumusan permasalahan mengenai langkah-langkah dalam menganalisis manajemen risiko sistem informasi keamanan data rumah sakit. Adapun batasan masalah yang terdapat dalam penelitian ini adalah (a) Penelitian difokuskan pada operasional bisnis yang berhubungan dengan penerapan teknologi informasi pada Rumah Sakit yang mencakup uji data, infrastruktur, hardware, software, jaringan, aplikasi, dan juga karyawan dan (b) Evaluasi manajemen risiko keamanan informasi diukur menggunakan metode *Octave Allegro*.

Melalui kegiatan penelitian ini, diharapkan akan diperoleh hasil analisis penilaian manajemen risiko keamanan informasi bagi Rumah Sakit Umum Daerah XYZ dapat digunakan untuk mengetahui risiko-risiko yang terjadi sehingga dapat dijadikan panduan untuk menyempurnakan penerapan teknologi informasi secara keseluruhan. Disamping itu, penelitian juga memberikan alternatif solusi dari risiko yang telah ditemukan untuk mengurangi terjadinya kerugian dalam bidang teknologi informasi yang mungkin terjadi pada Rumah Sakit Umum Daerah XYZ. Penelitian ini juga dapat dijadikan sebagai bahan acuan bagian peneliti selanjutnya berkaitan manajemen risiko keamanan informasi Rumah Sakit.

2. Tinjauan Pustaka

Berdasarkan latar belakang permasalahan terkait dengan risiko yang dimungkinkan dapat terjadi pada instansi kesehatan atau rumah sakit, dilakukan beberapa tinjauan pada pustaka terkait mengenai keamanan sistem informasi, manajemen dan penilaian risiko, serta metode *Octave Allegro* sebagai komponen utama dalam penelitian ini.

2.1 Keamanan Sistem Informasi

Keamanan informasi mengacu pada proses dan metodologi yang dirancang dan dilaksanakan untuk melindungi informasi elektronik atau bentuk lainya yang bersifat rahasia, informasi pribadi serta data yang sensitif dari akses yang tidak sah, penyalahgunaan, pengungkapan, perusakan dan modifikasi serta gangguan. Prinsip utama keamanan informasi terdiri dari *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan) atau sering disingkat CIA [1] seperti tampak pada Gambar 1.

Dalam konsep keamanan informasi, kita mengenal istilah ancaman (*threats*) yang merupakan setiap peristiwa yang jika terjadi, dapat menyebabkan kerusakan pada sistem dan membuat hilangnya kerahasiaan, ketersediaan, atau integritas. Ancaman dapat menjadi berbahaya, seperti modifikasi yang disengaja terhadap informasi penting seperti dalam perhitungan transaksi atau penghapusan file.

Gambar 1. Prinsip Utama Keamanan Informasi

Ancaman memiliki korelasi dengan kerentanan (*vulnerability*), yakni kelemahan dalam sistem yang dapat dieksploitasi oleh ancaman tersebut. Upaya mengurangi aspek kerentanan dari sistem dapat mengurangi risiko ancaman pada sistem.

2.2 Manajemen Risiko dan Penilaian Risiko

Manajemen risiko secara umum merupakan proses dengan tujuan mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan peluang yang tediri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus menerus dalam pengambilan keputusan dan peningkatan kinerja [2]. Bahwa manajemen risiko merupakan proses memungkinkan manajer IT untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi [3]. Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, yang merupakan suatu proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko [4].

Tujuan utama melakukan analisis risiko adalah untuk mengukur dampak dari potensi ancaman, menetukan berapa besar kerugian yang diderita akibat hilangnya potensi bisnis[1]. Dua hasil utama dari analisis risiko diantaranya adalah identifikasi risiko dan jumlah biaya berbanding manfaatnya untuk penanggulangan risiko kerusakan. Standar ISO/ISEC 17799 telah mendefinisikan penilaian risiko sebagai sebuah pertimbangan yang sistematis dari (a) Hal yang membahayakan bisnis yang mungkin merupakan akibat dari kegagalan keamanan, dengan mempertimbangkan konsekuensi potensial dari hilangnya kerahasiaan, integritas atau ketersediaan informasi dan aset lainnya. (b) Mencegah kemungkinan kegagalan yang terjadi dengan cara menggali informasi ancaman dan kerentanan yang ada dan kontrol yang diterapkan saat ini.

Terdapat beberapa jenis metode yang umum digunakan dalam kegiatan penilaian risiko. Pada Gambar 2 berikut ditampilkan perbandingan antar metode-metode yang

biasanya digunakan untuk melakukan penilaian risiko[1]. Salah satu metode tersebut adalah metode OCTAVE, yang akan digunakan lebih lanjut dalam pembahasan penelitian ini.

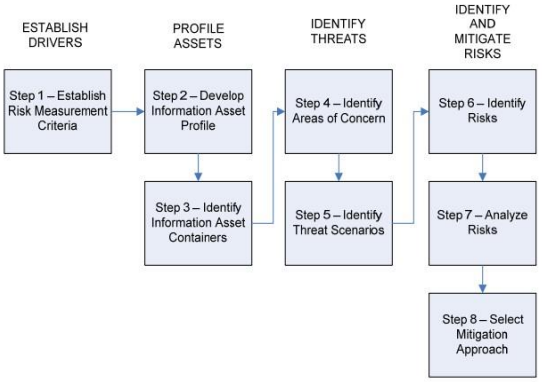
Attributes / Methods	Risk identification	Risk Analysis	Risk Evaluation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only) (information assessed in June 2006)	Size of organization	Skills needed[a]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	••	•	•	•••	•••	•••	•••	DE	Free	All	**	N	N	Prototype (free of charge)
Cramm	•••	•••	•••					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	•••	•••	•••					NL	Free	All	*	N	N	
Ebios	•••	•••	•••	•••	•••	•••	•••	EN, FR, DE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	•••	•••	•••	•••	•••	•••	•••	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	••	••	••	••	•••	•••	•••	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	•				•			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001					•	•		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	•••	•••	•••	•••	•••	•••	•••	EN, DE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	•••	•••	•••					EN, FR	Not free	Large	*	N	N	
Mehari	•••	•••	•••					EN, FR	€100-500	All	**	N	N	RISICARE
Octave	••	••	••	••	••	••	••	EN	Free	SME	**	N	N	
SP800-30 (NIST)	•••	•••		•••	•••	•••		EN	Free	All	**	N	N	

Gambar 2. Perbandingan Metode Penilaian Risiko

2.3 Metode OCTAVE Allegro

OCTAVE merupakan suatu metodologi yang digunakan untuk mengidentifikasi dan mengevaluasi risiko keamanan informasi [5]. Saat ini, terdapat tiga varian OCTAVE yang bisa digunakan [6], [7], yaitu: *OCTAVE method*, *OCTAVE-S*, dan *OCTAVE Allegro*. Penelitian ini menerapkan metode *OCTAVE Allegro* dikarenakan tujuan yang ingin dicapai oleh *OCTAVE Allegro* adalah penilaian yang luas terhadap lingkungan risiko operasional suatu organisasi dengan tujuan menghasilkan hasil yang lebih baik tanpa perlu pengetahuan yang luas dalam hal penilaian risiko. Pendekatan ini berbeda dari pendekatan OCTAVE, dimana *OCTAVE Allegro* lebih berfokus terhadap aset informasi dalam konteks bagaimana mereka digunakan, dimana mereka disimpan, dipindahkan, dan diolah, dan bagaimana mereka terkena ancaman, kerentanan, dan gangguan sebagai hasil yang ditimbulkan.

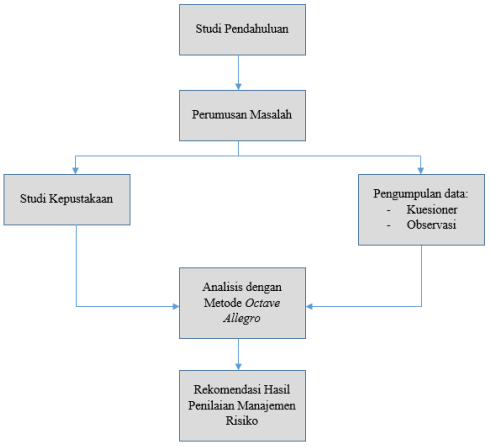
Penerapan metode *OCTAVE Allegro* terdiri atas 8 (delapan) langkah utama yang disajikan pada Gambar 3. Penelitian mengimplementasikan seluruh metode mulai dari langkah ke-1 (*establish risk measurement criteria*) hingga langkah ke-7 yaitu menganalisis risiko (*analyze risks*) yang ada pada Rumah Sakit Umum Daerah XYZ. Langkah ke-8 untuk upaya mitigasi masih memerlukan pengembangan berikutnya yang memerlukan persetujuan lebih lanjut dari pihak Rumah Sakit yang bertindak sebagai mitra.



Gambar 3. Langkah Metode *Octave Allegro*

3. Metodologi Penelitian

Kegiatan penelitian ini dilakukan dengan alur seperti tertera pada Gambar 4. Kegiatan diawali dengan studi pendahuluan dan perumusan awal masalah yang ada pada Rumah Sakit Umum Daerah XYZ. Selanjutnya, dilakukan pengumpulan data dan observasi untuk meninjau keamanan informasi dari Rumah Sakit dengan menggunakan langkah-langkah yang diterapkan dari metode *Octave Allegro*. Langkah-langkah secara mendetail akan dijelaskan pada masing-masing sub-bab berikutnya.



Gambar 4. Alur Penelitian

3.1 Membangun Kriteria Pengukuran Risiko

Langkah ini memiliki dua aktivitas, yaitu diawali dengan membangun *organizational drivers* yang digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* yang paling penting. Aktivitas pertama yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas kedua adalah memberikan nilai prioritas *impact area* menggunakan *Impact Area Ranking Worksheet*.

3.2 Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi yang dilanjutkan dengan upaya penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat yaitu mengumpulkan informasi mengenai *information asset* yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam adalah membuat deskripsi aset informasi kritis tersebut. Aktifitas tujuh mengisi kebutuhan keamanan sesuai dengan aspek *confidentiality*, *integrity* dan *availability*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

3.3 Mengidentifikasi *Container* dari Aset Informasi

Hanya ada satu aktivitas yang merujuk pada tiga poin penting terkait dengan keamanan dan konsep dari *container of information asset* yaitu mengidentifikasi cara aset informasi dilindungi. Tiga poin penting tersebut adalah tingkat perlindungan atau pengamanan aset informasi dan kerentanan serta ancaman terhadap *container* dari aset informasi.

3.4 Mengidentifikasi Area Masalah

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. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat *area of concern*. Berpedoman pada dokumen *Information Asset Risk Worksheet* selanjutnya dilakukan review dari *container* untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

3.5 Mengidentifikasi Skenario Ancaman

Aktivitas pertama yang ada pada langkah kelima ini yaitu melakukan identifikasi skenario ancaman tambahan (dapat menggunakan *Threat Scenarios Questionnaries*). Aktivitas kedua adalah melengkapi *Information Asset Risk Worksheets* untuk setiap scenario ancaman yang umum.

3.6 Mengidentifikasi Risiko

Aktivitas yang ada pada langkah ke-enam adalah menentukan *threat scenario* yang telah didokumentasikan di *Information Asset Risk Worksheets* yang dapat memberikan dampak bagi organisasi.

3.7 Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada Information Asset Risk Worksheets. Aktivitas satu dimulai dengan melakukan review risk measurement criteria dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan

3.8 Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas kedua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut. Langkah kedua memerlukan bentuk koordinasi lebih lanjut dengan pihak manajemen Rumah Sakit Umum Daerah XYZ.

4. Hasil dan Pembahasan

Tahapan Penilaian Risiko dengan Metode *Octave Allegro* pada Rumah Sakit Umum Daerah XYZ, mengacu pada 8 langkah OCTAVE Allegro yang telah dibahas pada bab Metodologi Penelitian. Pada bab ini, diberikan hasil penelitian yang dapat ditampilkan. Keterbatasan penjabaran hasil dan studi kasus merupakan didasarkan pada upaya penulis untuk menaati kode etik penyebaran informasi yang telah disetujui bersama dengan Rumah Sakit yang menjadi mitra dalam penelitian berikut.

Berikut ditampilkan pembahasan hasil yang didapat dari masing-masing langkah yang ada dalam metode.

4.1 Hasil Langkah 1: Membangun Kriteria Pengukuran Risiko

Dalam langkah 1, ada dua aktivitas yaitu penentuan *impact area* dan penentuan skala prioritas pada impact area yang telah ditentukan. Dari lima *impact area* yang ditentukan (reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dan kesehatan, dan denda dan penalti), diperoleh hasil sebagai berikut:

a. *Impact area - Reputasi dan kepercayaan pelanggan*
   Dampak terhadap reputasi dan kepercayaan pelanggan dikategorikan *high* (tinggi) jika reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki. Dampak terhadap kerugian pelanggan dikategorikan *high* (tinggi) jika terjadi lebih dari 12% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan.
b. *Impact area - Finansial*
   Dampak terhadap biaya operasional dikategorikan *high* (tinggi) jika terjadi peningkatan lebih dari 12% pada biaya operasional per tahun Dampak terhadap *revenue loss* dikategorikan *high* (tinggi) jika terjadi lebih dari 12% per tahun *revenue loss*. Dampak yang terjadi terhadap one-time *financial loss* dikategorikan high (tinggi) jika terjadi lebih dari Rp.120.000.000,-

c. *Impact area - Produktivitas*
Dampak terhadap jam kerja karyawan dikategorikan *high* (tinggi) jika jam kerja karyawan meningkat lebih dari 12% dari 7 sampai dengan 14 hari
d. *Impact area - Keamanan dan Kesehatan*
Dampak terhadap kehidupan dikategorikan *high* (tinggi) jika terjadi hilangnya nyawa pasien atau karyawan. Dampak terhadap kesehatan dikategorikan *high* (tinggi) jika terjadi penurunan permanen dari kesehatan pasien atau karyawan. Dampak terhadap Keselamatan dikategorikan *high* (tinggi) jika keselamatan pasien atau karyawan terganggu.
e. *Impact area - Denda dan Penalti*
Denda dikategorikan *high* (tinggi) jika bernilai lebih dari Rp.120.000.000,- . Tuntutan Hukum dikategorikan *high* (tinggi) jika tuntutan dengan nilai lebih dari Rp.120.000.000,- akan dikenakan kepada RSUD XYZ. Investigasi dikategorikan *high* (tinggi) jika pemerintah atau organisasi investigasi lainnya akan memulai penyelidikan yang lebih mendalam terhadap praktek RSUD tersebut terkait dengan tuntutan.

Dari kelima *impact area* tersebut, reputasi dan kepercayaan pelanggan merupakan prioritas yang paling pertama diikuti yaitu oleh finansial, denda dan penalti, produktivitas, serta keamanan dan kesehatan.

4.2 Hasil Langkah 2: Mengembangkan *Information Asset Profile*

Aset informasi yang telah diidentifikasikan yaitu profil dokter, profil karyawan, profil pasien, jadwal praktek dokter, transaksi pembayaran pasien, data laboratorium. Ada tiga kebutuhan keamanan, yaitu *confidentiality*, *integrity*, dan *availability*. Dari profil aset informasi ini, kebutuhan keamanan yang paling penting, mayoritas terletak pada *integrity*. Hal ini dikarenakan aset informasi harus dapat dipertanggungjawabkan kebenarannya untuk digunakan dalam berbagai kegiatan operasional di RSUD XYZ.

4.3 Hasil Langkah 3: Identifikasi *Information Asset Containers*

Information asset container terbagi menjadi tiga, yaitu *technical*, *physical*, dan *people* dimana masing-masing mempunyai sisi internal dan eksternal. Dari hasil analisis terhadap 9 *critical asset information*, yang paling banyak mempunyai *container* adalah data pasien. Data pasien diakses, disimpan, atau dikirim melalui suatu aplikasi yang digunakan di Rumah Sakit Umum Daerah XYZ tersebut.

4.4 Hasil Langkah 4: Identifikasi *Areas of Concern*

Dikaitkan dengan data pasien yang memiliki *container* paling banyak, maka profil pasien juga mempunyai *area of concern* yang paling banyak. Dari *area of concern* tersebut, hasil analisis menunjukkan bahwa ancaman keamanan yang paling sering adalah *bug/error* pada aplikasi dan pemanfaatan celah keamanan lewat aplikasi baik pihak dalam maupun luar, serta kesalahan saat *deploy* aplikasi.

4.5 Hasil Langkah 5: Identifikasi *Threat Scenarios*

Hasil yang diperoleh dari langkah ke-4 (*areas of concern*) kemudian diperluas menjadi *threat scenario* yang mendetailkan lebih jauh mengenai *property* dari *threat*. *Property* dari *threat* antara lain mencakup *actor*, *means*, *motives*, *outcome*, dan *security requirement* (hasil analisis disajikan pada tabel 1 yang merupakan salah satu contoh *threat scenarios*)

Tabel 1.Analisis *Threat Scenario* pada Data Pasien RSUD XYZ

Property and threats	
Actor	Staff RSUD XYZ
Means	Staff menggunakan aplikasi
Motives	Terjadi disebabkan karena *human error* (*accindental*)
Outcome	*Modification, Interruption*
Security Requirements	Penambahan validasi (validasi terhadap data di masing-masing field yang diinput oleh staff)

4.6 Hasil Langkah 6: Identifikasi Risiko

Langkah ini bertujuan untuk menentukan bagaimana *threat scenario* yang telah dicatat dapat memberikan dampak bagi pihak rumah sakit dimulai dengan melakukan pengkajian pada *risk measurement criteria*, fokus terhadap bagaimana definisi dampak *high*, *medium*, dan *low* untuk perusahaan. Kemudian *relative risk score* akan dihitung dan dapat digunakan untuk menganalisa risiko sehingga membantu organisasi untuk memutuskan strategi terbaik dalam menghadapi risiko. Setiap *area of concern* dari tiap information asset yang telah didefinisikan selanjutnya dipertimbangkan terkait konsekuensi yang mungkin terjadi. Konsekuensi tersebut mempunyai *impact area* yang dinilai tingkat value-nya yang kemudian diberikan *score*. *Score* diperoleh melalui perkalian *priority* dengan *value* dari *impact area*. Hasil perhitungan *score* dapat dilihat di Tabel 2.

Tabel 2. *Score per Impact Areas*

Impact Areas	*Priority*	*Low*	*Moderate*	*High*
Reputasi dan kepercayaan pelanggan	5	5	10	30
Finansial	4	4	8	12
Produktivitas	2	2	4	6
Keamanan dan Kesehatan	1	1	2	3
Denda dan Penalti	3	3	6	9

4.7 Hasil Langkah 7: Analisis Risiko

Dari analisis dan pengamatan yang dilakukan, diperoleh hasil rata-rata yang paling besar *score*nya adalah *Impact Area* pertama yaitu reputasi dan kepercayaan pelanggan (*Reputation & Customer Confidence*) dengan hasil penilaian sebesar 12 (*medium*) dengan perbandingan nilai *relative risk score* sebesar 27.

4.8 Hasil Langkah 8: Pemilihan *Mitigation Approach*

Dari pengelompokan risiko yang ada, selanjutnya diambil langkah mitigasi risiko-risiko tersebut. Pembagian pengambilan langkah mitigasi dikelompokkan seperti terlihat pada Gambar 5.

Relative Risk Matrix		
Risk Score		
30 to 45	16 to 29	0 to 15
POOL 1	POOL 2	POOL3

POOL	**Mitigation Approach**
1	Mitigate
2	Defer/Mitigate
3	Accept

Gambar 5. Pengelompokan Langkah Mitigasi Risiko

Proses ini masih memerlukan persetujuan dan koordinasi lebih lanjut. Langkah mitigasi yang direkomendasikan diantaranya adalah membuat peraturan yang tertulis mengenai tanggung jawab dalam menjaga keamanan informasi dan sanksi bagi yang melanggar serta melakukan sosialisasi mengenai peraturan tersebut secara bertahap kepada karyawan Rumah Sakit Umum Daerah XYZ. Selanjutnya membuat simulasi secara visual untuk memudahkan karyawan untuk mengerti bagaimana pentingnya aset informasi, ancaman dan risiko yang mungkin terjadi, serta konsekuensi yang harus mereka hadapi bila terjadi.

5. Kesimpulan

Dari keseluruhan hasil penelitian, dapat ditarik beberapa kesimpulan dan saran sebagai berikut.

5.1 Simpulan

Telah dilakukan upaya evaluasi dengan menerapkan metode *OCTAVE Allegro* pada RSUD XYZ untuk menilai aset infomasi yang sifatnya kritis serta ancaman dan risiko yang mungkin terjadi guna membuat perencanaan pengurangan risiko untuk mengurangi dampak yang mungkin terjadi di masa mendatang. Evaluasi dilakukan pada lima *impact areas* yaitu: reputasi dan kepercayaan pelanggan, finansial, produktivitas, keamanan dan kesehatan, serta denda dan penalti. Hasil penelitian menunjukkan bahwa *impact area* reputasi dan kepercayaan pelanggan (*Reputation & Customer Confidence*) memberikan hasil penilaian analisis risiko tertinggi sebesar 12 (*medium*) dengan perbandingan nilai *relative risk score* sebesar 27. Hal ini berhubungan dengan hasil analisis terhadap *critical asset information*, yang menunjukkan bahwa data yang paling banyak mempunyai *container* adalah data pasien yang merupakan pelanggan pada instansi rumah sakit. Keseluruhan hasil menunjukkan bahwa data-data terkait pelanggan, dalam hal ini adalah pasien, merupakan aset informasi yang bersifat kritis pada RSUD XYZ sehingga membutuhkan upaya perencanaan untuk penanganan dan mitigasi resiko di masa mendatang.

5.2 Saran

Untuk memperoleh kualitas penilaian yang baik, RSUD XYZ dapat melakukan evaluasi keamanan informasi kembali dengan menggunakan *OCTAVE Allegro* secara berkala, misalnya satu tahun sekali.

6. Daftar Rujukan

[1] Krutz, R. L., & Vines, R. D., 2001. *The CISSP prep Guide: Mastering the ten domains of Computer Security* (pp. 183-213). New York: Wiley.

[2] Ross, R. S., 2011. Managing Information Security Risk: Organization, Mission, and Information System View. *Special Publication (NIST SP)-800-39*.

[3] Goguen, A., Stoneburner, G., & Feringa, A., 2017. Risk Management Guide for Information Technology Systems and Underlying Technical Models for Information Technology Security.

[4] Maulana, M. M., & Supangkat, S. H., 2006. Pemodelan Framework Manajemen Risiko Teknologi Informasi untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.

[5] Alberts, C. J., & Dorofee, A., 2002. *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc.

[6] Wheeler, E., 2011. *Security risk management: Building an information security risk management program from the Ground Up*. Elsevier.

[7] Calder, A., & Watkins, S. G., 2010. *Information security risk management for ISO27001/ISO27002*. It Governance Ltd.