Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika
Volume 3, Nomor 4, Juli 2025
e-ISSN: 3031-8912; p-ISSN: 3031-8904; Hal. 215-223
DOI: https://doi.org/10.61132/merkurius.v3i4.947
Available online at: https://journal.arteii.or.id/index.php/Merkurius

Analisis Manajemen Risiko Teknologi Informasi pada Dinkominfo Surabaya Menggunakan Metode *Failure Mode and Effect Analysis* (FMEA)

Fidyah Salsabila Putri Sillehu[1*], Marisca Amanda Hidayat[2], Raihana Sakhi Aswanda[3], Audrey Septya Rosanti[4], Agung Brastama Putra[5], Amalia Anjani Arifiyanti[6]
[1-5]Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia
Email: *22082010047@student.upnjatim.ac.id[1], 22082010065@student.upnjatim.ac.id[2], 22082010068@student.upnjatim.ac.id[3], 22082010197@student.upnjatim.ac.id[4], agungbp.si@upnjatim.ac.id[5], amalia_anjani.fik@upnjatim.ac.id[6]

Jl. Rungkut Madya, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur 60294
Korespondensi penulis: 22082010047@student.upnjatim.ac.id

Abstract. *The use of information technology (IT) in the government sector requires structured risk management to ensure the continuity of public services. The Department of Communication and Information Technology (Dinkominfo), as a digital service provider, faces various potential risks such as network disruptions, hardware failures, and cyberattacks that could interfere with daily operations. This study employs the Failure Mode and Effect Analysis (FMEA) method to identify, analyze, and formulate strategies to mitigate existing IT risks. Through the FMEA approach, each potential failure is evaluated based on its severity, occurrence, and detection capability, which are then used to calculate a Risk Priority Number (RPN). The analysis reveals that the highest RPN values are associated with information system errors, hardware failures, and network overloads. As mitigation measures, the study recommends conducting regular system audits, upgrading network capacity, and performing preventive maintenance on devices. This approach demonstrates that FMEA is an effective method for managing IT risks within government institutions.*

Keywords*: Dinkominfo, FMEA, risk management, information system, information technology*

Abstrak. Pemanfaatan Teknologi Informasi (TI) dalam sektor pemerintahan menuntut adanya pengelolaan risiko yang terstruktur untuk memastikan keberlangsungan layanan publik. Dinas Komunikasi dan Informatika (Dinkominfo) Kota Surabaya sebagai penyedia layanan digital menghadapi berbagai potensi risiko, seperti gangguan jaringan, kerusakan perangkat keras, hingga serangan siber yang dapat mengganggu operasi harian. Penelitian ini menggunakan metode *Failure Mode and Effect Analysis* (FMEA) untuk mengidentifikasi, menganalisis, dan merumuskan strategi mitigasi risiko TI yang ada. Melalui pendekatan FMEA, setiap potensi kegagalan dievaluasi berdasarkan *severity*, *occurrence*, dan *detection*, yang kemudian dihitung menjadi nilai *Risk Priority Number* (RPN). Hasil analisis menunjukkan bahwa risiko dengan nilai RPN tertinggi terdapat pada kesalahan sistem informasi, kerusakan perangkat keras, dan overload jaringan. Sebagai upaya mitigasi, penelitian ini merekomendasikan penerapan audit sistem secara berkala, peningkatan kapasitas jaringan, serta pemeliharaan perangkat secara preventif. Pendekatan ini membuktikan bahwa FMEA efektif digunakan dalam pengelolaan risiko TI di instansi pemerintahan.

Kata kunci: Dinkominfo, FMEA, manajemen risiko, sistem informasi, teknologi informasi

1. LATAR BELAKANG

Pelayanan publik merupakan komponen penting dalam pelaksanaan pemerintahan karena bertujuan untuk memenuhi kebutuhan masyarakat secara adil dan merata. Seiring dengan kemajuan teknologi informasi (TI), pemerintah dituntut untuk terus melakukan inovasi agar layanan publik menjadi lebih efektif, efisien, transparan, dan akuntabel (Mansyur, Subagja, & Hakim, 2025). Di tengah tuntutan masyarakat terhadap pelayanan yang cepat, transparan, dan

Received: Juni 07, 2025; Revised: Juni 21, 2025; Accepted: Juli 05, 2025; Published: Juli 08, 2025

akuntabel, pemanfaatan TI menjadi faktor penting dalam mendukung proses kerja dan pengambilan keputusan. Salah satu instansi yang sangat bergantung pada teknologi informasi dalam menjalankan fungsinya adalah Dinas Komunikasi dan Informatika Kota Surabaya.

Sebagai instansi yang bertanggung jawab atas pengelolaan infrastruktur teknologi dan informasi publik, Dinkominfo Surabaya menghadapi berbagai potensi risiko yang dapat mengganggu kelancaran operasional dan layanan digital yang disediakan. Risiko tersebut tidak hanya datang dari pihak eksternal yang semakin kompleks, seperti *ransomware* dan *malware*, tetapi juga terdapat ancaman dari dalam organisasi, seperti kesalahan dalam konfigurasi sistem, pengelolaan data yang tidak tepat, dan rendahnya kesadaran akan keamanan di antara pengguna (Kesehatan et al., 2024). Dampak dari risiko tersebut dapat merugikan organisasi, mulai dari kerugian finansial, rusaknya reputasi, hingga terganggunya operasional yang berpotensi menghambat kelangsungan bisnis (Kuncoro et al., 2023; Sinaga & Rochmoeljati, 2024). Dalam organisasi publik, menilai risiko bersifat penting karena menunjukkan upaya organisasi dalam memperkuat tata kelola secara kelembagaan (Pradesa, Purba, et al., 2021). Sehingga diperlukan suatu pendekatan sistematis untuk mengidentifikasi dan menganalisis risiko-risiko tersebut agar tidak berdampak negatif terhadap layanan publik.

Menurut Koeswara dan Harjito dalam Maychael & Pangestuti (2022), pembentukan komite manajemen risiko oleh suatu perusahaan merupakan salah satu strategi yang dapat dimanfaatkan untuk meningkatkan nilai tambah perusahaan. Strategi serupa juga dapat diterapkan dalam organisasi pemerintahan sebagai upaya memperkuat pengelolaan risiko, terutama dalam menghadapi dinamika dan kompleksitas teknologi informasi. Dengan pengelolaan risiko yang baik, instansi pemerintah dapat menjaga stabilitas operasional serta meningkatkan keandalan layanan publik berbasis digital.

Salah satu metode yang dapat digunakan untuk mengelola risiko teknologi informasi secara proaktif adalah *Failure Mode and Effect Analysis* (FMEA). FMEA merupakan metode yang digunakan secara sistematis dan terstruktur untuk mengidentifikasi serta menganalisis dampak dari kegagalan pada suatu sistem atau proses, serta membantu dalam menurunkan kemungkinan terjadinya kegagalan tersebut (Anthony, 2021). Dengan penerapan FMEA, organisasi dapat mengambil langkah preventif sebelum risiko benar-benar terjadi.

2. KAJIAN TEORITIS

Penelitian ini menganalisis risiko pada proses layanan digital di lingkungan instansi pemerintahan, dalam penelitian ini digunakan metode *Failure Mode and Effects Analysis* (FMEA) sebagai pendekatan untuk mengidentifikasi potensi kegagalan sistem serta mengevaluasi dampaknya terhadap kinerja layanan. Secara umum, FMEA merupakan teknik analisis risiko yang digunakan untuk mengidentifikasi kemungkinan metode kegagalan dari suatu sistem, mengevaluasi efek dari kegagalan tersebut, serta menetapkan prioritas risiko berdasarkan nilai numerik yang dikenal sebagai *Risk Priority Number* (RPN) (Muad'zah et al., 2020). Nilai RPN dihitung berdasarkan tiga parameter utama, yaitu tingkat keparahan (*Severity*), kemungkinan terjadinya (*Occurrence*), dan kemampuan deteksi (*Detection*) (Yaqin et al., 2022). Sebagai alat bantu analisis, nilai RPN dihitung dengan menggunakan formula:

RPN = S x O x D

Ket: RPN *(Risk Priority Number)*, S *(Severity)*, O *(Occurrence)*, D *(Detection)*

Nilai masing-masing parameter ditentukan berdasarkan skala penilaian tertentu. Semakin tinggi nilai RPN, semakin besar prioritas penanganan terhadap risiko tersebut harus diberikan.

Severity Rating		***Occurrence Rating***		***Detection Rating***	
1	M	1	U	1	VH
2-3	L	2	VL	2-5	H
4-6	Md	3-4	L	6-8	Md
7-8	H	5-6	Md	9	L
9-10	VH	7-8	H	10	
		9-10	VH		

Ket: M *(Minor)*, L *(Low)*, Md *(Moderate)*, H *(High)*, VH *(Very High)*, U *(Unliked)*, VL *(Very Low)*

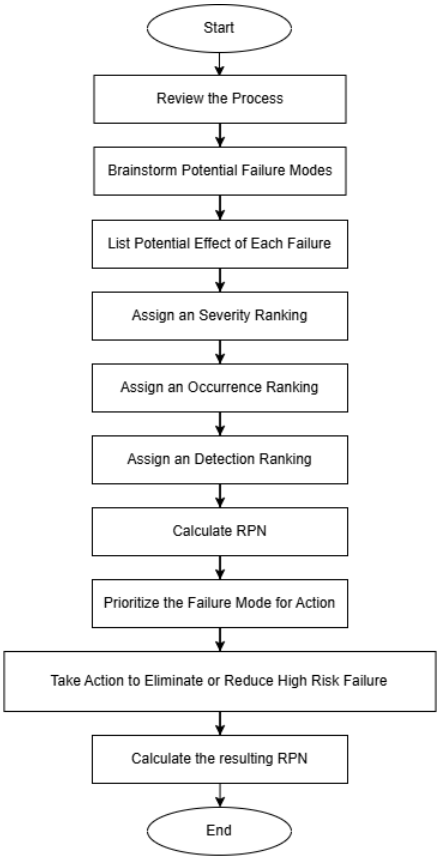
Dalam hal ini, penggunaan FMEA dapat membantu memberikan pemetaan risiko, menemukan, menganalisis, menilai, dan mengatasi risiko secara menyeluruh terhadap proses operasional sistem (Thenu et al., 2020). Oleh karena itu, penerapan FMEA sebagai bagian dari strategi manajemen risiko dapat membantu instansi pemerintah dalam menyiapkan respons dini terhadap berbagai potensi gangguan yang mungkin muncul dalam sistem layanan digitalnya. Tahapan utama dalam penerapan FMEA meliputi: (1) Mengidentifikasi kemungkinan bentuk

kegagalan dalam suatu proses atau sistem, (2) Menilai tingkat keparahan dari kegagalan tersebut, (3) Menentukan seberapa sering risiko itu bisa terjadi, dan (4) Mengevaluasi seberapa besar peluang bahwa kegagalan tersebut bisa terdeteksi sebelum berdampak lebih luas.

Melalui pendekatan ini, FMEA dapat memberikan gambaran yang sistematis terhadap risiko-risiko yang muncul pada proses operasional, sekaligus membantu dalam merumuskan tindakan perbaikan yang tepat.

3. METODE PENELITIAN

Metodologi penelitian memuat tahapan-tahapan yang dijalankan dalam pelaksanaan studi kasus ini. Salah satu tahapan penting dalam penelitian ini adalah melakukan analisis risiko menggunakan metode *Failure Mode and Effects Analysis* (FMEA). Metode *Failure Mode and Effects Analysis* (FMEA) bertujuan untuk mengidentifikasi potensi kegagalan dalam suatu sistem serta mengevaluasi dampaknya sebelum kegagalan tersebut terjadi (Puja dan Jarot, 2020). Pada penelitian ini, metodologi penelitian ditunjukkan pada Gambar 1.



Gambar 1. Metodologi Penelitian

4. HASIL DAN PEMBAHASAN

Untuk meningkatkan kinerja sistem informasi yang menjadi bagian penting dari proses bisnis di Dinas Komunikasi dan Informatika Kota Surabaya, diperlukan analisis komprehensif terhadap potensi kegagalan serta dampak yang mungkin terjadi akibat kegagalan tersebut dalam pelaksanaan tugas dan layanan Dinkominfo Surabaya.

Review the Process

Pada tahap ini, dilakukan proses wawancara dengan staf yang bertugas di Dinkominfo Surabaya untuk mengidentifikasi berbagai kendala yang dihadapi (Mutiara, 2022). Berdasarkan hasil wawancara, ditemukan sejumlah permasalahan dan kesalahan yang terjadi dalam operasional sistem informasi.

1. Daftar Aset Kritis

Adapun daftar aset yang ada di Dinkominfo Surabaya beserta alasan aspek tersebut seperti berikut:

Tabel 2. Daftar Aset Dinkominfo Surabaya

Aset Kritis	Alasan
Jaringan	Digunakan untuk mengakses layanan dan pertukaran data antar sistem informasi.
Sistem Informasi	Menjadi tulang punggung proses bisnis dan pelayanan publik yang dikelola oleh Dinkominfo.
Data	Berisi informasi penting dan sensitif terkait layanan pemerintahan yang harus dijaga kerahasiaan, integritas, dan ketersediaannya.
Sumber Daya Manusia (SDM)	SDM yang kompeten sangat penting untuk mengelola dan mengamankan infrastruktur TI.
Server	Menyimpan data dan aplikasi yang digunakan oleh berbagai unit kerja dalam lingkup Dinkominfo.
Perangkat Komputer (Laptop/PC)	Digunakan oleh staf untuk mengakses sistem dan menjalankan operasional harian.

2. Hasil Identifikasi Risiko

Risiko yang diidentifikasi diperoleh melalui pendekatan *Risk Breakdown Structure* (RBS), yaitu metode yang mengelompokkan risiko berdasarkan kategori tertentu.

Tabel 3. Identifikasi Risiko Dinkominfo Surabaya

Level 0	Level 1	Level 2	Level 3	RBS Code
Sistem	Risiko Eksternal	Gangguan Fasilitas Umum	Pemadaman Listrik	RBS-01
		Cyber Threat	Serangan *Ransomware*	RBS-02
	Risiko Internal	Operasional	Gangguan Jaringan	RBS-03
			Server Down	RBS-04
			Sistem Informasi *Error*	RBS-05
			Kegagalan *Backup*	RBS-06
			Human Error	RBS-07
			Perangkat Keras Rusak	RBS-08
			Overload Traffic Jaringan	RBS-09

Brainstorm Potential Failure Modes

Kegagalan yang mengganggu jalannya proses bisnis perusahaan memerlukan langkah identifikasi terhadap kerentanan sistem yang ada (Sidik, Andalia, & Tamalika, 2022). Berikut ini merupakan *failure mode* yang teridentifikasi di Dinkominfo Surabaya berdasarkan hasil wawancara dengan staf.

Tabel 4. *Potential Failure Modes* Dinkominfo Surabaya

RBS Code	Potential Failure Mode
RBS-01	Pemadaman listrik mendadak atau genset yang berfungsi.
RBS-02	Serangan ransomware pada sistem informasi dan antivirus tidak *update.*
RBS-03	Kabel LAN rusak, dan kesalahan konfigurasi jaringan.

RBS Code	Potential Failure Mode
RBS-04	Server *down* akibat *overheat* dan beban tinggi
RBS-05	Sistem informasi *error/bug* karena sistem tidak stabil
RBS-06	Kegagalan *backup* karena *storage* tidak terhubung
RBS-07	Kesalahan input data oleh operator atau penghapusan data secara tidak sengaja
RBS-08	Perangkat keras rusak karena kurangnya *maintenance*.
RBS-09	*Overload traffic* jaringan karena banyak akses bersamaan menyebabkan lambatnya sistem *bandwidth*

List Potential Effect of Each Failure

Kegagalan yang terjadi pada Dinkominfo Surabaya menyebabkan menghambatnya proses bisnis yang sedang berjalan. Adapun kegagalan yang terjadi di Dinkominfo Surabaya sebagai berikut.

Tabel 5. *Potential Effect of Each Failure* Dinkominfo Surabaya

	RBS Code	Potential Failure Mode
Sistem Dinkominfo Surabaya	RBS-01	Pemadaman listrik mendadak atau genset yang berfungsi.
	RBS-02	Serangan *ransomware* pada sistem informasi dan antivirus tidak *update.*
	RBS-03	Kabel LAN rusak, dan kesalahan konfigurasi jaringan.
	RBS-04	*Server down* akibat *overheat* dan beban tinggi
	RBS-05	Sistem informasi *error/bug* karena sistem tidak stabil
	RBS-06	Kegagalan *backup* karena *storage* tidak terhubung

	RBS Code	Potential Failure Mode
	RBS-07	Kesalahan input data oleh operator atau penghapusan data secara tidak sengaja
	RBS-08	Perangkat keras rusak karena kurangnya *maintenance*.
	RBS-09	*Overload traffic* jaringan karena banyak akses bersamaan menyebabkan lambatnya sistem *bandwidth*

Assign an Severity Ranking

Berdasarkan wawancara yang dilakukan dengan satu orang staf, berikut ini adalah hasil penentuan *severity* dari masing-masing potensi kegagalan yang teridentifikasi.

Tabel 6. Tabel *Severity* Dinkominfo Surabaya

RBS *Code*	Potensi Kegagalan	*Severity* (Rating Keparahan)	Keterangan
RBS-01	Pemadaman Listrik	2	Pemadaman listrik mendadak atau genset yang berfungsi.
RBS-02	Serangan *Ransomware*	4	Serangan *ransomware* pada sistem informasi dan antivirus tidak *update.*
RBS-03	Gangguan Jaringan	4	Kabel LAN rusak, dan kesalahan konfigurasi jaringan.
RBS-04	*Server Down*	6	*Server down* akibat *overheat* dan beban tinggi
RBS-05	Sistem Informasi Error	6	Sistem informasi *error/bug* karena sistem tidak stabil
RBS-06	Kegagalan *Backup*	2	Kegagalan *backup* karena *storage* tidak terhubung

RBS *Code*	Potensi Kegagalan	*Severity* (Rating Keparahan)	Keterangan
RBS-07	*Human Error*	3	Kesalahan input data oleh operator atau penghapusan data secara tidak sengaja
RBS-08	Perangkat Keras Rusak	4	Perangkat keras rusak karena kurangnya *maintenance*.
RBS-09	*Overload Traffic* Jaringan	4	*Overload traffic* jaringan karena banyak akses bersamaan menyebabkan lambatnya sistem *bandwidth*

Berdasarkan Tabel 6, tingkat keparahan tertinggi terdapat pada RBS-04 dan RBS-05 dengan nilai *severity* masing-masing sebesar 6. Dari hasil wawancara, *server down* disebabkan oleh *overheat* dan beban kerja yang tinggi sehingga sistem tidak bisa merespons dan mengganggu operasional layanan secara keseluruhan. Sementara itu, *error* pada sistem informasi disebabkan oleh ketidakstabilan sistem akibat kurangnya pengujian dan perawatan rutin, yang berdampak pada terganggunya akses pengguna terhadap layanan penting dan menurunkan produktivitas kerja.

Assign an Occurrence Ranking

Berdasarkan dari hasil wawancara maka didapatkan nilai *occurrence* untuk setiap kegagalan seperti Tabel 7.

Tabel 7. Tabel *Occurence* Dinkominfo Surabaya

RBS Code	Potensi Kegagalan	Penyebab Kegagalan	Occurrence
RBS-01	Pemadaman Listrik	Pemadaman listrik mendadak atau genset yang berfungsi.	3
RBS-02	Serangan *Ransomware*	Serangan *ransomware* pada sistem informasi dan antivirus tidak *update*.	4
RBS-03	Gangguan Jaringan	Kabel LAN longgar/rusak, konfigurasi tidak tepat	4
RBS-04	*Server Down*	*Server down* akibat *overheat* dan beban tinggi	3
RBS-05	Sistem Informasi *Error*	Sistem informasi *error/bug* karena sistem tidak stabil	4
RBS-06	Kegagalan *Backup*	Kegagalan *backup* karena *storage* tidak terhubung	3
RBS-07	*Human Error*	Kesalahan input data oleh operator atau penghapusan data secara tidak sengaja	5
RBS-08	Perangkat Keras Rusak	Perangkat keras rusak karena kurangnya *maintenance*.	5
RBS-09	*Overload* Traffic Jaringan	*Overload traffic* jaringan karena banyak akses bersamaan menyebabkan lambatnya sistem *bandwidth*	4

Berdasarkan hasil wawancara, diperoleh nilai *occurrence* sebesar 5 untuk RBS-07 dan RBS-08. Pada *human error*, kesalahan input data atau penghapusan data secara tidak sengaja oleh operator sering terjadi karena kurangnya validasi sistem. Sementara itu, perangkat keras

rusak menunjukkan bahwa kerusakan perangkat keras kerap terjadi akibat kurangnya perawatan rutin.

Assign an Detection Ranking

Berdasarkan dari hasil wawancara maka didapatkan nilai *detection* seperti pada Tabel 8.

Tabel 8. Tabel Deteksi Dinkominfo Surabaya

RBS Code	Potensi Kegagalan	Penyebab Kegagalan	Identifikasi Pencegahan Saat Ini	Detection
RBS-01	Pemadaman Listrik	Pemadaman listrik mendadak atau genset yang berfungsi.	Ada UPS untuk beberapa perangkat; genset jarang diuji	3
RBS-02	Serangan *Ransomware*	Serangan *ransomware* pada sistem informasi dan antivirus tidak *update.*	Ada antivirus dasar; belum ada *firewall* canggih	4
RBS-03	Gangguan Jaringan	Kabel LAN longgar/rusak, konfigurasi tidak tepat	Monitoring manual, belum ada sistem pemantauan *real-time*	3
RBS-04	*Server Down*	*Server down* akibat *overheat* dan beban tinggi	Belum ada sistem notifikasi suhu atau *load server* otomatis	5
RBS-05	Sistem Informasi *Error*	Sistem informasi *error/bug* karena sistem tidak stabil	Tidak ada QA/testing rutin; perbaikan setelah terjadi gangguan	5

RBS Code	Potensi Kegagalan	Penyebab Kegagalan	Identifikasi Pencegahan Saat Ini	Detection
RBS-06	Kegagalan *Backup*	Kegagalan *backup* karena *storage* tidak terhubung	Jadwal *backup* ada, tapi tidak dipantau hasilnya secara rutin	2
RBS-07	*Human Error*	Kesalahan input data oleh operator atau penghapusan data secara tidak sengaja	Hanya ada manual kerja, belum ada sistem validasi *input*	4
RBS-08	Perangkat Keras Rusak	Perangkat keras rusak karena kurangnya *maintenance*.	Tidak ada sistem *preventive maintenance*	5
RBS-09	*Overload Traffic* Jaringan	*Overload traffic* jaringan karena banyak akses bersamaan menyebabkan lambatnya sistem *bandwidth*	Tidak ada *load balancing* atau monitoring *bandwidth*	6

Calculate RPN

Setelah dilakukan penilaian terhadap tingkat keparahan, kemungkinan terjadinya, dan kemampuan deteksi terhadap setiap potensi kegagalan, diperoleh nilai *Risk Priority Number* (RPN) yang menggambarkan besarnya tingkat risiko dari masing-masing kejadian. Nilai RPN ini membantu dalam menentukan skala prioritas perbaikan yang harus segera dilakukan. Seperti yang dijelaskan oleh Pakarbudi et al. (2023), RPN merupakan alat ukur untuk menilai tingkat risiko dari suatu kegagalan dan menjadi dasar dalam menyusun urutan prioritas penanganan secara sistematis. Sedangkan hasil RPN dari Dinkominfo Surabaya dapat dilihat pada Tabel 9.

Tabel 9. Tabel RPN Dinkominfo Surabaya

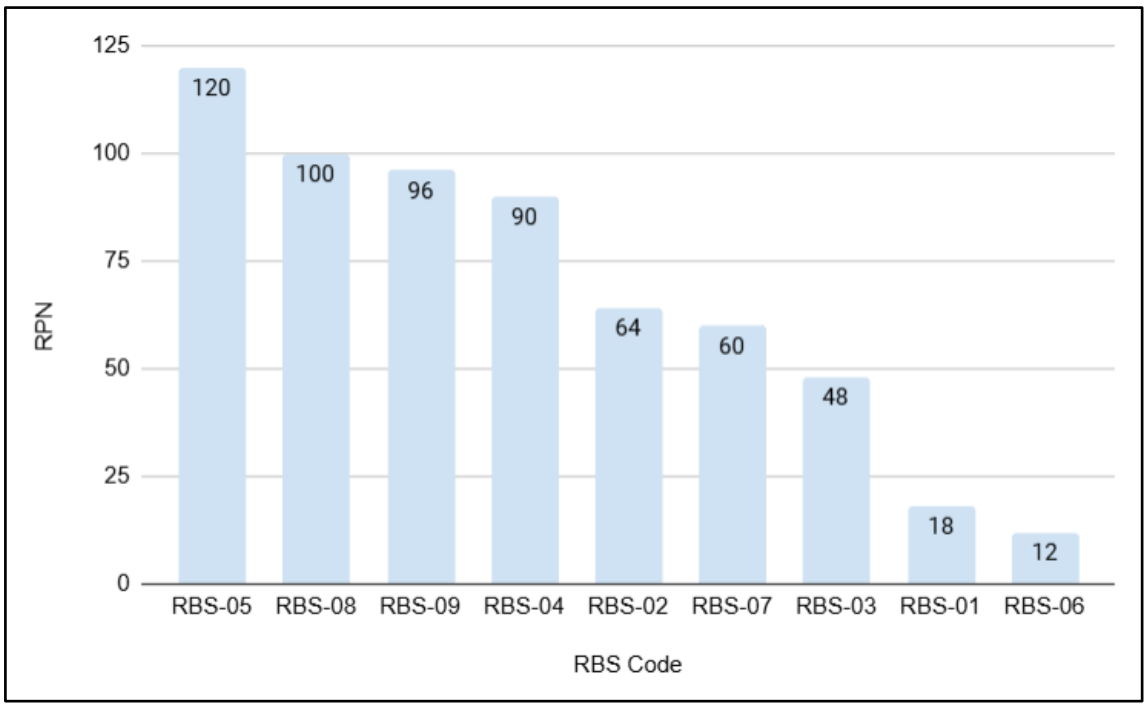
RBS Code	Potensi Kegagalan	Penyebab Kegagalan	RPN
RBS-01	Pemadaman Listrik	Pemadaman listrik mendadak atau genset yang berfungsi.	18
RBS-02	Serangan *Ransomware*	Serangan *ransomware* pada sistem informasi dan antivirus tidak *update.*	64
RBS-03	Gangguan Jaringan	Kabel LAN longgar/rusak, konfigurasi tidak tepat	48
RBS-04	*Server Down*	*Server down* akibat *overheat* dan beban tinggi	90
RBS-05	Sistem Informasi *Error*	Sistem informasi *error/bug* karena sistem tidak stabil	120
RBS-06	Kegagalan *Backup*	Kegagalan *backup* karena *storage* tidak terhubung	12
RBS-07	*Human Error*	Kesalahan input data oleh operator atau penghapusan data secara tidak sengaja	60
RBS-08	Perangkat Keras Rusak	Perangkat keras rusak karena kurangnya *maintenance*.	100
RBS-09	*Overload Traffic* Jaringan	*Overload traffic* jaringan karena banyak akses bersamaan menyebabkan lambatnya sistem *bandwidth*	96

Berdasarkan hasil perhitungan, potensi kegagalan dengan nilai RPN tertinggi adalah Sistem Informasi Error dengan nilai 120, yang menunjukkan bahwa sistem yang tidak stabil bisa sangat mengganggu layanan. Kemudian pada Perangkat Keras Rusak dengan nilai 100, *Overload Traffic* Jaringan dengan nilai 96, dan *Server Down* dengan nilai 90, yang semuanya

termasuk risiko tinggi dan harus segera ditangani. Risiko lain seperti Serangan *Ransomware*, *Human Error*, dan Gangguan Jaringan masuk kategori sedang sampai rendah, tapi tetap perlu perhatian. Sementara itu, Kegagalan *Backup* dan Pemadaman Listrik termasuk risiko rendah karena nilai RPN-nya paling kecil.

Prioritize the Failure Mode for Action

Setelah menganalisis nilai *severity*, *occurrence*, dan *detection*, langkah berikutnya adalah menghitung nilai RPN (*Risk Priority Number*). Nilai maksimum RPN sendiri adalah 1000, karena masing-masing komponen memiliki nilai tertinggi 10. Hasil perhitungan RPN untuk Dinkominfo Surabaya dapat dilihat pada Gambar 2.



Gambar 2. Grafik RPN Dinkominfo Surabaya

Setelah dilakukan perhitungan nilai RPN, langkah selanjutnya adalah menyusun prioritas risiko berdasarkan besarnya nilai tersebut. Daftar nilai RPN disusun dari yang paling tinggi hingga paling rendah, dan risiko dengan nilai RPN tertinggi akan menjadi prioritas utama karena berpotensi menimbulkan kerugian yang paling besar.

Tabel 10. Nilai RPN Dinkominfo Surabaya dari besar ke kecil

RBS Code	Potensi Kegagalan	Penyebab Kegagalan	RPN	Kategori
RBS-05	Sistem Informasi Error	Sistem informasi *error/bug* karena sistem tidak stabil	120	*High* (Tinggi)
RBS-08	Perangkat Keras Rusak	Perangkat keras rusak karena kurangnya *maintenance*.	100	*Moderate* (Sedang)
RBS-09	*Overload Traffic* Jaringan	*Overload traffic* jaringan karena banyak akses bersamaan menyebabkan lambatnya sistem *bandwidth*	96	*Moderate* (Sedang)
RBS-04	*Server Down*	*Server down* akibat *overheat* dan beban tinggi	90	*Moderate* (Sedang)
RBS-02	Serangan *Ransomware*	Serangan *ransomware* pada sistem informasi dan antivirus tidak *update.*	64	*Low* (Rendah)
RBS-07	*Human Error*	Kesalahan input data oleh operator atau penghapusan data secara tidak sengaja	60	*Low* (Rendah)
RBS-03	Gangguan Jaringan	Kabel LAN longgar/rusak, konfigurasi tidak tepat	48	*Low* (Rendah)
RBS-01	Pemadaman Listrik	Pemadaman listrik mendadak atau genset yang berfungsi.	18	*Low* (Rendah)

RBS Code	Potensi Kegagalan	Penyebab Kegagalan	RPN	Kategori
RBS-06	Kegagalan *Backup*	Kegagalan *backup* karena *storage* tidak terhubung	12	*Low* (Rendah)

Take Action to Elimination or Reduce High Risk Failure

Sistem Informasi Error yang melonjak secara drastis saat jumlah pengguna tinggi menunjukkan adanya batas kemampuan sistem dan ketidakstabilan dalam menangani beban yang besar (Hamidah et al., 2025). Untuk mengatasi hal ini, Dinkominfo Surabaya perlu memperkuat proses pengembangan perangkat lunak dengan menerapkan audit kode secara berkala, penggunaan pengujian otomatis (*automated testing*), serta sistem pemantauan dan pencatatan log secara *real-time*. Selain itu, penerapan prosedur *code review* yang ketat dan kontrol versi akan membantu mencegah *bug* yang tidak terdeteksi masuk ke sistem produksi. Pembaruan sistem juga harus dilakukan secara terjadwal dan disertai dengan mekanisme *rollback* jika terjadi kegagalan.

Sementara itu, kerusakan perangkat keras yang disebabkan oleh usia perangkat dan kurangnya perawatan menunjukkan risiko sedang. Untuk mengurangi risiko ini, langkah yang dapat diambil Dinkominfo meliputi pendataan dan evaluasi berkala atas kondisi perangkat yang ada, serta pelaksanaan jadwal perawatan preventif yang konsisten. Penggantian perangkat yang sudah melebihi masa pakai sangat penting, dan penyediaan komponen cadangan menjadi langkah mitigasi cepat jika terjadi kerusakan. Penggunaan sistem pemantauan kesehatan perangkat keras secara *real-time* juga disarankan agar potensi kegagalan dapat terdeteksi sejak dini.

Pada kasus *overload traffic* jaringan akibat banyaknya akses bersamaan, Dinkominfo dapat mengurangi dampaknya dengan menerapkan *load balancer* untuk mendistribusikan beban secara merata antar server. Selain itu, peningkatan kapasitas jaringan, penggunaan *caching*, serta pemanfaatan *Content Delivery Network* (CDN) dapat membantu mempercepat akses dan mengurangi tekanan pada jaringan utama. Pengawasan terhadap trafik secara *real-time* dan penyesuaian infrastruktur berdasarkan pola penggunaan juga perlu dilakukan agar sistem tetap responsif pada jam sibuk.

Kemudian, masalah *server down* yang disebabkan oleh *overheat* dan beban tinggi sebaiknya ditangani dengan langkah-langkah pencegahan sejak awal. Dinkominfo disarankan untuk memastikan sistem pendingin di ruang server berfungsi dengan optimal serta

mempertimbangkan penggunaan teknologi *auto-scaling* untuk menyesuaikan kapasitas server secara dinamis terhadap beban. Monitoring suhu dan beban server harus dilakukan secara terus-menerus, dan sistem *failover* perlu disiapkan agar layanan tetap berjalan jika terjadi gangguan. Selain itu, pengujian ketahanan perlu dilakukan untuk mengetahui batas maksimal kemampuan server sebelum ditempuh peningkatan kapasitas.

Calculate the resulting RPN

Ketika tindakan perbaikan atau mitigasi diterapkan sebagai upaya untuk menurunkan tingkat kerentanan sistem, maka nilai RPN (*Risk Priority Number*) secara otomatis akan mengalami penurunan. Nilai RPN sendiri diperoleh dari hasil perkalian antara *severity*, *occurrence*, dan *detection*. Setelah nilai ini dihitung, dilakukan proses evaluasi kembali terhadap risiko yang ada, untuk menentukan langkah selanjutnya yang lebih efektif. Evaluasi ini juga mempertimbangkan tindakan pencegahan terbaru yang telah diidentifikasi, agar potensi kegagalan serupa dapat diminimalkan secara berkelanjutan.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penerapan metode *Failure Mode and Effect Analysis* (FMEA) mampu mengidentifikasi dan memprioritaskan berbagai risiko teknologi informasi yang dihadapi oleh Dinas Komunikasi dan Informatika (Dinkominfo) Surabaya. Risiko dengan nilai *Risk Priority Number* (RPN) tertinggi ditemukan pada potensi kegagalan sistem informasi yang disebabkan oleh *bug* atau ketidakstabilan sistem, diikuti oleh kerusakan perangkat keras, *overload* jaringan, dan *server down* akibat *overheat*. Penerapan FMEA telah memungkinkan identifikasi yang sistematis terhadap tingkat keparahan, kemungkinan terjadi, dan kemampuan deteksi dari masing-masing risiko. Berdasarkan hasil tersebut, disarankan agar Dinkominfo menerapkan langkah-langkah mitigasi seperti audit kode dan pengujian otomatis untuk sistem informasi, preventif *maintenance* untuk perangkat keras, peningkatan kapasitas jaringan dengan teknologi *load balancer*, serta pemantauan suhu server secara *real-time* untuk mencegah *downtime*. Keterbatasan dalam penelitian ini terletak pada ruang lingkup data yang hanya mencakup satu instansi pemerintah, sehingga generalisasi ke instansi lain perlu dilakukan dengan hati-hati. Untuk penelitian selanjutnya, disarankan metode FMEA dikombinasikan dengan pendekatan manajemen risiko lain, serta diterapkan pada sektor atau instansi yang berbeda guna memperoleh hasil yang lebih komprehensif.

DAFTAR REFERENSI

Anthony, M. B. (2021). Analisis penyebab kerusakan unit pompa pendingin AC dan kompresor menggunakan metode FMEA. *Jurnal Teknologi*, *11*(1), 5–13. https://doi.org/10.35134/jitekin.v11i1.24

Hamidah, I., Haromain, I., & Drehem, I. M. (2025). Evaluasi pengujian kinerja menggunakan JMeter untuk menunjang stabilitas aplikasi layanan perbankan pada PT Bank Rakyat Indonesia Tbk. *DBESTI: Journal of Digital Business and Technology Innovation*, *2*(1), 114–126. https://doi.org/10.54914/dbesti.v2i1.1621

Kesehatan, P., Kepentingan Majduddin, P., & Kunang, Y. N. (2024). Analisis kritis atas tantangan dan strategi manajemen risiko teknologi informasi di Rumah Sakit Ernaldi Bahar: Panduan praktis. *Journal of Information Technology and Society*, *2*(1). https://jits.unmuhbabel.ac.id/

Kuncoro, S. D., Ghaisan, R. A., Zaky, M. U., Wulansari, A., & Artikel, S. (2023). Manajemen risiko pada teknologi informasi: Studi kasus pada perusahaan jasa. *Jurnal Ilmiah Sain dan Teknologi*, *1*(3).

Mansyur, M. N., Subagja, I. K., & Hakim, A. (2025). Pengaruh pemanfaatan teknologi informasi terhadap kualitas layanan serta kepuasan masyarakat dalam pelayanan publik. *Jurnal Ekonomi Manajemen Sistem Informasi (JEMSI)*, *6*(5), 3112–3119. https://doi.org/10.38035/jemsi.v6i5.

Maychael, M., & Pangestuti, D. C. (2022). Peran manajemen risiko dalam memoderasi rasio keuangan terhadap nilai perusahaan. *Owner: Riset dan Jurnal Akuntansi*, *6*(4), 3398–3411. https://doi.org/10.33395/owner.v6i4.1137

Mu'adzah, M. A., & Firmansyah, N. A. (2020). Manajemen risiko K3 pada divisi produksi menggunakan FMEA dan RCA di PT. XYZ. *Jurnal Teknologi dan Manajemen Industri*, *1*(2), 15–22.

Mutia, S. Z. (2022). Manajemen risiko teknologi informasi menggunakan metode FMEA (studi kasus: Diskominfo Pemprov Riau). *Jurnal Komputer Terapan*, *8*(2), 381–390.

Pakarbudi, A., Piay, D. T., Nurmadewi, D., & Rachman, A. (2023). Analisa efektivitas metode OCTAVE Allegro dan FMEA dalam penilaian risiko aset informasi pada institusi pendidikan tinggi. *JURIKOM (Jurnal Riset Komputer), 10*(2), 488–496.

Pradesa, H. A., Purba, C. O., & Priatna, R. (2021). Menilai risiko dari organisasi yang bertransformasi: Pelajaran terbaik untuk penguatan akuntabilitas pendidikan tinggi di Indonesia. *Jurnal Akuntabilitas Manajemen Pendidikan*, *9*(2), 146–158. http://journal.uny.ac.id/index.php/jamp

Puja, H., & Jarot, S. (2020). Analisis risiko sistem informasi pada RSIA Eria Bunda menggunakan metode FMEA. *Jurnal Komputer Terapan*, *8*(2), 381–390. https://jurnal.pcr.ac.id/index.php/jkt/article/view/3728

Sidik, J., Andalia, W., & Tamalika, T. (2022). Identifikasi perawatan mesin press hidrolik dengan menggunakan metode FMEA dan FTA (studi kasus di Bengkel Cahaya Ilahi). *Jambura Industrial Review*, *2*(2), 57–64.

Sinaga, B., & Rochmoeljati, R. (2024). Analisis manajemen risiko aset teknologi informasi dan pemeliharaan aset menggunakan *quantitative risk analysis* WH-TGR. *Industri*, *27*(1). http://univ45sby.ac.id/ejournal/index.php/industri/index

Thenu, P. P., Wijaya, A. F., & Rudianto, C. (2020). Analisis manajemen risiko teknologi informasi menggunakan COBIT 5. *Jurnal Bina Komputer, 2*(1), 1–13. https://doi.org/10.33557/binakomputer.v2i1.799

Yaqin, R. I., Arianto, D., Siahaan, J. P., Priharanto, Y. E., Tumpu, M., & Umar, M. L. (2022). Studi perawatan berbasis risiko sistem pelumasan mesin induk KM Mabrur dengan pendekatan FMEA. *SITEKIN: Jurnal Sains, Teknologi dan Industri, 19*(2), 218–226.