Indonesian Journal of Computer Science
ISSN 2302-4364 (*print*) dan 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam, No. 1, Padang, Indonesia, Telp. (0751) 7056199, 7058325
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Analisis Manajemen Risiko Pada Teknologi Informasi PT. Pos Indonesia Menggunakan ISO 31000

Hani Alifia Mattjik[1], Dwi Rosa Indah[2], Putri Eka Sevtiyuni[3]
09031282025054@student.unsri.ac.id, indah812@unsri.ac.id, putrieka@unsri.ac.id
Universitas Sriwijaya

Informasi Artikel

Diterima : 6 Nov 2023
Direview : 19 Nov 2023
Disetujui : 20 Des 2023

Kata Kunci

Manajemen Risiko, ISO 31000, PT. Pos Indonesia, Teknologi Informasi, Aset Teknologi

Abstrak

Sebagai badan usaha yang beroperasi di bidang kurir pengiriman, logistik, dan transaksi uang, PT. Pos Indonesia tidak dapat terlepas dari penggunaan teknologi informasi sebagai aset pendukung proses bisnis. Fokus pada penelitian ini adalah PT. Pos Indonesia Palembang 30000, yang merupakan cabang utama dari PT. Pos Indonesia yang ada di kota Palembang. Selama penggunaan teknologi informasi, terdapat beberapa permasalahan dan risiko yang kerap muncul seperti terjadi kerusakan hardware, kegagalan dalam *update* dan *backup* data sehingga menyebabkan kehilangan data, kegagalan sistem yang disebabkan oleh gangguan infrastruktur jaringan sehingga sistem tidak dapat diakses oleh karyawan. Saat ini, PT. Pos Indonesia belum melakukan analisis dan evaluasi risiko yang diterapkan secara khusus terhadap teknologi informasi sehingga hal ini dapat menjadi risiko yang menyebabkan kegagalan dalam menjalankan aktivitas bisnis. Penelitian ini menggunakan ISO 31000 sebagai panduan analisis manajemen risiko. Hasil dari penelitian ini berupa dokumentasi risiko yang mana dari 31 identifikasi risiko terdapat 2 risiko tingkatan high, 26 risiko tingkatan medium, dan 3 risiko tingkatan low. Identifikasi dari 31 risiko tersebut akan diberikan saran atau usulan mengenai perlakukan risiko yang diharapkan dapat mengurangi risiko dan dapat digunakan untuk pencegahan terhadap risiko pada teknologi informasi PT. Pos Indonesia di kemudian harinya.

Keywords

Risk Management, ISO 31000, PT. Pos Indonesia, *Information Technology*, *Technology Assets*

Abstrak

As a company operating in courier delivery, logistics, and financial transaction services, PT. Pos Indonesia cannot be separated from the use of information technology as a supporting asset for its business processes. The focus of this research is PT. Pos Indonesia Palembang 30000, which is the main branch of PT. Pos Indonesia in the city of Palembang. During the use of information technology, there are several recurring issues and risks, such as hardware damage, failure in data updates and backups resulting in data loss, and system failures caused by network infrastructure disruptions, rendering the system inaccessible to employees. Currently, PT. Pos Indonesia has not conducted a specific analysis and evaluation of risks related to information technology, which can pose a risk to the success of its business activities. This research utilizes ISO 31000 as a guide for risk management analysis. The results of this research consist of risk documentation, wherein out of 31 identified risks, there are 2 high-level risks, 26 medium-level risks, and 3 low-level risks. Identification of these 31 risks will be accompanied by recommendations or suggestions regarding risk management, which are expected to mitigate these risks and can be used for prevention of information technology-related risks at PT. Pos Indonesia in the future.

A. Pendahuluan

Hampir dalam segala aspek mempunyai keterkaitan terhadap teknologi informasi. Penerapan teknologi informasi di instansi atau organisasi merupakan kondisi yang tidak dapat dilepas dalam menjalankan proses bisnisnya. Peran teknologi informasi memberikan manfaat yang baik bagi organisasi. Selain memberikan manfaat yang baik, teknologi informasi juga dapat membawa risiko yang dapat menimbulkan kerentanan dan ancaman dalam keberlangsungan proses bisnisnya [1]. Pentingnya proses pemeriksaan dalam penggunaan teknologi informasi dikarenakan proses ini memberikan wawasan tentang keberhasilan implementasi suatu teknologi informasi. Organisasi atau perusahaan harus mengenal dan mengidentifikasi ancaman dengan metode yang tepat guna meminimalisir risiko kerusakan yang akan muncul [2].

PT. Pos Indonesia termasuk Badan Usaha Milik Negara (BUMN) Indonesia yang beroperasi di bidang kurir pengiriman, logistik, dan transaksi uang. PT. Pos Indonesia berfokus untuk meningkatkan kualitas layanannya dengan mengedepankan kepuasan pelanggan dan mempertimbangkan efisiensi dan efektivitas penggunaan sumber daya, serta kemampuan untuk meningkatkan keuntungan bisnis melalui penggunaan pengetahuan dan teknologi. PT. Pos Indonesia Palembang 30000 merupakan cabang utama dari PT. Pos Indonesia yang ada di kota Palembang. Teknologi informasi PT. Pos Indonesia ini dikelola oleh bidang solusi teknologi informasi. Berdasarkan hasil wawancara dengan staf dari bidang solusi teknologi informasi, bidang ini mempunyai tugas pokok untuk mengelola kesinambungan layanan teknologi informasi, mengelola insiden, penanganan, dan pelaporan layanan teknologi informasi, mengawasi pelaksanaan pemeliharaan dan perbaikan perangkat teknologi, mengelola kebutuhan kantor cabang utama, kantor cabang, dan kantor cabang pembantu terkait dengan layanan teknologi informasi.

Sebagai badan usaha yang yang beroperasi dalam sektor pengiriman, logistik, dan transaksi keuangan, PT. Pos Indonesia tidak dapat terlepas dari penggunaan teknologi informasi sebagai aset pendukung proses bisnis. Selama penggunaan teknologi informasi, berdasarkan hasil observasi terdapat beberapa permasalahan dan risiko yang kerap muncul di PT. Pos Indonesia, diantaranya terjadi kerusakan hardware, kegagalan dalam *update* dan *backup* data sehingga menyebabkan kehilangan data, kegagalan sistem yang disebabkan oleh gangguan infrastruktur jaringan sehingga sistem tidak dapat diakses oleh karyawan. Selain itu, adanya permasalahan non teknis seperti staf teknis yang terbatas sehingga sering merangkap tugas, pengetahuan terhadap pengelolaan teknologi informasi yang masih rendah. Hal tersebut berdampak pada terganggunya proses bisnis pada PT. Pos Indonesia. Staf bidang solusi teknologi informasi juga menjelaskan bahwa pada PT. Pos Indonesia saat ini sudah melakukan mitigasi risiko terhadap manajemen risiko teknologi informasi tetapi belum melakukan analisis dan evaluasi risiko yang diterapkan secara khusus terhadap teknologi informasi sehingga hal ini dapat menjadi risiko yang menyebabkan kegagalan dalam menjalankan aktivitas bisnis.

Dalam penggunaan teknologi informasi tersebut banyak kemungkinan terjadi kegagalan atau kerusakan yang tidak diinginkan [2]. Risiko-risiko yang muncul dapat mengganggu aktivitas yang berkaitan dengan teknologi informasi sehingga

tidak dapat berjalan secara optimal bahkan dapat menggagalkan aktivitas dan proses bisnis organisasi [3]. Maka dari itu, sesuai yang diatur pada Peraturan Menteri BUMN Nomor Per-01/MBU/2011 mengenai Penerapan Good Corporate Governance pada BUMN dan Nomor Per-5/MBU/09/2022 yang diterbitkan awal September oleh Kementerian BUMN mengenai Manajemen Risiko pada BUMN [4]. Kementerian BUMN dengan tegas mengintegrasikan manajemen risiko sebagai bagian integral dari pengawasan internal dan tata kelola terintegrasi (Pasal 1 Ayat 9). Dikarenakan adanya kebijakan tersebut, organisasi perlu menjabarkan lebih lanjut dan rinci pada tataran operasional terutama dalam hal penyempurnaan pedoman risiko mereka. Panduan manajemen risiko untuk BUMN juga harus sesuai dengan standar nasional manajemen risiko yaitu ISO 31000 yang merupakan standar internasional yang diakui [5]. Oleh karena itu, diperlukan antisipasi dengan melakukan identifikasi dan analisis manajemen risiko untuk melindungi aset penting PT. Pos Indonesia. Manajemen risiko didefinisikan sebagai aktivitas terkoordinasi yang memungkinkan instansi untuk diarahkan dan dikendalikan dalam hal risiko [6]. Pengelolaan risiko memiliki kepentingan besar, karena hal ini memungkinkan pihak internal dan eksternal untuk mengidentifikasi dan menghindari potensi adanya risiko yang dapat menyebabkan kerugian dari segi finansial maupun operasional [7].

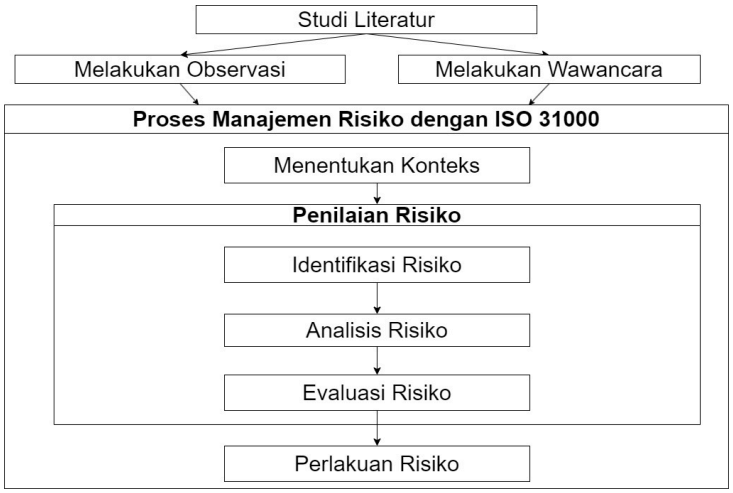
Kinerja suatu teknologi informasi dapat dievaluasi dan diukur menggunakan beberapa beberapa framework antara lain COBIT, ITIL, NIST SP 800-30, dan ISO 31000 yang dikeluarkan oleh ISACA [8]. Diantara keempat framework tersebut, dipilih framework yang digunakan sebagai pedoman dalam melakukan manajemen risiko yaitu ISO 31000 [9]. Pada penelitian ini, standar ISO 31000 akan diterapkan untuk analisis manajemen risiko. ISO 31000 merupakan salah satu standar internasional yang menyediakan panduan serta prinsip untuk menerapkan manajemen risiko. Penerapan ISO 31000 dapat memberikan kontribusi pada peningkatan kesempatan mencapai tujuan, memperkuat kemampuan mengidentifikasi peluang dan ancaman, serta mengoptimalkan pemanfaatan sumber daya dalam manajemen risiko [10]. Kelebihan ISO 31000 jika dibandingkan dengan framework lainnya yaitu dalam hal penerapan ISO 31000 lebih mudah diimplementasikan, prinsip dan panduannya yang bersifat umum sehingga dapat digunakan di semua tingkat organisasi dalam beragam bidang, termasuk dalam konteks manajemen risiko pada teknologi informasi [11]. Beberapa penelitian terdahulu yang telah melakukan analisis manajemen risiko menggunakan ISO 31000, seperti pada penelitian [12], [13], [14], [15], [16] yang berfokus pada analisis risiko teknologi informasi. Penelitian [12] dan [13] menemukan 21 kemungkinan risiko. Pada [12] dengan 8 kemungkinan risiko tingkat *medium* dan 17 kemungkinan risiko tingkat *low*, sedangkan pada penelitian [13] dengan 8 risiko berada pada *level high*, 10 risiko pada *level medium*, dan 3 risiko pada *level low*. Penelitian [14] menemukan 26 kemungkinan risiko terdapat pada aset penting teknologinya, dengan 2 risiko *level high*, 18 risiko *level medium*, dan 6 risiko *level low*. Penelitian [15] menemukan 2 kemungkinan risiko dengan tingkat rendah, 11 kemungkinan risiko dengan tingkat menengah, dan 4 kemungkinan risiko dengan tingkat tinggi. Serta pada penelitian [16] menemukan 24 kemungkinan risiko dimana 3 risiko pada level tinggi, 10 risiko level sedang, dan 11 risiko level rendah.

Berdasarkan pemetaan penelitian terdahulu dan permasalahan yang telah dijelaskan, analisis manajemen risiko akan dilakukan pada teknologi informasi PT. Pos Indonesia untuk mengetahui tingkat risiko yang ada dan diharapkan dapat meminimalisir terjadinya kegagalan pada teknologi informasi.

B. Metode Penelitian

1. Tahapan Penelitian

Sumber data dalam penelitian ini adalah data primer yang dikumpulkan dari PT. Pos Indonesia secara langsung berupa hasil wawancara dengan pegawai PT. Pos Indonesia dan data sekunder yang dikumpulkan melalui pembacaan buku dan jurnal penelitian terdahulu yang berkaitan dengan analisis manajemen risiko menggunakan ISO 31000. Penelitian ini menggunakan ISO 31000 yang merupakan standar dari ISO (*International Standard Organization*) untuk melakukan analisis manajemen risiko [9]. Berikut ini tahapan penelitian dalam analisis manajemen risiko menggunakan standar ISO 31000.



Gambar 1. Tahapan Penelitian

Dari tahapan penelitian tersebut, maka dapat dijelaskan tahapan yang akan dilakukan yaitu:

a. Studi Literatur. Studi literatur dilakukan dengan membaca referensi buku dan jurnal terkait objek penelitian.
b. Melakukan Observasi. Survei lapangan ke PT. Pos Indonesia (Persero) Palembang 30000 untuk melihat dan memperhatikan tugas, pokok, fungsi teknologi informasi yang digunakan, dan risiko yang telah dihadapi.
c. Melakukan Wawancara. Melakukan kegiatan tanya jawab dengan pegawai di bidang solusi teknologi informasi PT. Pos Indonesia (Persero) Palembang 30000.

2. Proses Manajemen Risiko dengan ISO 31000

Proses manajemen risiko merupakan serangkaian aktivitas yang sistematis untuk mendukung pihak pemangku kepentingan dalam mengelola peluang dan ancaman untuk mencapai sasaran yang dapat diukur dan terkendali. Penerapan proses manajemen risiko tidak boleh diabaikan, proses ini harus diintegrasikan ke

dalam setiap proses bisnis dan operasional organisasi. Dalam hal ini, tidak ada proses bisnis yang boleh dijalankan tanpa mempertimbangkan risiko, baik yang membawa dampak negatif sebagai ancaman, maupun risiko yang memberikan peluang positif untuk mencapai tujuan dan sasaran [17]. Rangkaian aktivitas dari proses dari manajemen risiko ISO 31000 sebagai berikut.

a. Menentukan Konteks
   Penentuan konteks ditentukan sesuai cara kerja PT. Pos Indonesia. Tahap menentukan konteks ditentukan dari tujuan, ruang lingkup, serta bagian organisasi yang melakukan manajemen risiko. Dalam proses ini, konteks yang perlu diperhatikan yaitu konteks eksternal, internal, proses manajemen risiko, dan kriteria risiko.
b. Identifikasi Risiko
   Proses ini dimulai dari mengidentifikasi berbagai kemungkinan risiko, penyebab risiko, dan dampak risiko yang muncul. Setelah mencatat daftar risiko yang dapat terjadi, langkah selanjutnya adalah mengelompokkannya sesuai dengan sumber kemungkinan risiko dan dampak yang mungkin timbul dari risiko tersebut. Pendekatan yang digunakan untuk mengidentifikasi risiko adalah dengan menggunakan Risk Breakdown Structure (RBS) untuk mengorganisir risiko-risiko yang terjadi pada teknologi informasi PT. Pos Indonesia.
c. Analisis Risiko
   Dilakukan tahap analisis risiko untuk menilai tingkat risiko berdasarkan kombinasi kemungkinan dan dampak dari setiap risiko yang telah diidentifikasi pada tahap menetapkan konteks dengan menggunakan kuesioner yang dibagikan kepada pegawai yang memiliki pengetahuan, pengalaman, dan yang terkait langsung dengan teknologi informasi di PT. Pos Indonesia. Hasil dari tahap analisis risiko ini yaitu pengelompokan penilaian risiko berdasarkan tingkat *likelihood* dan tingkat *impact*.
d. Evaluasi Risiko
   Tahap ini memperoleh informasi yang sesuai mengenai risiko yang mempengaruhi ketercapaian sasaran yang dapat membantu dalam proses pengambilan keputusan. Melalui proses ini, risiko-risiko yang perlu ditangani akan diidentifikasi dan diprioritaskan. Dalam menentukan tingkat risiko, digunakan sebuah matriks yang terdiri dari nilai kemungkinan (*likelihood*) dan nilai dampak (*impact*). Matriks ini terbagi menjadi tiga tingkatan sesuai dengan prioritas penanganan risiko yang telah ditetapkan, yaitu rendah (*low*), sedang (*medium*), dan tinggi (*high*).
e. Perlakuan Risiko
   Tahap perlakuan risiko melibatkan pemberian saran dan rekomendasi terhadap temuan risiko yang telah dievaluasi. Hal ini bertujuan untuk mengurangi atau menghilangkan dampak dan kemungkinan terjadinya risiko [17]. Setelah dilakukan perlakuan risiko, didapatkan cara penanggulangan risiko berdasarkan tingkatnya dan memberikan saran dan rekomendasi pada PT. Pos Indonesia. Pada tahap ini dihasilkan daftar usulan tindakan yang akan dilakukan berdasarkan daftar peringkat risiko dari tahap evaluasi risiko.

C. Hasil dan Pembahasan

1. Menentukan Konteks

1) Konteks Eksternal

Konteks eksternal membahas mengenai kondisi eksternal organisasi seperti peraturan pemerintah yang membahas mengenai pentingnya dilakukan manajemen risiko, kondisi alam dan lingkungan pada PT. Pos Indonesia (Persero) Palembang 30000.

a. Peraturan Pemerintah

PT. Pos Indonesia merupakan Badan Usaha Milik Negara yang berfokus pada pelayanan jasa pengiriman, logistik, dan transaksi keuangan. Dalam Peraturan Kementerian BUMN Nomor Per-01/MBU/2011 tentang *Good Corporate Governance* (Penerapan Tata Kelola Perusahaan yang Baik) pada BUMN. Serta pada Nomor Per-5/MBU/09/2022 terkait Manajemen Risiko pada BUMN. Kementerian BUMN menjelaskan manajemen risiko merupakan bagian integral dari pengawasan internal dan tata kelola terintegrasi manajemen risiko (Pasal 1 Ayat 9). PT. Pos Indonesia berkewajiban untuk menjabarkan lebih lanjut dan rinci pada tataran operasional terutama dalam hal penyempurnaan manajemen risiko.

b. Kondisi Alam dan Lingkungan

Kondisi cuaca di Kota Palembang pada bulan Agustus 2023 masuk ke kategori cuaca yang tidak menentu dan berubah-ubah. Dalam hasil wawancara dengan staf solusi teknologi menjelaskan tingginya curah hujan dapat menyebabkan gangguan jaringan internet dan menimbulkan risiko banjir. Di sisi lain, kondisi suhu udara yang tinggi menyebabkan perangkat keras berisiko *overheat* yang bisa berdampak pada kerusakan perangkat keras. Tidak menentunya cuaca seperti perubahan suhu udara dan curah hujan dapat mempengaruhi proses bisnis dan aktivitas PT. Pos Indonesia.

2) Konteks Internal

Konteks internal menjelaskan mengenai lingkungan internal PT. Pos Indonesia (Persero) berupa visi dan misi organisasi, struktur organisasi, dan aset dari komponen pada teknologi informasi.

a. Visi dan Misi PT. Pos Indonesia. Visi: menjadi postal operator, penyedia jasa kurir, logistik, dan keuangan paling kompetitif. Misi: bertindak efektif untuk mencapai performance terbaik.
b. Struktur Organisasi PT. Pos Indonesia. Struktur organisasi berkaitan dengan posisi dan tugas pokok bidang di PT. Pos Indonesia (Persero) Palembang 30000.
c. Sumber Daya Manusia Bagian Solusi Teknologi PT. Pos Indonesia. SDM pada bidang solusi teknologi di PT. Pos Indonesia (Persero) Palembang 30000 yang mengelola teknologi informasi.

3) Konteks Manajemen Risiko

a. Tujuan dan Sasaran Manajemen Risiko

Penelitian ini dilakukan untuk menganalisa manajemen risiko terkait teknologi informasi pada PT. Pos Indonesia, dan tujuan untuk PT. Pos Indonesia yaitu untuk menciptakan nilai tambah dan melindungi Perusahaan. Sasaran yang akan dicapai oleh manajemen risiko ini adalah dapat menghindari risiko-risiko yang dapat membuat kerusakan dan kerugian

terhadap teknologi informasi sehingga tidak akan terjadi masalah pada proses bisnis PT. Pos Indonesia.

b. Identifikasi Penyusunan Kuesioner Manajemen Risiko
Metode untuk menentukan penyusunan kuesioner dalam manajemen risiko adalah menggunakan RACI Chart yang berfungsi sebagai panduan dalam memilih partisipan penelitian dan bertujuan untuk mengidentifikasi siapa yang akan berperan sebagai responden dalam penelitian sehingga jawaban dari hasil kuesioner ini akan cukup valid untuk dilakukan analisis manajemen risiko pada teknologi informasi PT. Pos Indonesia. Identifikasi responden dengan menggunakan RACI Chart disajikan pada Tabel 1.

Tabel 1. Identifikasi Responden

RACI *Respondent*	***Actual Respondent***
Head Development, Chief Technology Officer, Chief Information Officer	Manajer Solusi Teknologi Informasi
Head IT Operations, Head IT Administration, Service Manager	Staf Solusi Teknologi Informasi
Chief Operating Officer, Service Manager	Bagian Pelayanan Outlet dan Operasi Cabang
Business Continuity Manager	Bagian Penjualan Korporat Kurir dan Logistik
Business Continuity Manager	Bagian Penjualan Ritel dan Kemitraan

Penentuan *stakeholders* dan peran masing-masing *stakeholders* dalam proses manajemen risiko dilakukan berdasarkan matriks RACI Chart. Pada tabel 2 merupakan rincian *stakeholders* menggunakan RACI Chart.

Tabel 2. RACI Chart *Stakeholder*

No	**Proses Manajemen Risiko**	**Manajer Solusi Teknologi**	**Staf Solusi Teknologi**	**Pelayanan Outlet & Operasi Cabang**	**Penjualan Korporat Kurir & Logistik**	**Penjualan Ritel & Kemitraan**
1.	Menentukan konteks	A/C/I	R/C	-	-	-
2.	Identifikasi risiko	A/I	R/C	C	C	C
3.	Analisis risiko	A/I	R/C	C	C	C
4.	Evaluasi risiko	A/I	C	C	C	C
5.	Perlakuan risiko	A/I	C	C	C	C

c. Kriteria Risiko

a) Kriteria Kemungkinan Risiko (*likelihood*)
Di tahap ini, nilai kemungkinan ditentukan dengan menetapkan kriteria berdasarkan probabilitas terjadinya risiko pada teknologi informasi PT. Pos Indonesia. Hal ini bertujuan untuk memberikan tingkat kemungkinan yang sesuai dalam menganalisis risiko.

Tabel 3. Kriteria Kemungkinan Frekuensi Kejadian

Likelihood		**Keterangan**	**Frekuensi per kejadian**
Nilai	**Kriteria**		
1	*Rare*	Risiko hampir tidak mungkin terjadi	> 24 bulan
2	*Unlikely*	Risiko jarang terjadi	12-24 bulan
3	*Possible*	Risiko terkadang terjadi	7-12 bulan
4	*Likely*	Risiko sering terjadi	4-6 bulan

5	*Certain*	Risiko selalu terjadi	1-3 bulan

b) Kriteria Dampak Risiko (*impact*)
Penelitian ini menggunakan kriteria dampak untuk memberikan pengukuran konsisten terhadap tingkat dampak pada PT. Pos Indonesia. Penelitian ini menetapkan lima tingkat dampak risiko, masing-masing dengan deskripsi risiko yang sesuai.

Tabel 4. Kriteria Dampak Risiko

Impact		**Keterangan**
Nilai	**Kriteria**	
1	*Insignificant*	Aktivitas perusahaan tidak terganggu
2	*Minor*	Aktivitas perusahaan sedikit terhambat tetapi dapat masih bisa berjalan lancar
3	*Moderate*	Mengganggu sebagian besar aktivitas perusahaan
4	*Major*	Mengganggu hampir seluruh aktivitas perusahaan
5	*Catastrophic*	Sangat mengganggu dan menghambat sehingga menyebabkan terhentinya aktivitas perusahaan

c) Kriteria Tingkat Risiko (*Risk Level*)
Kriteria tingkat risiko ditetapkan dengan matriks evaluasi risiko yang menggambarkan hubungan antara tingkat dampak dan kemungkinan [17]. Matriks evaluasi risiko dibagi menjadi tiga tingkatannya yaitu *low*, *medium*, dan *high*.

2. Penilaian Risiko

1) Identifikasi Risiko

Dalam tahap identifikasi risiko dilaksanakan melalui proses wawancara dengan karyawan dan dilakukan observasi pada PT. Pos Indonesia (Persero) Palembang 30000. Tahap ini dimulai dengan identifikasi aset komponen teknologi informasi yang dimiliki PT. Pos Indonesia (Persero) Palembang 30000. Berikut rincian aset teknologi informasi yang disajikan pada tabel 5 berikut ini.

Tabel 5. Identifikasi Aset

Komponen Teknologi Informasi	**Aset**
Data	Data karyawan, data pelanggan, data transaksi, data mitra biller
Perangkat Lunak (*software*)	ICWahana
Perangkat Keras (*hardware*)	Personal computer, monitor, printer, server database, server web service, LAN, router, switch
Bangunan	Bangunan gedung PT. Pos Indonesia (Persero) Palembang 30000

Tahapan berikutnya adalah identifikasi kemungkinan risiko yang dapat mengancam teknologi informasi. Proses identifikasi risiko dilakukan dengan melalui proses wawancara dan hasil observasi lapangan, kemudian disusun menggunakan *Risk Breakdown Structure* (RBS). Pengelompokkan risiko disusun berdasarkan sumber risiko. Adapun pengelompokkan tersebut terbagi menjadi faktor alam atau lingkungan, manusia, dan sistem atau infrastruktur. Berikut kemungkinan risiko yang terjadi dapat dilihat pada tabel 6.

Tabel 6. Identifikasi Kemungkinan Risiko

Sumber risiko	ID Risiko	Kemungkinan risiko
Alam/Lingkungan	R1	Kerusakan perangkat akibat radiasi panas
	R2	Kerusakan perangkat akibat debu
	R3	Kerusakan infrastruktur yang disebabkan jamur
	R4	Kerusakan perangkat akibat banjir
	R5	Kerusakan perangkat akibat sambaran petir
	R6	Kerusakan perangkat akibat kebakaran
	R7	Kerusakan perangkat akibat gempa bumi
Manusia	R8	Pegawai merangkap tugas karena SDM terbatas
	R9	Kesalahan input data (*human error*)
	R10	Informasi diakses oleh pihak yang tidak berwenang
	R11	Kehilangan data
	R12	Prosedur penggunaan sistem kurang dipahami
	R13	Kurangnya pemahaman terhadap IT
	R14	Penyalahgunaan hak akses/user id
	R15	Pencurian perangkat
	R16	Data dan informasi tidak sesuai fakta
	R17	Kebocoran data/informasi internal perusahaan
	R18	Memasukkan malware
	R19	Kerusakan akibat kelalaian pegawai
Sistem dan	R20	Pemadaman listrik
Infrastruktur	R21	Jaringan internet tidak stabil/terputus
	R22	Kerusakan pada hardware
	R23	Kerusakan pada data
	R24	Overload
	R25	Server down
	R26	Kegagalan dalam *update* data
	R27	Kegagalan dalam *backup* data
	R28	Kegagalan proses pemeliharaan yang tidak tepat waktu
	R29	Kerusakan akibat masalah catu daya/ tegangan listrik
	R30	Penyusupan terhadap jaringan komputer
	R31	Serangan malware

Dari kemungkinan-kemungkinan risiko yang telah ditemukan akan dilakukan identifikasi dampak seperti apa yang akan terjadi oleh risiko tersebut pada teknologi informasi PT. Pos Indonesia. Berikut adalah tabel dampak dari tiap kemungkinan risiko.

Tabel 7. Identifikasi Dampak Risiko

Sumber Risiko	ID Risiko	Kemungkinan Risiko	Dampak
Alam/ Lingkungan	R1	Kerusakan perangkat akibat radiasi panas	Terjadi kerusakan aset IT, aktivitas bisnis perusahaan terhambat
	R2	Kerusakan perangkat akibat debu	Kerusakan aset IT, aktivitas bisnis perusahaan terhambat
	R3	Kerusakan infrastruktur yang disebabkan jamur	Kerusakan aset IT, aktivitas bisnis perusahaan terganggu
	R4	Kerusakan perangkat akibat banjir	Kerusakan infrastruktur yang membuat aktivitas bisnis perusahaan terhambat
	R5	Kerusakan perangkat akibat sambaran petir	Ketersediaan koneksi jaringan terganggu, terjadi kerusakan aset IT, aktivitas bisnis perusahaan terhambat,

			dan kerugian finansial
	R6	Kerusakan perangkat akibat kebakaran	Terjadi kerusakan aset-aset IT, aktivitas bisnis perusahaan terhenti, dan kerugian finansial
	R7	Kerusakan perangkat akibat gempa bumi	Terjadi kerusakan aset-aset IT, aktivitas bisnis perusahaan terhenti, dan kerugian finansial
Manusia	R8	Pegawai merangkap tugas karena SDM terbatas	Waktu penyelesaian tugas tidak tepat waktu dan pekerjaan terlambat
	R9	Kesalahan input data (*human error*)	Data yang diinput tidak valid, data sulit untuk diakses, aktivitas bisnis perusahaan terganggu
	R10	Informasi diakses oleh pihak yang tidak berwenang	Kebocoran data-data penting, kemungkinan terjadinya manipulasi data
	R11	Kehilangan data	Aktivitas bisnis perusahaan terhambat, kerugian waktu dan tenaga staf
	R12	Prosedur penggunaan sistem kurang dipahami	Menghambat proses kerja
	R13	Kurangnya pemahaman terhadap IT	Memperlambat proses kerja, kerusakan terhadap aset IT
	R14	Penyalahgunaan hak akses/user id	Kebocoran data dan informasi penting perusahaan, terjadinya manipulasi data
	R15	Pencurian perangkat	Kehilangan aset-aset IT dan data penting, kerugian finansial
	R16	Data dan informasi tidak sesuai fakta	Data pelanggan tidak valid, terjadinya manipulasi data
	R17	Kebocoran data/informasi internal perusahaan	Data dapat disalahgunakan, kerugian finansial, kerusakan reputasi perusahaan
	R18	Memasukkan *malware*	Terjadi kerusakan dan kebocoran pada data perusahaan, data perusahaan dicuri, aktivitas bisnis perusahaan terganggu, dan kerugian finansial
	R19	Kerusakan akibat kelalaian pegawai	Kerusakan aset IT, aktivitas perusahaan terhambat, kerugian finansial
Sistem dan Infrastruktur	R20	Pemadaman listrik	Aktivitas bisnis perusahaan terhenti sementara, namun dapat dibantu adanya genset
	R21	Jaringan internet tidak stabil/terputus	Terjadi kegagalan atau terhambat dalam mengakses sistem/data, tidak dapat melakukan pelayanan, proses bisnis terganggu
	R22	Kerusakan pada *hardware*	Tidak dapat melakukan aktivitas *online*, proses bisnis perusahaan terhambat
	R23	Kerusakan pada data	Kehilangan data penting perusahaan, aktivitas perusahaan terhambat
	R24	*Overload*	Kinerja server menjadi lambat/*down*, kehilangan data, penyimpanan *database* penuh
	R25	*Server down*	Kesulitan mengakses sistem, mengalami sistem error, aktivitas bisnis perusahaan terhambat
	R26	Kegagalan dalam *update* data	Kehilangan data, tidak adanya pembaharuan data, data menjadi tidak lengkap

	R27	Kegagalan dalam *backup* data	Kehilangan data, tidak adanya pembaharuan data, data tidak lengkap
	R28	Kegagalan proses pemeliharaan yang tidak tepat waktu	Kinerja perangkat mengalami penurunan, memungkinkan cepat mengalami kerusakan
	R29	Kerusakan akibat masalah catu daya/ tegangan listrik	Menyebabkan malfungsi *hardware*, listrik bermasalah, mempercepat kerusakan aset IT
	R30	Penyusupan terhadap jaringan komputer	Pencurian data penting, terdapat akses yang tidak sah, kerugian informasi perusahaan, aktivitas bisnis terganggu
	R31	Serangan *malware*	Terjadi kerusakan data, kerugian informasi/ finansial, aktivitas bisnis perusahaan terganggu

2) Analisis Risiko

Setelah melakukan identifikasi risiko, diperoleh nilai dari kemungkinan dan dampak dari hasil pengisian kuesioner kepada pegawai. Kuesioner tersebut sudah melalui proses validasi dan dinyatakan lulus validasi oleh ahli yang berkaitan dengan manajemen risiko. Kemudian akan digabungkan kedua nilai tersebut berdasarkan tiap risikonya. Penilaian kemungkinan (*likelihood*) dan dampak (*impact*) seperti pada tabel 8.

Tabel 8. Penilaian kemungkinan (*likelihood*) dan dampak (*impact*)

Sumber Risiko	ID Risiko	Risiko	Kemungkinan	Dampak
Alam/ Lingkungan	R1	Kerusakan perangkat akibat radiasi panas	2	3
	R2	Kerusakan perangkat akibat debu	2	2
	R3	Kerusakan infrastruktur yang disebabkan jamur	2	2
	R4	Kerusakan perangkat akibat banjir	2	3
	R5	Kerusakan perangkat akibat sambaran petir	2	3
	R6	Kerusakan perangkat akibat kebakaran	2	4
	R7	Kerusakan perangkat akibat gempa bumi	1	3
Manusia	R8	Pegawai merangkap tugas karena SDM terbatas	3	3
	R9	Kesalahan input data (*human error*)	3	3
	R10	Informasi diakses oleh pihak yang tidak berwenang	2	4
	R11	Kehilangan data	3	3
	R12	Prosedur penggunaan sistem kurang dipahami	3	3
	R13	Kurangnya pemahaman terhadap IT	3	3
	R14	Penyalahgunaan hak akses/user id	2	4
	R15	Pencurian perangkat	2	4
	R16	Data dan informasi tidak sesuai fakta	2	3
	R17	Kebocoran data/informasi internal perusahaan	2	4
	R18	Memasukkan *malware*	3	4
	R19	Kerusakan akibat kelalaian pegawai	2	4
Sistem dan Infrastruktur	R20	Pemadaman listrik	3	3
	R21	Jaringan internet tidak stabil/terputus	3	4
	R22	Kerusakan pada *hardware*	2	3
	R23	Kerusakan pada data	2	3

R24	*Overload*	2	3
R25	*Server down*	2	3
R26	Kegagalan dalam *update* data	2	3
R27	Kegagalan dalam *backup* data	2	3
R28	Kegagalan proses pemeliharaan yang tidak tepat waktu	2	3
R29	Kerusakan akibat masalah catu daya/ tegangan listrik	2	3
R30	Penyusupan terhadap jaringan komputer	2	3
R31	Serangan *malware*	2	3

3) Evaluasi Risiko

Tahap ini merupakan proses dalam pengambilan keputusan dalam manajemen risiko [17]. Dalam tahap ini dilakukan pemetaan terhadap level risiko berdasarkan matriks evaluasi risiko. Risiko yang telah diidentifikasi akan dibagi menjadi tiga tingkatan risiko yaitu low, medium, high.

Tabel 9. Matriks Evaluasi Risiko

			Dampak (*impact*)				
			1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Kemungkinan (*likelihood*)	5	*Certain*					
	4	Likely					
	3	Possible			R8, R9, R11, R12, R13, R20	R18, R21	
	2	Unlikely		R2, R3	R1, R4, R5, R16, R22, R23, R24, R25, R26, R27, R28, R29, R30, R31	R6, R10, R14, R15, R17, R19	
	1	Rare			R7		

Setelah kemungkinan dan dampak risiko dimasukkan ke matriks evaluasi risiko, langkah selanjutnya akan dilakukan penjabaran dari 31 risiko yang telah diidentifikasi ke dalam risk level risiko berdasarkan tingkatan high, medium, low yang disajikan di tabel 10.

Tabel 10. *Risk Level*

ID Risiko	**Risiko**	**Kemungkinan (*likelihood*)**	**Kategori**	**Dampak (*impact*)**	**Kategori**	***Risk Level***
R18	Memasukkan *malware*	3	*Possible*	4	*Major*	High
R21	Jaringan internet tidak stabil/terputus	3	*Possible*	4	*Major*	High
R8	Pegawai merangkap tugas karena SDM terbatas	3	*Possible*	3	*Moderate*	Medium
R9	Kesalahan input data (*human error*)	3	*Possible*	3	*Moderate*	Medium
R11	Kehilangan data	3	*Possible*	3	*Moderate*	Medium
R12	Prosedur penggunaan sistem kurang dipahami	3	*Possible*	3	*Moderate*	Medium
R13	Kurangnya pemahaman terhadap IT	3	*Possible*	3	*Moderate*	Medium
R20	Pemadaman listrik	3	*Possible*	3	*Moderate*	Medium
R1	Kerusakan perangkat akibat radiasi panas	2	*Unlikely*	3	*Moderate*	Medium

R4	Kerusakan perangkat akibat banjir	2	*Unlikely*	3	*Moderate*	Medium
R5	Kerusakan perangkat akibat sambaran petir	2	*Unlikely*	3	*Moderate*	Medium
R16	Data dan informasi tidak sesuai fakta	2	*Unlikely*	3	*Moderate*	Medium
R22	Kerusakan pada *hardware*	2	*Rare*	3	*Moderate*	Medium
R23	Kerusakan pada data	2	*Rare*	3	*Moderate*	Medium
R24	*Overload*	2	*Rare*	3	*Moderate*	Medium
R25	*Server down*	2	*Rare*	3	*Moderate*	Medium
R26	Kegagalan dalam *update* data	2	*Rare*	3	*Moderate*	Medium
R27	Kegagalan dalam *backup* data	2	*Rare*	3	*Moderate*	Medium
R28	Kegagalan proses pemeliharaan yang tidak tepat waktu	2	*Rare*	3	*Moderate*	Medium
R29	Kerusakan akibat masalah catu daya/ tegangan listrik	2	*Rare*	3	*Moderate*	Medium
R30	Penyusupan terhadap jaringan komputer	2	*Rare*	3	*Moderate*	Medium
R31	Serangan *malware*	2	*Rare*	3	*Moderate*	Medium
R6	Kerusakan perangkat akibat kebakaran	2	*Unlikely*	4	*Major*	Medium
R10	Informasi diakses oleh pihak yang tidak berwenang	2	*Unlikely*	4	*Major*	Medium
R14	Penyalahgunaan hak akses/user id	2	*Unlikely*	4	*Major*	Medium
R15	Pencurian perangkat	2	*Unlikely*	4	*Major*	Medium
R17	Kebocoran data/informasi internal perusahaan	2	*Unlikely*	4	*Major*	Medium
R19	Kerusakan akibat kelalaian pegawai	2	*Rare*	4	*Major*	Medium
R2	Kerusakan perangkat akibat debu	2	*Unlikely*	2	*Minor*	Low
R3	Kerusakan infrastruktur yang disebabkan jamur	2	*Unlikely*	2	*Minor*	Low
R7	Kerusakan perangkat akibat gempa bumi	1	*Rare*	3	*Moderate*	Low

4) Perlakuan Risiko

Setelah dilakukan identifikasi, analisis, serta evaluasi risiko. Tahap terakhir memberikan perlakuan pada risiko. Dalam tahap ini akan memberikan saran atau usulan mengenai perlakukan risiko yang diharapkan dapat digunakan untuk pencegahan terhadap timbulnya risiko pada teknologi informasi PT. Pos Indonesia yang sedang muncul atau mungkin akan muncul di kemudian harinya. Adapun saran atau usulan yang diberikan untuk risiko yang telah diidentifikasi disajikan pada tabel 11.

Tabel 11. Usulan Perlakuan Risiko [12], [15], [16], [18], [19]

ID Risiko	Risiko	Level Risiko	Opsi perlakuan	Perlakuan risiko
R18	Memasukkan	*High*	*Risk*	Pemeriksaan *software* secara rutin

	malware		*Mitigation*	Melakukan *scanning antivirus* secara berkala Melakukan pemasangan *firewall* dan *internet security*
R21	Jaringan internet tidak stabil/terputus	*High*	*Risk Sharing*	Melaporkan ke bidang solusi teknologi informasi jika terjadi gangguan jaringan internet Mengganti Penyedia Jasa Internet (ISP) dengan yang baru
			Risk Mitigation	Melakukan pemeriksaan jaringan secara rutin dan menambahkan perangkat penguat sinyal *router* agar koneksi jaringan tetap dapat terhubung
R8	Pegawai merangkap tugas karena SDM terbatas	*Medium*	*Risk Mitigation*	Melakukan pembagian tugas sesuai dengan tugas masing-masing bagian Pegawai menyelesaikan pekerjaan sesuai tugas dan waktu yang tepat
R9	Kesalahan input data (*human error*)	*Medium*	*Risk Mitigation*	Melakukan pengecekan ulang sebelum submit data Memberikan pelatihan kepada pegawai sesuai dengan prosedur kerja yang ada
R11	Kehilangan data	*Medium*	*Risk Mitigation*	Melakukan *backup* dan *recovery* data secara rutin Memeriksa *antivirus* komputer secara berkala
R12	Prosedur penggunaan sistem kurang dipahami	*Medium*	*Risk Mitigation*	Melakukan *knowledge sharing* kepada pegawai yang belum memahami prosedur penggunaan sistem Memberikan pelatihan kepada pegawai tentang prosedur sistem
R13	Kurangnya pemahaman terhadap IT	*Medium*	*Risk Mitigation*	Memberikan pelatihan kepada pegawai sesuai dengan prosedur kerja yang ada
R20	Pemadaman listrik	*Medium*	*Risk Mitigation*	Menggunakan energi cadangan seperti genset otomatis yang langsung aktif dan dapat meng*cover* seluruh bagian saat pemadaman listrik
R1	Kerusakan perangkat akibat radiasi panas	*Medium*	*Risk Mitigation*	Melakukan pengecekan dan perawatan perangkat secara rutin Melakukan *backup* data secara rutin Memastikan suhu ruangan harus tetap dingin dan stabil
R4	Kerusakan perangkat akibat banjir	*Medium*	*Risk Mitigation*	Menyimpan aset IT dengan lebih aman dan jauh dari jangkauan banjir, dan sebaiknya tidak di lantai dasar Melakukan *backup* data secara rutin
R5	Kerusakan perangkat akibat sambaran petir	*Medium*	*Risk Mitigation*	Memasang alat penangkal petir di luar bangunan gedung untuk menghindari sambaran petir
R16	Data dan informasi tidak sesuai fakta	*Medium*	*Risk Mitigation*	Melakukan monitoring data sesuai fakta yang ada Melakukan pengecekan ulang terhadap data yang akan diinputkan ke dalam sistem
R22	Kerusakan pada *hardware*	*Medium*	*Risk Sharing*	Melaporkan ke bidang solusi teknologi informasi jika terjadi kerusakan *hardware*
			Risk Mitigation	Melakukan perawatan *hardware* secara rutin Menyediakan *hardware* cadangan/baru jika pada suatu saat tidak dapat digunakan lagi
R23	Kerusakan pada data	*Medium*	*Risk Mitigation*	Melakukan *backup* data Melakukan pembersihan komputer agar mencegah munculnya virus Melakukan pemeriksaan *antivirus* secara berkala

R24	*Overload*	*Medium*	*Risk Mitigation*	Melakukan *refresh* dan pengecekan *database log* dan RAM secara teratur seminggu sekali untuk mencegah penumpukan masalah pada sistem
R27	*Server down*	*Medium*	*Risk Mitigation*	Rutin melakukan pemeriksaan *database*, CPU, dan RAM Peningkatan *antivirus* agar terhindar dari *malicious code*
			Risk Sharing	Melakukan monitoring kepada penyedia *hosting* secara berkala
R26	Kegagalan dalam *update* data	*Medium*	*Risk Mitigation*	Melakukan pemeliharaan sistem secara rutin Memperhatikan penggunaan memori penyimpanan *database* yang diperlukan
R27	Kegagalan dalam *backup* data	*Medium*	*Risk Mitigation*	Memeriksa penggunaan memori penyimpanan yang digunakan agar tidak terjadi *overload* yang menyebabkan kegagalan *backup* data Melakukan *maintenance plan* secara berkala
R28	Kegagalan proses pemeliharaan yang tidak tepat waktu	*Medium*	*Risk Mitigation*	Meningkatkan pemeriksaan dan pengendalian *maintenance* aset IT Membuat jadwal rutin untuk melakukan pemeliharaan aset-aset IT
R29	Kerusakan akibat masalah catu daya/ tegangan listrik	*Medium*	*Risk Mitigation*	Menggunakan *stabilizer* untuk mengembalikan keseimbangan tegangan apabila listrik tiba-tiba mati dan kemudian tiba-tiba hidup kembali Memakai *Uninterruptible Power Supply* (UPS) untuk membuat tegangan listrik menjadi lebih stabil, alat ini dapat menyimpan energi listrik cadangan
			Risk Sharing	Melakukan monitoring listrik dengan pihak PLN secara rutin
R30	Penyusupan terhadap jaringan komputer	*Medium*	*Risk Mitigation*	Peningkatan *password* yang unik dan kuat Memonitoring dan melakukan pemeliharaan jaringan secara berkala Meningkatkan penggunaan *firewall* dan *internet security*
R31	Serangan *malware*	*Medium*	*Risk Mitigation*	Melakukan *scanning antivirus* secara berkala Melakukan pemasangan *firewall* dan *internet security* Pemeriksaan *software* secara rutin
R6	Kerusakan perangkat akibat kebakaran	*Medium*	*Risk Mitigation*	Menghindari hal-hal yang dapat menimbulkan kebakaran dari aset-aset TI Mempersiapkan alat pemadam kebakaran untuk di dalam gedung, serta rencana penyediaan cadangan infrastruktur *hardware* dan perangkat jaringan Menyiapkan server cadangan di lokasi yang aman dan terpisah Melakukan mirroring database penyimpanan otomatis yang tersimpan di server cadangan
R10	Informasi diakses oleh pihak yang tidak berwenang	*Medium*	*Risk Mitigation*	Tidak sembarangan membagikan password yang bersifat rahasia kepada pihak lain Membuat pembaharuan/update password Memasang kamera pengawas seperti CCTV pada bangunan Membuat setiap aktivitas akses terekam

				oleh sistem
			Risk Avoidance	Melakukan penanganan terhadap pelanggaran SOP secara tertulis dan resmi
R14	Penyalahgunaan hak akses/user id	*Medium*	*Risk Avoidance*	Membuat batasan hak akses tiap user
			Risk Avoidance	Melakukan penanganan terhadap pelanggaran SOP
			Risk Mitigation	Melakukan manajemen hak akses user dengan mengatur pergantian *password* secara berkala
				Melarang setiap pegawai untuk membagikan *password* user id
				Membuat setiap aktivitas akses pegawai terekam oleh sistem
R15	Pencurian perangkat	*Medium*	*Risk Mitigation*	Memperbanyak kamera pengawas CCTV pada ruangan penting
				Membuat keamanan akses ruangan hanya dimiliki oleh pegawai menggunakan kartu akses karyawan
			Risk Sharing	Memperketat penjagaan *security*
R17	Kebocoran data/informasi internal perusahaan	*Medium*	*Risk Mitigation*	Melakukan enkripsi data
				Melepaskan akses pegawai kepada data/informasi yang bukan lagi tanggung jawab aksesnya
				Menghapus data/informasi pada perangkat yang akan dibuang
R19	Kerusakan akibat kelalaian pegawai	*Medium*	*Risk Mitigation*	Memperketat pengawasan pegawai
				Memberikan peringatan kepada pegawai yang melanggar
R2	Kerusakan perangkat akibat debu	*Low*	*Risk Mitigation*	Melakukan perawatan dan pembersihan aset IT secara rutin
				Melakukan *backup* data secara rutin
R3	Kerusakan infrastruktur yang disebabkan jamur	*Low*	*Risk Mitigation*	Memastikan suhu ruangan stabil dan tidak lembab
				Melakukan pembersihan secara rutin
R7	Kerusakan perangkat akibat gempa bumi	*Low*	*Risk Mitigation*	Mempersiapkan perencanaan penyediaan cadangan infrastruktur *hardware* dan perangkat jaringan, dikarenakan gempa bumi merupakan bencana alam yang tidak terduga
				Melakukan *mirroring* database penyimpanan otomatis yang tersimpan di server cadangan

D. Simpulan

Dari hasil penelitian analisis manajemen risiko pada teknologi informasi PT. Pos Indonesia menggunakan ISO 31000 yang telah dilakukan melalui berbagai tahapan dalam proses manajemen risiko yaitu penentuan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko. Diperoleh identifikasi risiko sebanyak 31 kemungkinan risiko pada teknologi informasi PT. Pos Indonesia, diketahui tingkat risiko yang ada pada teknologi informasi yaitu terdapat 2 risiko dengan tingkatan high yang terdiri dari jaringan internet tidak stabil/terputus dan memasukkan malware. 26 risiko dengan tingkatan medium. Serta 3 risiko dengan tingkatan low yaitu kerusakan perangkat akibat gempa bumi, debu, dan jamur. Dari risiko-risiko yang muncul, PT. Pos Indonesia meminimalisir

kemungkinan risiko dengan memilih opsi perlakuan risiko yang diantaranya risk mitigation yaitu melakukan penyelesaian masalah dengan mengurangi kemungkinan timbulnya risiko atau dampaknya, *risk sharing* yaitu berbagi risiko dengan pihak ketiga, dan *risk avoidance* yaitu melakukan tindakan pencegahan risiko dengan menghilangkan sumber ancaman yang menjadi penyebab timbulnya risiko.

E. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada pihak yang telah berkontribusi dalam penelitian, khususnya PT. Pos Indonesia (Persero) Palembang 30000.

F. Referensi

[1] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," *Procedia Comput. Sci.*, vol. 135, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.

[2] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[3] L. N. Francisca and V. I. Radiant, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," pp. 1–23, 2016.

[4] Peraturan Menteri BUMN, "PerMen BUMN Nomor: Per- 5/MBU/09/2022 Tentang Manajemen Risiko pada BUMN," Jakarta, 2022.

[5] CRSM, "Manajemen Risiko pada BUMN," 2022.

[6] ISO, *ISO 31000: 2018. Risk Management-Guidelines*. Switzerland: BSI Group, 2018.

[7] 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.

[8] G. Breda and M. Kiss, "Overview of information security standards in the field of special protected industry 4.0 areas & industrial security," *Procedia Manuf.*, vol. 46, no. 2019, pp. 580–590, 2020, doi: 10.1016/j.promfg.2020.03.084.

[9] G. H. S. Rampini, H. Takia, and F. T. Berssaneti, "Critical success factors of risk management with the advent of ISO 31000 2018 - Descriptive and content analyzes," *Procedia Manuf.*, vol. 39, pp. 894–903, 2019, doi: 10.1016/j.promfg.2020.01.400.

[10] ISO, *Risk Management-Principles and guidelines*. Switzerland: BSI Group, 2009.

[11] A. P. Aisyah and L. Dahlia, "Enterprise Risk Management Berdasarkan ISO 31000 Dalam Pengukuran Risiko Operasional pada Klinik Spesialis Esti," *J. Akunt. dan Manaj.*, vol. 19, no. 02, pp. 78–90, 2022, doi: 10.36406/jam.v19i02.483.

[12] A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP," *J. SITECH Sist. Inf. dan Teknol.*,

vol. 2, no. 1, pp. 13–20, 2019, doi: 10.24176/sitech.v2i1.3122.

[13] D. P. Natalie and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000:2018 pada PT Bayu Buana Tbk," *JURIKOM (Jurnal Ris. Komputer)*, vol. 9, no. 5, p. 1290, 2022, doi: 10.30865/jurikom.v9i5.4797.

[14] S. Agustinus, A. Nugroho, and A. D. Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *Resti (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 1, pp. 19–25, 2017.

[15] M. I. Fachrezi, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 2, pp. 764–773, 2021, doi: 10.35957/jatisi.v8i2.789.

[16] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.

[17] V. R. Susilo, L. J. & Kaho, *Manajemen Risiko Berbasis ISO 31000:2018 – Panduan untuk Risk Leaders dan Risk Practitioners*. Jakarta Pusat: Gramedia Widiasarana Indonesia, 2018.

[18] P. Kanantyo and F. S. Papilaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 1896–1908, 2021, doi: 10.35957/jatisi.v8i4.1082.

[19] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000 : 2018 (Studi Kasus: Cv. Xy)," *Sebatik*, vol. 23, no. 1, pp. 277–284, 2019, doi: 10.46984/sebatik.v23i1.572.