ANALISIS MANAJEMEN RESIKO APLIKASI INLIS LITE PADA PERPUSTAKAAN KANTOR DPRD KOTA SALATIGA MENGGUNAKAN FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

Akwila Engka[1], Melkior Sitokdana[2]
[1,2]Program Studi Sistem Informasi Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
e-mail: [1]682019060@student.uksw.edu, [2]melkior.sitokdana@uksw.edu

ABSTRAK

Aplikasi INLIS LITE adalah aplikasi yang dikembangkan dan dibangun secara resmi oleh Perpustakaan Nasional Republik Indonesia. Aplikasi ini digunakan untuk membantu proses kegiatan pengelolaan bahan Pustaka di Perpustakaan, namun tidak dapat dipungkiri Aplikasi Inlis Lite pasti memiliki kemungkinan permasalahan yang akan mengganggu fungsi dari pada aplikasi tersebut. Dalam menggunakan teknologi informasi maka digunakan metode Failure Mode & Effect Analysis (FMEA) pada Perpustakaan Kantor DPRD Kota Salatiga yang bertujuan untuk menganalisis risiko yang dihadapi dan langkah-langkah yang diambil untuk meminimalkan risiko. Dari hasil penelitian di dapatkan bahwa terdapat 22 penyebab kegagalan terdapat 1 aktivitas kategori High (Tinggi), 17 aktivitas kategori Low (Rendah) dan 4 dengan kategori Very Low (Sangat Rendah).

ABSTRACT

The INLIS LITE application is officially developed by the National Library of the Republic of Indonesia. While it aids in the management of library materials, it is acknowledged that the application may encounter potential issues. To address this, Information Technology utilizes the Failure Mode and Effect Analysis (FMEA) method at the Library of the City DPRD Salatiga, aiming to analyze risks and implement measures to minimize them. The research revealed 22 failure causes, with 1 falling into the High category, 17 in the Low category, and 4 in the Very Low category.

Kata kunci: Failure Mode & Effect Analysis (FMEA), INLIS LITE, Manajemen Resiko.

PENDAHULUAN

Pada saat ini perkembangan zaman dan teknologi informasi semakin berkembang pesat, perkembangan ini disebabkan semakin meningkatnya kebutuhan aktifitas manusia untuk menggunakan teknologi informasi, kebutuhan seperti Pemerintahan, Pendidikan dan juga bisnis pada saat ini sangat bergantung pada teknologi informasi, begitu juga dengan Perpustakaan kantor DPRD Kota Salatiga, dengan adanya aplikasi pada kantor DPRD Kota Salatiga memudahkan bagi para staff atau pegawai dalam menelusuri dan mencari informasi koleksi yang ada pada perpustakaan. Maka dari pada itu diperlukan

ISSN 2798-141X

analisis manajemen resiko pada aplikasi yang digunakan pada Perpustakaan kantor DPRD Kota Salatiga agar bisa melihat atau meminimalisir kekurangan, kelemahan dan resiko yang ada pada aplikasi tersebut.

Inlis Lite (*Intergrated Library System*) adalah aplikasi perangkat lunak (software) yang dikembangkan dan dibangun secara resmi oleh Perpustakaan Nasional Republik Indonesia dari tahun 2011. Aplikasi ini digunakan untuk membantu proses kegiatan pengelolaan bahan Pustaka di Perpustakaan, namun tidak dapat dipungkiri Aplikasi Inlis Lite pasti memiliki kemungkinan permasalahan yang akan mengganggu fungsi dari pada aplikasi tersebut, dalam menggunakan teknologi informasi. Organisasi juga harus memiliki kebijakan dan manajemen keamanan, serta keahlian dalam pemeliharaan aset terkait teknologi informasi, sumber daya manusia, dan layanan. Dengan bantuan manajemen risiko, risiko dan ancaman yang terjadi dapat diminimalkan.

Manajemen diperlukan tidak hanya untuk menjamin keamanan sumber daya informasi, tetapi juga untuk menjaga fungsi perusahaan setelah terjadi bencana atau pelanggaran sistem keamanan. Kegiatan yang berkaitan dengan keamanan aset informasi disebut manajemen keamanan informasi (Ramadhani, 2018). Penerapan manajemen risiko membantu mengembangkan strategi untuk mencapai tujuan perusahaan, menjaga keseimbangan kepentingan seluruh stakeholder dan melindungi kebijakan sumber daya perusahaan. Untuk memastikan bahwa praktik manajemen risiko dapat memberikan dampak positif terhadap tata kelola perusahaan, sepanjang praktik manajemen risiko konsisten dengan prinsip dan prosedur manajemen risiko (Sari dkk, 2022). Tujuannya adalah untuk menemukan, memprediksi, dan merespons risiko dari berbagai sumber, termasuk organisasi, politik, lingkungan, manusia, dan teknologi. Untuk mengelola suatu organisasi secara efektif, penting untuk dapat menentukan sejauh mana kemajuan organisasi tersebut (Yudha dkk, 2023).

Ada berbagai metode dan alat untuk melakukan analisis manajemen risiko dan salah satu yang paling sering digunakan adalah FMEA (*Failure Mode & Effect Analysis*). FMEA adalah metode terstruktur dimana jenis kegagalan dapat diidentifikasi, diprioritaskan dan dicegah jika memungkinkan. Dengan FMEA, sumber kesalahan dan masalah kualitas dapat ditelusuri. FMEA dapat membantu mengidentifikasi risiko dari setiap mode kegagalan potensial menentukan dampak dari setiap kegagalan, memprioritaskan risiko dari mode kegagalan yang teridentifikasi, dan membantu mengambil tindakan korektif yang tepat untuk mengurangi kemungkinan kegagalan dan mencegah kecelakaan yang berbahaya.

Berdasarkan permasalahan yang ada, maka dirasa perlu untuk melakukan sebuah analisis manajemen resiko pada aplikasi Inlise Lite menggunakan metode FMEA yang bertujuan untuk menganalisis risiko yang dihadapi dan langkah-langkah yang diambil untuk meminimalkan risiko dan dapat mengambil tindakan pencegahan sebaik mungkin sehingga potensi risiko tidak terjadi dan mengganggu oprasional perpustakaan.

KAJIAN TEORI

Penelitian Terdahulu

Analisis Manajemen Resiko menggunakan *Failure Mode and Effect Analysis* (FMEA) yang dilakuakan oleh Yesi Ramayani (2022) pada Sistem Informasi Akademik

ISSN 2798-141X

UIN Raden Fatah Palembang terdapat 11 mode identifikasi potensi risiko dan kesalahan pada SIMAK, 6 kategori sangat tinggi, tinggi, sedang, rendah, sangat rendah dan hampir tidak ada kesalahan. Berdasarkan kategori tersebut, terdapat 1 poin sangat tinggi, 3 poin tinggi, 4 poin sedang, 3 poin rendah, 6 poin sangat rendah, dan 1 poin mendekati nol tidak ada kegagalan(Ramayani, 2022).

Analisis risiko mengunakan *Failure Mode and Effect Analysis* (FMEA) yang dilakuakan oleh Rizqi Ilmal Yaqin dkk (2020) pada Bahan Bakar Mesin Induk KM. Sidomulyo, dari hasil pemeliharaan menggunakan FMEA teridentifikasi bahwa komponen injector dan filter bahan bakar adalah komponen yang harus diprioritaskan. Komponen injektor dan filter bahan bakar memiliki *Risk Priority Number* (RPN) masing-masing 192 dan 168. Prioritas servis didasarkan pada RPN komponen yang melebihi RPN kritis sistem bahan bakar utama mesin dan termasuk komponen yang diprioritaskan dalam diagram Pareto (Yaqin dkk, 2020).

Manajemen resiko mengunakan metode *Failure Mode and Effect Analysis* (FMEA) yang dilakuakan oleh Kori Puspita Ningsi (2020) pada RS Condong Catur Yogyakarta manajemen resiko tersebut terdapat 6 proses beresiko dan terdapat 15 mode kegagalan, yaitu 7 jenis kesalahan berpotensi disebabkan oleh Sumber Daya Manusia (SDM), 4 jenis kesalahan berpotensi disebabkan oleh infrastruktur dan 4 jenis kesalahan disebabkan oleh sistem. Setelah dilakukan redesign, nilai RPN tertinggi mengalami penurunan pada prosedur penyimpanan pada error mode "petugas yang mengerjakan rekam medis tidak sesuai dengan urutan *Terminal Digit Storage* (TDF) system" dengan nilai RPN diturunkan dari 336 menjadi 72 (Ningsih dkk., 2020).

Manajemen Resiko mengunakan *Failure Mode and Effect Analysis* (FMEA) yang dilakuakan oleh Mutia Sari Zulvi (2022) pada Diskominfo pemprov Riau hasil Analisis yang potensi kegagalan terbesar adalah kerusakan perangkat keras akibat pemeliharaan yang tidak teratur dan penggunaan RPN 144 yang tidak tepat. Berdasarkan analisis yang dilakukan, dimungkinkan untuk mengidentifikasi potensi kesalahan mana yang memiliki nilai RPN tertinggi dan harus diprioritaskan terlebih dahulu (Zulvi, 2022).

Analisis Resiko menggunakan pendekatan *Failure Mode and Effect Analysis* (FMEA) yang dilakuakan oleh Hafidh Munarwih (2020) pada PT. Kubota Indonesia terhadap Downtime pada Line Crank Case terdapat 20 jenis gangguan pada mesin HN 50 C pada line crank case dengan downtime sebesar 2262 menit dengan nilai RPN tertinggi yaitu Ls shutter dan kabel pada kegagalan fungsional APC (*Auto Pallet Change*) dan yang tidak normal sebesar 288 (Munawir dkk, 2020).

Berdasarkan kajian tersebut, peneliti akan melakukan analisis manajemen resiko aplikasi Inlise Lite menggunakan metode *Failure Mode & Effect Analysis* (FMEA) yang bertujuan untuk mengidentifikasi resiko dari setiap kegagalan, menentukan dampak dan membantu mengambil tindakan agar mengurangi kemungkinan kegagalan, sehingga pencegahan dapat dilakukan dengan sebaik mungkin dan tidak menghambat proses pelaksanaan kinerja Perpustakaan kantor DPRD Kota Salatiga.

Landasan Teori

Manajemen risiko menekankan pada berbagai tindakan, mengidentifikasi (*Risk Indentification*), menilai (*risk assessment*), pengontrolan dan meminimalkan risiko (*risk*

ISSN 2798-141X

minimise and control) yang mungkin timbul. Manajemen risiko dalam evaluasi proyek adalah proses evaluasi yang mengoptimalkan tujuan proyek. Beberapa dari hasil ini mungkin bertentangan dengan rencana semula. Pendekatan evaluasi proyek membantu manajer proyek membuat Keputusan (Sandyavitri, 2008).

Analisis manajemen risiko adalah kegiatan manajemen yang secara sistematis mencari dan menganalisis bentuk kerugian apa yang mungkin diderita perusahaan dari risiko dan metode pengendalian apa yang paling cocok untuk menangani kerugian terkait bisnis, besarnya keuntungan Perusahaan (Putri dan Irnanda, 2022).

FMEA telah banyak digunakan dalam dunia industri. Dasar FMEA pertama kali diambil dari metode standar FMECA (*Failure Mode, Effect, Critical Analysis*), yang dijelaskan dalam dokumen militer US Army MIL-P-1629 (1949). Pada awal 1960-an, kontraktor Badan Penerbangan dan Antariksa Nasional (NASA) menggunakan varian FMECA yang dikenal sebagai FMEA (Budiarto, 2017).

FMEA juga secara sistematis mengidentifikasi konsekuensi dari kegagalan sistem atau proses dan mengurangi atau menghilangkan potensi kegagalan. FMEA adalah dokumen yang hidup dan oleh karena itu harus diperbarui secara berkala agar dapat digunakan untuk pencegahan dan prediksi kegagalan (Hendra dan Effendi, 2018).

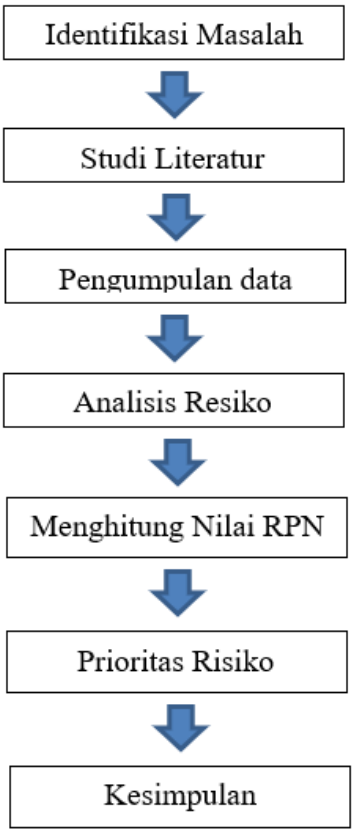
METODE PENELITIAN

Metode yang di gunakan dalam penelitian ini adalah metode kualitatif. Dalam penelitian kualitatif, konseptualisasi, klasifikasi, dan deskripsi dikembangkan berdasarkan "peristiwa" yang diperoleh selama kerja lapangan (Sandre dkk, 2021). Oleh karena itu, tidak mungkin memisahkan fungsi pengumpulan data dan analisis data. Keduanya terjadi secara bersamaan, prosesnya bersifat siklis dan interaktif, tidak linier (Rijali, 2019).

Analisis risiko adalah kegiatan yang, dengan mempertimbangkan tindakan pengendalian yang dilakukan, menentukan tingkat probabilitas/frekuensi risiko yang terjadi dan pengaruhnya terhadap pencapaian tujuan (Yunarto, 2022). Seperti yang dapat dilihat pada Gambar 1, penelitian ini terdiri dari beberapa langkah, diantaranya :

1. Identifikasi Masalah: Pada tahap ini peneliti memperoleh pemahaman tentang masalah yang dihadapi untuk menghasilkan solusi.
2. Studi Literatur: Pada tahap ini, peneliti melakukan penelitian terhadap penelitian terdahulu yang relevan dan teori-teori yang menjadi landasan penelitian.
3. Pengumpulan Data: Tahap ini peneliti melakukan pengumpulan data dengan metode kualitatif. Proses yang dilakuan dalam pengumpulan data yaitu observasi dan wawancara, pada proses Observasi dilakukan untuk melihat secara langsung proses-proses yang sedang terjadi pada Perpustakaan Kantor DPRD Kota Salatiga dan pada tahapan wawancara peneliti melakukan wawacara kepada pegawai *IT Operation Support* (Sudibyo Budi Susanto A.Md) tentang INLIS Lite pada Perpustakaan Kantor DPRD Kota Salatiga.
4. Analisis Resiko: Pada tahap ini peneliti melakukan analisis resiko sesuai dengan pendekatan *Failure Mode and Effect Analysis* (FMEA). Dimana terdapat sepuluh tahap analisis resiko.

ISSN 2798-141X



Gambar 1. Diagram Tahapan Penelitian

5. Menghitung Nilai RPN (*Risk Priority Number*): Tahap ini melakukan perhitungan Nilai RPN (*Risk Priority Number*) dengan mengkalikan *Severity*, *Occurrence*, dan *Detection*.
6. Prioritas Risiko: Prioritas Risiko membantu mengetahui kesalahan mana yang memiliki risiko tertinggi. Kategori yang digunakan untuk menetapkan prioritas risiko berdasarkan hasil perhitungan nilai RPN.
7. Kesimpulan: Pada fase ini dilakukan penarikan kesimpulan berdasarkan hasil analisis risiko dan usulan penelitian selanjutnya.

HASIL PENELITIAN DAN PEMBAHASAN

Review the process or product

Pada Langkah pertama proses ini, peneliti melakukan wawancara terhadap salah satu pegawai Perpustakaan Kantor DPRD Kota Salatiga yang merupakan *IT Operation Support*. Dalam proses wawancara didapatkan bahwa sistem yang bermigrasi baru berjalan kurang lebih satu tahun ini, dalam proses ini ada beberapa kesalahan yang terjadi dalam proses migrasi.

Daftar aset tersedia di Perpustakaan Kantor DPRD Kota Salatiga dari hasil wawancara dapat dilihat pada Tabel 1.

ISSN 2798-141X

Tabel 1. Daftar Aset

Table Aset	
kategori	Aset
Data	Data user, Data anggota, Data Buku
Software	Aplikasi Inlis Lite,Sistem Operasi, Softwere.
Hardware	Personal Computer, Server Database.
SDM	Admin,Umum,*User*.

Dari hasil Identifikasi kemungkinan resiko, ditemukan kemungkinan resiko atau ancaman yang berasal dari alam, manusia, dan sistem atau infrastruktur dari aplikasi Inlis Lite seperti yang dijabarkan pada Tabel 2.

Tabel 2. Identifikasi Risiko

Faktor	**Code**	**Kemungkinan Resiko**
Alam/Lingkungan	RBS-01	Gempa Bumi
	RBS-02	Kebakaran
	RBS-03	Banjir
	RBS-04	Petir
Manusia	RBS-05	Penyalagunaan Hak Akses
	RBS-06	Human Error
	RBS-07	Haking
	RBS-08	Pencurian data/perangkat keras
	RBS-09	UI design yang sulit dipahami
Sistem/Infrastruktur	RBS-10	Trouble Web Server
	RBS-11	Server Down
	RBS-12	Listrik Padam Secara Tiba-Tiba
	RBS-13	Koneksi Jaringan Gangguan
	RBS-14	Kerusakan Hardware
	RBS-15	Data Corrupt

Brainstrom Potential Failure Modes

Kesalahan dalam sistem informasi yang mengganggu proses bisnis Aplikasi, perlu untuk mengidentifikasi titik lemah dari sistem informasi yang ada. Tabel 3 merupakan *failure mode*.

Tabel 3. Potential Failure Modes

Code	**Potential Failure Modes**
RBS-01	Pergerakan kerak bumi atau gunung meletus
RBS-02	Hubungan arus pendek/korsleting Listrik
RBS-03	Adanya hujan lebat dan peningkatan volume air yang mengakibatkan air meluap
RBS-04	Adanya perbedaan potensi antara awan dengan bumi dan awan lainya
RBS-05	Pegawai memberikan hak akses ke orang lain
	tidak mengganti password secara berkala
RBS-06	Kelalaian dalam pengimputan data
	Meiliki data yang tidak lengkap/update

ISSN 2798-141X

Code	Potential Failure Modes
RBS-07	Penipuan melalui rekayasa social
	Password yang digunakan secara berulang-ulang
	Antivirus yang tidak pernah di update
RBS-08	Kurangnya keamanan dari pihak kantor
RBS-09	Kurangnya pengetahuan dari pengguna
RBS-10	Terblokirnya Akses IP
	Ada masalah pada Domain Name Server (*DSN*)
RBS-11	Terjadi lonjakan traffic pengunjung/pengguna melebihi kemampuan server
RBS-12	Terjadi gangguan kerusakan langsung pada generator sehingga listrik mengalami kesulitan pulih dengan cepat
RBS-13	Jaringan yang terlalu sibuk
	Perangkat pada jaringan yang memenuhi batas
RBS-14	Masuknya virus ke software yang mengakibatkan kerusakan pada hardwere
	Penggunaan yang tidak sesuai prosedur
RBS-15	Data atau file mengalami kerusakan

List Potential Failure Mode

Kegagalan pada Aplikasi Inlise Lite yg menghambat proses bisnis yang sedang berjalan. Mengenai kesalahan yang terjadi dapat dilihat pada Tabel 4.

Tabel 4. List Potential Failure

	Code	Potential Failure Mode
Sistem Aplikasi Inlis Lite (Graphasoft)	RBS-02	Hubungan arus pendek/korsleting Listrik
	RBS-O3	Adanya hujan lebat dan peningkatan volume air yang mengakibatkan air meluap
	RBS-O4	Adanya perbedaan potensi antara awan dengan bumi dan awan lainnya
	RBS-O5	Pegawai memberikan hak akses ke orang lain
		tidak mengganti password secara berkala
	RBS-O6	Kelalaian dalam pengimputan data
		Meiliki data yang tidak lengkap/update
	RBS-O7	Penipuan melalui rekayasa social
		Password yang digunakan secara berulang-ulang
		Antivirus yang tidak pernah di update
	RBS-O8	Kurangnya keamanan dari pihak kantor
	RBS-O9	Kurangnya pengetahuan dari pengguna
	RBS-11	Terjadi lonjakan traffic pengunjung/pengguna melebihi kemampuan server
	RBS-12	Terjadi gangguan kerusakan langsung pada generator sehingga listrik mengalami kesulitan pulih dengan cepat
	RBS-13	Jaringan yang terlalu sibuk
		Perangkat pada jaringan yang memenuhi batas
	RBS-14	Masuknya virus ke software yang mengakibatkan kerusakan pada hardwere

ISSN 2798-141X

		Penggunaan yang tidak sesuai prosedur
	RBS-15	Data atau file mengalami kerusakan

Assign a Severity Ranking for Each Effect

Berdasarkan hasil wawancara dengan pegawai *IT Operation Support*, Tabel 5 adalah hasil penentuan rating keparahan (*severity*) dari setiap kemungkinan kegagalan pada sistem informasi.

Table 5. Tabel Severity

Code	Potesni Kegagalan	Rating	Keterangan
RBS-01	Gempa Bumi	3	Menyebabkan Sedikit terhambat
RBS-02	Kebakaran	6	Menyebabkan terjadinya gangguan
RBS-03	Banjir	3	Menyebabkan Sedikit terhambat
RBS-04	Petir	5	Menyebabkan gangguan
RBS-05	Penyalahgunaan Hak Akses	4	Menyebabkan Sedikit terhambat
RBS-06	Human Error	6	Menyebabkan gangguan
RBS-07	Hacking	4	Menyebabkan Sedikit terhambat
RBS-08	Pencurian Data/Perangkat keras	3	Menyebabkan Sedikit terhambat
RBS-09	UI Design yang Sulit di pahami	3	Menyebabkan Sedikit terhambat
RBS-10	Trouble Web Site	3	Menyebabkan Sedikit terhambat
RBS-11	Server Down	3	Menyebabkan Sedikit terhambat
RBS-12	Listrik Padam Secara Tiba-Tiba	5	Menyebabkan gangguan
RBS-13	Koneksi Jaringan Gangguan	6	Menyebabkan gangguan
RBS-14	Kerusakan Hardware	3	Menyebabkan Sedikit terhambat
RBS-15	Data Corrupt	3	Menyebabkan Sedikit terhambat

Assign an Occurent Ranking for Each Effect

Pada tahap selanjutnya peneliti mendapatkan nilai dari *Occurent* dari setiap kegagalan yang ditunjukan pada Tabel 6.

Tabel 6. Tabel *Occurent*

Potensi Kegagalan	Penyebab Kegagalan	Occurent
Gempa Bumi	Pergerakan kerak bumi atau gunung Meletus	3
Kebakaran	Hubungan arus pendek/korsleting Listrik	3
Banjir	Adanya hujan lebat dan peningkatan volume air yang mengakibatkan air meluap	2
Petir	Adanya perbedaan potensi antara awan dengan bumi dan awan lainya	5
Penyalah Gunaan Akses	Pegawai memberikan hak akses ke orang lain	2
	tidak mengganti password secara berkala	3
Human Error	Kelalaian dalam pengimputan data	4
	Meiliki data yang tidak lengkap/update	4
Hacking	Penipuan melalui rekayasa social	3
	Password yang digunakan secara berulang-ulang	3
	Antivirus yang tidak pernah di update	4

ISSN 2798-141X

Potensi Kegagalan	Penyebab Kegagalan	Occurent
Pencurian Data/Perangkat Keras	Kurangnya keamanan dari pihak kantor	3
UI Design yang sulit dipahami	Kurangnya pengetahuan dari pengguna	2
Trouble Web Server	Terblokirnya Akses IP	2
	Ada masalah pada Domain Name Server (*DSN*)	4
Server Down	Terjadi lonjakan traffic pengunjung/pengguna melebihi kemampuan server	4
Listrik Padam Secara Tiba-Tiba	Terjadi gangguan kerusakan langsung pada generator sehingga listrik mengalami kesulitan pulih dengan cepat	5
Koneksi Jaringan Gangguan	Jaringan yang terlalu sibuk	3
	Perangkat pada jaringan yang memenuhi batas	5
Kerusakan Hardwere	Masuknya virus ke software yang mengakibatkan kerusakan pada hardwere	3
	Penggunaan yang tidak sesuai prosedur	2
Data Corrupt	Data atau file mengalami kerusakan	3

Assign a Detection Ranking for Each Effect

Pada tahap ini peneliti menemukan nilai *Detection* dari setiap kegagalan seperti yang ditunjukan pada Tabel 7.

Tabel 7. Tabel Detection

Potensi Kegagalan	Penyebab Kegagalan	Identifikasi Pencegahan	Detection
Gempa Bumi	Pergerakan kerak bumi atau gunung Meletus	Menyediakan *server* cadangan dan tempat yang aman	2
Kebakaran	Hubungan arus pendek/korsleting Listrik	Menyediakan penyemprot api dan memiliki air yang cukup	2
Banjir	Adanya hujan lebat dan peningkatan volume air yang mengakibatkan air meluap	membangun saluran air/membersihkanya agar ketiga hujan lebat air tidak meluap	2
Petir	Adanya perbedaan potensi antara awan dengan bumi dan awan lainya	Menyiapkan alat penangkal petir	2
Penyalah Gunaan Akses	Pegawai memberikan hak akses ke orang lain	Memberikan sanksi kepada staff/kariawan sesuai kebijakan yang berlaku	4
	Tidak mengganti password secara berkala	Mengganti pasasword secara berkala	4
Human Error	Kelalaian dalam pengimputan data	Lebih teliti dalam mengimput data	2
	Meiliki data yang tidak lengkap/update	Mengupdate data secara berkala	3

ISSN 2798-141X

Potensi Kegagalan	Penyebab Kegagalan	Identifikasi Pencegahan	Detection
Hacking	Penipuan melalui rekayasa social	melakukan pemblokiran terhadap situs/link yang dianggap berbahaya	5
	Password yang digunakan secara berulang-ulang	kata sandi diganti secara berkala untuk meminimalisir terjadinya hacking	2
	Antivirus yang tidak pernah di update	Melakukan update secara berkala untuk mengantisipasi virus masuk	3
Pencurian Data/Perangkat Keras	Kurangnya keamanan dari pihak kantor	Pemasangan video surveillance (cctv) di setiap sudut rawan	2
UI Design yang sulit dipahami	Kurangnya pengetahuan dari pengguna	Melakukan pelatihan terhadap pengguna	3
Trouble Web Server	Terblokirnya Akses IP	melakukan pengecekan status website atau memuali ulang internet	4
	Ada masalah pada *Domain Name Server* (DSN)	melakukan pembersihan terhadap chace dan merefresh konfigurasi DSN	4
Server Down	Terjadi lonjakan traffic pengunjung/pengguna melebihi kemampuan server	Melakukan pemeriksaan beban/penggunaan server secara berkala	3
Listrik Padam Secara Tiba-Tiba	Terjadi gangguan kerusakan langsung pada generator sehingga listrik mengalami kesulitan pulih dengan cepat	menyediakan UPS sebagai dukungan sementara	2
Koneksi Jaringan Gangguan	Jaringan yang terlalu sibuk	Melakukan pengecekan terhadap jaringan	3
	Perangkat pada jaringan yang memenuhi batas	Mengupdate driver wireless network	4
Kerusakan Hardwere	Masuknya virus ke *software* yang mengakibatkan kerusakan pada *hardwere*	Memasang antivirus pada s*oftware*	4
	Penggunaan yang tidak sesuai prosedur	Mempelajari prosedur sebelum digunakan	3
Data Corrupt	Data atau file mengalami kerusakan	Membersihkan data yang tidak perlu	3

Calculate RPN Value

Setelah mendapatkan nilai dari *Severiti*, *Occurrence* dan *Detection* kemudian pada tahap selanjutnya adalah menghitung nilai PRN (*Risk Priority Number*). RPN memiliki nilai Masimal 1000, karena nilai yang di dapat dari *Severiti*, *Occurrence* dan *Detection* ialah 10 seperti yang ditunjukan pada Tabel 8.

ISSN 2798-141X

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

Tabel 8. Tabel RPN

Potensi Kegagalan	Penyebab Kegagalan	RPN
Gempa Bumi	Pergerakan kerak bumi atau gunung meletus	18
Kebakaran	Hubungan arus pendek/korsleting Listrik	36
Banjir	Adanya hujan lebat dan peningkatan volume air yang mengakibatkan air meluap	36
Petir	Adanya perbedaan potensi antara awan dengan bumi dan awan lainya	50
Penyalah Gunaan Akses	Pegawai memberikan hak akses ke orang lain	32
	tidak mengganti password secara berkala	48
Human Error	Kelalaian dalam pengimputan data	48
	Memiliki data yang tidak lengkap/update	72
Hacking	Penipuan melalui rekayasa social	60
	Password yang digunakan secara berulang-ulang	24
	Antivirus yang tidak pernah di update	48
Pencurian Data/Perangkat Keras	Kurangnya keamanan dari pihak kantor	18
UI Design yang sulit dipahami	Kurangnya pengetahuan dari pengguna	18
Trouble Web Server	Terblokirnya Akses IP	24
	Ada masalah pada Domain Name Server (*DSN*)	48
Server Down	Terjadi lonjakan traffic pengunjung/pengguna melebihi kemampuan server	36
Listrik Padam Secara Tiba-Tiba	Terjadi gangguan kerusakan langsung pada generator sehingga listrik mengalami kesulitan pulih dengan cepat	50
Koneksi Jaringan Gangguan	Jaringan yang terlalu sibuk	54
	Perangkat pada jaringan yang memenuhi batas	120
Kerusakan Hardwere	Masuknya virus ke software yang mengakibatkan kerusakan pada hardwere	36
	Penggunaan yang tidak sesuai prosedur	18
Data Corrupt	Data atau file mengalami kerusakan	27

Dalam evaluasi yang di lakukan terhadap 22 penyebab kegagalan terdapat 1 kegagalan yang beresiko *High* (Tinggi), 17 beresiko *Low* (Rendah) dan 4 beresiko *Very Low* (Sangat Rendah).

Prioritize the Failure Mode for Action

Kemudian selanjutnya dilakukan evaluasi dari ketingkatan resiko terhadap 22 penyebab kegagalan yang dapat dilihat pada Tabel 9.

ISSN 2798-141X

Table 9. Nilai RPN

Potensi Kegagalan	Penyebab Kegagalan	RPN	Kategori
Koneksi Jaringan Gangguan	Perangkat pada jaringan yang memenuhi batas	120	*High* (tinggi)
Human Error	Memiliki data yang tidak lengkap/update	72	*Low* (Rendah)
Hacking	Penipuan melalui rekayasa social	60	*Low* (Rendah)
Koneksi Jaringan Gangguan	Jaringan yang terlalu sibuk	54	*Low* (Rendah)
Listrik Padam Secara Tiba-Tiba	Terjadi gangguan kerusakan langsung pada generator sehingga listrik mengalami kesulitan pulih dengan cepat	50	*Low* (Rendah)
Petir	Adanya perbedaan potensi antara awan dengan bumi dan awan lainya	50	*Low* (Rendah)
Penyalah Gunaan Akses	tidak mengganti password secara berkala	48	*Low* (Rendah)
Human Error	Kelalaian dalam pengimputan data	48	*Low* (Rendah)
Hacking	Antivirus yang tidak pernah di update	48	*Low* (Rendah)
Trouble Web Server	Ada masalah pada Domain Name Server (*DSN*)	48	*Low* (Rendah)
Kebakaran	Hubungan arus pendek/korsleting Listrik	36	*Low* (Rendah)
Banjir	Adanya hujan lebat dan peningkatan volume air yang mengakibatkan air meluap	36	*Low* (Rendah)
Server Down	Terjadi lonjakan traffic pengunjung/pengguna melebihi kemampuan server	36	*Low* (Rendah)
Kerusakan Hardwere	Masuknya virus ke software yang mengakibatkan kerusakan pada hardwere	36	*Low* (Rendah)
Penyalah Gunaan Akses	Pegawai memberikan hak akses ke orang lain	32	*Low* (Rendah)
Data Corrupt	Data atau file mengalami kerusakan	27	*Low* (Rendah)
Hacking	Password yang digunakan secara berulang-ulang	24	*Low* (Rendah)
Trouble Web Server	Terblokirnya Akses IP	24	*Low* (Rendah)
Kerusakan Hardwere	Penggunaan yang tidak sesuai prosedur	18	*Very Low* (Sangat Rendah)
UI Design yang sulit dipahami	Kurangnya pengetahuan dari pengguna	18	*Very Low* (Sangat Rendah)
Pencurian Data/Perangkat Keras	Kurangnya keamanan dari pihak kantor	18	*Very Low* (Sangat Rendah)
Gempa Bumi	Pergerakan kerak bumi atau gunung Meletus	18	*Very Low* (Sangat Rendah)

ISSN 2798-141X

Pada Tabel 9 dilakukan pengurutan nilai RPN yang paling besar ke nilai RPN yang paling rendah. 1 kegagalan yang beresiko High (Tinggi), 17 beresiko Low (Rendah) dan 4 beresiko Very Low (Sangat Rendah).

Take Action to Elimination or Raduce High Risk *Flaure*

Pada tahap selanjutnya adalah Rencana Mitigasi Resiko yang menjadi perhatian kusus dari aplikasi INLISE LITE pada Perpustakaan Kantor DPRD Kota Salatiga. Yang harus di mitigasia adalah pada koneksi jaringan yang mendapat nilai RPN 120 *High* (Tinggi) yang sering mengalami masalah terhadap perangkat jaringan yang sering memenuhi batas dimana pihak perpustakaan bisa menambahkan ruter untuk penambahan kapasitas perangkat pada jaringan.

***Calculate the Resulting* RPN**

Jika tindakan yang disarankan adalah memitigasi kerentanan yang muncul, RPN juga akan menurun. Setelah nilai RPN ditentukan dengan mengalikan Severity, Occurrence, dan Detection, dilakukan estimasi untuk mengambil tindakan lebih lanjut untuk mengatasi masalah kegagalan dengan merujuk pada identifikasi pencegahan terkini.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan dari hasil penelitian yang telah dilakukan pada aplikasi INLIS LITE menggunakan metode *Failure Mode And Effect Analysis* (FMEA), di dapatkan bahwa terdapat 22 penyebab kegagalan dari aplikasi INLIS LITE pada Perpustakaan Kantor DPRD kota Salatiga. Dari 22 penyebab kegagalan terdapat 1 aktivitas kategori *High* (Tinggi), 17 aktivitas kategori *Low* (Rendah) dan 4 dengan kategori *Very Low* (Sangat Rendah). Adapun kegagalan yang perlu di perhatikan dari aplikasi INLIS LITE Kantor DPRD Kota Salatiga adalah Koneksi jaringan gangguan yang di sebabkan oleh Perangkat pada jaringan yang memenuhi batas mendapatkan nilai RPN 120 kategori *high* (tinggi). Dengan hasil penelitian yang telah dilakuakn dari aplikasi INLIS LITE pada Perpustakaan Kantor DPRD Kota Salatiga kiranya dapat digunakan untuk *Standard Operasional Procedure* (SOP) dan dapat meminimalkan resiko-resiko yang akan mengganggu operasional Perpustakaan.

Saran

Setelah peneliti menyelesaikan kajian analisis manajemen resiko menggunakan FMEA (*Failure Modes and Effects Analysis*) pada aplikasi Inlis Lite di Perpustakaan Kantor DPRD Kota Salatiga, peneliti selanjutnya dapat melakukan penelitian dengan cakupan secara holistik dan komprehensif, diharapkan penelitian selanjutnya dapat dilakukan secara menyeluruh agar temuan yang ada dapat digunakan dalam pengembangan dokumen manajemen risiko dan diterapkan pada seluruh bagian perpustakaan yang ada.

ISSN 2798-141X

DAFTAR PUSTAKA

Budiarto, R. (2017). Penerapan Metode FMEA Untuk Keamanan sistem Informasi (Studi Kasus: Website Polri). *Seminar Nasional IPTEK Terapan(SENIT)2017*, *1*, 73–78. http://conference.poltektegal.ac.id/index.php/senit2017

Hendra, F., & Effendi, R. (2018). Identifikasi Penyebab Potensial Kecacatan Produk dan Dampaknya dengan Menggunakan Pendekatan Failure Mode Effect Analysis (FMEA). *SINTEK JURNAL: Jurnal Ilmiah Teknik Mesin*, *12*(1), 17–24. http://jurnal.umj.ac.id/index.php/sintek

Munawir, H., Ulfa, R. M., & Djunaidi, M. (2020). Analisa Risiko Kegagalan Terhadap Downtime Pada Line Crank Case Menggunakan Metode Failure Mode Effect Analysis. *Prosiding IENACO 2020*, 149–156.

Ningsih, K. P., Tunnisa, U., & Erviana, N. (2020). Manajemen Resiko Redesign Sistem Penjajaran Rekam Medis dengan Metode Failure Mode and Effect Analysis (FMEA). *Indonesian of Health Management Journal*, *8*(1), 8–20.

Putri, A. A., & Irnanda, D. I. (2022). *Volume 4 issue 1 1 Aisyah Journal of Informatics and Electrical Engineering ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 (STUDI KASUS : APLIKASI J&T EXPRESS INDONESIA)*. *4*(1), 1–9. http://jti.aisyahuniversity.ac.id/index.php/AJIEE

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara - Journal of Information and Library Studies*, *1*(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

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

Rijali, A. (2019). Analisis Data Kualitatif. *Alhadharah: Jurnal Ilmu Dakwah*, *17*(33), 81. https://doi.org/10.18592/alhadharah.v17i33.2374

Sandre, H. I., Paat, W. R. L., & Pratasik, S. (2021). Analisis Pembelajaran Daring Pada SMK. *Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, *1*(1), 90-96.

Sandyavitri, A. (2008). Manajemen Resiko di Proyek Konstruksi. *Media Komunikasi Teknik Sipil Universitas Riau*, 23–38.

Sari, M., Hanum, S., & Rahmayati, R. (2022). Analisis Manajemen Resiko Dalam Penerapan Good Corporate Governance : Studi pada Perusahaan Perbankan di Indonesia. *Owner*, *6*(2), 1540–1554. https://doi.org/10.33395/owner.v6i2.804

Yaqin, R. I., Zamri, Z. Z., Siahaan, J. P., Priharanto, Y. E., Alirejo, M. S., & Umar, M. L. (2020). Pendekatan FMEA dalam Analisa Risiko Perawatan Sistem Bahan Bakar Mesin Induk: Studi Kasus di KM. Sidomulyo. *Jurnal Rekayasa Sistem Industri*, *9*(3), 189–200. https://doi.org/10.26593/jrsi.v9i3.4075.189-200

Yudha, S. F., Soemitra, A., & Nawawi, Z. M. (2023). Manajemen Resiko Bank Wakaf. *Jurnal EMT KITA*, *7*(2), 362–372. https://doi.org/10.35870/emt.v7i2.931

Yunarto, S. (2022). *Analisis Manajemen Risiko Pengadilan Negeri Nanga Bulik*.

Zulvi, M. S. (2022). Manajemen Risiko Teknologi Informasi Menggunakan Metode Fmea (Studi Kasus: Diskominfo Pemprov Riau). *Jurnal Komputer Terapan*, *8*(2), 381–390.

ISSN 2798-141X