SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK I - Surabaya, 26 Juni 2021
Fakultas Teknik Elektro dan Teknologi Informasi ,Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2025.7157

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Analisis dan Penerapan Manajemen Risiko Keamanan Sistem Informasi di RSUD XYZ Menggunakan Metode OCTAVE Allegro

Syafiq Al-Ghiffari[1], Elsa Maya Bahri[2], Reisa Permatasari[3], Agung Brastama Putra[4]

[1,2,3,4]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur

e-mail: 22082010246@student.upnjatim.ac.id

ABSTRACT

The use of information technology is very important for hospital operations, but has risks that can disrupt business continuity if not managed properly. This study aims to assess and manage information security risks at XYZ Hospital using Allegro's OCTAVE framework. The main focus of the study was on critical information assets such as patient data and electronic medical records (EMR), with integrity as the primary security requirement. The results showed that reputation and customer trust were the most crucial risk impact areas, with the highest scores in the risk analysis. The identified threats were classified into three risk levels: high, medium and low, with customized mitigation strategies, such as the implementation of two-factor authentication, data encryption and security training for employees. The implementation of these mitigation strategies is expected to increase the effectiveness of risk management, maintain service continuity, and increase public confidence in the hospital's overall operations.

Keywords: *Risk assessment, information security, OCTAVE Allegro, hospital operations, mitigation strategy*

ABSTRAK

Penggunaan teknologi informasi sangat penting bagi operasional rumah sakit, namun memiliki risiko yang dapat mengganggu kelangsungan bisnis jika tidak dikelola dengan baik. Penelitian ini bertujuan untuk menilai dan mengelola risiko keamanan informasi di RSUD XYZ dengan menggunakan kerangka kerja OCTAVE Allegro. Fokus utama penelitian adalah pada aset informasi penting seperti data pasien dan rekam medis elektronik (EMR), dengan integritas sebagai kebutuhan keamanan utama. Hasil penelitian menunjukkan bahwa reputasi dan kepercayaan pelanggan merupakan area dampak risiko yang paling krusial, dengan skor

tertinggi dalam analisis risiko. Ancaman yang teridentifikasi diklasifikasikan ke dalam tiga tingkat risiko: tinggi, sedang, dan rendah, dengan strategi mitigasi yang disesuaikan, seperti penerapan autentikasi dua faktor, enkripsi data, serta pelatihan keamanan bagi karyawan. Penerapan strategi mitigasi ini diharapkan dapat meningkatkan efektivitas pengelolaan risiko, menjaga keberlangsungan layanan, serta meningkatkan kepercayaan publik terhadap operasional rumah sakit secara keseluruhan.

Kata kunci: Penilaian risiko, keamanan informasi, OCTAVE Allegro, operasional rumah sakit, strategi mitigasi

PENDAHULUAN

Penggunaan teknologi informasi di rumah sakit memiliki peran penting dalam mendukung proses operasional, pelayanan pasien, serta pengambilan keputusan yang lebih efisien dan akurat [3]. Namun, pesatnya digitalisasi dalam layanan kesehatan juga menimbulkan tantangan serius terkait keamanan informasi, khususnya terhadap data pasien yang bersifat sensitif. Tanpa adanya manajemen risiko yang tepat, insiden seperti kebocoran data, akses tidak sah, dan gangguan sistem dapat terjadi dan mengganggu keberlangsungan layanan rumah sakit [4][5].

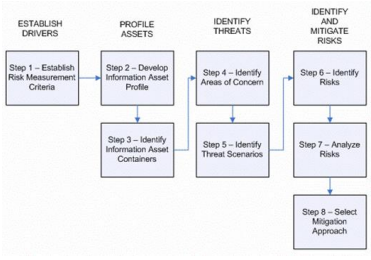
Beberapa penelitian sebelumnya telah membahas pendekatan manajemen risiko informasi di sektor kesehatan. Misalnya, penelitian oleh Smith et al menunjukkan bahwa rumah sakit yang tidak memiliki strategi keamanan informasi yang terstruktur berpotensi mengalami serangan siber yang signifikan[1]. Studi oleh Prasetyo dan Nugroho juga menekankan pentingnya integrasi sistem keamanan informasi berbasis kerangka kerja dalam institusi pelayanan publik, termasuk rumah sakit[2].

Dalam konteks manajemen risiko informasi, kerangka kerja OCTAVE Allegro (Operationally Critical Threat, Asset, and Vulnerability Evaluation) telah digunakan sebagai salah satu pendekatan sistematis yang berorientasi pada aset dan konteks organisasi. Beberapa studi menyebutkan bahwa OCTAVE Allegro efektif dalam mengidentifikasi dan memprioritaskan risiko terhadap aset informasi, terutama pada institusi dengan kompleksitas tinggi seperti rumah sakit[6][7]. Namun, pemanfaatannya di lingkungan rumah sakit di Indonesia masih sangat terbatas, sehingga diperlukan studi kasus aktual untuk mengkaji implementasi dan efektivitasnya secara langsung.

RSUD XYZ saat ini telah menggunakan sistem informasi terkomputerisasi dalam mengelola data pasien dan operasional lainnya. Namun, belum terdapat upaya formal dalam menilai dan mengelola risiko keamanan informasi yang muncul. Dengan mengacu pada kekosongan tersebut, penelitian ini bertujuan untuk menerapkan metode OCTAVE Allegro dalam menilai dan mengelola risiko keamanan informasi di RSUD XYZ. Fokus utamanya adalah pada aset kritis seperti data pasien dan rekam medis elektronik (RME), dengan harapan dapat memberikan kontribusi nyata terhadap peningkatan keamanan dan keberlanjutan operasional rumah sakit.

METODE

Pada kegiatan ini, kami akan menggunakan metode OCTAVE Allegro untuk meninjau keamanan data di Rumah Sakit XYZ. Setiap langkah akan dibahas lebih lanjut dalam subbab berikutnya.



Gambar 1. Langkah - langkah OCTAVE Allegro

A. Langkah 1 – Membangun Kriteria Pengukuran Risiko

Langkah awal ini bertujuan untuk menentukan bagaimana risiko akan diukur dan dievaluasi. Pada RSUD XYZ, tim IT dan manajemen rumah sakit bersama-sama menyusun Risk Measurement Criteria Worksheets yang mencerminkan tujuan strategis organisasi, seperti keberlanjutan pelayanan pasien, kepatuhan terhadap regulasi kesehatan, dan perlindungan privasi pasien. Kriteria yang ditetapkan meliputi area dampak seperti: finansial, hukum, reputasi, operasional, dan keselamatan pasien. Sebagai contoh, risiko yang menyebabkan keterlambatan layanan IGD lebih dari 30 menit dikategorikan berdampak tinggi pada keselamatan pasien.

B. Langkah 2 – Mengembangkan Profil Aset Informasi

Dalam tahap ini, tim mengidentifikasi aset informasi kritis, yaitu; Sistem Informasi Rumah Sakit (SIRS), Database Rekam Medis Elektronik (RME), Server Data Pasien, dan Akses User ke Sistem RME. Setiap aset dianalisis berdasarkan kebutuhan *confidentiality, integrity*, dan *availability* (CIA). Contoh: RME memerlukan tingkat *confidentiality* sangat tinggi, karena berisi informasi medis sensitif yang tidak boleh bocor.

C. Langkah 3 – Mengidentifikasi *container* dari Aset Informasi

Aset informasi tersebut kemudian ditelusuri container-nya, yaitu media atau sistem tempat data berada. Misalnya; RME berada di server lokal yang terhubung dengan jaringan internal, Data juga diakses melalui aplikasi berbasis web. Tim mencatat kerentanan seperti tidak adanya *firewall* yang diperbarui, backup manual, dan akses tidak terenkripsi sebagai potensi risiko terhadap container tersebut.

D. Langkah 4 – Mengidentifikasi Area Masalah

Tim menyusun *Risk Environment Map* berdasarkan hasil wawancara dengan bagian IT dan staf medis. Salah satu *area of concern* yang muncul adalah akses login staf medis yang sering dibagikan antar shift, yang berpotensi menyebabkan penggunaan tidak sah atau penyalahgunaan data.

E. Langkah 5 – Mengidentifikasi Skenario Ancaman

Tim mengembangkan Threat Scenario Worksheets, contohnya; Staf non-medis mengakses data pasien melalui akun login yang dibagikan tanpa izin, Data RME tidak dapat diakses karena server down saat pasien kritis tiba di IGD. Skenario ancaman disusun berdasarkan temuan dan potensi nyata yang sudah pernah terjadi atau dikhawatirkan oleh pihak RSUD..

F. Langkah 6 – Mengidentifikasi Risiko

Setiap skenario ancaman dievaluasi lebih lanjut untuk melihat dampaknya terhadap operasional rumah sakit. Misalnya, jika akses ilegal ke data pasien terjadi, maka konsekuensinya mencakup; Pelanggaran hukum (UU Perlindungan Data Pribadi), Rusaknya kepercayaan pasien, dan Potensi sanksi dari instansi pengawas kesehatan.

G. Langkah 7 – Menganalisis Risiko

Tim menghitung tingkat risiko berdasarkan skor gabungan dari kemungkinan terjadinya dan tingkat dampaknya, mengacu pada *Risk Measurement Criteria*. Contoh analisis; risiko "akses ilegal oleh staf non-medis" memiliki kemungkinan tinggi dan dampak tinggi, sehingga masuk dalam prioritas utama mitigasi.

H. Langkah 8 – Memilih Pendekatan Pengurangan

Berdasarkan hasil analisis, pendekatan mitigasi ditentukan bersama manajemen RSUD XYZ. Contoh langkah mitigasi; Penerapan autentikasi dua faktor untuk akses login sistem RME, Pendidikan berkala tentang keamanan data untuk seluruh staf, dan Audit rutin terhadap log akses pengguna.

HASIL DAN PEMBAHASAN

Pada Bab ini menyajikan temuan penting dari penelitian yang dilakukan pada Rumah Sakit XYZ. Hasil dari studi kasus tersebut dan penjelasan pendekatan OCTAVE Allegro digunakan untuk menilai risiko di rumah sakit. Berikut ini adalah penjelasan tentang hasil dari teknik ini pada setiap tahap.

A. Hasil Langkah 1: Membangun Kriteria Pengukuran Risiko

Tujuan dari langkah ini adalah untuk menciptakan standar pengukuran risiko yang sesuai untuk RSUD XYZ dengan menentukan area dampak dan menetapkan skala prioritas untuk area tersebut. Prosedur ini memastikan bahwa setiap dampak yang mungkin terhadap aset informasi RSUD XYZ dianalisis secara menyeluruh berdasarkan relevansinya dengan tujuan perusahaan.

Tabel 1. Impact Area

Aktivitas	Deskripsi
Penentuan *Impact Area*	Mengidentifikasi *5 impact area* dianggap signifikan dan relevan terhadap RSUD XYZ, meliputi reputasi dan kepercayaan pelanggan, keuangan, produktivitas, keamanan dan kesehatan, serta denda dan hukuman.
Penentuan Skala Prioritas	Memberi peringkat *impact area* berdasarkan seberapa besar dampaknya terhadap organisasi karena menjaga kepercayaan masyarakat, reputasi dan kepercayaan pelanggan sangat penting. Finansial, denda dan hukuman, produktivitas, serta keamanan dan kesehatan adalah prioritas berikutnya.

B. Hasil Langkah 2: Mengembangkan Information Asset Profile

Langkah ini menekankan kebutuhan keamanan: kerahasiaan, integritas, dan ketersediaan dengan integritas sebagai prioritas utama. Aset informasi kritis diidentifikasi berdasarkan aktivitas penting organisasi, seperti data pasien dan rekam medis elektronik (RME), kemudian dicatat dalam lembar kerja informasi aset kritis.

1. Data Pasien : Informasi identitas pasien yang mencakup nama, alamat, nomor telepon, dan riwayat medis.
2. Rekam Medis Elektronik (RME) : Catatan lengkap riwayat medis pasien, termasuk diagnosis, hasil laboratorium, dan pengobatan.

C. Hasil Langkah 3: Identifikasi *Information Asset Containers*

Dengan menggunakan *worksheet Information Asset Risk Environment Map*, contoh RSUD XYZ, dapat mengidentifikasi *information asset container* terbagi menjadi: *technical*, *physical* dan *people*. Setiap kategori memiliki sisi eksternal dan internal. Pada RSUD XYZ Rekam Medis Elektronik untuk mengelola rekam medis pasien yang dikelola oleh Administrasi dan IT, serta Portal Pasien yang memungkinkan pasien mengakses riwayat pemeriksaan dan jadwal janji temu.

D. Hasil Langkah 4: *Identifikasi Areas of Concern*

Dalam studi kasus RSUD XYZ, proses identifikasi *areas of concern* diawali dengan melakukan evaluasi terhadap setiap komponen *container* yang digunakan. Setiap *area of concern* yang ditemukan dicatat secara mendetail, lalu dikembangkan menjadi *threat scenarios* yang relevan.

Tabel 2. *Area of Concern*

No.	Area of Concern	Deskripsi
1.	Akses Tidak Sah ke Data Pasien	Ketika data pasien diakses oleh pihak yang tidak berwenang, ada risiko pelanggaran privasi dan kebocoran data sensitif.

2.	Kegagalan Sistem Rekam Medis	Potensi sistem rekam medis tidak dapat diakses karena masalah perangkat keras, perangkat lunak, atau serangan siber.

E. Hasil Langkah 5: Identifikasi *Threat Scenarios*

Pada langkah ini diperluas menjadi *threat scenario* yang memberikan informasi lebih lanjut. *Property* dari *threat* antara lain mencakup *actor, means, motives, outcome,* dan *security requirement* (hasil analisis disajikan pada tabel 3 yang merupakan salah satu contoh *threat scenarios*).

Tabel 3. *Properties Of Threat*

Area of Concern	***Threat of Properties***		***Medium (2)***	***High (3)***
Akses Tidak Sah ke Data Pasien	***1. Actors**:*	*Insiders (karyawan RS) dan pihak eksternal*	*10*	*15*
	***2. Means**:*	*Penggunaan kredensial curian atau eksploitasi celah sistem*	*8*	*12*
	***3. Motives**:*	*Mencuri data untuk dijual atau disalahgunakan*	*6*	*9*
	***4. Outcome**:*	*Kebocoran data pasien, pelanggaran privasi*	*2*	*3*
	***5. Security Requirements**:*	*Implementasi autentikasi dua faktor, kontrol akses berbasis peran (RBAC), dan monitoring log aktivitas pengguna*	*4*	*6*

F. Hasil Langkah 6: Identifikasi Risiko

Langkah ini bertujuan untuk menilai dampak dari *threat scenario* yang dicatat pada RSUD XYZ, dimulai dengan pengkajian *risk measurement criteria* untuk mendefinisikan dampak *high, medium, dan low*. Selanjutnya, dihitung *relative risk score* untuk menganalisis risiko dan menentukan strategi mitigasi yang tepat. Tabel 4 menunjukkan hasil perhitungan *relative score*.

Tabel 4. Perhitungan Score *Impact Area*

Impact areas	***Priority***	***Low (1)***	***Medium (2)***	***High (3)***
Reputasi dan kepercayaan pelanggan	*5*	*5*	*10*	*15*
Finansial	*4*	*4*	*8*	*12*
Produktivitas	*3*	*3*	*6*	*9*
Keamanan dan Kesehatan	*1*	*1*	*2*	*3*
Denda dan Penalti	*2*	*2*	*4*	*6*

G. Hasil Langkah 7: Analisis Risiko

Dari analisis dan pengamatan yang dilakukan, diperoleh hasil bahwa *impact area* dengan rata-rata skor tertinggi adalah reputasi dan kepercayaan pelanggan dengan nilai penilaian sebesar 10 *(medium)* dan perbandingan *relative risk score* sebesar 29.

H. Hasil Langkah 8: Pemilihan *Mitigation Approach*

Analisis risiko di RSUD XYZ menjadi dasar penyusunan strategi mitigasi disesuaikan dengan kondisi rumah sakit. Tabel 5 pengelompokan langkah mitigasi, sedangkan tabel 6 langkah mitigasi yang disesuaikan.

Tabel 5. *Relative Risk Matrix*

Risk Score	**30 TO 45**	**16 TO 29**	**0 TO 15**
Mitigation Pool	POOL 1	POOL 2	POOL 3

Tabel 6. *Mitigation Approach*

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

KESIMPULAN

Penelitian ini bertujuan memahami manajemen risiko aset informasi di RSUD XYZ menggunakan OCTAVE Allegro. Hasilnya menunjukkan bahwa reputasi dan kepercayaan pelanggan adalah area risiko paling penting, sementara data pasien dan rekam medis elektronik (RME) menjadi aset utama yang membutuhkan integritas untuk mendukung operasi yang andal. Tiga kategori strategi mitigasi risiko dibedakan berdasarkan tingkat risiko: mitigasi terencana untuk risiko menengah, mitigasi langsung untuk risiko tinggi, dan pemantauan berkala untuk risiko rendah. Otentikasi dua faktor, enkripsi data, dan pelatihan keamanan karyawan merupakan strategi mitigasi yang disarankan. Melalui kebijakan mitigasi risiko berbasis analisis yang menyeluruh, penelitian ini membantu Rumah Sakit XYZ dalam mengelola risiko aset informasinya, meningkatkan keamanan dan efektivitas operasional.

DAFTAR PUSTAKA

[1] J. Smith et al., "*Cybersecurity strategies in healthcare: A structured approach," Journal of Cybersecurity in Healthcare,* vol. 8, no. 4, pp. 22–35, 2020.

[2] A. Prasetyo and B. Nugroho, "Pentingnya integrasi sistem keamanan informasi berbasis kerangka kerja dalam institusi pelayanan publik," Jurnal Teknologi Informasi Kesehatan, vol. 10, no. 2, pp. 112–125, 2021.

[3] *Healthcare Information and Management Systems Society (HIMSS), "The Role of Health Information Technology in Improving Patient Care,"* 2020. [Online]. *Available*: https://www.himss.org. [*Accessed: Oct. 2023*].

[4] ISO/IEC 27005, *"Information technology — Security techniques — Information security risk management," International Organization for Standardization*, 2018.

[5] *National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity,"* 2018. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: Oct. 2023].

[6] *L. Zhang et al., "Evaluating the effectiveness of OCTAVE Allegro in high-complexity institutions," International Journal of Information Security, vol. 12, no. 1, pp. 78–92, 2019.*

[7] D. Kurniawan et al., "*Implementing OCTAVE Allegro in Indonesian hospitals: A case study," Journal of Health Information Management*, vol. 15, no. 3, pp. 45–60, 2022.