Journal of Computer and Information Systems Ampera
Vol. 2, No. 1, January 2021 e-ISSN: **2775-2496**
https://journal-computing.org/index.php/journal-cisa/index

Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Mengunakan ISO 31000

Ryan Haryo Pangestu[1], Ariya Dwika Cahyono[2], Penidas Fiodinggo Tanaem[3]

[1,2,3]Information System Departement, Satya Wacana Christian University, Salatiga, Idnonesia
Email: [1]682017098@student.uksw.edu, [2]ariyadc@uksw.edu, [3]penidas.fiodinggo@uksw.edu

Abstract

SIPP application is a case tracing information system whose function is to provide information to the general public or severe parties concerned with the case and the information contained in sipp has been adjusted to the applicable regulations. In implementing the information system there must be risks that hinder the process of the system, so here is required risk analysis aimed at preventing or minimizing the risks that will occur. By using ISO 31000 at salatiga district court office, it is expected to minimize the possibility of risks that will occur around SIPP application. The results will be from iso 31000 risk analysis in the form of a document of possible risks that occur around sipp application, grouping the possible risks and their impacts. So that the results of this research can be useful for the salatiga district court office to prevent or at least minimize the risks that may occur in the SIPP application.

Keywords: ISO 31000, SIPP Application, Risk Management.

1. PENDAHULUAN

Di zaman yang modern sekarang ini perkembangan teknologi berkembang sangat pesat dan dari seluruh aspek kehidupan yang ada hampir sangat bergantung dengan yang namanya teknologi informasi begitu juga dengan Pengadilan Negeri salatiga, perkambangnya teknologi tersebut ditunjang dengan aplikasi yang ada di pengadilan negeri salatiga yang membantu pegawai dalam melakukan pekerjaan mengenai perkara dan masyarakat yang ingin mencari informasi mengenai perkara, tetapi juga setiap aplikasi

mempunyai dampak negatifnya seperti kejahatan online atau hacker dan carding pada sebuah aplikasi. Maka dari itu perlu di lakukan analisi manajemen resiko di aplikasi tersebut secara berkala agar bias meminimalisir kesalahan-kesalahan yang ada seperti program atau bug serta kelemahan pada program aplikasi, yang bertujuan untuk mengetahui kelemahan atau kemungkinan resiko-resiko yang terjadi di aplikasi dan memberikan saran dan rekomendasi dari kemungkinan resiko-resiko yang akan terjadi.

Sistem Informasi Penelusuran Perkara (SIPP) merupakan sebuah aplikasi berbasis web di Pengadilan Negeri Salatiga kelas 1B yang berfungsi untuk menginput informasi – informasi yang berkaitan dengan perkara seperti data umum, penetapan jadwal untuk sidang, penetapan hakim siapa yang akan memimpin siding, penetapan panitera pengganti, kemudian juga bisa sebagai informasi bagi masyarakat yang mungkin berhubungan dengan perkara dan masyarakat yang terkena tilang juga bisa langsung mengecek denda tilangnya di SIPP Pengadilan Negeri Salatiga kelas 1B.

Dengan adanya aplikasi SIPP pasti memiliki kemungkinan resiko-resiko yang akan terjadi di kemudian hari yang akan mengganggu proses aplikasi tersebut tidak berjalan atau berfungsi dengan optimal. Berdasarkan permasalahan tersebut, maka diperlukan penelitian mengenai kemungkinan resiko-resiko yang akan terjadi pada aplikasi SIPP di kemudian hari. Untuk meminimalisir kemungkinan resiko tersebut maka dilakukan penelitian analisis manajemen resiko menggunakan ISO 31000. Penelitian mengunakan ISO 31000 pernah dilakukan oleh Angraini, Indri Dian Pertiwi pada suatu perusahaan dan hasilnya terdapat 13 resiko diantaranya 6 resiko tinggi salah satunya koneksi jaringan terganggu dan SOP DCRM tidak sepenuhnya diterapkan,6 resiko sedang,1 resiko rendah yang dapat berdampak pada perusahaan tesebut[1].

Berdasarkan penelitian dari Grialdo Willy Lantang dkk (2019) pada PT Serasi Autoraya terdapat 15 resiko yang berpotensi menggangu kinerja aplikasi SAP diantaranya terdapat 2 resiko tinggi(high) seperti koneksi internet putus dan listrik mati, 7 resiko sedang(moderate),6 resiko rendah(low)[2]. Kemudian penelitian selanjutnya juga pernah dilakukan oleh Fawwaz Afif Alvian dkk (2020) tentang analisis manajemen resiko mengunakan ISO 31000 pada Universitas Islam Negeri Sunan Ampel Surabaya dan hasilnya terdapat 8 resiko tinggi (high) salah satunya yaitu tidak stabilnya listrik pada laboratorium biologi yang dikarenakan adanya

UPS,3 resiko sedang (moderate),1 resiko rendah(low) agar resiko tersebut dapat dihindari diperlukan perlakuan pada masing-masing tingkat resikonya[3].

Berdasarkan penelitian diatas bahwa terdapat hubungan dengan penelitian yang akan dilakukan penulis yaitu analisi manajemen resiko pada aplikasi Sistem informasi Penelusuran Perkara (SIPP) di Pengadilan Negeri Salatiga menggunakan analisis resiko ISO 31000 yang bertujuan menganalisis resiko yang mungkin akan muncul, dampak dari resiko itu sendiri, tingkat resiko, dan tindakan terhadap kemungkinan resiko-resiko yang ada pada aplikasi SIPP sehingga Pengadilan Negeri Salatiga dapat melakukan pencegahan sebaik mungkin sehingga kemungkinan resiko-resiko tersebut tidak terjadi dan mengganggu proses kinerja kantor.

2. METODE

Metode 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[4].

2.1. METODE PENELITIAN

Kemudian pada penelitian ini dilakukan analisis resiko mengunakan International Organization for Standardization (ISO 31000) pada aplikasi SIPP di Pengadilan Negeri Salatiga. ISO 31000 merupakan standar yang berkaitan dengan manajemen risiko yang dimodifikasi oleh International Organization for Standardization (ISO) atau Organisasi Internasional untuk Standarisasi. Tujuan dari ISO 31000 sendiri adalah untuk memberikan prinsip-prinsip dan pedoman untuk manajemen risiko yang di akui secara universal[5]. Di dalam ISO 31000 atau international Organization for Standardization pada gambar 1 menjelaskan susunan kerangka kerja dari manajemen resiko secara universal yang dimana terdapat 2 tahap dalam proses analisis manajemen resiko.

Tahap pertama yaitu penilain resiko(risk assessment) yang di dalamnya lagi ada 3 proses yaitu Identifikasi resiko(risk identification), Analisis resiko(risk analysis), Evaluasi resiko(risk evaluation). Identifikasi resiko adalah usaha untuk menemukan atau mengetahui resiko-resiko yang akan

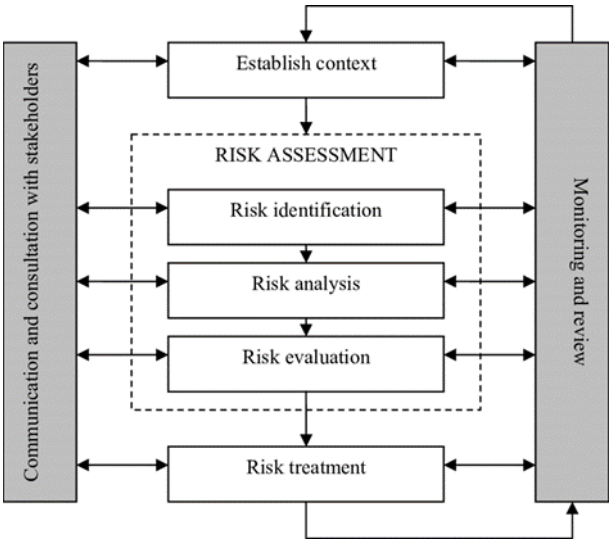
timbul pada proses bisnis perusahaan atau organisasi. Identifikasi resiko biasanya dilakukan pada semua proses bisnis yang ada pada sebuah organisasi atau perusahaan. Hal ini memiliki tujuan untuk mengetahui semua resiko-resiko yang timbul dari berbagai faktor, faktor tersebut bisa dari faktor manusia, faktor sistem yang diimplementasikan pada perusahaan atau organisasi , dan bisa jadi faktor dari insfrastruktur[6]. Identifikasi resiko ini dilakukan pada aplikasi SIPP di Pengadilan Negeri Salatiga kelas 1B.

Analisis resiko merupakan sebuah kajian yang penting untuk menjamin keberhasilan proyek sesuai dengan tujuan yang telah ditetapkan, terutama untuk mendukung kegiatan-kegiatan pengembangan[7]. proses analisis resiko pada penelitian ini berfokus pada menentukan resiko-resiko yang berpotensi menghambat kinerja dari aplikasi SIPP di kantor Pengadilan Negeri Salatiga. Evaluasi resiko merupakan proses evaluasi resiko-resiko berdasarkan tingkat yang palimg tinggi resikonya sampai yang paling rendah resikonya berdasarkan kriteria yang sudah di buat. Pada proses ini nanti berfokus pada evalusai resiko-resiko yang ada pada aplikasi SIPP.

Tahapan kedua setelah Risk Assesment yaitu Risk Treatment dimana pada tahap ini peneliti memberikan rekomendasi atau tindakan terhadap kemungkinan resiko-resiko yang bertujuan utntuk menanganinya atau meminimalisir resiko-resiko yang ada pada aplikasi SIPP. Pada penelitian ini akan dilakukan dengan dua tahap yaitu, pertama peneliti melakukan pencarian informasi yang di butuhkan melalui wawancara langsung dengan narasumber internal Pengadilan Negeri Salatiga, tahap kedua peneliti mengelola data yang sudah di dapat dari wawancara yang kemudian di analisi berdasarkan proses tahapan pada kerangka kerja ISO 31000.

Metode yang akan penulis gunakan dalam penelitian ini yaitu Case study research, yang dimana metode ini berfokus pada satu objek studi kasus. Sehingga dengan metode ini penulis dapat berfokus pada objek yang diteliti dan dapat mengumpulkan data yang dibutuhkan dengan terarah serta bisa menjawab mengenai permasalahan yang terjadi. Data dalam penelitian ini berupa data primer yang didapatkan dari narasumber langsung yang terkait dengan SIPP (Sistem Informasi Penelusuran Perkara) Pengadilan Negeri Salatiga. Narasumber dalam penelitian ini ada yaitu salah satu pegawai Pengadilan Negeri Salatiga yang tugasnya

mengelola dan mengawasi aplikasi Sistem Informasi Penelusuran Perkara (SIPP).



Gambar 1. Tahapan Risk Management

3. HASIL DAN PEMBAHASAN

3.1. Tahap Penilaian Resiko (Risk Assement)

Pada tahap ini peneliti melakukan penilaian resiko terhadap aplikasi SIPP 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 SIPP yang dilakukan dengan cara mewawancarai salah satu pegawai Pengadilan Negeri Salatiga yang merupakan IT Operation Support. Pada proses ini berfokus pada identifikasi asset dari data, software dan hardware yang berkaitan dengan aplikasi SIPP.

Tabel 1. Identifikasi Asset Aplikasi SIPP

Komponen Sistem Informasi	Asset SIPP
Data	Data User, Data Buku
Hardware	Server Database, Personal Computer
Software	Aplikasi SIPP

Setelah dilakukan identifikasi asset yang berkaitan dengan aplikasi SIPP seperti Data, Hardware, Software. Maka selanjutnya melakukan identifikasi kemungkinan resiko-resiko yang akan muncul di sekitar aplikasi SIPP. Disini peneliti mengkelompokan resiko berdasarkan 3 faktor yaitu factor Alam/Lingkungan, Manusia, Sistem dan Infastruktur serta memberikan No ID pada setiap resiko-resiko yang ditemukan.

Tabel 2. Identifikasi Kemungkinan Resiko

Faktor	ID	Kemungkinan
Alam/Lingkungan	R01	Gempa Bumi
	R02	Kebakaran
	R03	Banjir
	R04	Petir
Manusia	R05	Penyalagunaan Hak Akses
	R06	Human Error
	R07	Hacking
	R08	Pencurian Data/Perangkat keras
System/Infrastruktur	R09	Trouble Web Server
	R010	Server Down
	R011	Kerusakan genset kantor
	R012	Koneksi Jaringan Gangguan
	R013	Kerusakan Hardware
	R014	Data Corrupt

Dari tahap indentifikasi resiko ditemukan 14 kemungkinan resiko-resiko yang berasal dari ketiga factor yaitu Alam/Lingkungan, Manusia, System dan Infrastruktur yang berpotensi bisa mengancam proses kinerja aplikasi SIPP. Kemudian kemungkinan resiko-resiko yang sudah teridentifikasi pada table 2 tersebut, dilakukan lagi identifikasi dampak-dampak apa saja

yang akan muncul dari kemungkinan resiko-resiko yang sudah di identifikasi. Identifikasi dampak-dampaknya Dapat di lihat pada table 3 berikut.

Tabel 3. Identifikasi Dampak Resiko

ID	Kemungkinan Resiko	Dampak
R01	Gempa Bumi	Kerusakan infrastruktur dan Aktitivitas kantor jadi terganggu
R02	Kebakaran	Kerusakan infrastruktur dan proses kinerja kantor terhenti
R03	Banjir	Aktivitas kantor jadi terganggu
R04	Petir	Kerusakan infrastruktur pada kantor
R05	Penyalagunaan Hak Akses	Data user akan tersadap atau hak user akan disalah gunakan
R06	Human Error	Proses layanan kantor tidak berjalan optimal
R07	Hacking	System mengalami gangguan atau disadap
R08	Pencurian Data/Perangkat Keras	Kantor mengalami Kerugian finansial dan kehilangan data.
R09	Trouble Web Server	Pegawai kantor tidak dapat mengakses aplikasi SIPP karena mengalami trouble.
R010	Server Down	Server data base bermasalah mengakibatkan pegawai kantor tidak bisa mengakses aplikasi yang berkaitan dengan server termasuk SIPP.
R011	Kerusakan genset kantor	Sewaktu-waktu listrik padam pegawai kantor tidak bisa menggunakan hardware pada kantor untuk kerja.
R012	Koneksi Jaringan Gangguan	Membutuhkan waktu yang agak lama untuk Mengakses aplikasi SIPP.
R013	Kerusakan Hardware	Kinerja kantor jadi terhambat karena perlu malakukan set up data di hardware baru

R014	Data Corrupt	Pegawai tidak bisa mngakses data karena datanya tidak valid/corrupt

3.1.2 Analisis Resiko (*Risk Analysis)*

Setelah melakukan identifikasi kemungkinan resiko-resiko beserta dampak-dampaknya, kemudian selanjutnya melakukan proses analisis resiko. Pada tahap ini di lakukan analisis tehadap kemungkinan resiko-resiko yang sebelumnya sudah di identifikasi, pada tahap ini terdapat 2 table kriteria yaitu Likehood dan Impact yang menjadi acuan untuk tahap analisis resiko. pada tabel 4 terdapat table kriteria likehood yang dimana table tersebut terdapat 5 kriteria yang dibedakan berdasarkan seberapa banyak kemungkinan resiko dapat terjadi dalam kurun waktu tertentu.

Tabel 4. Kriteria Likelihood

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

Kemudian pada table 5 terdapat table nilai impact yang merupakan dampak jika kemungkinan resiko-resiko tersebut terjadi pada kantor Pengadilan Negeri Salatiga. Di dalam table penilaian impact terdapat 5 kriteria dampak yang mungkin terjadi, yang dibedakan berdasarkan dampak yang tidak berpengaruh bagi kantor Pengadilang Negeri Salatiga hingga dampak yang paling mempengaruhi kinerja kantor.

Tabel 5. Kriteria Impact

Nilai	Kriteria	Keterangan
1.	*Insignificant*	Tidak mengganggu aktivitas kantor
2.	*Minor*	Aktivitas kantor sedikit terhambat namun aktivitas inti perpustakaan tidak mengganggu
3.	*Moderate*	Menyebapkan gangguan pada proses kinerja sehingga jalannya aktivitas perpustakaan terhambat

4.	*Major*	Menghambat hampir seluruh aktivitas kantor
5.	*Catasirophic*	Akivitas kantor berhenti karena proses kinerja mengalami ganguan total

Setelah menentukan nilai Likelihood pada tabel 4 dan impact pada tabel 5, selanjutnya melakukan penilaian terhadap kemungkinan resiko-resiko yang sudah di identifikasikan pada tahap sebelumnya. Dari 14 kemungkinan resiko-resiko yang sudah diidentifikasikan tersebut masing-masing resiko ditentukan nilai Likelihood dan nilai impact nya yang acuannya sudah dibuat pada tabel 4 dan tabel 5. Tabel penilaiann terhadap kemungkinan resiko-resiko bisa di lihat pada tabel 6 berikut.

Tabel 6. Penilaian Terhadap Kemungkinan Resiko

Faktor	ID	Kemungkinan Resiko	Likelihood	Impact
Alam/Lingkungan	R01	Gempa Bumi	1	5
	R02	Kebakaran	2	5
	R03	Banjir	1	1
	R04	Petir	1	1
Manusia	R05	Penyalagunaan Hak Akses	1	1
	R06	Human Error	1	1
	R07	Hacking	2	4
	R08	Pencurian Data/Perangkat Keras	1	1
System/Infrastruktur	R09	Trouble Web Server	1	2
	R010	Server Down	2	2
	R011	Kerusakan genset kantor	1	3
	R012	Koneksi Jaringan Gangguan	2	5
	R013	Kerusakan Hardware	2	5
	R014	Data Corrupt	1	2

3.1.3 Evaluasi Resiko (Risk Evaluation)

Pada proses terakhir yaitu evaluasi resiko (risk evaluation) untuk tahap risk assessment (penilaian resiko). Pada proses ini mengunakan acuan

berupa tabel matrix evaluasi resiko yang berdasarkan pada pedoman kerangka kerja ISO 31000 dimana dalam tabel matrix evaluasi resiko di bedakan menjadi 3 risk level yaitu low, medium, dan high. Pada tabel. 7 dibawah ini merupakan tabel matrix evaluasi resiko yang sudah di tentukan risk level berdasarkan likelihood dan impact nya.

Tabel 7. Matrix Evaluasi Resiko

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

Setelah itu kemungkinan resiko-resiko yang sudah di tentukan nilai likelihood dan impact nya akan di masukan kedalam matrix evaluasi resiko disesuaikan dengan pemetaan pada tabel tersebut. Pada tabel. 8 dibawah ini merupakn hasil dari kemungkinan resiko-resiko yang sudah di masukan kedalam tabel matrix evaluasi resiko sesuai dengan kriteria likelihood dan kriteria impact yang sudah ditentukan pada tahap sebelumnya.

Table 8. Matrix Evaluasi Resiko Berdasarkan nilai likelihood dan impact

Likelihood	*Certain*	5					
	Likely	4					
	Possible	3					
	Unlikely	2		R010		R07	R02 R012 R013
	Rare	1	R03 R04 R05 R06 R08	R09 R014	R011		R01
	Impact		1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*

Selanjutnya setelah semua kemungkinan resiko-resiko yang sudah teridentifikasi di masukan kedalam matrix evaluasi resiko yang

disesuaikan dengan nilai likelihood dan impact nya pada table 9 berikut akan dikelompokan dari 14 kemungkinan resiko-resiko yang ada dan di sesuaikan dengan tingkat risk level nya high, medium dan low berdasarkan data yang ada di table 8 sebelumnya.

Table 9. Tabel Ketingkatan risk level berdasarkan masing-masing resiko

ID	Kemungkinan Resiko	Likelihood	Impact	Risk level
R02	Kebakaran	2	5	Medium
R013	Kerusakan Hardware	2	5	Medium
R012	Koneksi Jaringan Gangguan	2	5	Medium
R01	Gempa Bumi	1	5	Medium
R07	Hacking	2	4	Medium
R011	Kerusakan genset kantor	1	3	Low
R010	Server Down	2	2	Low
R09	Trouble Web Server	1	2	Low
R014	Data Corrupt	1	2	Low
R03	Banjir	1	1	Low
R04	Petir	1	1	Low
R05	Penyalagunaan Hak Akses	1	1	Low
R06	Human Error	1	1	Low
R08	Pencurian Data/Perangkat Keras	1	1	Low

Hasil pada proses evaluasi resiko terdapat 14 kemungkinan resiko yang sudah di kelompokkan berdasarkan risk levelnya bisa di lihat pada tabel 9 diatas. Pada hasil yang ada pada tabel tersebut tidak terdapat kemungkinan resiko dengan risk level high. Sedangkan pada tingkat risk level medium terdapat 5 kemungkinan resiko yaitu : R013(kerusakkan hardware), R012(koneksi jaringan gangguan), R02(kebakaran), R01(gempa bumi), R07(hacking). Serta terdapat 9 kemungkinan resiko pada tingkat risk level low 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).

3.2 Perlakuan Resiko(*risk Treatment)*

Setelah melakukan tahapan risk assement yang di delamnya terdapat 3 proses tahapan yaitu risk identification, risk analysis, dan risk evaluation maka selanjutnya akan masuk ke tahapan seleanjutnya yaitu proses risk treatment yang dimana pada tahap ini peneliti memberikan tindakan atau

masukan terhadap kemungkinan resiko-resiko yang sudah di identifikasi dan sudah di kelompokkan berdasarkan risk level pada tabel 9 sebelumnya. Pada tabel 10 di bawah ini merupakan usulan atau tindakkan dari peneliti terhadap resiko-resiko yang ada. Sehingga usulan tersebut dapat digunakan oleh kantor Pengadilan Negeri Salatiga untuk melakukan pencegaan atau setidaknya meminimalisir terhadap kemungkinan resiko yang ada.

Tabel 10. Usulan Perlakuan Terhadap Resiko

ID	Kemungkinan Resiko	*Risk level*	Usulan terhadap resiko
R02	Kebakaran	Medium	Menyediakan alat untuk pemadam api seperti APAR trolley, hydrant dan memasang sprinkler di ruang tertentu yang dianggap vital atau sangat penting bagi kantor.
R013	Kerusakan Hardware	Medium	Harus di adakan pengecekan hardware setiap bulan atau setiap 3 bulan agar kalau ada hardware yang rusak bisa di perbaiki oleh teknisi dan melakukan pencadangan hardware agar kalau ada hardware yang sudah tidak bisa di perbaiki bisa diganti dengan yang baru.
R012	Koneksi Jaringan Gangguan	Medium	Jika jaringan terjadi ganguan laporkan kepada bagian jaringan. Mengganti ISP (*Internet Service Provider)* baru jika ganguan jaringannya parah sekali.
R01	Gempa Bumi	Medium	Menyediakan server cadangan di tempat lain. Atau menyediakan tempat yang cukup aman untuk perangkat-perangkat yang menunjang *SAP* pada kantor tersebut.
R07	Hacking	Medium	Meningkatkan system security pada kantor. Seperti *protect with password* yang dimana semua akses yang menyangkut ke jaringan maupun data harus

			di jaga dengan nama pengguna dan kata sandi yang unik. Ada juga *Design safe system* yang dimana jauhkan akses yang tidak perlu pada hardware maupun software kantor agar mencegah mudahnya peretas pada system.
R011	Kerusakan genset kantor	Low	Segera melakukan pengadakan genset baru yang kualitasnya lebih bagus dari genset sebelumnya dan Menyediakan UPS (*Uninterruptible Power Supply)* pada perangkat-perangkat tertentu yang menunjang *SAP* pada kantor. Alat ini berguna untuk melindungi perangkat dari arus listrik yang tidak stabil seperti listrik padam secara tiba-tiba dan sebaginya.
R010	Server Down	Low	Melakukan pengecekan secara berkala tehadap data base dari aplikasi SIPP atau data base utama kantor.
R09	Trouble Web Server	Low	Melakukan pemberitahuan kepada pegawai atau user kalau web server sedang trouble. Pemberitahuan tersebut bisa berguna buat pegawai atau user agar pegawai bisa mengerjakan pekerjaan yang lain dulu. Serta segera melakukan perbaikan dan pengecekan hal apa yang menyebapkan trouble web server.
R014	Data Corrupt	Low	Melakukan backup data secara berkala dan melakukan pembersihan pada PC menggunakan aplikasi yang *recommended* atau scan mengguakan anti virus pada PC agar mencegah munculnya virus pada PC yang nanti bisa

			menyebapkan data *corrupt* karena virus tersebut. Lakukan hal tersebut secara berkalah.
R03	Banjir	Low	Menyediakan tempat atau ruang untuk perangkat-perangkat penunjang *SAP* yang dianggap vital bagi kantor yang sekiranya aman dari banjir
R04	Petir	Low	Menyediakan alat penangkal petir agar sewaktu-waktu kalau ada petir tidak terjadi hal yang tidak diinginkan terhadap perangkat-perangkat yang mendukung *SAP* pada kantor.
R05	Penyalagunaan Hak Akses	Low	Mengadakan *maintenance password* secara berkala. Memberikan konfirmasi login yag berkaitan dengan pribadi user Memasang CCTV pada ruangan kerja kantor.
R06	Human Error	Low	Melakukan pelatihan atau *training* sebelumnya kepada pegawai atau user terhadap penggunaan aplikasi SIPP agar tidak terjadi kesalahan atau bingung pada saat menggunakannya.
R08	Pencurian Data/Perangkat Keras	Low	Memasang CCTV pada bagian-bagian ruangan yang ada perangkat kerasnya dan kalau bisa melakukan *maintenance password* agar tidak terhadi pencurian data.

4. KESIMPULAN

Analisi manajemen resiko yang menggunakan International Organization Standardization atau ISO 31000 pada aplikasi SIPP di kantor Pengadilan Negeri Salatiga kelas 1B telah dilaksanakan. Analisi manajemen resiko di laksanakan dengan prosedur yag ada pada ISO 31000 yang dimulai dari tahapan risk assessment yang dimana tahap itu ada 3 proses atau langkah yaiu risk identification, risk analysis, dan risk

evaluation. Selanjutnya setelah 3 proses itu sudah di lewati, masuk pada tahap terakhir yaitu risk treatment yang dimana tahap itu peneliti membuat saran atau perlakuan terhadap kemungkinan resiko yang ada pada aplikasi SIPP.

Dari hasil penelitian analisis resiko terdapat 14 kemungkinan resiko yang dapat mengganggu kinerja dari aplikasi SIPP di kantor Pengailan 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(kerusakkan hardware), R012(koneksi jaringan gangguan), R02(kebakaran), R01(gempa bumi), R07(hacking). Serta terdapat 9 kemungkinan resiko pada tingkat risk level low 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). Dengan demikian hasil penelitian ini dapat dipergunakan Pengadilan Negeri Salatiga untuk mengatur Standard Operasional Procedure atau untuk meminimalisir kemungkinan resiko-resiko yang akan terjadi pada SAP kantor kemudian hari.

DAFTAR PUSTAKA

[1] 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://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/4317.

[2] 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.

[3] F. A. Alvian *et al.*, "Manajemen risiko pada laboratorium integrasi universitas islam negeri sunan ampel surabaya menggunakan iso 31000 of sunan ampel surabaya using iso 31000," vol. 12, no. 1, pp. 56–67, 2020.

[4] Wahidmurni, "PEMAPARAN METODE PENELITIAN KUALITATIF Oleh:," *J. Sains dan Seni ITS*, vol. 6, no. 1, pp. 51–66, 2017.

[5] S. Agustinus, A. Nugroho, and A. D. Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 3,

pp. 250–258, 2017, doi: 10.29207/resti.v1i3.94.

[6] 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.

[7] F. Asmin, "Analisis Resiko Implementasi Kegiatan Pengembangan Masyarakat Sekitar Hutan Di Sumatera Barat 194," *J. Sist. (Sistem Informasi)*, vol. 8, pp. 194–203, 2019.