

**MANAJEMEN RISIKO KEAMANAN SIBER SIMRS RSUD ULIN
BANJARMASIN MENGGUNAKAN PENDEKATAN NIST
CYBERSECURITY FRAMEWORK**

SKRIPSI

Diajukan untuk Memenuhi Salah Satu Syarat
Sarjana Strata-1 Teknologi Informasi

Oleh:

MUHAMMAD AMMARIN IHSAN

NIM.2010817210002



**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS LAMBUNG MANGKURAT
2024**

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

SKRIPSI PROGRAM STUDI S-1 TEKNOLOGI INFORMASI

Manajemen Risiko Keamanan Siber SIMRS RSUD Ulin Banjarmasin menggunakan Pendekatan NIST Cybersecurity Framework

Oleh

Muhammad Ammarin Ihsan (2010817210002)

Telah dipertahankan di depan Tim Penguji pada 01 Juli 2024 dan dinyatakan

LULUS

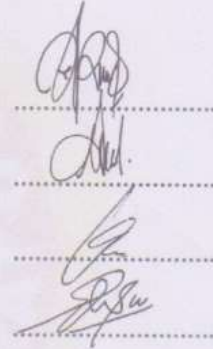
Komite Penguji :

Ketua : Nurul Fathanah Mustamin, S.Pd., M.T.
NIP. 199110252019032018

Anggota 1 : Muti'a Maulida, S.Kom., M.T.I.
NIP. 198810272019032013

Anggota 2 : Muhammad Bahit, S.Kom., M.Eng
NIP. 198904162024211002

Pembimbing Utama : Ir. Eka Setya Wijaya, S.T., M.Kom.
NIP. 198205082008011010



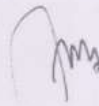
Banjarbaru, ...09 JUL 2024
Diketahui dan disahkan oleh:

Wakil Dekan Bidang Akademik
Fakultas Teknik ULM,



Dr. Mahmud, S.T., M.T.
NIP. 197401071998021001

Koordinator Program Studi
S-1 Teknologi Informasi,



Andrevan Rizky Baskara, S.Kom., M.Kom.
NIP. 199307032019031011

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini,

Nama : Muhammad Ammarin Ihsan
NIM : 2010817210002
Fakultas : Teknik
Prodi : Teknologi Informasi
Judul Tugas Akhir : Manajemen Risiko Keamanan Siber SIMRS
RSUD Ulin Banjarmasin menggunakan pendekatan NIST Cybersecurity Framework
Pembimbing Utama : Ir. Eka Setya Wijaya, S.T., M.Kom.

Dengan ini saya menyatakan bahwa dalam Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar akademik di suatu perguruan tinggi, dan sepanjang pengetahuan saya, juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar rujukan.

Banjarmasin, 21 Juni 2024

Penulis,



Muhammad Ammarin Ihsan

LEMBAR PERSETUJUAN SKRIPSI

PERSETUJUAN SKRIPSI

MANAJEMEN RISIKO KEAMANAN SIBER SIMRS RSUD ULIN
BANJARMASIN MENGGUNAKAN PENDEKATAN NIST CYBERSECURITY
FRAMEWORK

OLEH
MUHAMMAD AMMARIN IHSAN
NIM.2010817210002

Telah diperiksa dan terpenuhi semua persyaratan akademik, administrasi, dan
disetujui untuk dipertahankan di hadapan dewan penguji

Banjarmasin, 21 Juni 2024

Pembimbing Utama,



Ir. Eka Setya Wijaya, S.T., M.Kom.

NIP. 198205082008011010

ABSTRAK

Temuan *Miningware* pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) Rumah Sakit Umum Daerah (RSUD) Ulin Banjarmasin menyoroiti perlunya evaluasi implementasi keamanan siber. Penelitian ini bertujuan untuk menerapkan manajemen risiko keamanan siber berdasarkan kerangka kerja NIST Cybersecurity Framework (NIST CSF) dan kontrol keamanan siber dari NIST SP 800-53. Metode yang digunakan meliputi observasi dan wawancara, studi literatur, identifikasi kerentanan menggunakan ZAP, identifikasi profil keamanan menggunakan NIST CSF, dan analisis kontrol dengan NIST SP 800-53 rev. 5 berdasarkan profil *Ransomware*. Melalui analisis menyeluruh, penelitian ini mengidentifikasi dan menilai risiko yang ada pada sistem tersebut menggunakan ZAP dan meninjau sejauh mana SIMRS telah mengimplementasikan langkah-langkah keamanan sesuai dengan lima fungsi utama dalam NIST CSF: *Identify, Protect, Detect, Respond, dan Recover*. Hasil penelitian ini menunjukkan temuan kerentanan pada SIMRS yaitu satu tipe kerentanan risiko tingkat tinggi dengan sembilan temuan, tiga tipe kerentanan risiko tingkat sedang dengan tiga temuan, dan tiga tipe kerentanan risiko tingkat rendah dengan 163 temuan. Sementara itu, tingkat implementasi keamanan siber menurut penilaian *Maturity Indicator Levels* dari Facility Cybersecurity Framework pada SIMRS rata-rata berada di bawah angka satu, mengindikasikan kebutuhan mendesak untuk peningkatan lebih lanjut. Rekomendasi kontrol yang disesuaikan dengan NIST SP 800-53 berdasarkan profil *Ransomware* disertakan untuk membantu memperkuat profil keamanan NIST CSF yang digunakan oleh RSUD Ulin Banjarmasin.

Kata Kunci: Keamanan Siber, Manajemen Risiko Keamanan Siber, NIST Cybersecurity Framework, NIST SP 800-53, Sistem Informasi Manajemen Rumah Sakit.

ABSTRACT

The findings of Miningware on the Hospital Management Information System (SIMRS) at Ulin Banjarmasin Regional General Hospital (RSUD) highlight the need for evaluating the implementation of cybersecurity. This study aims to implement cybersecurity risk management based on the NIST Cybersecurity Framework (NIST CSF) and cybersecurity controls from NIST SP 800-53. The methods used include observation and interviews, literature review, vulnerability identification using ZAP, security profile identification using NIST CSF, and control analysis with NIST SP 800-53 rev. 5 based on the Ransomware profile. Through thorough analysis, this study identifies and assesses the existing risks in the system using ZAP and reviews the extent to which SIMRS has implemented security measures in accordance with the five main functions of NIST CSF: Identify, Protect, Detect, Respond, and Recover. The results of this study indicate findings of vulnerabilities in SIMRS, including one type of high-risk vulnerability with nine findings, three types of medium-risk vulnerabilities with three findings, and three types of low-risk vulnerabilities with 163 findings. Meanwhile, the level of cybersecurity implementation according to the Maturity Indicator Levels assessment from the Facility Cybersecurity Framework in SIMRS averages below one, indicating an urgent need for further improvement. Control recommendations tailored to NIST SP 800-53 based on the Ransomware profile are included to help strengthen the NIST CSF security profile used by RSUD Ulin Banjarmasin.

Keywords: *Cybersecurity, Cybersecurity Risk Management, Hospital Management Information System, NIST Cybersecurity Framework, NIST SP 800-53.*

KATA PENGANTAR

Dengan penuh rasa syukur dan terima kasih, Saya memanjatkan puji dan syukur kepada Allah SWT, Tuhan Yang Maha Pengasih dan Maha Penyayang, atas segala nikmat dan rezeki yang telah diberikan kepada kita. Segala cita-cita dan harapan Saya menjadi lebih mudah tercapai dan bermanfaat bagi banyak orang. Tidak lupa Saya kirimkan sholawat dan salam kepada junjungan kita, Nabi Besar Muhammad SAW, yang telah membimbing kita ke jalan yang benar. Berkat anugerah dan karunia-Nya, Saya berhasil menyelesaikan skripsi dengan judul: “Manajemen Risiko Keamanan Siber SIMRS RSUD Ulin Banjarmasin menggunakan pendekatan NIST Cybersecurity Framework”. Skripsi ini disusun sebagai syarat untuk memperoleh gelar sarjana Strata-1 Teknologi Informasi dari Fakultas Teknik, Universitas Lambung Mangkurat, Banjarmasin. Pada kesempatan ini, Saya ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Ketua Program Studi Teknologi Informasi Bapak Andreyan Rizky Baskara, S.Kom., M.Kom. yang telah memberikan arahan dan solusi dalam penyelesaian skripsi.
2. Bapak Prof. Juhriyansyah Dalle, S.Pd., S.Si., M.Kom., Ph.D. selaku Dosen Pembimbing Akademik Saya, yang telah memberikan waktu, bimbingan, dan arahan dalam proses perkuliahan Saya.
3. Bapak Eka Setya Wijaya, S.T., M.Kom. selaku Dosen Pembimbing Utama Skripsi Saya, yang telah memberikan petunjuk, arahan, meluangkan waktu, dan bimbingan dalam penyelesaian skripsi ini.
4. Staf di Instalasi SIMRS RSUD Ulin Banjarmasin yang memberikan data-data terkait sehingga memudahkan penulisan dalam menyelesaikan Skripsi.
5. Dosen-dosen beserta staff di Program Studi Teknologi Informasi yang telah mengarahkan dan teman-teman yang membantu dalam proses penyelesaian skripsi.
6. Orang tua dan keluarga di rumah yang telah memberikan dorongan, motivasi, serta doa demi kelancaran penyelesaian skripsi saya.

Sebagai penutup, Saya ingin menyampaikan terima kasih kepada semua pihak yang telah membantu Saya dalam menyelesaikan skripsi ini. Harapan Saya, isi dari

skripsi ini dapat memberikan manfaat, baik untuk diri Saya sendiri, teman-teman, maupun para pembaca. Saya juga sangat mengharapkan masukan dan kritik yang konstruktif untuk peningkatan dan perbaikan skripsi ini. Semoga skripsi ini bermanfaat bagi para pembaca dan semua pihak yang memerlukannya.

Banjarmasin, 21 Juni 2024
Penulis



Muhammad Ammarin Ihsan

DAFTAR ISI

HALAMAN SAMPUL	i
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN	iv
LEMBAR PERSETUJUAN SKRIPSI.....	v
ABSTRAK.....	vi
ABSTRACT.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	5
BAB II TINJAUAN PUSTAKA.....	6
2.1 Landasan Teori.....	6
2.1.1 SIMRS RSUD Ulin Banjarmasin	6
2.1.2 Manajemen Risiko Keamanan Siber.....	9
2.1.3 NIST Cybersecurity Framework.....	10
2.1.4 ZAP.....	12
2.1.5 Facility Cybersecurity Framework	14
2.1.6 NIST SP 800-53 Rev 5.....	15
2.2 Penelitian Terkait	16
2.2.1 Manajemen Risiko Serangan Siber Menggunakan Framework NIST Cybersecurity di Universitas ZXC.....	16

2.2.2	Perancangan Kerangka Kerja Keamanan Siber menggunakan NIST Cybersecurity Framework dan CIS Controls	17
2.2.3	Security Audit for Vulnerability Detection and Mitigation of UPT Integrated Laboratory (ILab) ITERA Website Based on OWASP...18	
2.2.4	Developing an Abstraction Framework for Managing and Controlling Saudi Banks' Cybersecurity Threats Based on the NIST Cybersecurity Framework and ISO/IEC 27001	18
2.2.5	Manajemen Risiko Sistem Informasi Mengacu pada NIST SP 800-30 dan NIST SP 800-53 rev.5	19
2.2.6	Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping	20
2.3	Kerangka Pemikiran.....	24
BAB III METODOLOGI PENELITIAN.....		25
3.1	Alat dan Bahan Penelitian.....	25
3.2	Lokasi dan Objek Penelitian	26
3.3	Prosedur Penelitian	26
3.3.1	Identifikasi Masalah dan Tujuan	27
3.3.2	Studi Literatur	28
3.3.3	Menentukan Prioritas dan <i>Scope</i>	28
3.3.4	<i>Orient</i>	28
3.3.5	Menentukan Profil Saat ini (<i>Current Profile</i>)	29
3.3.6	Membuat Profil Target	33
3.3.7	Menentukan dan Menganalisa Prioritas <i>Gap</i>	33
3.3.8	Membuat Dokumen Rencana Manajemen Risiko	34
3.3.9	Kesimpulan	34
BAB IV HASIL DAN PEMBAHASAN.....		35
4.1	Prioritas dan <i>Scope</i>	35
4.2	Orientasi	35
4.3	Menentukan Profil Saat Ini	37
4.3.1	Identify	42
4.3.2	Protect	45

4.3.3	Detect	47
4.3.4	Respond.....	49
4.3.5	Recover	51
4.4	Menentukan Profil Target	53
4.5	Menentukan dan Menganalisa Prioritas Gap	53
4.6	Membuat Dokumen Rencana Manajemen Risiko	57
BAB V KESIMPULAN DAN SARAN.....		59
5.1	Kesimpulan	59
5.2	Saran	60
DAFTAR PUSTAKA		61
LAMPIRAN.....		66

DAFTAR TABEL

Tabel 2.2 Penelitian Terkait.....	21
Tabel 3.1 Skala jawaban penentuan profil saat ini.....	30
Tabel 4.1 Temuan kerentanan menggunakan ZAP.....	35
Tabel 4.2 Total sub-kategori yang tingkat implementasinya di bawah largely Implemented dan dipetakan terhadap profile Ransomware.....	54

DAFTAR GAMBAR

Gambar 1.1 Temuan <i>MiningPool Malware</i> dalam <i>server SIMRS</i>	2
Gambar 2.1 Topologi jaringan yang terhubung pada publik.....	6
Gambar 2.2 Tampilan SIMRS fitur pendaftaran pasien baru.....	7
Gambar 2.3 Tampilan SIMRS fitur RME	8
Gambar 2.4 Tampilan SIMRS fitur kasir	8
Gambar 2.5 Tampilan SIMRS fitur E-Resep	9
Gambar 2.6 Ukuran data pada <i>database backup SIMRS</i>	9
Gambar 2.7 Perbandingan komponen standar dan <i>framework</i> keamanan siber ...	10
Gambar 2.8 Perbandingan metode dalam mengontrol berbagai jenis ancaman ...	11
Gambar 2.9 Kriteria WASSEC.....	13
Gambar 2.10 Hasil evaluasi menggunakan WASSEC untuk setiap WVS.....	13
Gambar 2.11 Perbandingan nilai rata-rata WASSEC untuk setiap WVS.....	13
Gambar 2.12 Deteksi kerentanan ZAP dan Skipfish pada WAVSEP.....	14
Gambar 2.13 Deteksi kerentanan ZAP dan Skipfish pada DVWA	14
Gambar 2.14 Kelompok kontrol NIST SP 800-53	15
Gambar 2.15 Struktur kontrol NIST SP 800-53	16
Gambar 2.16 Kerangka Pemikiran.....	24
Gambar 3.1 Prosedur Penelitian.....	26
Gambar 3.2 Langkah untuk mendeteksi kerentanan	29
Gambar 3.3 Tampilan contoh proses penentuan profil saat ini	31
Gambar 3.4 Tampilan hasil <i>assessment</i> profil berdasarkan fungsi NIST CSF	32
Gambar 3. 5. Syarat MIL pada fungsi <i>Identify</i>	32
Gambar 3. 6. Tampilan hasil <i>assessment</i> profil berdasarkan kategori dari fungsi <i>Identify</i>	33
Gambar 4.1. Proses <i>assessment</i> profil NIST CSF	37
Gambar 4.2. Sub-kategori 1 kategori <i>Business Environment</i>	38
Gambar 4.3. Hasil tingkat implementasi fungsi NIST CSF	38
Gambar 4.4. Bagan Pie hasil <i>assessment</i> berdasarkan Fungsi NIST CSF	39
Gambar 4.5. Syarat capaian MIL	40
Gambar 4.6. Hasil jawaban kategori <i>Business Environment</i> fungsi <i>Identify</i>	41

Gambar 4.7. Hasil <i>assessment</i> pada fungsi Identify	42
Gambar 4.8. Syarat sub-kategori yang dibutuhkan terhadap MIL pada fungsi <i>Identify</i> dan hasil kondisi implementasi saat ini.....	43
Gambar 4.9. Hasil tingkat implementasi pada kategori fungsi Identify	44
Gambar 4.10. Tingkat implementasi yang tercapai pada fungsi <i>Identify</i>	44
Gambar 4.11. Syarat sub-kategori yang dibutuhkan terhadap MIL pada fungsi <i>Protect</i> dan hasil kondisi implementasi saat ini	46
Gambar 4.12. Hasil tingkat implementasi pada kategori fungsi <i>Protect</i>	46
Gambar 4.13. Tingkat implementasi yang tercapai pada fungsi <i>Protect</i>	47
Gambar 4.14. Syarat sub-kategori yang dibutuhkan terhadap MIL pada fungsi <i>Detect</i> dan hasil kondisi implementasi saat ini	48
Gambar 4.15. Hasil tingkat implementasi pada kategori fungsi <i>Detect</i>	48
Gambar 4.16. Tingkat implementasi yang tercapai pada fungsi <i>Detect</i>	49
Gambar 4.17. Syarat sub-kategori yang dibutuhkan terhadap MIL pada fungsi <i>Respond</i> dan hasil kondisi implementasi saat ini	50
Gambar 4.18. Hasil tingkat implementasi pada kategori fungsi <i>Respond</i>	50
Gambar 4.19. Tingkat implementasi yang tercapai pada fungsi <i>Respond</i>	51
Gambar 4.20. Syarat sub-kategori yang dibutuhkan terhadap MIL pada fungsi <i>Recover</i> dan hasil kondisi implementasi saat ini.....	52
Gambar 4.21. Hasil tingkat implementasi pada kategori fungsi <i>Recover</i>	52
Gambar 4.22. Tingkat implementasi yang tercapai pada fungsi <i>Recover</i>	53
Gambar 4.23. Sampul dokumen rencana manajemen risiko.....	57

DAFTAR LAMPIRAN

Lampiran 1 Transkrip Wawancara Pra Penelitian	67
Lampiran 2 Kuesioner Identifikasi Profil Saat ini	69
Lampiran 3 Pemetaan Rekomendasi Kontrol NIST SP 800-53	73
Lampiran 4 Surat Pernyataan Kesiediaan Calon Pembimbing	79
Lampiran 5 Lembar Konsultasi Proposal.....	80
Lampiran 6 Lembar Persetujuan Proposal	81
Lampiran 7 Rekomendasi ZAP untuk Temuan Kerentanan.....	82
Lampiran 8 Hasil Core Assessment Facility Cybersecurity Framework	85
Lampiran 9 Dokumentasi Assessment	104
Lampiran 10 Tabel Profil Target	105
Lampiran 11 Tabel Analisa Kesenjangan Kontrol	108
Lampiran 12 Dokumen Rencana Manajemen Risiko Keamanan Siber.....	116
Lampiran 13 Penjelasan kontrol NIST SP 800-53	144
Lampiran 14 Lembar Pernyataan Keaslian Data	175
Lampiran 15 Lembar Konsultasi Skripsi	176