



Penerapan ISO 31000:2018 untuk Analisis Manajemen Risiko pada Sistem Informasi Smart Operation di PT. XYZ

Jericho¹, Endang Haryani²

^{1,2}Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia

Email: ¹1682020014@student.uksw.edu, ²endang_hry@uksw.edu

Abstract

This study objectives to analyze risk management on the Information System of Smart Operation at PT. XYZ, through identifying risks, describing the impact of these risks, and recommending risk treatment. This system manages sales transactions, from sales orders to financial reporting. This study is driven by the importance of information technology investment to improve a company's efficiency. However, this investment has uncertainties about the values that can be attained and the risks that may occur. The research applied a qualitative method and ISO 31000:2018 as the referred framework. The analysis identified 12 risks in the 5 sectors. The research found that there is no high-level risk, 8 medium-level risks and 4 low-level risks. Based on these findings, the study concludes that related to the implementation of the information system, there are no risks that endanger and harm the company. Based on the risk impact, the recommended risk treatment is to mitigate or reduce risks. There are 4 medium risks that have the greatest score of 6, among others are order recording errors, number of goods decrease, accidental loss of goods/theft, and wrong goods selection. Actions to reduce the risk are regular log checking, training on the use of applications, regular stock-opname, placing goods within CCTV range and rechecking documents with goods sent. Meanwhile, the risk of counterfeit money has the least score of 1, because the company has an accurate detection device.

Keywords: ISO 31000:2018; Information System; Risk; Risk Impact; Risk Treatment

Abstrak

Penelitian ini bertujuan untuk menganalisis manajemen risiko pada Sistem Informasi Smart Operation di PT. XYZ, melalui identifikasi risiko, deskripsi dampak yang ditimbulkan oleh risiko tersebut, dan rekomendasi perlakuan risiko. Sistem informasi ini mengelola transaksi penjualan yang mencakup penanganan order penjualan hingga pelaporan keuangan. Penelitian ini didorong oleh pentingnya investasi teknologi informasi untuk meningkatkan efisiensi operasional perusahaan. Namun, investasi ini seringkali disertai dengan ketidakpastian mengenai manfaat yang diperoleh dan risiko yang mungkin muncul. Riset ini menerapkan metode kualitatif dan ISO 31000:2018 sebagai framework yang dirujuk. Analisis penilaian risiko mengidentifikasi 12 risiko untuk 5 sektor risiko. Penelitian ini menemukan bahwa tidak ada risiko tinggi, 8 risiko menengah dan 4 risiko rendah. Berdasarkan temuan ini, penelitian ini menyimpulkan bahwa terkait dengan implementasi Sistem Informasi Smart Operation di PT. XYZ, tidak ada risiko yang membahayakan dan merugikan perusahaan. Berdasarkan dampak risiko tersebut, perlakuan risiko yang direkomendasikan adalah untuk melakukan mitigasi atau pengurangan risiko. Terdapat 4 risiko menengah yang memiliki dampak paling besar dengan skor 6 adalah kesalahan pencatatan order, penurunan jumlah barang, kehilangan barang disengaja/pencurian, dan kesalahan pemilihan barang. Tindakan untuk menurunkan risiko pada 4 hal ini adalah pengecekan log secara berkala, training penggunaan aplikasi, stock opname secara berkala, penempatan barang dalam jangkauan CCTV dan pengecekan ulang dokumen dengan barang dikirim. Sedangkan risiko adanya uang palsu adalah yang memiliki dampak paling kecil dengan skor 1, karena perusahaan memiliki alat pendeteksi yang akurat.

Kata kunci: ISO 31000:2018; Sistem informasi; Risiko; Dampak Risiko; Perlakuan Risiko

1. PENDAHULUAN

Pada era modern ini, Teknologi Informasi (TI) menjadi hal yang umum digunakan di berbagai organisasi. Kehadiran TI tentunya memberikan dampak baik pada perusahaan, seperti mampu meringankan prosedur kompleks dalam operasional perusahaan, meningkatkan kinerja pegawai, dan meningkatkan efisiensi serta kinerja perusahaan [1], [2], [3]. Meski demikian, pengembangan dan pengimplementasian TI memerlukan investasi yang tentunya tidak sedikit [4], [5]. Investasi TI ini diharapkan memberikan manfaat yang signifikan pada proses bisnis organisasi. Namun ada ketidakpastian seberapa besar manfaat yang akan dihasilkan, apakah berdampak luar biasa atau malah tidak membantu apapun dalam proses bisnis. Oleh karena itu, pengelolaan/manajemen atas ketidakpastian atau risiko TI tersebut menjadi suatu hal yang diperlukan perusahaan [6]. Selain perusahaan dapat mengelola risiko yang terjadi dan bahkan mengurangi dampak yang dihasilkan risiko tersebut [7], [8], juga dapat memastikan bahwa tujuan investasi TI dapat tercapai.

Salah satu perusahaan yang menerapkan TI adalah PT. XYZ. Perusahaan ini bergerak dalam bidang distribusi produk-produk yang terkait dengan perawatan pribadi, rumah tangga, minuman dan makanan, yang beroperasi di daerah Purworejo. Perusahaan telah mengimplementasikan TI dalam bentuk sistem informasi terintegrasi dalam pengelolaan transaksi penjualan yaitu Sistem Informasi *Smart Operation*. Pengelolaan data transaksi mencakup penanganan order penjualan, inventori atau barang dagangan, pengiriman, penagihan, penerimaan kas hingga pelaporan keuangan. Sistem informasi ini membantu kegiatan bisnis perusahaan dari pendataan, pengelolaan dan pelaporan transaksi. Dari pengelolaan transaksi tersebut, ada potensi risiko yang terjadi. Misalnya dalam penanganan order penjualan, ada risiko data order tidak lengkap. Hal ini dapat mengakibatkan kesalahan pengiriman. Sedangkan terkait penanganan inventori atau barang dagangan, ada kemungkinan terjadi kehilangan karena pencurian. Hal ini mempengaruhi ketersediaan barang dan menimbulkan kerugian materi. Dalam pengiriman pun juga berpotensi menimbulkan risiko, seperti adanya kesalahan dalam pengiriman barang ataupun kehilangan barang. Hal ini juga dapat mempengaruhi penagihan dan penerimaan kas karena ada barang yang tidak sesuai dengan order.

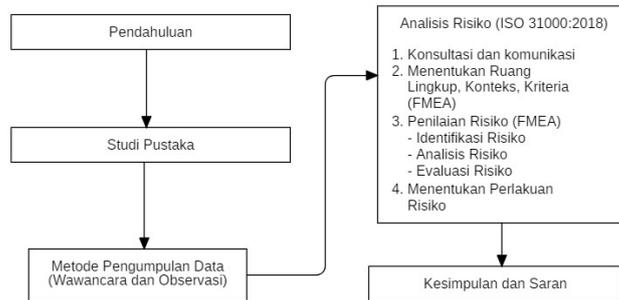
Pengelolaan risiko dapat dikaji menggunakan berbagai *framework*, salah satu *framework* yang sering diterapkan adalah ISO 31000. Studi terdahulu terkait manajemen risiko sistem informasi menggunakan ISO 31000 antara lain penelitian [9], [10], [11], [12], [13], [14]. Penelitian tersebut menginvestigasi risiko pada sistem informasi, yaitu SAP pada PT Serasi Autoraya [9], Aplikasi *Smart Canteen* pada SMA XYZ [10], Aplikasi *Point of Sales* pada perusahaan Tripio Purwokerto [11], SAP pada PT. XYZ [12], Sistem Informasi pembangunan Daerah [13], dan Sistem Informasi Kesejahteraan Sosial-*Next Generation* [14]. Penelitian [9] menemukan dua kemungkinan risiko berlevel tinggi, berkaitan terhadap pemadaman listrik dan gangguan internet sehingga dapat menghambat aktivitas bisnis yang ada pada PT Serasi Autoraya, lalu ditemukan tujuh potensi risiko menengah, dan enam potensi risiko rendah. Riset [10] mengidentifikasi satu

kemungkinan risiko tingkat ekstrim pada Aplikasi *Smart Canteen* yaitu penyalahgunaan hak akses, dua risiko tingkat tinggi, empat risiko tingkat sedang, dan lima risiko tingkat rendah. Dari semua risiko tersebut dilakukan mitigasi risiko untuk mengurangi ancaman dari dampak risiko tersebut. Penelitian [11] menganalisis enam risiko tingkat tinggi, tujuh risiko tingkat menengah, dan dua risiko tingkat rendah. Penelitian [12] menemukan 26 risiko, dimana 15 risiko dikategorikan sebagai risiko tingkat rendah, 5 risiko tingkat menengah, 5 risiko tingkat menengah ke atas, dan 1 risiko tingkat tinggi. Penelitian [13] mengkaji tentang SIPD dan menemukan 17 kemungkinan risiko yang dapat terjadi yang diantaranya ada tiga risiko pada tingkat tinggi, dua risiko pada tingkat sedang, dan 12 risiko pada tingkat rendah. Perlakuan risiko yang dilakukan contohnya pada risiko level tinggi adalah dengan melakukan prinsip kehati-hatian, backup data, dan pengintegrasian sistem untuk meningkatkan pengawasan. Penelitian terakhir pada Sistem Informasi Kesejahteraan Sosial *Next Generation* [14] ditemukan 16 kemungkinan risiko, yang 3 diantaranya termasuk dalam risiko berlevel tinggi, 8 risiko pada level *medium*, dan 5 risiko pada level *low*.

Dari pemetaan diatas dapat diketahui bahwa ISO 31000 masih menjadi *framework* yang relevan dan efektif dalam manajemen risiko. Di sisi lain, analisis risiko sistem informasi belum pernah dilakukan pada aplikasi Smart Operation di PT. XYZ. Selama ini manajemen risiko yang dilakukan oleh pihak internal perusahaan dilakukan berdasarkan hasil temuan audit tahunan. Dengan demikian, ada kebutuhan perusahaan akan manajemen risiko atas implementasi sistem informasi Smart Operation ini, namun faktanya saat ini belum ada kajian khusus manajemen risiko pada aplikasi ini. Mempertimbangkan celah risiko yang terjadi dan kemampuan ISO 31000 dalam pengelolaan risiko sistem informasi, maka penelitian ini bertujuan untuk menganalisis manajemen risiko pada Sistem Informasi aplikasi Smart Operation di PT. XYZ. Analisis ini secara khusus akan mengidentifikasi kemungkinan risiko yang terjadi, mendeskripsikan tingkat atau besar dampak yang ditimbulkan oleh risiko tersebut, dan memberikan usulan terhadap perlakuan risiko yang ada. Penelitian ini diharapkan dapat menyajikan gambaran tentang pengelolaan risiko pada sistem informasi Smart Operation.

2. METODOLOGI PENELITIAN

Penelitian ini mengaplikasikan metode deskriptif kualitatif, yang dilakukan dengan cara memahami peristiwa yang terjadi pada perusahaan, sehingga peneliti dapat memperoleh gambaran yang utuh dan penjelasan menyeluruh mengenai masalah yang diteliti [15]. Penelitian ini merujuk pada framework ISO 31000:2018 [16]. *Framework* ini berisi *guidelines*/panduan analisis pengelolaan risiko dan merupakan sebuah standar yang menjadi pedoman bagi organisasi maupun korporasi dalam pengelolaan risiko [17]. Bagian tidak terpisahkan dari *framework* ini adalah IEC 31010 yang menjelaskan beberapa teknik penilaian risiko yang dapat digunakan. Teknik penilaian risiko yang dipilih pada penelitian ini adalah model FMEA (*Failure Modes and Effects Analysis*) [18].



Gambar 1. Tahapan Penelitian

Gambar 1 mendeskripsikan langkah-langkah pada penelitian ini. Tahap pertama adalah penelitian pendahuluan, yang mencakup mengidentifikasi masalah, menetapkan ruang lingkup penelitian, merumuskan tujuan penelitian. Penelitian dilanjutkan dengan studi pustaka untuk memahami cara kerja manajemen risiko melalui teori dan penerapannya pada penelitian yang relevan. Data utama dalam riset ini diperoleh melalui interview dengan Kepala Operasional, staf Bagian Ekspedisi, dan staf Bagian Keuangan dan observasi langsung, khususnya pada proses bisnis pengelolaan penjualan pada Sistem Informasi Smart Operation. Sedangkan data sekunder dikumpulkan dari analisis dokumen dan catatan.

Berikutnya adalah langkah penilaian risiko (*risk assessment*) berdasarkan ISO 31000:2018 [19]. Tahap-tahapannya sebagai berikut:

a) Komunikasi dan konsultasi.

Pada tahap ini, diskusi fokus pada langkah-langkah penilaian risiko secara menyeluruh. Sehingga kedua belah pihak, peneliti dan perusahaan, memahami bersama tentang risiko, dan rangkaian mekanisme manajemen risiko, serta data dan informasi yang dibutuhkan.

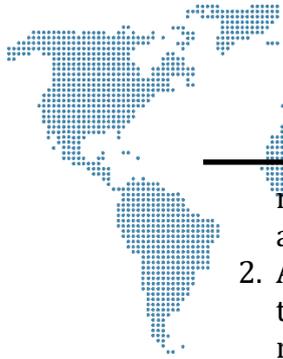
b) Penentuan ruang lingkup, konteks dan kriteria.

Pada tahapan ini mendefinisikan ruang lingkup dan konteks penilaian secara tepat [16]. Ruang lingkup dan konteks pada penelitian ini adalah mengidentifikasi potensi risiko yang akan terjadi dan mengelompokkannya berdasarkan kriteria risiko. Risiko dibatasi dalam konteks proses bisnis untuk pengelolaan transaksi penjualan menggunakan Sistem Informasi *Smart Operation*. Sedangkan kriteria mencakup kriteria risiko yang terdiri dari *likelihood* dan *impact* dalam mengukur tingkat risiko.

c) Penilaian risiko

Teknik penilaian risiko pada riset ini adalah FMEA (*Failure Modes and Effects Analysis*). Teknik ini mengidentifikasi risiko yang mungkin terjadi, seberapa besar kemungkinan terjadinya, seberapa jauh dampaknya pada organisasi jika risiko tersebut terjadi dan melanjutkan analisis kritis untuk setiap risiko [19]. Teknik FMEA ini dipilih karena mencakup menentukan peringkat risiko, sehingga mempermudah pengambilan keputusan untuk perlakuannya [19]. Adapun tahapannya sebagai berikut [18]:

1. Identifikasi risiko (*risk identification*) melalui interview dan observasi untuk menginvestigasi opsi yang ada dalam program aplikasi, kemudian



menemukan potensi ancaman dan dampak dari tiap-tiap pilihan fitur yang ada dalam sistem informasi.

2. Analisis risiko (*risk analysis*) mengkombinasikan dan mengukur peluang terjadinya risiko dengan imbas dari risiko, agar dapat dijadikan input dalam mengevaluasi penetapan preferensi risiko bagi perusahaan. Untuk itu dibutuhkan kriteria risiko. Kriteria *likelihood* digunakan untuk menentukan seberapa sering terjadinya risiko, sedangkan kriteria *impact* digunakan untuk menentukan seberapa besar dampak kerugian risiko terhadap perusahaan. Kedua kriteria tersebut dikalikan untuk menghitung nilai risiko.
3. Evaluasi risiko (*risk evaluation*) memetakan risiko pada 3 ruang, yaitu ruang hijau untuk risiko rendah (*low risk*), ruang kuning untuk risiko menengah (*medium risk*), dan ruang merah untuk risiko tinggi (*high risk*). Hasil dari evaluasi risiko ini adalah ukuran atau level risiko dari masing-masing risiko yang dianalisis.

d) Perlakuan risiko.

Tahap terakhir ini ditujukan untuk menentukan strategi yang dapat mengurangi maupun mencegah kemungkinan risiko melalui rekomendasi perlakuan risiko. Perlakuan risiko ada 4 macam, meliputi Tolak, Turunkan, Transfer, dan Terima [18].

Tahap akhir proses penelitian ini yaitu menarik kesimpulan dan membangun rekomendasi. Kesimpulan menjawab tujuan penelitian sebelumnya. Saran tidak hanya untuk PT. XYZ, namun juga rekomendasi penelitian berikutnya.

3. HASIL DAN PEMBAHASAN

3.1. Konsultasi dan Komunikasi

Tahapan awal yang perlu dilakukan dalam melakukan pengelolaan risiko adalah komunikasi dan konsultasi. Tahapan ini bertujuan agar penetapan konteks dapat dilakukan secara tepat. Tujuan dari komunikasi dan konsultasi adalah untuk memberikan kesadaran dan pemahaman akan risiko dan manajemen risiko, serta mengkomunikasikan informasi untuk melakukan manajemen risiko.

3.2. Menentukan Ruang Lingkup, Konteks dan Kriteria

Ruang lingkup analisis risiko untuk aplikasi Smart Operation yaitu proses pengelolaan data transaksi, penanganan order penjualan, inventori atau barang dagangan, pengiriman, penagihan, penerimaan kas hingga pelaporan keuangan pada PT. XYZ. Sedangkan kriteria yang akan digunakan adalah *likelihood* dan *impact* (Tabel 1 dan Tabel 2).

Tabel 1. Kriteria *Likelihood* [20]

Kriteria	Definisi	Frekuensi	Nilai
<i>Rare</i>	Risiko hampir tidak pernah muncul	< 2 kali setahun	1
<i>Unlikely</i>	Risiko jarang muncul	> 2 kali setahun	2
<i>Possible</i>	Risiko kadang-kadang muncul	7-12 kali setahun	3
<i>Likely</i>	Risiko sering muncul	4-6 kali sebulan	4
<i>Certain</i>	Risiko pasti muncul	1-3 kali sebulan	5

Likelihood dibentuk berdasarkan 5 kriteria yang tercantum dalam Tabel 1 yang dibedakan berdasarkan frekuensi terjadinya. Sedangkan kriteria *Impact* dibedakan menjadi 5 berdasarkan pengaruh terhadap proses bisnis perusahaan yang dapat dilihat dalam Tabel 2.

Tabel 2. Kriteria *Impact* [20]

Kriteria	Definisi	Nilai
<i>Insignificant</i>	Tidak mengakibatkan hambatan proses bisnis	1
<i>Minor</i>	Terjadi gangguan pada proses bisnis, namun aktivitas utama dapat berjalan secara wajar	2
<i>Moderate</i>	Terjadi gangguan pada proses bisnis dan memicu sebagian aktivitas mengalami penangguhan	3
<i>Major</i>	Terjadi gangguan pada proses bisnis dan menyebabkan aktivitas mengalami penundaan	4
<i>Catastrophic</i>	Terjadi gangguan pada proses bisnis secara total hingga seluruh proses bisnis tidak tercapai	5

Tahap selanjutnya adalah membuat matriks evaluasi risiko. Matriks dibuat berdasarkan dua kriteria yang telah dirumuskan, yaitu *Likelihood* dan *Impact*, yang bertujuan untuk memetakan risiko yang ada menjadi tiga tingkatan *high*, *medium*, *low*, dan kemudian untuk mengetahui prioritas risiko mana yang sebaiknya ditindaklanjuti terlebih dahulu. Pemetaan matriks evaluasi risiko ditunjukkan pada Tabel 3 sebagai keterangan warna risiko.

Matriks evaluasi risiko menilai risiko berdasarkan ukuran *Likelihood* dan *Impact*. Nilai risiko pada kriteria *Likelihood* dikalikan dengan nilai pada kriteria *Impact* untuk mendapatkan total nilai risiko. Nilai ini digunakan untuk menentukan prioritas penanganan, di mana risiko dengan nilai lebih tinggi akan diprioritaskan karena lebih berisiko.

Tabel 3. Matrix Evaluasi Risiko [20]

Certain	5	Medium (5)	Medium (10)	High (15)	High (20)	High (25)
Likely	4	Medium (4)	Medium (8)	Medium (12)	High (16)	High (20)
Possible	3	Low (3)	Medium (6)	Medium (9)	Medium (16)	High (15)
Unlikely	2	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium (10)
Rare	1	Low (1)	Low (2)	Low (3)	Medium (4)	Medium (5)
Impact	1		2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic

3.3. Penilaian Risiko

Tahapan ini berisi identifikasi, analisis, dan evaluasi risiko. Identifikasi risiko akan dibagi menjadi beberapa sektor risiko, meliputi proses bisnis penjualan dari transaksi dan order penjualan, inventori dan pengiriman, penagihan, penerimaan, serta pelaporan kas; lingkungan aplikasi yaitu sistem infrastruktur dan data, dan sumber daya manusia.

3.3.1. Identifikasi Risiko

Identifikasi risiko melibatkan analisis atau identifikasi untuk menemukan risiko yang berpotensi untuk menghambat atau mengganggu proses bisnis yang

ada. Identifikasi risiko dikelompokkan menjadi beberapa sektor risiko. Adapun risiko yang teridentifikasi diuraikan di Tabel 4.

Tabel 4. Identifikasi Risiko

Sektor Risiko	id	Risiko	Dampak Risiko
Transaksi dan Order Penjualan	R001	Order fiktif	Order tidak dapat diselesaikan, dikarenakan sebenarnya orderan tidak ada.
	R002	Kesalahan pencatatan order	Order tidak dapat diselesaikan karena kesalahan pencatatan detail order.
Inventori dan Pengiriman	R003	Penurunan jumlah barang/stok	Kegagalan pengiriman dikarenakan stok barang tidak ada
	R004	Kehilangan barang disengaja/pencurian	Perusahaan mengalami kerugian materi
	R005	Kesalahan pemilihan barang	Pengembalian barang/retur dapat terjadi.
Penagihan, Penerimaan, serta Pelaporan Kas	R006	Kegagalan pencatatan keuangan	Pencatatan keuangan melewati tahap <i>input</i> manual oleh staff kasir, kesalahan pencatatan dapat terjadi, namun tidak berdampak besar karena masih melewati tahap check dari sistem, dan dapat dikoreksi kembali
	R007	Adanya uang palsu	Bisa saja terjadi pembayaran menggunakan uang palsu pada sistem pembayaran kontan.
	R008	Kegagalan penerimaan kas	Setoran tidak tepat waktu
	R009	Ketidaksesuaian jumlah setoran dengan tagihan	Jumlah setoran yang diberikan tidak sesuai dengan nota penjualan
Sistem Infrastruktur dan Data	R010	Server down	Proses bisnis terganggu, dapat mengakibatkan keterlambatan
	R011	<i>Virus</i> dan <i>malware</i>	Perangkat komputer tidak dapat digunakan dengan benar karena terkena virus/gangguan <i>malware</i> .
Sumber Daya Manusia	R012	Karyawan tidak memahami cara pengoperasian aplikasi	Proses bisnis tertentu dapat mengalami gangguan karena karyawan yang kurang paham pengoperasian aplikasi

3.3.2. Analisis Risiko

Analisis risiko akan memetakan risiko - risiko yang sudah diidentifikasi dan dikelompokkan sesuai sektor risiko, kemudian akan digunakan untuk menentukan kriteria risiko seperti *likelihood* dan *impact*. Kedua kriteria tersebut akan dikalikan nilainya untuk menghitung Nilai Risiko. Nilai inilah yang digunakan untuk memetakan risiko seperti dalam Tabel 3. Nilai risiko juga dijadikan acuan dalam mengambil tindakan prioritas risiko yang perlu dilakukan. Hasil analisis risiko diuraikan pada Tabel 5.

Tabel 5. Analisis Risiko

ID Risiko	<i>Likelihood</i>	<i>Impact</i>	Nilai Risiko
R001	1	4	4
R002	2	3	6
R003	2	3	6
R004	2	3	6
R005	3	2	6
R006	3	1	3
R007	1	1	1



ID Risiko	Likelihood	Impact	Nilai Risiko
R008	1	4	4
R009	3	1	3
R010	1	4	4
R011	1	4	4
R012	1	2	2

3.3.3. Evaluasi Risiko

Tahap selanjutnya adalah evaluasi risiko, dimana risiko yang telah diketahui Nilai Risikonya akan dimasukkan dalam matriks evaluasi risiko. Tabel 6 menunjukkan bahwa dari 12 risiko, tidak ada risiko ruang merah atau jenis *High Risk*. Hal ini berarti tidak ada risiko yang dapat mengancam dan merugikan perusahaan. Sedangkan pada ruang kuning atau *Medium Risk* terdapat 8 risiko. Kedelapan risiko ini dapat menyebabkan gangguan, namun dapat diatasi dengan kebijakan dan pengawasan perusahaan. Adapun 4 risiko ada pada ruang hijau atau *Low Risk*, dimana keempatnya tidak terlalu berpengaruh pada perusahaan.

Tabel 6. Pemetaan Risiko menggunakan Matrix Evaluasi Risiko

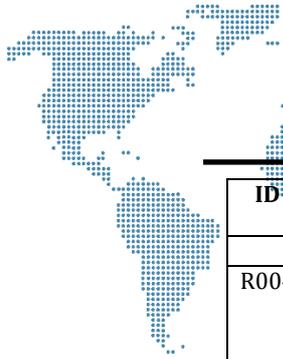
<i>Certain</i>	5					
<i>Likely</i>	4					
<i>Possible</i>	3	R006, R009	R005			
<i>Unlikely</i>	2			R002, R003, R004		
<i>Rare</i>	1	R007	R0012		R001, R008, R010, R011	
<i>Impact</i>		1	2	3	4	5
		<i>Insignificant</i>	<i>Minor</i>	<i>Moderate</i>	<i>Major</i>	<i>Catastrophic</i>

3.4. Perlakuan Risiko

Bagian ini menganalisis rekomendasi mengenai perlakuan risiko atas kemungkinan risiko dari implementasi aplikasi *Smart Operation*. Uraian rekomendasi terkait perlakuan risiko disusun berdasarkan tingkatan risiko dari level tinggi hingga level rendah, seperti yang disajikan pada Tabel 7.

Tabel 7. Rekomendasi Perlakuan Risiko

ID	Level Risiko	Perlakuan Risiko	Tindakan Risiko
R001	<i>Medium</i>	Turunkan	Hak akses pembuatan order diperketat, Melakukan pengecekan berkala terhadap log sistem riwayat pengeditan data, agar lebih cepat mendeteksi adanya orderan fiktif.
R002	<i>Medium</i>	Turunkan	Melakukan pengecekan log secara berkala, Memberikan training penggunaan aplikasi agar karyawan lebih memahami cara pengoprasian aplikasi dengan baik.
R003	<i>Medium</i>	Turunkan	Melakukan <i>stock opname</i> secara berkala, agar dapat mendeteksi adanya penurunan dengan cepat, Mempersiapkan penjadwalan pemesanan kembali/ <i>reorder</i> sesuai jumlah persediaan aman/ <i>safety stock</i> agar menciptakan



ID	Level Risiko	Perlakuan Risiko	Tindakan Risiko
			ketersediaan stok yang stabil.
R004	Medium	Turunkan	Melakukan <i>stock opname</i> untuk mencocokkan fisik barang dan catatan kartu gudang secara rutin. Penempatan barang dalam jangkauan CCTV untuk mengurangi kemungkinan terjadinya risiko.
R005	Medium	Turunkan	Melakukan pengecekan ulang dokumen pengiriman dan barang yang akan dikirim setelah barang selesai dimuat.
R008	Medium	Turunkan	Melakukan penjadwalan penagihan Berkomunikasi dengan pelanggan untuk piutang yang sudah dan akan jatuh tempo.
R010	Medium	Turunkan	Melakukan pengecekan dan perbaikan rutin untuk mengurangi kemungkinan terjadinya <i>server down</i> . Membuat <i>backup system</i> dan backup data untuk mengurangi dampak bila terjadi <i>server down</i> .
R011	Medium	Turunkan	Memperketat hak akses, melakukan pengecekan log sistem secara berkala. Meningkatkan keamanan sistem seperti memasang antivirus, serta menerapkan protokol perlindungan data.
R006	Low	Turunkan	Pengecekan secara berkala pencatatan keuangan pada aplikasi, dan Melakukan pemeriksaan pencatatan keuangan menggunakan sistem untuk mencocokkan pencatatan keuangan sistem dengan yang disetorkan.
R007	Low	Turunkan	Membawa alat cek portable untuk mencegah adanya uang palsu Mengarahkan untuk melakukan pembayaran non tunai untuk mengurangi peluang terjadinya risiko
R009	Low	Turunkan	Rekonsiliasi secara berkala antara setoran tunai/non tunai dengan tagihan
R012	Low	Turunkan	Memberikan training pengoperasian aplikasi terhadap karyawan, sehingga meminimalkan risiko karyawan tidak paham dalam pengoperasian aplikasi

4. SIMPULAN

Penelitian ini menerapkan kerangka kerja ISO 31000:2018 dalam rangka menganalisis manajemen risiko atas implementasi Sistem Informasi Smart Operation di PT. XYZ. Langkah awal dengan melakukan konsultasi dan komunikasi memastikan bahwa semua pemangku kepentingan terlibat dan memahami proses penilaian yang berlangsung. Perumusan cakupan, konteks, dan kriteria menjadi dasar untuk mekanisme penilaian risiko. Analisis penilaian risiko mengidentifikasi 12 risiko untuk 5 sektor risiko. Temuan penelitian ini menunjukkan bahwa tidak ada risiko dengan jenis *High Risk*, 8 risiko dengan jenis *Medium Risk* dan 4 risiko dengan jenis *Low Risk*. Berdasarkan temuan ini, penelitian ini menyimpulkan bahwa terkait dengan implementasi Sistem Informasi *Smart Operation* di PT. XYZ, tidak ada risiko yang membahayakan dan merugikan perusahaan. Meskipun terdapat 8 risiko menengah, namun dengan tindakan risiko yang direkomendasikan dan dengan kebijakan, serta pengawasan perusahaan, maka risiko tersebut diharapkan dapat diturunkan. Perlakuan risiko yang direkomendasikan adalah untuk melakukan mitigasi atau pengurangan risiko. Terdapat 4 risiko menengah yang memiliki dampak paling besar dengan skor 6 adalah kesalahan pencatatan order, penurunan jumlah barang, kehilangan barang disengaja/pencurian, dan kesalahan pemilihan barang. Tindakan untuk

menurunkan risiko pada 4 hal ini adalah pengecekan log secara berkala, *training* penggunaan aplikasi, *stock opname* secara berkala, penempatan barang dalam jangkauan CCTV dan pengecekan ulang dokumen dengan barang dikirim. Sedangkan risiko adanya uang palsu adalah yang memiliki dampak paling kecil dengan skor 1, karena perusahaan memiliki alat pendeteksi yang akurat.

Fokus penelitian ini pada penggunaan Sistem Informasi *Smart Operation* untuk proses bisnis transaksi penjualan. Oleh karena itu, penelitian selanjutnya diharapkan dapat mengkaji pada proses bisnis dan aplikasi yang lain. Sehingga analisis manajemen risiko menjadi lebih komprehensif. Rekomendasi lain adalah menggunakan analisis secara kuantitatif untuk teknik penilaian risiko FMEA. Sehingga diharapkan mendapatkan kajian yang lebih detail dan melengkapi kajian kualitatif yang ada.

DAFTAR PUSTAKA

- [1] K. Farina and S. Opti, "Pengaruh Pemanfaatan Sistem Informasi Akuntansi dan Penggunaan Teknologi Informasi Terhadap Kinerja UMKM," *Jesya*, vol. 6, no. 1, pp. 704–713, Jan. 2023, doi: 10.36778/jesya.v6i1.1007.
- [2] N. K. A. Apriliani and P. Y. Wijaya, "Peran Komunikasi dan Penerapan Teknologi Informasi Dalam Meningkatkan Kinerja Pegawai Putu Yudy Wijaya," *Widya Amrita, Jurnal Manajemen, Kewirausahaan dan Pariwisata*, vol. 1, no. 3, pp. 954–961, 2021, [Online]. Available: <https://ejournal.unhi.ac.id/index.php/widyaamrita/article/download/1355/851/>
- [3] E. Putri Primawanti and H. Ali, "Pengaruh Teknologi Informasi, Sistem Informasi Berbasis Web Dan Knowledge Management Terhadap Kinerja Karyawan (Literature Review Executive Support Sistem (Ess) for Business)," *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 3, pp. 267–285, 2022, doi: 10.31933/jemsi.v3i3.818.
- [4] H. Sulistiani, D. Alita, and P. Dellia, "Pemanfaatan Analisis Biaya Dan Manfaat Dalam Perhitungan Kelayakan Investasi Teknologi Informasi," *Jurnal Ilmiah Edutic*, vol. 6, no. 2, 2020, doi: 10.21107/edutic.v6i2.7220.
- [5] R. Salwa and N. M. I. Padli, "Inovasi Bisnis Organisasi Melalui Pemanfaatan Sistem Dan Teknologi Informasi," *CEMERLANG: Jurnal Manajemen dan Ekonomi Bisnis*, vol. 4, no. 1, pp. 21–31, 2024, doi: <https://doi.org/10.55606/cemerlang.v4i1.2231>.
- [6] M. A. G. Wattimena and A. R. Tanaamah, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 (Studi Kasus: TSI/Teknologi dan Sistem Informasi Perpustakaan UKSW)," *Journal of Information Systems and Informatics*, vol. 3, no. 3, pp. 483–498, 2021, doi: 10.51519/journalisi.v3i3.183.
- [7] E. Sudarmanto *et al.*, *Manajemen Risiko*. Bandung: Widina Bhakti Persada, 2020.
- [8] H. Anam, "Manajemen Risiko Operasional Bank Syariah; Teori dan Manfaat," *Jurnal At-Tamwil: Kajian Ekonomi Syariah*, vol. 5, no. 1, pp. 16–31, 2023, doi: 10.33367/at.v5i1.1476.
- [9] 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, Jun. 2019, doi: 10.46984/sebatik.v23i1.441.
- [10] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, p. 91, Feb. 2020, doi: 10.30865/jurikom.v7i1.1791.

- [11] I. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, pp. 389–396, May 2021, doi: 10.30812/matrik.v20i2.1093.
- [12] L. D. Ivander and S. F. Papilaya, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2009," *Jurnal Ekonomi Volume 18, Nomor 1 Maret201*, vol. 2, no. 1, pp. 41–49, 2023, doi: 10.30865/klik.v4i2.1174.
- [13] M. M. Sine and E. Maria, "Analisis Manajemen Risiko pada Penerapan Sistem Informasi Pembangunan Daerah (SIPD) Menggunakan IEC/ISO 31010:2019," *Building of Informatics, Technology and Science (BITS)*, vol. 4, no. 1, Jun. 2022, doi: 10.47065/bits.v4i1.1531.
- [14] E. Malau and E. Maria, "Penerapan IEC/ISO 31010:2019 untuk Manajemen Risiko pada Sistem Informasi Kesejahteraan Sosial-Next Generation," *Journal of Information System Research*, vol. 4, no. 4, pp. 1063–1071, 2023, doi: 10.47065/josh.v4i4.3459.
- [15] M. R. Fadli, "Memahami desain metode penelitian kualitatif," *Humanika*, vol. 21, no. 1, pp. 33–54, Apr. 2021, doi: 10.21831/hum.v21i1.38075.
- [16] D. Makajić-Nikolić, "ISO 31000: Risk Management Guidelines," in *Encyclopedia of Sustainable Management*, Cham: Springer International Publishing, 2023, pp. 2078–2080. doi: 10.1007/978-3-031-25984-5_314.
- [17] F. A. Hardianto and Y. S. Dharmawan, "Manajemen Risiko TI ISO 31000 Dengan Cobit 5 Dan FMEA (PT. XYZ)," *Jurnal SITECH : Sistem Informasi dan Teknologi*, vol. 4, no. 2, pp. 133–146, Feb. 2022, doi: 10.24176/sitech.v4i2.6649.
- [18] C. R. Vorst, D. S. Priyarsono, and A. Budiman, *Manajemen Risiko Berbasis SNI ISO 31000*. Jakarta: Badan Standardisasi Nasional, 2018.
- [19] International Electrotechnical Commission, *International Standart Risk management – Risk assessment techniques*, 2.0. 2019.
- [20] Usman and A. A. Yudhistira, "Jurnal It Risk Management Analisis Resiko Teknologi Informasi Pada Toko Puntadewa Outdoor," *Jurnal Syntax Fusion*, vol. 1, no. 03, pp. 54–64, 2021, doi: 10.54543/fusion.v1i03.54.