

ANALISIS MANAJEMEN RESIKO APLIKASI SIMFONI PADA DINAS PPA DI KAB. MINAHASA TENGGARA MENGGUNAKAN ISO 31000

¹Ferro G Punusingon, ²Melkior N N Sitokdana

^{1,2} Program Studi Sistem Informasi Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana

Jl.O.Notohamidjojo, Salatiga 50711, Indonesia, telp. (0298) 321212

e-mail: 1682015089@student.uksw.edu, melkior.sitokdana@uksw.edu

Abstrak

Aplikasi SIMFONI merupakan Sistem Informasi Perlindungan Perempuan dan Anak yang berfungsi sebagai pendataan, pencatatan, monitoring dan evaluasi kasus kekerasan, dimana data yang di tampilkan merupakan data yang up to date, real time, dan akurat. Dalam proses implementasi suatu sistem informasi pasti memiliki resiko yang akan menghambat proses pada sistem tersebut, maka di perlukan analisis resiko yang memiliki tujuan untuk mencegah atau menghindari resiko yang akan terjadi. Dengan menggunakan ISO 31000 pada kantor Dinas PPA di Kabupaten Minahasa Tenggara diharapkan dapat meminimalisir kemungkinan resiko yang akan terjadi pada aplikasi SIMFONI. Hasil analisis resiko terdapat 14 resiko yang terdiri dari 4 tingkat Risk Level High yaitu: R06(Human Error), R10(Server Down), R11(Listrik Padam), R14(Data Corrupt), kemudian terdapat 4 kemungkinan resiko tingkat Risk Level Medium yaitu: R04(Petir), R08(Pencurian Data/Perangkat Keras), R09(Trouble Web Server), R12(Gangguan Koneksi Jaringan). Serta terdapat 6 tingkat Risk Level Low yaitu: R01(Gempa Bumi), R02(Kebakaran), R03(Banjir), R05(Penyalagunaan Hak Akses), R07(Hacking). R13(Kerusakan Hardware).

Kata kunci: ISO 31000, Aplikasi SIMFONI PPA, Manajemen Resiko.

Abstract

The SIMFONI application is a Women and Children Protection Information System that functions as data collection, recording, monitoring and evaluation of cases of violence, where the data displayed is up to date, real time, and accurate data. In the process of implementing an information system, it must have risks that will hinder the process in the system, so a risk analysis is needed that has the aim of preventing or avoiding the risks that will occur. By using ISO 31000 at the PPA Office in Southeast Minahasa Regency, it is hoped that it can minimize the possible risks that will occur in the SIMFONI application. The results of the risk analysis there are 14 risks consisting of 4 levels of Risk Level High, namely: R06 (Human Error), R10 (Server Down), R11 (Power Outage), R14 (Data Corrupt), then there are 4 possible risk levels of Risk Level Medium, namely: R04 (Lightning), R08 (Data / Hardware Theft), R09 (Web Trouble Server), R12 (Network Connection Disruption). And there are 6 levels of Risk Level Low, namely: R01 (Earthquake), R02 (Fire), R03 (Flood), R05 (Use of Access Rights), R07 (Hacking). R13(Hardware Corruption).

Keywords: ISO 31000, SIMFONI PPA application, Risk Management.

1. PENDAHULUAN

Di era perkembangan zaman dan teknologi informasi yang sangat cepat dan pesat seluruh aspek kehidupan saat ini bergantung dengan teknologi, seperti pada kantor Dinas Pemberdayaan Perempuan dan Anak di Kabupaten Minahasa Tenggara yang memanfaatkan perkembangan Teknologi Informasi tersebut untuk membantu pegawai dalam melakukan pekerjaan pencatatan dan pelaporan kekerasan lintas kabupaten melalui system aplikasi yang terpadu dan komprehensif. Akan tetapi setiap aplikasi mempunyai resiko seperti *hacker* atau kejahatan *online* yang dapat merugikan, maka dari itu diperlukan analisis manajemen resiko pada aplikasi SIMFONI PPA secara berkala agar dapat

meminimalisir dampak yang akan terjadi seperti *bug* dan *error*. Yang memiliki tujuan untuk mengetahui kelemahan dan kemungkinan resiko yang akan terjadi pada aplikasi tersebut dimasa yang akan datang serta memberikan saran dan rekomendasi agar terhindar dari resiko tersebut.

Sistem Informasi Online Perlindungan Perempuan dan Anak SIMFONI PPA merupakan salah satu aplikasi berbasis *website* pada kantor dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara yang berfungsi sebagai pendataan, monitoring dan evaluasi data kekerasan perempuan dan anak, melalui sistem pencatatan dan pelaporan kekerasan lintas kabupaten maupun lintas provinsi. Pada aplikasi tersebut semua unit layanan penanganan korban kekerasan perempuan dan anak di tingkat nasional, provinsi, dan kabupaten/kota secara mendapatkan data terbaru dan akurat.

Pengelolaan resiko dinilai sebagai tantangan strategis untuk perusahaan dimana mereka akan menghadapi berbagai ancaman yang kompleks [1]. Maka penelitian ini menggunakan pendekatan ISO 31000, yaitu pendekatan yang dirancang oleh organisasi swasta *International Organization for Standardization* (ISO) untuk meningkatkan proses manajemen resiko [2]. Pendekatan ISO 31000 ini bertujuan untuk membantu menyelesaikan permasalahan terkait segala bentuk resiko secara terstruktur dan dalam berbagai lingkup dan konteks permasalahan [3]. Menurut ISO sendiri pendekatan ini dapat diterapkan diberbagai organisasi/perusahaan seperti dari bidang serta level berbeda serta dapat disesuaikan dalam berbagai fungsi, kegiatan dan proyek [3]. Penelitian ini selain menggunakan pendekatan ISO 31000 secara prosesnya namun juga pendekatan *Failure Mode and Effects Analysis* (FMEA) sebagai analisis resikonya seperti pada penelitian [4] dan [5]. Dimana menurut [5] memang dalam ISO 31000 memiliki tahapan yang telah terstruktur namun tidak menunjukkan teknik atau metode apa yang harus digunakan, maka penelitian ini juga mengusulkan dengan menggunakan FMEA dalam proses analisinya.

Setiap aplikasi selalu memiliki resiko yang akan terjadi di kemudian hari dimana akan mengganggu setiap proses pada aplikasi seperti tidak berjalan dan tidak berfungsi secara optimal. Berdasarkan permasalahan tersebut, maka perlu di lakukan penelitian mengenai resiko yang akan terjadi pada aplikasi SIMFONI PPA. Untuk menghindari kemungkinan resiko terjadi maka dilakukan analisis manajemen resiko menggunakan ISO 31000.

1.1 Tinjauan Pustaka

Analisis Manajemen Resiko menggunakan ISO 31000 yang dilakukan oleh Pangestu (2021) pada Pengadilan Negeri Salatiga kelas 1B pada aplikasi SIPP hasil penelitian manajemen resiko tersebut terdapat 14 kemungkinan resiko yang dapat mengganggu kinerja dari aplikasi SIPP di kantor Pengadilan Salatiga. Dimana ke 14 resiko tersebut tidak ada kemungkinan resiko yang memiliki tingkat risk level high. Kemudian terdapat 5 kemungkinan resiko yang tingkat *risk level medium* yaitu: R013 (kerusakan *hardware*), R012 (koneksi jaringan gangguan), R02 (kebakaran), R01 (gempa bumi), R07 (*hacking*). Serta terdapat 9 kemungkinan resiko pada tingkat *risk level low* yaitu: R011 (listrik padam secara tiba-tiba), R010 (*server down*), R09 (*trouble web server*), R014 (*data corrupt*), R03 (banjir), R04 (petir), R05 (penyalagunaan hak akses), R06 (*human error*), R08 (pencurian data/perangkat keras) [6].

Penelitian tentang analisis manajemen resiko menggunakan ISO 31000. Penelitian menggunakan ISO 31000 yang dilakukan oleh Pertiwi (2019) pada suatu perusahaan dan hasilnya terdapat 13 resiko di antaranya 6 resiko tinggi yaitu: (koneksi jaringan terganggu), (SOP DCRM tidak sepenuhnya diterapkan), (penggandaan dokumen), (pencurian dokumen), (kurangnya pemahaman TI). Kemudian 6 resiko sedang yaitu: (lemahnya *maintenance* aplikasi), (keterlambatan pengambilan dokumen), (kehilangan dokumen), (inveksi virus komputer), (kurangnya *supervise* TI), (kesalahan operasional). Dan yang terakhir terdapat 1 resiko rendah yaitu: (kerusakan *hardware*) [7].

Berdasarkan penelitian dari Lantang (2019) pada PT Serasi Autoraya terdapat 15 resiko yang berpotensi mengganggu kinerja aplikasi SAP diantaranya terdapat 2 resiko tinggi(*high*) seperti R006(koneksi *internet* putus) dan R008(listrik mati), 7 resiko sedang(*moderate*) seperti R002(*data corrupt*), R010(*overheat*), R005(kerusakan perangkat keras), R003(gempa bumi), R004(kebakaran), R011(petir), R014(peretas terhadap jaringan), dan 6 resiko rendah(*low*) seperti R015(*web service*

mati), R013(pencurian perangkat keras/PC, *hardisk*), R012(pencurian data), R009(memori penuh), R007(kurangnya SDM secara kualitas dan kuantitas), R001(banjir)[8].

Berdasarkan penelitian-penelitian tersebut penulis akan melakukan penelitian dan penulisan yang berhubungan yaitu analisis manajemen resiko aplikasi Sistem Informasi *Online* Perlindungan Perempuan dan Anak SIMFONI PPA pada Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara, menggunakan ISO 31000 yang memiliki tujuan untuk menganalisa kemungkinan resiko yang akan terjadi dan dampak dari resiko pada aplikasi SIMFONI PPA. Sehingga dapat dilakukan pencegahan sebaik mungkin agar tidak menganggu proses kinerja kantor Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara.

1.2 Landasan Teori

Menurut pendapat Jogiyanto yang dikutip oleh Rahmat Sulaiman Naibaho, Teknologi informasi adalah teknologi yang berkaitan dengan pengolahan data menjadi informasi, meliputi pengolahan, pengumpulan, penyusunan, penyimpanan, dan pengolahan data dengan berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, digunakan untuk individu, bisnis perusahaan dan di pemerintahan. Serta menjadi informasi yang strategis untuk pengambilan keputusan. Teknologi ini menggunakan perangkat komputer untuk mengolah data, jaringan untuk menghubungkan satu komputer dengan komputer lain saat dibutuhkan, dan teknologi komunikasi yang digunakan agar data dapat disebarluaskan dan diakses ke seluruh dunia [9].

Manajemen Resiko adalah untuk mengidentifikasi sumber resiko dan menganalisis strategi yang akan dihadapi. Setelah pelatihan, pelaku usaha dapat mengidentifikasi masalah, menganalisis masalah dan memecahkan masalah secara mandiri. Manajemen resiko adalah bagian penting dari manajemen bisnis. Dengan manajemen yang baik, suatu organisasi akan dapat terhindar dari kerugian, bahkan kebangkrutan. Demikian pula, usaha kecil, mikro, dan menengah tanpa kecukupan modal dan operasi yang kurang maksimal sangat rentan terhadap resiko perubahan. Dalam setiap bisnis, resiko adalah hal yang mutlak. Resiko juga bisa datang dari berbagai sumber. Masalahnya adalah bagaimana mengelola resiko tersebut. Proses manajemen resiko mutlak diperlukan jika kita ingin menghindari kerugian dalam bisnis. Proses ini diyakini berperan penting dalam keberlangsungan operasional UMKM. Hal ini merupakan upaya bagi UMKM, termasuk UMKM kecil, untuk bertahan dari ketidakpastian [10].

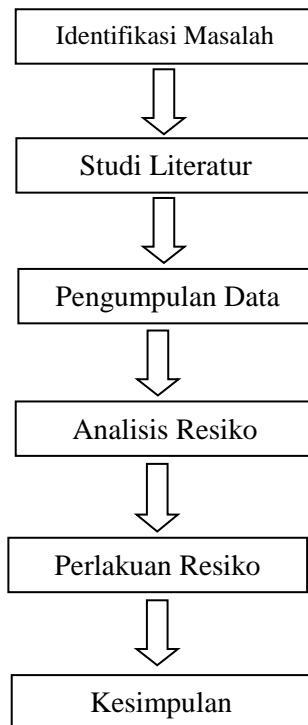
ISO 31000 adalah standar kinerja manajemen resiko yang diterbitkan oleh *International Organization for Standardization* pada 13 November 2009. Yang merupakan pedoman yang akan digunakan untuk melakukan analisis manajemen resiko yang mempunyai beberapa tahap, yaitu tahap pertama *Risk Assessment* atau Penilaian Resiko yang mempunyai 3 tahapan yaitu (*Risk Identification*) Identifikasi Resiko, (*Risk Analyst*) Analisis Resiko, (*Risk Evaluation*) Evaluasi Resiko dan tahapan selanjunya adalah (*Risk Treatment*) Perlakuan Resiko. Standar ini dimaksudkan agar dapat diterapkan dan bisa disesuaikan untuk semua jenis organisasi dengan menyediakan struktur umum dan pedoman yang berlaku untuk semua aktivitas yang terkait dengan manajemen resiko [11].

2. Metode Penelitian

Metode pengumpulan data yang digunakan dalam penelitian ini menggunakan metode kualitatif dimana metode tersebut adalah sebagai perbedaan penelitian yang menghasilkan data deskriptif yang berupa kata -kata tertulis atau lisan dari orang-orang atau perilaku yang dapat diamati, pendekatan ini diarahkan pada latar dan individu tersebut secara holistik, jadi dalam hal ini tidak boleh mengisolasi individu atau organisasi kedalam variabel atau hipotesis, tetapi memandangnya sebagai suatu keutuhan [12].

Metode penelitian yang di gunakan dalam penelitian ini yaitu metode kualitatif yang dimana metode kualitatif merupakan suatu cara yang digunakan untuk menjawab masalah penelitian yang berkaitan dengan data berupa narasi yang bersumber dari aktivitas wawancara, pengamatan, pengalian dokumen[13].

Analisis resiko merupakan sebuah kajian yang penting untuk menjamin keberhasilan proyek sesuai dengan tujuan yang telah ditetapkan, terutama untuk mendukung kegiatan-kegiatan pengembangan[14].



Gambar 1. Diagram Tahapan Penelitian

Sesuai yang ada pada gambar 1 Penelitian ini mempunyai beberapa tahap, yaitu:

1. Identifikasi Masalah

Pada proses ini peneliti mendapatkan wawasan tentang masalah yang ada untuk mendapatkan solusi.

2. Studi Literatur

Tahap ini peneliti melakukan kajian penelitian terdahulu yang relevan serta teori yang akan menjadi landasan dalam penelitian ini.

3. Pengumpulan Data

Tahap ini peneliti melakukan pengambilan data dengan melakukan wawancara secara langsung pada Pegawai Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara.

4. Analisis Resiko

Tahap ini peneliti melakukan analisis resiko yang sesuai dengan International Organization for Standardization (ISO) 31000. Dimana pada proses analisis resiko terdapat tiga tahapan, yaitu:

1) Risk Identification atau Identifikasi Resiko. Ini meliputi identifikasi resiko yang mungkin terjadi selama operasi. Identifikasi yang tepat, akurat dan lengkap sangat penting dalam manajemen resiko. Ini adalah aspek penting dari manajemen resiko. Teknik yang bisa kita gunakan adalah wawancara, survei, informasi sejarah dan sejenisnya.

2) Risk Analyst atau Analisis Resiko. Langkah ini mempertimbangkan kemungkinan akan terjadinya resiko, tingkat kerusakan yang akan ditimbulkan oleh resiko tersebut. Probabilitas suatu peristiwa sangat subjektif dan lebih tergantung pada pengalaman dan alasan.

3) Risk Evaluation atau Evaluasi Resiko. Pada tahap ini, masalah yang ada pada saat penentuan manajemen resiko serta membandingkan tingkat resiko dengan standar yang telah ditentukan. Tujuan dari penilaian resiko adalah untuk memprioritaskan dari atas ke bawah dan untuk mengetahui tingkat resiko apa yang harus segera dibenahi dan tingkat resiko apa yang harus diperhatikan [15].

5. Risk Treatment atau Perlakuan pada Resiko

Pada tahap ini peneliti melakukan upaya penyelesaian pilihan yang bisa mengurangi atau bahkan menghindari kemungkinan serta dampak dari resiko yang akan ditimbulkan dan penerapan proses perbaikan.

6. Kesimpulan. Pada tahap ini peneliti akan membuat kesimpulan berdasarkan hasil analisis resiko serta rekomendasi untuk penelitian lebih lanjut.

3. HASIL PENELITIAN DAN PEMBAHASAN

3.1 Tahap Penilaian Resiko (*Risk Assessment*)

Pada tahap ini peneliti melakukan penilaian resiko terhadap aplikasi SIMFONI PPA yang dilakukan sesuai pedoman analisis manajemen resiko ISO 31000. Dimana tahap ini terdapat 3 proses yaitu Identifikasi Resiko (*risk identification*), Analisis Resiko (*risk Analysis*), Evaluasi Resiko (*risk evaluation*).

3.1.1 Identifikasi Resiko (*Risk Identification*)

Pada proses pertama ini yang dilakukan peneliti yaitu mengidentifikasi aset yang terkait dengan aplikasi SIMFONI PPA yang dilakukan dengan cara mewawancara salah satu pegawai Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara yang merupakan *IT Operation Support*. Pada proses ini berfokus pada identifikasi asset dari data, *software* dan *hardware* yang berkaitan dengan aplikasi SIMFONI PPA.

Tabel 1. Identifikasi Aset Aplikasi SIMFONI PPA

Komponen Sistem Informasi	Asset SIMFONI PPA
<i>Data</i>	<i>Data User, Data Website</i>
<i>Hardware</i>	<i>Server Database, Personal Computer</i>
<i>Software</i>	Aplikasi SIMFONI PPA

Setelah melakukan identifikasi asset yang berkaitan dengan aplikasi SIMFONI PPA seperti *Data*, *Hardware*, *Software*. Tahap selanjutnya melakukan identifikasi kemungkinan resiko yang akan muncul pada aplikasi SIMFONI PPA. Tahap ini peneliti mengelompokan resiko berdasarkan 3 faktor yaitu faktor Alam/Lingkungan, Manusia, Sistem atau Infrastruktur serta memberikan No ID pada setiap resiko yang ditemukan.

Tabel 2. Identifikasi Kemungkinan Resiko

Faktor	ID	Kemungkinan Resiko
Alam/Lingkungan	R01	Gempa Bumi
	R02	Kebakaran
	R03	Banjir
	R04	Petir
Manusia	R05	Penyalagunaan Hak Akses
	R06	<i>Human Error</i>
	R07	<i>Hacking</i>
	R08	Pencurian Data/Perangkat keras
System/Infrastruktur	R09	<i>Trouble Web Server</i>
	R10	<i>Server Down</i>
	R11	Listrik Padam
	R12	Gangguan Koneksi Jaringan
	R13	Kerusakan <i>Hardware</i>
	R14	<i>Data Corrupt</i>

Pada tahap identifikasi resiko terdapat 14 kemungkinan resiko yang berasal dari ketiga faktor yaitu Alam/Lingkungan, Manusia, *System* atau Infrastruktur yang dapat mengancam proses kinerja aplikasi SIMFONI PPA. Kemudian kemungkinan resiko yang akan terjadi sudah teridentifikasi pada tabel 2, kembali dilakukan identifikasi dampak-dampak apa saja yang akan muncul dari kemungkinan resiko yang sudah teridentifikasi. Untuk identifikasi dampak apa saja dapat di lihat pada tabel 3.

Tabel 3. Identifikasi Dampak Resiko

ID	Kemungkinan Resiko	Dampak
R01	Gempa Bumi	Aktitivitas kantor sedikit terhambat namun aktifitas inti tidak terganggu
R02	Kebakaran	Tidak mengganggu aktivitas kantor
R03	Banjir	Tidak mengganggu aktivitas kantor
R04	Petir	Akvitas kantor berhenti karena proses kinerja mengalami gangguan total
R05	Penyalagunaan Hak Akses	Aktitivitas kantor sedikit terhambat namun aktifitas inti tidak terganggu
R06	<i>Human Error</i>	Menyebabkan gangguan pada proses kinerja sehingga jalannya aktivitas kantor terhambat
R07	<i>Hacking</i>	Aktitivitas kantor sedikit terhambat namun aktifitas inti tidak terganggu
R08	Pencurian Data/Perangkat Keras	Menyebabkan gangguan pada proses kinerja sehingga jalannya aktivitas kantor terhambat
R09	<i>Trouble Web Server</i>	Aplikasi SIMFONI PPA tidak dapat di akses dan Aktivitas kantor sedikit terhambat namun aktifitas inti tidak terganggu
R10	<i>Server Down</i>	Menyebabkan gangguan pada proses kinerja sehingga jalannya aktivitas kantor terhambat
R11	Listriik Padam	Akvitas kantor berhenti karena proses kinerja mengalami gangguan total
R12	Gangguan Koneksi Jaringan	Aktitivitas kantor sedikit terhambat namun aktifitas inti tidak terganggu
R13	Kerusakan <i>Hardware</i>	Aktitivitas kantor sedikit terhambat namun aktifitas inti tidak terganggu
R14	<i>Data Corrupt</i>	Menyebabkan gangguan pada proses kinerja sehingga jalannya aktivitas kantor terhambat

3.1.2 Analisis Resiko (*Risk Analysis*)

Setelah melakukan identifikasi kemungkinan resiko dan dampaknya, selanjutnya masuk pada proses analisis resiko. Pada tahap ini dilakukan analisis terhadap kemungkinan resiko yang sebelumnya sudah diidentifikasi, pada tahap ini terdapat 2 tabel kriteria yaitu *Likelihood* dan *Impact* yang menjadi acuan untuk tahap analisis resiko. Pada tabel 4, terdapat tabel kriteria *likelihood* yang dimana tabel tersebut memiliki 5 kriteria berdasarkan seberapa banyak kemungkinan resiko yang dapat terjadi dalam periode waktu tertentu.

Tabel 4. Kriteria *Likelihood*

Nilai	Kriteria	Keterangan	Frekuensi Kejadian
1	<i>Rare</i>	Resiko tersebut hampir tidak pernah terjadi	>2 tahun
2	<i>Unlikely</i>	Resiko tersebut jarang terjadi	1-2 tahun
3	<i>Possible</i>	Resiko tersebut kadang terjadi	7-12 bulan
4.	<i>Likely</i>	Resiko tersebut sering terjadi	4-6 bulan
5	<i>Certain</i>	Resiko tersebut pasti terjadi	1-3 bulan

Kemudian pada tabel 5 terdapat tabel nilai *impact* yang merupakan dampak jika kemungkinan resiko tersebut terjadi pada kantor Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara. Di dalam tabel penilaian *impact* memiliki 5 kriteria dampak yang mungkin terjadi, dan dibedakan berdasarkan dampak yang tidak berpengaruh bagi kantor hingga dampak yang paling mempengaruhi kinerja kantor.

Tabel 5. Kriteria Impact

Nilai	Kriteria	Keterangan
1	<i>Insignificant</i>	Tidak mengganggu aktivitas kantor
2	<i>Minor</i>	Aktivitas kantor sedikit terhambat namun aktivitas inti tidak terganggu
3	<i>Moderate</i>	Menyebabkan gangguan pada proses kinerja sehingga jalannya aktivitas terhambat
4	<i>Major</i>	Menghambat hampir seluruh aktivitas kantor
5	<i>Catastrophic</i>	Aktivitas kantor berhenti karena proses kinerja mengalami gangguan total

Setelah selesai menentukan nilai *Likelihood* pada tabel 4 dan *impact* pada tabel 5, tahap berikutnya melakukan penilaian terhadap kemungkinan resiko yang sudah teridentifikasi pada tahap sebelumnya. Dari 14 kemungkinan resiko yang sudah diidentifikasi masing-masing resiko ditentukan nilai *Likelihood* dan nilai *impact* yang acuannya sudah dibuat pada tabel 4 dan tabel 5. Tabel berikutnya yaitu penilaian terhadap kemungkinan resiko dapat dilihat pada tabel 6.

Tabel 6. Penilaian Terhadap Kemungkinan Resiko

Faktor	ID	Kemungkinan Resiko	Likelihood	Impact
Alam/lingkungan	R01	Gempa Bumi	2	2
	R02	Kebakaran	1	1
	R03	Banjir	1	1
	R04	Petir	5	1
	R05	Penyalagunaan Hak Akses	2	2
	R06	<i>Human Error</i>	5	2
	R07	<i>Hacking</i>	1	2

Manusia	R08	Pencurian Data/Perangkat Keras	2	3
	R09	<i>Trouble Web Server</i>	5	2
	R010	<i>Server Down</i>	5	3
	R011	<i>Listriik Padam</i>	5	4
System/infrastruktur	R012	Gangguan Koneksi jaringan	4	2
	R013	Kerusakan <i>Hardware</i>	1	2
	R014	<i>Data Corrupt</i>	5	3

3.1.3 Evaluasi Resiko (*Risk Evaluation*)

Proses evaluasi resiko terakhir yaitu (*risk evaluation*) pada tahap *risk assessment* (penilaian resiko). Pada proses ini menggunakan acuan berupa tabel *matrix* untuk evaluasi resiko yang berdasarkan pada panduan kerangka kerja ISO 31000 dimana pada tabel *Matrix Evaluasi resiko* terdapat 3 level (*risk level*) yaitu *low*, *medium*, dan *high*. Dapat di lihat pada tabel 7 dibawah ini yaitu tabel *matrix* evaluasi resiko yang sudah sesuai dengan *risk level* berdasarkan *likelihood* dan *impact* nya.

Tabel 7. Matrix Evaluasi Resiko

Likelihood	Impact	Certain	Medium	Medium	High	High	High
		Likely	Medium	Medium	Medium	High	High
Possible	3	Low	Medium	Medium	Medium	High	
Unlikely	2	Low	Low	Medium	Medium	Medium	Medium
Rare	1	Low	Low	Low	Medium	Medium	Medium
Impact	1		2	3	4	5	
	Insignificant		Minor	Moderate	Major	Catastrophic	

Pada tahap ini kemungkinan resiko yang sudah di dapat nilai *likelihood* dan *impact* akan di masukkan kedalam tabel *matrix* resiko sesuai dengan pemetaan yang ada pada tabel tersebut, tabel 8 dibawah ini merupakan hasil dari kemungkinan resiko yang sudah dimasukan kedalam tabel *matrix*.

Tabel 8. Matrix Evaluasi Resiko Berdasarkan Nilai *Likelihood* dan *Impact*

Likelihood	Impact	Certain	5	R04	R09	R06 R10 R14	R11	
		Likely	4		R12			
Possible	3							
Unlikely	2				R01 R05	R08		
Rare	1			R02 R03	R07 R13			
Impact	1		2	3	4	5		
	Insignificant		Minor	Moderate	Major	Catastrophic		

Selanjutnya semua kemungkinan resiko yang sudah terkumpul di masukan kedalam tabel *matrix* evaluasi resiko yang sesuai dengan nilai *likelihood* dan *impact* nya, pada tabel 9 akan dikelompokan dari 14 kemungkinan resiko yang ada dan di sesuaikan dengan tingkat *risk level* nya *high*, *medium* dan *low* berdasarkan data yang ada di tabel 8.

Tabel 9. Ketingkatan Risk Level Berdasarkan Masing-masing Resiko

ID	Kemungkinan Resiko	Likelihood	Impact	Risk level
R06	<i>Human Error</i>	5	3	High
R10	<i>Server Down</i>	5	3	
R11	Listrik Padam	5	4	
R14	<i>Data Corrupt</i>	5	3	
R04	Petir	5	1	Medium
R08	Pencurian Data/Perangkat Keras	2	3	Medium
R09	<i>Trouble Web Server</i>	5	2	Medium
R12	Gangguan Koneksi	4	2	Medium
R01	Gempa Bumi	2	2	Low
R02	Kebakaran	1	1	
R03	Banjir	1	1	
R05	Penyalagunaan Hak Akses	2	2	
R07	<i>Hacking</i>	1	2	Low
R13	Kerusakan Hardware	1	2	Low

Pada tabel diatas merupakan hasil dari proses evaluasi resiko dimana terdapat 14 kemungkinan resiko yang telah di kelompokkan berdasarkan *Risk Levelnya*.

3.1.4 Perlakuan Resiko (*Risk Treatment*)

Setelah melakukan tahapan pada tabel di atas yang terdapat 3 proses tahapan yaitu *risk identification*, *risk analysis*, dan *risk evaluation* maka tahap selanjutnya yaitu proses *risk treatment* yang dimana pada tahap ini peneliti memberikan masukan atau saran terhadap kemungkinan resiko yang sudah di identifikasi dan dikelompokkan berdasarkan *risk level* pada tabel 9. Dapat di lihat pada tabel 10 usulan dari peneliti yang dapat digunakan oleh kantor Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara agar terhindar dari resiko dan meminimalisir resiko yang akan terjadi.

Tabel 10. Usulan Perlakuan Terhadap Resiko

ID	Kemungkinan Resiko	Risk level	Usulan terhadap resiko
R06	<i>Human Error</i>	High	Harus memberikan pelatihan atau <i>training</i> kepada para pegawai atau staf yang akan menggunakan aplikasi SIMFONI PPA, agar <i>user</i> lebih menguasai pada saat implementasi di lapangan.
R10	<i>Server Down</i>	High	Melakukan pengecekan secara rutin pada load/pemakaian server.
R11	Listrik Padam	High	Menyediakan UPS sebagai penunjang sementara pada setiap perangkat yang ada dikantor, untuk tahap selanjutnya diperlukan genset agar dapat menunjang aktivitas perkantoran.
R14	<i>Data Corrupt</i>	High	Dapat melakukan <i>back up</i> data secara rutin dan melakukan penggecekan atau pembersihan data-data yang tidak

R04	Petir	Medium	digunakan agar <i>space</i> pada <i>server</i> tetap terjaga dan stabil.
R08	Pencurian Data/Perangkat Keras	Medium	Melakukan pemasangan alat penangkal petir di luar bangunan untuk mencegah jika terjadi sambaran petir yang dapat merusak kelistrikan dan komputer.
R09	<i>Trouble Web Server</i>	Medium	Menggunakan aplikasi pihak ke 3 untuk mencegah <i>user</i> menggunakan <i>flash disk</i> dengan bebas agar terhindar dari pencurian data dan memasang CCTV pada bagian tertentu untuk mencegah pencurian perangkat keras.
R12	Gangguan Koneksi Jaringan	Medium	Melakukan pengecekan terhadap <i>web server</i> , <i>domain</i> dan <i>hosting</i> apakah bermasalah atau masa berlaku sudah habis.
R01	Gempa Bumi	Low	Melakukan pengecekan pada perangkat jaringan yang ada dikantor baik itu kabel, <i>modem</i> atau <i>router</i> dan <i>lan card</i> yang ada pada setiap komputer atau laptop yang digunakan <i>user</i> , jika masih terjadi gangguan maka langsung menghubungi pihak ISP agar dapat segera di perbaiki.
R02	Kebakaran	Low	Menyediakan <i>server</i> cadangan di tempat lain dan menyediakan tempat aman agar perangkap penunjang terhindar dari kerusakan.
R03	Banjir	Low	Menyediakan alat pemadam kebakaran seperti APAR dan sumber air yang cukup.
R05	Penyalagunaan Hak Akses	Low	Meletakan alat penunjang dan komputer pada tempat yang aman dari banjir.
R07	<i>Hacking</i>	Low	Melakukan <i>maintenance</i> seperti <i>update password</i> pada akses <i>user login</i> dan memasang CCTV pada ruang kerja.
R13	Kerusakan <i>Hardware</i>	Low	Memastikan <i>system security</i> yang ada pada aplikasi berjalan dengan benar dan terenkripsi sesuai dengan metode yang digunakan. Kemudian rutin melakukan pergantian <i>password</i> .
			Melakukan pengecekan secara berkala jika ditemukan perangkat yang rusak dapat segera diganti atau dilakukan <i>service</i> .

3.2. Pembahasan

Sesuai dengan penelitian yang dilakukan Pangestu pada aplikasi SIPP merupakan sebuah sistem informasi penelusuran perkara yang fungsinya untuk menyediakan informasi kepada masyarakat umum atau para pihak yang bersangkutan dengan perkara dan informasi yang ada didalam SIPP telah disesuaikan dengan peraturan yang berlaku. Dalam proses implementasi sistem informasi tersebut tentu memiliki resiko yang dapat menghambat proses kerja, maka dibutuhkan analisis resiko yang memiliki tujuan mengurangi dan mencegah resiko yang akan terjadi pada kantor Pengadilan Negeri Salatiga. Penulis menggunakan metode ISO 31000 dan menggunakan tahapan yang sama seperti digunakan pada penelitian ini akan tetapi memiliki hasil yang berbeda, hasil yang di dapatkan oleh Pangestu tidak ada kemungkinan resiko yang memiliki tingkat *Level High Risk*, kemudian terdapat 5 kemungkinan resiko yang tingkat *Level Medium Risk* yaitu: R013(kerusakan *hardware*), R012(koneksi jaringan gangguan), R02(kebakaran), R01(gempa bumi), R07(*hacking*). Serta terdapat 9 kemungkinan resiko pada tingkat *Level Low Risk* yaitu: R011(kerusakan genset kantor), R010(*server down*), R09(*trouble web server*), R014(*data corrupt*), R03(banjir), R04(petir), R05(penyalagunaan hak akses), R06(*human error*), R08(pencurian data/perangkat keras). Hasil yang didapatkan pada penelitian yang dilakukan oleh Pangestu seperti pada penjelasan diatas mendapatkan hasil yang berbeda, penelitian yang dilakukan pangestu tidak memiliki *Risk Level High* sedangkan pada penelitian yang saya lakukan terdapat 4 *Risk Level High* dikarenakan terdapat beberapa hal dan faktor yang menjadi pembeda pada hasil penelitian yang kami lakukan seperti faktor alam dan lingkungan di setiap daerah, serta perbedaan sumber daya manusia yang ada pada kantor Pengadilan Negeri Salatiga dan Kantor Dinas PPA di Minahasa Tenggara dan perbedaan infrastruktur yang ada pada setiap kantor.

4. KESIMPULAN

Hasil dari penelitian ini menemukan ada 14 kemungkinan resiko yang akan terjadi dan dapat mengganggu kinerja dari aplikasi SIMFONI PPA pada Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara. Dimana 14 resiko tersebut terdapat 4 tingkat *Risk Level High* yaitu: R06(*Human Error*), R10(*Server Down*), R11(Listrik Padam), R14(*Data Corrupt*), kemudian terdapat 4 kemungkinan resiko tingkat *Risk Level Medium* yaitu: R04(Petir), R08(Pencurian Data/Perangkat Keras), R09(*Trouble Web Server*), R12(Gangguan Koneksi Jaringan). Serta terdapat 6 tingkat *Risk Level Low* yaitu: R01(Gempa Bumi), R02(Kebakaran), R03(Banjir), R05(Penyalagunaan Hak Akses), R07(*Hacking*). R13(Kerusakan *Hardware*). Dengan ini berikut hasil penelitian yang dapat digunakan oleh Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Minahasa Tenggara agar SOP (*Standard Operasional Procedure*) tidak terganggu dan dapat meminimalisir kemungkinan resiko yang akan terjadi di masa yang akan datang.

Saran untuk penelitian kedepannya sebaiknya melakukan pengolahan resiko dari lingkup yang kecil terlebih dahulu yang bertujuan untuk mendapatkan hasil yang lebih efektif, serta memperhatikan konsep yang ada secara detail agar proses penerapan manajemen resiko berbasis ISO 31000 dapat lebih sempurna.

Daftar Pustaka

- [1] C. Lalonde and O. Boiral, “Managing risks through ISO 31000: A critical analysis,” *Risk Manag.*, vol. 14, no. 4, pp. 272–300, Nov. 2012.
- [2] A. J. Prieto Ibáñez, J. M. Macías Bernal, M. J. Chávez de Diego, and F. J. Alejandre Sánchez, “Expert system for predicting buildings service life under ISO 31000 standard. Application in architectural heritage,” *J. Cult. Herit.*, vol. 18, pp. 209–218, Mar. 2016.
- [3] U. R. de Oliveira, F. A. S. Marins, H. M. Rocha, and V. A. P. Salomon, “The ISO 31000 standard in supply chain risk management,” *J. Clean. Prod.*, vol. 151, pp. 616–633, May 2017.
- [4] B. Purwanganono and A. Margarette, “Risk assessment of underpass infrastructure project based on ISO 31000 and ISO 21500 using fishbone diagram and RFMEA (project risk failure mode and effects analysis) method,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 277, no. 1, p. 012039, Dec. 2017.

- [5] F. Shirvani, W. Scott, G. A. L. Kennedy, and A. P. Campbell, “Enhancement of FMEA risk assessment with SysML,” *Aust. J. Multi-Disciplinary Eng.*, vol. 15, no. 1, pp. 52–61, Jan. 2019.
- [6] R. H. Pangestu, A. D. Cahyono, dan P. F. Tanaem, “Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Menggunakan ISO 31000,” *J. Comput. Inf. Syst. Ampera*, vol. 2, no. 1, hal. 43–57, 2021, doi: 10.51519/journalcisa.v2i1.59.
- [7] Angraini and I. D. Pertiwi, “Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000,” *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 3, no. 2, pp. 70–76, 2017, [Online]. Available: <http://ejurnal.uin-suska.ac.id/index.php/RMSI/article/view/4317>.
- [8] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, “Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000,” *Sebatik*, vol. 23, no. 1, pp. 36–43, 2019, doi: 10.46984/sebatik.v23i1.441.
- [9] R. S. Naibaho, “Peranan Dan Perencanaan Teknologi Informasi Dalam Perusahaan,” *J. War.*, no. April, hal. 4, 2017, [Daring]. Tersedia pada: <https://media.neliti.com/media/publications/290731-peranan-dan-perencanaan-teknologi-inform-ad00d595.pdf>.
- [10] A. Susetyo dan A. Prasetyo, “Pelatihan Manajemen Resiko Bagi Usaha Mikro Kecil dan Menengah di Era Pandemi Covid-19,” *JCSE J. Community ...*, vol. 1, no. 1, hal. 81–87, 2020, [Daring]. Tersedia pada: <http://journal.stieputrabangsa.ac.id/index.php/jcse/article/view/681>.
- [11] E. Muryanti dan K. D. Hartomo, “Analisis Resiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 3, hal. 1265–1277, 2021, doi: 10.35957/jatisi.v8i3.948.
- [12] Moleong, Lexy J. (2014). Metodologi Penelitian Kuantitatif. Bandung: PT Remaja Rosdakarya.
- [13] Wahidmurni, “PEMAPARAN METODE PENELITIAN KUALITATIF Oleh:,” *J. Sains dan Seni ITS*, vol. 6, no. 1, pp. 51–66, 2017.
- [14] F. Asmin, “Analisis Resiko Implementasi Kegiatan Pengembangan Masyarakat Sekitar Hutan Di Sumatera Barat 194,” *J. Sist. (Sistem Informasi)*, vol. 8, pp. 194–203, 2019.
- [15] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, “Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.



ZONAsi: Jurnal Sistem Informasi
is licensed under a [Creative Commons Attribution International \(CC BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/)