ZONAsi Jurnal Sistem Informasi
ZONAsi VOL. 5 NO. 2 MEI 2023
Page: 372 - 381
ISSN: 2656-7407 (Online)
2656-7393 (Print)

ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI MENGGUNAKAN ISO 31000:2018 di PT. XYZ

Tierza Widy Chrisanty[1], Johan Tambotoh[2]
[1]Program Studi Sistem Informasi Fakultas Teknologi Informasi Universitas Kristen Satya Wacana

Jl. Diponegoro No.52-60, Salatiga, Jawa Tengah, telp. 0811 270 0049
e-mail: [1]tierzachrisanty29@gmail.com, [2]johan.tambotoh@uksw.edu

Abstrak

Dalam perkembangan teknologi yang semakin pesat, kemungkinan ancaman dan risiko yang muncul juga harus menjadi perhatian karena berbagai ancaman dan risiko yang mengganggu dapat melumpuhkan aktivitas kinerja di dalamnya, termasuk penggunaan sistem, sehingga sistem tidak berjalan secara ptimal. Begitu juga halnya yang terjadi pada PT. XYZ tepatnya pada direktorat Marketing dikarenakan masih menggunakan cara manual pada proses administrasi, data tidak terpantau dengan baik, dan lain sebagainya. Oleh karena itu, peneliti tertarik menggunakan kerangka kerja ISO 31000:2018 untuk melakukan analisis manajemen risiko terdapat 4 tahapan yaitu identifikasi risiko, analisis risiko, evaluasi risiko, dan perlakuan risiko. Dari hasil penelitian yang telah dilakukan terdapat 21 risiko yang mungkin terjadi dibagi menjadi 3 golongan yaitu terdapat 3 risiko pada golongan low, 15 risiko golongan medium, 3 risiko pada golongan high. Adapun yang dapat dilakukan adalah dengan menjalankan rekomendasi yang telah diusulkan pada performa sistem informasi agar lebih berkembang dan menjadi lebih baik.
Kata kunci: *Manajemen risiko, sistem informasi, telekomunikasi*

Abstract

In the rapid development of technology, the possibility of risks that arise must also be a concern because it can interfere with performance activities in it including the use of the system, so that the system does not run optimally. This also happens to the marketing directorate of PT XYZ because it still uses manual methods in the administrative process, data is not monitored properly, and so on. Therefore, researchers are interested in using the ISO 31000: 2018 framework to analyze risk management, there are 4 stages, namely identification, analysis, evaluation, and risk treatment. The results of the research that has been carried out are 21 risks that may occur, namely there are 3 low-class risks, 15 medium-class risks, and 3 high-class risks. What can be done is to carry out the proposed recommendations so that the performance of the information system is more developed and gets better.
Keywords: *Risk management, information systems, telecommunication*

1. PENDAHULUAN

Perkembangan teknologi di Indonesia masih menjadi salah satu pusat perhatian masyarakat khususnya di era industri 4.0. Berkembangnya teknologi yang dimaksud adalah perubahan teknologi yang semakin canggih dan mengarah ke hal digital untuk mempermudah segala sesuatu agar bisa lebih efektif dan efisien. Banyak sekali hal-hal yang harus diperhatikan dalam revolusi industri 4.0 salah satunya yaitu *Internet of Things* (IoT). IoT menjadi bagian dari industri teknologi yang tengah menjadi bahan pembicaraan diberbagai kalangan, termasuk di kalangan industri telekomunikasi. Industri telekomunikasi ini dibutuhkan sebagai penyedia jaringan untuk menghubungkan satu sama lain pada sistem informasi di kehidupan sehari-hari maupun dunia kerja. Sistem informasi merupakan salah satu aset penting dalam sebuah organisasi maupun perusahaan untuk membuat aktivitas menjadi lebih mudah. Hal ini juga diterapkan pada salah satu perusahaan di Indonesia yaitu PT. XYZ, dimana PT. XYZ merupakan perusahaan yang bergerak dibidang telekomunikasi dengan menjalankan bisnis penyewaan tower, yang memiliki sistem informasi untuk mendukung proses bisnis yang dijalankan.

Dalam perkembangannya yang semakin pesat, kemungkinan ancaman dan risiko yang muncul juga harus menjadi perhatian karena berbagai ancaman dan risiko yang mengganggu dapat

melumpuhkan aktivitas kinerja di dalamnya, termasuk penggunaan sistem, sehingga sistem tidak berjalan secara optimal. Begitu juga halnya yang terjadi pada PT. XYZ dikarenakan masih menggunakan cara manual pada proses administrasi, data tidak terpantau dengan baik, dan lain sebagainya.

Berdasarkan hal tersebut, perlu adanya pengelolaan manajemen risiko yang baik. Manajemen risiko merupakan suatu proses pengendalian risiko yang bertujuan mengidentifikasi dan mengelola risiko dengan baik. Pada penelitian yang dilakukan oleh Gina, Ahmad dan Novia tahun 2022 [5], disampaikan bahwa manajemen risiko pada kerangka kerja ISO 31000:2018 dinilai efisien dalam mengelola suatu keadaan ketidakpastian dengan ditemukannya 15 kemungkinan risiko dari 5 tahapan manajemen risiko pada PT. Schlumburger. Kerangka kerja ISO 31000:2018 merupakan standar versi terbaru tentang manajemen risiko yang sudah dikembangkan oleh *International Organization for Standardization (ISO)*. Kerangka ini berfungsi untuk mengidentifikasi serta memperbaiki risiko yang ada pada organisasi maupun perusahaan.

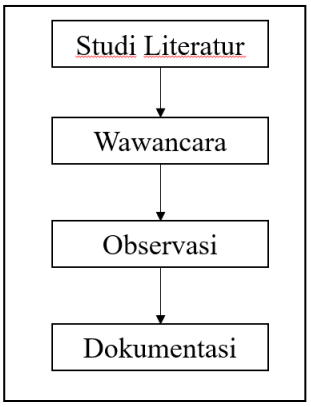
Berdasarkan penelitian sebelumnya, peneliti tertarik menggunakan kerangka kerja ISO 31000:2018 untuk melakukan analisis manajemen risiko pada PT. XYZ tepatnya pada direktorat *M*arketing. Selain terdapat cara kerja yang belum efektif dan efisien, direktorat *Marketing* pada PT.XYZ juga belum pernah dilakukannya manajemen risiko.

Hasil dari penelitian ini ialah untuk mendukung dan melindungi aset pada PT. XYZ dengan cara mengetahui tingkatan risiko pada penggunaan sistem informasi dan merancang strategi mitigasi untuk meminimalisir risiko yang akan terjadi. Dengan penelitian ini diharapkan dapat berdampak pada performa sistem informasi pada PT. XYZ untuk lebih berkembang dan menjadi lebih baik.

2. METODE PENELITIAN

Metode penelitian yang dilakukan yakni ada 2 yaitu pengumpulan data dan analisis data. Dimana penelitian ini termasuk ke dalam pendekatan deskriptif kualitatif sehingga tahapan pengumpulan data dilakukan untuk mendapatkan data terkait proses sistem informasi yang nantinya akan dilanjutkan dengan menganalisis data menggunakan kerangka kerja ISO 31000:2018.

2.1. Metode Pengumpulan data



Gambar 1. Tahapan Pengumpulan Data

2.1.1. Studi Literatur

Studi literatur sama dengan mempelajari buku maupun jurnal yang bertujuan untuk mendapatkan pemahaman terkait bahasan pada penelitian yang dilakukan.

2.1.2. Wawancara

Wawancara merupakan teknik pengumpulan data melalui tanyajawab dengan bertatapmuka secara langsung dengan narasumber. Hal ini bertujuan untuk mengetahui hal-hal yang lebih mendalam untuk menemukan permasalahan.

2.1.3. Observasi

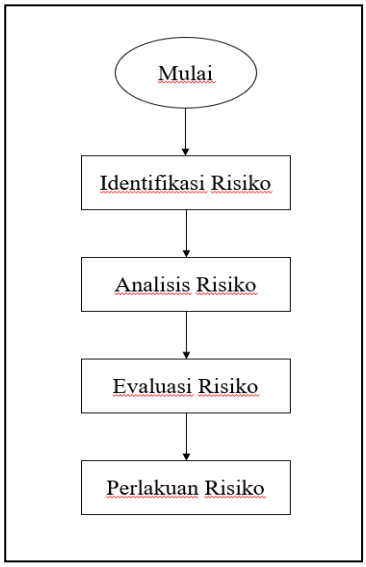
Observasi ialah teknik pengumpulan data dengan cara melihat dan mengamati secara langsung pada setiap objek yang dilakukan di lapangan. Melalui teknik ini, dapat menemukan hal yang lebih spesifik dibandingkan dengan teknik pengumpulan data lainnya.

2.1.4. Dokumentasi

Dokumentasi adalah cara pengumpulan data dengan membaca dan mencatat dokumen-dokumen yang ada pada objek studi kasus dengan masalah yang dibahas.

2.2. Metode Analisis Data

Analisis data merupakan proses untuk mencari dan menyusun data secara terstruktur dari penentuan masalah hingga pada pembuatan kesimpulan. Hal ini berdasarkan data yang diperoleh dari pengumpulan data yang telah dilakukan seperti studi literatur, wawancara, observasi, dokumentasi, dan lain sebagainya. Metode analisis data pada penelitian ini yakni menggunakan kerangka kerja ISO 31000:2018 yang bertujuan untuk mengidentifikasi kemungkinan ancaman risiko yang terjadi pada PT. XYZ. Berikut tahapan analisis data pada penelitian ini.



Gambar 2. Metode Analisis Data

2.2.1. Identifikasi Risiko

Hal yang dilakukan pada tahapan ini adalah identifikasi, menerima dan menjabarkan risiko untuk menunjang pencapaian pada sebuah organisasi/ perusahaan.

2.2.2. Analisis Risiko

Tahapan ini bertujuan untuk memahami sifat dan peringkat risiko dengan mempertimbangkan detail terkait sumber risiko, dampak, pengendalian risiko dan keefektifannya.

2.2.3. Evaluasi Risiko

Di tahapan ini, dilakukan evaluasi guna untuk memperbaiki dan membantu proses pengambilan keputusan berdasarkan evaluasi dengan mempertimbangkan risiko terhadap kriteria yang telah ditentukan. Untuk mengukur tingkat tinggi rendahnya sebuah risiko tersebut peneliti menggunakan tabel skala *likelihood* untuk menentukan golongan risiko seperti tinggi, sedang, dan rendah yang ditunjukkan pada tabel 1.

Tabel 1. Skala *Likelihood*

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*
		1	2	3	4	5
		Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
				Impact		

2.2.4. Perlakuan Risiko

Tahap selanjutnya, akan dilakukan penyeleksian opsi perlakuan risiko, perlakuan tanggap darurat, pemulihan bendana, dan menyiapkan serta melaksanakan perlakuan risiko.

3. HASIL DAN PEMBAHASAN

3.1. Hasil

3.1.1. Identifikasi Risiko

Tahapan ini bertujuan untuk mengetahui permasalahan dan menetapkan tujuan serta konsep yang akan dibawa dalam penelitian ini. Dari informasi yang sudah diperoleh akan diolah sesuai proses kerangka kerja pada manajemen risiko.

Tabel 2. Identifikasi Kemungkinan dan Dampak Risiko

No. Risiko	Kemungkinan Risiko	Dampak dari Risiko
KR01	*Human Error* (salah dalam *input* data, terjadi *input* berulang, ketidaksadaran dalam *input* data dan lainnya)	Proses pekerjaan selanjutnya terhadap data-data tersebut menjadi tidak valid sehingga dapat menimbulkan kerugian pada perusahaan
KR02	Kurangnya kuantitas SDM	Dibutuhkannya waktu yang lebih lama dalam proses pengerjaann
KR03	Adanya kebocoran atau kehilangan data	Hilangnya data-data perusahaan yang mengakibatkan penyalahgunaan data tersebut
KR04	UI sistem yang sulit dipahami	SDM yang mengoperasikan sistem sering mengalami kesalahan dikarenakan tampilan yang tidak *user friendly.*
KR05	Mantan karyawan masih memiliki akses informasi	Data perusahaan dapat tersebar dan disalahgunakan
KR06	Kurangnya transparansi dan koordinasi dengan *stakeholder*	Pekerjaan tidak sesuai dengan *timeline* yang sudah dibuat
KR07	Pemadaman listrik	Terhentinya proses bisnis dikarenakan wifi juga ikut mati sehingga tidak bisa melakukan penginputan data ke sistem
KR08	Koneksi jaringan bermasalah	Terhambatnya proses bisnis dikarenakan penginputan data ke sistem membutuhkan jaringan yang stabil
KR09	Tidak adanya arsip data	Tidak adanya arsip untuk data yang ada sehingga apabila terjadi kegagalan sistem maupun kehilangan data maka data tersebut tidak bisa diselamatkan
KR10	*Maintenance* sistem tidak terjadwal	Kurangnya kinerja sistem yang optimal yang akan mempengaruhi produktifitas, kualitas, efisiensi, dan lainnya
KR11	Data *corrupt*	*File* yang diberikan *error* sehingga tidak bisa melakukan penginputan maupun memproses data tersebut
KR12	Kurangnya kelengkapan data	Tidak dapat memproses data karena

		detail/ kelengkapan data yang diperlukan dalam proses yang dilakukan tidak ada
KR13	Terinfeksi virus	Perangkat akan mengalami kerusakan pada *software*
KR14	*Overcapacity* data	Data yang terbaru tidak masuk ke dalam sistem karena sistem yang ada sudah tidak dapat menampung lagi
KR15	Jaringan keamanan lemah	Jaringan mudah mengalami penyadapan
KR16	Data di sistem tidak diperbarui	Informasi yang didapatkan oleh pihak yang membutuhkan bukan data terbaru
KR17	Data tidak termonitor	Menyebabkan pengkategorian yang kurang tepat, adanya duplikat, dan progres dari data tersebut tidak terlihat
KR18	Pengumpulan data masih manual	data yang dikumpulkan membutuhkan waktu yang lama dan mempengaruhi keakuratan data
KR19	Tidak bisa melakukan *input* data karena *server down*	terhambatnya proses input data ke sistem karena penuhnya *traffic* yang menyebabkan server menjadi *down* atau *error* karena *hosting overload*
KR20	Tidak diterapkannya SOP untuk *input* data	Kurangnya kelengkapan data yang ada di sistem
KR21	*Database* tidak sinkron dengan data di sistem	kurangnya validitas data sehingga waktu yang dibutuhkan untuk proses bisnis yang dilakukan menjali lebih lama

3.1.2. Analisis Risiko

Dari data identifikasi dan dampak risiko pada sistem informasi pada PT. XYZ yang didapatkan dari wawancara dengan karyawan PT. XYZ dan observasi secara langsung. Berikut adalah hasil dari proses analisis risiko terhadap sistem informasi pada PT. XYZ yang ditunjukkan pada tabel 3, berdasarkan identifikasi kemungkinan dan dampak risiko pada tabel 2.

Tabel 3. Analisis Risiko

No. Risiko	Kemungkinan Risiko	*Likelihood*	*Impact*
KR01	*Human Error* (salah dalam *input* data, terjadi *input* berulang, ketidaksadaran dalam *input* data dan lainnya)	2	4
KR02	Kurangnya kuantitas SDM	2	4
KR03	Adanya kebocoran atau kehilangan data	1	5
KR04	UI sistem yang sulit dipahami	1	3
KR05	Mantan karyawan masih memiliki akses informasi	1	5
KR06	Kurangnya transparansi dan koordinasi dengan *stakeholder*	1	5

KR07	Pemadaman listrik	2	3
KR08	Koneksi jaringan bermasalah	3	4
KR09	Tidak adanya arsip data	1	4
KR10	*Maintenance* sistem tidak terjadwal	1	3
KR11	Data *corrupt*	3	3
KR12	Kurangnya kelengkapan data	3	5
KR13	Terinfeksi virus	1	5
KR14	*Overcapacity* data	1	3
KR15	Jaringan keamanan lemah	1	5
KR16	Data di sistem tidak diperbarui	1	4
KR17	Data tidak termonitor	3	5
KR18	Pengumpulan data masih manual	4	3
KR19	Tidak bisa melakukan *input* data karena *server down*	2	4
KR20	Tidak diterapkannya SOP untuk *input* data	2	4
KR21	*Database* tidak sinkron dengan data di sistem	3	5

3.1.3. Evaluasi Risiko

Evaluasi risiko dilakukan berdasarkan data analisis risiko yang telah dibuat pada tahapan sebelumnya. Cara yang digunakan untuk evaluasi risiko ini yaitu dengan menyesuaikan antara nilai *likelihood* dan *impact*. Dari sini akan terlihat pada 3 kuadran sesuai dengan level prioritas penanganan dari risiko-risiko tersebut. Berikut hasil perhitungan dari nilai *likelihood* dan nilai *impact* yang ditunjukkan pada tabel 4.

Tabel 4. Evaluasi Risiko

Likelihood		1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*
Certain	5					
Likely	4			KR18		
Possible	3			KR11	KR08	KR12, KR17, KR21
Unlikely	2			KR07	KR01, KR02, KR19, KR20	
Rare	1			KR04, KR10, KR14	KR09, KR16	KR03, KR05, KR06, KR13, KR15

Impact

3.1.4. Perlakuan Risiko

Setelah mendapatkan data dari proses evaluasi risiko, proses selanjutnya adalah perlakuan risiko. Tahapan ini merupakan sebuah Tindakan untuk meningkatkan peluang dan mengurangi ancaman dari kemungkinan dan dampak risiko yang ditimbulkan. Berikut hasil perlakuan risiko yang ditunjukkan pada tabel 5.

Tabel 5. Perlakuan Risiko

No. Risiko	Kemungkinan Risiko	*Risk Level*	Usulan
KR01	*Human Error* (salah dalam *input* data, terjadi *input* berulang, ketidaksadaran dalam *input* data dan lainnya)	*Medium*	Mengadakan pelatihan untuk karyawan secara berkala agar meminimalisir kesalahan dan memberikan teguran apabila sering melakukan kesalahan baik lisan maupun tertulis
KR02	Kurangnya kuantitas SDM	*Medium*	Menganalisis kebutuhan tenaga ahli pada direktorat yang dibutuhkan lalu merecruit tenaga sesuai jumlah yang dibutuhkan
KR03	Adanya kebocoran atau kehilangan data	*Medium*	Membatasi sistem keamanan dengan kontrol akses hanya untuk orang terpercaya yang dapat melihat data tersebut
KR04	UI sistem yang sulit dipahami	*Low*	Melakukan sosialisasi terkait UI yang digunakan agar seluruh SDM yang menggunakan UI sistem tersebut bisa memahami fitur yang tersedia
KR05	Mantan karyawan masih memiliki akses informasi	*Medium*	Menghapus akses karyawan tersebut setelah dinyatakan sudah tidak lagi bekerja di perusahaan
KR06	Kurangnya transparansi dan koordinasi dengan *stakeholder*	*Medium*	Mempublikasikan laporan pencapaian pada *website* dan memperkuat komunikasi dengan *stakeholder*
KR07	Pemadaman listrik	*Medium*	Menyiapkan generator set atau menggunakan koneksi data pribadi untuk melakukan penginputan
KR08	Koneksi jaringan bermasalah	*Medium*	Memperbarui antivirus, menggunakan *bandwidth management*, atau anti *spyware*. Apabila masih tidak bisa maka bisa mengunakan *browser* yang ringan
KR09	Tidak adanya arsip data	*Medium*	Membuat dan melaksanakan penjadwalan *backup* data secara berkala atau dapat disimpan pada *cloud storage*
KR10	*Maintenance* sistem tidak terjadwal	*Low*	Melakukan *maintenance* secara berkala untuk merawat dan menjaga sistem tetap pada kondisi yang baik sehingga dapat melakukan penginputan sesuai yang direncanakan

KR11	Data *corrupt*	*Medium*	Memasang antivirus untuk laptop yang digunakan atau saat melakukan penyimpanan *file* pastikan *file* tersebut sudah benar tersimpan
KR12	Kurangnya kelengkapan data	*High*	Membuat *database* terhadap setiap data yang akan maupun sudah diproses sebagai arsip maupun histori dan melakukan *update* pada *database* tersebut agar detail pada sebuah data tersimpan menjadi satu
KR13	Terinfeksi virus	*Medium*	Mempertebal pertahanan keamanan antivirus di komputer server hingga komputer karyawan
KR14	*Overcapacity* data	*Low*	Meningkatkan kapasitas storage untuk penyimpanan data dan menghapus data yang tidak diperlukan
KR15	Jaringan keamanan lemah	*Medium*	Memperbarui jaringan *software* jaringan secara berkala dan memastikan keamanannya diperkuat setiap melakukan *update*
KR16	Data di sistem tidak diperbarui	*Medium*	Melakukan sinkronisasi data di sistem secara berkala agar data selalu ter*update*
KR17	Data tidak termonitor	*High*	Membuat *dashboard* yang berisi terkait data-data *request* dan melakukan *controlling* terhadap progres dari data-data tersebut
KR18	Pengumpulan data masih manual	*Medium*	Membuat pengumpulan data secara otomatis baik menggunakan rumus maupun *coding*. Hal ini dapat meningkatkan keakuratan data
KR19	Tidak bisa melakukan *input* data karena *server down*	*Medium*	Meningkatkan kapasitas layanan hosting sehingga *website* bisa menghindari terjadinya server *down* pada saat terjadinya *traffic*
KR20	Tidak diterapkannya SOP untuk *input* data	*Medium*	Mempertegas penerapan SOP untuk penginputan data ke sistem sehingga kelengkapan data dapat terjamin
KR21	Database tidak sinkron dengan data di sistem	*Hard*	Menerapkan integrasi IT data secara berkala sehingga seluruh sistem terintegrasi dan satu perangkat dengan perangkat lain akan saling terhubung

Hasil yang didapatkan dari 4 tahapan yang telah dilakukan yaitu pada identifikasi masalah, peneliti mengumpulkan kemungkinan risiko yang terjadi melalui studi literatur dari berbagai jurnal seperti [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19] dan hasil observasi secara langsung olen peneliti melalui program *intern* sehingga peneliti mengetahui cara kerja yang diterapkan oleh direktorat *Marketing* dan menjadikannya

sebagai kemungkinan risiko, Lalu pada tahapan analisis risiko, hasil dari *likelihood* dan *impact* didapatkan dari hasil wawancara dengan karyawan dan kepala departemen dari direktorat *Marketing*. mewawancarai serta mengobservasi langsung proses bisnis yang dijalankan pada direktorat *Marketing* PT. XYZ. Tahapan selanjutnya yaitu evaluasi risiko didapatkan melalui *range* yang diberikan pada tahapan analisis dan menuangkannya pada tabel skala *likelihood* yang memiliki 3 golongan yaitu *low, medium* dan *hard.* Pada tahapan yang terakhir yaitu perlakuan risiko didapatkan dari usulan yang dilakukan peneliti dari berbagai aspek serta hasil diskusi bersama kepala departemen.

3.2. Pembahasan

Dari hasil penelitian yang telah dilakukan didapatkan 21 kemungkinan risiko yang terdiri dari 3 risiko level *high,* 15 risiko level *medium,* 3 risiko level *low* yang dapat terjadi pada sistem informasi direktorat *Marketing* PT. XYZ. Oleh karena itu, diberikan juga mitigasi yang dapat dilakukan untuk mencegah kemungkinan resiko itu terjadi sesuai pada tahapan metode ISO 31000:2018. Seperti pada penelitian sebelumnya oleh [1] memiliki 24 kemungkinan risiko yang dikategorikan level *high* sebanyak 3 risiko, level *medium* sebanyak 10 risiko dan level *low* sebanyak 11 risiko. Hal ini juga dilakukan oleh penelitian lainnya yang memiliki hasil kemungkinan risiko yang berbeda-beda dikarenakan studi kasus yang berbeda sehingga menghasilkan kemungkinan risiko yang berbeda juga. Walaupun memiliki hasil yang berbeda tetapi penelitian yang telah dilakukan memiliki tujuan yang sama yaitu untuk meminimalisir terjadinya risiko dengan menganalisis kemungkinan risiko dan memberikan mitigasi untuk mencegah risiko pada sebuah perusahaan maupun organisasi.

4. KESIMPULAN

Berdasarkan penelitian terkait analisis manajemen risiko menggunakan kerangka kerja ISO 31000:2018 pada direktorat *Marketing* di PT. XYZ. Kerangka kerja ini dilakukan melalui 4 tahapan yaitu pertama identifikasi risiko, yang menghasilkan kemungkinan risiko serta dampak yang dapat ditimbulkan. Kedua analisis risiko, yang menghasilkan *likelihood* serta *impact* dari kemungkinan risiko. Ketiga evaluasi risiko, yang menghasilkan skala likelihood berdasarkan tahapan analisis risiko. Keempat perlakuan risiko, yang menghasilkan usulan yang perlu dilakukan dari peneliti untuk meminimalisir kemungkinan risiko tersebut. Dari 4 tahapan yang telah dilakukan terdapat 21 risiko yang mungkin terjadi pada direktorat *Marketing* pada PT. XYZ. Pada risiko tersebut terdapat 3 golongan yaitu *low, medium dan high*. Adapun detail golongan dari 21 risiko tersebut, terdapat 3 risiko pada golongan *low* yaitu KR04, KR10, dan KR14. Pada golongan *medium* terdapat 15 risiko yaitu KR01, KR02, KR03, KR05, KR06, KT07, KT08, KR09, KR11, KR13, KR15, KR16, KR18, KR19 dan KR20. Lalu pada golongan *high* terdapat 3 risiko yaitu KR12, KR17, dan KR21.

Dari 21 risiko tersebut telah diberikan perlakuan risiko atau usulan yang dapat diimplementasikan oleh pihak direktorat *Marketing* PT. XYZ untuk pengembangan efisiensi proses bisnis yang berjalan. Adapun saran yang dapat dilakukan adalah dengan menjalankan saran-saran yang telah diusulkan dan melakukan *monitoring* serta *review* pada manajemen risiko secara berkala.

Referensi

[1] 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.

[2] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, "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, 2015.

[3] E. C. Sianipar, I. Santosa, and R. A. Nugraha, "Analisis Manajemen Risiko dan Kontrol pada Seksi Sistem Informasi Berdasarkan ISO 31000 Studi Kasus : Pt . Nusantara Regas," *e-*

Proceeding Eng., vol. 9, no. 2, pp. 610–618, 2022.
[4] L. D. Berliana and A. R. Tanamaah, "Analisis Risiko dengan Metode ISO 31000 pada Disperinnaker Kota Salatiga Bidang Industri," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 3, pp. 1105–1118, 2021, doi: 10.35957/jatisi.v8i3.1037.
[5] Gina Patriani Manuputty, "Analisis Manajemen Risiko Berbasis Iso 31000 Pada Aspek Operasional Teknologi Informasi Pt. Schlumberger Geophysics Nusantara," *Pap. Knowl. . Towar. a Media Hist. Doc.*, vol. 3, no. April, pp. 49–58, 2022.
[6] T. F. Rahardian and A. F. Wijaya, "Risk Analysis of Web-Based Information Systems on CV Mega Komputama Uses ISO 31000," *J. Inf. Syst. Informatics*, vol. 4, no. 2, pp. 428–443, 2022, [Online]. Available: http://journal-isi.org/index.php/isi
[7] Y. Erlika, M. I. Herdiansyah, and A. H. Mirza, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000," *J. Ilm. Inform. Glob.*, vol. 11, no. 1, 2020, doi: 10.36982/jig.v11i1.1073.
[8] E. A. Syahnur *et al.*, "Balance : Jurnal Akuntansi dan Manajemen," vol. 1, no. 3, 2022.
[9] A. A. Putri and D. I. Irnanda, "ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 (STUDI KASUS : APLIKASI J & T EXPRESS INDONESIA) Aisyah Journal of Informatics and Electrical Engineering Aisyah Journal of Informatics and Electrical Engineering," vol. 4, no. 1, pp. 1–9.
[10] F. Alfandy Firmanza and I. Helga Kurniawan, "Sistem Informasi Manajemen Risiko pada PT. XYZ Framework ISO 31000 Risk Management Information System at PT. XYZ Framework ISO 31000," vol. 4, no. 1, pp. 26–30, 2021.
[11] W. Harefa, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 1, pp. 407–420, 2022, doi: 10.35957/jatisi.v9i1.1478.
[12] H. C. Christian and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi pada BANK ABC menggunakan Framework ISO 31000," *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 1, pp. 735–748, 2022.
[13] G. K. Geofanny, A. R. Tanaamah, S. Informasi, F. T. Informasi, U. Kristen, and S. Wacana, "Sistem Manajemen Risiko Berbasis ISO 31000 : 2018 Di PT . Bawen Mediatama," vol. 9, no. 4, 2022.
[14] L. F. Putra, A. Profita, P. Studi, T. Industri, F. Teknik, and U. Mulawarman, "ANALISIS RISIKO WEBSITE TELKOM EMAS DATA VALIDATION MENGGUNAKAN ISO 31000," vol. 10, no. 2, pp. 175–183, 2022.
[15] D. Andika and A. Wijaya, "Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2018 Pada Pt. Trust Lerinvital Timur," *J. Mnemon.*, vol. 5, no. 2, pp. 111–118, 2022, doi: 10.36040/mnemonic.v5i2.4778.
[16] 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.
[17] V. P. P. Wijaya, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1295–1307, 2022, doi: 10.35957/jatisi.v9i2.2087.
[18] 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.
[19] D. Prabowo and A. F. Wijaya, "Risk Management Analysis on KKM LKF FTI UKSW Website Using ISO 31000 Framework," *J. Inf. Syst. Informatics*, vol. 4, no. 1, pp. 65–76, 2022, doi: 10.51519/journalisi.v4i1.219.