Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000 pada Aplikasi Ayo SRC

Deni Rohmat
Universitas Sebelas April Sumedang
Jl. Angkrek Situ No.19, Situ, Kec. Sumedang Utara, Kabupaten Sumedang, Jawa Barat 45323
email: denirohmat46@gmail.com

ABSTRACT
The development of technology is currently very fast and rapid so that technology becomes a very intimate need in everyday life, especially in the business world. But from all that there must be a risk that arises. Risk (risk) is the effect of uncertainty on a goal. Influence is a deviation from the expected result, the result can be positive, negative or both so that it can overcome, create or generate opportunities and threats. Toko Komar is a wholesaler that already uses the application of information technology to support its business activities. The store uses the Ayo SRC application which is used to support sales, record inventory, and record daily expenses needed. However, in the world of management, there are always possible risks that may occur and can disrupt business activities in using the system. That way risk analysis is needed for the resources contained in the store. Using ISO 31000 is expected to minimize the risks contained in the Ayo SRC application. The results of this risk analysis are in the form of an analysis of possible risks, grouping possible risks based on their impact so as to produce risk action proposals for possible risks contained in the Ayo SRC application, so that the store can treat possible risks according to the priority level of risk and can prevent and minimize so as not to disrupt business activities.

Keywords **-** *Information Technology Risk Management*, *Risk Analysis*, ISO 31000, Ayo SRC

1. Introduction

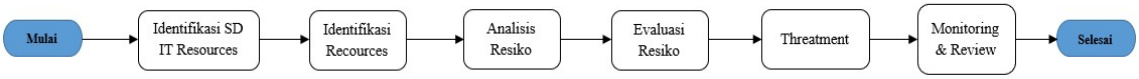
Perkembangan teknologi saat ini sangat cepat dan pesat sehingga teknologi menjadi kebutuhan yang sangat intim dalam kehidupan sehari hari terutama dalam dunia bisnis[1]. Namun dari semua itu pasti terdapat risiko yang muncul. Risiko (risk) adalah pengaruh ketidakpastian pada suatu tujuan. Pengaruh adalah penyimpangan dari hasil yang diharapkan, hasilnya bisa positif, negatif atau keduanya sehingga dapat mengatasi, menciptakan, atau menghasilkan peluang dan ancaman.[2]

Kemajuan di bidang teknologi informasi dan jaringan internet serta perdagangan bebas dunia turut mengakselerasi globalisasi ekonomi maupun perkembangan ekonomi digital[3]. Digital marketing ini lebih prospektif karena memungkinkan pelanggan untuk memperoleh segala macam informasi mengenai produk dan bertransaksi melalui internet. SRC adalah singkatan dari Sampoerna Retail Community yang memudahkan akses bagi para mitra SRC untuk bisa saling berbagi ilmu bisnis, mendapatkan informasi, lalu memudahkan cara mengelola toko yang benar. Hadir sejak tahun 2008, kini SRC sudah mulai dikenal dan memiliki banyak mitra. Dimana mereka juga baru meluncurkan aplikasi mobile untuk Android yang bernama aplikasi Ayo SRC. Dimana aplikasi ini akan memudahkan para mitra SRC seperti di Grosir Toko Komar Rancakalong yang sudah bergabung dengan Ayo SRC yang dimana warung-warung kecil dapat berbelanja secara online dan bisa di delivery melalui aplikasi ini. Namun dalam pelaksanaannya tentu terdapat berbagai tantangan dan risiko yang dapat mengancam proses pembelian jarak jauh.

Tujuan penelitian analisis ini untuk membantu dalam menganalisis kemungkinan - kemungkinan risiko pada aplikasi AYO SRC di Grosir Toko Komar yang akan terjadi di kemudian hari, sehingga toko yang terhubung dapat melakukan pencegahan agar kemungkinan- kemungkinan risiko tersebut tidak

terjadi dan menganggu proses bisnis,dan membahas tindakan yang perlu dilakukan pada kemungkinan berbagai ancaman dan risiko yang muncul menggunakan ISO 31000.

2. Research Method



Gambar 1. Metode ISO 31000 yang diterapkan pada analisis

Dalam mengidentifikasikan manajemen risiko pedoman yang dipakai adalah ISO 31000. ISO 31000 merupakan standar yang berkaitan dengan manajemen risiko yang diterbitkan pada tanggal 13 November 2009 oleh International Organization for Standardization (ISO)[4]. Manajemen Risiko adalah aktivitas manajemen yang dilakukan berdasarkan tingkatan pada tingkat pimpinan pelaksana. Kegiatan penemuan serta analisis sistematis terhadap kerugian yang mungkin dihadapai oleh perusahaan atau organisasi[5].

2.1 Identifikasi Sumber daya IT (IT Resources Identification)

Identifikasi Sumber daya merupakan langkah awal dalam memenuhi kebutuhan dalam mengidentifikasi risiko IT. Dalam identifikasi ini, perlu diketahui lebih lanjut tentang komponen apa saja yang dimiliki oleh suatu organisasi/perusahaan dalam menunjang berjalannya aplikasi agar tetap berjalan baik. Beberapa sumber daya IT yang diidentifikasi berdasarkan COBIT dapat dikelompokkan menjadi 4 yaitu :

a) Aplikasi (Application) - Aplikasi adalah sumber daya berdasarkan tools atau sarana yang digunakan untuk menunjang selama masa berjalannya suatu objek yang akan dianalisis.
b) Informasi (Information) - Informasi adalah data-data yang terdapat pada suatu objek yang dianalisis, data ini dapat mencangkup data mengenai internal objek tersebut atau eksternal objek (data user, dll)
c) Infrastruktur (Infrastructure) - Infrastruktur merupakan fasilitas-fasilitas yang dimiliki oleh suatu organisasi dalam menunjang berjalannya objek yang dianalisis.
d) Sumber Daya Manusia/SDM (People) - SDM adalah sekumpulan orang-orang yang berperan untuk menjalankan/mengawasi suatu objek.[6]

2.2 Penilaian Risiko (Risk Assessment)

Penilaian Risiko dilakukan dengan 3 (tiga) tahap, yaitu Identifikasi Risiko(Risk identification),Analisis Risiko (Risk Analysis),Evaluasi Risiko (Risk Evaluation)[4].

2.3 Perlakuan Terhadap Risiko (Risk Treatment)

Pada risk treatment terdapat 4 (empat) jenis dalam menanggapi risiko, yaitu Risk Avoidance (Menghindari Risiko),Risk Reduction (Mengurangi/memperkecil kemungkinan adanya risiko (likelihood) dan dampak dari risiko tersebut), Risk Sharing (Berbagi Risiko), dan Risk Acceptance (Menerima Risiko)

2.4 Monitoring dan Review

Monitoring merupakan kegiatan pemantauan rutin terhadap kinerja aktual proses manajemen risiko. Review adalah peninjauan atau pengkajian berkala atas kondisi saat ini dan dengan fokus tertentu. Monitoring dan review merupakan bagian dari proses manajemen risiko yang memastikan bahwa seluruh tahapan proses dan fungsi manajemen risiko memang berjalan dengan baik.

3. Result and Analysis

3.1 Identifikasi Sumber daya IT

Tabel.1 Sumber Daya IT Resources

No	IT Resources	
1	*Application*	• Aplikasi Ayo SRC • Web www.src.id • Aplikasi Berbelanja Online dan Manajemen stok
2	*Information*	• Data dan Informasi Pengguna • Data dan Informasi Barang • Data Transaksi dan Penjualan
3	*Infrastructure*	PC, *web server, database server, client* sistem operasi, *web services technologies* dan *network devices*
4	*People*	SDM : *Administrator*, *Operator*, *Maintenance, FO*

3.2 Penilaian Risiko (Risk Assestment)

Penilaian risiko yang dilakukan meliputi identifikasi risiko (risk identification), analisis risiko (risk analysis) dan evaluasi risiko (risk evaluation).

a. Identifikasi risiko (*risk identification*)

Identifikasi risiko bertujuan untuk memetakan setiap risiko yang dimiliki aplikasi Ayo SRC.

Berikut rincian identifikasi dari beberapa risiko pada tabel 2 dibawah ini:

Tabel 2. Identifikasi Risiko Sumber Daya TI

No	IT Resources	ID	Identifikasi Risiko
1	Application	A01	Aplikasi Crush(Down)
		A02	Peretas Aplikasi
		A03	Aplikasi Terkena Virus
2	Information	IF01	Kehilangan/Pencurian Data
		IF02	Database Rusak/Eror
		IF03	Data Overload
3	Infrastructure	IS01	Kerusakan *Hardware*
		IS02	Bencana Alam
		IS03	Koneksi jaringan putus/rusak
4	People	P01	Human Erors
		P02	Kurangnya SDM Pengelola Sistem
		P03	SDM baru yang belum mengerti betul alur kerja sistem

b. Analisis Risiko (Risk Analysis)

Tahap selanjutnya Analisis risiko yaitu tahap mendetailkan risiko, tahap ini menentukan status risiko berdasarkan peringkat frekuensi dan dampak kejadian[7]. Analisis risiko dilakukan dengan cara memberikan nilai dari setiap risiko yang muncul. Dari tiap-tiap risiko yang muncul akan dilakukan penilaian (bobot) dari sisi frekuensi kejadian dan dampak yang diakibatkan. Pada proses ini dilakukan penilaian terhadap kemungkinan-kemungkinan risiko yang sudah di identifikasi pada proses sebelumnya dengan menggunakan tabel kriteria likelihood dan tabel kriteria impact sebagai acuan untuk proses menganalisis risiko. [8]

Tabel 3. Kriteria Nilai Frekuensi Kejadian dan Dampak

Frekuensi kejadian (likelihood)		Dampak yang diakibatkan	
Nilai	Keterangan	Nilai	Keterangan
(1)	(2)	(3)	(4)
1	Sangat jarang terjadi	1	Sangat kecil
2	Jarang terjadi	2	Kecil
3	Biasa terjadi	3	Biasa
4	Sering terjadi	4	Besar
5	Sangat sering terjadi	5	Sangat besar

Tabel 4. Analisis Resiko Aplikasi

No	IT Resources	Identifikasi Risiko	Frekuensi	Dampak
1	Application (A)	1. Aplikasi Crush(Down)	2	5
		2. Peretasan Aplikasi	2	4
		3. Aplikasi Terkena Virus	3	3
2	Information (IF)	1. Kehilangan/Pencurian Data	2	4
		2. Database Rusak/Eror	2	5
		3. Data Overload	3	4
3	Infrastucture (IS)	1. Kerusakan *Hardware*	3	4
		2. Bencana Alam	2	5
		3. Koneksi jaringan putus/rusak	2	4
4	People (P)	1. Human Erors	3	4
		2. Kurangnya SDM Pengelola Sistem	3	3
		3. SDM baru yang belum mengerti betul alur kerja sistem	2	3

c. Evaluasi Risiko (Risk Evaluation)

Tujuan dari evaluasi risiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis risiko[9]. Grafik hasil evaluasi risiko tersebut dikategorikan menjadi 3 area yaitu Low, Medium dan High berdasarkan matriks hasil kombinasi antara likelihood (frekwensi kejadian) dengan dampak yang ditimbulkan sebagai berikut[10]:

Tabel 5. Matriks Evaluasi Risiko

Frekuensi kejadian (likelihood)						
	5	Medium	Medium	High	High	High
	4	Low	Medium	High	High	High
	3	Low	Low	Medium	High	High
	2	Low	Low	Medium	Medium	High
	1	Low	Low	Low	Medium	Medium
		1	2	3	4	5
		Dampak yang diakibatkan				

Tabel 6. Matriks Sebelum Risk Treatment

Frekuensi kejadian (likelihood)						
	5					
	4					
	3			A03, P02	IF03,IS01, P01	
	2			P03	A02, IF01,IS03	A01,IF02,IS02
	1					
		1	2	3	4	5
		Dampak yang diakibatkan				

3.3 Perlakuan Terhadap Risiko (Risk Treatment)

Perlakuan risiko adalah saran tindakan lanjutan untuk menangani risiko yang ada[11]. Berikut table 6 untuk masing masing perlakuan risiko:

Tabel 7. Perlakuan Risiko

IT Resources	ID	Identifikasi Risiko	F	D	Risiko	Treatment	Sumber
Application	A01	Aplikasi Crush(Down)	2	4	Medium	Melakukan pengecekan secara berkala terhadap CPU usage dan RAM usage pada server	[12]
	A02	Peretasan Aplikasi	2	2	Low	Menggunakan jaringan private agar sulit untuk diretas	[8]
	A03	Aplikasi Terkena Virus	2	2	Low	Menyediakan antivirus, melakukan update dan monitoring software dan database antivirus	[6]
Information	IF01	Kehilangan/Pencurian Data	2	3	Medium	Mengadakan maintenance passwordsecara berkala	[13]
	IF02	Database Rusak/Eror	2	3	Medium	Membuat SOP backup dan melakukan backup secara berskala.	[1]
	IF03	Data Overload	3	3	Medium	Melakukan pengecekan secara berkala terhadap database	[13]
Infrastructure	IS01	Kerusakan Hardware	1	3	Low	Melakukan perawatan terhadap aset hardware yang dimiliki	[12]
	IS02	Bencana Alam	1	4	Medium	Mensosialisasikan mitigasi bencana alam, dan selalu untuk mengecek informasi di media sosial terkait berita terburu bencana alam yang terjadi.	[7]
	IS03	Koneksi jaringan putus/rusak	1	3	Low	Mengecek kecepatan jaringan dan koneksi	[14]
People	P01	Human Erors	2	4	Medium	Melakukan pelatihan terhadap karyawan baru.Membuat knowledge management systemsebagai dokumentasi pengetahuan bagi karyawan baru agar tidak melakukan kesalahan yang sama.	[13]
	P02	Kurangnya Pengelola Sistem oleh SDM	1	2	Low	Merekrut staff tambahan untuk mengelola sistem agar dapat dikelola secara optimal	[7]

	P03	SDM baru yang belum mengerti betul alur kerja sistem	1	3	Low	Membuat SOP kerja sistem dan melakukan training kepada pegawai baru	[1]

Tabel 8. Matriks Sebelum Risk Threatment

Frekuensi kejadian (likelihood)						
	5					
	4					
	3			A03, P02	IF03,IS01, P01	
	2			P03	A02, IF01,IS03	A01,IF02,IS02
	1					
		1	2	3	4	5
		Dampak yang diakibatkan				

Tabel 9. Matriks Setelah Risk Threatment

Frekuensi kejadian (likelihood)						
	5					
	4					
	3			IF03		
	2		A02, A03	IF01,IF02	A01, P01	
	1		P02	IS01,IS03, P03	IS02	
		1	2	3	4	5
		Dampak yang diakibatkan				

Tabel 8 menunjukan sebelum risl treatment dan tabel 9 menunjukan evaluasi risiko setelah dilakukan proses mitigasi risiko melalui program penanganan risiko (risk reduction) yang berdampak terhadap penurunan nilai likelihood dan dampak risiko[13].

3.4 Monitoring dan Review

Monitong merupakan kegiatan pemantauan rutin terhadap kinerja aktual proses manajemen risiko dibandingkan dengan rencana/harapan yang telah ditetapkan. Sedangkan review merupakan peninjauan/pengkajian berkala atas kondisi saat ini dan dengan fokus tertentu. Dan monitoring dan review merupakan bagian dari proses manajemen risiko yang memastikan bahwa seluruh tahapan proses dan fungsi manajemen risiko berjalan dengan baik.[15]. Terdapat tiga macam bentuk monitoring dan review yang harus dilakukan terus menerus oleh instansi yaitu Pemeriksaan berkala dan pemantauan berkelanjutan. Dilaksanakan secara terjadwal.

4. Conclusion

Berdasarkan penelitian analisis risiko menggunakan ISO 31000 pada aplikasi Ayo SRC, yang telah digunakan Mitra Toko Komar Rancakalong mulai dari tahapan penilaian risiko, identifikasi risiko, analisis risiko, evaluasi risiko, hingga tahap perlakukan risiko. Dari tahapan - tahapan tersebut, analisis risiko ini mendapatkan 12 kemungkinan risiko yang dapat sewaktu-waktu bisa menganggu kinerja dari aplikasi Ayo SRC maupun mengganggu proses bisnis yang terdapat di Grosir Toko Komar. Sebelum Risk Threatment terdapat 6 kemungkinan risiko dengan tingkat High meliputi aplikasi down(crush),database rusak,data overload,kerusakan hardware,bencana alam dan human erors. Kemudian terdapat 6 kemungkinan risiko dengan tingkat Medium meliputi Peretasan Aplikasi, Aplikasi Terkena Virus, Kehilangan/Pencurian Data, Koneksi jaringan putus/rusak, SDM baru yang belum mengerti betul alur kerja sistem, dan Kurangnya Pengelola Sistem oleh SDM. Namun setelah dilakukan perlakuan terhadap risiko(Risk treatment) terdapat hasil 6 Medium yang meliputi Aplikasi Crush(Down), Kehilangan/Pencurian Data, Database Rusak/Eror, Data Overload, Bencana Alam,dan Human Erors. Kemudian terdapat 6 Low meliputi Peretasan Aplikasi, Aplikasi Terkena Virus, Kerusakan Hardware, Koneksi jaringan putus/rusak, SDM baru yang belum mengerti betul alur kerja sistem, dan Kurangnya Pengelola Sistem oleh SDM.

Penanganan risiko yang disarankan adalah dengan cara menghindari terjadinya kemungkinan risiko (risk avoidance), meningkatkan kualitas sistem dan SDM yang terkait dengan Aplikasi Ayo SRC juga mempersiapkan apabila terjadi keadaan terburuk dengan menyiapkan backup baik hardware, software maupun SDM yang memadai untuk menanggulangi risiko yang akan terjadi.

Selain itu perlunya dilakukan pengawasan monitoring agar risiko tidak berkembang menjadi risiko yang tinggi (high risk).

References

[1] N. V. Richardo and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Perusahaan Toko Surabaya Cabang Surakarta," Journal of Information Systems and Informatics, vol. 3, no. 1, 2021, [Online]. Available: http://journalisi.org/index.php/isi

[2] I. Putu, A. Eka, P. #1, and T. S. Pratika, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," Jurnal Telematika, vol. 15, no. 2.

[3] P. Umkm, D. I. Indonesia Bahtiar, E. Lubis, and H. Harahap, "Hlm 65-98 PENGATURAN KAIDAH MANAJEMEN RISIKO ATAS PENAWARAN SAHAM BERBASIS TEKNOLOGI INFORMASI (EQUITY CROWDFUNDING) UNTUK," vol. 3, 2021.

[4] J. Ecleas and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000," 2021. [Online]. Available: http://jurnal.mdp.ac.id

[5] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office," 2020. [Online]. Available: http://jurnal.mdp.ac.id

[6] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," Journal of Computer Science and Engineering (JCSE), vol. 1, no. 2, pp. 128–146, Aug. 2020, doi: 10.36596/jcse.v1i2.76.

[7] V. Patrick, P. Wijaya, and A. D. Manuputty, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018," vol. 9, no. 2, pp. 1295–1307, 2022.

[8] R. P. Pangestu and A. F. Wijaya, "Analisis Manajemen Risiko Aplikasi SINTESA Pada Perpustakaan XYZ."

[9] F. Mulyana, S. Tinggi, M. Informatika, D. Komputer, S. Sumedang, and B. -Barati, "Analisis Manajemen Risiko Teknologi Informasi pada Sistem Informasi Akademik STMIK Sumedang Menggunakan ISO 31000," 2021. [Online]. Available: https://www.researchgate.net/publication/355983038

[10] D. Kurniawan, R. Prabowo, J. Ilmu Komputer FMIPA Universitas Lampung Jalan Sumantri Brojonegoro No, and B. Lampung, "Analisis Manajemen Risiko Sistem Informasi Pengelolaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan Metode ISO 31000," 2020.

[11] 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.

[12] A. Journal, A. A. Putri, and D. I. Irnanda, "Volume 4 issue 1 1 Aisyah Journal of Informatics and Electrical Engineering ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 (STUDI KASUS : APLIKASI J&T EXPRESS INDONESIA)", [Online]. Available: http://jti.aisyahuniversity.ac.id/index.php/AJIEE

[13] A. Rahmawati, A. F. Wijaya, A. R. Fakultas, and T. Informasi, "ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI ITOP Penulis Korespondensi."[Online]. Available: http://www.jurnal.umk.ac.id/sitech

[14] P. P. Thenu, A. F. Wijaya, C. Rudianto, U. Kristen, and S. Wacana, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 (STUDI KASUS: PT GLOBAL INFOTECH)," 2020.

[15] K. M. Linda Lole and E. Maria, "Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018," Jurnal Sistem Komputer dan Informatika (JSON), vol. 3, no. 3, p. 319, Mar. 2022, doi: 10.30865/json.v3i3.3891.