Institute of Research and Publication Indonesia
IJIRSE: Indonesian Journal of Informatic Research and Software Engineering
Journal Homepage: https://journal.irpi.or.id/index.php/ijirse
Vol. 5. No.1. Maret 2025, pp: 40 - 50
E-ISSN: 2775-5754 | P-ISSN: 2797-2712

Security Risk Management Analysis Of Siam At Poltekes Kemenkes Riau Using Fmea And ISO 27001:2013 Controls

Analisis Manajemen Risiko Keamanan Siam Poltekes Kemenkes Riau Menggunakan Fmea Dan Kontrol ISO 27001:2013

Sonya Meitarice[1*], Monika Nababan[2], Yanti Andriyani[3] , Evfi Mahdiyah[4]

[1,2,3,4]Ilmu Komputer, Universitas Riau, Indonesia
E-Mail: [1]Sonya@lecturer.unri.ac.id, [2]Yanti.andriyani@lecturer.unri.ac.id, [3]Evfi.mahdiyah@lecturer.unri.ac.id

Makalah: Diterima 20 Januari 2025 ; Diperbaiki 15 Februari 2025; Disetujui 20 Maret 2025
Corresponding Author: Sonya Meitarice

Abstrak

Sistem Informasi Akademik Mahasiswa (SIAM) di Poltekkes Kemenkes Riau mendukung layanan akademik penting seperti KRS, KHS, transkrip nilai, dan jadwal kuliah. Namun, sistem ini menghadapi berbagai permasalahan, seperti gangguan server saat pengisian KRS, penataan ruang server yang tidak memadai, kabel longgar, sistem yang tiba-tiba ter-refresh, serangan siber, serta kehilangan data akibat kesalahan staf IT dan teknologi usang. Penelitian ini bertujuan menganalisis manajemen risiko keamanan SIAM dan memberikan rekomendasi mitigasi menggunakan metode Failure Mode and Effect Analysis (FMEA) serta kontrol ISO 27001:2013. Proses analisis mencakup identifikasi mode kegagalan, penilaian tingkat keparahan, kemungkinan terjadi, deteksi, dan perhitungan Risk Priority Number (RPN) yang didapat kan dari hasil wawancara dan pengisian kuisioner. Hasil analisis menunjukkan bahwa sebagian besar risiko berada pada kategori rendah, mencerminkan bahwa sistem masih dapat dikendalikan, tetapi memerlukan perbaikan preventif untuk meningkatkan keandalannya. Beberapa risiko sedang juga teridentifikasi dan membutuhkan penanganan prioritas. Rekomendasi mitigasi diformulasikan melalui kombinasi strategi pengurangan risiko, penghindaran, dan penerimaan, serta diselaraskan dengan kontrol ISO 27001:2013. Temuan ini memberikan kontribusi penting dalam pengembangan SIAM yang lebih aman dan dapat menjadi acuan dalam pengelolaan risiko sistem informasi di institusi pendidikan tinggi.

Kata Kunci : Analisis, FMEA, ISO/IEC 27001:2013, Manajemen Resiko, Rekomendasi.

Abstract

The Student Academic Information System (SIAM) at Poltekkes Kemenkes Riau supports essential academic services such as course registration (KRS), grade reports (KHS), academic transcripts, and class schedules. However, the system faces various issues, including server disruptions during registration periods, inadequate server room organization, loose cabling, unexpected system refreshes, cyberattacks, and data loss due to IT staff errors and outdated technology. This study aims to analyze the security risk management of SIAM and provide mitigation recommendations using the Failure Mode and Effect Analysis (FMEA) method and ISO 27001:2013 controls. The analysis process includes identifying failure modes, assessing severity, occurrence, and detection levels, and calculating the Risk Priority Number (RPN), based on data gathered through interviews and questionnaire responses. The analysis results show that most risks fall into the low category, indicating that the system remains manageable but requires preventive improvements to enhance its reliability. Several moderate-level risks were also identified, which require prioritized handling. The proposed mitigation strategies involve a combination of risk reduction, avoidance, and acceptance, aligned with ISO 27001:2013 controls. These findings contribute significantly to the development of a more secure SIAM and may serve as a reference for information system risk management in higher education institutions.

Keywords: Analysis, FMEA, ISO/IEC 27001:2014, Recommendations, Risk Management

1. PENDAHULUAN

Sistem informasi akademik telah banyak diadopsi oleh institusi pendidikan untuk mengelola informasi akademik dan mendukung proses bisnis internal secara efisien. Sistem ini berfungsi sebagai pengelola data akademik, termasuk layanan seperti pengisian KRS, pelaporan nilai, jadwal kuliah, dan layanan administratif lainnya [1]. Dalam konteks sistem informasi, keamanan informasi menjadi aspek krusial yang perlu dikelola secara sistematis untuk memastikan sistem berjalan dengan andal dan terhindar dari gangguan operasional [2].

Politeknik Kesehatan Kementerian Kesehatan Riau (Poltekkes Kemenkes Riau) merupakan Unit Pelaksana Teknis (UPT) dari Badan Pengembangan dan Pemberdayaan Sumber Daya Manusia Kesehatan, Kementerian Kesehatan Republik Indonesia [3]. Institusi ini menggunakan Sistem Informasi Akademik Mahasiswa (SIAM) sebagai platform utama dalam mendukung aktivitas akademik mahasiswa dan kinerja administrasi akademik. Fitur utama dalam SIAM mencakup pengisian KRS, pengambilan KHS, pencetakan transkrip nilai, registrasi akademik, serta jadwal perkuliahan dan ujian.

Namun, implementasi SIAM di Poltekkes Kemenkes Riau masih menghadapi sejumlah permasalahan. Berdasarkan wawancara dengan staf IT, tercatat insiden seperti gangguan server saat periode pengisian KRS akibat lonjakan pengguna, kondisi ruang server yang kurang tertata, serta kabel longgar yang menyebabkan sistem mengalami restart otomatis. Selain itu, sistem sering mengalami refresh secara tiba-tiba, serta terdapat laporan serangan siber yang mengakibatkan hilangnya data akademik, yang diperburuk oleh penggunaan teknologi lama dan kesalahan manusia. Hingga saat ini, belum ada standar keamanan informasi yang diadopsi secara resmi untuk melindungi aset teknologi informasi di institusi tersebut.

Beberapa pendekatan telah digunakan dalam manajemen risiko keamanan informasi, antara lain OCTAVE Allegro, NIST SP 800-30, dan Failure Mode and Effect Analysis (FMEA) [13][14]. Studi sebelumnya menunjukkan bahwa penerapan FMEA yang dikombinasikan dengan standar ISO 27001:2013 dapat menurunkan tingkat risiko hingga 30% [4]. Dalam konteks pendidikan tinggi, kebutuhan akan sistem informasi yang aman menjadi sangat penting mengingat tingginya volume data akademik yang bersifat sensitif. Kegagalan dalam pengelolaan risiko dapat mengganggu layanan akademik dan menurunkan kepercayaan sivitas akademika terhadap institusi [12].

Oleh karena itu, penelitian ini bertujuan untuk menganalisis risiko keamanan pada SIAM di Poltekkes Kemenkes Riau menggunakan metode FMEA dan merumuskan rekomendasi mitigasi yang selaras dengan kontrol keamanan ISO 27001:2013. Pendekatan ini diharapkan dapat memberikan kontribusi terhadap peningkatan keamanan sistem dan menjadi rujukan dalam pengelolaan risiko sistem informasi di institusi pendidikan tinggi lainnya [5].

2. METODE DAN BAHAN

Terdapat enam tahapan utama yang dilakukan dalam penelitian ini, yakni tahap perencanaan dan studi literatur, pengumpulan data, analisis dengan mengunakan FMEA yang terdiri dari 1) Meninjau Proses dan Produk, 2) Braistorming potensi kegagalan, 3) Menentukan tingkat keparahan (severity), 4) Menentukan nilai kejadian, 5) Menentukan nilai deteksi (Detection), 6) Menghitung RPN [6]. Langkah selanjutnya setelah RPN diketahui dilakukan Perlakukan Resiko dan memberikan Rekomendasi resiko berdasarkan ISO/IEC 27001 : 2013. Metodologi penelitian dapat dilihat pada Gambar 1.

2.1 Analisis dengan FMEA

Metode penelitian ini menggunakan metode penelitian semi-kuantitatif, untuk mengukur dan mengevaluasi sejauh mana tingkat risiko keamanan aset teknologi informasi. Berikut adalah langkah-langkah analisis dan pemrosesan data dalam metode FMEA untuk melakukan evaluasi SIAM yang berjalan dalam Poltekkes Kemenkes [10]:

1. Meninjau Proses Atau Produk (*Review the Process or Product*)

Mengidentifikasi aset yang mendukung proses bisnis SIAM dan risiko yang kemungkinan terjadi pada proses berjalan SIAM dengan wawancara kepada pihak yang bersangkutan dan observasi lokasi.

2. Melakukan *Brainstorming* Potensi Mode Kegagalan

Mengidentifikasi penyebab risiko potensial terjadi kemungkinan risiko pada keamanan aset yang mendukung proses kerja pada pengelolaan SIAM dari hasil wawancara dan observasi yang telah dilakukan

3. Menentukan Nilai Keparahan (*Severity*) Memberikan kuesioner kepada pihak yang bersangkutan untuk memberi nilai tingkat keparahan dengan rating 1-10 berdasarkan akibat dari potensi mode kegagalan yang ditemukan.

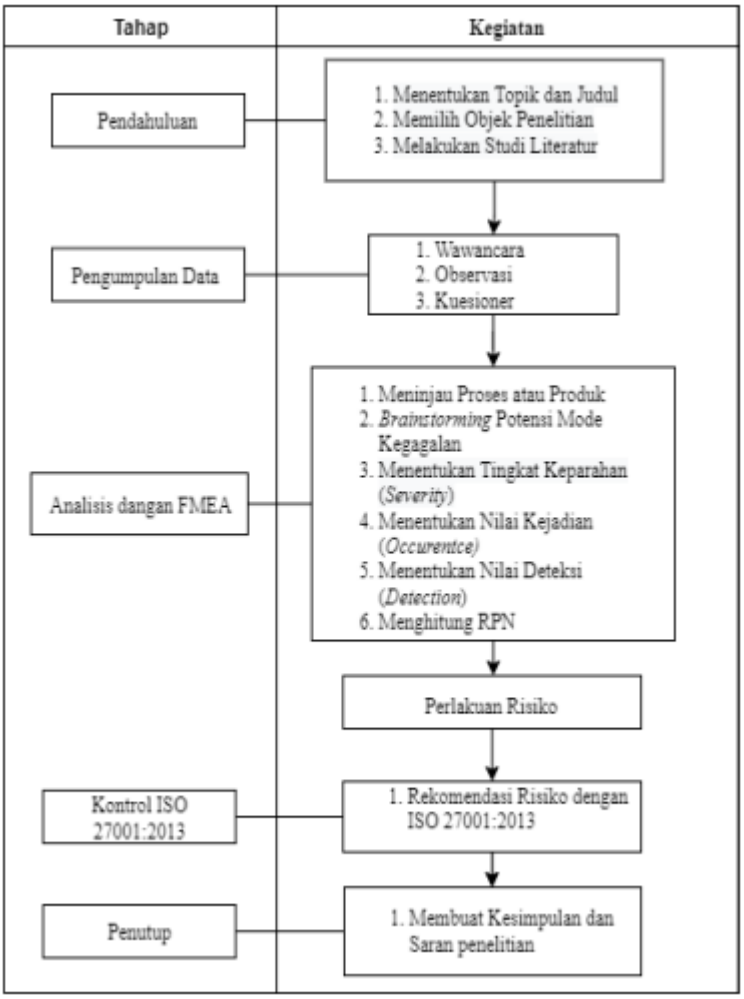
4. Menentukan Nilai Kemungkinan Terjadi (*Occurrence*)

Memberikan kuesioner kepada pihak yang bersangkutan untuk memberi nilai tingkat penyebab dengan rating 1-10 berdasarkan penyebab pada potensi mode kegagalan yang ditemukan.

5. Menentukan Nilai Deteksi (Detection)

Memberikan kuesioner kepada pihak yang bersangkutan untuk memberi nilai tingkat deteksi dengan rating 1-10 berdasarkan potensi mode kegagalan yang ditemukan.

6. Menghitung Risk Priority Number (RPN)
Menentukan nilai Risk Priority Number (RPN) berdasarkan persamaan yaitu dengan menghitung hasil kali antara severity (nilai keparahan), occurrence (tingkat kemungkinan terjadi) dan detection (nilai deteksi).



Gambar 1. Metode Penelitian

2.2 Perlakuan Resiko

Setelah hasil perhitungan RPN, tahapan selanjutnya menentukan perlakuan risiko. Kategori Level pada RPN terbagi menjadi tiga yaitu tinggi, sedang, dan rendah [7]. Setelah mendapatkan level dari masing-masing resiko di tentuka perlakukan resiko. Perlakuan resiko untuk masing-masing level dapat dilihat pada Tabel 1. [8]

Tabel 1. Perlakuan Risiko

RPN	Kategori	Perlakuan Risiko
192 - 1000	Tinggi	Lakukan perbaikan saat ini
65–191	Sedang	Upaya untuk melakukan perbaikan
0 - 64	Rendah	Risiko dapat diabaikan

2.3 Rekomendasi Risiko

Dalam penelitian ini memberikan rekomendasi sesuai dengan ISO 27001:2013. Rekomendasi mitigasi risiko dilakukan dengan setelah menerapkan pemetaan perlakuan risiko pada keamanan sistem informasi. Proses rekomendasi mitigasi ini disesuaikan dari hasil pemetaan perlakuan risiko yang memerlukan tindakan. Upaya mitigasi risiko ini sesuai dengan ketentuan klausul-klausul pada standar ISO 27001:2013.[9]

3. HASIL DAN PEMBAHASAN

Tahap ini penulis menganalisis aset pengelola SIAM, mengetahui penyebab terjadi kemungkinan risiko, penilaian risiko serta level tingkat risiko yang ada pada proses keamanan aset SIAM Poltekkes Kemenkes Riau. Berikut hasil dari analisis risiko menggunakan metode FMEA.

3.1 Meninjau Proses atau Produk (Review the Process or Product)

Tahapan ini merupakan awal dalam Failure Mode And Effect Analysis (FMEA). Identifikasi ini dilakukan dengan wawancara langsung kepada 3 staff IT sebagai eksekutor dalam mendukung berjalan SIAM Politeknik Kemenkes Riau.

a. Daftar Aset

Berdasarkan wawancara dan observasi maka didapatkan daftar aset yang tersedia dalam mendukung proses berjalannya SIAM Poltekkes Kemenkes Riau dapat dilihat pada Tabel 2

Tabel 2. Daftar Aset

Kategori	Aset
Hardware	Aset PC, Server, kabel, UPS, Switch
Data	Data biodata mahasiswa, rencana studi, hasil studi, perkuliahan (kehadiran, jadwal kuliah, jadwal ujian) administrasi (transaksi pembayaran), hasil complain, dan sertifikat mahasiswa
Jaringan	Internet
People	Kepala Unit IT, Staff IT
Software	SIAM, Firewall

b. Hasil Identifikasi Resiko

Hasil dari identifikasi risiko ditemukan dari kemungkinan risiko atau ancaman keamanan dari SIAM yang diperoleh dari hasil wawancara dan pemetaan pada bagian pembahasan penelitian sebelumnya yang dapat dilihat dari Tabel 3.

Tabel 3. Hasil Identifikasi Resiko

Aset	Resiko
Hardware -PC -Kabel -Server -UPS -Switch	Hardware tiba-tiba mati Kerusakan hardware atau tidak berfungsinya hardware
Data -Data biodata mahasiswa -Rencana studi -Hasil studi -Perkuliahan (kehadiran, jadwal kuliah, jadwal ujian) -Administrasi (transaksi pembayaran) -Hasil complain -Sertifikat mahasiswa	Data mengalami kesalahan atau data hilang Pencurian data atau modifikasi data
Jaringan Internet	Server down Ketidaktersediaan layanan Jaringan tidak stabil Serangan hacker
People -Staff IT	Human error
Software -SIAM -Firewall	Software kurang beroperasi dengan baik Serangan virus Serangan Hacker

3.2 Melakukan Brainstorming Potensi Mode Kegagalan

Identifikasi potensi kegagalan dilakukan adanya penyebab peluang risiko keamanan sistem informasi dari proses bisnis yang dijalankan oleh Poltekkes Kemenkes Riau. Berikut ini Potential failure mode yang terdapat SIAM Poltekkes Kemenkes Riau sesuai dengan hasil wawancara yang dilakukan kepada staff IT dari identifikasi risiko maka dapat dilihat pada Tabel 4.

Tabel 4. *Potential Failure Mode*

Aset	Risiko	***Potential Failure Mode***
	Hardware tiba-tiba mati	Kabel perangkat longgar

		Kurangnya *maintenance*
Hardware	Kerusakan *hardware* atau tidak berfungsinya *hardware*	Pemadaman listrik
		Kapasitas penyimpanan penuh
		Rentan terhadap debu dan kelembapan
		Terjadinya bencana alam
		Data tidak di *backup*
Data	Data mengalami kesalahan atau data hilang	Serangan *Malware*
		Server down
		Kesalahan pegawai dalam backup data
Jaringan	Server down	Penggunaan melebihi kemampuan server
	Ketidaktersediaan layanan	Gangguan pada sistem operasi jarungan seperti router atau swicth
	Jaringan tidak stabil	Rusaknya perangkat jaringan
	Serangan hacker	Keamanan IT yang lemah
People	*Human error*	Tidak mengikuti prosedur
Software	Software kurang beroperasi dengan baik	Kurang pengetahuan tentang sistem serangan DDOS
	Serangan virus	Lemahnya keamanan IT
		Tidak update antivirus
	Serangan *Hacker*	Penerapan teknologi yang masih lama

3.3 Menentukan Nilai Keparahan (Severity)

Berdasarkan hasil pengisian kuesioner dari ketiga staff IT Poltekkes Kemenkes Riau, maka diperoleh hasil severity (tingkat keparahan) yang dapat dilihat pada Tabel 4. Nilai *severity* pada *Potential Failure Mode* SIAM dengan nilai *detection* tertinggi bernilai 7 yang terdapat pada *server down*, *Severity* bernilai 3 merupakan yang terendah yaitu rentan terhadap debu dan kelembapan dan terjadinya bencana alam.

Tabel 5. Hasil Tingkat Keparahan (Severity)

Risiko	***Potential Failure Mode***	***Severity***
Hardware tiba-tiba mati	Kabel perangkat longgar	6
	Kurangnya *maintenance*	6
Kerusakan *hardware* atau tidak berfungsinya *hardware*	Pemadaman listrik	4
	Kapasitas penyimpanan penuh	5
	Rentan terhadap debu dan kelembapan	3
	Terjadinya bencana alam	3
Data mengalami kesalahan atau data hilang	Data tidak di *backup*	6
	Serangan *Malware*	5
	Server down	7
	Kesalahan pegawai dalam backup data	5
Server down	Penggunaan melebihi kemampuan server	5
Ketidaktersediaan layanan	Gangguan pada sistem operasi jarungan seperti *router* atau *swicth*	6
Jaringan tidak stabil	Rusaknya perangkat jaringan	6
Serangan *hacker*	Keamanan IT yang lemah	6
	Tidak mengikuti prosedur	5

Human error	Kurang pengetahuan tentang sistem	6
Software kurang beroperasi dengan baik	Serangan DDOS	6
Serangan virus	Lemahnya keamanan IT	6
	Tidak update antivirus	6
Serangan Hacker	Penerapan teknologi yang masih lama	6

3.4 Menentukan Nilai Kemungkinan Terjadi (Occurrence)

Berdasarkan hasil pengisian kuesioner dari ketiga *staff IT* Poltekkes Kemenkes Riau, maka diperoleh hasil *Occurrence* (Kemungkinan Terjadi) yang dapat dilihat pada Tabel 6.

Tabel 6. Hasil Occurrance

Risiko	*Potential Failure Mode*	*Occurrence*
Hardware tiba-tiba mati	Kabel perangkat longgar	2
	Kurangnya *maintenance*	3
Kerusakan *hardware* atau tidak berfungsinya *hardware*	Pemadaman listrik	2
	Kapasitas penyimpanan penuh	2
	Rentan terhadap debu dan kelembapan	2
	Terjadinya bencana alam	3
Data mengalami kesalahan atau data hilang	Data tidak di *backup*	3
	Serangan *Malware*	3
	Server down	2
	Kesalahan pegawai dalam backup data	3
Server down	Penggunaan melebihi kemampuan server	1
Ketidaktersediaan layanan	Gangguan pada sistem operasi jarungan seperti *router* atau *swicth*	2
Jaringan tidak stabil	Rusaknya perangkat jaringan	3
Serangan *hacker*	Keamanan IT yang lemah	3
Human error	Tidak mengikuti prosedur	3
	Kurang pengetahuan tentang sistem	2
Software kurang beroperasi dengan baik	Serangan DDOS	4
Serangan virus	Lemahnya keamanan IT	2
	Tidak update antivirus	2
Serangan *Hacker*	Penerapan teknologi yang masih lama	3

3.5 Menentukan Nilai Deteksi (Detection)

Berdasarkan hasil pengisian kuesioner dari ketiga *staff IT* Poltekkes Kemenkes Riau, maka diperoleh hasil *Detection* (Deteksi) yang dapat dilihat pada Tabel 6. Detection pada Potential Failure Mode SIAM dengan nilai detection tertinggi bernilai 5 terdapat pada serangan malware, penggunaan melebihi kemampuan server, gangguan pada sistem operasi seperti router atau switch, rusaknya perangkat jaringan, keamanan IT yang lemah.

Tabel 7. Hasil *Detection*

Risiko	*Potential Failure Mode*	*Detection*
Hardware tiba-tiba mati	Kabel perangkat longgar	3
	Kurangnya *maintenance*	4
	Pemadaman listrik	3

Kerusakan *hardware* atau tidak berfungsinya *hardware*	Kapasitas penyimpanan penuh	4
	Rentan terhadap debu dan kelembapan	4
	Terjadinya bencana alam	3
Data mengalami kesalahan atau data hilang	Data tidak di *backup*	4
	Serangan *Malware*	5
	Server down	4
	Kesalahan pegawai dalam backup data	3
Server down	Penggunaan melebihi kemampuan server	5
Ketidaktersediaan layanan	Gangguan pada sistem operasi jarungan seperti *router* atau *swicth*	5
Jaringan tidak stabil	Rusaknya perangkat jaringan	5
Serangan *hacker*	Keamanan IT yang lemah	5
Human error	Tidak mengikuti prosedur	3
	Kurang pengetahuan tentang sistem	3
Software kurang beroperasi dengan baik	Serangan DDOS	5
Serangan virus	Lemahnya keamanan IT	4
	Tidak update antivirus	4
Serangan *Hacker*	Penerapan teknologi yang masih lama	4

3.6 Menghitung Nilai RPN

Setelah melakukan pemberian penilaian risiko dari tingkat keparahan (*severity*), tingkat kejadian (*occurrence*), dan tingkat deteksi *(detection*), Selanjutnya dilakukan perhitungan *Risk Priority Number* (RPN) dengan mengalikan nilai Severity, occurrence dan detection. Berikut hasil RPN tiap-tiap risiko. [11]

Tabel 8. Nilai RPN

Aset	Risiko	*Potential Failure Mode*	RPN
Hardware	*Hardware* tiba-tiba mati	Kabel perangkat longgar	36
	Kerusakan	Kurangnya *maintenance*	72
	hardware atau tidak berfungsinya *hardware*	Pemadaman listrik	24
		Kapasitas penyimpanan penuh	40
		Rentan terhadap debu dan kelembapan	24
Data	Data mengalami kesalahan atau data hilang	Terjadinya bencana alam	27
		Data tidak di *backup*	72
		Serangan *Malware*	75
		Server down	56
Jaringan	*Server down*	Kesalahan pegawai dalam backup data	45
		Penggunaanmelebihi kemampuan server	25
	Ketidaktersediaan layanan	Gangguan pada sistem operasi jarungan seperti *router* atau *swicth*	60
	Jaringan tidak stabil	Rusaknya perangkat jaringan	90
	Serangan *hacker*	Keamanan IT yang lemah	90
People	Human Eror	Tidak mengikuti prosedur	45

		Kurang pengetahuan tentang sistem	36
Software	*Software* kurang	Serangan DOS	120
	Serangan virus	Lemahnya keamanan IT	48
		Tidak update antivirus	48
	Serangan *Hacker*	Penerapan teknologi yang masih lama	72

3.7 Perlakuan Resiko

Setelah mendapatkan nilai RPN, selanjutnya menntukan Level Resiko dan perlakuan resiko berdasarkan tabel 1. Hasil tingkat risiko dan perlakuan yang telah diurutkan berdasarkan hasil RPN yang diperoleh dapat dilihat pada Tabel 9.

Tabel 9. Perlakuan Resiko

Potential Failure Mode	**RPN**	**Tingkat Risiko**	**Perlakuan Risiko**
Serangan DDOS	120	Sedang	*Risk Reduction*
Rusaknya perangkat jaringan	90	Sedang	*Risk Reduction*
Keamanan IT yang lemah	90	Sedang	*Risk Reduction*
Serangan *Malware*	75	Sedang	*Risk Reduction*
Kurangnya *maintenance*	72	Sedang	*Risk Reduction*
Data tidak di *backup*	72	Sedang	*Risk Reduction*
Penerapan teknologi yang masih lama	72	Sedang	*Risk Reduction*
Gangguan pada sistem operasi jaringan seperti *router* atau *swicth*	60	Rendah	*Risk Acceptance*
Server down	56	Rendah	*Risk Acceptance*
Lemahnya keamanan IT	48	Rendah	*Risk Acceptance*
Tidak update antivirus	48	Rendah	*Risk Acceptance*
Kesalahan pegawai dalam *backup* data	45	Rendah	*Risk Acceptance*
Tidak mengikuti prosedur	45	Rendah	*Risk Acceptance*
Kapasitas penyimpanan penuh	40	Rendah	*Risk Acceptance*
Kabel perangkat longgar	36	Rendah	*Risk Acceptance*
Kurang pengetahuan tentang sistem	36	Rendah	*Risk Acceptance*
Terjadinya bencana alam	27	Rendah	*Risk Acceptance*
Penggunaan melebihi kemampuan *server*	25	Rendah	*Risk Acceptance*
Pemadaman listrik	24	Rendah	*Risk Acceptance*
Rentan terhadap debu dan kelembapan	24	Rendah	*Risk Acceptance*

3.8 Rekomendasi Mitigasi Risiko Standar ISO 27001:2013

Berdasarkan hasil pemetaan perlakuan risiko pada Tabel 8 maka *cause failure* yang akan di beri rekomendasi mitigasi adalah 6 risiko yaitu serangan DDOS, rusaknya perangkat jaringan, keamanan IT yang lemah, serangan *Malware*, kurangnya *maintenance*, data tidak di *backup* dan penerapan teknologi yang masih lama. Pada Tabel 9 merupakan rekomendasi mitigasi yang dilakukan berdasarkan standar ISO 27001:2013.[15]

Tabel 9. Rekomendasi Mitigasi Resiko

Potential Failure Mode	**Rekomendasi Mitigasi berdasarkan ISO 27001:2013**	
	Kontrol	**Rekomendasi**
Serangan DDOS	Klausul A.16.1 manajemen insiden keamanan informasi & Perbaikan	A.16.1.1 (Tangung jawab dan prosedur): tanggung jawab dan prosedur manajemen harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan tepat untuk insiden keamanan informasi
	Klausul 17.1 Keberlangsung keamanan informasi	Klausul A.17.1.2 (Mengimplemtasikan keberlangsungan keamanan informasi): organisasiharus menetapkan, mendokumentasikan, menerapkan dan menjaga proses, prosedur, & kendali memastikan tingkat yang dibutuhkan dalam keberlangsungan keamanan informasi selama situasi yang merugikan.
Rusaknya perangkat jaringan	Klausul A.8.1 Tanggung Jawab terhadap aset	A.8.1.1 (Inventaris aset): Aset yang berhubungan dengan informasi & fasilitas pengolahan informasi harus diidentifikasikan dan inventaris dari aset-aset ini harus dicatat dan dipelihara
	Klausul A.11.1 Daerah Aman	A.11.1.4 (Melindungi terhadap ancaman eksternal dan lingkungan): Melindungi fisik terhadap bencana alam, serangan jahat atau kecelakaan harus dirancang & diterapkan
Keamanan IT yang lemah	Klausul 13.1 Manajemen Keamanan Jaringan	A.13.1.1 (Kendali jaringan): Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem & aplikasi A.13.1.2 (Keamanan layanan jaringan): Mekanisme keamanan, tingkat layanan & persyaratan manajemen dari semua layanan jaringan harus diidentifikasi & dimasukkan dalam perjanjian layanan jaringan yang dapat dikerjakan sendiri atau dialihdayakan
Serangan Malware	A.12.2 Perlindungan dari malware	A.12.2.1 (Kendali terhadap malware) Kendali deteksi, pencegahan dan pemulihan untuk melindungi terhadap malware harus diimplementasikan, digabungkan dengan kepedulian pengguna yang sesuai.
Kurangnya maintenance	A.12.1 Prosedur dan tanggung jawab operasional	A.12.1.2 (Manajemen perubahan Perubahan) terhadap organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan.
Data tidak di *backup*	A.12.3 Cadangan	A.12.3.1 (Cadangan informasi) Salinan cadangan informasi, perangkat lunak dan image sistem harus diambil dan diuji secara berkala sesuai dengan kebijakan cadangan yang disetujui.

Penerapan teknologi yang masih lama	A.14.2 Keamanan dalam proses pengembangan dan dukungan	A.14.2.3 (Tinjau teknis aplikasi setelah perubahan platform operasi) Ketika platform operasi diubah, aplikasi kritis bisnis harus ditinjau dan diuji untuk memastikan tidak adanya dampak yang merugikan pada operasi atau keamanan organisasi.

4. KESIMPULAN

Berdasarkan hasil penelitian dapat diperoleh kesimpulan sebagai berikut:

1. Penelitian mengenai analisis manajemen risiko keamanan SIAM Poltekkes Kemenkes Riau mendapatkan 20 daftar Potential Failure mode menyebakan adanya risiko dengan 3 risiko kategori moderate (sedang), 17 risiko kategori low (rendah).
2. Rekomendasi mitigasi pada Analisis Keamanan Risiko SIAM Poltekkes Kemenkes Riau berdasarkan kontrol kemanan ISO 27001:2013 antara lain A.16.1.1 tanggung jawab dan prosedur, A.17.1.2 mengimplemtasikan keberlangsungan keamanan informasi, A.8.1.1 inventaris aset, A.11.1.4 melindungi terhadap ancaman eksternal dan lingkungan, A.13.1.1 kendali jaringan, A.13.1.2 keamanan layanan jaringan, A.12.2.1 kendali terhadap malware, A.12.1.2 manajemen perubahan, A.12.3.1 cadangan informasi dan A.14.2.3 review teknis aplikasi setelah perubahan platform operasi.
3. Penelitian berikutnya diharapkan dapat melanjutkan hingga ke proses pemantauan (*monitoring)*

REFERENSI

[1] Ramayani, Y. (2022). Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA). *INOVTEK Polbeng - Seri Informatika*, *7*(2), 289. https://doi.org/10.35314/isi.v7i2.2631

[2] Meitarice, S., Febyana, L., Fitriansyah, A., Kurniawan, R., & Nugroho, R. A. (2024). Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005:2018 Standard and ISO/IEC 27001:2013 Security Controls. *Journal of Information Technology and Cyber Security*. 2(2), 81-90. https://doi.org/10.30996/jitcs.12099

[3] Askrening. (2020). Rencana Strategis Poltekkes Kemenkes Kendari Tahun 2020.

[4] Assa, M., Ahsyar, T. K., & Afdal, M. (2023). *Analisa Manajemen Risiko Sistem Informasi Perpustakaan Menggunakan Metode Failure Mode Effect and Analysis (FMEA)*. *3*(6). https://doi.org/10.30865/klik.v3i6.867

[5] Munaroh, L., Amrozi, Y., & Nurdian, R. A. (2020). Pengukuran Risiko Keamanan Aset Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013. *Technomedia Journal*, *5*(2 Februari), 167–181. https://doi.org/10.33050/tmj.v5i2.1377

[6] Hanifah, P., & S Suroso, J. (2020). Analisis Risiko Sistem Informasi Pada RSIA Eria Bunda menggunakan Metode FMEA. *Jurnal Komputer Terapan*, *6*(2), 210–221. https://doi.org/10.35143/jkt.v6i2.3728

[7] Gani, M., Histiarini, A. R., Ahistasari, A., & Wariori, R. Y. (2023). Analisis resiko kebakaran di bandara rr menggunakan metode fmea. *Jurnal Teknik Industri*, *9*(1), 22–33.

[8] Munawar, M. F., Aini, U. A. N., Novrido, D. H., Jannah, R. M., Syahanifadhel, M. V., & 'Azzam, A. (2023). Analisis Perencanaan Produksi Dan Quality Control Dompet Pria Menggunakan Metode MRP Dan FMEA. *Jurnal Teknik Industri: Jurnal Hasil Penelitian Dan Karya Ilmiah Dalam Bidang Teknik Industri*, *9*(2), 362. https://doi.org/10.24014/jti.v9i2.21895

[9] Tutik, Mutiah, N., & Rusi, I. (2022). Analisis Dan Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis (FMEA) Dan Kontrol ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas). *CODING : Jurnal Komputer Dan Aplikasi*, *10*(02), 249–261.

[10] Ramayani, Y. (2022). Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA). INOVTEK Polbeng - Seri Informatika, 7(2), 289. https://doi.org/10.35314/isi.v7i2.2631

[11] Alijoyo, A., Wijaya, Q. B., & Jacob, I. (2020). Failure Mode Effect Analysis Analisis Modus Kegagalan

dan Dampak RISK EVALUATION RISK ANALYSIS: Consequences Probability Level of Risk. Crms, 19. www.lspmks.co.id

[12] M. F., Sayuti, A. M., Safitri, D. A., Berlianty, T., Julike, W., Wicaksono, G., Marietza, Fenny Kartawinata, B. R., & Utami, F. (2021). MANAJEMEN RISIKO. In *CV Widina Media Utama*. CV Widina Media Utama.

[13] Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi Dan Informasi*, *12*(2), 106–117. https://doi.org/10.34010/jati.v12i2.6829

[14] Hardani, M. S., & Ramli, K. (2022). Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30. *JURIKOM (Jurnal*

[15] International Organization for Standardization. (2013). Internasional Standard ISO/IEC 27001:2013. *Information Technology — Security Techniques — Information Security Management Systems — Requirements*, *2014*(ISO/IEC 27001:2013)