KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 3, No 6, Juni 2023, Hal 698-707
DOI 10.30865/klik.v3i6.867
https://djournals.com/klik

Analisa Manajemen Risiko Sistem Informasi Perpustakaan Menggunakan Metode Failure Mode Effect and Analysis (FMEA)

Maisarah Assa'diyah*, Tengku Khairil Ahsyar, M Afdal

Fakultas Sains dan Teknologi, Sistem Informasi, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia
Email: [1,*]maisarahassadiyah@gmail.com, [2]tengkukhairil@uin-suska.ac.id, [3]m.afdal@uin-suska.ac.id
Email Penulis Korespondensi: maisarahassadiyah@gmail.com

Abstrak−Perpustakaan umum yang sudah menerapkan teknologi informasi pada proses bisnisnya memiliki tanggung jawab yang besar dalam pelayanan dan pengelolaannya karena pemustaka yang berkunjung merupakan masyarakat umum. Dalam menerapkan teknologi informasi, menjaga keamanan data user, anggota, sumber daya, dan informasi perpustakaan sangatlah penting. Perpustakaan digital harus memiliki pertimbangan mengenai risiko serta ancaman yang dapat terjadi. Risiko serta ancaman yang dapat terjadi yaitu seperti kerusakan server, kerusakan hardware, kelalaian staff, kehilangan, dan bencana alam. Tujuan dari penelitian ini adalah untuk menganalisa manajemen risiko dengan mengidentifikasi risiko dan mengukur tingkat risiko dari salah satu Dinas Perpustakaan dan Kearsipan Provinsi Riau yang sudah menggunakan sistem otomasi perpustakaan yaitu INLISLite. Metode yang digunakan untuk mengidentifikasi dan menilai risiko adalah metode Failure Mode Effect and Analysis (FMEA). Penilaian risiko berdasarkan perhitungan nilai Risk Priority Number (RPN) yang dihasilkan dari mengalikan parameter tingkat severity, occurrence, dan detection. Penilaian risiko dilakukan berdasarkan kategori daftar komponen asset yang mendukung berjalannya sistem yaitu, hardware, software, data, people, dan network. Dari perhitungan yang telah dilakukan terdapat enam kategori level RPN yaitu 1 nilai di level very high, 3 nilai berada di level high, 2 nilai berada di level medium, 16 nilai berada di level low, dan 1 nilai berada di level very low. Dari hasil nilai RPN yang perlu diberikan rekomendasi tindakan yaitu nilai RPN yang berada pada level very high dan high.

Kata Kunci: Manajemen Risiko; Perpustakaan; Penilaian Risiko; FMEA; INLISLite

Abstract−Public libraries that have implemented information technology in their business processes have a great responsibility in service and management because the visiting users are the general public. In implementing information technology, maintaining the security of user data, members, resources, and library information is very important. Digital libraries must have consideration of the risks and threats that may occur. The risks and threats that can occur are as follows server damage, hardware damage, staff negligence, loss, and natural disasters. The purpose of this research is to analyze risk management by identifying risks and measuring the level of risk from one of the Riau Province Library and Archives Services which already uses a library automation system, namely INLISLite. The method used to identify and assess risk is the Failure Mode Effect and Analysis (FMEA) method. Risk assessment is based on calculating the value of the Risk Priority Number (RPN) resulting from multiplying the level parameters severity, occurrence, and detection. Risk assessment is carried out based on the category list of asset components that support the running of the system, namely, hardware, software, data, people, and network. From the calculations that have been carried out, there are six categories of RPN levels, namely 1 score at a very high level, 3 scores at a high level, 2 scores at a medium level, 16 scores at a low level, and 1 score at a very low level. From the results of the RPN value that needs to be given recommendations for action, namely the RPN value which is at very high and high levels.

Keywords: Risk Management; Library; Risk Assessment; FMEA; INLISLite

1. PENDAHULUAN

Perpustakaan merupakan fasilitas yang menyediakan sumber pendidikan, budaya, penelitian, informasi dan layanan kepada penggunanya [1]. Banyak organisasi meningkatkan pelayanan dan pengelolaan perpustakaan dengan memanfaatkan teknologi informasi [2]. Perpustakaan Nasional RI membangun dan mengembangkan aplikasi otomasi perpustakaan yang disebut dengan INLISLite Sejak tahun 2011 [3]. INLISLite dimanfaatkan dalam rangka menggabungkan koleksi nasional Perpustakaan Digital Nasional Indonesia. INLISLite juga membantu dalam pengembangan, pengelolaan, dan pelayanan perpustakaan berbasis teknologi informasi dan komunikasi. INLISLite banyak digunakan oleh beberapa Dinas Perpustakaan dan Kearsipan di berbagai daerah [4], universitas [5], dan sekolah [6]. Namun, pustakawan harus memahami dan menyesuaikan perubahan pada transaksi *online* dan memiliki pemahaman tentang risiko keamanan serta privasi data *online* [7]. Perpustakaan digital akan menghadapi risiko keamanan yang besar karena sangat tergantung pada teknologi komputer, jaringan, komunikasi data, dan teknologi informasi lainnya [8].

Dalam penerapan teknologi informasi, organisasi juga harus memiliki kebijakan serta manajemen perlindungan dan staff yang ahli dalam menjaga asset yang berhubungan dengan teknologi informasi, personal, dan layanan [9]. Pada perlindungan perpustakaan digital yang perlu diperhatikan yaitu pada sumber daya, pemustaka dan data pustakawan [10]. Penggunaan teknologi informasi pada proses bisnis di organisasi dalam hal ini perpustakaan digital perlu mempertimbangkan risiko serta ancaman yang dapat terjadi [11]. Risiko serta ancaman yang terjadi dapat diminimalisir dengan manajemen risiko [12]. Manajemen risiko perlu dilakukan karena para ahli menemukan bahwa kegagalan dapat terjadi disebabkan dari berbagai aspek yang berbeda pada risiko teknologi informasi [13]. Manajemen risiko mencakup tiga proses yaitu identifikasi risiko, penilaian risiko dan pengelolaan risiko [7]. Pada manajemen risiko, hal yang penting dilakukan untuk meningkatkan perlindungan serta mitigasi risiko terhadap teknologi informasi adalah aspek penilaian risiko [14].

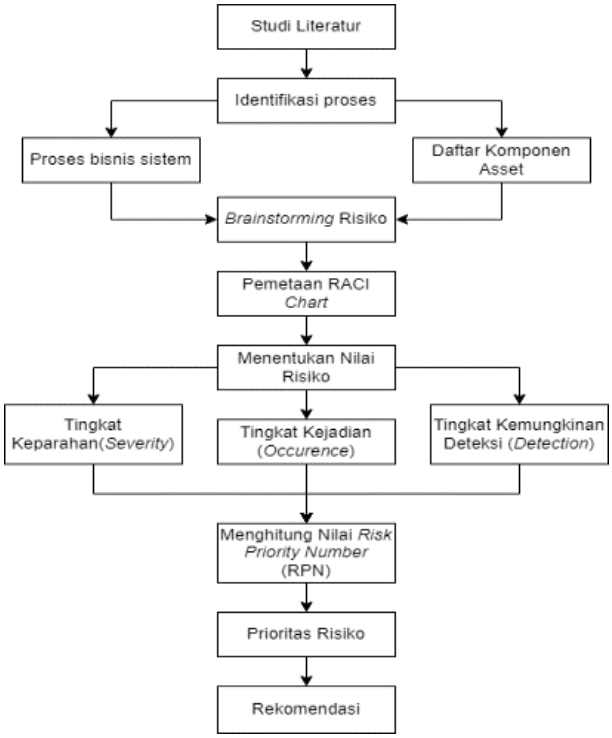
Penelitian mengenai manajemen risiko pada objek teknologi informasi terutama pada penilaian risiko sudah dilakukan oleh [11], [13], [15], [16], [17]. Penelitian tersebut menggunakan metode *Failure Mode Effect and Analysis* (FMEA) untuk mengukur tingkat risiko penggunaan teknologi informasi. Pada penelitian [13] menghasilkan identifikasi

risiko IT dengan melakukan penilaian risiko oleh dua tim untuk menghasilkan nilai *Risk Priority Number* (RPN) dengan mengukur tingkat keparahan, kejadian, dan deteksi pada setiap risiko. Tim A menghasilkan satu risiko sangat tinggi, satu risiko tinggi dan empat belas risiko sedang, sedangkan Tim B menghasilkan sepuluh risiko sangat tinggi dan sepuluh risiko tinggi. Namun, FMEA sebagai metode semi kuantitatif yang menggabungkan analisis kegagalan (kualitatif) dan perhitungan nilai RPN (kuantitatif) dapat digunakan untuk penilaian risiko IT karena metode tersebut efektif, relevan dan mudah digunakan. Penelitian [15] menggunakan RACI *Chart* untuk menentukan pihak yang melakukan penilaian risiko dan menghasilkan tiga risiko yang dapat mengancam sistem Karoline yaitu munculnya *cybercrime*, kegagalan sistem dan kegagalan manusia. Hasil akhir dari penelitian tersebut yaitu memberikan rekomendasi sebagai tindakan untuk mengurangi munculnya risiko dan penanganannya. Penelitian [11] melakukan analisis risiko dan aset kritis komponen sistem dan menemukan beberapa penyebab terjadinya risiko yaitu pengendalian dan pemeliharaan sistem belum dilakukan secara berkala, *hacking* yang mengganggu situs *web* dan jaringan dan tidak memiliki standar manajemen keamanan informasi. Penilaian risiko yang dilakukan dengan menggunakan FMEA menghasilkan delapan belas risiko termasuk empat risiko dengan tingkat rendah dan empat belas risiko dengan tingkat sangat rendah. Menurut penelitian [16] metode FMEA membantu akademika untuk menganalisis tingkat keamanan sistem informasi dalam proses pembelajaran *online* menggunakan sepuluh tahapan dan lembar kerja dari FMEA. Penelitian [17] menghasilkan nilai RPN yang sangat tinggi yaitu dari faktor teknologi manual dengan nilai RPN 729, kepatuhan hukum dengan nilai 729, biaya daur ulang 729 dan faktor lainnya pada kategori sedang dan rendah.

Berdasarkan penelitian terdahulu, metode FMEA dapat digunakan untuk manajemen risiko sebagai metode penilaian risiko pada objek teknologi informasi. FMEA merupakan teknik analisis yang digunakan untuk mengidentifikasi, mengurangi kegagalan, masalah yang diketahui dari sistem, desain, proses dan layanan [18]. Metode FMEA cocok digunakan untuk penilaian risiko IT [13][19]. FMEA menyediakan metode sistematis yang dapat digunakan berbagai jenis organisasi seperti manufaktur, industri, otomotif, medis dan organisasi pemerintah [20]. Penggunaan FMEA memiliki perbedaan pengukuran berdasarkan objek yang diteliti. Penggunaan FMEA pada objek teknologi informasi menilai risiko dari aspek keamanan informasi yaitu kerahasiaan, integritas dan ketersediaan [19]. Maka, penilaian risiko sistem informasi otomasi perpustakaan pada penelitian ini menggunakan metode *Failure Mode Effect and Analysis* (FMEA).

Penelitian ini bertujuan untuk menganalisis manajemen risiko dengan mengidentifikasi risiko dan mengukur risiko dari sistem otomasi perpustakaan. Objek penelitian ini adalah Dinas Perpustakaan dan Kearsipan Provinsi Riau yang menggunakan sistem INLISLite sebagai sistem otomasi perpustakaan. Identifikasi risiko dan pengukuran risiko menggunakan metode *Failure Mode Effect and Analysis* (FMEA) dengan mengukur tingkat keparahan (*severity*), tingkat kejadian (*occurrence*) dan tingkat deteksi (*detection*) yang nantinya akan menjadi perhatian utama dengan perhitungan *Risk Priority Number* (RPN). Setelah melakukan penilaian risiko, maka selanjutnya memberikan rekomendasi kontrol sebagai pencegahan dari risiko serta ancaman yang akan terjadi.

2. METODOLOGI PENELITIAN



Gambar 1. Metodologi Penelitian

Penelitian ini berfokus pada analisa evaluasi FMEA yang mengambil dua tindakan [18] yaitu melakukan identifikasi data historis atau asset yang penting dan mitigasi risiko. Metodologi penelitian dapat dilihat pada Gambar 1.

2.1 Studi Literatur

Pada penelitian ini, studi literatur digunakan sebagai metode pengumpulan data. Sumber data yang digunakan untuk studi literatur adalah artikel penelitian sebelumnya, buku, internet, dan dokumen terkait. Studi literatur mengumpulkan berbagai topik penelitian yang berkaitan dengan analisa dan manajemen risiko, keamanan informasi, teknologi informasi, dan penilaian risiko berdasarkan metode *Failure Mode Effect anda Analysis* (FMEA).

2.2 Identifikasi Proses

Tahap ini merupakan tahap awal dari metode *Failure Mode Effect and Analysis* (FMEA). Identifikasi proses bertujuan untuk mengetahui proses bisnis INLISLite dan daftar komponen asset sistem.

a. **Proses bisnis**, mengidentifikasi masing-masing proses serta memastikan proses yang memerlukan analisis. Identifikasi proses bisnis dilakukan dengan observasi dan wawancara dengan staff IT yang bertujuan guna mengetahui proses bisnis yang ada pada INLISLite.
b. **Daftar komponen asset**, sebelum tahap penilaian risiko maka perlu melakukan identifikasi daftar komponen asset IT yang memiliki risiko kritis. Daftar asset komponen IT diperoleh dari hasil observasi dan wawancara kepada staff IT Dinas Perpustakaan dan Kearsipan Provinsi Riau.

2.3 *Brainstorming* Risiko

Brainstorming risiko merupakan tahap peninjauan dan penentuan proses. Pada tahap ini, dilakukan dengan mengidentifikasi modus kegagalan yang dapat terjadi. Identifikasi modus kegagalan dilakukan dengan menganalisa kekuatan dan kelemahan dari Dinas Perpustakaan dan Kearsipan Provinsi Riau dan sistem INLISLite. Hasil tabel analisa kekuatan dan kelemahan instansi dan sistem dijadikan sebagai acuan dalam perancangan kuisioner untuk menentukan *current process controls* pada penilaian deteksi (*detection*). Setelah mengetahui kekuatan dan kelemahan dari instansi dan sistem maka perlu mengidentifikasi efek yang mungkin terjadi.

2.4 Pemetaan RACI *Chart*

RACI *Chart* digunakan sebagai acuan dalam memilih pihak yang berpartisipasi pada penelitian yaitu pihak yang akan menjadi responden. Penentuan RACI *Chart* dilakukan dengan diskusi bersama staff IT Dinas Perpustakaan dan Kearsipan Provinsi Riau. Singkatan dari RACI berasal dari perbedaan peran yang terlibat dalam sebuah proses. Adapun penjelasan dari kepanjangan RACI, yaitu [21]:

a. *Responsible* (R) yaitu orang yang melakukan kegiatan atau yang melakukan pekerjaan secara langsung.
b. *Accountable* (A) yaitu orang yang memiliki hak untuk menetapkan hasil akhir atau keputusan.
c. *Consulted* (C) yaitu orang memberi masukan atau saran dan memberi bantuan dalam proses pekerjaan.
d. *Informed* (I) yaitu orang yang menerima informasi hasil dari keputusan.

2.5 Menentukan Nilai Risiko

Sebelum melakukan penilaian risiko, perlu terlebih dahulu menentukan kriteria untuk setiap parameter *Severity, Occurrence,* dan *Detection.* Kriteria parameter harus memiliki skala yang sama. Pada penelitian ini, menggunakan skala ranking dimulai dari 1-10 dimana 1 menunjukkan nilai terendah dan 10 menunjukkan nilai tertinggi.

a. **Tingkat keparahan (*Severity*),** pada penilaian ini dilakukan penilaian tingkat keparahan yang berasal dari kegagalan yang terjadi berdasarkan kriteria parameter yang ditentukan. Jika tingkat keparahan yang ditimbulkan bersifat serius, maka nilai tingkat keparahan akan tinggi dan sebaliknya.
b. **Tingkat kejadian (*Occurrence*),** penilaian ini menentukan seberapa sering terjadi kegagalan.
c. **Tingkat kemungkinan deteksi (*Detection*)**, penilaian ini menilai kemampuan mengendalikan modus kegagalan.

2.6 Menentukan Nilai *Risk Priority Number* (RPN)

Pada tahapan ini dilakukan perhitungan nilai *Risk Priority Number* (RPN) dengan cara mengalikan setiap parameter *Severity, Occurrence,* dan *Detection*. Nilai RPN berfungsi untuk menentukan prioritas dari risiko yang membutuhkan penanganan serius.

2.7 Prioritas Risiko

Setelah menghitung nilai RPN, selanjutnya adalah menentukan prioritas risiko. Prioritas risiko berguna untuk mengetahui kegagalan yang memiliki risiko tertinggi. Kategori dalam membuat prioritas risiko yaitu berdasarkan hasil perhitungan nilai RPN. Berdasarkan perhitungan nilai RPN maka dibuat prioritas risiko dari *level* tertinggi hingga terendah. *Level* RPN dapat dilihat pada Tabel 1.

Tabel 1. *Level* RPN

RPN	*Calculation Level*
0-19	*Very Low*
20-79	*Low*
80-119	*Medium*
120-199	*High*
Lebih dari 200	*Very High*

2.8 Rekomendasi

Pada tahap ini dilakukan dengan membuat rekomendasi kontrol untuk mengurangi risiko sebagai proses akhir dari manajemen risiko yaitu tahap evaulasi.

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Proses

Sistem INLISLite yang dapat dilihat pada Gambar 2 digunakan untuk membantu dalam pengembangan, pengelolaan, dan pelayanan perpustakaan berbasis teknologi informasi dan komunikasi termasuk pada Dinas Perpustakaan dan Kearsipan Provinsi Riau. INLISLite memiliki 9 modul yaitu modul *back office*, baca ditempat, buku tamu, keanggotaan *online*, layanan koleksi digital, *Online Public Access Catalogue* (OPAC), pendaftaran anggota, statistic, dan survey. Pengguna dari sistem INLISLite pada Dinas Perpustakaan dan Kearsipan Provinsi Riau adalah admin, *user*/pustakawan, dan umum. Alur yang terdapat pada sistem INLISLite dimulai dari anggota perpustakaan atau non anggota. Proses awal yang dilakukan pemustaka pada sistem adalah proses pengisian buku tamu untuk mencatat kehadiran pemustaka setiap harinya. Jika pemustaka belum terdaftar dan ingin melakukan peminjaman buku, maka perlu melakukan pendaftaran anggota dengan pendaftaran mandiri ditempat yang sudah disediakan. Jika pemustaka hanya ingin membaca ditempat, maka pemustaka tidak diharuskan mendaftar sebagai anggota perpustakaan. Setelah melakukan pendaftaran, pemustaka mendapatkan kartu tanda anggota yang digunakan untuk sirkulasi perpustakaan. Pemustaka tidak akan dapat melakukan sirkulasi apabila belum terdaftar sebagai anggota perpustakaan. Proses bisnis sistem yang memiliki potensi dampak risiko yaitu pada proses sirkulasi perpustakaan. Permasalahan yang terjadi adalah tidak sesuainya data yang dimasukkan pada sistem menyebabkan masalah pada saat transaksi peminjaman dan pengembalian buku, kode *barcode* yang tidak terdeksi pada sistem, kesalahan pada penagihan buku dan denda, dan kegagalan akses data. Permasalahan yang pernah terjadi pada Dinas Perpustakaan dan Kearsipan Provinsi Riau adalah kerusakan pada *hardware*, salah *input* data, *server down*, seringnya terjadi gangguan jaringan karena infrastruktur yang sudah lama, dan sering terjadi kesalahan verifikasi yang disebabkan oleh kurangnya sosialisasi pada pustakawan. Hal tersebut menyebabkan terhambatnya proses bisnis pada pelayanan perpustakaan.

Gambar 2. INLISLite [3]

Selanjutnya, identifikasi data historis atau data asset pendukung berjalannya sistem dapat dikategorikan sebagai sumber risiko. Pada penelitian ini, mendapatkan 5 kategori asset yang dapat berdampak buruk menimbulkan risiko yang tidak diinginkan. Asset komponen TI dikategorikan berdasarkan *hardware, software, network*, data, dan *people.* Kategori *hardware* sebanyak 7, *software* sebanyak 2, *network* sebanyak 3, data sebanyak 3, dan *people* sebanyak 3. Berdasarkan kategori asset yang didapatkan, akan digunakan sebagai acuan untuk menghasilkan daftar risiko dan ancaman yang dapat terjadi. Kategori tersebut menjadi sumber risiko kritis karena jika asset rusak, hilang, ataupun tidak berfungsi dengan baik maka, sistem tidak dapat berjalan dan memiliki potensi dampak dengan terhambatnya kegiatan operasional. Risiko serta ancaman juga dapat berasal dari internal atau external dan disengaja atau tidak disengaja. Risiko yang dapat terjadi seperti

adanya penyalahgunaan hak akses [22], pencurian, bencana alam, kerusakan. Berdasarkan hasil wawancara dan observasi, Tabel 2 menunjukkan daftar komponen asset yang mendukung berjalannya sistem INLISLite.

Tabel 2. Daftar Komponen Asset

Kategori	Asset
Hardware	PC, *Server*, Printer, UPS, CCTV, Ac, *Harddisk*
Software	INLISLite, Sistem Operasi
Network	Diskominfo, LAN, Kabel Jaringan
Data	Data koleksi buku, Data anggota, Data *user*
People	Admin, *User*, Umum

3.2 *Brainstorming* Risiko

Pada tahap ini, dilakukan *brainstorming* risiko dengan menganalisis kekuatan dan kelemahan dari instansi dan sistem. Tabel 3 menunjukkan hasil analisa kekuatan dan kelemahan dari instansi. Kelemahan tersebut dapat menimbulkan risiko yang besar jika tidak segera di perbaiki. Dari hasil analisa kekuatan dan kelemahan instansi ditemukan bahwa instansi tersebut masih kurang memiliki sumber daya manusia dibidang teknologi dan infrastruktur yang dimiliki sudah lama. Seperti pada penelitian [23] menghasilkan nilai RPN tertinggi dengan risiko layanan sistem tidak tersedia karena masalah pengelolaan keamanan sistem dan penanganan lama terhadap layanan sistem yang bermasalah. Risiko serta efek yang ditimbulkan dari kurangnya sumber daya manusia dibidang teknologi juga dapat merusak reputasi instansi.

Tabel 3. Kekuatan dan Kelemahan Instansi

Kekuatan Instansi	Kelemahan Instansi
Dilengkapi CCTV	Komputer yang belum berstandar ISO
Lokasi kantor strategis	Sistem pengambilan keputusan bersifat terpusat
Adanya hak akses ruangan *server*	Kurangnya sumber daya manusia dibidang teknologi
Sistem pelayanan cepat	Ruangan *server* dilantai bawah
Adanya petugas yang menjaga keamanan	Pelatihan sumber daya manusia sangat kurang
Pendaftaran dapat dilakukan via *online*	Infrastruktur jaringan sudah lama
Fasilitas komputer dan fasilitas pengunjung cukup lengkap	Kurangnya fasilitas cetak kartu anggota

Hasil analisa kekuatan dan kelemahan dari sistem dapat dilihat pada Tabel 4. Sistem INLISLite yang digunakan oleh Dinas Perpustakaan dan Kearsipan Provinsi Riau menerapkan untuk melakukan *backup* data secara rutin untuk mencegah risiko yang berkaitan mengenai data pada sistem. Namun, jika terjadi permasalahan pada sistem seperti adanya *error* pada fitur yang ada di sistem dan pihak Dinas Perpustakaan dan Provinsi Riau tidak dapat memperbaikinya, maka yang dapat menyelesaikan adalah pihak konsultan.

Tabel 4. Kekuatan dan kelemahan sistem

Kekuatan Sistem	Kelemahan Sistem
Terdapat 3 hak akses pada sistem	*Upgrade* dilakukan pada pusat
Login hanya dapat dilakukan jika memiliki hak akses terhadap sistem	Belum adanya identifikasi ancaman pada sistem
Adanya antivirus setiap PC	Jika terjadi masalah pada sistem, yang bisa menyelesaikan hanya pihak konsultan
Backup data dilakukan setiap hari	Pada saat pusat melakukan *upgrade* sistem, sistem yang berada diluar pusat juga harus melakukan *upgrade* sistem
Menyediakan fitur pendaftaran *online*	Terdapat *error* pada beberapa fitur
Dapat diakses dari luar	

Berdasarkan hasil dari Tabel 3 dan Tabel 4, maka selanjutnya dilakukan analisa efek dan menemukan sebanyak 14 risiko yang dapat terjadi pada sistem otomasi perpustakaan. Risiko tersebut berpotensi besar terutama untuk pelayanan perpustakaan. Dapat dilihat pada Tabel 5, efek yang banyak terjadi yaitu pada kegiatan operasional atau kinerja terhambat dengan jumlah 10, sedangkan untuk yang diluar dari potensi efek kegiatan operasional yang terhambat berjumlah 4. Maka dapat disimpulkan bahwa, terdapat banyak risiko yang memiliki potensi besar pada kegiatan operasional dan dapat menghambat kinerja dan pelayanan. Dari potensi efek yang ditimbulkan oleh risiko yang ada, reputasi organisasi juga dapat terancam. Hasil analisa risiko dan potensi efek digunakan sebagai penambahan referensi untuk kuisioner.

Tabel 5. Analisa Efek

Risiko	Potensi Efek
Kebakaran *server*	Kegiatan operasional ataupun kinerja terhenti dan kerugian finansial
Server down	Kegiatan operasional ataupun kinerja terhambat
Kerusakan *server*	Server tidak dapat digunakan
Kerusakan komputer	Kegiatan operasional ataupun kinerja terhambat

Komputer tidak dapat digunakan	Kegiatan operasional ataupun kinerja terhambat
Kegagalan jaringan	Kegiatan operasional ataupun kinerja terhambat
Kerusakan perangkat jaringan	Kegiatan operasional ataupun kinerja terhambat
Kegagalan *hardware*	Kegiatan operasional ataupun kinerja terhenti dan kerugian finansial
Kegagalan *software*	Kegiatan operasional ataupun kinerja terhambat
Kegagalan sistem	Kegiatan operasional ataupun kinerja terhenti
Kegagalan manusia	Profesionalitas kinerja pelayanan terhadap pengunjung perpustakaan tidak maksimal
Kesalahan manusia	Profesionalitas kinerja pelayanan terhadap pengunjung perpustakaan tidak maksimal
Bencana alam	Kegiatan operasional ataupun kinerja terhambat
Pemalsuan atau penyalahgunaan hak akses	Reputasi instansi

3.3 Pemetaan RACI Chart

RACI *Chart* menunjukkan pihak yang memiliki peran dan tanggung jawab dalam proses manajemen [24] dalam pengelolaan IT terutama pada sistem INLISLite di Dipersip Riau. Penentuan pihak yang memiliki tanggung jawab pada RACI *Chart* dilakukan dengan diskusi bersama staff IT Dipersip Riau. Dari hasil pemetaan RACI Chart terdapat empat pihak yang menjadi responden pada penelitian ini yaitu Tim IT, *User* atau pustakawan, Eselon III dan Eselon IV. Pemetaan RACI *Chart* dapat dilihat pada Tabel 6.

Tabel 6. RACI Chart

Tugas atau peranan	Tim IT	*User*/pustakawan	Eselon III	Eselon IV
Pengembangan, pengelolaan, pengoperasian, dan memelihara infrastruktur sistem jariingan, server dan database pada Dipersip Riau.	R	C	A	I
Mengelola, mengoperasikan dan mengevaluasi kegiatan operasi IT.	C	R	A	I
Memutuskan dan menyetujui serta bertanggung jawab atas seluruh pegawai Dipersip Riau.	C	I	R	A
Memberikan solusii bisnis Dipersip Riau.	C	I	R	A
Memberikan rekomendasi untuk perbaikan.	C	R	A	I

3.4 Menentukan Nilai Risiko

Dari daftar asset serta analisa risiko yang sudah ditentukan, maka dilakukan penilaian risiko yang dinilai oleh responden. Terdapat 36 analisa risiko dengan lima kategori proses yaitu *hardware*, *software*, data, *people* dan *network*. Nilai-nilai risiko yang terdiri dari nilai *severity*, *occurrence*, dan *detection* digunakan sebagai acuan untuk mengetahui risiko mana yang tertinggi. Kuisioner yang disebar yaitu sebanyak 4. Penilaian risiko dapat dilihat pada Tabel 7.

Tabel 7. Menentukan Nilai Risiko

Code	*Process Function (Category)*	*Critical assets*	*Potential failure modes (process defects)*	*Potential effects of failure*	SEV	*Potential causes of failure*	OCC	*Current process controls*	DET
HW01	*Hardware*	*Server*	Kebakaran *server*	Kegiatan operasional ataupun kinerja terhenti	9	*Server* mengalami *overheat*	2	Melakukan pengecekan ruangan *server* setiap hari	2
HW02			Kebakaran *server*	Kerugian finansial	9	Hubungan arus pendek (*power failure*)	1	Melakukan pengecekan terhadap infrastruktur TI yang rusak	5
HW03			*Server overheat*	Kegiatan operasional ataupun kinerja terhambat	6	Tidak berfungsinya AC pada ruangan *server*	3	Melakukan pengecekan ruangan *server* setiap hari	2
HW04			*Server down*	Kegiatan operasional ataupun	5	Terlalu banyaknya unit yang mengakses server pada waktu	3	Melakukan pengecekkan terhadap	3

				kinerja terhambat			bersamaan ataupun serangan DDOS		infrastruktur TI yang rusak		
HW05			Kerusakan *Server*	Server tidak dapat digunakan	6	Tidak adanya proses *controlling* dan *maintenance* secara rutin	5	Melakukan pengecekkan terhadap infrastruktur TI yang rusak		3	
…	…	…	…	…	…	…	…	…		…	
NT04	*Network*	Internet, intranet	Adanya kesalahan pengalamatan IP	Tidak ada koneksi jaringan	8	*Human error*	2	Melakukan pengecekan terhadap infrastrktur TI yang rusak		3	

3.5 Menentukan Nilai *Risk Priority Number* (RPN)

Berdasarkan penilaian risiko dari tingkat keparahan (*severity)*, tingkat kejadian (*occurrence)*, dan tingkat deteksi (*detection)* yang diberikan kepada 4 responden dari pihak Dinas Perpustakaan dan Kearsipan Provinsi Riau menilai sebanyak 36 risiko. Hasil perhitungan nilai RPN mendapatkan enam kategori *level* RPN dimana ancaman kegagalan sistem berada pada *level very high* dengan nilai RPN sebesar 504, ancaman koneksi jaringan putus, komputer tidak dapat digunakan, dan konektifitas jaringan menurun berada di *level high* dengan nilai RPN sebesar 180-144, ancaman kegagalan manusia (*human* failure) dan kerusakan komputer berada di *level medium* dengan nilai RPN sebesar 108-84, ancaman kegagalan sistem, perangkat komputer *out of dated,* pemalsuan atau penyalahgunaan hak akses, hilangnya komponen PC, kegagalan jaringan, kerusakan printer/scanner, penuhnya kapasitas, kegagalan manusia (*human failure*), *cyber crime*, hilangnya printer, kebakaran *server,* akses informasi PC secara illegal, koneksi jaringan putus, tidak cocoknya data pada sistem dengan data fisik, kerusakan perangkat jaringan, dan *server overheat* berada di *level low* dengan nilai RPN sebesar 75-20 dan ancaman koneksi jaringan putus karena kegagalan jaringan berada di *level very low* dengan nilai RPN sebesar 18. Hasil nilai RPN dapat dilihat pada Tabel 8.

Tabel 8. Nilai RPN

Code	*Process Function (Category)*	*Critical assets*	*Potential failure modes (process defects)*	*Potential effects of failure*	SEV	*Potential causes of failure*	OCC	*Current process controls*	DET	RPN
HW01	Hardware	*Server*	Kebakaran *server*	Kegiatan operasional ataupun kinerja terhenti	9	Server mengalami overheat	2	Melakukan pengecekan ruangan server setiap hari	2	36
HW02			Kebakaran *server*	Kerugian finansial	9	Hubungan arus pendek (power failure)	1	Melakukan pengecekan terhadap infrastruktur TI yang rusak	5	45
HW03			*Server overheat*	Kegiatan operasional ataupun kinerja terhambat	6	Tidak berfungsinya AC pada ruangan server	3	Melakukan pengecekan ruangan server setiap hari	2	36
HW04			*Server down*	Kegiatan operasional ataupun kinerja terhambat	5	Terlalu banyaknya unit yang mengakses server pada waktu bersamaan ataupun serangan DDOS	3	Melakukan pengecekan terhadap infrastruktur TI yang rusak	3	45

HW05			Kerusakan *Server*	*Server* tidak dapat digunakan	6	Tidak adanya proses *controlling* dan *maintenance* secara rutin	5	Melakukan pengecekan terhadap infrastrktur yang rusak	TI	3	90
…	…	…	…	…	…	…	…	…		…	…
NT04	Network	Internet, intranet	Adanya kesalahan pengalamatan IP	Tidak ada koneksi jaringan	8	Human error	2	Melakukan pengecekan terhadap infrastrktur yang rusak	TI	3	48

3.6 Prioritas Risiko

Dari nilai RPN yang telah dihasilkan maka dilakukan penyusunan urutan prioritas risiko yang dimulai dari risiko yang tertinggi sampai risiko yang terendah. Pada tabel 9, menunjukkan 23 *ranking* risiko yang telah diseleksi berdasarkan nilai RPN tertinggi dari 36 nilai RPN. Nilai RPN dengan *level very high* yaitu 504 dihasilkan dari kuisioner 3 yang diisi oleh pihak tim IT Dinas Perpustakaan dan Kearsipan Provinsi Riau. Modus kegagalan pada *level very high* adalah kegagalan sistem dengan permasalahan masih adanya *error* pada sistem dan dapat berpotensi kegiatan operasional ataupun kinerja terhambat. Permasalahan tersebut belum dapat diatasi oleh pihak Dinas Perpustakaan dan Kearsipan Provinsi Riau karena kode pemrograman pada sistem ada yang terkunci dan hanya pihak pusat yang dapat memperbaiki. Prioritas risiko yang telah diurutkan akan menjadi acuan untuk menentukan risiko mana yang memerlukan tindakan dengan membuat rekomendasi.

Tabel 9. Prioritas Risiko

Code	*Process Function Category*	*Potential Failure Modes (Process defects)*	SEV	OCC	DET	RPN	*Level*	*Rank*
SW01 (K.3)	*Software*	Kegagalan Sistem	9	7	8	504	*Very high*	1
NT01 (K.3)	*Network*	Koneksi Jaringan Putus	6	6	5	180	*High*	2
HW09 (K.3)	*Hardware*	Komputer tidak dapat digunakan	7	7	3	147	*High*	3
NT03 (K.1)	*Network*	Konektifitas jaringan menurun	8	6	3	144	*High*	4
PP02 (K.3)	*People*	Kegagalan manusia (*human failure*)	6	3	6	108	*Medium*	5
HW07 (K.3)	*Hardware*	Kerusakan komputer	7	3	4	84	*Medium*	6
SW01 (K.1)	*Software*	Kegagalan sistem	5	5	3	75	*Low*	7
HW11 (K.3)	*Hardware*	Perangkat komputer *out of dated*	6	3	4	72	*Low*	8
PP03 (K.3)	*People*	Pemalsuan atau penyalahgunaan hak akses	8	1	8	64	*Low*	9
HW12 (K.1)	*Hardware*	Hilangnya komponen PC	7	3	3	63	*Low*	10
HW15 (K.3)	*Hardware*	Kegagalan jaringan	6	3	3	54	*Low*	11
HW18 (K.4)	*Hardware*	Kerusakan printer/scanner	7	7	1	49	*Low*	12
DA01 (K.3)	Data	Penuhnya kapasitas	8	2	3	48	*Low*	13
PP01 (K.1)	*People*	Kegagalan manusia (*human failure*)	5	4	2	40	*Low*	14
DA05 (K.2)	Data	*Cyber crime (hacker attack)*	6	6	1	36	*Low*	15
HW20 (K.3)	*Hardware*	Hilangnya printer/scanner	8	2	2	32	*Low*	16
HW01 (K.1)	*hardware*	Kebakaran *server*	10	3	1	30	*Low*	17
HW13 (K.1)	*Hardware*	Akses informasi PC secara ilegal	1	4	7	28	*Low*	18
NT02 (K.4)	*Network*	Koneksi jaringan putus	5	5	1	25	*Low*	19
DA03 (K.2)	Data	Tidak cocoknya data pada sistem dengan data fisik	6	4	1	24	*Low*	20
HW16 (K.1)	*Hardware*	Kerusakan perangkat jaringan	7	1	3	21	*Low*	21
HW03 (K.1)	*Hardware*	*Server overheat*	5	4	1	20	*Low*	22
NT01 (K.2)	*Network*	Koneksi Jaringan Putus	3	6	1	18	*Very low*	23

3.7 Rekomendasi

Berdasarkan hasil Tabel 9 sebelumnya, maka *potential failure modes* yang akan diberikan rekomendasi yaitu pada *code* SW01, NT01, dan HW09 karena memiliki *level* yang sangat tinggi dan tinggi. Tabel rekomendasi dapat dilihat pada Tabel 10.

Tabel 10. Rekomendasi

Code	Potensi Kegagalan	Penyebab	Rekomendasi

SW01 (K.3)	Kegagalan sistem	Masih terdapat *error* pada sistem yang tidak mudah untuk diperbaiki oleh pihak IT Dinas Perpustakaan dan Kearsipan Provinsi Riau karena bahasa pemrograman yang digunakan cukup sulit karena menggunakan *framework* Yii dan juga pemeliharaan sistem dilakukan oleh pusat.	Melakukan sosialisasi atau pelatihan kepada seluruh staff bidang IT
NT01 (K.3)	Koneksi jaringan putus	Kegagalan jaringan yang menyebabkan sistem tidak dapat diakses	Melakukan pengecekan pada infrastruktur TI secara berkala dan mengganti infrastruktur jaringan yang sudah lama.
HW09 (K.3)	Komputer tidak dapat digunakan	Lisensi *software* yang digunakan oleh instansi sudah melebihi batas waktu	Menggunakan *software open source* untuk jangka panjang

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dengan menggunakan metode *Failure Mode Effect and Analysis* (FMEA), diperoleh beberapa risiko yang dikategorikan dari daftar asset komponen IT yaitu *hardware, software, people,* data, dan *network.* Terdapat beberapa risiko yang memiliki potensi kegagalan dan dapat menghambat proses bisnis. Potensi kegagalan yang memiliki potensial besar yaitu kegagalan *software,* koneksi jaringan putus, kerusakan *hardware*, dan *human failure.* Kegagalan *software, hardware,* jaringan, *human failure* dapat menyebabkan proses bisnis dan kegiatan operasional akan menjadi tidak optimal. Dari hasil penilaian RPN yang dikategorikan dengan 5 *level* RPN memiliki 1 risiko pada *level very high,* 3 risiko pada *level high,* 2 risiko pada *level medium,* 16 risiko pada *level low*, dan 1 risiko pada *level very low*. Penilaian risiko menemukan risiko dengan nilai *Risk Priority Number* (RPN) tertinggi hingga terendah. Risiko tertinggi dengan nilai RPN 504, yaitu pada kategori *software* dengan risiko kegagalan sistem karena masih adanya *error* pada salah satu fitur di sistem tersebut. Pihak pengelola perpustakaan perlu melakukan pengecekan terhadap infrastruktur yang mendukung berjalannya sistem secara berkala dan mengganti infrastruktur yang sudah lama, dan menggunakan *software open source* untuk jangka panjang.

REFERENCES

[1] R. Chander, M. Dhar, and K. Bhatt, "Bibliometric analysis of studies on library security issues in academic institutions," J. Access Serv., vol. 19, no. 2–3, pp. 86–104, 2022, doi: 10.1080/15367967.2022.2118058.

[2] S. A. Wulandari, A. P. Dewi, M. Rizki Pohan, D. I. Sensuse, M. Mishbah, and Syamsudin, "Risk assessment and recommendation strategy based on COBIT 5 for risk: Case study sikn Jikn helpdesk service," Procedia Comput. Sci., vol. 161, pp. 168–177, 2019, doi: 10.1016/j.procs.2019.11.112.

[3] P. N. RI, "Tentang Inlislite Versi 3." Https://Inlislite.Perpusnas.Go.Id/ (Accessed May 18, 2023).

[4] M. Bugis, "Penerapan Software Inlislite Pada Pengolahan Bahan Pustaka Di Dinas Perpustakaan Dan Kearsipan Daerah Provinsi Sulawesi Utara | Bugis | Acta Diurna Komunikasi," Acta Diurna Komun., vol. 3, no. 2, p. :, 2021, [Online]. Available: https://ejournal.unsrat.ac.id/index.php/actadiurnakomunikasi/article/view/33449

[5] Zulhalim, A. Sulistyanto, and A. Z. Sianipar, "Implementasi Aplikasi Sistem Otomasi Perpustakaan Terintegrasi Menggunakan Inlislite Versi 3 Pada Perpustakaan Stmik Jayakarta," JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Researh, vol. 3(4), no. 4, pp. 1–9, 2019, [Online]. Available: http://journal.stmikjayakarta.ac.id/index.php/jisamar

[6] A. Asari, T. Kurniawan, and K. Andajani, "Penerapan Manajemen Perpustakaan Sekolah Berbasis Otomasi Inlislite | Asari | Bibliotika : Jurnal Kajian Perpustakaan dan Informasi," BIBLIOTIKA J. Kaji. Perpust. dan Inf. Vol., vol. 4, no. 2, pp. 246–252, 2020, [Online]. Available: http://journal2.um.ac.id/index.php/bibliotika/article/view/17567

[7] Sungadi, "Manajemen Keamanan Informasi Dan Internet," vol. 3, no. 1, pp. 105–120, 2020.

[8] Z. Han, S. Huang, H. Li, and N. Ren, "Risk assessment of digital library information security: A case study," Electron. Libr., vol. 34, no. 3, pp. 471–487, 2016, doi: 10.1108/EL-09-2014-0158.

[9] G. B. Newby, "Information Security for Libraries," Mod. Organ. Virtual Communities, vol. 8064, no. v, pp. 134–144, 2011, doi: 10.4018/978-1-931777-16-2.ch010.

[10] G. Farid, N. F. Warraich, and S. Iftikhar, "Digital information security management policy in academic libraries: A systematic review (2010–2022)," J. Inf. Sci., no. April, 2023, doi: 10.1177/01655515231160026.

[11] Y. S. Triana and R. A. M. Pangabean, "Risk Analysis in the Application of Financore Information Systems Using FMEA Method," J. Phys. Conf. Ser., vol. 1751, no. 1, 2021, doi: 10.1088/1742-6596/1751/1/012032.

[12] R. R. Putra, "Analisis Manajemen Risiko Ti Pada Keamanan Data E - Learning Dan Aset It Menggunakan Nist Sp 800 – 30 Revisi 1," JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 6, no. 1, pp. 96–105, 2019, doi: 10.35957/jatisi.v6i1.154.

[13] A. P. Subriadi, N. F. Najwa, B. D. Cahyabuana, and V. Lukitosari, "The consistency of using failure mode effect analysis (FMEA) on risk assessment of information technology," 2018 Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2018, pp. 61–66, 2018, doi: 10.1109/ISRITI.2018.8864467.

[14] H. M. Astuti, F. A. Muqtadiroh, E. W. T. Darmaningrat, and C. U. Putri, "Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk," Procedia Comput. Sci., vol. 124, pp. 569–576, 2017, doi: 10.1016/j.procs.2017.12.191.

[15] M. Megawati, O. Okfalisa, and M. Alkarim, "Security risk assessment of online fish quarantine information system using FMEA," AIP Conf. Proc., vol. 2347, no. July, 2021, doi: 10.1063/5.0053584.

[16] A. Leonard, I. Journal, A. Leonard, N. Anggito, F. Sialagan, and J. S. Suroso, "Information System Security Risk Management

E-Learning Using FMEA in University," vol. 9, no. 5, pp. 7565–7568, 2020.
[17] D. Rimantho, D. Rimantho, E. Noor, Eriyatno, and H. Effendi, "Risk Assessment on Failure Factors of e-waste Management Process Using FMEA Method," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 10, no. 6, pp. 2504–2510, 2020, doi: 10.18517/ijaseit.10.6.7433.
[18] H. D. Stamatis, Failure Mode and Effect Analysis FMEA from Theory to Execution. 2003.
[19] A. P. Subriadi and N. F. Najwa, "The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment," Heliyon, vol. 6, no. 1, p. e03161, 2020, doi: 10.1016/j.heliyon.2020.e03161.
[20] R. E. McDermott, R. J. Mikulak, and M. E. Beauregard, The Basics of FMEA (2nd ed.), 2nd Editio. 2008. doi: https://doi.org/10.1201/b16656.
[21] E. Brewster, R. Griffiths, A. Lawes, and S. John, IT Service Management. 2009.
[22] D. R. Donaldson and L. Bell, "Security, archivists, and digital collections," J. Arch. Organ., vol. 15, no. 1–2, pp. 1–19, 2018, doi: 10.1080/15332748.2019.1609311.
[23] R. J. Gagas, I. Syah, and F. Febryanto, "Analisis, Evaluasi, Dan Mitigasi Risiko Aset Teknologi Informasi Menggunakan Framework Octave Dan Fmea (Studi Kasus: Unit Pengelola Teknis Teknologi Informasi Dan Komunikasi Universitas Xyz)," J. Khatulistiwa Inform., vol. 9, no. 2, pp. 121–133, 2021, doi: 10.31294/jki.v9i2.11368.
[24] R. Morgan, "How to Do RACI Charting and Analysis: A Practical Guide," Retrieved Oct., pp. 1–3, 2008, [Online]. Available: http://www.spanglefish.com/SystemSafetySolutions/documents/Safety-Documents/How-to-do-RACI-Charting-and-Analysis.pdf