UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

Analisis Tingkat Keamanan Sistem Informasi Manajemen Rumah Sakit (E-HOS System) Menggunakan Metode OCTAVE

Oleh:

Tasya Rafiiqa

Uce Indahyanti

Manajemen Informasi Kesehatan

Universitas Muhammadiyah Sidoarjo

Juni, 2023

Pendahuluan

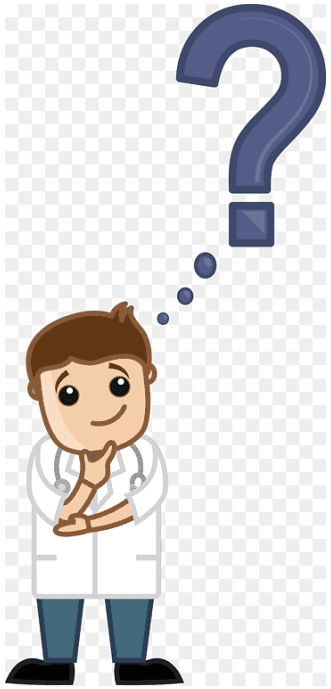
Sistem Informasi Manajemen Rumah Sakit (SIMRS) merupakan bagian wajib dari setiap RS dalam menunjang pelayanan dan operasionalnya.
Regulasi dari PERMENKES Republik Indonesia Nomor 82 Tahun 2013 tentang SIMRS, menetapkan setiap RS melakukan, melaksanakan pengelolaan dan meningkatkan pengembangan SIMRS.

Kualitas sistem RS berkaitan dengan kualitas sistem yang baik, karena keamanan informasi meliputi kerahasiaan (*confidentiality)*, integritas (*integrity)*, dan ketersediaan (*availability)*.
Jika data RS dikelola secara umum tanpa bantuan SIMRS akan mengakibatkan *unintregated data,* redudansi data*, out of date information* dan *human error*.

Keamanan data melindungi terhadap pengungkapan dan modifikasi data. Sistem informasi tentunya memiliki risiko dari faktor manusia, kerusakan sistem dari virus, aliran data dari *hacker*, dll

UU Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, hak asasi manusia yang ditujukan untuk menjamin hak warga negara atas PDP dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya PDP.

Pertanyaan Penelitian (Rumusan Masalah)



Bagaimana RSUD Ibnu Sina Kab. Gresik menggunakan metode OCTAVE untuk menganalisis tingkat keamanan SIMRS (E-HOS System)?

Penelitian Terdahulu (Research Gap)

Penelitian yang dilakukan oleh Rizqi Satria Andhika dkk, di RS Bhayangkara Sespima Polri Jakarta Tahun 2021 :

- Keamanan pada sistem informasi rumah sakit yang masih lemah,
- Pihak RS jarang melakukan audit internal,
- Sistem sering mengalami *error* dan *down*.
- Kesimpulan : Penelitian ini menemukan perlunya perbaikan pada keamanan akses, keamanan komputer dan pembaruan profil risiko.

Penelitian yang dilakukan oleh Ito Setiawan dkk, di RS Wishnu Husada Banyumas Tahun 2020 :

- Mengetahui aset kritis sistem informasi berupa database server dan SIMRS,
- Terdapat kendala pada penerapan SIMRS data yang hilang atau tidak bisa dibuka karena terkena virus, jaringan bermasalah,
- Sistem aplikasi tidak bisa digunakan karena *human error,*
- Standar operasional prosedur masih kurang diterapkan dengan baik, bahkan belum semua memiliki SOP
- Kesimpulan : Belum adanya beberapa standar prosedur di 6 bagian praktek keamanan.

Penelitian yang dilakukan oleh Hakim dkk Tahun 2021 :

- Penerapan teknologi informasi memiliki permasalahan adanya data loss,
- Data *corrupt* dan
- Penyalahgunaan hak akses.

Metode Penelitian

- **Jenis Penelitian**

Penelitian kualitatif dengan pendekatan metode OCTAVE

- **Lokasi dan Waktu Penelitian**

RSUD Ibnu Sina Kab. Gresik
Periode Bulan Desember 2022 – Mei 2023

- **Subjek Penelitian :**

Ka. Unit Teknologi Informatika (TI),
2 Staff TI, dan Pengguna/*user*

- **Objek Penelitian :**

Aplikasi E-HOS System

- **Data Penelitian**

Data Primer : Hasil wawancara & Observasi
Data Sekunder : Jurnal, buku dan informasi yang berhubungan dengan tingkat keamanan simrs menggunakan metode OCTAVE

- **Instrumen Penelitian**

Pedoman wawancara dan *Checklist* observasi

Metode Penelitian

VARIABEL PENELITIAN

- Variabel Independennya ialah Perangkat yang digunakan (*Hardware), E-HOS System (Software), Kualitas Jaringan (Network)*, dan Hak Akses (*User)*
- Variabel Dependen ialah keamanan sistem informasi (E-HOS System).

TEKNIK DAN PENGUMPULAN DATA

- Pengumpulan data menggunakan metode wawancara, observasi dan studi literatur.

PENGOLAHAN DAN ANALISIS DATA

1) Fase pertama, membangun profil ancaman berdasarkan aset dengan mewawancarai pihak IT berdasarkan daftar pertanyaan wawancara yang telah disediakan.
2) Fase kedua, mengidentifikasi terkait kerentanan infrastruktur dengan menentukan komponen kunci dari aset kritis.
3) Fase ketiga, mengembangkan strategi perlindungan dengan melakukan penilaian risiko menggunakan *FMEA* berdasarkan daftar dari kerentanan aset kritis disertai dengan memberikan usulan mitigasi.

Manfaat Penelitian

- **Tujuan Penelitian**

Menganalisis tingkat keamanan simrs (E-HOS System) dengan mengidentifikasi ancaman aset kritis dan kerentanan infrastruktur, melakukan penilaian terhadap risiko serta memberikan rekomendasi mitigasi.

- **Manfaat Penelitian**

Guna mengetahui risiko apa saja yang akan terjadi dan dapat mencegah risiko pada keamanan sistem informasi RSUD Ibnu Sina Gresik.

Hasil dan Pembahasan

❑ **Hasil Langkah Tahap Pertama : Membangun Aset Berbasis Ancaman Profil**

1. Identifikasi Aset Kritis
2. Identifikasi Ancaman

❑ **Hasil Langkah Tahap Kedua : Mengidentifikasi Kerentanan Infrastruktur**

1. Identifikasi Komponen Utama/Kunci
2. Identifikasi Kerentanan Aset
3. Identifikasi Risiko

❑ **Hasil Langkah Tahap Ketiga : Mengembangkan Rencana dan Strategi Keamanan**

1. Penilaian Risiko
2. Klasifikasi Risiko
3. Mitigasi Risiko Menggunakan ISO 27001

Hasil Langkah Tahap Pertama : Membangun Aset Berbasis Ancaman Profil

1. **Identifikasi Aset Kritis Pada Aplikasi E-HOS System**

Melakukan wawancara secara pribadi dengan Ka. Unit TI dan 2 staff TI, menemukan daftar aset penting yang dimiliki oleh pihak TI RSUD Ibnu Sina Kab. Gresik:

Aset Kritis berdasarkan 4 Kategori :

- *Software*

(Aplikasi E-HOS System)

- *Hardware*

(Komputer, Server, AC, Printer, CCTV)

- *Network*

(Kualitas Jaringan)

- *User*

(Pengguna)

2. **Identifikasi Ancaman**

Proses pendeteksian ancaman dilakukan dengan mendefinisikan kejadian berdasarkan terjadinya risiko yang disebabkan oleh faktor eksternal maupun internal:

Aplikasi E-HOS System	→ Pembobolan sistem
Komputer	→ Teserang virus
Server	→ Server down
AC	→ Power failure
Printer	→ *Maintenance* yang kurang
CCTV	→ CCTV rusak
Perangkat Jaringan	→ Kerusakan infrastruktur jaringan
Pengguna	→ Penyalahgunaan hak akses, *Password* PC diketahui orang lain

Hasil Langkah Tahap Kedua : Mengidentifikasi Kerentanan Infrastruktur

1. Identifikasi Komponen Utama/Kunci

Key Classes of Components

(Komponen Kunci)

- Aplikasi E-HOS System
- Komputer
- Server
- Perangkat Jaringan
- Pengguna (*user)*

2. Identifikasi Kerentanan Aset

Kerentanan didefinisikan sebagai keadaan di mana tidak ada tindakan keamanan, kontrol fisik, atau sebaliknya.

- Pembobolan sistem:

(Peretas menyerang aplikasi)

- Teserang virus:

(Membahayakan nilai informasi yang disimpan di komputer)

- Server down:

(Beban kerja server yang tinggi)

- Kerusakan infrastruktur jaringan:

(Sambungan kabel yang tidak memadai)

- Penyalahgunaan hak akses:

(Kurangnya pengetahuan pengguna tentang keamanan)

3. Identifikasi Risiko

Pada tahap ini, ancaman dan kerentanan organisasi dapat dilihat dari dua perspektif. Risiko berupa kejadian yang dapat terjadi atau bahkan sering terjadi dapat disebabkan oleh faktor eksternal dan internal.

No.	Kategori	Asset	Potensial Cause	Risiko
1.	***Software***	Aplikasi E-HOS System	PC terserang virus	*Human* atau *Technician error*
2.	***Hardware***	Komputer	Maintenance yang tidak sesuai dengan protokol	*Hardware failure*
3.		Server	Kerusakan fisik yang terjadi pada server	*Failed backup* data
4.	***Network***	Perangkat jaringan	Kerusakan infrastruktur jaringan	*Network failure*
5.	***User***	Pengguna	Staff tidak logout ketika meninggalkan komputer	Penyalahgunaan hak akses

Hasil Langkah Tahap Ketiga : Mengembangkan Rencana dan Strategi Keamanan

1. Penilaian Risiko

Dilakukan berdasarkan tingkat keparahan (*severity*), kejadian (*occurrence*), dan deteksi (*detection*). Langkah ini menjelaskan lebih rinci informasi risiko yang akan digunakan untuk menghitung parameter *Risk Priority Number* (RPN) menggunakan *Failure Mode & Effect Analysis* (FMEA).

2. Klasifikasi Risiko

Skala	Level
>151	*Very High*
101-150	*High*
51-100	*Medium*
20-50	*Low*
0-19	*Very Low*

Prioritas Risiko

Level	Risiko	Potential Causes	Sev	Occ	Det	RPN
Very High	Penyalah gunaan hak akses	Staff tidak logout ketika meninggalkan komputer	9	9	2	162
High	Human atau Technician error	Kesalahan penginputan dan penghapusan data	9	8	2	144
High	Penyalah gunaan hak akses	Adanya share login	9	7	2	126
High		Kata sandi tidak diubah secara teratur	9	7	2	126

Prioritas risiko yang dipilih adalah risiko dengan nilai level risiko yang sangat tinggi *(very high)* dan tinggi *(high)* karena tingkat risiko ini dapat memiliki dampak kerugian yang signifikan terhadap proses bisnis yang sedang berlangsung.

3. Mitigasi Risiko Menggunakan ISO 27001

Mitigasi risiko adalah tahap pemrosesan risiko, karena faktor risiko yang dipilih berasal dari tahap pertama, yang dievaluasi dengan bantuan langkah-langkah pemrosesan**.** Dalam ISO, ini disebut standar penilaian risiko (*risk assessment*) yang mencakup proses identifikasi risiko. Dari hasil identifikasi dan penilaian risiko, pengendalian objektif standar ISO 27001 berikut direkomendasikan untuk mengelola risiko yang teridentifikasi.

Mitigasi Risiko

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
User: **Pengguna**	Penyalah gunaan hak akses	Staff tidak logout ketika meninggalkan komputer	Pihak yang tidak berkepentingan dapat mengakses informasi penting.	Access Control: (A.9.4) Merupakan kontrol akses sistem dan informasi guna mencegah akses tidak sah ke sistem aplikasi.	Access Control to Program Source Code: (A.9.4.5) Merupakan langkah-langkah untuk membatasi source code yang digunakan.	• Untuk melindungi data penting, organisasi harus mengontrol ketat terkait akses ke kode sumber program. • Untuk memastikan bahwa orang luar tidak dapat mengakses data penting, organisasi menetapkan aktivitas log. • Organisasi membuat peraturan untuk mengontrol akses ke sistem dan aplikasi.

Simpulan

- Terdapat 8 aset kritis dan dikelompokkan menjadi 4 kelas aset berdasarkan kategori *Hardware, Software, Network* dan *User* sehingga diperoleh 1o risiko dengan 17 kejadian risiko pada aset kritis.
- Hasil penilaian risiko yang paling tinggi dengan nilai RPN 162 pada kategori *User* dengan risiko Penyalahgunaan hak akses dan risiko yang paling rendah dengan nilai RPN 15 pada kategori *Network Failure*.
- Untuk mengendalikan risiko, prosedur untuk menangani risikonya dengan standar ISO 27001 yang berfokus pada rekomendasi manajemen risiko, *Access Control, Human Resource Security*, dan *Communications Security*. Sehingga risiko dapat dicegah atau diminamilisir pada area TI RSUD Ibnu Sina Kab. Gresik.

Referensi

[1] D. R. A. Tiorentap, “Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP,” 2020.

[2] R. S. A. Gusni and I. W. W. Pradnyana, “Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit Bhayangkara Sespima Polri Jakarta Menggunakan COBIT 2019,” 2021.

[3] KEMENKES RI, “Peraturan Menteri Kesehatan Republik Indonesia Nomor 1171/Menkes//Per/VI/2011 Tentang Sistem Informasi Rumah Sakit.”

[4] R. I. Menteri Kesehatan, “Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 Tentang Sistem Informasi Manajemen Rumah Sakit.”

[5] S. Nurul, S. Anggrainy, and S. Aprelyani, “Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review SIM),” vol. 3, no. 5, 2022.

[6] R. I. Presiden, “Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.”

[7] R. S. A. Gusni, “Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit XYZ Menggunakan Cobit 2019 (Studi Kasus pada Rumah Sakit XYZ)”.

[8] P. I. Listyorini and I. Sintya, “Sistem Keamanan SIMRS Di Rumah Sakit”.

[9] R. I. Kepala Arsip Nasional, “Peraturan Arsip Nasional Republik Indonesia Nomor 15 Tahun 2021 Tentang Sistem Manajemen Keamanan Informasi Di Ligkungan Arsip Nasional Republik Indonesia.”

[10] K. Aswar and M. H. R. Hafizh, “Empirical study on organizational performance: the moderating effect of organizational culture,” *Pressacademia*, vol. 7, no. 3, pp. 287–297, Sep. 2020, doi: 10.17261/Pressacademia.2020.1295.

[11] R. Kurnia, “Analisis Risiko Keamanan Aset Informasi Pada Universitas Bina Darma”.

[12] M. E. Whitman and H. J. Mattord, *Principles of information security*, Fifth edition. Boston, MA: Cengage Learning, 2016.

[13] A. Wiranata, Ade Wiradito, Muhammad Reza Ardhana, and Triase, “Sistem Pengamanan Sistem Informasi Rawat Jalan Di Klinik,” *JINTEKS*, vol. 5, no. 1, pp. 1–6, Feb. 2023, doi: 10.51401/jinteks.v5i1.2238.

[14] D. R. P. Mudiono, S. Hernawati, and S. Bukhori, “Dampak Kualitas Sistem, Pengguna Sistem dan Organisasi dalam Pemanfaatan Kinerja Sistem Informasi Manajemen Rumah Sakit di RSU Dr. H. Koesnadi Bondowoso,” *multijournal*, vol. 1, no. 1, p. 25, Sep. 2018, doi: 10.19184/multijournal.v1i1.8594.

[15] J. A. R. Hakim, “Identifikasi, Penilaian, Dan Mitigasi Risiko Keamanan Informasi Pada Sistem Electronic Medical Record (Studi Kasus : Aplikasi Healthy Plus Modul Rekam Medis Di RSU Haji Surabaya)”.


UMSIDA
DARI SINI PENCERAHAN BERSEMI