Aisyah Journal of Informatics and Electrical Engineering
Universitas Aisyah Pringsewu

Journal Homepage
http://jti.aisyahuniversity.ac.id/index.php/AJIEE

ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 (STUDI KASUS : APLIKASI J&T EXPRESS INDONESIA)

Anindhita Ari Putri[1], Deva Istifadhah Irnanda[2]

[1,2]Program Studi Sistem Informasi, Fakultas Teknologi Informasi dan Kreatif
Universitas Internasional Semen Indonesia
anindhita.putri17@student.uisi.ac.id[1], deva.irnanda17@student.uisi.ac.id[2]

ABSTRACT

This article introduces a method for measuring the level of risk in information technology that is appropriate for dealing with risk. J&T Express Indonesia is a shipping service company in the form of documents and packaging. J&T Express is a new company that also uses IT when providing services, they provide the advantage of taking goods. If the customer wants to send goods, no need to go to the J&T office, just contact J&T via android and iOS based applications or via their official hotline. Information technology supports the company's business operations. In this way the risk of information technology can occur at any time. Therefore, an information technology risk analysis will be carried out using ISO 31000. This method will be used to seek the results of measuring risk and solving risk problems and risk management to run smoothly. The risk priority of each possible risk has been determined or identified. Thus, the results of this risk analysis can be used to help minimize risks that are handled appropriately.
Keywords: *Risk Management; ISO 31000; Risk; Information Technology*

ABSTRAK

Artikel ini memperkenalkan metode untuk mengukur tingkat risiko teknologi informasi yang tepat untuk menangani risiko. J&T Express Indonesia perusahaan jasa pengiriman berbentuk dokumen dan kemasan. J&T Express adalah perusahaan baru yang juga menggunakan IT saat memberikan layanan, mereka memberikan keuntungan mengambil barang. Jika customer ingin mengirim barang, tidak perlu ke kantor J&T, cukup hubungi pihak J&T melalui aplikasi berbasis android dan iOS atau melalui hotline resmi mereka. Teknologi informasi mendukung operasional bisnis perusahaan. Dengan cara ini risiko teknologi informasi dapat terjadi kapan saja. pleh karena itu akan dilakukan analisis risiko teknologi informasi menggunakan ISO 31000. Metode ini akan digunakan untuk mengupayakan hasil ukur risiko dan menyelesaikan masalah risiko serta manajemen risiko dapat berjalan dengan lancar. Prioritas risiko dari setiap kemungkinan risiko telah ditentukan atau diidentifikasi. Dengan demikian, hasil analisis risiko ini dapat digunakan untuk membantu meminimalkan risiko yang ditangani dengan tepat.

Kata Kunci: *Manajemen Risiko; ISO 31000; Risiko; Teknologi Informasi*

I. PENDAHULUAN

Pada abad ini kemajuan dalam dunia teknologi informasi terus berkembang yang berdampak pada segala aspek kehidupan manusia. Semua aspek termasuk pendidikan, bisnis, pemerintahan, dll. Pada awal 1990-an, aplikasi komputerisasi masih merupakan satu hal yang jarang digunakan atau dikembangkan di banyak departemen, namun pada milenium baru, karena biaya operasi yang tinggi dan keuntungan yang cukup rendah. Aplikasi komputerisasi mulai diterapkan di berbagai bidang dan berkembang pesat. Berbagai sistem dikembangkan melalui penggunaan media komputer dan pendukungnya, memungkinkan sebagian besar departemen mulai mengembangkan sistem informasi untuk proses bisnis yang dilakukan bersama.

Di satu sisi merupakan bagian penting dari sistem informasi dan pengembangan adalah semua aspek keamanan dan manajemen risiko. Dengan berkembangnya sistem informasi saat ini, beberapa faktor penting telah menjadi faktor penentu pengoperasian sistem operasi yang benar, karena selain dampak positif dari perkembangan sistem informasi, masalah keamanan dan manajemen sumber daya teknologi informasi juga terjadi. Organisasi yang mengandalkan sistem informasi untuk Sebagian besar proses bisnisnya akan menghadapi masalah serius ketika sistem gagal beroperasi secara normal.

Penggunaan teknologi informasi dapat menimbulkan kemungkinan risiko. Banyak penelitian yang menunjukkan bahwa teknologi informasi dan asetnya rentan terhadap kerusakan fisik dan logis. Risiko kerusakan fisik terkait dengan perangkat keras seperti bencana alam, pencurian, kebakaran, lonjakan listrik dan vandalisme. Risiko kerusakan logis mengacu pada akses yang tidak sah, kerusakan yang disengaja atau tidak disengaja terhadap informasi dan asset informasi dan aset informasi yang terkandung di dalamnya. Untuk itu diperlukan identifikasi ancaman dan analisis risiko untuk meningkatkan keamanan dan mengurangi risiko kerusakan sistem informasi.

J&T Express Indonesia perusahaan jasa pengiriman berbentuk dokumen dan kemasan. J&T Express adalah perusahaan baru yang juga menggunakan IT saat memberikan layanan, mereka memberikan keuntungan mengambil barang. Jika customer ingin mengirim barang, tidak perlu ke kantor J&T, cukup hubungi pihak J&T melalui aplikasi berbasis android dan iOS atau melalui hotline resmi mereka.

Setiap aplikasi pasti memiliki berbagai kemungkinan risiko interferensi yang menyebabkan aplikasi tidak berjalan dengan optimal. Tidak terkecuali aplikasi pada J&T ini, aplikasi ini juga dapat menghadapi potensi risiko di sekitarnya. Berdasarkan permasalahan tersebut perlu dilakukan penelitian untuk mencatat berbagai kemungkinan risiko dan prioritasnya bagi perusahaan. Oleh karena itu, untuk tujuan ini, ISO 31000 dapat digunakan untuk analisis manajemen risiko.

II. TINJAUAN PUSTAKA

Lembaga penelitian pendidikan tinggi juga menggunakan ISO 31000 untuk melakukan penelitian analisis risiko teknologi informasi. Hasil dari penelitian ini adalah memberikan serangkaian risiko teknologi informasi, termasuk rangkaian risiko dan faktor, risiko dan faktor tersebut membantu atau memicu kejadian tertentu yang mengancam penggunaan teknologi informasi oleh lembaga penelitian pendidikan tinggi. [5]

Analisis manajemen risiko merupakan kegiatan yang dilakukan pada tingkat pimpinan eksekutif, yaitu menemukan dan menganalisis secara sistematis bentuk kerugian yang mungkin dihadapi perusahaan akibat risiko dan metode pengendalian yang paling tepat untuk menangani kerugian terkait bisnis. Tingkat keuntungan perusahaan. [5]

Analisis risiko memiliki beberapa tujuan yaitu:

a. Tujuan sebelum kerugian meningkatkan kepercayaan dalam bentuk efisiensi dan menyelesaikan tanggung jawab pihak luar.

b. Setelah mengalami kerugian dalam bentuk operasi yang berkelanjutan, tujuannya adalah agar dapat terus bertahan, dengan pendapatan dan pertumbuhan yang stabil. [10]

ISO 31000 adalah standar terkait manajemen risiko yang dikembangkan oleh Organisasi Internasional untuk Standardisasi

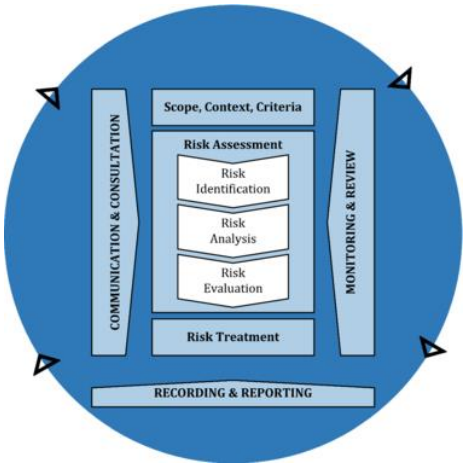
(ISO). Tujuan dari ISO itu sendiri adalah untuk memberikan prinsip dan pedoman yang diterima untuk manajemen risiko. [11]

III. METODOLOGI

Metode yang akan digunakan dalam penelitian ini adalah metode studi kasus, yaitu hanya untuk satu kasus, dan sampel yang digunakan berupa individu atau kelompok. Dengan cara ini penulis dapat mengumpulkan lebih banyak data tentang objek yang diteliti untuk menjawab pertanyaan yang ada. Data dalam penelitian ini adalah data mentah, dimana sumber datanya dikumpulkan dalam bentuk dokumen yang telah diverifikasi dan diverifikasi oleh sumber data. Makalah atau sumber data kertas tidak dapat digunakan karena berisi data tingkat ketiga.

3.1 Proses Manajemen Risiko

Proses manajemen risiko membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manajemen risiko bertujuan untuk mengelola risiko tersebut agar memperoleh hasil yang terbaik.



Tahap pertama adalah risk assessment, yaitu proses penentuan risiko yang dapat mengganggu perusahaan dalam mencapai tujuan bisnisnya. Pada tahap penilaian risiko terdapat 3 proses yaitu identifikasi risiko, analisis risiko dan penilaian risiko. Identifikasi risiko merupakan proses mengidentifikasi potensi risiko yang dapat menghambat perkembangan perusahaan.Analisis risiko adalah proses mengidentifikasi risiko yang dapat menghambat perusahaan dalam mencapai tujuan bisnisnya.Penilaian risiko adalah proses mengevaluasi semua kemungkinan proses. Risiko didasarkan pada tingkat gravitasi, berdasarkan standar yang ditetapkan. Langkah selanjutnya adalah risk treatment, dimana peneliti akan menyeleksi kemungkinan risiko sebelumnya. Hal ini dapat meningkatkan atau mengurangi kemungkinan risiko dan dampak risiko.

IV. HASIL DAN PEMBAHASAN

4.1 Tahap Penilaian Risiko

Proses tahap penilaian risiko pada penelitian ini akan terdiri dari 3 tahapan, yaitu tahap identifikasi risiko, tahap analisis risiko dan tahap evaluasi risiko.

4.1.1 Identifikasi Risiko

Identifikasi aset

Detail aset-aset terkait dapat dilihat pada tabel di bawah ini.

Tabel 1. Tabel Identifikasi Aset Terkait

Komponen Sistem Informasi	Aset
Data	Data administration and benefits
	Data time and attendance
	Data training and administration
	Data leave and permission
Software	Human resource management system
Hardware	Server database
	Server web service
	Server load balancer
	Server compelant
	Server remote desktop protocol

Identifikasi kemungkinan risiko

Setelah melakukan identifikasi aset, kemudian dilakukan identifikasi kemungkinan risiko yang ada di sekitar aset-aset terkait, dapat dilihat pada tabel di bawah ini.

Tabel 2. Tabel Identifikasi Kemnungkinan Risiko

ID	Kemungkinan Risiko
PR01	Data corrupt
PR02	Kegagalan backup data
PR03	Web service mati mendadak
PR04	Server down
PR05	Listrik padam
PR06	Koneksi terputus
PR07	Overload
PR08	Overhead
PR09	Dokumentasi program tidak lengkap
PR10	User interface sulit dimengerti
PR11	Pencurian data
PR12	Kurangnya SDM
PR13	Banjir
PR14	Kebakaran
PR15	Kerusakan hardware
PR16	Hacking terhadap jaringan

Identifikasi dampak risiko

Tahap berikutnya yaitu melakukan identifikasi dampak risiko. Tahap ini mengidentifikasi dampak yang dialami jika kemungkinan risiko telah teridentifikasi sebelumnya, bisa dilihat pada tabel berikut.

Tabel 3. Tabel Indentifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak
PR01	Data corrupt	Data menjadi rusak dan tidak dapat diakses
PR02	Kegagalan backup data	Maintenance tidak dapat berjalan dengan baik
PR03	Web service mati mendadak	Gagal mengakses ke program dan database utama perusahaan
PR04	Server down	Gagal mengakses ke program dan database utama perusahaan
PR05	Listrik padam	Aktifitas perusahaan terganggu
PR06	Koneksi terputus	Gagal mengakses ke program dan database utama perusahaan
PR07	Overload	Terjadi bottleneck yang diakibatkan log database dan log temp database yang penuh
PR08	Overhead	Kinerja hardware terhenti dan menjadi tidak maksimal
PR09	Dokumentasi program tidak lengkap	Mempersulit programmer untuk mengembangkan program
PR10	User interface sulit dimengerti	Aplikasi sulit dijalankan / sulit dipahami
PR11	Pencurian data	Mengalami kerugian secara informasi / finansial yang berkaitan dengan rahasia perusahaan
PR12	Kurangnya SDM	Program pendukung yang diselesaikan tidak tepat waktu
PR13	Banjir	Mengalami kerusakan infrastruktur dan aktivitas perusahaan terganggu
PR14	Kebakaran	Mengalami kerusakan infrastruktur dan aktivitas perusahaan terganggu
PR15	Kerusakan hardware	Gagal mengakses ke program dan database utama perusahaan
PR16	Hacking terhadap jaringan	Penyalahgunaan terhadap sumber daya jaringan

4.1.2 Analisi Risiko

Setelah menyelesaikan tahap identifikasi, tahap selanjutnya adalah tahap analisis risiko. Dalam proses ini, kemungkinan risiko yang teridentifikasi akan dievaluasi. Penentuan nilai ini akan didasarkan pada kemungkinan

(*likelihood*) dan efek (*impact*) yang ditunjukkan pada Tabel 4 dan Tabel 5.

Tabel 4. Kriteria *Likelihood*

Likelihood		Deskripsi	Frekuensi Kejadian
Nilai	Kriteria		
1	*Rare*	Risiko hampir tidak pernah terjadi	>2 tahun
2	*Unlikely*	Risiko jarang terjadi	1-2 tahun
3	*Possible*	Risiko kadang terjadi	7-12 bulan
4	*Likely*	Risiko sering terjadi	4-6 bulan
5	*Certain*	Risiko pasti terjadi	1-3 bulan

Tabel penilaian dampak atau *impact* dibagi menjadi 5 kriteria, dari kelompok yang berdampak paling kecil hingga yang paling berdampak.

Tabel 5. Kriteria *Impact*

Likelihood		Deskripsi
Nilai	Kriteria	
1	*Insignificant*	Tidak mengganggu aktivitas bisnis perusahaan
2	*Minor*	Aktivitas sedikit terhambat namun aktivitas utama tidak terganggu
3	*Moderato*	Menghambat proses bisnis sehingga Sebagian aktivitas terganggu
4	*Major*	Menghambat hamper seluruh aktivitas perusahaan
5	*Catastrophic*	Aktivitas perusahaan terhenti total karena suatu aktivitas

Setelah menentukan nilai kemungkinan dan dampak, langkah selanjutnya adalah menilai kemungkinan risiko secara individual. Diantara 16 kemungkinan risiko tersebut, nilai probabilitas dan dampak ditentukan satu per satu sesuai tabel yang telah direferensikan sebelumnya, yang dapat dilihat secara detail pada Tabel 6.

Tabel 6. Penilaian *Likelihood* dan *Impact*

ID	Kemungkinan Risiko	Likelihood	Impact
PR01	Data corrupt	2	4
PR02	Kegagalan backup data	2	4
PR03	Web service mati mendadak	3	4
PR04	Server down	4	3
PR05	Listrik padam	3	5
PR06	Koneksi terputus	3	4
PR07	Overload	2	2
PR08	Overhead	1	1
PR09	Dokumentasi program tidak lengkap	2	3
PR10	User interface sulit dimengerti	3	3
PR11	Pencurian data	1	3
PR12	Kurangnya SDM	1	2
PR13	Banjir	2	5
PR14	Kebakaran	1	5
PR15	Kerusakan hardware	3	4
PR16	Hacking terhadap jaringan	1	4

4.1.3 Evaluasi Risiko

Tahap terakhir adalah tahap penilaian risiko. Tahapan ini menggunakan acuan berupa matriks penilaian risiko, dimana tingkat risiko dipetakan berdasarkan penilaian kemungkinan risiko dan ancaman.

Tabel 7. Matriks Evaluasi Risiko

	Likelihood				
Impact	**1**	**2**	**3**	**4**	**5**
1					
2					
3					
4					
5					

Keterangan :

Low	
Medium	
High	

Tabel 8. Matriks Evaluasi Risiko Berdasarkan *Likelihood* dan *Impact*

	Likelihood				
Impact	**1**	**2**	**3**	**4**	**5**
1	PR08				
2	PR12	PR07			
3	PR11	PR09	PR10	PR04	
4	PR16	PR01 PR02	PR03 PR06 PR15		
5	PR14	PR13	PR05		

Setelah memasukkan kemungkinan risiko ke dalam matriks penilaian risiko, 16 kemungkinan risiko tersebut dikelompokkan menurut level tinggi, sedang dan rendah.

Tabel 9. Tabel Evaluasi Risiko Berdasarkan Likelihood dan Impact serta Risk Level

ID	Risiko	Likelihood	Impact	Risk level
PR07	Overload	2	2	
PR08	Overhead	1	1	
PR11	Pencurian data	1	3	
PR12	Kurangnya SDM	1	2	
PR01	Data corrupt	2	4	
PR02	Kegagalan backup data	2	4	
PR03	Web service mati mendadak	3	4	
PR04	Server down	4	3	
PR06	Koneksi terputus	3	4	
PR09	Dokumentasi program tidak lengkap	2	3	
PR10	User interface sulit dimengerti	3	3	
PR15	Kerusakan hardware	3	4	
PR16	Hacking terhadap jaringan	1	4	
PR05	Listrik padam	3	5	
PR13	Banjir	2	5	
PR14	Kebakaran	1	5	

4.2 Penanganan Risiko

Setelah tahap identifikasi risiko, lengkah selanjutnya adalah penanganan risiko. Pada tahap ini akan diberikan rekomendasi untuk semua kemungkinan risiko di sekitar aset terkait guna menghadapi kemungkinan risiko tersebut serta dapat meminimalisir kemungkinan terjadinya risiko sehingga aktivitas dapat beroperasi secara optimal atau meminimalkan kerugian perusahaan saat risiko muncul.

Tabel 10. Tabel Penanganan Risiko

ID	Risiko	Risk Level	Penanganan Risiko
PR08	Overhead		Menyediakan pendingin ruangan

			tambahan agar suhu tetap stabil
PR11	Pencurian data		Memasang alat cctv di setiap ruangan Mengunci file yang berisi data rahasia perusahaan
PR01	Data corrupt		Lebih memperhatikan file yang diunduh dari internet sehingga mencegah kerusakan data
PR02	Kegagalan backup data		Melakukan pengecekan secara berkala
PR03	Web service mati mendadak		Memperbaiki web server sesegera mungkin agar dapat diakses kembali
PR04	Server down		Melakukan pengecekan secara berkala terhadap CPU usage dan RAM usage pada server
PR06	Koneksi terputus		Melaporkan pada petugas internet service provider
PR09	Dokumentasi program tidak lengkap		Memperbaiki program yang tidak lengkap agar proses dokumentasi dapat berjalan normal
PR10	User interface sulit dimengerti		Memberikan panduan tentang penggunaan aplikasi kepada semua karyawan.
PR15	Kerusakan hardware		Melakukan perawatan terhadap aset hardware yang dimiliki
PR16	Hacking terhadap jaringan		Memasang jaringan privat agar sulit diretas
PR05	Listrik padam		Menyediakan generator dengan daya yang disesuaikan dengan kondisi perusahaan
PR13	Banjir		Menyediakan server cadangan di lokasi yang berbeda / ke tempat yang lebih aman dari banjir
PR14	Kebakaran		Menambah alat pemadam kebakaran di setiap ruangan kerja

V. PENUTUP

Berdasarkan penelitian yang telah diselesaikan, analisis risiko penerapan TI dilakukan dalam dua tahap utama. Tahap pertama adalah tahap penilaian risiko yang meliputi identifikasi risiko, analisis risiko dan penilaian risiko. Tahap kedua adalah tahap penanganan risiko berdasarkan hasil penelitian yang telag diselesaikan terdapat 3 rasio tinggi, 9 tingkat risiko sedang dan 4 tingkat risiko rendah. Tingkat risiko yang tinggi merupakan tingkat risiko yang pasti akan terjadi secara langsung mempengaruhi kegiatan bisnis perusahaan. Oleh karena itu, perlu tindakan-tindakan risiko untuk meminimalkannya.

Proses manajemen risiko untuk risiko di sekitar aset aplikasi J&T Express sudah berjalan, namun proses manajemen risiko hanya berdasarkan pengalaman dan tidak ada dokumen yang jelas mengenai manajemen risiko perusahaan. Penelitian ini dapat digunakan sebagai alat bantu dalam pengambilan keputusan atau kebijakan perusahaan dan dapat menghasilkan dokumen jangka panjang terkait manajemen risiko.

DAFTAR PUSTAKA

[1] Rahmawati, Aprilia, and Agustinus Fritz Wijaya. "Analisis risiko teknologi informasi menggunakan ISO 31000 pada Aplikasi ITOP." Jurnal SITECH: Sistem Informasi dan Teknologi 2.1 (2019): 13-20.

[2] Hutabarat, Felisia Meini, and Augie David Manuputty. "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000." Jurnal Bina Komputer 2.1 (2020): 52-65.

[3] Zagoto, Sermon Paskah, and Melkior NN Sitokdana. "ANALISIS RISIKO TEKNOLOGI INFORMASI DI ORGANISASI XYZ CABANG SALATIGA MENGGUNAKAN ISO 31000." Mnemonic: Jurnal Teknik Informatika 4.1 (2021): 1-9.

[4] Miftakhatun, Miftakhatun. "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000." Journal of Computer Science and Engineering (JCSE) 1.2 (2020): 129-146.

[5] Agustinus, Stefan, Adi Nugroho, and Ariya Dwika Cahyono. "Analisis risiko teknologi informasi menggunakan ISO 31000 pada program HRMS." Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi) 1.3 (2017): 250-258.

[6] Putra, Riszullah Ramadhan, Eman Setiawan, and Awalludiyah Ambarwati. "ANALISIS MANAJEMEN RISIKO TI PADA KEAMANAN DATA E-LEARNING DAN ASET IT MENGGUNAKAN NIST SP 800–30 Revisi 1." JATISI (Jurnal Teknik Informatika dan Sistem Informasi) 6.1 (2019): 96-105.

[7] Driantami, Hana Talitha Iddo, and Andi Reza Perdanakusuma Suprapto. "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus: Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)." Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN 2548 (2018): 964X.

[8] Susilo, Leo J. Manajemen Risiko Berbasis ISO 31000: 2018: Panduan untuk Risk Leaders dan Risk Practitioners. Gramedia Widiasarana Indonesia, 2018.

[9] Iin, Hurin. Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan XYZ Melalui Kombinasi COBIT, PMBOK, Dan ISO 31000. Diss. Institut Teknologi Sepuluh Nopember, 2017.

[10] Rilyani, Andi Novia, Yanuar Firdaus Arie Wibowo, and Dawam Dwi Jatmiko Suwawi. "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus: i-Gracias Telkom University)" eProceedings of Engineering 2.2 (2015).

[11] Atmojo, Sukma Arta, and Augie David Manuputty. "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office." JATISI (Jurnal Teknik Informatika dan Sistem Informasi) 7.3 (2020): 546-558.