Matriks Evaluasi Risiko Penerapan IS/IT Menggunakan Standar ISO 31000:2018 (Studi Kasus: PT XYZ)

Ivana Celesta[#1], Maria Bellaniar Ismiati[#2]

[#]*Program Studi Sistem Informasi, Universitas Katolik Musi Charitas Palembang*
Jl. Bangau No. 60, Palembang, Indonesia

[1]ivana.celesta@gmail.com

[2]bella@ukmc.ac.id

Abstract*— PT XYZ is one of the largest trading companies in Palembang city. PT XYZ utilizes IS/IT to support its business processes. PT XYZ uses computers, LANs, servers, supported applications, and applications made by the IT team. IS/IT implementation at PT XYZ was not always smooth. PT XYZ had experienced problems, such as Wi-Fi problems, applications problems, not updated applications, and other human errors. PT XYZ has concerns that those problems will risk burdening the business processes in the company. The purpose of this research is to analyzee the risk of implementing IS/IT using the ISO 31000:2018 standard. All steps in IS/IT implementation risk management with ISO 31000:2018 standards have been implemented well at PT XYZ. From the results of this study, there are 21 possible risks with the risk management option plan chosen by the company, 10% risk is acceptable, 57% risk can be mitigated, 29% risk must be avoided, and 5% risk will be shared for handling the risk. Handling this risk is expected to assist the company in dealing with IS/IT implementation risks that can occur at any time.

***Keywords*— risk management, ISO 31000:2018, risk of implementation IS/IT, IS/IT risk, risk treatment**

Abstrak*— PT XYZ ialah salah satu perusahaan dagang terbesar di kota Palembang. PT XYZ memanfaatkan IS/IT untuk menunjang proses bisnisnya. PT XYZ menggunakan komputer, LAN, server, aplikasi pendukung, dan aplikasi buatan tim IT. Penerapan IS/IT di PT XYZ tidak selalu lancer. PT XYZ pernah mengalami kendala, seperti Wifi bermasalah, aplikasi bermasalah dan tidak ter-*update*, dan *human error* lainnya. PT XYZ memliki kekuatiran kendala yang sudah pernah terjadi tersebut akan berisiko membebani proses bisnis di perusahaannya. Tujuan penelitian ini adalah untuk menganalisis risiko penerapan IS/IT menggunakan standar ISO 31000:2018. Semua Langkah pada manajemen risiko penerapan IS/IT dengan standar ISO 31000:2018 telah diterapkan dengan baik di PT XYZ. Dari hasil penelitian ini terdapat 21 kemungkinan risiko dengan rencana opsi penanganan risiko yang dipilih perusahaan, yaitu 10% risiko dapat diterima, 57% risiko dapat dimitigasi, 29% risiko harus dihindari, dan 5% risiko akan dibagi untuk penanganan risikonya. Penanganan risiko ini diharapkan dapat membantu perusahaan dalam menghadapi risiko penerapan IS/IT yang dapat terjadi kapan saja.

***Kata Kunci*— manajemen risiko, ISO 31000:2018, risiko penerapan IS/IT, risiko IS/IT, penanganan risiko**

I. PENDAHULUAN

Information System and Information Technology (IS/IT), atau Sistem Informasi dan Teknologi Informasi, yang meningkat pesat menjadi peran penting untuk organisasi atau perusahaan untuk memberikan inovasi produk serta layanan menggunakan IS/IT. Menurut Astuti dalam [1], saat ini IS/IT digunakan di berbagai bidang kehidupan, seperti pendidikan, perbankan, kesehatan, telekomunikasi, dan bisnis. Menurut Ramdhany dan Krisdiawan dalam Larasati dalam [2], elemen dan komponen sistem yang dapat dijalankan dengan baik adalah hal yang penting untuk menunjang kinerja. IS/IT PT XYZ merupakan perusahaan dagang di kota Palembang yang menerapkan IS/IT di perusahaannya agar lebih efisien dan efektif. Menurut Marakas dan O'Brien dalam [3], IS adalah kombinasi dari orang, perangkat keras, perangkat lunak, jaringan komunikasi, sumber daya data, dan kebijakan dan prosedur untuk menyimpan, mengambil, mengubah, dan menyebarkan informasi dalam suatu organisasi. Menurut Kadir dalam [4], IT yang terdiri dari perangkat keras, perangkat lunak, dan jaringan komunikasi disebut sebagai teknologi informasi.

IS/IT di PT XYZ diterapkan pada semua divisi, yaitu *purchasing*, penjualan, keuangan dengan subdivisi IT, gudang, dan audit IAID. PT XYZ menggunakan seperangkat komputer, *server*, LAN, *Ms. Office*, dan aplikasi *web-based* buatan tim IT untuk aplikasi *purchasing*, penjualan, HRD, dan stok barang. Penerapan IS/IT di PT XYZ tidak selalu lancer. PT XYZ pernah mengalami masalah *Wi-Fi error*, aplikasi *error*, aplikasi tidak ter-*update*, dan *human error*. Komisaris PT XYZ memiliki kekhawatiran akan masalah-masalah terkait penggunaan IS/IT di perusahaan yang dapat menghambat jalannya proses bisnis dan mengurangi produktivitas karyawan, serta khawatir terhadap kemungkinan risiko lain yang mungkin terjadi di kemudian hari. Menurut Hanafi dalam [5], terdapat dua jenis risiko yaitu risiko murni dan risiko spekulatif.

Dalam penelitian ini akan dilakukan manajemen risiko yang dimulai dari identifikasi risiko, analisis risiko, evaluasi risiko, serta penanganan risiko pada penerapan IS/IT di PT XYZ menggunakan standar ISO 31000:2018 [6]. Alasan digunakannya standar ini karena standar ini merupakan versi terkini dari versi yang sebelumnya, yaitu ISO 31000:2009 [7].

Penelitian ini dilakukan agar perusahaan dapat mengelola risiko pada penerapan IS/IT dengan mengidentifikasi risiko, menganalisis risiko, mengevaluasi risiko, serta melakukan penanganan risiko yang kemungkinan akan terjadi. Tujuan penelitian ini yaitu untuk menganalisis risiko-risiko penerapan IS/IT (identifikasi risiko penerapan IS/IT, analisis risiko penerapan IS/IT, evaluasi risiko penerapan IS/IT, dan penanganan risiko penerapan IS/IT) dengan menggunakan standar ISO 31000:2018 di PT XYZ.

Penelitian ini diharapkan dapat menjadi bahan acuan bagi PT XYZ untuk mengetahui dan memahami risiko-risiko yang dapat muncul pada IS/IT yang digunakan. Penelitian ini juga dapat menjadi bahan evaluasi bagi PT XYZ dalam penerapan IS/IT untuk menunjang pelaksanaan proses bisnisnya. Diharapkan juga PT XYZ mampu melakukan mitigasi risiko dan manajemen risiko yang efektif dan efisien [8] sehingga mampu mencapai tujuan dan targetnya.

II. METODOLOGI

A. Jenis Penelitian

Jenis penelitian yang akan digunakan adalah wawancara serta observasi terhadap IS/IT yang digunakan pada PT XYZ untuk melakukan manajemen risiko. Penelitian ini merupakan jenis penelitian kualitatif.

B. Waktu dan Tempat Penelitian

Penelitian ini dilaksanakan di PT XYZ Palembang pada bulan Juni hingga Agustus.

PT XYZ merupakan perusahaan dagang yang terletak di kota Palembang. Sejak tahun 1996 PT XYZ mulai mendistribusikan produknya secara kecil-kecilan. Sejak saat itu distribusi produknya semakin lancar dan meningkat. Hal ini merupakan peluang yang baik bagi pemilik bisnis. Didukung oleh adanya permintaan pasar yang besar akan produknya, pemilik bisnis kemudian mulai memperluas bisnisnya hingga memiliki agen-agen besar. Perusahaan pun menjadi distributor produk. Perusahaan menguasai pasar produknya di kota Palembang. Perusahaan menyesuaikan diri dengan perkembangan jaman dengan menerapkan IS/IT pada semua kegiatan operasional sehari-hari.

C. Populasi dan Sampel Penelitian

Populasi dan sampel penelitian menggunakan teknik *purposive sampling*. Menurut Sugiyono dalam [9], *purposive sampling* merupakan teknik penentuan sampel dengan kriteria/pertimbangan tertentu. Kriteria sampel pada penelitian ini adalah karyawan PT XYZ yang menggunakan IS/IT untuk melaksanakan pekerjaannya. Populasi penelitian sebanyak 20 orang, sampel sebanyak 7 orang.

D. Teknik Pengumpulan Data

Untuk memperoleh data yang diperlukan untuk memenuhi tujuan penelitian, digunakan prosedur pengumpulan data. Proses pengumpulan data dilakukan dengan cara observasi dan wawancara.

E. Analisis Data

Langkah-langkah dalam analisis data yaitu dengan mengikuti kerangka kerja dan proses manajemen risiko sesuai standar ISO 31000:2018 sebagai berikut:

1. Mengajukan pertanyaan klausul kerangka kerja manajemen risiko ISO 31000:2018 kepada para pemangku kepentingan untuk mengetahui tingkat kematangan manajemen risiko perusahaan.
2. Melakukan penilaian manajemen risiko, yaitu identifikasi risiko IS/IT, analisis risiko IS/IT, dan evaluasi risiko IS/IT.
3. Melakukan penanganan untuk setiap risiko IS/IT sehingga dapat menentukan bagaimana masing-masing risiko akan ditangani. Penanganan risiko bisa berupa menerima risiko, menghindari risiko, membagi risiko, dan menghilangkan risiko. Setelah itu, ditentukan solusi penanganan masing-masing risiko yang didapatkan dari penilaian risiko.
4. Mendapatkan hasil keseluruhan manajemen risiko penerapan IS/IT pada PT XYZ setelah melakukan proses manajemen risiko,
5. Mendapatkan hasil dan kesimpulan penelitian.

F. Kerangka Kerja ISO 31000:2018

Kerangka kerja dirangkum dalam bentuk pertanyaan untuk memudahkan dalam memahami kerangka kerja manajemen risiko ISO 31000:2018. Hasilnya digunakan untuk mengetahui tingkat manajemen risiko suatu perusahaan. Panduan dalam pengisian respon untuk pertanyaan ini diuraikan berikut ini.

Pertanyaan diukur dengan memberikan nilai sebagai berikut dan disesuaikan dengan organisasi terkait.

0 = tidak ada
1 = ada hanya sebagian atau belum diterapkan
2 = ada dan telah diimplementasikan

Pertanyaan terkait klausul kerangka kerja ISO 31000:2018 dapat dilihat pada Tabel I.

Setelah mendapatkan nilai respon, maka langkah selanjutnya adalah menjumlahkan nilai tersebut dalam baris total. Total nilai yang didapatkan ini digunakan untuk mengetahui kategori kematangan manajemen risiko pada organisasi terkait dan dikonversi menjadi beberapa kategori, seperti pada Tabel II.

G. Proses Manajemen Risiko ISO 31000:2018

1) Komunikasi dan Konsultasi

Komunikasi dan konsultasi dilaksanakan selama proses manajemen risiko IS/IT berlangsung dengan subjek penelitian.

2) Scope, Context, Criteria

Menentukan ruang lingkup manajemen risiko, konteks eksternal dan internal perusahaan, dan kriteria manajemen risiko.

3) Risk Assessment

- Identifikasi Risiko

Melakukan identifikasi risiko penerapan IS/IT di PT XYZ sebagai langkah awal proses manajemen risiko, yaitu

TABEL I
PERTANYAAN KLAUSUL *FRAMEWORK*/KERANGKA KERJA ISO 31000:2018

No.	Pertanyaan	Respon
	Klausul 1: *Leadership and Commitment*	
1	Adakah menyesuaikan dan mengimplementasikan semua komponen kerangka kerja?	
2.	Adakah menerbitkan pernyataan atau kebijakan yang menetapkan pendekatan rencana, atau arah tindakan manajemen risiko?	
3.	Adakah memastikan sumber daya yang diperlukan dialokasikan untuk pengelolaan risiko?	
4.	Adakah menetapkan kewenangan, tanggung jawab dan akuntabilitas pada tingkat yang diperlukan dalam organisasi?	
	Klausul 2: *Integration*	
1.	Adakah risiko dikelola di semua bagian struktur organisasi?	
2.	Apakah setiap orang di organisasi bertanggung jawab terhadap pengelolaan risiko?	
	Klausul 3: *Design*	
1.	Adakah pemeriksaan organisasi dan konteksnya?	
2.	Adakah penegasan komitmen manajemen risiko?	
3.	Adakah penetapan peran, wewenang, tanggung jawab, dan akuntabilitas organisasi?	
4.	Adakah alokasi sumber daya?	
5.	Adakah penyiapan komunikasi dan konsultasi?	
	Klausul 4: *Implementation*	
1.	Adakah mengembangkan rencana yang sesuai, termasuk waktu dan sumber daya?	
2.	Adakah mengidentifikasi di mana, kapan, bagaimana, dan oleh siapa beragam jenis keputusan dibuat diseluruh organisasi?	
3.	Adakah memodifikasi proses pengambilan keputusan yang sesuai (jika diperlukan)?	
4.	Sudahkah memastikan pengaturan organisasi dalam mengelola risiko dipahami dengan jelas dan dipraktikkan?	
	Klausul 5: *Evaluation*	
1.	Adakah mengukur kinerja kerangka kerja manajemen risiko secara berkala terhadap tujuan?	
2.	Adakah menentukan apakah kerangka kerja manajemen risiko tetap sesuai untuk mendukung pencapaian sasaran organisasi?	
	Klausul 6: *Improvement*	
1.	Adakah organisasi secara berkelanjutan memantau dan mengadaptasi kerangka kerja?	
2.	Apakah organisasi secara berkesinambungan meningkatkan kesesuaian, kecukupan dan efektivitas kerangka kerja manajemen risiko?	

TABEL II
KESIMPULAN TOTAL NILAI KEMATANGAN MANAJEMEN RISIKO

Nilai	Kategori
0-7	*Risk Naïve* (Belum sadar risiko)
8-14	*Risk Aware* (Sadar risiko)
15-20	*Risk Defined* (Risiko ditetapkan)
21-25	*Risk Managed* (Risiko dikelola)
di atas 26	*Risk Enable* (Dapat menangani risiko)

dengan melakukan wawancara kepada masing-masing subjek penelitian.

- Analisis Risiko
  Menganalisis semua risiko yang ditemukan saat mengidentifikasi risiko dengan menentukan tingkat frekuensi dan tingkat dampak untuk masing-masing risiko yang didapatkan dari identifikasi risiko.
- Evaluasi Risiko
  Mengevaluasi tingkat kemungkinan risiko terjadi dan dampak yang diakibatkan jika risiko terjadi. Menggunakan matriks evaluasi risiko dalam penentuan level untuk masing-masing risiko. Setelah penilaian risiko dilakukan, hasilnya akan diberikan kepada stakeholder untuk memastikan tidak ada risiko yang terlewat untuk dinilai.

4) Penanganan Risiko

Jika telah dipastikan semua risiko sudah dinilai, selanjutnya melakukan penanganan risiko. Jika masih ada risiko yang belum dinilai, maka akan kembali ke tahap pertama penilaian risiko, yaitu identifikasi risiko. Penanganan risiko bisa dilakukan dengan mitigasi risiko, menghindari risiko, berbagi risiko, dan menerima risiko.

5) Monitoring dan Review

Pemantauan dan peninjauan dilakukan di semua tahap proses untuk memastikan dan meningkatkan kualitas dan efektivitas manajemen risiko penerapan IS/IT.

6) Recording dan Reporting

Setelah proses manajemen risiko dilakukan, akan dilaporkan dan didokumentasikan hasil manajemen risiko penerapan IS/IT menggunakan standar ISO 31000:2018 yang didapatkan.

III. HASIL DAN PEMBAHASAN

A. Kerangka Kerja Manajemen Risiko ISO 31000:2018

Hasil pertanyaan klausul *framework*/kerangka kerja ISO 31000:2018 didapatkan dengan mencari nilai rata-rata dari masing-masing respon yang diberikan oleh subjek penelitian. Tabel III memperlihatkan hasil pertanyaan klausul *framework*/kerangka kerja ISO 31000:2018.

TABEL III
HASIL PERTANYAAN KLAUSUL *FRAMEWORK*/KERANGKA KERJA ISO 31000:2018

No.	Pertanyaan	Respon
	Klausul 1: *Leadership and Commitment*	
1.	Adakah menyesuaikan dan mengimplementasikan semua komponen kerangka kerja?	0
2.	Adakah menerbitkan pernyataan atau kebijakan yang menetapkan pendekatan, rencana, atau arah Tindakan manajemen risiko?	0
3.	Adakah memastikan sumber daya yang diperlukan dialokasikan untuk pengelolaan risiko?	0
4.	Adakah menetapkan kewenangan, tanggung jawab dan akuntabilitas pada tingkat yang diperlukan dalam organisasi?	1
	Klausul 2: *Integration*	
1.	Adakah risiko dikelola di semua bagian struktur organisasi?	0
2.	Apakah setiap orang di organisasi bertanggungjawab terhadap pengelolaan risiko?	1
	Klausul 3: *Design*	
1.	Adakah pemeriksaan organisasi dan konteksnya?	0
2.	Adakah penegasan komitmen manajemen risiko?	0
3.	Adakah penetapan peran, wewenang, tanggung jawab, dan akuntabilitas organisasi?	1
4.	Adakah alokasi sumber daya?	0
5.	Adakah penyiapan komunikasi dan konsultasi?	1
	Klausul 4: *Implementation*	
1.	Adakah mengembangkan rencana yang sesuai, termasuk waktu dan sumber daya?	0
2.	Adakah mengidentifikasi di mana, kapan, bagaimana, dan oleh siapa beragam jenis keputusan dibuat diseluruh organisasi?	0
3.	Adakah memodifikasi proses pengambilan keputusan yang sesuai (jika diperlukan) ?	0
4.	Sudahkah memastikan pengaturan organisasi dalam mengelola risiko dipahami dengan jelas dan dipraktikkan?	0
	Klausul 5: *Evaluation*	
1.	Adakah mengukur kinerja kerangka kerja manajemen risiko secara berkala terhadap tujuan?	0
2.	Adakah menentukan apakah kerangka kerja manajemen risiko tetap sesuai untuk mendukung pencapaian sasaran organisasi?	0
	Klausul 6: *Improvement*	
1.	Adakah organisasi secara berkelanjutan memantau dan mengadaptasi kerangka kerja?	0
2.	Apakah organisasi secara berkesinambungan meningkatkan kesesuaian, kecukupan dan efektivitas kerangka kerja manajemen risiko?	0
	TOTAL	4

Total respon untuk pertanyaan klausul *framework*/kerangka kerja ISO 31000:2018 adalah 4. Setelah mendapatkan total respon hasil pertanyaan klausul *framework*/kerangka kerja ISO 31000:2018, maka nilai yang didapatkan akan dikonversikan sesuai Tabel IV.

TABEL IV
KESIMPULAN TOTAL NILAI KEMATANGAN MANAJEMEN RISIKO

Nilai	Kategori
0-7	*Risk Naïve* (Belum sadar risiko)
8-14	*Risk Aware* (Sadar risiko)
15-20	*Risk Defined* (Risiko ditetapkan)
21-25	*Risk Managed* (Risiko dikelola)
di atas 26	*Risk Enable* (Dapat menangani risiko)

Total respon adalah 4, artinya perusahaan atau organisasi masuk ke dalam kategori *Risk Naïve* atau belum sadar akan adanya risiko terutama risiko penerapan IS/IT di PT XYZ.

B. Proses Manajemen Risiko ISO 31000:2018

1) Komunikasi dan Konsultasi

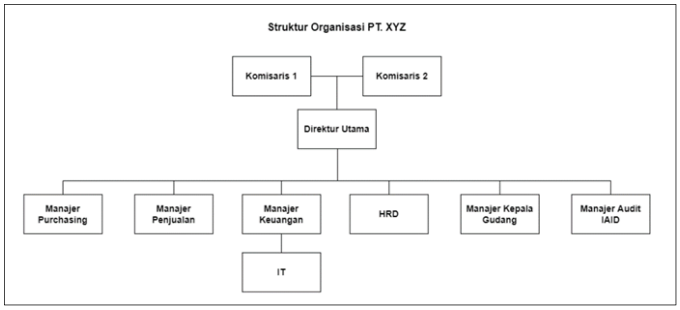
Komunikasi dan konsultasi dilakukan selama proses manajemen risiko penerapan IS/IT berlangsung untuk pertukaran informasi yang faktual, tepat waktu, relevan, akurat, dan dapat dimengerti, serta mendapatkan umpan balik dan informasi untuk mendukung pengambilan keputusan.

2) Ruang Lingkup, Konteks, dan Kriteria

a. Ruang Lingkup
Ruang lingkup pada penelitian ini yaitu penerapan IS/IT pada PT XYZ dalam menjalankan proses bisnisnya.

b. Konteks Internal

1. Sejarah PT XYZ
PT XYZ merupakan perusahaan dagang yang terletak di kota Palembang. Berdiri sejak 1996, PT XYZ mulai mendistribusikan produk secara kecil-kecilan. Sejak saat itu distribusi produknya semakin lancar dan meningkat. Bisnis diperluas ke toko-toko. Hingga kini perusahaan memiliki agen-agen besar dan perusahaan pun menjadi distributor produk. Perusahaan pun menguasai pasar produknya di kota Palembang.
2. Visi PT XYZ
"Menjadi perusahaan distributor terbaik yang kreatif, inovatif, dan dapat dipercaya oleh masyarakat Indonesia."
3. Misi PT XYZ
   - Berkomitmen mendistribusikan produk secara merata ke seluruh Nusantara serta meningkatkan layanan kepada pelanggan melalui berbagai program promosi.
   - Berkomitmen menjadi mitra terbaik bagi *supplier* agar dapat saling menguntungkan.
   - Berkomitmen meningkatkan kualitas sistem manajemen perusahaan secara efektif dan efisien sesuai SOP yang jelas, serta pembaruan teknologi yang cepat dan tepat.
   - Berkomitmen meningkatkan kesejahteraan karyawan serta melakukan pengembangan SDM melalui berbagai forum untuk mendapatkan



Gambar 1 Struktur organisasi PT XYZ

- karyawan profesional yang handal dan memiliki etos kerja yang baik.

4. Struktur Organisasi PT XYZ
   Struktur organisasi PT XYZ dapat dilihat pada Gambar 1.

c. Konteks Eksternal
   1. Pesaing
      Adanya pesaing produk membuat PT XYZ selalu berupaya agar bisnisnya dapat terus berjalan dengan berupaya meningkatkan efisiensi dalam material produk yang digunakan. Diharapkan dapat membuat produk yang ramah lingkungan namun tetap berkualitas baik dan mampu bersaing di pasarnya.
   2. Perkembangan Teknologi
      PT XYZ berupaya untuk mengikuti perkembangan teknologi dengan menggunakan aplikasi buatan Tim IT perusahaan. Tim IT juga melakukan *maintenance* pada aplikasi agar dapat digunakan secara maksimal guna mendukung proses bisnis perusahaan.

d. Kriteria Risiko
   Risiko pada penelitian ini terbagi ke dalam lima kriteria yaitu: risiko hardware, risiko software, risiko brainware, risiko jaringan/infrastruktur, dan risiko bencana alam.
   1. Penilaian Risiko
      a) Identifikasi Risiko
         i. Identifikasi Aset
            Identifikasi aset IS/IT di PT XYZ dapat dilihat di Tabel V.
         ii. Identifikasi Kemungkinan Risiko
            Terdiri dari 5 faktor, yaitu *hardware*, *software*, *brainware*, jaringan/infrastruktur, dan bencana alam. Identifikasi kemungkinan risiko penerapan IS/IT pada PT XYZ dapat dilihat Tabel VI.

TABEL V
IDENTIFIKASI ASET IS/IT DI PT XYZ

Aset	Jenis
Data	Data *Purchasing*
	Data Penjualan
	Data Keuangan
	Data IT
	Data Gudang
	Data HRD
	Data Audit IAID
Software	Aplikasi Ms. Word
	Aplikasi Ms. Excel
	Aplikasi Ms. Excel
	Aplikasi Purchasing
	Aplikasi Penjualan
	Aplikasi HRD
	Aplikasi Gudang/Stok Barang
Hardware	Komputer
	Keyboard
	Mouse
	Printer
	CPU
	Server
	Perangkat Jaringan
	WiFi
	Handphone

TABEL VI
IDENTIFIKASI KEMUNGKINAN RISIKO PENERAPAN IS/IT PT XYZ

Faktor	ID	Kemungkinan Risiko
Hardware	R01	Perangkat perlu di-*upgrade*
	R02	*Hardware* rusak
	R03	Debu atau kotoran
	R04	Listrik padam
Software	R05	Aplikasi yang digunakan mati tiba-tiba
	R06	Serangan virus
	R07	*Database error*
	R08	Gagal melakukan penyimpanan
	R09	*Hacking*
	R10	*Overload*
Brainware	R11	*Human error*
	R12	Kehilangan data
	R13	Penyalahgunaan hak akses
	R14	Kurangnya sumber daya manusia
	R15	*Maintenance* tidak terjadwal
	R16	Mantan karyawan masih memiliki akses informasi data penting
Jaringan/	R17	Koneksi jaringan terputus
Infrastruktur	R18	Kegagalan backup data
	R19	*Server down*
Bencana alam	R20	Kebakaran
	R21	Petir

iii. Identifikasi Dampak Risiko
   Identifikasi dampak risiko dilakukan untuk dapat mengetahui dampak yang ditimbulkan jika kemungkinan-kemungkinan risiko terjadi. Identifikasi dampak risiko dapat dilihat di Tabel VII.

TABEL VII
IDENTIFIKASI DAMPAK RISIKO

ID	Kemungkinan Risiko	Dampak Risiko
R01	Perangkat perlu di-*upgrade*	• Menghambat kinerja karyawan. • Proses kerja melambat.
R02	*Hardware* rusak	• Data pada perangkat hilang. • Perangkat harus diperbaiki jika memungkinkan. Jika tidak, harus diganti baru. • Pekerjaan terhambat.
R03	Debu atau kotoran	• Aplikasi tidak berjalan secara maksimal. • Perangkat *overheat* dan menjadi lambat.
R04	Listrik padam	• Perusahaan mengalami kerugian operasional. • Mengganggu proses kerja.
R05	Aplikasi yang digunakan mati tiba-tiba	• Kemungkinan hilangnya data. • Tidak bisa melakukan pekerjaan. • Data tidak tersimpan.
R06	Serangan *virus*	• Data pada perangkat hilang. • Proses kerja perangkat menjadi lambat. • Menghabiskan memori penyimpanan perangkat. • Merusak *file-file* pada komputer/ *file corrupt*.
R07	*Database error*	• Data tidak ter-*update*. • Data berpotensi hilang • Pekerjaan terhambat
R08	Gagal melakukan penyimpanan	• Data harus di-*input* ulang.
R09	*Hacking*	• Kebocoran data perusahaan. • Reputasi perusahaan menurun karena mudah diretas. • Kerugian materil.
R10	*Overload*	• Kinerja *server* menurun. • Proses *loading* lama.
R11	*Human error*	• Pekerjaan terhambat. • Data tidak valid.
R12	Kehilangan data	• Data hilang. • Pekerjaan terhambat karena harus *input* ulang data. • Data tidak sesuai fakta.
R13	Penyalahgunaan hak akses	• Kebocoran data dan informasi penting perusahaan. • Manipulasi data yang merugikan perusahaan.
R14	Kurangnya sumber daya manusia	• Beban kerja karyawan meningkat. • Pekerjaan terhambat.
R15	*Maintenance* tidak terjadwal	• Redundansi data. • Tidak mengetahui masalah pada setiap perangkat. • - Aplikasi *error*
R16	Mantan karyawan masih memiliki akses informasi data penting	• Kebocoran data perusahaan. • Manipulasi data yang merugikan perusahaan.
R17	Koneksi jaringan terputus	• Proses distribusi terhambat. • Pekerjaan terhambat.
R18	Kegagalan *backup* data	• Harus melakukan *backup* data dari awal. • Pekerjaan subdivisi IT terhambat. • Jadwal *backup* data terganggu.
R19	*Server Down*	• Aplikasi tidak bisa dioperasikan. • Kinerja karyawan menurun. • *Database* tidak bisa diakses. • Pekerjaan terhambat
R20	Kebakaran	• Sarana dan prasarana rusak. • Kerugian materil. • Aktivitas perusahaan terhambat.
R21	Petir	• Sarana dan prasarana rusak. • Pekerjaan terhambat

b) Analisis Risiko

Tahap selanjutnya adalah melakukan analisis risiko dengan menetapkan nilai kemungkinan risiko yang telah diidentifikasi berdasarkan kriteria kemungkinan dan dampak. Tingkat kemungkinan dan dampak yang digunakan adalah Tabel VIII dan Tabel IX. Analisis risiko didapat dengan mencari nilai rata-rata dari masing-masing respon subjek penelitian, yang dapat dilihat di Tabel X.

c) Evaluasi Risiko

Pada tahap ini akan ditentukan prioritas dalam penanganan penerapan IS/IT di PT XYZ berdasarkan level risiko yang diperoleh dari hasil analisis risiko pada tahapan sebelumnya. Menurut Badan Standarisasi Nasional dalam [10], evaluasi risiko menggunakan matriks evaluasi risiko yang dapat dilihat di Tabel XI.

TABEL VIII
TINGKAT KEMUNGKINAN

Kemungkinan		Deskripsi	Frekuensi Kejadian
Nilai	Kriteria		
1	Sangat Jarang	Risiko sangat jarang terjadi	>2 tahun
2	Jarang	Risiko jarang terjadi	1-2 tahun
3	Mungkin	Risiko cukup sering terjadi	7-12 bulan
4	Kemungkinan Besar	Risiko sering terjadi	4-6 bulan
5	Hampir Pasti	Risiko selalu terjadi	1-6 bulan

TABEL IX
TINGKAT DAMPAK

Dampak		Deskripsi
Nilai	Kriteria	
1	Tidak signifikan	Risiko tidak mengganggu aktivitas dan proses bisnis pada instansi.
2	Kecil	Aktivitas pada instansi sedikit terhambat, namun tidak mengganggu aktivitas inti pada instansi.
3	Sedang	Risiko mengganggu jalannya proses bisnis pada instansi, sehingga aktivitas bisnis sedikit terhambat.
4	Besar	Risiko menghambat hampir seluruh jalannya proses bisnis pada instansi.
5	Katastrope	Risiko mengganggu jalannya proses bisnis yang ada secara menyeluruh dan menghentikan aktivitas instansi secara total.

Masing-masing kemungkinan risiko akan diurutkan berdasarkan besaran risiko dan dikelompokkan berdasarkan level risikonya, pada Tabel XII.

Dengan melihat tabel di atas dapat diketahui bahwa dari total 21 kemungkinan risiko penerapan IS/IT di PT XYZ, terdapat 10 kemungkinan risiko dengan level sangat tinggi, 2 risiko dengan level tinggi, 2 risiko dengan level sedang, 6 risiko dengan level rendah, dan 1 risiko dengan level sangat rendah. Digambarkan menggunakan *pie chart* yang dapat dilihat di Gambar 2.

2. Penanganan Risiko

Terdapat empat pilihan/opsi dalam menangani risiko, yaitu menerima risiko, menghindari risiko, mitigasi/pengurangan risiko, dan membagi risiko. Penanganan untuk masing-masing risiko yang telah dinilai dapat dilihat pada Tabel XIII. Persentase opsi penanganan risiko digambarkan menggunakan *pie chart* yang dapat dilihat pada Gambar 3.

TABEL X
ANALISIS RISIKO

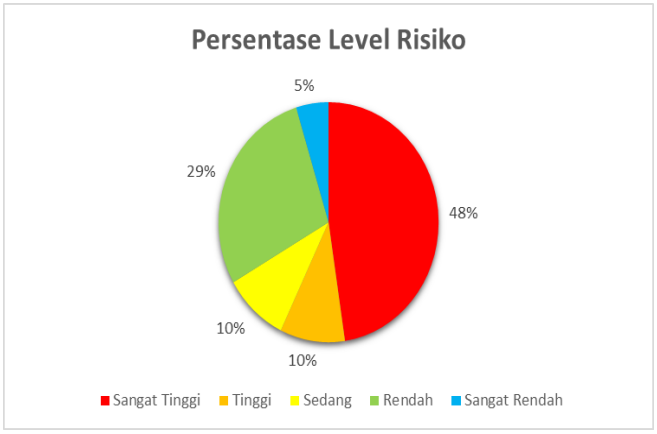
ID	Kemungkinan Risiko	Kemung-kinan	Dampak
R01	Perangkat perlu di-*upgrade*	2	2
R02	*Hardware* rusak	1	4
R03	Debu atau kotoran	2	3
R04	Listrik padam	3	5
R05	Aplikasi yang digunakan mati tiba-tiba	1	3
R06	Serangan *virus*	1	5
R07	*Database error*	1	4
R08	Gagal melakukan penyimpanan	3	5
R09	*Hacking*	1	5
R10	*Overload*	2	4
R11	*Human error*	3	4
R12	Kehilangan data	2	5
R13	Penyalahgunaan hak akses	1	5
R14	Kurangnya sumber daya manusia	1	4
R15	*Maintenance* tidak terjadwal	2	4
R16	Mantan karyawan masih memiliki akses informasi data penting	1	5
R17	Koneksi jaringan terputus	3	4
R18	Kegagalan *backup* data	2	5
R19	*Server down*	2	5
R20	Kebakaran	1	5
R21	Petir	1	4

TABEL XI
MATRIKS EVALUASI RISIKO PENERAPAN IS/IT DI PT XYZ

Matriks Evaluasi Risiko		Dampak				
		1	2	3	4	5
		Tidak signifikan	Kecil	Sedang	Besar	Kata-strope
Kemungkinan	5 Hampir Pasti					
	4 Kemung-kinan Besar					
	3 Mungkin					
	2 Jarang					
	1 Sangat jarang					

TABEL XII
KEMUNGKINAN RISIKO PENERAPAN IS/IT BERDASARKAN BESARAN RISIKO DAN LEVEL RISIKO

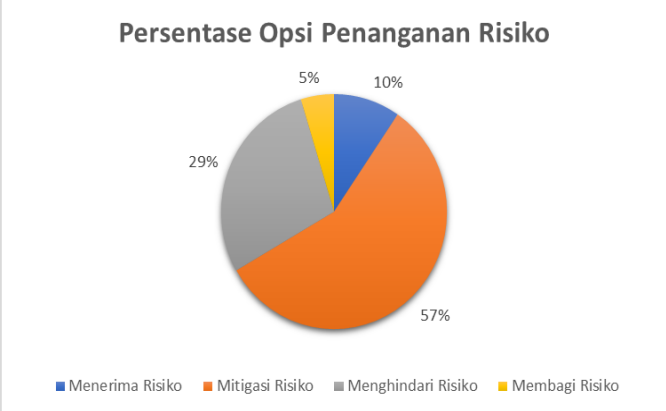
ID	Kemungkinan Risiko	Besaran Risiko	Level Risiko
R04	Listrik padam	22	Sangat Tinggi
R08	Gagal melakukan penyimpanan	22	Sangat Tinggi
R12	Kehilangan data	21	Sangat Tinggi
R18	Kegagalan *backup* data	21	Sangat Tinggi
R19	*Server down*	21	Sangat Tinggi
R06	Serangan *virus*	20	Sangat Tinggi
R09	*Hacking*	20	Sangat Tinggi
R13	Penyalahgunaan hak akses	20	Sangat Tinggi
R16	Mantan karyawan masih memiliki akses informasi data penting.	20	Sangat Tinggi
R20	Kebakaran	20	Sangat Tinggi
R11	*Human error*	17	Tinggi
R17	Koneksi jaringan terputus	17	Tinggi
R10	*Overload*	13	Sedang
R15	*Maintenance* tidak terjadwal	13	Sedang
R03	Debu atau kotoran	11	Rendah
R02	*Hardware* rusak	8	Rendah
R07	*Database error*	8	Rendah
R14	Kurangnya sumber daya manusia	8	Rendah
R21	Petir	8	Rendah
R01	Perangkat perlu di-*upgade*	7	Rendah
R05	Aplikasi yang digunakan mati tiba-tiba	5	Sangat Rendah



Gambar 2 Persentase level risiko penerapan IS/IT di PT XYZ

TABEL XIII
PENANGANAN RISIKO BERDASARKAN LEVEL RISIKO

ID	Kemungkinan Risiko	Level Risiko	Opsi Penanganan Risiko
R04	Listrik padam	Sangat Tinggi	Mitigasi risiko
R08	Gagal melakukan penyimpanan	Sangat Tinggi	Mitigasi risiko
R12	Kehilangan data	Sangat Tinggi	Menghindari risiko
R18	Kegagalan backup data	Sangat Tinggi	Mitigasi risiko
R19	*Server down*	Sangat Tinggi	Mitigasi risiko
R06	Serangan *virus*	Sangat Tinggi	Menghindari risiko
R09	*Hacking*	Sangat Tinggi	Menghindari risiko
R13	Penyalahgunaan hak akses	Sangat Tinggi	Menghindari risiko
R16	Mantan karyawan masih memiliki akses informasi data penting	Sangat Tinggi	Menghindari risiko
R20	Kebakaran	Sangat Tinggi	Membagi risiko
R11	*Human error*	Tinggi	Mitigasi risiko
R17	Koneksi jaringan terputus	Tinggi	Mitigasi risiko
R10	*Overload*	Sedang	Mitigasi risiko
R15	*Maintenance* tidak terjadwal	Sedang	Menghindari risiko
R03	Debu atau kotoran	Rendah	Mitigasi risiko
R02	*Hardware* rusak	Rendah	Mitigasi risiko
R07	*Database error*	Rendah	Mitigasi risiko
R14	Kurangnya sumber daya manusia	Rendah	Mitigasi risiko
R21	Petir	Rendah	Mitigasi risiko
R01	Perangkat perlu di-*upgade*	Rendah	Menerima risiko
R05	Aplikasi yang digunakan mati tiba-tiba	Sangat Rendah	Menerima risiko



Gambar 3 Persentase opsi penanganan risiko penerapan IS/IT di PT XYZ

3. Pemantauan dan Peninjauan Ulang
   Pada proses pemantauan dan peninjauan ulang, di PT XYZ telah direncanakan untuk pembentukan tim manajemen risiko sehingga pemantauan dapat lebih terfokus. Untuk peninjauan ulang manajemen risiko akan dilakukan dua tahun sekali, atau jika tidak memungkinkan, akan dilakukan tiga tahun sekali.
4. Pencatatan dan Pelaporan
   Pencatatan dan pelaporan dilakukan selama proses manajemen berlangsung. Untuk proses pencatatan telah dilakukan dalam penelitian ini selama proses manajemen risiko penerapan IS/IT berlangsung, sedangkan untuk pelaporan, laporan akan diberikan laporan dalam bentuk *hardcopy* kepada perusahaan. Laporan berisi hasil dari proses manajemen risiko penerapan IS/IT yang sudah dilakukan di PT XYZ.

C. Pembahasan

1) Level Risiko

a. Level risiko sangat tinggi
   Level risiko sangat tinggi mendominasi level risiko lainnya, dengan jumlah sebanyak 10 risiko dan persentase sebesar 48%. Level risiko ini mendominasi dikarenakan pada hasil wawancara subjek penelitian mengungkapkan bahwa kemungkinan risiko ini jarang hingga cukup sering terjadi di perusahaan. Namun, jika risiko ini terjadi dapat mengakibatkan terganggunya proses bisnis secara menyeluruh dan mengakibatkan terhentinya aktivitas di perusahaan secara total. Hal ini berdampak fatal bagi perusahaan sehingga perusahaan akan mengalami kerugian. Sepuluh risiko yang termasuk dalam level sangat tinggi di PT XYZ perlu tindakan segera untuk pengelolaan risikonya.
b. Level risiko rendah
   Level risiko rendah dengan jumlah sebanyak 6 risiko dan persentase sebesar 29%. Berdasarkan hasil wawancara dengan subjek penelitian, kemungkinan risiko ini jarang, bahkan sangat jarang terjadi di perusahaan. Jika risiko ini terjadi, dapat mengakibatkan terganggunya sebagian proses bisnis perusahaan dan sedikit menghambat proses bisnis perusahaan, serta dampaknya ringan bagi perusahaan. Perusahaan dapat melakukan beberapa penanganan untuk mengurangi tingkat kemungkinan dan tingkat dampak risiko di perusahaan. Enam risiko yang termasuk ke dalam level rendah di PT XYZ akan diambil tindakan penanganan risiko jika diperlukan.
c. Level risiko tinggi
   Level risiko tinggi dengan jumlah sebanyak 2 risiko dan persentase sebesar 10%. Berdasarkan hasil wawancara, subjek penelitian mengungkapkan bahwa kedua risiko ini cukup sering terjadi di perusahaan dan jika terjadi dampaknya mengganggu proses bisnis serta menghambat hampir seluruh aktivitas di perusahaan. Dua risiko yang termasuk ke dalam level tinggi di PT XYZ, diperlukan tindakan untuk pengelolaan risikonya.
d. Level risiko sedang
   Level risiko sedang dengan jumlah sebanyak 2 risiko dan persentase sebesar 10%. Berdasarkan hasil wawancara dengan subjek penelitian, kedua risiko ini jarang terjadi di perusahaan. Namun, jika terjadi, dapat mengakibatkan hampir seluruh proses bisnis di perusahaan terganggu dan mengakibatkan aktivitas di perusahaan sedikit terhambat. Dua risiko yang termasuk ke dalam level risiko sedang di PT XYZ, akan diambil tindakan penanganan risiko jika sumber daya tersedia.
e. Level risiko sangat rendah
   Level risiko sangat rendah dengan jumlah 1 risiko dan persentase sebesar 5%. Berdasarkan hasil wawancara dengan subjek penelitian, risiko ini sangat jarang terjadi di perusahaan. Apabila terjadi, dampaknya tidak terlalu mengganggu proses bisnis maupun aktivitas di perusahaan. Satu risiko yang termasuk dalam level sangat rendah di PT XYZ tidak diperlukan tindakan apapun.

2) Hubungan antara level risiko dengan opsi penanganan risiko

a. Risiko level sangat tinggi
   Dari 10 risiko dengan level sangat tinggi, opsi penanganan yang dipilih PT XYZ sebanyak 4 risiko dimitigasi, yaitu: risiko listrik padam, gagal melakukan penyimpanan, kegagalan *backup* data, dan *server down*; 5 risiko dihindari, yaitu: kehilangan data, serangan virus, *hacking*, penyalahgunaan hak akses, dan mantan karyawan masih memiliki akses informasi data penting; dan 1 risiko dibagi, yaitu kebakaran.
   Berdasarkan hasil wawancara, opsi penanganan dengan level sangat tinggi adalah dengan dimitigasi. Mitigasi dilakukan karena dapat mengurangi dampak yang diakibatkan bagi perusahaan, tidak menghambat pekerjaan, dan menjaga kinerja karyawan di perusahaan. Risiko dengan level sangat tinggi ini dihindari untuk mencegah terjadinya dampak yang sangat fatal bagi perusahaan dan mencegah terjadinya kerugian di perusahaan. Risiko dengan level sangat tinggi, yaitu risiko kebakaran, akan dibagi kepada pihak asuransi. Hal ini merupakan opsi terbaik agar perusahaan dapat melindungi gedung dan aset perusahaan, serta mengurangi dampak yang dapat terjadi sesuai dengan nilai pertanggungan yang disesuaikan dengan perusahaan.
b. Risiko level tinggi
   Dari 2 risiko dengan level tinggi, yaitu *human error* dan koneksi jaringan terputus, opsi penanganan yang dipilih yaitu mitigasi risiko. Mitigasi dilakukan oleh perusahaan agar dapat mengurangi penurunan kinerja karyawan dan mengurangi terjadinya kesalahan yang mungkin terjadi.

c. Risiko level sedang
Terdapat 2 risiko dengan level sedang, yaitu *overload* dan *maintenance* tidak terjadwal. Opsi penanganan yang dipilih untuk risiko *overload*, yaitu mitigasi risiko, agar jam kerja karyawan dapat digunakan dengan maksimal dan meningkatkan kinerja karyawan. Opsi penanganan yang dipilih untuk risiko *maintenance* tidak terjadwal, yaitu menghindari risiko. Jika risiko terjadi, dapat menghambat pekerjaan dan menimbulkan dampak pada jam kerja yang tidak digunakan dengan maksimal.

d. Risiko level rendah
Terdapat 6 risiko dengan level rendah, yaitu debu atau kotoran, *hardware* rusak, *database error*, kurangnya sumber daya manusia, petir, dan perangkat perlu di-*upgrade*. Opsi penanganan yang dipilih untuk risiko perangkat perlu di-*upgrade*, yaitu menerima risiko. Berdasarkan wawancara dengan subjek penelitian, tidak ada tindakan yang dapat dilakukan selain menerima risiko tersebut dan dampak yang diakibatkan tidak mengganggu aktivitas karyawan. Lima risiko lainnya dimitigasi karena dapat dilakukan berbagai penanganan sesuai dengan masing-masing risiko. Hal ini dilakukan agar dampak yang diakibatkan oleh risiko dapat berkurang.

e. Risiko level sangat rendah
Terdapat 1 risiko dengan level sangat rendah, yaitu aplikasi yang digunakan mati tiba-tiba. Opsi penanganan yang dipilih adalah menerima risiko. Risiko ini diterima karena, menurut subjek penelitian, tidak ada tindakan yang perlu dilakukan sehingga perusahaan hanya bisa menerima risiko tersebut.

IV. KESIMPULAN

Proses manajemen risiko penerapan IS/IT menggunakan standar ISO 31000:2018 telah dilaksanakan dengan baik di PT XYZ. Hal ini dibuktikan dengan telah diterapkannya semua langkah-langkah manajemen risiko sesuai dengan standar ISO 31000:2018.

Berdasarkan hasil dan pembahasan penelitian manajemen risiko penerapan IS/IT di PT XYZ, disimpulkan bahwa opsi penanganan risiko yang paling sering dipilih, yaitu mitigasi risiko dengan melakukan penanganan yang terencana dan berkelanjutan agar bisa mengurangi dampak dari masing-masing risiko yang dapat merugikan perusahaan. Opsi penanganan risiko yang paling jarang dipilih, yaitu membagi risiko karena hanya beberapa risiko yang dapat dibagi kepada pihak ketiga.

Perusahaan yang bergerak di bidang distribusi produk (PT XYZ) didominasi oleh risiko penerapan IS/IT dengan level yang sangat tinggi karena PT XYZ belum pernah melakukan manajemen risiko.

Oleh karena itu, disarankan agar perusahaan mengajukan standarisasi ISO 31000:2018 kepada Badan Standarisasi Nasional (BSN) untuk semua ruang lingkup di perusahaan sehingga dapat meningkatkan kredibilitas perusahaan. Perusahaan juga dapat mengimplementasikan penanganan risiko dan melanjutkan proses manajemen risiko ke tahap pemantauan dan peninjauan ulang sesuai yang direncanakan dalam 2 tahun sekali dengan tim internal manajemen risiko PT XYZ. Diharapkan level risiko dari masing-masing kemungkinan risiko penerapan IS/IT dapat menurun jika berada pada level sangat tinggi, tinggi, dan sedang, serta dapat mempertahankan level risiko sangat rendah dan rendah.

Pengembangan penelitian selanjutnya disarankan untuk menggunakan standar atau kerangka kerja lainnya dan melakukan manajemen risiko dengan lebih spesifik, seperti manajemen risiko keamanan data dengan menggunakan gabungan antara standar ISO 31000:2018 dan ISO/IEC 27002:2022, atau lain sebagainya.

DAFTAR REFERENSI

[1] N. F. Astuti, "Manfaat Teknologi Informasi di Berbagai Bidang, Memudahkan Kehidupan Manusia." *Merdeka* (30 Desember 2020). [Daring]. Tersedia: https://www.merdeka.com/jabar/manfaat-teknologi-informasi-di-berbagai-bidang-memudahkan-kehidupan-manusia-kln.html

[2] D. Larasati, "Manajemen Risiko pada Sistem Informasi Distribusi Produk Menggunakan ISO 31000:2009 (Studi Kasus: PT Sinar Niaga Sejahtera Distributor Produk Garudafood Depo Lahat)," Skripsi, Prodi Sistem Informasi Universitas Sriwijaya, Palembang, 2021.

[3] G. M. Marakas dan J. A. O'Brien, *Pengantar Sistem Informasi (Introduction to Information Systems)*, Ed. 16. Jakarta: Salemba Empat, 2017.

[4] A. Kadir, *Pengenalan Sistem Informasi*, Revisi. Yogyakarta: Andi, 2014.

[5] D. M. M. Hanafi, *Manajemen Risiko*, Ed. 1. Yogyakarta: Unit Penerbit dan Percetakan Sekolah Tinggi Ilmu Manajemen YKPN, 2006.

[6] ISO, "ISO 31000:2018 Risk Management - Guidelines," 2018. [Daring]. Tersedia: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en [21 Feb 2022].

[7] ISO, "ISO 31000:2009 Risk Management - Principles and Guidelines," 2009. [Daring]. Tersedia: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en [21 Feb 2022].

[8] S. A. K. Rafiie, *Manajemen: Teori dan Aplikasi*, Ed. 1. Bandung: Alfabeta, 2017.

[9] Sugiyono, *Metode Penelitian Bisnis*, Ed. 1, Bandung: Alfabeta, 2014.

[10] Badan Standardisasi Nasional, "Penerapan Manajemen ISO 31000:2018," hlm. 173, 2018. [Daring]. Tersedia: http://www.hzg.de/imperia/md/content/gkss/zentrale_einrichtungen/bibliothek/berichte/gkss_berichte_2008/gkss_2008_1.pdf

Ivana Celesta, kelahiran kota Palembang. Saat ini merupakan mahasiswi Universitas Katolik Musi Charitas Palembang dengan Program Studi S1 Sistem Informasi angkatan 2018. Merupakan penerima beasiswa Siswa Berprestasi Universitas Katolik Musi Charitas Palembang.