Jurnal SANTI (Sistem Informasi dan Teknologi Informasi)
Vol. 6 No. 1 Tahun 2026
DOI: https://doi.org/10.58794/santi.v6i2.2217

Evaluasi dan Mitigasi Risiko Sistem Raileo PT KAI Divre III Palembang Menggunakan Pendekatan FMEA

Nining Ariati[1], Ar-razy Dwi Kurniawan[2], M. Raihan Pratama[3], Deno Fernando Rahmadani[4], Rena Dwi Arianti[5]
[1-5]Sistem Informasi, Universitas Indo Global Mandiri
e-mail: [1]nining@uigm.ac.id, [2]2023210015@students.uigm.ac.id, [3]2022210029@students.uigm.ac.id, [4]2023210008@students.uigm.ac.id, [5]2023210040@students.uigm.ac.id

(Received :1 Juni 2026; Revised: 4 Juni 2026; Accepted: 14 Juni 2026; Available online: 15 Juni 2026)

Abstrak

Penggunaan platform digital RAILEO memegang peranan penting dalam kelancaran kegiatan operasional PT KAI (Persero) Divisi Regional III Palembang. Namun, ketergantungan masif terhadap sistem ini membawa konsekuensi logis berupa risiko kegagalan yang berpotensi menghambat kinerja. Berbeda dengan penelitian sebelumnya yang hanya berfokus pada satu kategori risiko, penelitian ini secara komprehensif mengidentifikasi dan mengevaluasi seluruh modus kegagalan lintas kategori aset pada sistem RAILEO menggunakan pendekatan Failure Mode and Effect Analysis (FMEA). Pengumpulan data primer dilaksanakan melalui observasi serta wawancara terstruktur bersama dua narasumber kompeten, yaitu Manajer Unit Sistem Informasi dan Staf Keamanan Jaringan PT KAI (Persero) Divre III Palembang. Evaluasi risiko dijalankan dengan meninjau tiga indikator utama: tingkat dampak keparahan (Severity), intensitas terjadinya kendala (Occurrence), serta kemampuan deteksi kesalahan (Detection), yang dinilai melalui teknik expert judgment dengan skala 1 hingga 10. Hasil pengujian menemukan sembilan potensi kegagalan, mencakup malfungsi perangkat keras, kelalaian pengguna (human error), gangguan koneksi jaringan, serangan ransomware, hingga masalah pencadangan data. Kalkulasi nilai Risk Priority Number (RPN) menunjukkan malfungsi perangkat keras menempati urutan risiko tertinggi dengan skor 105. Temuan ini memberikan kontribusi berupa kerangka prioritas risiko berbasis data yang dapat dijadikan acuan manajemen dalam menyusun kebijakan pemeliharaan sistem informasi secara berkelanjutan, termasuk optimalisasi jadwal perawatan fisik dan manajemen suku cadang, demi menjamin keandalan sistem jangka panjang.

Kata kunci: FMEA, Manajemen Risiko, PT KAI, RAILEO, RPN.

Abstract

The deployment of the RAILEO digital platform plays a significant role in operational activities at PT KAI (Persero) Regional Division III Palembang. However, massive reliance on this system introduces potential failure risks that could hinder performance. Unlike previous studies that focused on a single risk category, this research comprehensively identifies and evaluates all failure modes across asset categories within the RAILEO system using the Failure Mode and Effect Analysis (FMEA) methodology. Primary data collection was executed through direct observation and structured interviews with two competent informants, namely the Information Systems Unit Manager and the Network Security Staff of PT KAI (Persero) Divre III Palembang. The risk evaluation was carried out by examining three primary indicators: severity

impact (Severity), constraint occurrence frequency (Occurrence), and error recognition ability (Detection), assessed through expert judgment technique using a scale of 1 to 10. The examination revealed nine potential failures, encompassing hardware malfunctions, user negligence (human error), network disruptions, ransomware attacks, and data backup issues. The Risk Priority Number (RPN) calculation indicates hardware malfunction ranks as the highest risk with a score of 105. These findings contribute a data-driven risk prioritization framework that can serve as a managerial reference for developing sustainable information system maintenance policies, including optimizing equipment maintenance and spare parts management, ensuring long-term system reliability.

Keywords: *FMEA, Management Risk, PT KAI, RAILEO, RPN.*

1. Pendahuluan

Transformasi digital saat ini menjadi pilar utama bagi organisasi dalam meningkatkan efisiensi dan daya saing operasional di tengah dinamika lingkungan bisnis yang cepat [1]. Integrasi antara perencanaan operasional yang terstruktur dengan metode analisis risiko yang adaptif menjadi kunci krusial untuk memastikan keberlangsungan layanan serta mitigasi ancaman strategis secara proaktif [2]. Keamanan informasi merupakan aspek fundamental yang harus dijaga untuk melindungi aset data organisasi dari berbagai ancaman siber dan akses yang tidak sah [3]. Ketidakmampuan dalam mengelola keamanan informasi dapat berakibat fatal, tidak hanya pada kebocoran data, tetapi juga pada lumpuhnya operasional layanan publik secara luas [4].

Kegagalan sistem (system failure) sering kali menjadi titik balik yang mengganggu produktivitas organisasi, yang ditandai dengan ketidakmampuan sistem untuk menjalankan fungsinya sesuai spesifikasi [5]. Mengingat kompleksitas ini, evaluasi berkala diperlukan untuk mendiagnosis akar permasalahan dari setiap modus kegagalan serta mengukur dampak yang ditimbulkan terhadap reliabilitas sistem secara keseluruhan [6]. Infrastruktur teknologi informasi, yang meliputi perangkat keras dan jaringan, merupakan tulang punggung yang memastikan ketersediaan sistem dalam setiap aktivitas bisnis [7]. Kerusakan pada perangkat keras sering menjadi pemicu utama terhentinya aliran data dan komunikasi operasional, sehingga pemeliharaan yang terukur menjadi syarat mutlak untuk mempertahankan integritas data [8].

Di luar aspek teknis, human error atau kesalahan manusia tetap menjadi faktor yang tak terelakkan dalam ekosistem digital yang rentan [9]. Kesalahan operasional akibat kurangnya pemahaman pengguna atau kelalaian dalam prosedur dapat membuka celah keamanan yang merusak pertahanan sistem [10]. Dalam konteks manajemen risiko TI, metode Failure Mode and Effect Analysis (FMEA) hadir sebagai solusi untuk memetakan kegagalan secara kualitatif maupun kuantitatif[11]. FMEA bekerja dengan mengidentifikasi bentuk kegagalan, penyebab, dan dampaknya, kemudian menilainya melalui parameter Risk Priority Number (RPN) [12]. Melalui perhitungan RPN, organisasi dapat memprioritaskan risiko mana yang paling kritis untuk segera dimitigasi secara terukur [13]. Pendekatan FMEA terbukti efektif dalam memberikan rekomendasi perbaikan yang spesifik dan sistematis bagi berbagai jenis sistem informasi yang kompleks [14].

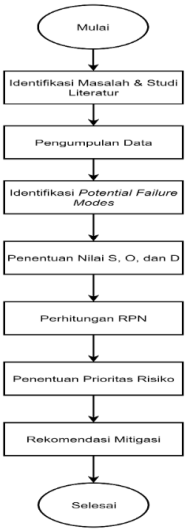
Beberapa penelitian terdahulu telah menerapkan metode FMEA dalam konteks manajemen risiko sistem informasi. Kusnandar et al. [6] menggunakan FMEA berbasis ISO/IEC 27001 pada instansi pemerintahan dan menemukan bahwa risiko infrastruktur jaringan mendominasi nilai RPN tertinggi, namun kajian tersebut tidak mencakup aspek human error maupun sistem e-office internal. Sahira et al. [9] mengaplikasikan FMEA dengan framework ISO/IEC 27002:2022 pada website sistem informasi dengan fokus utama pada risiko keamanan siber, tetapi belum menyentuh sistem mobile e-office berbasis internal organisasi. Sementara itu, Zulvi [7] menerapkan FMEA pada lingkungan Diskominfo Pemprov Riau dengan cakupan risiko TI yang lebih luas, namun prioritas mitigasi lintas kategori aset belum diuraikan secara eksplisit.

Sillehu et al. [12] melakukan pemeringkatan risiko berbasis RPN pada Dinkominfo Surabaya dengan hasil yang cukup komprehensif, meskipun objek kajiannya tidak menyasar sektor transportasi publik. Dari tinjauan tersebut, teridentifikasi kesenjangan penelitian berupa belum adanya kajian FMEA yang secara khusus diterapkan pada sistem e-office internal sektor transportasi publik dengan cakupan identifikasi risiko yang menyeluruh lintas seluruh kategori aset.

PT Kereta Api Indonesia (Persero) mengandalkan RAILEO, sebuah aplikasi Mobile E-Office internal, untuk mendukung aktivitas administrasi dan operasional pegawai [15]. Karena seluruh aktivitas krusial ini dikelola secara real-time dan paperless, maka diperlukan analisis risiko yang mendalam guna menjamin stabilitas sistem tersebut. Berbeda dari penelitian sebelumnya yang umumnya berfokus pada satu kategori risiko atau satu framework standar tertentu, kebaruan penelitian ini terletak pada penerapan FMEA yang dikombinasikan dengan pendekatan Risk Breakdown Structure (RBS) untuk mengidentifikasi dan memprioritaskan risiko secara komprehensif lintas lima kategori aset (hardware, software, jaringan, data, dan SDM) pada sistem e-office internal sektor transportasi publik yang belum pernah dikaji sebelumnya. Melalui penerapan metode FMEA, penelitian ini bertujuan untuk mengidentifikasi, memetakan, dan memprioritaskan risiko pada sistem RAILEO untuk menghasilkan rekomendasi mitigasi yang tepat guna meningkatkan kualitas layanan [16].

2. Metode Penelitian

Metodologi penelitian menjelaskan serangkaian tahapan yang dilakukan dalam pelaksanaan studi kasus ini. Salah satu tahapan utama yang diterapkan adalah analisis risiko menggunakan metode *Failure Mode and Effects Analysis* (FMEA). Metode FMEA digunakan untuk mengidentifikasi berbagai kemungkinan kegagalan yang dapat terjadi dalam suatu sistem serta menganalisis dampak yang ditimbulkan sebelum kegagalan tersebut terjadi [12]. Dalam penelitian ini, alur metodologi penelitian disajikan pada Gambar 1.



Gambar 1. Kerangka Penelitian

2.1. Idenifikasi Masalah dan Studi Literatur

Tahap awal dalam penelitian ini difokuskan pada identifikasi masalah guna memetakan pokok persoalan yang menjadi dasar evaluasi pada sistem informasi RAILEO di PT KAI (Persero) Divre III Palembang. Proses ini bertujuan untuk memahami kondisi keamanan informasi terkini, mendeteksi potensi kerentanan sistem yang belum disadari, serta memberikan arah yang jelas dalam pengumpulan data agar hasil penelitian lebih relevan. Identifikasi dilakukan melalui observasi lapangan dan wawancara awal dengan pihak terkait untuk mendapatkan gambaran utuh mengenai alur bisnis sistem serta daftar aset informasi yang krusial bagi organisasi.

Secara simultan, peneliti melaksanakan studi literatur untuk memperoleh landasan teori yang kuat mengenai konsep manajemen risiko keamanan informasi dan metodologi *Failure Mode and Effect Analysis* (FMEA). Studi literatur ini melibatkan pengumpulan informasi dari berbagai jurnal penelitian terdahulu dan referensi standar keamanan informasi yang relevan. Hal ini dilakukan untuk mendukung penyusunan instrumen penilaian risiko serta memastikan bahwa proses analisis memiliki dasar ilmiah yang kredibel dan dapat dipertanggungjawabkan.

2.2. Teknik Pengumpulan Data

Proses perolehan data dalam penelitian ini dirancang untuk mendapatkan informasi yang mendalam dan valid mengenai profil risiko pada sistem informasi RAILEO di PT KAI (Persero) Divre III Palembang. Peneliti menerapkan pendekatan kualitatif melalui studi kasus dengan menggunakan instrumen pengumpulan data primer sebagai berikut:

A. Observasi Lapangan
   Kegiatan ini dilakukan dengan mengamati secara langsung mekanisme operasional website RAILEO serta infrastruktur IT pendukungnya guna mengidentifikasi kendala teknis dan potensi kerentanan sistem dalam kondisi nyata.
B. Wawancara Terstruktur (*Expert Judgment*)
   Peneliti ini menggunakan teknik wawancara terstruktur yang dilakukan bersama narasumber perwakilan pihak PT KAI (Persero) Divre III Palembang seperti Manajer Unit Sistem Informasi dan Staf Keamanan Jaringan. Kedua narasumber dipilih berdasarkan kriteria memiliki pengalaman minimal tiga tahun dalam pengelolaan dan pengamanan sistem informasi RAILEO serta memahami secara langsung operasional teknis sistem tersebut. Fokus wawancara diarahkan untuk menggali informasi terkait inventaris aset kritis, riwayat gangguan sistem, modus kegagalan (*failure modes*), serta efektivitas kontrol deteksi yang telah diterapkan oleh organisasi saat ini.

Seluruh data yang terhimpun melalui teknik tersebut akan menjadi basis input dalam matriks FMEA untuk ditentukan nilai *Severity* (S), *Occurrence* (O), dan *Detection* (D) melalui diskusi bimbingan bersama para ahli tersebut.

2.3. Identifikasi Potential Failure Modes

Tahapan ini merupakan fase fundamental dalam kerangka kerja FMEA yang difokuskan untuk mengenali dan mendokumentasikan berbagai modus kegagalan yang berpotensi menghambat operasional sistem informasi RAILEO. Melalui proses curah pendapat (*brainstorming*) dan analisis mendalam terhadap hasil wawancara dengan Unit Sistem Informasi PT KAI (Persero) Divre III Palembang, peneliti memetakan titik-titik kerentanan sistem secara komprehensif.

Setiap temuan kegagalan diuraikan berdasarkan akar penyebabnya (*potential cause*) dan efek negatif yang ditimbulkan terhadap keberlangsungan layanan organisasi (*potential effect*). Daftar modus kegagalan ini selanjutnya diklasifikasikan ke dalam kategori aset utama, yakni perangkat keras (*hardware*), perangkat lunak (*software*), infrastruktur jaringan (*network*), data, serta sumber daya manusia (*people*) guna memberikan gambaran risiko yang sistematis untuk dilakukan penilaian pada tahap berikutnya.

2.4. Penentuan Nilai Severity, Occurrence, dan Detection

Setelah seluruh potensi kegagalan pada sistem RAILEO berhasil dipetakan, langkah selanjutnya adalah melakukan penilaian risiko menggunakan tiga kriteria utama dalam metode FMEA, yaitu *Severity* (S), *Occurrence* (O), dan *Detection* (D). Proses pemberian nilai ini dilakukan melalui teknik *expert judgment* dengan mekanisme konsensus, yaitu kedua narasumber memberikan penilaian secara independen terlebih dahulu, kemudian hasil penilaian didiskusikan bersama hingga dicapai kesepakatan nilai akhir untuk setiap modus kegagalan. Variabel *Severity* digunakan untuk menilai besarnya dampak kegagalan terhadap operasional organisasi,

Occurrence mengukur probabilitas frekuensi kemunculan risiko, sementara *Detection* mengevaluasi sejauh mana prosedur kontrol saat ini mampu mengidentifikasi kegagalan secara dini. Seluruh parameter ini dinilai menggunakan skala 1 hingga 10, di mana skor yang lebih tinggi menunjukkan tingkat kerentanan yang lebih kritis.

2.5. Perhitungan Risk Priority Number (RPN)

Proses yang dilakukan setelah tahap evaluasi parameter adalah mengalkulasikan nilai *Risk Priority Number* (RPN) pada setiap potensi kegagalan yang ada di website RAILEO. RPN berfungsi sebagai indikator kuantitatif untuk menentukan seberapa kritis sebuah risiko bagi organisasi. Skor ini diperoleh melalui perkalian matematis antara bobot *Severity* (S), *Occurrence* (O), dan *Detection* (D) dengan persamaan berikut:

$$RPN = S \times O \times D$$

Besaran nilai RPN merefleksikan tingkat keparahan risiko secara terukur. Semakin besar angka yang dihasilkan, semakin mendesak pula potensi gangguan tersebut bagi operasional PT KAI (Persero) Divre III Palembang. Oleh karenanya, hasil perolehan skor ini dijadikan acuan utama dalam menentukan skala prioritas penanganan masalah.

2.6. Prioritas Risiko dan Rekomendasi Mitigasi

Langkah terakhir penelitian ini berfokus pada pengurutan tingkat risiko serta perumusan mitigasi tepat sasaran. Setelah kalkulasi *Risk Priority Number* (RPN) pada seluruh modus kegagalan sistem RAILEO, hasilnya diurutkan dari nilai tertinggi hingga terendah. Risiko dengan skor RPN tertinggi ditetapkan sebagai kerentanan paling kritis. Masalah tersebut menjadi prioritas utama PT KAI (Persero) Divre III Palembang untuk diselesaikan demi mencegah gangguan sistem lebih luas.

Berbekal hasil pemeringkatan tersebut, peneliti menyusun rekomendasi perbaikan dengan mengombinasikan kajian literatur dan masukan profesional (*expert judgment*) Unit Sistem Informasi. Usulan mitigasi dirancang memberikan solusi pencegahan maupun perbaikan yang berfokus pada tiga aspek utama: menurunkan kemungkinan kegagalan (*Occurrence*), mengurangi keparahan saat insiden terjadi (*Severity*), dan memperkuat kapabilitas mendeteksi ancaman (*Detection*). Untuk memudahkan penentuan prioritas mitigasi, nilai RPN diklasifikasikan ke dalam beberapa kategori tingkat risiko. Standar pengelompokan rentang nilai prioritas RPN disajikan pada Tabel 1.

Tabel 1. Kategori Tingkat Risiko RPN

Rentang Nilai RPN	Kategori Prioritas	Keterangan Tindakan
1 - 4	Sangat Rendah	Risiko dapat diterima, cukup dilakukan pemantauan berkala.
5 - 9	Rendah	Risiko masih dalam batas aman, tidak memerlukan tindakan mendesak.
10 - 49	Menengah	Membutuhkan evaluasi prosedur dan tindakan pencegahan menengah.
≥ 50	Tinggi	Risiko kritis, wajib segera dilakukan mitigasi dan perbaikan sistem.

3. Hasil dan Pembahasan

3.1. Hasil Identifikasi Risiko

Setelah menentukan aset-aset kritis, langkah berikutnya adalah memetakan berbagai potensi risiko yang dapat mengganggu jalannya sistem RAILEO. Dalam penelitian ini, proses pemetaan risiko dilakukan dengan menerapkan metode *Risk Breakdown Structure* (RBS). Sesuai dengan pendekatan yang digunakan, Risiko yang diidentifikasi diperoleh melalui pendekatan *Risk*

Breakdown Structure (RBS), yaitu metode yang mengelompokkan risiko berdasarkan kategori tertentu[12]. Metode ini kemudian diaplikasikan secara sistematis untuk mempermudah proses analisis dan penentuan prioritas penanganan. Berdasarkan analisis kondisi operasional di PT KAI (Persero) Divre III Palembang, identifikasi risiko dirinci ke dalam sembilan poin utama sebagaimana terlihat pada Tabel 2.

Tabel 1. Identifikasi Risiko Sistem

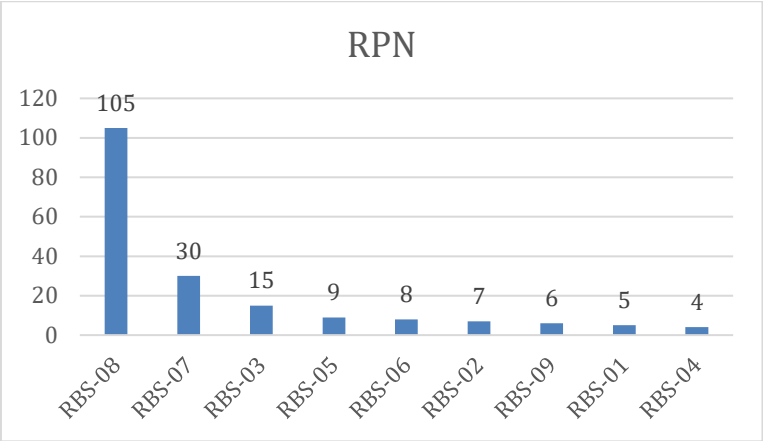
Level 0	Level 1	Level 2	Level 3 (Potensi Risiko)	RBS Code
Sistem	Risiko Eksternal	Gangguan Fasilitas	Pemadaman Listrik	RBS-01
		Ancaman Siber	Serangan Ransomware	RBS-02
	Risiko Internal	Operasional	Gangguan Jaringan Lokal	RBS-03
			Server Down	RBS-04
			Sistem Informasi Error/Bug	RBS-05
			Kegagalan Backup Data	RBS-06
			Human Error (Operator)	RBS-07
			Perangkat Keras Rusak	RBS-08
			Overload Traffic Jaringan	RBS-09

Sumber : (Diadaptasi dari Sillehu et al. ,2025).

Langkah awal berupa pemetaan dan identifikasi kerentanan sangatlah vital untuk memastikan evaluasi sistem informasi berjalan sukses. Sejalan dengan kajian yang memadukan kerangka manajemen risiko pada operasional organisasi, ditekankan bahwa identifikasi dan analisis risiko yang tepat memungkinkan perusahaan merancang solusi mitigasi yang relevan dan bersifat preventif[1]. Dengan adanya kategorisasi risiko yang terstruktur seperti penjabaran di atas, pihak manajemen tidak sekadar bertindak reaktif pasca-insiden, tetapi juga dapat menyusun langkah preventif demi menjaga keandalan sistem dan perlindungan aset data.

3.2. Peniliaian Severity (S), Occurrence (O), Detection (D), dan RPN

Tahap selanjutnya adalah melakukan penilaian terhadap tingkat keparahan (*severity*), frekuensi kejadian (*occurrence*), dan kemampuan deteksi (*detection*). Penentuan nilai S, O, dan D dilakukan menggunakan skala 1 hingga 10 guna mendapatkan data yang valid sesuai kondisi aktual di lapangan. Seluruh hasil penilaian variabel S, O, D, dan kalkulasi akhir RPN disajikan secara komprehensif pada Tabel 3. Sebelum merujuk pada rincian detail di dalam tabel tersebut, pemetaan tingkat kekritisan risiko juga disajikan melalui ringkasan visual pada Gambar 2, di mana perolehan nilai RPN telah diurutkan dari skor tertinggi hingga terendah.



Gambar 2. Grafik Perbandingan Nilai RPN

Tabel 3. Penilaian Severity (S), Occurrence (O), Detection (D), dan RPN

RBS Code	Potensi Kegagalan	Efek / Dampak (Severity)	Penyebab Kegagalan Aktual (Occurrence)	Pencegahan Saat Ini (Detection)	S	O	D	RPN	Kategori
RBS-08	Perangkat Keras Rusak	PC operasional tidak bisa digunakan hingga selesai perbaikan.	Kurangnya maintenance rutin dan sering terimbas pemadaman paksa.	Tidak ada monitoring hardware; bergantung laporan user.	7	3	5	105	Tinggi
RBS-07	Human Error	Kekeliruan input NIPP atau salah unggah ijazah.	Kurangnya ketelitian saat menginput atau memvalidasi berkas.	Terdapat prosedur verifikasi berjenjang oleh atasan.	5	2	3	30	Menengah
RBS-03	Gangguan Jaringan	Menghambat kecepatan validasi dokumen pelamar.	Kerusakan infrastruktur seperti kabel LAN longgar atau putus.	Belum ada monitoring LAN otomatis; staf memeriksa secara manual.	5	1	3	15	Menengah
RBS-05	Sistem Informasi Error	Lambatnya proses loading pada web portal.	Kemunculan bug kritis hampir tidak pernah terjadi.	Berdasarkan laporan keluhan langsung dari pengguna.	3	1	3	9	Rendah
RBS-06	Kegagalan Backup	Berpotensi menghilangkan arsip lokal pegawai.	Proses pencadangan manual ke harddisk jarang korup.	Proses backup dipantau langsung oleh pengguna.	4	1	2	8	Rendah
RBS-02	Serangan Ransomware	Mengancam siklus paperless dan berisiko mengekspos	Telah mengoperasikan server lokal untuk pembaruan Antivirus.	Tersedia warning system yang memantau anomali aktivitas.	7	1	1	7	Rendah

		kerahasiaan data.							
RBS-09	Overload Traffic	Menyebabkan web terasa lambat saat memuat halaman.	Staf mengakses bersamaan menjelang batas pelaporan.	Terpantau melalui sistem monitoring jaringan.	3	2	1	6	Rendah
RBS-01	Pemadaman Listrik	Dokumen yang belum di-save bisa hilang.	Insiden padamnya suplai daya PLN secara mendadak.	Genset otomatis aktif saat suplai daya terputus.	5	1	1	5	Rendah
RBS-04	Server Down	Pekerjaan input data tertunda.	Insiden beban tinggi jarang ditemui.	Notifikasi pusat dan aktifnya pengalihan ke server cadangan.	4	1	1	4	Sangat Rendah

Hasil penilaian menunjukkan bahwa sebagian besar risiko memperoleh nilai Occurrence (O) yang rendah, yaitu pada rentang 1–3. Hal ini mencerminkan kondisi aktual di lapangan berdasarkan keterangan narasumber bahwa insiden seperti server down, kegagalan backup, dan serangan ransomware belum pernah terjadi secara signifikan selama periode operasional sistem RAILEO. Meskipun demikian, rendahnya nilai O pada risiko seperti ransomware (O=1) tidak berarti risiko tersebut dapat diabaikan, mengingat nilai Severity-nya tetap tinggi (S=7). Sejalan dengan temuan Kusnandar et al. [6] yang menyatakan bahwa ancaman siber bersifat laten dan dapat muncul sewaktu-waktu tanpa riwayat insiden sebelumnya, sehingga justifikasi nilai O yang rendah harus diimbangi dengan penguatan mekanisme deteksi dan pencegahan secara proaktif.

3.3. Rekomendasi Tindakan (Recommended Actions)

Berdasarkan peringkat RPN yang telah dihasilkan, penelitian ini mengarahkan rekomendasi perbaikan pada kategori risiko tinggi dan menengah. Fokus ini diambil guna memastikan strategi mitigasi di PT KAI (Persero) Divre III Palembang berjalan lebih efisien serta terarah pada titik kerentanan yang paling mendesak untuk segera ditangani.

Fokus utama adalah menanggulangi kerusakan perangkat keras (RBS-08) yang mencatatkan skor RPN tertinggi sebesar 105. Dominasi perangkat keras sebagai risiko tertinggi sejalan dengan temuan Zulvi [7] dan Sillehu et al. [12] yang sama-sama menempatkan infrastruktur fisik sebagai sumber risiko utama dalam lingkungan sistem informasi pemerintahan dan transportasi. Tingginya nilai RPN pada RBS-08 dipicu oleh kombinasi nilai Severity yang besar (S=7) akibat ketergantungan penuh operasional pada PC, nilai Detection yang lemah (D=5) karena tidak adanya sistem monitoring hardware otomatis, serta frekuensi kejadian yang tidak dapat diprediksi (O=3) akibat minimnya jadwal pemeliharaan rutin. Kondisi ini mengindikasikan bahwa PT KAI (Persero) Divre III Palembang masih mengandalkan pendekatan reaktif dalam penanganan kerusakan perangkat keras, sehingga berdampak pada terhentinya layanan administrasi secara tidak terduga. Solusi yang diusulkan mencakup penerapan pemeliharaan fisik secara rutin setiap bulan serta penyediaan suku cadang cadangan (*spare parts*) untuk komponen kritis. Langkah ini dinilai krusial untuk mencegah kelumpuhan layanan administrasi akibat minimnya perawatan berkala yang sering kali menjadi pemicu utama kerusakan perangkat di lapangan [16]. Keandalan infrastruktur fisik merupakan fondasi utama bagi ketersediaan layanan sistem informasi secara berkelanjutan [6].

Selanjutnya, human error (RBS-07) dengan RPN sebesar 30 merupakan risiko menengah yang perlu mendapat perhatian serius. Temuan ini konsisten dengan Sahira et al. [9] yang menyatakan bahwa faktor manusia merupakan celah keamanan yang persisten dalam sistem informasi berbasis e-office, terutama karena kesalahan input data tidak selalu terdeteksi oleh

sistem secara otomatis. Tingginya nilai Detection (D=3) pada risiko ini menunjukkan bahwa mekanisme verifikasi berjenjang yang ada saat ini belum sepenuhnya mampu mencegah kekeliruan operator secara dini. Implikasinya bagi PT KAI adalah perlunya program pelatihan berkala bagi operator RAILEO disertai penerapan validasi data otomatis pada form input kritis untuk meminimalkan kesalahan yang bersifat prosedural.

Terakhir, untuk memitigasi gangguan jaringan lokal (RBS-03), langkah perbaikan mencakup pemeriksaan fisik kabel LAN secara berkala serta optimalisasi konfigurasi jaringan kantor. Meskipun nilai RPN gangguan jaringan (15) lebih rendah dibandingkan hardware, risiko ini tetap memiliki potensi dampak menengah (S=5) yang apabila tidak ditangani dapat menghambat seluruh alur validasi dokumen administrasi secara bersamaan. Berbeda dengan penelitian Adhitya dan Suryadi [14] yang menemukan gangguan jaringan sebagai risiko dominan, pada konteks PT KAI Divre III Palembang risiko ini masih dapat dikelola dengan baik karena infrastruktur kabel yang relatif terpelihara. Dengan menjamin kualitas infrastruktur kabel tetap terjaga, hambatan komunikasi data antar unit dapat direduksi sehingga kelancaran administrasi pegawai tidak terganggu oleh koneksi yang tidak stabil [14]. Strategi ini sejalan dengan upaya menjaga integritas jaringan yang menjadi aset vital dalam koordinasi operasional perusahaan [11].

4. Kesimpulan

Melalui penerapan teknik *Failure Mode and Effect Analysis* (FMEA), riset ini telah mengidentifikasi sembilan variasi gangguan sistem pada aktivitas operasional di PT KAI (Persero) Divre III Palembang. Analisis berbasis *Risk Priority Number* (RPN) mengonfirmasi bahwa kerusakan infrastruktur perangkat keras (RBS-08) menjadi titik lemah utama dengan nilai 105, diikuti oleh kesalahan manusia (RBS-07) dan kendala jaringan lokal (RBS-03) dengan skor masing-masing 30 dan 15. Guna mereduksi dampak tersebut, manajemen didorong untuk mengadopsi skema perawatan fisik bulanan serta menjamin ketersediaan suku cadang untuk efisiensi pemulihan. Lebih lanjut, integrasi pengawasan jaringan secara *real-time* dan program edukasi teknis bagi operator secara periodik menjadi langkah krusial dalam memperkuat stabilitas serta akurasi data pada ekosistem teknologi informasi perusahaan di masa depan.

Secara akademik, penelitian ini berkontribusi dalam memperluas penerapan metode FMEA pada domain sistem e-office internal sektor transportasi publik yang selama ini belum banyak dikaji, sekaligus mendemonstrasikan efektivitas kombinasi pendekatan Risk Breakdown Structure (RBS) dan FMEA dalam menghasilkan pemeringkatan risiko yang terstruktur dan berbasis data. Namun demikian, penelitian ini memiliki keterbatasan pada jumlah narasumber expert judgment yang terbatas, yaitu dua orang, sehingga objektivitas penilaian S, O, dan D berpotensi bersifat subjektif. Penelitian selanjutnya disarankan untuk melibatkan lebih banyak ahli dari unit yang berbeda serta mengombinasikan metode FMEA dengan kerangka standar seperti ISO 27005 atau pendekatan OCTAVE guna memperoleh analisis risiko yang lebih komprehensif dan dapat digeneralisasi pada konteks organisasi yang lebih luas.

Daftar Pustaka

[1] Nining Ariati, Ben Bella Al Ghiffary Faesha Putra, Ajeng Armadi Rani, and Raja Amar Siregar, “Metode Perencanaan Arsitektur Perusahaan PT Ubersari Kertalangu dalam Pengelolaan Limbah B3 Medis dengan Pendekatan Manajemen Risiko,” *Bridge : Jurnal Publikasi Sistem Informasi dan Telekomunikasi*, vol. 3, no. 2, pp. 43–54, May 2025, doi: 10.62951/bridge.v3i2.420.

[2] H. Hermansyah, M. Musaruddin, H. Tari MOkoi, M. Nur Anshari, and A. Kadir, “ Penerapan Metode FMEA dalam Penilaian Risiko Sistem Pemerintahan Berbasis Elektronik” *semanTIK*, vol. 11, pp. 201–208, 2025, Accessed: May 02, 2026. [Online]. Available: https://semantik.uho.ac.id/index.php/journal

[3] C. Kirana Zarry, M. Tshamaroh, and S. Agesti, "Analisis Dampak Risiko It Pada Website Sistem Informasi Pelayanan Administrasi Surat Menyurat (Siasy) Menggunakan Metode Fmea," *Journal Informatics Nivedita* |, vol. 01, no. 1, 2024.

[4] S. N. Iftizam and D. Firmansyah, "Analisis Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effect Analysis (FMEA) (Studi Kasus: BPS Kota Pangkal Pinang)." [Online]. Available: https://jurnalmahasiswa.com/index.php/jriin

[5] N. Mutiah, I. Rusi, J. Sistem Informasi, and F. H. MIPA UniversitasTanjungpura Jalan Hadari Nawawi, "Coding : Jurnal Komputer dan Aplikasi Menggunakan Metode Failure Mode And Effects Analysis (Fmea) Dan Kontrol ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi dan Informatika Kabupaten Sambas)."

[6] A. Kusnandar, A. F. Rochim, and V. Gunawan, "Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan Metode FMEA Berbasis ISO/IEC 27001 pada Instansi XYZ untuk Keamanan Sistem Informasi," *Jurnal Sistem Informasi Bisnis*, vol. 14, no. 4, pp. 375–384, Oct. 2024, doi: 10.21456/vol14iss4pp375-384.

[7] M. S. Zulvi, "Jurnal Politeknik Caltex Riau Manajemen Risiko Teknologi Informasi Menggunakan Metode Fmea (Studi Kasus: Diskominfo Pemprov Riau)," 2022. [Online]. Available: https://jurnal.pcr.ac.id/index.php/jkt/

[8] J. Homepage *et al.*, "IJIRSE: Indonesian Journal of Informatic Research and Software Engineering Security Risk Management Analysis Of Siam At Poltekes Kemenkes Riau Using Fmea And ISO 27001:2013 Controls".

[9] M. S. Sahira, R. Indriati, and A. Ristyawan, "Analisis Risiko Website Sistem Keamanan Informasi Menggunakan Metode Fmea dan Framework ISO/IEC 27002:2022," *JSITIK: Jurnal Sistem Informasi dan Teknologi Informasi Komputer*, vol. 3, no. 2, pp. 128–138, Jun. 2025, doi: 10.53624/jsitik.v3i2.722.

[10] A. Sofianingtias and M. E. Prasetya, "Analisis Penilaian Risiko Pengembangan Aplikasi GA Service Menggunakan Failure Mode and Effect Analysis (FMEA) – Studi Kasus Perusahaan Jasa PT XYZ," *Owner*, vol. 8, no. 3, pp. 2116–2126, Jun. 2024, doi: 10.33395/owner.v8i3.2155.

[11] A. Syahri *et al.*, "Analisa Manajemen Risiko Sistem Informasi Penjualan Menggunakan Metode Failure Mode Effects and Analysis," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 11, no. 4, 2024.

[12] Fidyah Salsabila Putri Sillehu, Marisca Amanda Hidayat, Raihana Sakhi Aswanda, Audrey Septya Rosanti, Agung Brastama Putra, and Amalia Anjani Arifiyanti, "Analisis Manajemen Risiko Teknologi Informasi pada Dinkominfo Surabaya Menggunakan Metode Failure Mode and Effect Analysis (FMEA)," *Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 3, no. 4, pp. 215–223, Jul. 2025, doi: 10.61132/merkurius.v3i4.947.

[13] Y. Ramayani, T. Oktarina, D. A. Palembang Jl Jenderal Yani No, K. I. Seberang Ulu, and S. Selatan, "Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)," vol. 7, no. 2, p. 2022.

[14] A. G. Adhitya and C. Suryadi, "Pengembangan Model Pengelolaan Risiko Sistem Informasi Berbasis Fmea Dan Iso 31000:2009 Sebagai Pendukung K3l Di Laboratorium Lingkungan," vol. ISSN, no. 1, pp. 79–90, doi: 10.26760/rekalingkungan.v10i1.79-90.

[15] H. A. Setia, M. Safitri, V. R. Putri, and C. P. Wibowo, "Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI) 2023 Surabaya," 2023. [Online]. Available: https://dishub.jatimprov.go.id/.

[16] Y. Rizal, D. Setyo Oktaria, G. Anggun Prameswari, T. Arifianto, and H. Artikel, "Penerapan Metode Failure Mode And Effect Analysis Dalam Analisis Risiko Kegagalan Radio Lokomotif di Divisi Regional III Palembang," *Jurnal Media Elektro*, doi: 10.35508/jme.v0i0.20723.