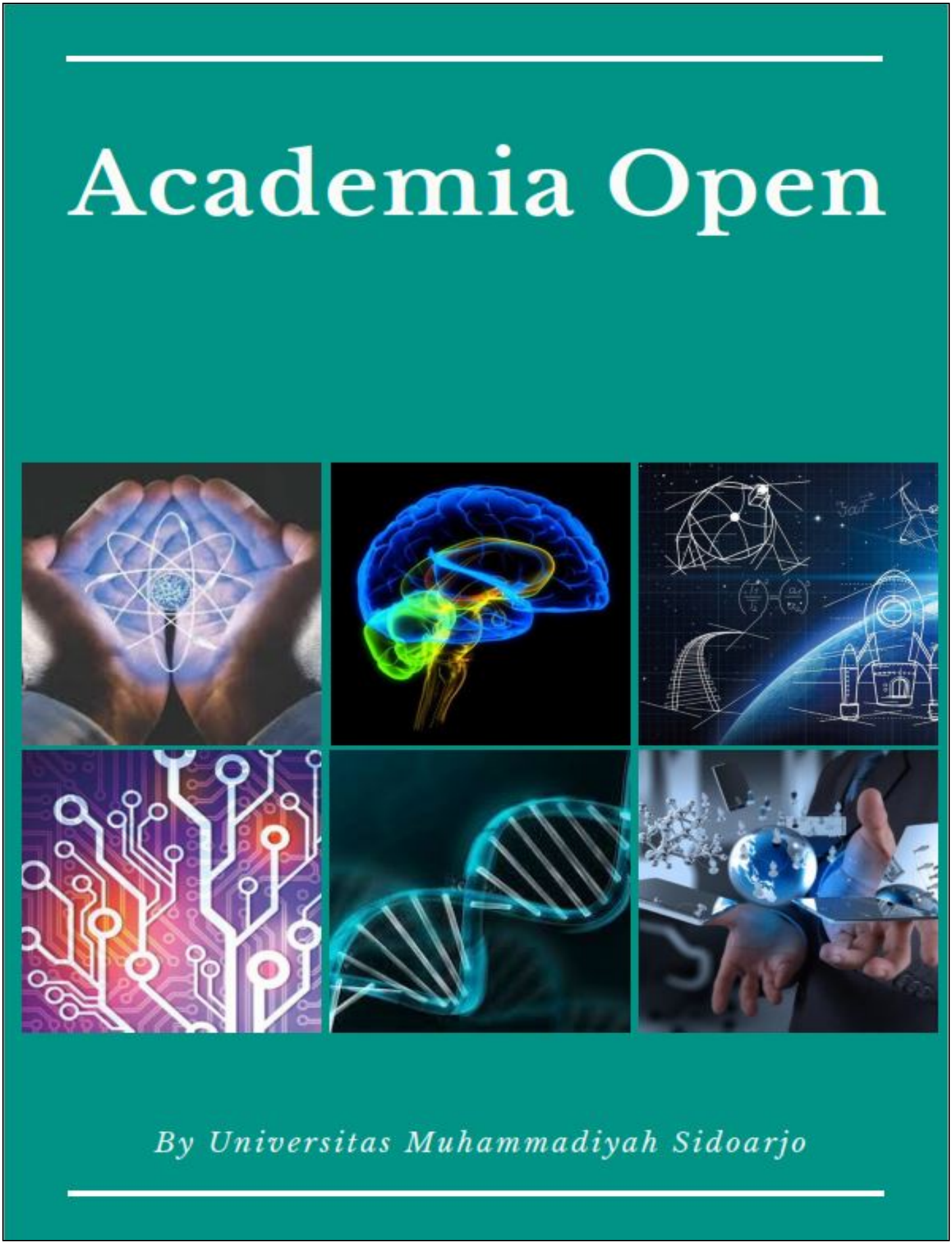
Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

Table Of Content

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)



ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

EDITORIAL TEAM

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

Revolutionizing Hospital IT Security through ISO 27001 Launched in Indonesia

Merevolusi Keamanan TI Rumah Sakit melalui ISO 27001 Diluncurkan di Indonesia

Tasya Rafiiqa, tasyarafiiqa19@gmail.com, (1)
Universitas Muhammadiyah Sidoarjo, Indonesia

Uce Indahyanti, uceindahyanti@umsida.ac.id, (0)
Universitas Muhammadiyah Sidoarjo [https://ror.org/017hvgd88], Indonesia

Umi Khoirun Nisak , umikhoirun@umsida.ac.id, (0)
Universitas Muhammadiyah Sidoarjo [https://ror.org/017hvgd88], Indonesia

(1) Corresponding author

Abstract

This study examines the security of the E-HOS System at RSUD Ibnu Sina Kab. Gresik, identifying critical threats and vulnerabilities, and offering mitigation strategies. Using qualitative methods, including interviews, observations, and documentation, data was collected from December 2022 to May 2023. The OCTAVE framework revealed 17 potential risk events, with user-related risks being the most significant, showing an RPN as high as 162 for access rights abuse. The study recommends implementing ISO 27001 controls—Access Control, Human Resource Security, and Communications Security—to enhance system security. These findings highlight the importance of robust IT security governance in healthcare settings.

Highlight:

1. **Critical Risks:** 17 events, highest risk in user access rights abuse.
2. **Methodology:** Used OCTAVE framework, interviews, observations, documentation.
3. **Recommendations:** Implement ISO 27001 controls: Access Control, HR Security, Communications Security.

Keyword: E-HOS System, SIMRS security, OCTAVE method, risk assessment, ISO 27001

Published date: 2024-05-21 00:00:00

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

Pendahuluan

Pesatnya perkembangan teknologi informasi di berbagai bidang merupakan fenomena umum di era digital saat ini. Salah satunya dibidang kesehatan, dengan penggunaan sistem informasi dalam layanan kesehatan [1]. Sistem Informasi Manajemen Rumah Sakit (SIMRS) merupakan bagian wajib dari setiap RS dalam menunjang pelayanan dan operasionalnya [2]. Sistem informasi digunakan sebagai alat atau metode yang membantu mengolah suatu data atau informasi menjadi suatu keluaran yang lebih informatif yang dapat digunakan sesuai dengan keinginan. Terbitnya Peraturan Menteri Kesehatan Republik Indonesia Nomor 1117/MENKES/PER/VI/2011 tentang Sistem Informasi Rumah Sakit, menimbang bahwa sesuai ketentuan pasal 52 ayat (1) Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit wajib melakukan pencatatan dan pelaporan tentang semua kegiatan penyelenggaraan rumah sakit dalam bentuk SIMRS [3]. Berdasarkan regulasi dari Peraturan Menteri Kesehatan (PERMENKES) Republik Indonesia Nomor 82 Tahun 2013 tentang SIMRS yang menetapkan setiap RS melakukan, melaksanakan pengelolaan dan meningkatkan pengembangan SIMRS [4]. Kualitas sistem RS berkaitan dengan kualitas sistem yang baik, karena keamanan informasi pada hakekatnya meliputi kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) [5]. Berdasarkan Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), bahwasannya PDP merupakan salah satu hak asasi manusia yang ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi [6]. Jika RS lalai akan adanya suatu keamanan pada sistem informasinya, maka risiko keamanan dapat terjadi karena faktor eksternal maupun internal [7]. Data RS untuk mengelolanya cukup besar dan kompleks baik dari segi data pasien maupun data administrasi, sehingga jika dikelola secara umum tanpa bantuan SIMRS akan mengakibatkan unintregated data, redudansi data, out of date information dan human error [8].

Pada pelatihan “Hospital Cyber Security, Bagaimana Menjaga Keamanan Siber pada RS yang sedang Berproses Menuju Digitalisasi” yang dilaksanakan oleh Perhimpunan Rumah Sakit Seluruh Indonesia (PERSI), Country Director Fortinet Indonesia Edwin Lim mengungkapkan serangan siber terhadap sistem informasi manajemen meningkat menjadi 260% pada tahun 2019, karena RS sebagai layanan kesehatan merupakan salah satu tujuan yang sangat penting. Salah satu penyebabnya yakni, ketidakmatangan sistem keamanan dan teknologi informasi, tingginya nilai data keuangan dan data pasien. Berdasarkan Peraturan Arsip Nasional Republik Indonesia Nomor 15 Tahun 2001 tentang Sistem Manajemen Keamanan Informasi bahwa Keamanan Informasi adalah terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi [9]. Aset Informasi adalah aset berupa data atau dokumen, perangkat lunak, aset berwujud dan aset tidak berwujud. Keamanan informasi pada sistem informasi RS sangat berpengaruh sebagaimana dapat mengakibatkan kerugian pada kualitas informasi, data, dan keamanan [10]. Bagi sebuah Institusi informasi ialah aset yang sangat penting, maka perlu diperhatikan secara serius terkait keamanan dan perlindungan terhadap informasi. Keamanan data juga melindungi akses pihak ketiga ke data dan melindungi terhadap pengungkapan dan modifikasi data. Sistem informasi tentunya memiliki risiko dari faktor manusia, kerusakan sistem dari virus, aliran data dari hacker, dan lain-lain. Adanya risiko tersebut menimbulkan kerugian finansial dan non finansial bagi instansi [11]. Oleh karena itu, diperlukan pengukuran tingkat keamanan manajemen risiko yang baik untuk meminimalkan potensi risiko. Bagi suatu instansi aset informasi sangat penting untuk melindungi dari risiko keamanan, komponen dari aset informasi mencakup software, hardware, network, user dan procedures [12].

Rumah Sakit Umum Daerah Ibnu Sina Kab. Gresik telah menerapkan E-HOS System pada tahun 2018. EHOS sendiri merupakan singkatan dari Enterprise Hospital System. E-HOS System yakni, sebuah aplikasi sejenis dengan SIMRS. E-HOS System hanya dapat digunakan secara online melalui web dan hanya staf yang mengimplementasikannya bersama dengan pengelola RSUD Ibnu Sina yang dapat login atau menggunakannya. Berdasarkan hasil studi pendahuluan yang dilakukan di RSUD Ibnu Sina, peneliti menemukan masalah terkait keamanan E-HOS System yakni, masih banyak pegawai yang tidak menghiraukan unit komputernya dalam keadaan menyala saat berangkat atau istirahat, dan masih banyak pegawai yang tidak mempedulikan hak login dan password. Hal ini tentunya membawa risiko oknum yang tidak berwenang menyalahgunakan hak akses, menyebabkan kegagalan pemrosesan data dan pencurian data. Kurangnya perlindungan yang cukup untuk mendukung aspek kemanan, integritas dan kesiapan investigasi juga menjadi ancaman, khususnya di bidang sistem informasi kesehatan [13]. Dengan demikian, penerapan E-HOS System belum optimal sebagaimana masih terdapat masalah yang mengakibatkan penggunaan dan pengorganisasian sistem tidak memenuhi harapan [14]. Penelitian lebih lanjut diperlukan untuk mengidentifikasi ancaman terhadap keamanan sistem informasi kesehatan. Salah satu cara untuk menjamin informasi kesehatan dapat tetap terjaga yaitu dengan menganalisis sistem keamanan (E-HOS System) untuk mengidentifikasi segala celah keamanan pada sistem.

Berdasarkan hasil penelitian yang dilakukan oleh Gusni dkk menyebutkan bahwa, keamanan data berfokus pada tiga hal: kerahasiaan, integritas dan ketersediaan. Sistem informasi memiliki beberapa masalah keamanan, seperti: ketidakcocokan data, keamanan sistem yang lemah, SOP penggunaan sistem tidak dilaksanakan oleh staf, audit internal jarang dilakukan di rumah sakit, dan sering terjadi kesalahan atau kegagalan sistem yang dapat merugikan pasien dan RS [2]. Sedangkan pada penelitian Hakim dkk, dalam penerapan teknologi informasi memiliki permasalahan yakni kehilangan data, korupsi data dan penyalahgunaan hak akses tentu saja menyebabkan terganggunya proses pelayanan RS [15]. Dalam penelitian Setiawan dkk tentang penggunaan sistem informasi, ada beberapa masalah yang muncul. Ini termasuk informasi pasien yang tidak dapat dibaca oleh sistem karena input data yang salah, virus yang membuat informasi hilang atau tidak dapat dibuka, kesalahan manusia yang membuat

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

sistem aplikasi tidak dapat digunakan, dan sistem informasi yang terbatas membuat RS tidak dapat mencapai tujuannya [16].

Berdasarkan data awal yang dilakukan di RSUD Ibnu Sina Kab. Gresik pada bulan Desember 2022 permasalahan yang terjadi didapatkan hasil dari wawancara terhadap Ka. Unit TI (Teknologi Informasi) dan Staf TI diperoleh hasil adanya penyalahgunaan terhadap hak akses. Karena user ID dan password digunakan secara bersamaan pada perangkat yang sama, sulit untuk menentukan siapa yang bertanggung jawab atas kesalahan data sistem. Berkaitan dengan pengguna, sering terjadi kesalahan pada saat memasukkan data pengguna ke dalam sistem, misalnya terjadi kesalahan pada saat memasuki poliklinik yang ditujukan untuk pasien. Pengguna seringkali mengentry double pada saat registrasi sehingga terjadi duplikasi dan mempengaruhi informasi [17]. Hal ini dipengaruhi karena kurangnya tingkat kesadaran user/pengguna terkait keamanan dan pentingnya data yang di entrykan ke dalam sistem informasi. Berdasarkan komponen dari aset informasi, terdapat beberapa aset yang dapat diteliti dikategorikan dalam aset perangkat keras (hardware) yaitu perangkat yang digunakan, perangkat lunak (software) yaitu Aplikasi E-HOS System, jaringan (network) yaitu perangkat jaringan, dan pengguna (user) yaitu hak akses. Hal ini mengakibatkan penggunaan E-HOS System masih belum optimal sebagaimana kondisi tersebut berbanding terbalik dengan tujuan SIMRS dan pengelolaan sistem yang baik, maka munculah sebuah pertanyaan Bagaimana RSUD Ibnu Sina Kab. Gresik menggunakan metode OCTAVE untuk menganalisis tingkat keamanan SIMRS (E-HOS System). Penelitian ini berfokus pada aset kritis yang dimiliki oleh RSUD Ibnu Sina, ancaman dan kerentanan dari aset kritis, serta memberikan strategi perlindungan untuk membantu pihak TI.

Dari permasalahan diatas, peneliti tertarik untuk melakukan penelitian mengenai “Analisis Tingkat Keamanan SIMRS (E-HOS System) Menggunakan Metode OCTAVE” di RSUD Ibnu Sina Kab. Gresik dengan tujuan mengidentifikasi ancaman aset kritis dan kerentanan infrastruktur, melakukan penilaian terhadap risiko serta memberikan rekomendasi mitigasi. Metode yang digunakan untuk menganalisis tingkat keamanan SIMRS Ibnu Sina dalam penelitian ini, yakni OCTAVE (Operationally Critiral Threat, Asset and Vulnerability Evaluation) merupakan sebuah metode yang dikembangkan oleh Carnegie Mellon Software Engineering Institute, Pittsburg [18]. OCTAVE adalah pendekatan yang komprehensif, sistematis dan terarah untuk penilaian risiko keamanan informasi. Metode ini menggunakan 3 fase diantaranya, fase pertama tahap membangun aset berbasis ancaman profil, fase kedua tahap identifikasi kerentanan infrastruktur, dan fase ketiga tahap akhir mengembangkan strategi perlindungan dan rencana mitigasi [19].

Metode

Jenis penelitian ini adalah penelitian kualitatif dengan menggunakan metode OCTAVE untuk mengukur tingkat keamanan simrs (E-HOS System) [20]. Penelitian dilakukan di RSUD Ibnu Sina Kab. Gresik pada bulan Desember 2022 sampai dengan bulan Mei 2023. Variabel penelitian ini berupa aset-aset yang mempengaruhi tingkat keamanan sistem informasi E-HOS System yaitu, hardware, software, network, dan user sebagai variabel independen (bebas), sedangkan keamanan sistem informasi sebagai variabel dependen (terikat). Subjek dalam penelitian ini ialah 4 orang narasumber yang terdiri dari 1 Kepala Unit Teknologi Informasi (TI) dan 2 orang Staff Teknologi Informasi (TI) serta 1 pengguna (user) di RSUD Ibnu Sina Kab. Gresik. Objek yang diteliti ialah aplikasi E-HOS System terkait keamanan SIMRS.

Teknik untuk mengumpulkan data dilakukan dengan studi lapangan menggunakan wawancara, observasi dan dokumentasi. Proses pengumpulan data penelitian ini juga menggunakan studi literatur dengan mengadakan penelahaan pada sumber referensi dari buku, artikel, jurnal dan hasil penelitian serta internet [21]. Data primer diperoleh berdasarkan pada hasil wawancara terkait aset-aset kritis yang digunakan. Data sekunder yang diperlukan seperti jurnal, buku dan data terkait analisis tingkat keamanan simrs menggunakan metode OCTAVE. Instrumen penelitian ini adalah peneliti melakukan wawancara sesuai dengan petunjuk wawancara yang disusun dari daftar pertanyaan yang diajukan kepada informasn dan checklist observasi dengan melihat dan mengamati langsung. Pengolahan dan penganalisisan data pada penelitian ini menggunakan metode OCTAVE. Langkah-langkah tahapan metode OCTAVE ditujukkan di bawah ini: 1) Fase pertama ialah, membangun profil ancaman berdasarkan aset dengan mewawancarai pihak IT berdasarkan daftar pertanyaan wawancara yang telah disediakan 2) Fase kedua yakni, mengidentifikasi terkait kerentanan infrastruktur dengan menentukan komponen kunci dari aset kritis 3) Fase ketiga yaitu, mengembangkan strategi perlindungan dengan melakukan penilaian risiko menggunakan FMEA berdasarkan daftar dari kerentanan aset kritis disertai dengan memberikan usulan mitigasi.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

Figure 1. *Fase OCTAVE*

Desain penelitian ini berupa kerangka acuan sehingga terarah dan sistematis seperti yang ditujukkan pada gambar 2.

Figure 2. *Desain Penelitian*

Berikut ialah paparan mengenai alur tahapan penelitian pada gambar diatas sebagai berikut:

a.Wawancara dan Observasi

Wawancara berisi daftar pertanyaan yang dilakukan berdasarkan hasil 3 (tiga) langkah metode OCTAVE. Sedangkan observasi juga terdapat tabel checklist mengenai aset apa saja yang dimiliki oleh organisasi.

b.Tahap Pertama : Membangun Aset Berbasis Ancaman Profil

Pada tahapan ini dapat menentukan terkait ancaman apa saja yang ada pada E-HOS System dengan penentuan aset kritis.

c.Tahap Kedua : Mengidentifikasi Kerentanan Infrastruktur

Pada tahapan ini dengan menentukan komponen kunci serta mengidentifikasi kerentanan dari aset kritis.

d.Tahap Ketiga : Mengembangkan Strategi Perlindungan dan Rencana Mitigasi

Pada tahapan ini, penilaian risiko dilakukan dengan menggunakan metode FMEA dan rencana mitigasi.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

Hasil dan Pembahasan

Pada hasil dan pembahasan, peneliti menyajikan data yang telah di peroleh melalui penelitian lapangan yang kemudian akan dianalisa berdasarkan teori yang telah dijelaskan diatas. Informasi berikut terdiri dari data primer yang diperoleh dari informasi wawancara dan data sekunder yang diperoleh dari sumber artikel tertulis untuk menguatkan data primer [22]. Permasalahan yang disajikan pada bab ini terkait dengan tingkat keamanan SIMRS (E-HOS System) dengan metode OCTAVE di RSUD Ibnu Sina Kab. Gresik. Wawancara merupakan salah satu metode untuk mendapatkan suatu informasi dari para narasumber mengenai keamanan E-HOS System, sesuai dengan data narasumber penelitian yang menjadi narasumber yakni, ada 4 (empat) orang. Pengumpulan data dilakukan dengan mengajukan pertanyaan kepada 4 narasumber yaitu: 1 Ka. Unit TI, 2 Staff TI, dan 1 pengguna.

Berikut ini dibahas hasil yang diperoleh dari hasil wawancara tentang keamanan sistem informasi pada aplikasi E-HOS System untuk setiap tahapan metode OCTAVE:

A.Proses Analisis Tingkat Keamanan berdasarkan metode OCTAVE

Dalam proses penggalian, analisis tingkat keamanan didasarkan pada tiga (3) langkah metode OCTAVE, yaitu:

Fase	Output
Fase 1 : Membangun Aset Berbasis Ancaman Profil	- Daftar Aset Kritis - Daftar Ancaman berdasarkan Aset Kritis
Fase 2 : Mengidentifikasi Kerentanan Infrastruktur	- Daftar Komponen Utama/Kunci - Daftar Kerentanan Infrastruktur - Daftar Risiko
Fase 3 : Mengembangkan Strategi Perlindungan dan Rencana Mitigasi	- Penilaian Risiko - Strategi Perlindungan - Rencana Mitigasi

Table 1. *Fase - Fase Metode OCTAVE*

a.Hasil Langkah Tahap Pertama : Membangun Aset Berbasis Ancaman Profil

Langkah pertama, aset dan ancaman diidentifikasi dengan mewawancarai tiga. Hal ini diperlukan guna mendapatkan suatu profil aset yang lengkap, karena analisis ini dapat digunakan untuk mengetahui aset mana yang dianggap kritis dan tindakan mana yang telah diambil untuk memastikan keamanan informasi saat ini. Adapun output yang dihasilkan pada fase 1 ini ialah berupa daftar tabel aset kritis dan tabel ancaman aset kritis. Aset kritis adalah item yang bernilai tinggi bagi organisasi. Berikut adalah panduan langkah-langkah untuk membuat profil ancaman dengan mengidentifikasi aset kritis organisasi. Menentukan aset penting dapat dilakukan dengan mengumpulkan informasi tentang aset organisasi, ancaman, kerentanan, dan kelemahan.

1.Identifikasi Aset Kritis Pada Aplikasi E-HOS System

Aset utama dapat diidentifikasi dengan mengumpulkan informasi. Melakukan wawancara secara pribadi dengan Ka. Unit TI dan 2 staff TI, peneliti menemukan daftar aset penting yang dimiliki oleh pihak TI RSUD Ibnu Sina Kab. Gresik serta dapat memastikan bahwa aset tersebut benar-benar dimiliki oleh pihak TI. Tabel berikut menunjukkan hasil identifikasi aset:

No.	Kategori	Aset
1.	Software	Aplikasi E-HOS System
2.	Hardware	Komputer
3.		Server
4.		AC
5.		Printer
6.		CCTV
7.	Network	Perangkat jaringan
8.	User	Pengguna

Table 2. *Aset Kritis*

2.Identifikasi Ancaman

Pada tahapan deteksi ancaman, hal ini ditentukan oleh Ka. Unit TI serta 2 staff TI. Proses pendeteksian ancaman dapat dilakukan dengan mendefinisikan kejadian berdasarkan terjadinya risiko yang disebabkan oleh faktor eksternal maupun internal. Di bawah ini adalah tabel hasil deteksi ancaman:

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

No.	Kategori	Aset	Ancaman
1.	Software	Aplikasi E-HOS System	Pembobolan sistem
2.	Hardware	Komputer/PC	Terserang virus
			Perawatan yang kurang teratur
			Kerusakan pada perangkat atau material
			Penyalahgunaan hak akses
3.		Server	Server down
			Kesalahan konfigurasi dan perawatan server
			Memori server penuh
			Server terserang virus/malware
			Overloaded user
			AC diruangan server mati/rusak
4.		AC	Power failure
			Freon kurang dingin
5. 6.		Printer	Perusakan peralatan
			Maintenance yang kurang
			Korosi, debu
			Pencurian
		CCTV	Hardware mati
			CCTV rusak
7.	Network	Perangkat jaringan	Kerusakan infrastruktur jaringan
			Konektifitas internet menurun
			Koneksi terputus
			Penyadapan informasi celah masuknya hacker
			Kesalahan pengalamatan IP
8.	User	Pengguna	Penyalahgunaan hak akses, Password PC diketahui orang lain
			Kesalahan penginputan dan penghapusan data
			Tidak ada batasan hak akses
			Kesalahan Penggunaan

Table 3. *Identifikasi Ancaman*

b.Hasil Langkah Tahap Kedua : Mengidentifikasi Kerentanan Infrastruktur

Langkah kedua fase ini, kerentanan infrastruktur diidentifikasi dengan evaluasi terhadap komponen kunci dari aset kritis dengan melakukan wawancara langsung kepada Ka. Unit TI dan 2 staff TI. Setelah ditemukan komponen kunci maka akan ditinjau berdasarkan kelemahannya. Komponen kunci ialah suatu komponen yang berperan penting bagi suatu aset dalam memproses serta menyimpan informasi penting.

1.Identifikasi Komponen Utama

Komponen utama adalah elemen kunci guna mendukung aplikasi SIMRS (E-HOS System). Ini dilakukan dengan memilih komponen utama yang mempengaruhi kinerja jaringan sistem komputer. Setiap komponen utama dapat diuji dengan menilai kerentanan perangkat keras dan perangkat lunak, sehingga mengkonfirmasi kerentanan keamanan jaringan dan mengambil tindakan perbaikan. Komponen utama infrastruktur TI aplikasi E-HOS System yaitu:

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

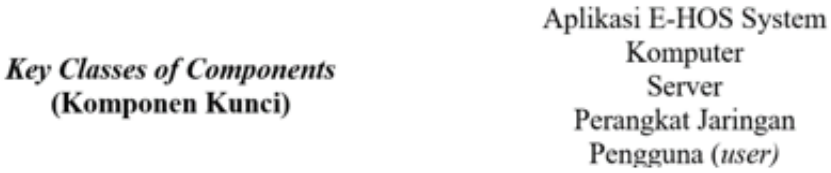


Figure 3. *Komponen Utama/Kunci*

2.Identifikasi Kerentanan Aset

Kerentanan didefinisikan sebagai keadaan di mana tidak ada tindakan keamanan, kontrol fisik, atau sebaliknya. Dengan menggunakan kategori aset kunci dan aset kritis, kerentanan dapat diidentifikasi. Tabel 5 menunjukkan kerentanan aset:

Aset	Ancaman	Kerentanan
Aplikasi E-HOS System	Pembobolan sistem	Peretas menyerang aplikasi
	Kurangnya identifikasi pengguna aplikasi dan mekanisme otentikasi	
	Pengguna kurang memperhatikan pentingnya perlindungan antivirus	Aplikasi terinfeksi virus
Komputer /PC	Terserang virus	Membahayakan nilai informasi yang disimpan di komputer
	Pencurian data	
	Maintenance yang tidak sesuai dengan protokol	Kurangnya perawatan rutin
		Kepekaan terhadap debu, kotoran, dan kelembaban
	Kerusakan pada perangkat atau material	Kurangnya sistem pergantian perangkat keras
	Penyalahgunaan hak akses	Pencurian data medis
Server	Server down	Beban kerja server yang tinggi
		Overloaded user
	Kesalahan konfigurasi dan perawatan server	Backup data setting sebelum melakukan perbaikan
	Ada masalah dengan AC di ruang server, sehingga suhunya sangat tinggi	Korsleting listrik/daya tidak stabil
		Mempengaruhi kecepatan akses data server
	Server lemot	Peningkatan kapasitas data/penyimpanan dalam pemrosesan data
Perangkat Jaringan	Konektifitas internet menurun	Kualitas jaringan buruk
	Kabel LAN digigit tikus	Pemasangan kabel acak (tanpa perlindungan)
	Kerusakan infrastruktur jaringan	Sambungan kabel yang tidak memadai
	Penyadapan informasi celah masuknya hacker	Saluran percakapan tidak aman
		Arsitektur jaringan yang kurang aman
	Kesalahan pengalamatan IP	Sumber daya manusia yang tidak kompeten
Pengguna	Penyalahgunaan hak akses, Password PC diketahui orang lain	Kurangnya pengetahuan pengguna tentang keamanan
	Penyalahgunaan aplikasi	
	Kesalahan entry dan penghapusan data	Pengguna kurang teliti
	Pengolahan data illegal Kesalahan Penggunaan Perangkat yang digunakan tidak sah	Kurangnya pengetahuan tentang mekanisme pengawasan Kekurangan dokumentasi tentang cara menggunakan sistem Kurangnya

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

		pelatihan peningkatan keamanan Kurangnya pedoman tentang penggunaan peralatan telekomunikasi yang benar

Table 4. *Kerentanan Aset*

3.Identifikasi Risiko

Sebelum melanjutkan penilaian risiko, pertama perlu dilakukan identifikasi risiko yang dapat membahayakan nilai informasi RSUD Ibnu Sina Kab. Gresik. 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
			Tidak ada pergantian password secara berkala	Penyalahgunaan hak akses
2.	Hardware	Komputer	Maintenance yang tidak sesuai dengan protokol	Hardware failure
			Kurangnya pengamanan organisasi	Pencurian informasi atau media penting
3.		Server	Kerusakan fisik yang terjadi pada server	Failed backup data
			Server terlalu panas	
			Penyimpanan server tidak memenuhi persyaratan (penyimpanan penuh)	Memori full
4.	Network	Perangkat jaringan	Keamanan informasi yang lemah dari sistem TI internal	Serangan hacker
			Kegagalan jaringan pada penyedia layanan	Network failure
			Kerusakan infrastruktur jaringan	
			Kesalahan mengonfigurasi titik akses	
5.	User	Pengguna	Kesalahan penginputan dan penghapusan data	Human atau Technician error
			Adanya share login	Penyalahgunaan hak akses
			Tidak ada peraturan yang mengatur keamanan data	
			Staff tidak logout ketika meninggalkan komputer	
			Kata sandi tidak diubah secara teratur	
			Pemrosesan data karyawan yang melanggar hukum	Perusakan dan pencurian basis data
			Kurangnya sosialisasi melalui peraturan dan	Melanggar aturan atau regulasi yang

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

			sanksi	berlaku

Table 5. *Identifikasi Risiko*

c.Hasil Langkah Tahap Ketiga : Mengembangkan Strategi Perlindungan dan Rencana Mitigasi

1.Strategi Perlindungan

Berdasarkan hasil analisis yang telah dilakukan terhadap metode OCTAVE pada langkah kesatu dan langkah kedua, langkah selanjutnya adalah menentukan perancangan strategi keamanan dan penerapannya. Dimana dalam perancangannya dilakukan kesesuaian dengan dokumen Standar Manajemen Keamanan Informasi (SMKI) berdasarkan ISO 27001:2013. Sehingga menghasilkan sebuah rencana mitigasi yang terarah terhadap kebutuhan pengamanan aset-aset penting instansi.

2.Penilaian Risiko

Berdasarkan hasil risiko yang telah di identifikasi, pada tahap ini dilakukan penentuan penilaian risiko yang 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) berdasarkan tingkat keparahan, kejadian dan deteksi. Untuk menentukan risiko dengan skor tertinggi dan terendah, proses penilaian risiko menggunakan Failure Mode & Effect Analysis (FMEA). Hasil penilaian risiko ini digunakan untuk memprioritaskan risiko yang akan dibuat rekomendasinya terlebih dahulu [23].

Metode FMEA pertama kali dikeluarkan akhir tahun 1940-an di dunia militer oleh US Armed Forces. FMEA merupakan suatu metode yang digunakan untuk mengidentifikasi dan memahami sepenuhnya kemungkinan mode kegagalan dan penyebabnya, serta efek kegagalan pada sistem [24]. FMEA memprioritaskan masalah dengan menilai risiko yang terkait dengan mode kegagalan yang teridentifikasi, efek dan penyebab, serta tindakan korektif sesuai dengan tingkat penilaian. Tujuan dari metode FMEA ialah untuk mengambil tindakan dalam meminimalisir kegagalan, yang dimulai dengan konsekuensi tertinggi. Adapun langkah-langkah dari pembuatan FMEA hanya mengambil langkah ketiga dan keempat sebagaimana mengidentifikasi potensi kegagalan yang dapat terjadi pada tiap proses severity, occurrence and detection serta menghitung RPN merupakan nilai yang digunakan untuk menentukan prioritas dari risiko/kegagalan [23].

a.Severity, Occurrence dan Detection

Severity adalah peringkat yang terkait dengan seberapa besar kemungkinan sebuah efek akan gagal. Menilai seberapa besar efek dari suatu kegagalan terhadap komponen, sistem, subsistem ke depannya. Occurrence adalah kemungkinan kesalahan dalam menggunakan sistem. Sedangkan Detection adalah ukuran kemampuan untuk mengontrol potensi kesalahan [24]. Menurut tingkat keseriusan, kejadian dan deteksi dinilai pada skala 1 sampai 10. Di bawah ini adalah perhitungan nilai yang diberikan Ka. Unit TI dan Staff TI pada tingkat keparahan, kejadian dan deteksi sebagai berikut:

Risiko	Potential Causes	Sev	Occ	Det	RPN	Level
Hardware failure	Perawatan yang tidak teratur	5	5	2	50	Low
Network failure	Kegagalan jaringan pada penyedia layanan	8	4	2	64	Medium
	Kerusakan infrastruktur jaringan	8	1	3	24	Low
	Kesalahan mengonfigurasi titik akses	5	1	3	15	Very Low
Failed backup data	Kerusakan fisik pada server	9	1	2	18	Very Low
	Server terlalu panas	8	2	2	32	Low
Human atau Technician error	PC terserang virus	9	2	2	36	Low
	Kesalahan	9	8	2	144	High

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

	penginputan dan penghapusan data					
Serangan hacker	Keamanan informasi yang lemah dari sistem TI internal	5	1	3	15	Very Low
Penyalah gunaan hak akses	Adanya share login	9	7	2	126	High
	Tidak ada peraturan yang mengatur keamanan data	7	1	3	21	Low
	Staff tidak logout ketika meninggalkan komputer	9	9	2	162	Very High
	Kata sandi tidak diubah secara teratur	9	7	2	126	High
Melanggar aturan atau regulasi yang berlaku	Kurangnya sosialisasi melalui peraturan dan sanksi	7	2	4	56	Medium
Perusakan dan pencurian basis data	Pemrosesan data karyawan yang melanggar hukum	9	1	3	27	Low
Memori full	Penyimpanan server tidak memenuhi persyaratan (penyimpanan penuh)	7	2	2	28	Low
Pencurian informasi atau media penting	Kurangnya pengamanan organisasi	9	2	2	36	Low

Table 6. *Risk Assessment*

3.Klasifikasi Risiko

Dalam proses ini, daftar risiko disusun menurut hasil perhitungan RPN tertinggi dan terendah. RPN didasarkan pada nilai koefisien tingkat keparahan, kejadian dan deteksi. Rumus RPN: S x O x D. Tabel 8 berikut menunjukkan skala RPN:

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

Table 7. *Skala RPN*

Tabel 7 menunjukkan bahwa skor risiko tertinggi berada pada level RPN very high yaitu 162 yang merepresentasikan risiko penyalahgunaan hak akses, dan risiko terendah pada level RPN very low yaitu 15 yang merepresentasikan risiko network failure. Hasil penilaian dibagi menjadi 5 tingkatan penilaian risiko yaitu, sangat tinggi, tinggi, sedang, rendah, dan sangat rendah. Berikut hasil RPNnya:

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 9 No 2 (2024): December
DOI: 10.21070/acopen.9.2024.7052 . Article type: (Medicine)

a)Tingkat sangat tinggi memiliki 1 (satu) risiko jika RPN >151.

b)Tingkat tinggi memiliki 3 (tiga) risiko jika RPN antara 101-150.

c)Tingkat sedang memiliki 3 (tiga) risiko jika RPN antara 51-100.

d)Tingkat rendah memiliki 8 (delapan) risiko jika RPN antara 21-50.

e)Tingkat sangat rendah memiliki 3 (tiga) risiko jika RPN antara 0-20.

Tujuan identifikasi risiko dan penilaian risiko selanjutnya adalah untuk mengurangi risiko setelah aset diidentifikasi berdasarkan profil ancaman [25]. Upaya perbaikan dilakukan sesuai standar ISO 27001.

4.Mitigasi Risiko Menggunakan ISO 27001

Pada tahapan ini, membuat rekomendasi manajemen risiko berdasarkan hasil prioritas risiko dari nilai RPN diatas [26]. 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.

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

Table 8. *Prioritas Risiko*

Mitigasi risiko adalah tahap pemrosesan risiko, karena faktor risiko yang dipilih berasal dari tahap pertama, yang dievaluasi dengan bantuan langkah-langkah pemrosesan. Adapun usaha yang dilakukan oleh pihak RSUD Ibnu Sina Kab. Gresik yakni, dengan melakukan monitoring dan evaluasi keamanan data dan informasi setiap 6 bulan sekali berlangsungan dengan kegiatan sosialisasi kepada pengguna/user. Mitigasi dilakukan melalui diskusi langsung dengan pihak TI dan penerapan standar di RSUD Ibnu Sina Kab. Gresik. Standar yang digunakan untuk membuat mitigasi ialah ISO 27001. Dalam ISO, ini disebut standar penilaian risiko (risk assessment) yang mencakup proses identifikasi risiko [27]. Dari hasil identifikasi dan penilaian risiko, pengendalian objektif standar ISO 27001 berikut direkomendasikan untuk mengelola risiko yang teridentifikasi. Berikut merupakan hasil rekomendasi mitigasi risiko ditujukkan pada tabel di bawah ini:

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 meninggal kan 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 lan gkah-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.

Table 9. *Mitigasi Risiko*

User: Pengguna	Human atau Technician Error	Kesalahan penginputan dan penghapusan data	· Kehilangan data · Data Termanipulasi	Human Resource Security: (A.7.2) Merupakan pemilihan karyawan yang cocok terhadap tanggung jawab yang diberikan.	Disciplinary Process: (A.7.2.3) Merupakan aturan yang dibuat oleh organisasi tentang keamanan informasi.	· Mengkomunikasikan kepada karyawan untuk memenuhi tanggung jawab tugas mereka terkait keamanan informasi di tempat kerja. · Organisasi harus memberi tahu seluruh karyawan mengenai aturan keamanan informasi. · Selama proses pengolahan data, log aktivitas.
User: Pengguna	Penyalah gunaan hak akses	Adanya share login	Semua orang mengetahui informasi penting.	Communications Security: (A.13.2) Merupakan pembatasan transfer informasi yang dilakukan oleh organisasi.	Information Transfer Policies and Procedure: (A.13.2.1) Merupakan kebijakan, prosedur dan kontrol transfer yang harus dilindungi dari entitas internal dan eksternal organisasi.	· Pengguna diminta untuk menandatangani guna memastikan bahwa password pribadi mereka tidak diketahui oleh orang lain. · Organisasi harus membatasi transfer informasi, baik di dalam maupun di luar organisasi.
Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
User: Pengguna	Penyalah gunaan hak akses	Kata sandi tidak diubah secara teratur	Hak akses disalahgunakan oleh orang lain.	Access Control: (A.9.4) Merupakan kontrol akses sistem dan informasi guna mencegah akses tidak sah ke sistem	Password Management System: (A.9.4.3) Merupakan prosedur terkait dengan pembuatan password.	· Password yang dibuat harus unik. · Password tidak boleh disimpan di sistem yang tidak dilindungi. · Organisasi

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

				aplikasi.		harus membuat peraturan yang mengatur akses ke sistem dan aplikasi.

Table 10.

Simpulan

Berikut ini adalah beberapa kesimpulan berdasarkan hasil penelitian: (1) Proses identifikasi risiko, mengidentifikasi 5 aset kritis yang digunakan di organisasi TI RSUD Ibnu Sina Kab.Gresik dan dikelompokkan menjadi 4 kelas aset dan diperoleh 10 risiko dengan 17 kejadian risiko yang dihadapi pada aset kritis. Oleh karena itu, ada beberapa kejadian risiko karena penyebab yang berbeda. Risiko yang paling banyak adalah user/pengguna terkait dengan risiko penyalahgunaan hak akses, total 5 (lima) kejadian risiko. (2) Dalam penilaian kesiapan dan kematangan keamanan teknologi informasi di RSUD Ibnu Sina Kab. Gresik, ada beberapa bagian penilaian dan masing-masing nilai dihasilkan. Nilai RPN 162 menunjukkan risiko yang sangat tinggi dalam kategori user/pengguna di mana terdeteksi penyalahgunaan hak akses, dan RPN 15 menunjukkan risiko yang sangat rendah dalam kategori risiko network failure. (3) Berdasarkan hasil penilaian risiko dan identifikasi, diterapkan perlakuan untuk mengendalikan risiko tersebut. Prosedur untuk menangani semua risiko tersebut terkait dengan standar ISO 27001, yang berfokus pada standarisasi Security Information Management Systems (ISMS). Untuk prioritas risiko yang teridentifikasi, terdapat 3 kontrol dalam ISO 27001 yang dapat digunakan sebagai acuan dalam menentukan rekomendasi manajemen risiko yaitu, Access Control, Human Resource Security dan Communications Security. Hasil evaluasi ISO 27001 menunjukkan bahwa penyalahgunaan hak akses, human atau technician error memiliki nilai tertinggi. Oleh karena itu, tata kelola keamanan teknologi informasi harus dilakukan. Jika ada rencana mitigasi keamanan TI yang memenuhi beberapa kekurangan dari hasil evaluasi yang bestatus belum ada atau belum diterapkan, maka rencana ini akan dimasukkan ke dalam perencanaan. Sehingga, nilai skor akhir dapat berkurang menjadi status kesiapannya membutuhkan perbaikan, atau berstatus baik sesuai dengan ISO 27001.

References

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, pp. 2022.
6. P. Republik Indonesia, “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 Lingkungan 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.
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.
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.
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).”
16. I. Setiawan, M. Sutopo, and A. Azis, “Manajamen Risiko SIMRS Menggunakan Metode OCTAVE-S dan Standar Pengendalian ISO/EIC 2700,” vol. 7, no. 3, 2020.
17. E. Oktaviana, W. H. N. Putra, and A. Rachmadi, “Evaluasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) RSUD Gambiran Kediri Menggunakan Framework Human, Organization, And Technology-Fit (HOT-FIT) Model.”

18. C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, “Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0:,” Defense Technical Information Center, Fort Belvoir, VA, Jun. 1999.
19. F. Husaini, A. Ambarwati, and L. Junaedi, “Analisis Risiko Aset TI Menggunakan Metode OCTAVE Pada SWD Resto,” 2019.
20. R. Pratama, D. Syamsuar, and Y. N. Kunang, “Evaluasi Risiko Keamanan Informasi Menggunakan Octave-S.”
21. B. A. Thalha Alhamid, “Resume: Instrumen Pengumpulan Data.” 2019.
22. W. K. Mohi, N. Sahi, and F. A. Mootalu, “Kualitas Pelayanan Administrasi Berdasarkan Pelaksanaan Sistem Informasi Manajemen Rumah Sakit (SIMRS) Pada Pelayanan Pasien Di RSUD Dr. MM Dunda Limboto Kabupaten Gorontalo,” vol. 01, no. 01, 2022.
23. F. A. Anshori, “Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten).”
24. Y. Ramayani, “Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA),” ISI, vol. 7, no. 2, p. 289, Nov. 2022.
25. R. F. Hamzah, I. D. Jaya, and U. M. Putri, “Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X,” JSF, vol. 6, no. 1, pp. 55–65, Jun. 2020.
26. W. A. P. Rima Dias Ramadhani, “Perancangan Contigency Planning Disaster Recovery Unit Teknologi
27. A. R. Riswaya, A. Sasongko, and A. Maulana, “Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks KAMI untuk Persiapan Standar SNI ISO/IEC 27001 (Studi Kasus: STMIK Mardira Indonesia)”.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo