Analisis Manajemen Risiko Teknologi Informasi *Software* PEGA Menggunakan ISO 31000

Joshua Ecleas[*1], Augie David Manuputty[2]

[1,2]Universitas Kristen Satya Wacana; Jl. Diponegoro No. 52-60, Salatiga,
Kec. Sidorejo, Kota Salatiga, Jawa Tengah 50711, (0298) 321212
[3]Program Studi Sistem Informasi, FTI UKSW, Salatiga
e-mail: *[1]682016031@student.uksw.edu , [2]augiemanuputty@gmail.com

Abstrak

PEGA merupakan software yang digunakan oleh PT. Asuransi Sinar Mas untuk mendukung pelayanan dan produktivitas, kegunaan dari PEGA antara lain untuk absensi karyawan, mengecek produktivitas karyawan, untuk menginput polis asuransi, dan melihat data polis. PEGA sangat berpengaruh untuk menunjang proses bisnis dari PT. Asuransi Sinar Mas yang berperan sebagai perusahaan yang memberikan jasa asuransi. Dalam menjalankan proses bisnisnya tentu banyak sekali kemungkinan risiko yang dapat mengancam kelancaran bisnis dari perusahaan itu sendiri, maka dari itu perlu adanya analisa manajemen risiko agar kemungkinan risiko yang akan terjadi dapat diminimalisir atau ditiadakan, agar perusahaan dapat mencapai tujuannya dengan baik. Dalam menganalisis kemungkinan risiko yang ada digunakan pedoman ISO 31000. Tahapan yang dilakukan yaitu Risk Assasement dan Risk Treatment. Hasil dari penelitian ini adalah berbagai kemungkinan risiko pada sistem PEGA yang teridentifikasi menggunakan matriks kemungkinan dan dampak. Penelitian ini diharapkan dapat dimanfaatkan oleh perusahaan untuk melakukan tindakan pencegahan risiko yang mungkin terjadi.

Kata kunci—Risiko, ISO 31000, PEGA, Manajemen risiko

Abstract

PEGA is a software that is used by PT. Asuransi Sinar Mas to support the service and and productivitsy of the company. PEGA has a number of uses, such as to record employee's absence, check the productivy of the employees, add new insurance policy, and read said policy. PEGA is influencial to support the business processes of PT. Asuransi Sinar Mas, an insurance company. While running said business processes, there is a lot of risk that threatens the flow of business the company has. Thus a risk management analysis is needed to lessen the chance of said risk to occur, so the company's business flow remains uninterrupted. The ISO 31000 risk management guidelines can be used to analyze those risk. Then, a risk assessment and treatment is needed to identify the risk and the solution to such risk. The results of this study are the various possible risks to the pega system identified using the likelihood and impact matrix. This research is expected to be used by companies to carry out risk prevention measures that may occur.

Keywords—*Risk, ISO 31000, PEGA, Risk Management*

1. PENDAHULUAN

PT. Asuransi Sinar Mas didirikan pada tahun 1985 merupakan Perusahaan asuransi umum yang menjadi market leader di industry asuransi di Indonesia. PT. Asuransi Sinar Mas saat ini memiliki 190 jaringan kantor cabang/pemasaran/*marketing point*, yang terdiri dari 34 kantor cabang, 76 kantor pemasaran, dan 80 kantor marketing point yang memiliki tujuan untuk mendukung layanan dan pengembangan bisnis dari perusahaan. PT. Asuransi Sinar Mas menyediakan berbagai produk asuransi umum dan layanan yang inovatif yang sesuai dengan kebutuhan dari nasabah [1].

Dalam menjalankan bisnisnya PT. Asuransi Sinar Mas menggunakan *software* PEGA. PEGA merupakan *software* yang difungsikan untuk mendukung pelayanan, dan produktivitas, serta inovasi dari PT. Asuransi Sinar Mas. *Software* PEGA digunakan untuk penerbitan polis, pendataan karyawan, pelaporan klaim, pelaporan kepada marketing. *Software* PEGA berperan penting bagi Perusahaan dalam menjalankan bisnisnya sebagai lembaga yang memberikan pelayanan di bidang asuransi.

Kebutuhan Perusahaan akan sistem informasi dan teknologi informasi menjadi aset yang sangat penting, dan berpengaruh untuk menunjang kemajuan dari suatu Perusahaan tersebut. Hal tersebut dapat dilihat dari pemanfaatan sistem informasi dan teknologi informasi yang digunakan untuk menjalankan berbagai aktivitas di dalam perusahaan atau instansi pemerintahan. Saat ini dalam menjalankan proses bisnisnya sebuah Perusahaan sangat bergantung pada sistem informasi dan teknologi informasi guna tercapainya tujuan dari Perusahaan, di sisi lain hal tersebut juga dapat memberikan berbagai manfaat dalam pelayanan untuk kebutuhan konsumen. Oleh sebab itu pemanfaatan teknologi informasi dan sistem informasi memegang peranan penting dalam menunjang bisnis dari berbagai perusahaan. Agar bisnis dari suatu perusahaan tetap berjalan dengan optimal maka hal yang menyangkut dengan teknologi informasi dan sistem informasi menjadi perhatian yang sangat penting. Maka dari itu untuk memulai sebuah bisnis diperlukan sebuah perencanaan yang matang agar visi dan misi dari sebuah Perusahaan tersebut dapat tercapai dengan baik dan maksimal.

Aspek keamanan menjadi hal yang sangat penting dalam sistem informasi. Hal ini merupakan suatu aset yang sangat penting yang harus diperhatikan dan dilindungi dengan baik, agar menjamin kelancaran bisnis dari Perusahaan. Saat ini semakin pesatnya perkembagan akan teknologi serta mudahnya penggunaan akan teknolgi akan menimbulkan adanya peluang akan risiko terhadap informasi, yang mana hal ini akan berpengaruh bagi kelancaran bisnis dari perusahaan. Jika dalam menjalankan bisnisnya sebuah Perusahaan tidak menjaga dengan baik dari segi keamanannya maka akan menimbulkan berbagai masalah yang dapat berpengaruh dalam proses bisnis Perusahaan tersebut. Disisi lain pengunaan teknologi informasi juga dapat menimbulkan dampak negatif bagi perusahaan, hal inilah yang dinamakan dengan risiko.

Risiko adalah kemungkinan terjadinya suatu peristiwa yang dapat mengakibatkan suatu kerugian bagi perusahaan. Tugiman (2009), mendefenisikan risiko sebagai kejadian yang merugikan atau tidak tercapainya tujuan yang diharapkan [2]. Risiko berhubungan dengan ketidakpastian. Ketidakpasitian ini terjadi karena kurangnya atau tidak tersedianya informasi yang menyangkut apa yang akan terjadi. Di dalam suatu Perusahaan ketidakpastian yang merugikan disebut dengan risiko.

Dalam mengidentifikasikan manajemen risiko pedoman yang dipakai adalah ISO 31000. ISO 31000 merupakan standar yang berkaitan dengan manajemen risiko yang diterbitkan pada tanggal 13 November 2009 oleh *International Organization for Standardization (ISO)* [3].

2. TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Analisis risiko teknologi informasi menggunakan ISO 31000 pada sistem *I-Gracias Telkom University* yang dilakukan oleh Andi Novia Rilyani, Yanuar Firdaus A W., ST., MT, dan Dawam Dwi Jatmiko ST., MT yang dilakukan pada tahun 2015 bertujuan untuk melakukan tahapan dan proses analisis risiko teknologi informasi berberbasis *risk management* sesuai dengan standar dan kerangka kerja ISO 31000 dan mengetahui tingkat risiko teknologi informasi pada *I-Gracias*, hasil dari penelitian tersebut ditemukan berbagai dampak dari risiko yang mungkin terjadi pada sistem *I-Gracias* jika tidak dilakukan penanganan, serta diketahui juga bahwa sistem tersebut membutuhkan komponen pendukung agar dapat berjalan dengan baik [4].

Pada tahun 2017 penelitian dengan menggunakan ISO 31000 juga dilakukan oleh Zainal Putra, Syafruddin Chan, dan Moenawar IHA, penelitian tersebut dilakukan pada PDAM Tirta Meulaboh, dari penelitian yang dilakukan tersebut diperoleh hasil bahwa terdapat potensi risiko yang jika tidak ditangani dengan segera dapat mempengaruhi kinerja dari perusahaan bahkan kelangsungan dari Perusahaan tersebut [2].

Analisis menggunakan *International Organiation for Standardization (ISO) 31000* pada tahun 2018 dilakukan oleh Tri Ramdhany dan Rio Andriyat Krisdiawan di PT. Remaja Rosdakarya, dengan tujuan untuk melakukan tahapan dan proses analisis risiko pada sistem informasi penjualan dan untuk mengetahui tingkat risiko sistem informasi penjualan serta perlakuan risiko yang diberikan [5].

2.2 Dasar Teori

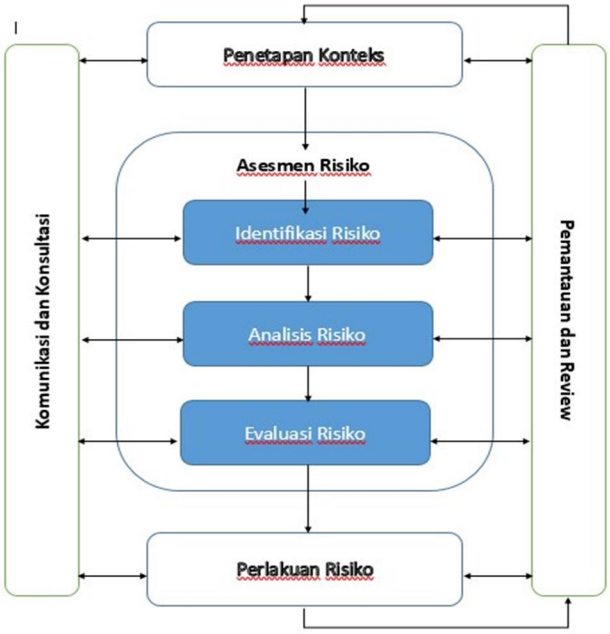
The International Organization for Standardization (ISO) 31000: 2009

The International Organization for Standardization (ISO) 31000: 2009 Risk Management – Principles and Guidelines merupakan suatu standar internasional yang dibuat dengan tujuan untuk digunakan sebagai prinsip dan pedoman menajemen risiko [5]. ISO 31000 memberikan prinsip, kerangka kerja, dan manajemen risiko yang dapat digunakan oleh berbagai Perusahaan dalam menganalisa suatu risiko yang ada. Dalam melakukan penelitian metode untuk mencari data dan informasi adalah dengan melakukan wawancara pada narasumber dari PT. Asuransi Sinar Mas, kemudian data yang sudah ada diolah dan nantinya dilakukan analisa sesuai dengan kerangka kerja ISO 31000. Pada tahapan pertama untuk menganalisa dilakukan dengan penilaian risiko (*risk assasement*). Di dalam proses penilaian risiko terbagi menjadi 3 tahapan yang dilakukan untuk menilai suatu risiko yaitu tahap identifikasi risiko (*risk identification*), analisa risiko (*risk analys*), kemudian tahap evaluasi risiko (*risk evaluation*). Pada tahap

penilaian risiko dilakukan penentuan kriteria kriteria risiko yang mungkin terjadi dan yang akan mempengaruhi kinerja dari suatu Perusahaan dalam usahanya dalam mencapai sebuah tujuan, kemudian pada tahap kedua dari manajemen risiko adalah perlakuan risiko (*risk treatment*), pada tahap ini peneliti melakukan seleksi dari kemungkinan risiko, mengurani dan menghilangkan dampak dari risiko yang mungkin terjadi pada suatu Perusahaan [6].

3. METODOLOGI PENELITIAN

3.1 Manajemen Risiko



Gambar 1. Proses Manajemen Risiko

Manajemen risiko adalah sebuah proses yang dilakukan untuk mengidentifikasi, mengukur risiko, dan membuat strategi yang digunakan untuk mengelola risiko yang belum terjadi pada suatu perusahaan [7]. SBC Warburg (dalam Tugiman, 2009) mengatakan manajemen risiko adalah seperangkat kebijakan, prosedur yang lengkap, yang dipunyai organisasi untuk mengelola, memonitor dan mengendalikan eksposur organisasi terhadap risiko [2]. Dengan menerapkan manajemen risiko dalam perusahaan, maka pemilik perusahaan dapat dengan mudah mengatur prosedur di dalam perusahaan untuk meminimalisir risiko yang akan terjadi, serta dapat mengatasi kendalam dalam perusahaan tersebut.

Metode kualitatif dilakukan dengan cara mengidentifikasi suatu risiko guna mengetahui potensi risiko yang ada di sistem PEGA [8]. Pada penelitian kali ini metode yang digunakan adalah dengan pendekatan kualitatif karena metode ini memiliki tujuan untuk mengeksplorasi dan memahami makna yang bersumber dari masalah sosial atau kemanusiaan. Pada proses penelitian kualitatif hal yang dilakukan adalah seperti mengajukan pertanyaan kepada narasumber, mengumpulkan data yang spesifik dari

lapangan dan narasumber, kemudian melakukan analisa terhadap data yang telah didapat secara induktif [9]. Penelitian dilakukan dengan melakukan wawancara dengan *staff IT* PEGA pada bagian penerbitan polis yang melakukan perancangan dan memprogram sistem PEGA dari Perusahaan Asuransi Sinar Mas, wawancara dilakukan dengan menanyakan fungsi dari sistem PEGA, data apa saja yang ada dalam sistem PEGA, kemungkinan risiko apa saja yang dapat terjadi dalam sistem PEGA, kemudian data yang dibutuhkan berfokus pada sistem PEGA yang digunakan pada perusahaan untuk menjalankan bisnisnya.

4. HASIL DAN PEMBAHASAN

4.1 Tahap Risk Assesment (Penilaian Risiko)

Pada tahap risk assessment dilakukan 3 tahapan untuk menganalisis sesuai dengan pedoman manajemen risiko ISO 31000, tahapan analisis tersebut yaitu tahap identifikasi risiko (*risk identification*), analisis risiko (*risk identification*), dan evaluasi risiko (*risk evaluation*)

4.1.1 Tahap Risk Identification (Identifikasi Risiko)

Identifikasi Asset PEGA

Tahap identifikasi terhadap asset yang digunakan pada Perusahaan, dilakukan melalui proses wawancara dengan *staff IT* terkait yang menangani bagian tersebut untuk menentukan risiko dan kemungkinan ancaman yang muncul pada sistem PEGA.

"*Data yang ada di aplikasi PEGA itu ada data polis yaitu data polis yaitu keseluruan data polis asuransi yang ada di Perusahaan, data karyawan yang berisi data diri karyawan yang bekerja di Perusahaan, kemudian ada data sumber bisnis dan data nasabah Mas" (IT PEGA)*

"Untuk hardwarenya yang ada di Perusahaan, di sini yang jelas semua sudah menggunakan PC mas, karena untuk kerja karyawan sebagian besar kan sudah by sistem, maka dari itu dari Kantor memberikan fasilitas tersebut, lalu ada server database untuk menyimpan data-data, terus ada server web service juga mas" (IT PEGA)

Tabel 1 Identifikasi Aset PEGA

Komponen sistem informasi	Aset PEGA
Data	Data polis, data karyawan, data sumber bisnis, data nasabah
Software	Sistem PEGA
Hardware	*Server database, personal computer, server web service*

Identifikasi Kemungkinan Risiko

Setelah dilakukan indentifikasi aset yang ada pada perusahaan, diperoleh hasil berupa data, *software*, dan *hardware*, langkah selanjutnya adalah mengidentifikasi

kemungkinan risiko yang berada di sekitar dari aset yang berhubungan dengan sistem PEGA. Kemungkinan risiko tersebut dapat dilihat dari macam macam faktor yang dapat mengancam sistem PEGA, Proses dilakukan dengan melakukan observasi dan wawancara dengan *staff IT* terkait, kemungkinan risiko tersebut dapat kita kategorikan pada tabel 2 berikut.

"*Risiko yang bisa terjadi pada sistem dan infrastruktur banyak mas, diantaranya ada server down, listrik padam tapi ini jarang terjadi mas, lalu virus yang bisa menyerang sistem meskipun ada anti virus tapi kemungkinan terserang kan ada, terputusnya koneksi jaringan bisa karena listrik padam tadi atau masalah di internet, terus server error mas, nah biasanya kalau error kita dari staff IT ada quality control untuk meminimalisir kemungkinan error yang ada di sistemnya, kemudian kalau ada kerusakan hardware biasanya kita bilang ke IT support untuk dilakukan perbaikan hardware, tapi untuk kerusakan hardware itu jarang terjadi karena biasanya kita dari IT juga melakukan cek kalau bisa jangan sampai ada kerusakan soalnya sebagian besar kerjaan kita lakukan dari PC masing masing, jadi kalau ada kerusakan bisa menghambat pekerjaan juga mas. Terus kalo faktor lainnya paling bug system, error waktu inputor melakukan input data polis di sistem, terus kinerja sistem yang lambat biasanya, tapi masalah ini biasanya dari user langsung info ke IT jadi dari bagian IT langsung melakukan perbaikan, biasanya juga dari IT langsung melakukan remote ke PC user yang bermasalah jadi bisa lebih cepat penanganannya. Kalau dari faktor sistem dan infrakstruktur paling itu mas, kalau dari User biasanya itu paling dia kurang memahami sistemnya aja, lalu faktor lainnya paling salah input data, nah kalau dari user sendiri untuk mengatasinya paling dari kita ada training sebelumnya, mereka dijelaskan langkah langkahnya terlebih dulu, dan biasanya kalau dari user ada yang kurang paham bisa langsung menanyakan langsung ke koordinator divisinya atau bisa email ke bagian IT kalau memang ada kendala di sistemnya. Kalau untuk risiko karena bencana alam yang mengganggu jalannya proses bisnis jarang sekali terjadi mas selama saya kerja disini, kebetulan kantor kita juga gak pernah kebanjiran, kalau kebakaran juga sampai sekarang tidak pernah, semisal terjadi di kantor kan ada alat pemadam kebakaran jadi api bisa cepat dipadamkan, untuk bencana lainnya juga jarang mas." (IT PEGA)*

Tabel 2. Identifikasi Kemungkinan Risiko

Sumber Risiko	Kode Risiko	Kemungkinan Risiko
Faktor Lingkungan / Alam	R1	Banjir
	R2	Kebakaran
	R3	Badai
	R4	Gempa bumi
	R5	Petir
Faktor Sistem dan Infrastruktur	R6	*Server down*
	R7	Serangan virus
	R8	Listrik padam
	R9	Terputusnya koneksi jaringan
	R10	*Server error*
	R11	*Bug* pada sistem
	R12	Kerusakan pada *hardware*
	R13	*Error* saat *input* data di sistem
	R14	Kinerja sistem yang lambat
	R15	Sistem *log out* secara otomatis
Faktor Manusia	R16	Kurangnya pengetahuan tentang penggunaan aplikasi
	R17	Kesalahan *input* data pada sistem
	R18	Kurang memahami alur kerja sistem
	R19	*Double input* data di sistem

Identifikasi Dampak Risiko

Tahap identifikasi dampak risiko di dapat setelah kita menganalisis kemungkinan risiko apa saja yang mungkin terjadi pada sistem PEGA, pada tahap sebelumnya ditemukan 19 kemungkinan risiko yang mungkin terjadi pada sistem PEGA, kemungkinan tersebut dapat timbul dari faktor lingkungan / alam, faktor sistem dan infrastruktur, dan faktor manusia. Pada proses ini kita menganalisis dampak apa saja yang ditimbulkan jika kemungkinan risiko yang sudah dianalisis sebelumnya terjadi pada sistem PEGA. Berikut adalah detail identifikasi dampak risiko yang ditimbulkan pada sistem

Tabel 3. Identifikasi Dampak Risiko

Kode Risiko	Kemungkinan Risiko	Dampak Risiko
R1	Banjir	Aktivitas bisnis terhambat, rusaknya infrastruktur perusahaan
R2	Kebakaran	Aktivitas bisnis Perusahaan terhenti dan rusaknya infrastruktur perusahaan

R3	Badai	Kerusakan infrastruktur Perusahaan
R4	Gempa Bumi	Kerusakan infrastruktur Perusahaan dan aktivitas bisnis terhambat
R5	Petir	Kerusakan infrastruktur Perusahaan, koneksi jaringan terputus
R6	*Server Down*	Menghambat aktivitas pekerjaan dan tidak dapat mengakses sistem PEGA
R7	Serangan Virus	Mengakibatkan *data corrupt* atau adanya *bug* di sistem PEGA
R8	Listrik Padam	Aktivitas kantor terhenti sementara, namun tidak begitu mempengaruhi kinerja bisnis dikarenakan ada *Generator set*
R9	Terputusnya koneksi Jaringan	Aktivitas bisnis terganggu dan menghambat kinerja bisnis dari Perusahaan
R10	*Server Error*	Tidak dapat mengakses *database*
R11	*Bug* pada sistem	Menimbulkan *error* pada kinerja sistem, menyebabkan *crash* pada sistem
R12	Kerusakan pada *hardware*	Kinerja bisnis menjadi terganggu, mengakibatkan kerugian dari segi finansial
R13	*Error* saat *input* data di sistem	Target tidak terpenuhi, menghambat kinerja bisnis dari perusahaan
R14	Kinerja sistem yang lambat	Memperlambat kinerja bisnis, target tidak terpenuhi
R15	Sistem *Log out* secara otomatis	Menginput ulang data yang tidak tersimpan, memperlambat alur kerja bisnis dari Perusahaan
R16	Kurangnya pengetahuan tentang penggunaan aplikasi	Kinerja menjadi tidak maksimal, pencapaian target Perusahaan menjadi tidak terpenuhi
R17	Kesalahan *input* data pada sistem	Data yang diinput menjadi tidak *valid*
R18	Kurang memahami alur kerja sistem	Kinerja bisnis menjadi tidak maksimal
R19	*Double input* data di sistem	Inputan menjadi tidak *valid*, sia sia dalam menginput data

4.1.2 Tahap Risk Analys (Analisis Risiko)

Tahap berikutnya adalah Tahap Analisis Risiko, tahap ini dilakukan untuk pengambilan keputusan tentang perlakuan risiko terhadap suatu risiko tersebut. Setelah menyelesaikan tahap identifikasi risiko pada sistem PEGA dan didapatkan beberapa kemungkinan risiko yang ada. Pada tahap ini dilakukan penilaian terhadap berbagai risiko yang muncul pada sistem PEGA penentuan nilai dilakukan dengan menggunakan kemungkinan terjadinya suatu risiko (*likelihood*) dan dampak dari suatu risiko (*impact*)[10].

Tabel 4. Kriteria Kemungkinan (*Likelihood*)

Kriteria	Deskripsi	Frekuensi kejadian	*Level* / Nilai
Rare	Suatu risiko yang hampir tidak pernah terjadi	>3 tahun	1
Unlikely	Suatu risiko yang jarang terjadi	1 - 2 tahun	2
Possible	Suatu risiko yang kadang terjadi	9 - 12 bulan	3
Likely	Suatu risiko yang sering terjadi	5 – 8 bulan	4
Certain	Suatu risiko yang pasti terjadi	1- 4 bulan	5

Tabel 5. Dampak Risiko (*Impact*)

Kriteria	Deskripsi	*Level* / Nilai
Insignificant	Risiko yang dampaknya tidak mengganggu proses bisnis dan jalannya aktivitas dari Perusahaan	1
Minor	Risiko yang dampaknya sedikit menghambat proses bisnis dan aktivitas perusahaan	2
Moderate	Risiko yang dampaknya menghambat sebagian jalannya bisnis dan aktivitas perusahaan	3
Major	Risiko yang menghambat seluruh proses bisnis dan aktivitas perusahaan	4
Catastrophic	Risiko yang dampaknya dapat menghentikan proses bisnis dan aktivitas perusahaan secara total	5

Setelah menentukan nilai dari kemungkinan terjadinya suatu risiko (*likelihood*) dan dampak dari suatu risiko (*impact*), langkah selanjutnya adalah menentukan penilaian terhadap kemungkinan risiko yang mempengaruhi sistem PEGA yang sebelumnya sudah diidentifikasi. Proses ini dilakukan dengan observasi dan wawancara degan *staff IT* terkait. Detail dari penilaian kemungkinan risiko dapat dilihat pada tabel 6 berikut.

"*Jika dilihat dari frekuensi kejadian risikonya, kalau dari faktor bencana alamnya disini termasuknya jarang terjadi mas, selama saya disini sih belum pernah kejadian kalau kebakaran, kalau banjir juga belum pernah, kalau gempa ada tapi gak yang sampai menimbulkan kerusakan sih mas, nah kalau yang termasuk lumayan sering itu paling dari usernya mas misalnya salah input data di sistem biasanya karna usernya kurang teliti sih mas, terus kayak double input data juga bisa mas itu kembali lagi ke usernya sih mas, kalau dari sistemnya sendiri sering ada info juga dari usernya mas kalau ada error atau kendala, tapi masalah itu biasanya dari IT langsung follow up untuk memperbaiki errornya mas, jadi errornya bisa cepat diperbaiki, kalau bug di sistem gitu disini kadang ada sih mas, biasanya pas ada upgrade versi gitu mas, kalau dari IT PEGAnya sendiri kita rutin melakukan maintenance mas terus kita juga rutin untuk pengecekan sistem PEGAnya. Kalau dari kerusakan hardware hampir tidak pernah sih mas, misalkan ada biasanya dari IT support langsung bisa menangani, dari user tinggal lapor aja kalau ada kerusakan. Terus kalau masalah sistemnya lambat dalam memproses itu biasanya karna faktor datanya yang besar dan banyak itu bisa jadi penyebabnya, atau juga karena jaringan internetnya yang lagi jelek mas, kalo menurut saya itu bisa masuk ke kategori sering sih mas" (IT PEGA)*

Tabel 6. Penilaian Kemungkinan Risiko Menggunakan *Likelihood* dan *Impact*

Kemungkinan Risiko	Kode Risiko	*Likelihood*	*Impact*
Banjir	R1	1	3
Kebakaran	R2	1	5
Badai	R3	1	2
Gempa Bumi	R4	2	5
Petir	R5	2	1
Server Down	R6	1	5
Serangan Virus	R7	1	1
Listrik Padam	R8	3	2
Terputusnya koneksi Jaringan	R9	2	3
Sistem *Error*	R10	4	3
Bug pada sistem	R11	3	2
Kerusakan pada *hardware*	R12	1	3
Error saat *input* data di sistem	R13	5	2
Kinerja sistem yang lambat	R14	4	2

Sistem *Log out* secara otomatis	R15	3	1
Kurangnya pengetahuan tentang penggunaan aplikasi	R16	4	1
Kesalahan *input* data pada sistem	R17	5	1
Kurang memahami alur kerja sistem	R18	3	1
Double input data di sistem	R19	3	1

4.1.3 Tahap Risk Evaluation (Evaluasi Risiko)

Kemungkinan Risiko yang telah diidentifikasi dan di analisis kemudian dimasukan dalam sebuah matrik evaluasi risiko yang ditentukan berdasarkan *likelihood* (kemungkinan) dan *impact* (dampak), Matrik risiko tersebut didapatkan dari parameter evaluasi risiko yang sudah ditentukan sebelumnya. Matrik risiko tersebut dapat dilihat pada tabel 7

Tabel 7. Matrik Evaluasi Risiko Berdasarkan Kemungkinan (*Likelihood*) dan Dampak (*Impact*)

Likelihood						
	Certain (5)	R17	R13			
	Likely (4)	R16	R14			
	Possible (3)	R15 R18 R19	R8 R11	R10		
	Unlikely (2)	R5		R9		R4
	Rare (1)	R7	R3	R1 R12		R2 R6
		Insignificant (1)	*Minor (2)*	*Moderate (3)*	*Major (4)*	*Catastrophic (5)*
	Impact					

Berdasarkan pengamatan terhadap kemungkinan kemungkinan risiko yang terjadi yang dievaluasi menggunakan matrik yang berdasar pada *likelihood* (kemungkinan) dan *impact* (dampak), selanjutnya risiko tersebut disusun berdasarkan *level* risikonya dari yang tertinggi (*high*) sampai yang terendah (*low*).

Tabel 8. Evaluasi *Level* Kemungkinan Risiko berdasarkan *Likelihood* dan *Impact*

Kode Risiko	Kemungkinan Risiko	*Likelihood*	*Impact*	*Level* Risiko
R1	Banjir	1	3	Low
R2	Kebakaran	1	5	Medium
R3	Badai	1	2	Low
R4	Gempa Bumi	2	5	Medium

R5	Petir	2	1	Low
R6	*Server Down*	4	3	Medium
R7	Serangan Virus	1	1	Low
R8	Listrik Padam	3	2	Medium
R9	Terputusnya koneksi Jaringan	2	3	Medium
R10	Sistem *Error*	3	3	Medium
R11	*Bug* pada sistem	3	1	Medium
R12	Kerusakan pada *hardware*	1	2	Low
R13	*Error* saat *input* data di sistem	5	2	Medium
R14	Kinerja sistem yang lambat	4	2	Medium
R15	Sistem *log out* secara otomatis	3	1	Low
R16	Kurangnya pengetahuan tentang penggunaan aplikasi	4	1	Medium
R17	Kesalahan *input* data pada sistem	5	1	Medium
R18	Kurang memahami alur kerja sistem	3	1	Low
R19	*Double input* data di sistem	3	1	Low

Dari tabel evaluasi *level* kemungkinan risiko berdasarkan *likelihood* dan *impact*, 19 kemungkinan risiko yang sudah diidentifikasi sebelumnya, diketahui ada 11 risiko yang dikategorikan masuk dalam *level* risiko *medium* yaitu: kebakaran, gempa bumi, *server down*, listrik padam, terputusnya koneksi jaringan, sistem *error*, *bug* pada sistem, *error* saat *input* data di sistem, kinerja sistem yang lambat, kurangnya pengetahuan tentang penggunaan aplikasi, kesalahan *input* data pada sistem, dan diketahui ada 8 risiko yang dikategorikan dalam level risiko *low* yaitu : banjir, badai, petir, serangan virus, kerusakan pada *hardware*, sistem *log out* secara otomatis, kurang memahami alur kerja sistem, *double input* data di sistem.

4.2 Risk Treatment (Perlakuan Risiko)

Perlakuan Risiko merupakan upaya untuk mengurangi atau menghilangkan dampak dari kemungkinan risiko yang akan terjadi, yang dimana pada tahap ini akan diberikan usulan yang dapat digunakan dan diterapkan guna meminimalisir kemungkinan risiko yang akan terjadi, sehingga dapat bermanfaat untuk kelancaran proses bisnis dari Perusahaan, *risk treatment* disusun berdasarkan *level* risiko yang sudah diidentifikasi sebelumnya, dari *level* risiko yang tinggi (*high*) ke *level* risiko yang rendah (*low*), detail usulan tersebut dapat dilihat pada tabel 9 berikut.

Tabel 9. *Risk Treatment* (Perlakuan Risiko)

Kode Risiko	Kemungkinan Risiko	*Level* Risiko	Perlakuan Risiko
R2	Kebakaran	Medium	Meletakkan *server* di tempat yang lebih aman, menyediakan APAR di titik sekitar *server*
R4	Gempa Bumi	Medium	Menyediakan *server* cadangan di tempat / lokasi lain yang lebih aman.
R6	*Server Down*	Medium	Melakukan pengecekan secara berkala pada sistem dalam satu hari, adanya *backup plan* (penerbitan polis secara *offline*, kemudian akan ter*upload* otomatis jika sudah kembali *online*)
R8	Listrik Padam	Medium	Memasang *Uninterrupitible Power Supply* (UPS) dan *Generator Set* dengan daya yang sesuai dengan kebutuhan perusahaan.
R9	Terputusnya Koneksi Jaringan	Medium	Melaporkan kepada bagian *IT* jaringan jika koneksi jaringan terputus.
R10	Sistem *Error*	Medium	Melakukan *Maintenance* berkala pada sistem dan pengecekan pada *database* yang digunakan
R11	*Bug* pada sistem	Medium	Melakukan cek pada sistem, melakukan pengujian sistem secara berkala, ada *Staff IT* bagian *customer service* yang menangani masalah *bug* di sistem
R13	*Error* saat *input* data di sistem	Medium	Melakukan *refresh* pada sistem jika terjadi *error* pada saat menginput
R14	Kinerja sistem yang lambat	Medium	Melakukan *refresh* pada sistem, melakukan pengecekan pada sistem secara rutin
R16	Kurangnya pengetahuan tentang penggunaan aplikasi	Medium	Melakukan sosialisasi tentang cara menggunakan aplikasi, mengadakan *training* mengenai penggunaan aplikasi

R17	Kesalahan *input* data pada sistem	Medium	Melakukan perbaikan kesalahan, menyediakan fitur edit data pada sistem, melakukan pengecekan sebelum dijalankan
R1	Banjir	Low	Menaruh *server* di tempat yang sulit dijangkau oleh banjir (di tempat yang lebih tinggi), Memiliki cadangan *server* di tempat yang berbeda
R3	Badai	Low	Meletakkan *server* di tempat yang aman di dalam gedung. Memberikan pelindung pada *server*
R5	Petir	Low	Memasang alat penangkal petir, Melakukan pencadangan pada *server* utama secara otomatis ke dalam *server* cadangan
R7	Serangan Virus	Low	Memasang antivirus yang bagus dan terpercaya, membatasi akses agar tidak sembarang orang dapat mengakses *Database* dan *Server* Utama
R12	Kerusakan pada *Hardware*	Low	Melaporkan pada *IT* terkait yang menangani kerusakan *Hardware*, Melakukan perawatan pada *Hardware*
R15	Sistem *Log out* secara otomatis	Low	Melakukan perbaikan dan melakukan tes kinerja sistem
R18	Kurang memahami alur kerja sistem	Low	Mempelajari alur kerja dan kegunaan sistem, mengadakan *training* mengenai penggunaan sistem
R19	Double *input* data di sistem	Low	Melakukan *dump* pada salah satu data yang *double* agar tidak menyebabkan *error* atau *bug* di sistem

5. KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan yang berdasar pada ISO 31000 pada sistem PEGA di PT. Asuransi Sinar Mas yang dilakukan menggunakan tahapan yang terdiri dari tahap identifikasi risiko (*risk identification*), analisis risiko (*risk analys*) dan evalusasi risiko (*risk evaluation*) serta tahap perlakuan risiko, maka dari penelitian

tersebut di dapatkan 19 kemungkinan risiko yang ada di sekitar asset yang terkait dengan sistem PEGA yang ada di PT. Asuransi Sinar Mas. Hasil tersebut kemudian dikelompokan menjadi 2 kategori *level* yang diidentifikasikan menggunakan matrik kemungkinan (*likelihood*) dan dampak (*impact*). Dari matrik tersebut didapatkan hasil kemungkinan risiko yang dikategorikan memiliki *level* risiko *medium* yaitu: kebakaran, gempa bumi, *server down*, listrik padam, terputusnya koneksi jaringan, sistem *error*, *bug* pada sistem, *error* saat *input* data di sistem, kinerja sistem yang lambat, kurangnya pengetahuan tentang penggunaan aplikasi, kesalahan *input* data pada sistem, dan diketahui ada risiko yang dikategorikan dalam level risiko *low* yaitu : banjir, badai, petir, serangan virus, kerusakan pada *hardware*, sistem *log out* secara otomatis, kurang memahami alur kerja sistem, *double input* data di sistem.

Dari hasil yang didapat dapat dilihat bahwa dalam mengatasi kemungkinan risiko yang ada Perusahaan sudah menerapkan langkah untuk meminimalisir dampak dari kemungkinan risiko yang mungkin terjadi, namun untuk masalah sistem *error* dari pihak Perusahaan dapat lebih memantau dan melakukan *maintenance* secara berkala pada sistem agar masalah sistem *error* dapat di minimalisir dan proses bisnis dapat berjalan dengan baik.

DAFTAR PUSTAKA

[1] ____, 2012, *Sejarah PT. Asuransi Sinar Mas,* https://www.sinarmas.co.id/tentang-kami/sejarah-asm.

[2] Z. Putra, S. Chan, and M. IHA. 2018, *Desain Manajemen Risiko Berbasis ISO 31000 pada PDAM Tirta Meulaboh*, *E-Kombis*, Vol. 3, No. 1, pp. 52 – 71.

[3] G. W. Lantang, A. D. Cahyono, and N. Ngalumsine, 2019, *Analisis Risiko Teknologi Informasi pada Aplikasi SAP di PT Serasi Autoraya Menggunakan ISO 31000, Sebatik 2621-069X*, Vol. 23 No. 1, pp. 36–43.

[4] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko. 2015, *Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based on Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)*, *e-Proceeding Eng.*, Vol. 2, No. 2, pp. 6201–6208.

[5] T. Ramdhany and R. A. Krisdiawan. 2018, *Analisis Risiko Sistem Informasi Penjualan Berbasis Iso 31000 - Risk Management di PT. Remaja Rosdakarya, Teknol. dan Manaj. Inform.*, Vol. 3, No. 1, pp. 1–7,

[6] 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.

[7] G. Soputan, B. Sompie, and R. Mandagi. 2014, *Manajemen Risiko Kesehatan dan Keselamatan Kerja (K3) (Study Kasus pada Pembangunan Gedung SMA Eben Haezar), J. Ilm. Media Eng.*, Vol. 4, No. 4, p. 99095.

[8] S. D. Fitri, D. L. Setyowati, and K. Duma. 2019, *Implementasi Manajemen Risiko Berdasarkan ISO 31000 : 2009 pada Program Perawatan Mesin di Area Workshop PT . X*, Vol. 6, No. 1, pp. 16–24.

[9] Z. Munawwaroh. 2017, *Analisis Manajemen Risiko pada Pelaksanaan Program Pendidikan Dalam Upaya Meningkatkan Mutu Pendidikan, J. Adm. Pendidik.*, Vol. 24, No. 2, pp. 71–79.

[10] F. L. Nice and R. V. Imbar. 2017, *Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000, J. Inform. dan Sist. Inf.*, Vol. 2, No. 2, pp. 1–11.