JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK) VOL 16, No.1, Maret 2025, pp. 100 - 119
p-ISSN : 2087-0868 (media cetak)
e-ISSN : 2598-9707 (media online)
http://ejurnal.provisi.ac.id/index.php/JTIKP

ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI PT. ETERINDO NUSA GRAHA MENGGUNAKAN FRAMEWORK ISO31000:2018

Umi Sekarwat Oktavia[1], Indra Gita Anugrah[2], Widyasari Puspa Permata Witra[3]
[1,2,3] Program Studi Sistem Informasi, Universitas Muhammadiyah Gresik
Jl. Sumatera No.101, Gn. Malang, Randuagung, Kec. Kebomas, Kabupaten Gresik, Jawa Timur 61121
Email : umi.sekarwati210609004@umg.ac.id[1] , indragitaanugrah@umg.ac.id[2] , widyasarippw@umg.ac.id[3]

ARTICLE INFO

Article history:

Received : 15 – Februari - 2025
Received in revised form : 16 – Februari - 2025
Accepted : 26 – Februari - 2025
Available online : 1 – Maret - 2025

ABSTRACT

The use of information technology in companies is a crucial element to support business process effectiveness and efficiency. However, it also presents various challenges and risks that need to be managed properly. Risk management is key to protecting company value, optimizing strategies, and securing assets. PT. Eterindo Nusa Graha, as an industrial company relying on information technology, faces risks related to data, software, hardware assets, as well as threats from natural, system, infrastructure, and human resources. To address these issues, the company implements the ISO 31000:2018 framework, known for its flexibility and structured approach in identifying, assessing, and managing risks. Analysis results show that out of 16 identified risks, 5 are categorized as low, 10 as medium, and 1 as high. This indicates that most risks are still controllable, although effective mitigation strategies are needed, especially for high-category risks. The implementation of ISO 31000:2018 at PT. Eterindo Nusa Graha has helped the company protect critical assets, build stakeholder trust, and ensure smooth business processes. Thus, the company has demonstrated good risk management capabilities, although it still needs to focus more on high risks to minimize potential impacts.

Keyword : *Risk management*, ISO31000:2018, *Information Technology, Governance*

1. PENDAHULUAN

Penggunaan teknologi informasi oleh suatu perusahaan merupakan komponen penting yang mendukung keberhasilan dan efisiensi operasi komersialnya [1]. Tidak diragukan lagi, penggunaan teknologi informasi dalam suatu bisnis mengandung sejumlah bahaya dan masalah. Risiko adalah potensi bahaya yang dapat terjadi akibat peristiwa terkini atau yang akan datang [2]. Manajemen risiko diperlukan untuk memastikan bahwa risiko tersebut tidak berdampak buruk terhadap pencapaian tujuan kerja [3]. Proses mengenali bahaya, mengevaluasi, dan mengambil tindakan untuk menurunkannya ke tingkat yang dapat dikelola dikenal sebagai manajemen risiko[4]. Penerapan manajemen risiko diharapkan dapat melindungi nilai perusahaan, mengoptimalkan strategi manajemen dan melindungi sumber daya dan aset yang dimiliki perusahaan [5].

Menerapkan manajemen risiko dalam suatu bisnis sulit dilakukan karena ada faktor-faktor yang menentukan keberhasilan yang bergantung pada keadaan bisnis dan dimaksudkan untuk menetapkan standar penanganan risiko oleh perusahaan. Berbagai kondisi risiko yang dihadapi memengaruhi pendekatan yang berbeda terhadap manajemen risiko, sehingga setiap organisasi memiliki masalah risiko yang unik dan berbagai pendekatan untuk mengatasinya[6]. PT. Eterindo Nusa Graha merupakan perusahaan industri yang

Received : 15 – Februari - 2025*;* 15 – Februari - 2025*;* 26 – Februari - 2025

p-ISSN : 2087-0868 e-ISSN : 2598-9707

menggunakan teknologi informasi dalam kegiatan operasional perusahaan. Penggunaan dan penerapan teknologi informasi tidak menutup kemungkinan adanya ancaman risiko yang muncul. Berdasarkan hasil wawancara dengan kepala divisi IT PT. Eterindo Nusa Graha ditemukan tiga permasalahan yang terjadi antara lain permasalahan terhadap aset data, aset *software* dan aset *hardware* serta beberapa ancaman dari alam dan lingkungan, sistem dan infrastruktur serta sumber daya manusia.

Setiap perusahaan harus mengenali risiko yang mungkin terjadi dengan harapan bahwa risiko dapat dicegah, dihindari, atau dikurangi dampaknya. Untuk memperkuat dan membangun pondasi proses bisnis yang solid di masa mendatang agar terhindar dari risiko kehilangan peluang bisnis serta aset berharga dibutuhkan sebuah metode untuk mengatasinya [3]. Terdapat berbagai metode dalam penanganan manajemen resiko antara lain ISO31000:2018. ISO31000:2018 merupakan *framework* yang dapat diterapkan untuk semua jenis organisasi dengan memberikan panduan umum dalam manajemen risiko memungkinkan analisis yang lebih terperinci dan spesifik terhadap risiko[7]. selain ISO31000:2018 terdapat *framework* COSO ERM. COSO ERM merupakan suatu *framework* yang fokusnya lebih pada integrasi manajemen resiko dengan strategi dan kinerja dalam konteks pelaporan keuangan perusahaan [8]. Salah satu metode yang banyak diadopsi oleh berbagai negara termasuk Indonesia dalam proses manajemen risiko adalah ISO 31000:2018. Pada survei tahun 2018 oleh CRMS Indonesia *framework* ISO 31000:2018 memiliki *presentase* (67,5%) dipilih sebagai standart kerangka yang paling sering digunakan oleh perusahaan di indonesia diikuti standart COSO ERM memiliki *presentase* (15%) [9].

Salah satu manfaat *framework* ISO31000:2018 adalah kemampuan adaptasinya, yang memungkinkan manajemen risiko digunakan dalam berbagai industri dan oleh perusahaan besar maupun kecil. *Framework* ini menawarkan panduan terorganisasi yang membantu organisasi menemukan, mengevaluasi, dan mengelola risiko dengan sukses. Badan Standardisasi Nasional (BSN) membuat standar ini sebagai standar pedoman manajemen risiko, dan menerapkan proses manajemen risiko secara konsisten dan menyeluruh sebagai panduan dan kaitan dengan bahaya di perusahaan. Dalam manajemen risiko, ISO 31000:2018 sebagian besar digunakan sebagai alat untuk mengembangkan dan menjaga nilai-nilai perusahaan yang ada, sehingga meningkatkan kemungkinan tercapainya tujuan penelitian [10]. Proses manajemen risiko dengan menggunakan *framework* ISO 31000:2018 terdiri dari beberapa tahapan antara lain komunikasi dan konsultasi, penetapan konteks, *scope*, kriteria, penilaian resiko yang terdiri dari identifikasi resiko, analisis resiko, evaluasi resiko, perlakuan resiko dan *monitoring* dan *review* [11].

Framework ISO31000:2018 digunakan dalam penerapan manajemen resiko di PT. Eterindo Nusa Graha yang bertujuan untuk menciptakan dan melindungi nilai yang sudah dimiliki perusahaan, membantu perusahaan dalam mengidentifikasi resiko, menilai resiko, dan mengusulkan perlakuan risiko untuk semua kemungkinan risiko yang akan bermunculan, baik yang sudah pernah terjadi maupun yang belum pernah terjadi agar perusahaan memiliki pedoman dalam menghadapi ancaman resiko. Penerapan ISO31000:2018 di PT. Eterindo Nusa Graha dapat memberikan manfaat melindungi aset penting perusahaan yang berhubungan dengan proses bisnis perusahaan, membangun kepercayaan *stakeholder* dengan menunjukan komitmen dengan harapan bahwa risiko dapat diminimalisir dampaknya [12].

1. TINJAUAN PUSTAKA

2.1 Teknologi Informasi

Alat yang membantu dalam pemrosesan informasi disebut teknologi informasi. Selain teknologi komputer, yang meliputi perangkat keras dan perangkat lunak untuk memproses dan menyimpan data, teknologi ini juga mencakup teknologi komunikasi, yang memungkinkan informasi untuk dikirimkan atau dibagikan [1].

2.2 Risiko

Risiko didefinisikan sebagai kemungkinan bahaya yang dapat muncul dari peristiwa yang terjadi di masa sekarang maupun di masa depan [13]. Konsep risiko dapat dijelaskan melalui berbagai perspektif, di mana maknanya dapat bervariasi tergantung pada konteks atau proses kerja yang dinilai. Risiko selalu terkait dengan ketidakpastian, sehingga dalam aktivitas apa pun, keberadaan risiko tidak dapat dihindari [14]. Risiko melekat pada segala jenis kegiatan, baik dalam pengelolaan keuangan, manajemen perusahaan, maupun dalam kehidupan sehari-hari. Oleh karena itu, diperlukan suatu pendekatan sistematis untuk mengatasi risiko, yang dikenal sebagai manajemen risiko [15].

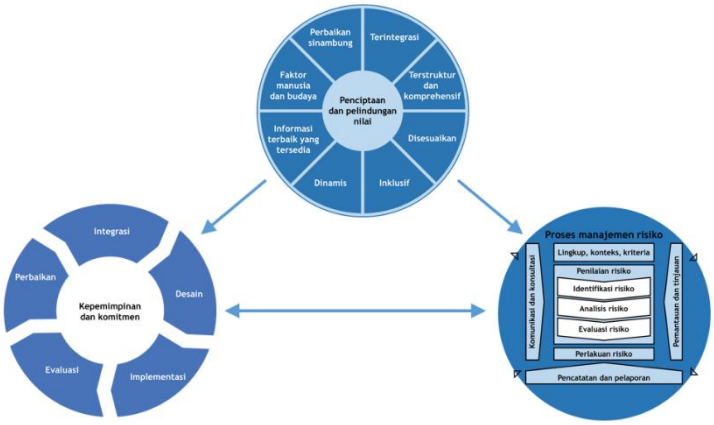
2.3 Manajemen Resiko

p-ISSN : 2087-0868 e-ISSN : 2598-9707

Proses sistematis untuk mengidentifikasi, mengevaluasi, dan mengantisipasi bahaya yang terkait dengan penggunaan teknologi informasi dikenal sebagai manajemen risiko[16]. Manajemen risiko teknologi informasi bertujuan untuk mengurangi potensi kerugian dari penggunaan TI sekaligus meningkatkan peluang dan keuntungan. Diharapkan bahwa penerapan manajemen risiko akan mampu melindungi sumber daya dan aset organisasi, mengoptimalkan taktik manajemen, dan mempertahankan nilai [17].

2.4 Framework ISO31000:2018

ISO 31000 merupakan standar yang berkaitan dengan manajemen risiko yang diterbitkan oleh ISO. Standar ini dapat digunakan di segala jenis organisasi dalam menghadapi ancaman risiko yang [18]. ISO31000:2018 dapat diterapkan dalam berbagai jenis usaha publik atau swasta serta mampu menyiapkan prinsip dan tahapan mengelola risiko sehingga bisa digunakan sebagai gambaran dalam manajemen risiko guna menerapkan manajemen risiko yang lebih efektif [19]. ISO31000:2018 memiliki tujuan yaitu untuk memberikan prinsip-prinsip dan pedoman untuk manajemen risiko yang diakui secara *universal*. ISO31000:2018 adalah panduan penerapan risiko yang terdiri atas tiga elemen: prinsip (*principle*), kerangka kerja (*framework*) dan proses (*process*). Prinsip memberikan acuan awal tentang manajemen risiko. Framework merupakan sistem manajemen risikonya dan proses merupakan langkah konkrit yang dilakukan dalam penyusunan manajemen risiko [20].



Gambar 1 Prinsip, Kerangka Kerja dan Proses

Pada tahun 2018 dalam buku manajemen risiko SNI ISO31000:2018[21] menjelaskan tentang prinsip-prinsip manajemen resiko menurut SNI ISO31000:2018, terdapat 8 (Delapan) prinsip manajemen risiko sebagai berikut :

a. Terintegrasi, kegiatan manajemen risiko adalah bagian integral dari seluruh aktivitas organisasi.
b. Terstruktur dan komprehensif, pendeketan yg menyeluruh dan konperhensif pada manajemen risiko memberikan hasil yg konsisten dan dapat dibandingkan
c. Disesuaikan, framework dan proses manajemen risiko disesuaikan dengan konteks internal dan eksternal organisasi.
d. Inklusif, penerapan manajemen resiko harus melibatkan seluruh pihak yang berkepentingan yang memungkinkan presepsi pihak yang berkepentingan menjadi bahan pertimbangan.
e. Dinamis, risiko dapat muncul dan berubah mengikuti perubahan konteks eksternal dan internal organisasi, sehingga manajemen resiko harus mampu mengantisipasi, mendeteksi dan menanggapi perubahan tersebut.
f. Informasi terbaik yang tersedia, seluruh data manajemen risiko didasarkan atas informasi masa lampau dan terkini, dan masa depan. Informasi yang disampaikan harus tepat waktu, relevan sesuai dan selalu tersedia.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

g. Faktor manusia dan budaya, perilaku dan budaya manusia berkaitan dengan pelaksanaan tugas organisasi sehari-hari. memengaruhi semua aspek manajemen risiko pada setiap tingkatan dan tahap.
h. Perbaikan berkelanjutan, penerapan manajemen resiko yang baik harus diperbaiki secara berkelanjutan melalui pembelajaran dan pengalaman. Prinsip ini bertujuan agar framework manajamen resiko dan proses selalu relevan dan dapat digunakan dimasa mendatang.

Framework yang digunakan pada framework ISO 31000:2018, yaitu :

a. Kepemimpinan dan Komitemen, menekankan peran penting pimpinan puncak dalam memastikan manajemen risiko terintegrasi ke dalam seluruh aktivitas organisasi. Pimpinan harus menunjukkan komitmen nyata dengan menetapkan kebijakan, mengalokasikan sumber daya, dan memastikan akuntabilitas semua pihak terkait.
b. Integrasi, sebagai proses yang berkelanjutan, melibatkan seluruh struktur organisasi, dan disesuaikan dengan konteks organisasi. Tujuannya adalah untuk memastikan bahwa manajemen risiko menjadi bagian integral dari tujuan, strategi, dan operasi organisasi.
c. Desain, perancangan desain dalam hal ni mencakup aktivitas-aktivitas seperti analisis konteks organisasi, penetapan kebijakan manajemen risiko, penentuan struktur organisasi untuk manajemen risiko, dan alokasi sumber daya yang diperlukan untuk implementasi sistem manajemen risiko.
d. Implementasi, memerlukan seluruh pemangku kepentingan terlibat aktif dalam pengambilan keputusan dan memastikan keberhasilan implementasi manajemen resiko
e. Evaluasi, dilakukan untuk melihat keefektifan kinerja manajamen resiko agar tetap sesuai untuk mendukung pencapaian sasaran organisasi.
f. Perbaikan, dilakukan secara berkesinambungan untuk meningkatkan kesesuaian, kecukupan dan efektivitas framework manajemen resiko.

Proses manajemen resiko berdasarkan *framework* ISO 31000:2018, meliputi :

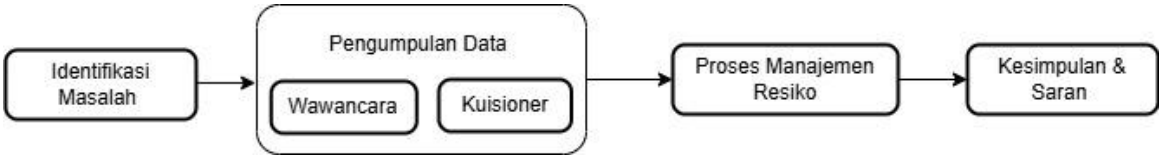
a. Komunikasi dan konsultasi, tahapan awal dalam proses manajemen resiko yang bertujuan agar membantu pemangku kepentingan memahami resiko sebagai dasar pengambilan keputusan
b. Penentuan Konteks, *scope*, kriteria, tahapan yang dilakukan untuk menyelaraskan proses manajemen risiko untuk mendapatkan hasil penilaian dan penanganan risiko yang tepat.
c. Penilaian Resiko, tahapan ini dilakukan untuk mendapatkan hasil penilaian manajemen risiko yang tepat. Penilaian risiko terdiri dari 3 tahapan yaitu identifikasi resiko, analisis resiko, evaluasi resiko.
d. Perlakuan Resiko, tahapan ini memberikan rekomendasi terkait perlakuan resiko berdasarkan hasil evaluasi resiko.
e. Monitoring dan Evaluasi, tahapan ini memastikan terlaksananya suatu aktivitas dalam proses manajemen resiko.

2. METODOLOGI PENELITIAN

PT. Eterindo Nusa Graha, merupakan perusahaan yang bergantung pada penggunaan teknologi informasi untuk mendukung kegiatan operasional perusahaan. Penggunan teknologi informasi tidak menutup kemungkinan terjadinya ancaman resiko terhadap aset data, aset *software*, aset *hardware* yang dapat

p-ISSN : 2087-0868 e-ISSN : 2598-9707

menganggu aktivitas perusahaan [22]. Analisis manajemen resiko diterapkan bertujuan untuk membantu perusahaan dalam mengidentifikasi, menganalisis menilai dan memberikan rekomendasi perlakuan resiko. Tahapan pertama dalam penelitian ini dimulai dengan mengidentifikasi permasalahan yang terjadi di PT. Eterindo Nusa Graha diakhiri dengan pemberian rekomendasi perlakuan resiko. Terdapat beberapa tahapan yang dilaksanakan pada penelitian ini yang ditinjau pada gambar berikut.



Gambar 2 Tahapan Penelitian

3.1 Identifikasi Masalah

Tahapan pertama yang dilakukan untuk pengumpulan informasi terkait potensi permasalahan yang mungkin atau pernah terjadi pada penggunaan teknologi informasi di PT. Eterindo Nusa Graha.

3.2 Pengumpulan Data

Tahapan pengumpulan data dilakukan menggunakan tiga metode untuk mendapatkan informasi terkait

permasalahan teknologi informasi yang pernah terjadi di PT. Eterindo Nusa Graha :

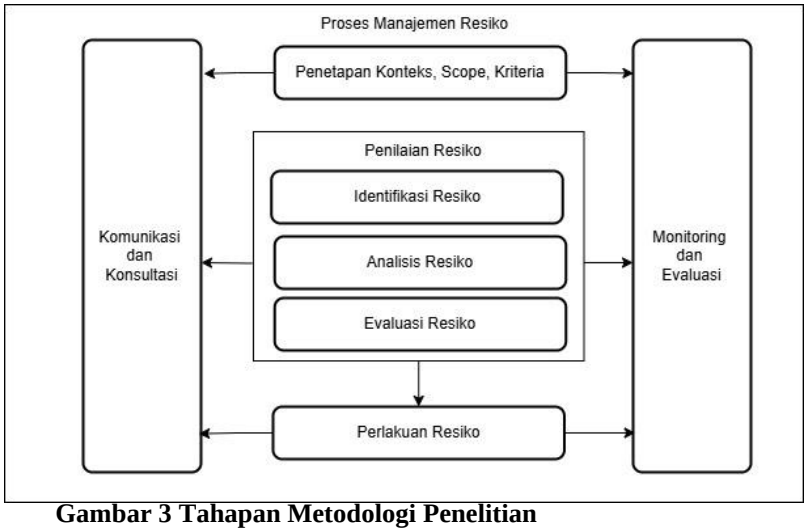
a. Wawancara

Wawancara dilakukan dengan kepala divisi IT PT. Eterindo Nusa Graha yang bertujuan untuk memperoleh informasi/data yang lebih mendalam tentang risiko atau permasalahan teknologi informasi yang pernah terjadi di PT. Eterindo Nusa Graha.

b. Kuisioner

Kuisioner dibagikan kepada beberapa divisi di PT. Eterindo Nusa Graha yang menggunakan teknologi informasi dalam aktivitasnya, tujuan dari kuisioner ini untuk menilai resiko berdasarkan kriteria *likelihood* dan kriteria *impac*t pada sebuah resiko teknologi informasi yang nantinya dapat memberikan rekomendasi perlakuan resiko.

3.3 Proses Manajemen Resiko berdasarkan ISO31000:2018



Gambar 3 Tahapan Metodologi Penelitian

Terdapat 5 Proses kegiatan yang digunakan pada *framework* ISO 31000:2018 antara lain :

a. Komunikasi dan Konsultasi, membantu memberikan pemahaman kepada pemangku kepentingan tentang ancaman resiko sebagai dasar pengambilan keputusan atas tindakan tertentu [23].

p-ISSN : 2087-0868 e-ISSN : 2598-9707

b. Penetapan Konteks, Scope, Kriteria

a. Konteks pada penelitian ini terbagi menjadi 2 konteks yaitu :
- Konteks Internal pada penelitian ini yaitu visi misi perusahaan, struktur organisasi perusahaan, sumber daya manusia.
- Konteks Eksternal pada penelitian ini yaitu stakeholder terkait

b. Scope pada penelitan ini melakukan analisis manajemen resiko teknologi informasi yang digunakan di PT. Eterindo Nusa Graha

c. Kriteria pada proses ini terdapat 2 kriteria resiko yaitu :
- Kriteria *likelihood* merupakan kriteria yang mengukur tingkat kemungkinan terjadinya suatu resiko dengan frekuensi kejadian.

Tabel 1 Kriteria Likelihood

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

- Kriteria *Impact* merupakan kriteria yang mengukur dampak yang terjadi dari sebuah resiko terhadap perusahaan tersebut.

Tabel 2 Kriteria Impact

Impact		**Keterangan**
Nilai	**Kriteria**	
1	*Insignificant*	Risiko yang dampaknya tidak mengganggu proses dan aktivitas perusahaan
2	*Minor*	Risiko yang dampaknya sedikit mengganggu proses dan aktivitas perusahaan
3	*Moderate*	Risiko yang dampaknya cukup mengganggu dan menghambat sebagian proses dan aktivitas perusahaan.
4	*Major*	Risiko yang dampaknya menghambat seluruh proses dan aktivitas perusahaan
5	*Catastrophic*	Risiko yang dampaknya dapat menghentikan total proses dan aktivitas perusahaan

c. Penilaian Resiko

Dalam melakukan penilaian risiko terdapat 4 tahapan, berikut penjelasan terkait tahapan penilian resiko tersebut:

1. Identifikasi aset, merupakan tahapan yang akan memberikan suatu gambaran mengenai aset-aset teknologi infromasi yang digunakan oleh PT. Eterindo Nusa Graha. Adapun identifikasi aset tersebut dikelompokkan ke dalam 3 bentuk, yaitu aset data, aset *software*, dan aset *hardware*.
2. Identifikasi risiko, merupakan tahapan untuk mengenali potensi risiko yang mungkin atau pernah terjadi, yang dapat mengancam aset dan aktivitas

p-ISSN : 2087-0868 e-ISSN : 2598-9707

perusahaan. Identifikasi risiko dikategorikan berdasarkan tiga faktor utama, yaitu alam dan lingkungan, sumber daya manusia, serta sistem dan infrastruktur. Tahapan ini memberikan penjelasan mengenai penyebab dan dampak dari setiap risiko yang teridentifikasi.

3. Analisis resiko, merupakan tahapan yang dilakukan setelah proses identifikasi risiko. Analisis risiko dilakukan dengan menggunakan rumus perkalian antara kriteria *likelihood* dengan kriteria *impact* untuk menghasilkan tingkatan resiko.

Tingkatan Resiko = Kriteria *Likelihood* × Kriteria *Impact* (1)

4. Evaluasi Resiko, merupakan tahapan untuk menentukan tingkat risiko dan mengidentifikasi risiko yang memerlukan penanganan secepatnya. Evaluasi ini dilakukan dengan memetakan kriteria *likelihood* (kemungkinan) dan kriteria *impact* (dampak) dari setiap risiko berdasarkan matriks evaluasi risiko. Evaluasi risiko menggunakan acuan berupa matriks risiko, matriks tersebut dibedakan ke dalam 3 level resiko yaitu rendah, sedang dan tinggi.

Tabel 3 Matriks evaluasi resiko

Likelihood	*Certain*	5	Sedang	Sedang	Tinggi	Tinggi	Tinggi
	Likely	4	Sedang	Sedang	Sedang	Tinggi	Tinggi
	Possible	3	Rendah	Sedang	Sedang	Sedang	Tinggi
	Unlikely	2	Rendah	Rendah	Sedang	Sedang	Sedang
	Rare	1	Rendah	Rendah	Rendah	Sedang	Sedang
Matriks Evaluasi Resiko			1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
			Impact				

Tabel 4 Level resiko

Level Resiko	Keterangan
Resiko Tinggi	Resiko berbahaya yang harus diatasi secepatnya
Resiko Sedang	Risiko ini harus dimonitor dan membutuhkann penanganann yang berkelanjutann.
Resiko Rendah	Risiko ini dapat diabaikann dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil

d. Perlakuan Resiko,

Berdasarkan hasil pemetaan menggunakan matriks evaluasi risiko, dapat diketahui tingkat level risiko. Tahap ini memberikan rekomendasi untuk penanganan risiko yang sesuai dengan tingkatannya. Mengacu pada *framework* ISO 31000:2018 yang dibagi menjadi 4 (empat) kategori perlakuan resiko yang dijelaskan pada tabel 5.

Tabel 5 Perlakuan Resiko

No	Perlakuan Resiko	Keterangan
1	*Acceptance*	Menerima beberapa risiko sebagai bagian penting dari aktivitas walaupun beberapa risiko dapat dihilangkan dengan cara mengurangi maupun berbagi.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

2	*Avoidance*	Menghindari bahaya dengan menjauhi atau tidak berpartisipasi dalam aktivitas berisiko.
3	*Transfer*	Berbagi risiko kepada pihak lain, umumnya melalui suatu kontrak (asuransi).
4	*Mitigasi*	Mengurangi kemungkinan terjadinya suatu risiko ataupun mengurangi dampak kerusakan yang dihasilkan oleh suatu risiko.

3. HASIL DAN PEMBAHASAN

4.1 Penetapan Konteks, Scope, Kriteria

Tahapan awal manajemen risiko TI adalah penetapan konteks, scope, kriteria. Dengan melalui tahapan
tersebut dapat bertujuan untuk mengetahui kondisi perusahaan agar dapat menghasilkan dokumen manajemen risiko TI yang baik dan tepat.

a. Konteks

Penetapan konteks pada proses manajemen risiko secara umum terdapat 2 (dua) konteks meliputi konteks internal dan konteks eksternal dengan penjelasan pada table berikut :

Tabel 6 Konteks Resiko

Konteks		Keterangan
Internal	-	Visi dan Misi PT. Eterindo Nusa Graha
	-	Struktur Organisasi
	-	Sumber Daya Manusia
Eksternal	-	PT. Petrowidada
	-	PT. Petrokimia Gresik
	-	PT. Jotun Indonesia
	-	PT. Nipsea Paint And Chemical Co. Ltd.

b. Scope

Penetapan *scope* dilakukan untuk membatasi ruang lingkup proses manajemen risiko agar lebih fokus dan terarah. Scope pada penelitian ini yaitu teknologi informasi yang digunakan dan milik PT. Eterindo Nusa Graha.

c. Kriteria

Terdapat dua kriteria yang menjadi indikator penilaian proses manajemen resiko. Kriteria *likelihood* dapat dilihat pada tabel 1 dan kriteria *impact* dapat dilihat pada tabel 2. Kedua kriteria tersebut nantinya akan dilakukan pengkalian yang menghasilkan tingkatan level resiko sebagai acuan untuk menentukan rekomendasi perlakukan resiko.

4.2 Penilaian Resiko

4.2.1 Identifikasi Aset

Tahap ini dilakukan identifikasi aset – aset yang dimiliki oleh perusahaan. Identifikasi aset tdikelompokkan ke dalam tiga kategori, yaitu aset data, aset *software*, dan aset *hardware*. Tabel 7 merupakan daftar aset yang dimiliki oleh PT. Eterindo Nusa Graha.

Tabel 7 Aset PT. Eterindo Nusa Graha

Jenis Aset	Bentuk Aset
Aset Data	- Data *Procurement* - Data *Production* - Data *Marketing* - Data *Inventory* - Data *Finance*
Aset Software	- Aplikasi Foxpro - Aplikasi Smart2k (Absensi)

p-ISSN : 2087-0868 e-ISSN : 2598-9707

Aset Hardware	- PC - PC DCS - CCTV - Laptop - WIFI - *Fingerprint* (Absensi)	- *Printer* - FO Converter Alied Telesyn - Cisco Router 1800 series - Switch HP Manageable - Switch TPLINK

4.2.2 Identifikasi Resiko

Tahap identifikasi resiko, pada tahap ini peneliti mengidentifikasi resiko yang mungkin akan/pernah terjadi di PT. Eterindo Nusa Graha berdasarkan hasil wawancara dengan kepala divisi IT PT. Eterindo Nusa Graha. Setelah itu resiko akan dikelompokan berdasarkan tiga faktor resiko, yaitu alam dan lingkungan, sumber daya manusia, sistem dan infrastruktur. Indentifikasi resiko dijelaskan pada tabel 8 dengan keterangan berdasarkan resiko yang mungkin terjadi, penyebab dan dampak dari resiko tersebut.

Tabel 8 Identifikasi Resiko PT. Eterindo Nusa Graha

FAKTOR RESIKO	KODE RESIKO	RESIKO YANG MUNGKIN TERJADI	PENYEBAB RESIKO	DAMPAK RESIKO
ALAM DAN LINGKUNGAN	**RAL01**	Gempa Bumi	Perusahaan berada di Wilayah Gresik yang merupakan Salah satu daerah yang terletak di sepanjang zona subduksi aktif rawan terjadinya bencana gempa bumi.	Gempa bumi dengan skala besar dapat menghentikan seluruh aktivitas Perusahaan. Bencana ini mengakibatkan kerusakan infrastruktur bangunan yang menyebabkan aset hardware mengalami kerusakan akibatnya aset software perusahaan tidak dapat diakses dan berpotensi perusahaan mengalami kehilangan data.
	RAL02	Angin Puting Beliung	Perusahaan berada di Wilayah Gresik yang merupakan Salah satu daerah yang terletak di sepanjang zona subduksi aktif rawan terjadinya bencana gempa bumi.	Angin puting beliung memiliki dampak yang cukup menganggu dan menghambat sebagian proses dan aktivitas perusahaan. Bencana ini menimbulkan dampak seperti rusaknya fasilitas fisik perusahaan, termasuk perangkat keras yang dapat mengakibatkan terganggunya operasional *software* serta hilangnya data penting karena kerusakan pada infrastruktur dan peralatan pendukung.
	RAL03	Hujan Badai	Perusahaan berada di Wilayah yang berjarak 6.0 Km dari pesisir laut Gresik yang rentan terhadap badai karena interaksi antara angin laut dan darat yang menciptakan tekanan	Hujan badai memiliki dampak yang cukup menganggu dan menghambat sebagian proses dan aktivitas perusahaan. Bencana ini menimbulkan rusaknya infrastruktur fisik akibat sambaran petir yang menyebabkan terganggunya operasional *software* dan

p-ISSN : 2087-0868 e-ISSN : 2598-9707

			rendah, memperkuat potensi cuaca ekstrem.	resiko hilangnya data penting perusahaan.
	RAL04	Kebakaran	Perusahaan memproduksi produk bahan kimia yang mempunyai sifat mudah terbakar dan perusahaan berada diwilayah yang merupakan kawasan industri kimia.	Kebakaran memiliki dampak yang cukup menganggu dan menghambat sebagian proses dan aktivitas perusahaan. Bencana ini mengakibatkan rusaknya perangkat keras seperti server, komputer, serta terganggunya operasional *software* dan resiko hilangnya data perusahaan jika tidak ada rencana pemulihan bencana yang efektif.
	RAL05	Ledakan	Perusahaan memproduksi produk bahan kimia yang mempunyai sifat mudah meledek dan perusahaan berada diwilayah yang merupakan kawasan industri kimia.	Kebakaran memiliki dampak dapat menghambat seluruh proses dan aktivitas perusahaan. Bencana ini menimbulkan dampak seperti kerusakan sarana dan prasarana perusahaan, rusaknya aset hardware perusahaan yang dapat mengakibatkan operasional *software* terganggu dan resiko kehilangan data perusahaan.
SUMBER DAYA MANUASIA	**RSDM01**	Penyalagunaan Hak Akses Perusahaan	Tedapat Kebijakan yang memperbolehkan pegawai membawa pulang aset hardware (laptop) berpotensi menyebabkan perangkat tersebut digunakan untuk mengakses hal-hal di luar kepentingan atau pekerjaan perusahaan.	Penyalahgunaan hak akses perusahaan dapat menyebabkan resiko aset *hardware* perusahaan digunakan untuk mengakses kepentingan pribadi yang dapat menyebabkan resiko serangan virus terhadap aset *software* perusahaan dan menyebabkan resiko pencurian dak kebocoran data perusahaan.
	RSDM02	*Humaneror*	Tenaga kerja yang tidak fokus bekerja, tidak mematuhi SOP perusahaan.	*Humaneror* dapat meninmbulkan dampak kesalahan dalam input data, tidak sengaja menghapus data perusahaan. Serta kerusakan aset hardware dikarenakan pegawai yang tidak mematuhi SOP penggunan aset dengan baik sehingga menyebabkan sistem *software* mengalami gangguan operasional dan aktivitas perusahaan terganggu.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

	RSDM03	Kurangnya SDM dari segi kuantitas	Kebijakan pengurangan tenaga kerja serta Anggaran untuk perekrutan atau penggajian yang tidak mencukupi.	Kurangnya SDM dari segi kuantitas dapat menyebabkan aktivitas perusahaan cukup terganggu karena lambatnya perbaikan apabila terjadi permasalahan kerusakan aset *sofware* dan *hardware* secara bersamaan, serta pengelolaan data yang menjadi tidak maksimal.
	RSDM04	Kurangnya SDM dari segi kualitas	Tidak semua SDM memiliki pengalaman kerja dan pengalaman pelatihan yang relevan dengan kebutuhan spesifik perusahaan.	Kurangnya SDM dari segi kualitas dapat menyebabkan aktivitas perusahaan cukup terganggu. Karena kurangnya pemahaman/pengetahuan pegawai dalam mengoperasikan aset *hardware* mengakibatkan aset mengalami kerusakan, serta pengelolaan data menjadi tidak maksimal dikarenakan adanya pegawai yang tidak dapat mengoperasikan aplikasi dikarenakan kurangnya pelatihan mengenai penggunaan aplikasi tersebut.
	RSDM05	Permasalahan dengan Pihak Ketiga	Pihak ketiga tidak memiliki kapasitas yang memadai untuk memenuhi peningkatan kebutuhan perusahaan.	Menyebabkan aktivitas perusahaan cukup terganggu karena resiko kehilangan / kerusakan aset karena pihak ketiga tidak mematuhi regulasi atau kebijakan dari perusahaan, serta resiko penyalagunaan hak akses sistem *software* yang dapat menyebabkan resiko kehilangan / pencurian data perusahaan.
SISTEM DAN INFRASTRUKTUR	**RSI01**	Pemadaman Listrik	Beban listrik yang melebihi kapasitas sistem sehingga terjadinya pemdaman lokal. Adanya gangguan teknis pada infrastruktur penyedia listrik, seperti kerusakan kabel atau trafo.	Menghambat seluruh proses dan aktivitas perusahaan karena kerusakan pada perangkat keras akibat mati listrik mendadak, serta kerusakan pada sistem operasi atau aplikasi yang sedang berjalan mengakibatkan data tidak tersimpan/kehilangan data jika tidak ada sistem cadagan (*backup*) yang memadai, file data yang diakses atau diproses bisa menjadi korup.
	RSI02	Aplikasi Software	Dalam menjalankan proses bisnisnya, perusahaan	Menyebabkan kehilangan data akibat *error / bug* pada saat mengoperasikan sistem

p-ISSN : 2087-0868 e-ISSN : 2598-9707

		Perusahaan Bermasalah	mengandalkan penggunaan aplikasi ERP yang dikembangkan oleh perusahaan. Ketergantungan ini dapat menimbulkan potensi masalah pada aplikasi ERP, seperti terjadinya kemacetan atau gangguan lainnya.	*software*, terganggunya operasional sistem IT, peningkatan beban kerja pada perangkat keras yang berpotensi memperpendek umur perangkat.
	RSI03	CCTV tidak berfungsi dengan baik	Kabel kamera yang rusak atau terputus	Menyebabkan tidak adanya bukti rekaman yang bisa digunakan untuk investigasi apabila seseorang melakukan pencurian aset data , aset *software*, aset *hardware* secara langsung.
	RSI04	Kerusahan *Hardware*	Penggunaan yang tidak sesuai dengan SOP, seperti kebijakan yang memperbolehkan pegawai membawa pulang hardware (laptop), berpotensi menyebabkan perangkat tersebut digunakan untuk keperluan di luar pekerjaan atau kepentingan perusahaan.	Menyebabkan gangguan fungsi *software* yang memerlukan perangkat keras untuk beroperasi, serta menyebabkan tidak dapat mengakses data penting yang disimpan pada perangkat sehingga menghambat aktifitas perusahaan.
	RSI05	*Serverdown*	Semua aktivitas perusahaan bergantung pada aplikasi yang menggunakan server yang sama, sehingga menyebabkan lalu lintas server menjadi sangat padat. Hal ini mengakibatkan server mengalami masalah atau *down* karena terlalu banyak pengguna yang mengakses aplikasi tersebut. Selain itu, komponen server yang sudah tua atau kurang terawat juga dapat memperburuk kondisi ini.	Menyebabkan kerusakan pada komponen server, *power suply*, akibat *shutdown* mendadak atau penggunaan yang tidak optimal , serta menyebabkan sistem aplikasi atau layanan yang bergantung pada server menjadi tidak dapat diakses atau tidak berfungsi sehingga menyebabkan kehilangan data jika *serverdown* terjadi saat proses penyimpanan atau transfer data sedang berlangsung
	RSI06	Jaringan Internet Tidak Stabil	Proses bisnis perusahaan sangat bergantung pada ketersediaan jaringan internet yang disediakan oleh penyedia layanan.	menyebabkan gangguan dalam akses dan *transfer* data, meningkatkan risiko kehilangan atau kerusakan data akibat koneksi yang

p-ISSN : 2087-0868 e-ISSN : 2598-9707

	Hal ini memungkinkan terjadinya masalah atau kelambatan koneksi internet dari penyedia layanan.	terputus, menghambat kinerja *software* berbasis *cloud* atau sistem terintegrasi, serta berpotensi merusak *hardware* jaringan akibat lonjakan beban kerja yang tidak teratur, yang pada akhirnya dapat mengganggu aktivitas perusahaan.

4.2.3 Analisis Resiko

Pada tahapan ini dilakukan penilaian menggunakan rumus persamaan (1) yang menghasilkan tingkatan resiko. Hasil penilaian analisis resiko dapat dilihat pada table 9.

Tabel 9 Penilaian Analisis Resiko

KODE RESIKO	RESIKO YANG MUNGKIN TERJADI	*Likelihood*	*Impact*	*Nilai Resiko*
RAL01	Gempa Bumi	1	4	4
RAL02	Angin Puting Beliung	1	3	3
RAL03	Hujan Badai	1	3	3
RAL04	Kebakaran	1	3	3
RAL05	Ledakan	2	4	8
RSDM01	Penyalagunaan Hak Akses Perusahaan	2	2	4
RSDM02	Human Eror	2	2	4
RSDM03	Kurangnya SDM dari segi kuantitas	2	3	6
RSDM04	Kurangnya SDM dari segi kualitas	2	3	6
RSDM05	Permasalahan dengan Pihak Ketiga	2	3	6
RSI01	Pemadaman Listrik	4	4	16
RSI02	Aplikasi Software Perusahaan Bermasalah	2	3	6
RSI03	CCTV tidak berfungsi dengan baik	2	3	6
RSI04	Kerusahan Hardware	2	3	6
RSI05	Serverdown	2	3	6
RSI06	Jaringan Internet Tidak Stabil	2	3	6

4.2.4 Evaluasi Resiko

Proses pemetaan untuk menentukan risiko yang perlu diprioritaskan. menggunakan acuan berupa matriks evaluasi resiko yang terbagi dalam tiga tingkatan yaitu, rendah, sedang dan tinggi.

Tabel 10 Pemetaan Risiko Menggunakan Matriks Evaluasi Resiko

Likelihood							
	Certain	5	1	2	3	4	5
	Likely	4	6	7	8	**RSI01**	10
	Possible	3	11	12	13	14	15
	Unlikely	2	16	**RSDM01, RSDM02**	**RSDM03,RSDM04, RSDM05,RSI02, RSI03,RSI04, RSI05, RSI06**	19	20
	Rare	1	21	22	**RAL02 , RAL03 , RAL04**	RAL001	25
	Matriks Evaluasi Resiko		*1*	*2*	*3*	*4*	*5*
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

p-ISSN : 2087-0868 e-ISSN : 2598-9707

				Impact

Berdasarkan pemetaan risiko pada tabel 10, risiko tersebar di berbagai tingkatan risiko, terdapat 16 kemungkinan resiko yang terdiri dari 5 resiko berada pada tingkatan rendah, 10 resiko berada pada tingkatan sedang dan 1 resiko yang berada pada tingkatan tinggi.

4.3 Perlakuan Resiko

Pada tahap ini akan diberikan rekomendasi perlakuan resiko yang dijelaskan pada table 11. Dengan adanya rekomendasi yang diusulkan diharapkan resiko yang terjadi dapat diminimalisir agar tidak terjadi kerugian ketika resiko-resiko tersebut muncul.

Tabel 11 Perlakuan Risiko

No	Faktor resiko	Resiko yang mungkin terjadi	Rekomendasi	Perlakuan Resiko
1	Faktor Alam dan Lingkungan terhadap Aset Data	Gempa Bumi , Angin Putting Beliung , Hujan Badai , Kebakaran , Ledakan	*Acceptance*	Mengakui bahwa risiko bencana tidak sepenuhnya dapat dihindari dan dampaknya dianggap dapat ditoleransi dalam batas tertentu dan diadaknnya pemusatan data utama menggunakan *Cloud System*
			Avoidance	Tidak menggunakan pemusatan data program secara lokal (internal)
			Transfer	Menggunakan beberapa *provider cloud system* dengan mekanisme replikasi data
			Mitigasi	Menggunakan beberapa *provider cloud system* dengan mekanisme replikasi data
2	Faktor Alam dan Lingkungan terhadap Aset Software	Gempa Bumi , Angin Putting Beliung , Hujan Badai , Kebakaran , Ledakan	*Acceptance*	Mengakui bahwa risiko bencana tidak sepenuhnya dapat dihindari dan dampaknya dianggap dapat ditoleransi dalam batas tertentu dan menggunakan *Virtual Private Server*
			Avoidance	Tidak hanya menggunakan server internal dalam menjalankan aplikasi

p-ISSN : 2087-0868 e-ISSN : 2598-9707

			Transfer	Mengunakan pihak eksternal (VPS) dalam tempat menjalankan aplikasi / *software*
			Mitigasi	Mengunakan pihak eksternal (VPS) dalam tempat menjalankan aplikasi / *software*
3	Faktor Alam dan Lingkungan terhadap Aset Hardware	Gempa Bumi , Angin Putting Beliung , Hujan Badai , Kebakaran , Ledakan	*Acceptance*	Mengakui bahwa risiko bencana tidak sepenuhnya dapat dihindari dan dampaknya dianggap dapat ditoleransi dalam batas tertentu dan menyediakan *spare part* untuk *hardware network*
			Avoidance	Pengunaan perangkat keras *mobile* oleh setiap *user* (laptop, modem)
			Transfer	Menggunakan asuransi untuk perlindungan aset data fisik terhadap kerusakan akibat kebakaran, ledakan, atau bencana alam
			Mitigasi	perlindungan struktural, penempatan aman, penggunaan perangkat pencegahan (braket anti-gempa, penutup anti-air, detektor asap), serta pemisahan dari area berisiko tinggi seperti zona rawan angin, banjir, kebakaran, dan ledakan.
4	Faktor Sumber Daya Manusia Terhadap Aset Data	Penyalagunaan Hak Akses , Human Eror , Kurangnya SDM dari segi kuantitas , Kurangnya SDM dari segi kualitas , Permasalahan dengan Pihak Ketiga	*Acceptance*	Menyadari bahwa *human error* tidak sepenuhnya dapat dihilangkan namun dapat diadakan pelatihan maupun koneseling untuk user oleh tim IT
			Avoidance	Menerapkan pemberian akses berupa paswoord sesuai akses level jabatan
			Transfer	Menggunakan layanan *cloud* pihak ketiga yang sudah memiliki

p-ISSN : 2087-0868 e-ISSN : 2598-9707

				sertifikasi keamanan yaitu *Google Cloud*
			Mitigasi	Perusahaan sudah menggunakan *firewall* untuk server dan anti virus AVG tiap PC user
5	Faktor Sumber Daya Manusia Terhadap Aset Software	Penyalagunaan Hak Akses , Human Eror , Kurangnya SDM dari segi kuantitas , Kurangnya SDM dari segi kualitas , Permasalahan dengan Pihak Ketiga	*Acceptance*	Menerima risiko *downtime* kecil akibat kesalahan dan melakukan penghapusan / *kill* user oleh tim IT
			Avoidance	Menghindari risiko dengan memastikan upgrade versi ERP untuk pembaruan *software* oleh tim IT
			Transfer	Perusahaan sudah menggunakan internal *resource* oleh tim IT
			Mitigasi	Menyediakan pelatihan kepada karyawan baru tentang penggunaan *software* ERP dan melakukan sosialisasi *upgrade* aplikasi terhadap user
6	Faktor Sumber Daya Manusia Terhadap Aset *Hardware*	Penyalagunaan Hak Akses , *Humaneror* , Kurangnya SDM dari segi kuantitas , Kurangnya SDM dari segi kualitas , Permasalahan dengan Pihak Ketiga	*Acceptance*	Menerima risiko kerusakan minor yang tidak memengaruhi operasional utama, seperti kerusakan perangkat dan perusahaan selalu ada *spare* untuk kerusakan minor oleh tim IT
			Avoidance	Menghindari risiko dengan menyediakan perangkat keras yang sesuai dengan standar, seperti pemasangan UPS disetiap titik *hardware* yang dirasa cukup penting
			Transfer	Membeli asuransi untuk melindungi perangkat keras dari kerusakan atau kehilangan. Selain itu, mengalihdayakan pemeliharaan perangkat

p-ISSN : 2087-0868 e-ISSN : 2598-9707

				keras kepada pihak ketiga.
			Mitigasi	Melakukan pemeliharaan rutin dan inspeksi berkala terhadap perangkat keras yang dilakukan oleh tim IT
7	Faktor Sistem dan Infrastruktur Terhadap Aset Data	Pemadaman Listrik , Aplikasi *Software* Perusahaan Bermasalah , CCTV tidak berfungsi dengan baik , Kerusahan *Hardware* , *Serverdown* , Jaringan Internet Tidak Stabil	*Acceptance*	Menerima risiko kecil seperti gangguan sementara akibat jaringan internet yang tidak stabil untuk akses data yang tidak mendesak dan sudah tersedia perangkat UPS di *server* maupun UPS dipanel *Box* CCTV
			Avoidance	Menghindari risiko dengan *backup* data otomatis menggunakan sistem *cloud* dn adanya perangkat UPS
			Transfer	Perusahaan sudah menggunakan penyedia layanan *cloud* yaitu *Google Cloud*
			Mitigasi	Sudah diterapakan perusahaan untuk backup secara otomatis
8	Faktor Sistem dan Infrastruktur Terhadap Aset *Software*	Pemadaman Listrik , Aplikasi *Software* Perusahaan Bermasalah , CCTV tidak berfungsi dengan baik , Kerusahan *Hardware* , *Serverdown* , Jaringan Internet Tidak Stabil	*Acceptance*	Menerima *downtime* kecil pada *software* yang tidak kritis, misalnya *software* internal untuk pengelolaan tugas *non-urgent* dan sudah adanya *autorecovery* untuk soft yang tidak kritis
			Avoidance	Menghindari risiko dengan menguji upgrade versi selalu dilakukan secara trial sebelum dishare ke user
			Transfer	Pembaruan selalu dilaksanakan oleh tim IT perusahaan

p-ISSN : 2087-0868 e-ISSN : 2598-9707

			Mitigasi	Melakukan inspeksi berkala terhadap *software* pendukung untuk mekmastikan *server* kompatibel dalam mendukung aplikasi berjalan dengan baik
9	Faktor Sistem dan Infrastruktur Terhadap Aset *Hardware*	Pemadaman Listrik , Aplikasi Software Perusahaan Bermasalah , CCTV tidak berfungsi dengan baik , Kerusahan *Hardware* , *Serverdown* , Jaringan Internet Tidak Stabil	*Acceptance*	Menerima risiko kerusakan kecil pada perangkat yang tidak krusial dan melakukan pengadaan permintaan barang sebagai spare
			Avoidance	Melakukan pemeliharaan berkala dan memastikan perangkat lunak pendukung CCTV selalu diperbarui oleh safety patrol
			Transfer	Perusahaan melakukan perawatan perangkat keras tersendiri
			Mitigasi	Melakukan inspeksi berkala terhadap perangkat keras untuk mendeteksi potensi kerusakan lebih awal. Menyediakan *hardware* cadangan seperti IP CAM, POE dan NVR sebagai *spare* , serta melakukan *upgrade server* sesuai dengan kebutuhan aplikasi.

4. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setalah dilakukan hasil analisis yang dilakukan, dapat disimpulkan bahwa PT. Eterindo Nusa Graha sudah cukup baik dalam menerapkan manajemen risiko. Dari total 16 kemungkinan risiko yang teridentifikasi, sebanyak 5 risiko dengan tingkat rendah , 10 risiko dengan tingkat sedang dan hanya 1 risiko dengan tingkat tinggi . Hal ini menunjukkan bahwa sebagian besar risiko masih dalam tingkat yang dapat dikendalikan, meskipun tetap diperlukan perhatian dan strategi mitigasi yang efektif untuk memastikan bahwa risiko-risiko tersebut tidak berkembang menjadi lebih serius. Keberhasilan perusahaan dalam mengelola sebagian besar risiko dengan baik mencerminkan adanya sistem pengelolaan risiko yang baik. Namun, risiko yang berada dalam kategori tinggi harus menjadi fokus utama dalam upaya mitigasi, mengingat dampaknya yang berpotensi besar terhadap operasional perusahaan.

5.2 Saran

Diharapkan dari hasil analisis manajemen risiko teknologi informasi di PT. Eterindo Nusa Graha menggunakan *framework* ISO 31000:2018 dapat diterapkan secara bertahap dan berkelanjutan.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

Mengingat risiko dalam dunia teknologi informasi terus berkembang seiring dengan kemajuan teknologi. Perusahaan perlu mengadopsi pendekatan yang fleksibel dan adaptif dalam pengelolaan risiko agar dapat menghadapi tantangan baru yang mungkin muncul di masa depan.

DAFTAR PUSTAKA

[1] A. Taufik, G. Sudarsono, I. K. Sudaryana, and T. T. Muryono, "Pengantar teknologi informasi," *Yayasan Drestanta Pelita Indonesia*, pp. 1–113, 2022.

[2] L. F. Putra, A. Profita, T. Industri, F. Teknik, and U. Mulawarman, "Analisis Risiko Website Telkom Emas Data Validation Menggunakan Iso 31000," *PROFISIENSI J. Progr. Stud. Tek. Ind*, vol. 10, no. 2, pp. 175–183, 2022.

[3] G. K. Geofanny, "Sistem manajemen risiko berbasis iso 31000: 2018 di pt. Bawen mediatama," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, no. 4, pp. 2870–2878, 2022.

[4] G. Gioferi and Y. Yulhendri, "Penilaian Risiko TI Pada Website DosenIT Dengan Framework ISO 31000 Dan ISO 27002," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 5, no. 4, pp. 409–419, 2023.

[5] J. N. Utamajaya, A. Afrina, and A. N. Fitriah, "Analisis Manajemen Risiko Teknologi Informasi Pada Perusahaan Toko Ujung Pandang Grosir Penajam Paser Utara Menggunakan Framework Iso 31000: 2018," *Sebatik*, vol. 25, no. 2, pp. 326–334, 2021.

[6] D. L. Ivander and F. S. Papilaya, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000: 2018," *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 4, no. 2, pp. 1042–1051, 2023.

[7] E. Muryanti and K. D. Hartomo, "Analisis Risiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 8, no. 3, pp. 1265–1277, 2021.

[8] S. Rikaz, A. D. Ulhaq, R. H. Mulyono, and R. Cahyaningtyas, "Perancangan Coso Enterprise Risk Management Pada Perusahaan Penerbit Dan Percetakan (Studi Kasus Pada CV. Gema Insani Press)," *E-Prosiding Akuntansi*, vol. 3, no. 1, 2022.

[9] CRMS Indonesia, *Survei Nasional Manajemen Resiko 2018*. 2018.

[10] R. I. Liperda and U. A. S. Nieng, "Analisis Manajemen Resiko Aplikasi Mypertamina Dengan Menggunakan Iso 31000," *INFOTECH journal*, vol. 9, no. 2, pp. 361–370, 2023.

[11] D. P. Natalie and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000: 2018 pada PT Bayu Buana Tbk," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 5, pp. 1290–1301, 2022.

[12] C. C. Turambi and C. Rudianto, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK ISO 31000 PADA UNIT PEGADAIAN CABANG (UPC) RATAHAN," *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, vol. 7, no. 2, pp. 220–235, 2024.

[13] R. H. Pangestu, A. D. Cahyono, and P. F. Tanaem, "Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Mengunakan ISO 31000," *Journal of Computer and Information Systems Ampera*, vol. 2, no. 1, pp. 43–57, 2021.

[14] C. C. Turambi and C. Rudianto, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK ISO 31000 PADA UNIT PEGADAIAN CABANG (UPC) RATAHAN," *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, vol. 7, no. 2, pp. 220–235, 2024.

[15] W. F. Worotikan and E. Maria, "Penerapan ISO 31000: 2018 untuk Manajemen Risiko E-Ticketing Taman Rekreasi XYZ," *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 3, no. 5, pp. 449–456, 2023.

[16] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office," *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, vol. 7, no. 3, pp. 546–558, 2020.

[17] R. H. Pangestu, A. D. Cahyono, and P. F. Tanaem, "Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Mengunakan ISO 31000," *Journal of Computer and Information Systems Ampera*, vol. 2, no. 1, pp. 43–57, 2021.

[18] K. M. L. 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, pp. 319–324, 2022.

[19] V. P. P. Wijaya, "Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000: 2018," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, no. 2, pp. 1295–1307, 2022.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

[20] H. C. S. Suawa and H. P. Chernovita, "Analisis Manajemen Risiko Aplikasi SRIKANDI Pada Kantor Diskominfo Kota Manado Menggunakan ISO 31000," *Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 3, no. 5, pp. 604–616, 2023.
[21] J. Susilo, Leo, R. Kaho, and Susilo, *Pedoman Manjemen Resiko ISO31000:2018* . Jakarta, 2018.
[22] B. Yolanda, M. Nasrullah, and A. Kusumawati, "Analisis Manajemen Risiko dengan Menggunakan Framework ISO 31000: 2018 pada Sistem Informasi E-Gudang Satpol PP Kota Surabaya," *TeIKa*, vol. 14, no. 2, pp. 79–91, 2024.
[23] A. A. Herlambang, A. A. Gani, and D. D. Alvianto, "Pendekatan ISO 31000: 2018 dalam Manajemen Risiko Teknologi Informasi pada Tracer Study Universitas Sebelas April," *Jurnal Intelek Dan Cendikiawan Nusantara*, vol. 1, no. 4, pp. 5651–5660, 2024.