KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 3, Juli (2024), pp. 1225-1232

Analisa Manajemen Resiko Keamanan Sistem Informasi Baznas Kampar dengan Metode *Failure Mode And Effect Analysis* (FMEA)

Alriwanda[1], Eki Saputra[2], Megawati[3], Tengku Khairil Ahsyar[4]*
[1,2,3,4]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi,
Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia
E-mail: Alriwanda142@gmail.com

Abstract

Risk management is a key element in an organization's activity strategy, one of the existing risk management methods is Failure mode effect and analysis (FMEA). Many researchers use this method to determine the risks that exist in the company. This research was conducted at the National Zakat Amil Agency (BAZNAS) Kampar using FMEA to determine the risks that exist at BAZNAS. In the research, the Risk Priority Number (RPN) was calculated by multiplying Severity, Occurance and Detection. The results obtained in research using FMEA produced 5 failure modes, namely Data, Hardware, Software, People / Human Error and Network and provided recommendations to BAZNAS.

Keywords: *FMEA, BAZNAS, RPN, Risk Management, Zakat*

Abstrak

Manajemen risiko merupakan elemen kunci dalam strategi kegiatan organisasi, salah satu metode manajamen risiko yang ada adalah Failure mode effect and analysis (FMEA). Banyak penilitian yang menggunakan metode ini untuk mengetahui risiko-risiko yang ada pada perusahaan. penelitian ini dilakukan di Badan Amil Zakat Nasional (BAZNAS) Kampar menggunakan FMEA untuk mengetahui risiko-risiko yang ada pada BAZNAS. Pada penelitian dilakukan perhitungan Risk Priority Number (RPN) dengan mengkalikan Severity, Occurance, dan Detection. Hasil yang didapat pada penelitian yang menggunakan FMEA dihasilkan 5 mode kagagalan yaitu Data, Hardware, Software, People / Human Error dan Network dan memberikan rekomendasi kepada pihak BAZNAS..

Kata kunci: *FMEA, BAZNAS, RPN, Manajeman Risiko, Zakat*

1. Pendahuluan

Manajemen risiko merupakan sebuah elemen kunci dari strategi kegiatan organisasi, secara umum manajemen risiko digunakan pada setiap tingkat dari aktifitas ekonomi untuk efektifitas yang maksimal dan memiliki sistemtika yang komprehensif [1] Managemen resiko adalah suatu pembuatan keputusan yang berkontribusi terhadap tercapainya tujuan perusahaan dengan penerapan baik di tingkat aktivitas individual dan dalam bidang fungsional[2]. Penerapan managemen resiko dapat meningkatkan shareholder value yang dapat meningkatkan metode dan proses pengambilan keputusan yang sistematis dan didasarkan atas ketersediaan informasi yang digunakan sebagai pengukuran data yang akurat [3] terhadap kinerja serta menciptakan infrastruktur managemen resiko yang kokoh dalam rangka meningkatkan kualitas.

Berdasarkan Undang-Undang pengelolaan zakat nomor 23 tahun 2011 [4], yang menyebutkan bahwa zakat dikelola oleh badan amil zakat nasional BAZ) dan lembaga amil zakat (LAZ). Ini berarti pengumpulan dan penyaluran zakat akan diatur oleh suatu organisasi [5] badan amil zakat (BAZ) yang berada disetiap wilayah yang ada di

ISSN: 2720-992X

Indonesia [6][7], salah satunya berada di Provinsi Kampar. Adapun manajemen zakat pada BAZNAS Kampar saat ini dilakukan dengan dengan menggunakan sistem informasi manajemen BAZNAS atau SIMBA.

Namun sering terjadi kendala penggunaan sistem, khususnya saat penginputan data zakat yang ingin dimasukan kedalam sistem. Selain itu terdapat maslah lain yang membuat pekerjaan terhambat, penggunaan waktu yang lama dan kurang maksimal. Di tambah lagi jika ingin memasukan data ke dalam SIMBA dalam waktu lama mengakibat sistem error atau pemrosesannya melambat, belum lagi terjadinya *human error*. Oleh sebab itu, perlu dilakukan cara agar manajemen sistem BAZNAS agar lebih efektif dan efisien. Serta dapat membantu pengelola zakat dalam penyaluran kepada mustahik agar berjalan dengan cepat dan lancar, pada penelitian ini akan dilakukan manajemen resiko menggunakan metode Failure Mode And Effect Analysis (FMEA).

Manajemen risiko bertujuan untuk membuat dan melindungi serta meningkatkan kinerja, mendorong inovasi dan mendukung pencapaian tujuan[8]. Didalam manajemen risiko terdapat 4 pendekatan untuk mengelolanya yaitu *abonding excessively risky activities* atau meninggalkan aktifitas yang terlalu berisiko, *reducing the degree of risk, or its diversification* yaitu mengurangi tingkat risiko atau diversifikasi, *risk delegation by outsourcing or insurance* atau pendelegasian risiko dengan outsourcing atau pertanggungan serta metode *taking risk and creating reserves or resserves to compensate for possible losses* yaitu mengambil risiko dan menciptakan cadangan atau cadangan untuk kompensasi kemungkinan kerugian [1].

Implementasi FMEA menggunakan teknik peringkat risiko yang disebut Risk Priority Number (RPN). RPN yang dihasilkan dari penilaian risiko dari tiga parameter *Severity, Occurance dan Detection (*Keparahan, kejadian, dan deteksi)[9]. Berdasarkan penelitian sebelumnya pada penelitian ini akan menggunakan menggunakan metode fmea agar mengetahui dampak dan risiko yang akan teradi dalam sistem informasi baznas tersebut dan memberikan rekomendasi untuk penanganan dampak yang terjadi. Berdasarkan penelitian sebelumnya pada penelitian ini akan menggunakan menggunakan metode FMEA agar mengetahui dampak dan risiko yang akan teradi dalam sistem informasi BAZNAS tersebut dan memberikan rekomendasi untuk penanganan dampak yang terjadi.

2. Metodologi Penelitian

2.1. Manajemen Risiko

Pada setiap organisasi akan memperhatikan tentang keamanan dan managemen risiko sebagai suatu proses yang penting unutk diteruskan. Manajemen risiko bukanlah sesuatu yang dapat dilakukan hanya sekali. Setiap bagian dari manajemen risiko proses terpisah tetapi dapat dan akan terjadi berkali-kali [10]. Manajemen risiko merupakan proses untuk mengidentifikasi resiko, menilai resiko dan mengembangkan tindakan untuk mengurangi resiko tersebut ke tingkat yang dapat diterima oleh organisasi. [11]. Penilaian resiko dilakukan berdasarkan dari kemungkinan ancaman dari dampak yang spesifik [12]

2.2. Failure Mode and Effect Analysis (FMEA)

Salah satu pendekatan penilaian risiko yang lazim adalah FMEA yang menyajikan dan menerapkan beberapa solusi untuk menghilangkan atau mengurangi kemungkinan masalah potensial [13]. FMEA sebagai alat dalam manajemen risiko. FMEA digunakan untuk mengidentifikasi potensi kegagalan dalam proses, produk, atau layanan. Jenis metode yang paling banyak digunakan dalam manajemen risiko adalah kualitatif dan deskriptif. FMEA termasuk dalam metode semikuantitatif [14]. Berbagai penelitian yang menggunakan teknik ini, risiko telah diprioritaskan berdasarkan Risk Priority Number (RPN) yang merupakan perkalian dari tiga faktor risiko sebagai *Seveiry/*Keparahan (S), *Occurance/*Kejadian (O) dan *Detection/*Deteksi (D)[15].

Dalam managemen risiko pada umumnya digunakan metode FMEA. Hal ini dikarenakan metode ini dapat digunakan dalam berbagai jenis tingkatan dalam

manajemen organisasi atau perusahaan. FMEA dapat digunakan oleh teknisi maupun non-teknisi karena metode FMEA menggunakan bahasa yang sangat mudah dipahami [16]. Tahapan yang dilalui oleh tim peniliti yang menggunakan FMEA adalah menganalisis mode kegagalan dan mengidentifikasi 3 parameter [17] parameter yang diidentifikasi adalah (Severity, Occurance, dan Detektion) dari potensi kegagalan. Metode ini digunakan unutk mengamil data angka dan penentuan failure mode mana yang diprioritaskan.[18]. Hasil Dari FMEA dapat mempermudah manager dan teknisi dalam mengidentifikasi mode kegagalan dan kasus serta mitigasu risiko yang ada [19].

FMEA merupakan metode yang sangat masuk akal dan efektif jika dilaksanakan dengan teliti. [20] adapun prosedur pembuatan FMEA adalah :

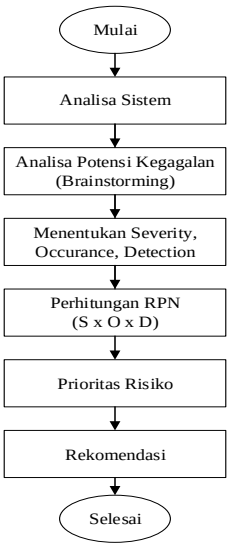
1. Idenify Proses Bisnis
2. Brainstorming Risiko
3. Mengidentifikasi potensi kegagalan berdasarkan tingkat *Severy (S), Occurence (O) dan Detection (D)*
4. Menghitung *Risk Priority Number (RPN)*

2.3. Alur Penilitian

Alur penilitian ini menujukan langkah-langkah dilalui saat melakukan penilitian. Pada penilitian ini dimulai dengan menganalisa sistem informasi yang ada pada BAZNAS Kampar dengan menggunakan diagram flowchart. Diagram tersebut didapat dari proses-proses yang ada dengan data-data yang didapat menjadi informasi. Selanjutnya setiap proses atau data yang diperoleh dianalisa setiap potensi kegagalan, dengan melakukan Brainstorming atau mencari kekuatan dan kelemahan pada organisasi ataupun sistem tersebut.

Pada tahap berikutnya akan dilakukan anilisis penyebab dari Sevrity, Occurance, dan Detection dari semua daftar potensi kegagalan. Selanjutnya setelah semua S,O,D didapatkan akan diubah dalam bentuk skala ordinal kemudain melakukan perhitungan RPN (Risk Priority Number).

Tahap selanjutnya adalah mendapatkan prioritas resiko dari hasil perhitungan RPN. Pada tahap ini setelah risiko-risiko tersebut di ukur tingkat severity, occurance dan detection, dilakukan susunan prioritas risiko mulai dari risiko yang tertinggi sampai risiko terendah. Setelah mendapatkan prioritas tertinggi dan terendah akan dibuat rekomendasi untuk menanggulangi risiko-risisko yang terjadi agar kedepannya sistem BAZNAS Kampar berjalan dengan lancar.



Gambar 1. Kerangka Penelitian

2.4. Pengumpulan Dan Pengolahan Data

Tahap pengumpulan data ini merupakan tahapan yang dilakukan untuk mengumpulkan data yang diperlukan untuk proses penilaian risiko yang akan dilakukan. Pengumpulan data dilakukan dengan cara wawancara, observasi, dan kuisioner. Pada tahap ini penulis melakukan pengumpulan data selama penelitian dilakukan.

1. Observasi
   Observasi merupakan kegiatan yang dilakukan dengan melihat langsung ke lapangan. Pada tahap ini observasi dilakukan di Badan Amil Zakat. Observasi ini bertujuan untuk mengumpulkan informasi yang dibutuhkan dan mengidentifikasi permasalahan yang ada pada perusahaan untuk mendukung penelitian.
2. Wawancara
   Wawancara merupakan suatu tahapan tanya jawab yang dilakukan peneliti pada penanggung jawab IT Badan Amil Zakat. Wawancara dilakukan untuk mengetahui masalah dan risiko yang pernah dialami.
3. Kuisioner
   Pada tahapan ini dilakukan penyebaran kuisioner yang berupa angket untuk mengumpulkan data. Kuesioner dalam penelitian ini dibuat untuk menilai risiko dari penggunaan teknologi informasi atau sistem informasi yang nantinya sesuai dengan harapan perusahaan. Pengambilan data dengan kuisioner dilakukan untuk mengetahui evaluasi aset berbasis ancaman, mengetahui tingkat risiko, mengidentifikasi aset, aset kritis penggunaan teknologi informasi pada Badan Amil Zakat menggunakan metode FMEA dengan masing- masing penilaian memiliki level tinggi, sedang dan rendah.

2.5. Variabel Penilitian

Penelitian mengguna sebuah variabel dependen yakni RPN (Risk Priority Number) dan tiga variabel Independent yakni occurrence, severity dan detection. Nilai RPN merupakan hasil kali besaran variabel occurrence, severity dan detection. Secara umum karena metode FMEA lebih sering digunakan pada ranah teknik industri semua variabel tersebut diukur per satuan produksi namun di sini karena objek yang diteliti adalah sebuah sistem informasi maka satuan yang digunakan akan disesuaikan. Berikut skala nilai dari severity, occurance dan detection

.

Tabel I. Menentukan Skala Severity

Dampak	**Peringkat**	**Kriteria**
Tidak ada akibat	1	Tidak ada dampak
Akibat Sangat Ringan	2	Tidak terganggu. Sangat sedikit berpengaruh pada kinerja sistem.
Akibat Ringan	3	Sedikit terganggu tanpa kehilangan sesuatu. Penurunan kinerja sistem.
Akibat Minor	4	Penurunan kinerja sistem secara signifikan (policy)
Akibat Moderat	5	Tidak dapat dioperasikan tanpa kerugian (Prosedur)
Akibat Signifikan	6	Tidak dapat dioperasikan dengan kerugian kecil (Proses)
Akibat Major	7	Tidak dapat dioperasikan dengan kerugian atau kerusakan peralatan.
Akibat Ekstrim	8	Tidak dapat dioperasikan dengan kegagalan yang merusak mengorbankan keamanan.
Akibat Serius	9	Potensial kegagalan atau risiko mempengaruhi keamanan sistem dengan peringatan.
Akibat Berbahaya	10	Potensial kegagalan atau risiko mempengaruhi keamanan sistem tanpa peringatan.

Tabel 2. Menentukan Skala Occurance

Kemungkinan	Peringkat	Kriteria
Kegagalan hampir/tidak pernah terjadi	1	Satu kali dalam 6-50 tahun
Kegagalan terjadi relative kecil dan sangat jarang	2	Satu kali dalam 3-6 tahun
Kegagalan terjadi relative kecil	3	Satu kali dalam 1-3 tahun
kegagalan jarang terjadi	4	Sekali dalam setahun
Kegagalan terjadi sesekali waktu	5	Satu kali dalam setahun
kegagalan terjadi saat waktu tertentu	6	Satu kali setiap 3 bulan tertentu
kegagalan sering terjadi	7	Satu kali dalam sebulan
Kegagalan terjadi berulang kali	8	Satu kali dalam seminggu
Kegagaln selalu terjadi	9	Satu kali setiap 3-4 hari
Kegagalan hampir/tidak dapat dihindari	10	Lebih dari satu kali tiap harinya

Tabel 3. Menentukan Detection

Kemungkinan Kegagalan	Peringkat	Kriteria Metode Deteksi
Hampir Pasti	1	Hampir pasti dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi.
Sangat Tinggi	2	Sangat tinggi dapat dideteksi dengan kontrol yang ada saat ini. Semua produk secara otomatis diperiksa.
Tinggi	3	Memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan.
Cukup Tinggi	4	Memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan.
Sedang	5	Memiliki tingkat efektifitas yang rata-rata.
Rendah	6	Memiliki tingkat efektifitas yang rendah.
Sangat Rendah	7	Tidak handal dalam mendeteksi tepat waktu sebulan.
Kecil	8	Tidak terbukti untuk mendeteksi tepat waktu.
Sangat Kecil	9	Tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi.
Hampir tidak mungkin	10	Kekurangan tidak dapat di deteksi.

3. Hasil Dan Pembahasan

Setelah melakukan analisa terhadap sistem BAZNAS dengan cara melihat langsung ke sistem, dan mengamatai flowchart dan dokumen atau data-data yang ada maka penilitian ini merumuskan daftar potensi kegagalan melalui Brainstorming yang mungkin terjadi. Selain menganalisa langsung terhadap sistem yang diteliti, dalam tahap ini juga melakukan studi pustaka merujuk pada literatur-literatur manajemen risiko dan keamanan sistem informasi serta wawancara langsung ke BAZNAS Kampar untuk menggali lebih banyak daftar potensi kegagalan yang mungkin terjadi. Berikut ini merupakan hasil analisis daftar potensi kegagalan:

1. Kegagalan Hardware
2. Kegagalan Software
3. Human Error
4. Data
5. Kegagalan Network

3.1. Perhitungan RPN

Setelah potensi kegagalan didapatkan, selanjutnya adalah menghitung RPN yang didapatkan dari mengkalikan Sevrity,occurance,dan Detection. Dari tiga paramater

tersebut dan diperoleh nilai RPN makan akan dijadikan landasan membuat prioritas risiko dari tertinggi sampai terendah. Berikut perhitungan RPN dapa dilihat pada tabel dibawah:

Tabel 4. Perhitungan RPN

Mode Kegagalan	SEV	OCC	DET	RPN
Hardware	5	7	2	70
Software	8	5	4	160
Human error/People	4	3	2	14
Data	9	6	4	216
Network	7	4	2	56

Dari perhitungan Sevrity, Occurance dan Detection yang telah di lakukan terdapat 5 nilai RPN yang dihasilkan. Dari 5 yang dihasilkan terdapat 4 kategory level RPN yaitu 216 di *level very high*, 160 berada di *level High*, 70-56 berada di *level medium*, dan 14 di *level low*. Dari 5 RPN yang telah dihasilkan nantinya akan diseleksi berdasarkan nilai tertinggi atau level tertinggi (*very high*) sampai ke *level low*

Tabel 5. Prioritas Risiko

Mode Kegagalan	SEV	OCC	DET	RPN	LEVEL
Data	9	6	4	216	Very High
Software	8	5	4	160	High
Hardware	5	7	2	70	Medium
Network	7	4	2	56	Medium
People/ Human Error	4	3	2	14	low

Dari Tabel 5 dapat dilihat prioritas risiko tertinggi terdapat pada mode kegagalan Data dan prioritas risiko terendah terdapat pada mode kegagalan *People/ Human Errror*. Langkah selanjutnya adalah memberikan rekomendasi yang dihasilkan dari menganalisa masalah atau risiko yang sudah didapat dari perhitungan RPN dan prioritas risiko.

Tabel 6. Rekomendasi

Mode Kegagalan	Risiko	Rekomendasi
Data	Cyber Crime	Pemasanagan aplikasi *firewall* disetiap komputer yang mengakses sistem.
Software	Kegagalan Sistem	Memakai perangkat lunak yang terbaru atau *Up to date* dan original.
Hardware	Kerusakan Komputer	Pengecekan perangkat keras yang rutin dan melakukan perawatan perangkat keras .
Network	Hilang nya jaringan	Memiliki jaringan cadangan.
People/ Human Error	Human Error	Pelatihan pegawai untuk memahami sistem agar lebih mudah dalam penggunanan sistem.

3.2. Hasil

Dari perhitungan RPN dan prioritas risiko yang sudah didapat selanjutnya memberikan rekomendasi agar penggunaan sistem dan proses yang ada pada BAZNAS dapat berjalan dengan lancar. Berikut tabel Rekomendasi*:*

Tabel 7. Rekomendasi

Mode Kegagalan	Risiko	Rekomendasi
Data	Cyber Crime	Pemasanagan aplikas *firewall* disetiap komputer yang mengakses sistem.
Software	Kegagalan	Memakai perangkat lunak yang terbaru

Mode Kegagalan	Risiko	Rekomendasi
	Sistem	atau *Up to date* dan original.
Hardware	Kerusakan Komputer	Pengecekan perangkat keras yang rutin dan melakukan perawatan perangkat keras .
Network	Hilang nya jaringan	Memiliki jaringan cadangan.
People/ Human Error	Human Error	Pelatihan pegawai untuk memahami sistem agar lebih mudah dalam penggunanan sistem.

Berdasarkan penilitian sebelumnya yang menganalisa dengan menggunakan Metode FMEA, memberikan rekomendasi-rekomendasi yang berguna bagi pihak perusahaan untuk meminimalisir kerugian atau mencegah risiko yang akan terjadi.

4. Kesimpulan

Berdasarkan penilitian yang telah dilakukan dapat diambil kesimpulan bahwa hasil rekomendasi yang telah didapat ada 5 rekomendasi yaitu pemasangan aplikasi firewall disetiap komputer agar tidak terjadi nya Cybercrime , memakai perangkat lunak yang terbaru dan original, melakukan pengecekan perangkat keras yang rutin dan melakukan perawatan perangkatkeras, menambahkan jaringan cadangan apabila terjadi kehilangan jaringan dan pelatihan bagi pegawi untuk memahi sistem yang ada agar memudahkan dalam penggunaan sistem. Hasil rekomendasi ini dapat menajadi acuan bagi pihak BAZNAS untuk mengevaluasi sistem dan proses-proses yang ada didalam perusahaan agar memudahkan pekerjaan dan menimalisir adanya risiko atau kegagalan sistem.

Daftar Pustaka

[1] Svitlana Filyppova, Iryna Bashynska, Borys Kholod, Larysa Prodanova, Larysa Ivanchenkova and Viacheslav Ivanchenkov, “Risk Management Through Systematization: Risk Management Culture”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Vol 8,2019, doi : 10.35940/ijrte.C5601.098319.

[2] Fikri, A. Fachryana. Managemen Risiko Strategis Bank Syariah. Jurnal Managemen, Ekonomi, Keuangan dan Akuntansi. 2020. Vol 1 No 2:61-66

[3] Irfan, M.dan Susilowati, I.H. Analisa MAnagemen Risiko K3 dalam Industri Manuactur di Indonesia : Literature Review. 2021. Jurnal Kesehatan Masyarakat, 5(1): 335-343.

[4] Sri Kusriyah, “Government Policy In Achieving Community Welfare Through The Effectiveness Of Management Of Zakat In Indonesia”, Journal of Critical Reviews, ISSN-2394-5125, Vol 7, Issue 5, 2020, doi:

[5] Khabib, N., Ulil, A,A Ana,F. Lora, L dan Muammar, T.L. Pengaruh Akuntabilitas dan Transparansi terhadap Minat Muzakki Membayar Zakat di BAZNAS Seragen. 2021. Jurnal Ilmiah Ekonomi Islam. Vol 7(1):341-349.

[6] A. Rio Makkulau Wahyu dan Wirani Aisiyah Anwar, “Management of Zakat at BAZNAS Regency Sidrap During COVID-19’s Pandemic”, jurnal iqtisaduna, 2020, doi: 10.24252/iqtisaduna.v1i1.15807

[7] Ahmad Roziq, Agung Budi Sulistiyo, Moch. Shulthoni, dan Eza Gusti Anugerah, “An Escalation Model of Muzakki’s Trust and Loyalty towards Payment of Zakat at BAZNAS Indonesia”, Journal of Asian Finance, Economics and Business Vol 8 No 3 (2021) 0551–0559, doi:10.13106/jafeb.2021.vol8.no3.0551

[8] Mustafa Jahangoshai Rezaee, Samuel Yousefi, Milad Eshkevari, Mahsa Valipour and Morteza Saberi, “Risk analysis of health, safety and environment in chemical industry integrating linguistic FMEA, fuzzy inference system and fuzzy DEA”, Stochastic Environmental Research and Risk Assessment (2020) 34:201–218, doi:10.1007/s00477-019-01754-3

[9] Apol Pribadi Subriadi, Nina Fadilah Najwa, “The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment”, heliyon 6 , 2020, doi:10.1016/j.heliyon.2020.e03161..

[10] Jikrillah, S., Ziyad, M dan Doni, S. Analisis Managemen Risiko Terhadap Keberlangsungan Usaha UMKM Di Kota Banjarmasin. 2021. Jurnal Wawasan Managemen. Vol 9(2).
[11] Ngamal, Yohanes. Penerapan Model Managemen Risiko Teknologi Digital Di Lembaga Perbankan Berkaca Pada Cetak Biru Transformasi Digital Perbankan Indonesia. 2022. Jurnal Managemen Risiko. Vol 2 (2)
[12] Nagita. B. F, Rachma, H. dan Murdiyati, D. Fungsi Internal Audit Dan Managemen Risiko Perusahaan : Sebuah Tinjauan Literatur. 2022. Jurnal Bisnis Dan Akuntansi. Vol 24(1):59-70
[13] Pinnarat Nuchpho, Santirat Nansaarng, and Adisak Pongpullponsak, "Modified Fuzzy FMEA Application in the Reduction of Defective Poultry Products", Engineering Journal Volume 23 Issue 1, Januari 2019, doi:10.4186/ej.2019.23.1.171..
[14] Nina Fadilah Najwa, Apol Pribadi Subriadi, Okfalisa, Eki Saputra and Muhammad Ariful Furqon, "The FMEA Traditional Modifications (FMEA Improvement) in IT Risk Assessment", International Applied Business and Engineering Conference 2021, E-ISSN : 2798 – 4664.
[15] Cahyani, D.P., Nastiti,H dan Renny, H. Analisis Risiko Operasional dengan Metode FMEA. 2022. Jurnal Akuntansi, Ekonomi dan Managemen Bisnis. Vol 10(2):177-186
[16] Darsini, Adhi, R.P dan Maria, P. Managemen Risiko Keselamatan Dan Kesehatan Kerja Pada Proyek Pembangunan Bendungan XYZ dengan Metode FMEA.Jural Infokar. Vol 6(1)
[17] Xiaojun Wu and Jing Wu, "The Risk Priority Number Evaluation of FMEA Analysis Basedon Random Uncertainty and Fuzzy Uncertainty", hindawi, Volume 2021, Article ID 8817667, 15 pages, doi:10.1155/2021/88176.
[18] Munaroh, L., Amrozi, Y dan Risky. 2021. Pengukuran Risiko Keamanan Aset TI menggunakan Metode FMEA dan Standar ISO / IEC 27001: 2013. Jurnal Teknomedia UIN Sunan Ampel Surabaya. Vol 5(2)
[19] Fajar, M. Kusnadi dan Fahriza, N. 2022, usulan Perbaikan Risiko Kecelakaan Kerja Dengan Metode FMEA dan Fishbone Diagram. Jurnal Pengabdian Masyarakat Berkemajuan . Selaparang. Vol 6 (1).
[20] Ningsih, S. S., Nur, F. S., Idria M dan Nesda, E. R. 2024. Penggunaan Metode FMEA Dalam Penilaian Managemen Risiko Keamanan Sistem Informasi Rumah Sakit. Jurnal Inovtek Polbeng. Seri Informatika. Vol 9(1).