Available online at http://icsejournal.com/index.php/JCSE
JCSE (Journal of Computer Science an Engineering)
e-ISSN 2721-0251
Vol. 1, No. 2, August 2020, pp. 129-146

Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000

Miftakhatun

Universitas Amikom Purwokerto, Jl. Let. Jend. Pol Sumarto Watumas, Purwonegoro - Purwokerto, 53127, Indonesia
Miftakhatunn2828@gmail.com

ARTICLE INFO

Article History:
Received Mei 10, 2020
Revised June 19, 2020
Accepted July 25, 2020
Available Online August 5, 2020

Keywords:
Ecofo Website;
ISO 31000;
Risk Management

Kata Kunci:
Website Ecofo;
ISO 31000;
Manajemen Resiko

Correspondance:
Telephon: +62 85951218906
E-mail: name@domain.email

ABSTRACT

The role of information technology in the current era is becoming large in aspects of life. One of them is in the State-Owned Enterprises (BUMN) in the East Banyumas KPH. The technology applied consists of a web-based information system that is used to manage ticket data designated by Ecofo. The application of technology is inseparable from the issuance of risks that arise that can hamper business processes. The purpose of this research is to study emerging issues and ways to save to minimize risks later on. This study uses the ISO 31000 method, which is a method that specifically discusses risk management, which has five stages of communication and consultation, determining context, risk assessment, risk analysis, risk evaluation), risk use, and monitoring & review. The results of this study consist of documentation found that identified 24 risks that have three levels of high risk, ten levels of medium risk, and 11 levels of low risk that can be used as a reference to improve, manage and finance information technology assets in the future.

ABSTRAK

Peran teknologi informasi di era sekarang berpengaruh besar dalam aspek kehidupan. Salah satunya yaitu di Badan Usaha Milik Negara (BUMN) pada KPH Banyumas Timur. Teknologi yang diterapkan berupa sistem informasi berbasis website yang digunakan untuk pengelolaan data tiket yang bernama Ecofo. Dalam penerapan teknologi tidak terlepas dari kemungkinan risiko yang muncul yang dapat menghambat proses bisnis. Tujuan dari penelitian ini untuk mengetahui kemungkinan muncul dan cara pencegahan maupun penanganan untuk meminimalisir risiko di kemudian hari. Penelitian ini menggunakan metode ISO 31000 yang merupakan sebuah metode yang khusus membahas manajemen risiko yang memiliki 5 tahapan yaitu komunikasi dan konsultasi, menentukan konteks, penilaian risiko (identifikasi risiko, analisis risiko, evaluasi risiko), perlakuan risiko dan monitoring & review. Hasil dari penelitian ini berupa dokumentasi risiko yang ditemukan yaitu teridentifikasi 24 kemungkinan risiko dimana terdapat 3 risiko level high, 10 risiko level medium, dan 11 risiko level low yang dapat dijadikan acuan pencegahan, penanganan dan pemeliharaan terhadap aset teknologi informasi di masa mendatang.

1. Pendahuluan

Peranan teknologi pada aktivitas manusia pada saat ini memang begitu besar. Hampir semua organisasi telah membuka mata dengan memberikan perhatian terhadap perkembangan teknologi khususnya teknologi informasi[1]. Teknologi informasi dapat dimanfaatkan dalam bentuk sistem informasi berbasis website yang mampu mengolah dan menghasilkan suatu informasi yang tepat dan bermanfaat bagi organisasi maupun instansi. Informasi yang dihasilkan tersebut bermanfaat sebagai pendukung perkembangan dan sebagai salah satu komponen utama yang harus diperhatikan oleh organisasi atau instansi yang ingin lebih berkembang [2].

Penggunaan Teknologi Informasi pada perusahaan khususnya pada Badan Usaha Milik Negara (BUMN) merupakan suatu hal penting dan tidak dapat dipisahkan dari proses bisnisnya. Akan tetapi, selama penggunaan dan implementasinya dapat dimungkinkan timbulnya berbagai risiko yang dapat mengancam keberlangsungan proses bisnis. Pengelolaan terhadap kemungkinan munculnya berbagai risiko ini merupakan hal yang perlu diperhatikan. Salah satu langkah awal dalam mengelola risiko-risiko ini yakni melakukan upaya pengukuran terhadap risiko teknologi informasi.

https://doi.org/10.36596/jcse.v1i2.76

Salah satu perusahaan BUMN yang menerapkan teknologi informasi yaitu Kesatuan Pemangkuan Hutan (KPH) Banyumas Timur, yang merupakan perusahaan umum dibawah naungan Perum Perhutani yang merupakan Badan Usaha bergerak dibidang pengelolaan dan pengembangan fungsi hutan dan pemanfataan hutan Milik Negara (BUMN) sebagaimana diatur dalam Undang – Undang Nomor 9 tahun 1969 [3]. Perum Perhutani KPH Banyumas Timur sebagai suatu perusahaan dengan sifat usaha sebagai penyedia pelayanan bagi kemanfaatan umum dan sekaligus memupuk keuntungan dimana dalam mengelola hutannya berdasarkan pada pengelolaan dan kelestarian sumber daya hutan.

KPH Banyumas Timur berupaya memberdayakan masyarakat sekitar hutan melalui industri pariwisata dengan menjalin kerjasama dengan Lembaga Masyarakat Desa Hutan (LMDH). Berdasarkan wawancara dengan junior manager bisnis menjelaskan bahwa sektor wisata yang dikelola KPH Banyumas Timur berupa pemanfaatan hutan sejumlah 24 wisata yang tersebar di Banyumas Raya, Banyumas dan Cilacap 12 Wisata, Purbalingga 8 wisata, dan Banjarnegara 4 wisata. Target keuntungan rata-rata setiap tahunnya sebesar 2,4 milyar yang disokong dari 3 objek wisata terbesar yaitu Selok Cilacap dengan perolehan 450 juta, Kawah Sikidang Banjarnegara 550 juta dan Curug Cipendok 450 juta dan objek wisata hutan lainya. Bagi hasil yang diterapkan dalam pengelolaan wisata itu sebesar 60 persen untuk LMDH dan 40 persen untuk Perhutani yang bertujuan guna meningkatkan kesejahteraan masyarakat daerah hutan. Pada divisi wisata, KPH Banyumas Timur telah menerapkan teknologi informasi untuk mendukung pekerjaan, seperti pendataan penjualan tiket di tempat wisata dengan menggunakan sistem terintegrasi antara KPH dengan tempat wisata. Teknologi informasi yang diguanakan yaitu berupa sistem informasi berbasis website yang bernama“ECOFO”.

Berdasarkan hasil wawancara dengan junior manager bisnis, dijelaskan bahwa Ecofo merupakan website pengelolaan tiket yang khusus digunakan untuk pengelolaan data tiket wisata yang berada di setiap lokasi wisata yang dikelola oleh KPH Banyumas Timur. Ecofo sangat berperan penting bagi perusahaan yang khusus dirancang untuk membantu pekerjaan dalam hal pelayanan pengolahan tiket yang meliputi penginputan, pendataan, dan pelaporan yang dibuat secara komputerisasi dan tersistem yang diharapkan dapat memudahkan perusahaan dalam melakukan proses bisnisnya.

Junior manager bisnis juga menjelaskan bahwa perusahaan belum menerapkan sebuah manajemen risiko. Terdapat permasalahan dan risiko yang kerap muncul, diantaranya sering terjadinya sistem error dimana petugas loket maupun admin tidak dapat melakukan login sebagai akses masuk terhadap website. Hal ini terjadi karena seringnya terdapat gangguan pada infrastruktur jaringan yang menyebabkan sistem tidak bisa di akses. Ketika sistem tidak bisa diakses maka akan melakukan proses transaksi secara manual. Transaksi secara manual memperlambat dalam proses perhitungan dan pelaporan data.

Permasalahan yang sering muncul juga terjadi pada form transaksi. Pada form transaksi terdapat tombol pilihan jenis tiket masuk yang ketika di klik akan memunculkan semua jenis tiket di seluruh wisata. Jenis tiket yang muncul tidak dikelompokan sesuai lokasi tertentu, sedangkan setiap lokasi wisata yang satu dengan yang lainya mempunyai jenis tiket yang berbeda. Oleh sebab itu petugas loket kesulitan dalam pemilihan jenis tiket yang memperlambat proses transaksi dan menimbulkan antrian panjang. Serta pada form laporan perolehan sering terjadi overloading, pada saat tombol pelaporan di klik proses untuk menampilkan data perolehan loading sangat lama, bahkan sering terjadinya gagal akses yang menyebabkan terhambatnya proses download perekapan data hasil perolehan. Website Ecofo juga terhubung dengan mesin android post yang merupakan mesin pencetak tiket yang terhubung melalui teknologi bluetooth yang biasanya sering terputus tiba-tiba yang membuat petugas harus menghubungkan ulang dan mengulangi proses transaksi. Mesin tersebut juga sering kehabisan baterai yang menyebabkan tidak bisa mencetak tiket otomatis.

Permasalahan lainnya yaitu Ecofo belum melakukan upgrade server hosting pada level bisnis yang menyebabkan seringnya terjadi server down dan website tidak dapat berjalan atau diakses. Hal ini sering terjadi pada waktu-waktu tertentu. sebagai contohnya, ketika Wisata Hutan Pinus Limpakuwus mengadakan sebuah event yang cukup besar seperti musik dan wedding, akan meningkatkan jumlah kunjungan yang menyebabkan sibuknya proses transaksi atau penginputan tiket. Pada waktu-waktu tersebut beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Melihat pentingnya sistem tersebut sudah seharusnya perusahaan memiliki server tersendiri yang lebih handal dan lebih menjamin keamanan data.

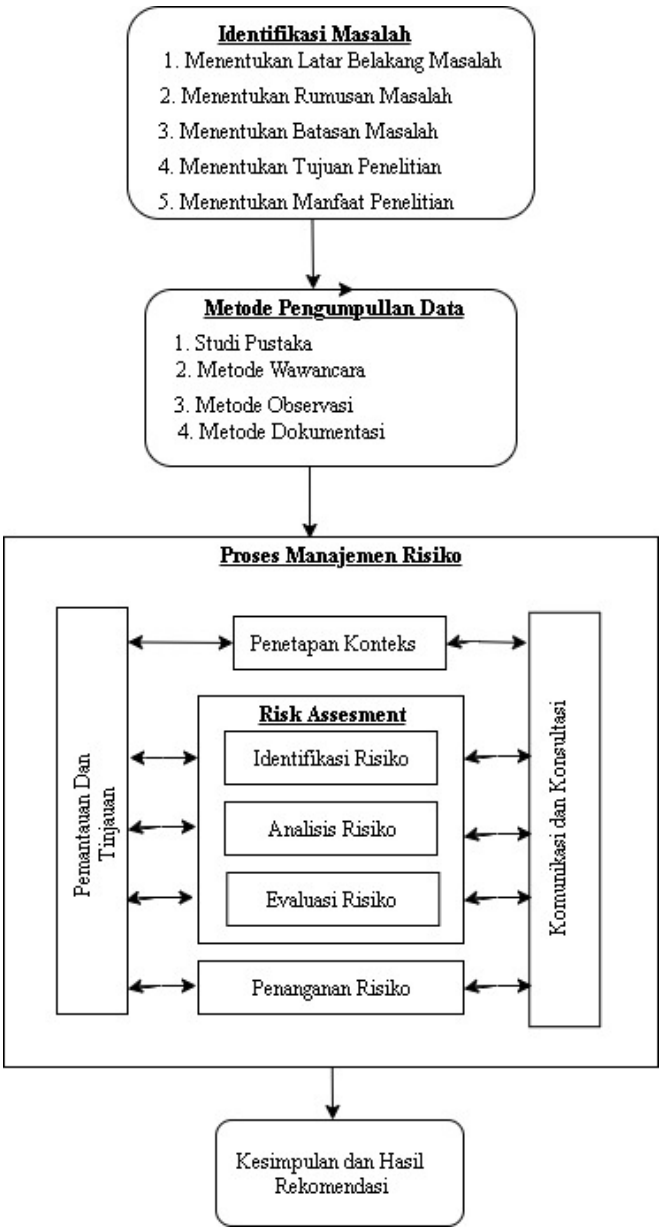
https://doi.org/10.36596/jcse.v1i2.76

Website Ecofo diperoleh dari pihak ketiga dan sampai saat ini perusahaan belum dapat mengatasi permasalahan yang ada, karena tidak ada bagian atau divisi khusus yang menangani sistem yang dipakai. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika risiko tersebut terjadi.
Permasalahan diatas selaras dengan penelitian sebelumnya [4] dijelaskan bahwa penerapan website tidak terlepas dari kendala dan risiko yang terjadi. Risiko yang muncul dapat mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal dan mengganggu proses bisnis perusahaan. Penelitian ini menggunakan metode ISO 31000 yang meliputi identifikasi risiko, penilaian risiko dan pemeliharaan risiko yang bertujuan melakukan pencegahan, penanganan dan pemeliharaan terhadap sistem dan aset pendukung kinerja sistem di masa depan. Hasil dari penelitian ini di dapatkan risiko aset sistem swifts yang membutuhkan koneksi jaringan dan asupan listrik yang konstan agar perangkat dapat berjalan untuk mendukung jalanya sistem secara optimal[5][6].
Suatu perusahaan maupun organisasi memerlukan adanya manajemen risiko. Manajemen Risiko adalah suatu sistem tentang bagaimana sebuah organisasi dipimpin, diarahkan, dan dikendalikan (lead, direct, control) untuk meningkatkan kinerja organisasi demi kepentingan pemegang saham, pemangku kepentingan, dan pertumbuhan ekonomi nasional. Peningkatan kinerja ini dilaksanakan dalam kerangka hukum dan norma-norma etika yang berlaku [7][8].
Pada penelitian ini penulis mengambil salah satu metode untuk manajemen risiko yang sesuai untuk penanganan permasalahan diatas. Metode yang dipilih yaitu ISO 31000 yang dapat digunakan untuk organisasi, perusahaan publik, perusahaan swasta, organisasi nirlaba, kelompok, ataupun perseorangan. Standar ini digunakan digunakan selama masa hidup organisasi dan untuk berbagai kegiatan, proses, fungsi, proyek, produk, jasa, aset, operasi dan pengambilan keputusan. Terdapat lima kegiatan risiko yang termasuk dalam proses manajemen risiko yaitu komunikasi dan konsultasi, menentukan konteks, assesment risiko, perlakuan risiko dan monitoring serta review. Identifikasi risiko, analisis risiko dan evaluasi risiko ketiga hal tersebut termasuk dalam bagian asessment risiko [9][10]

2. Metode

Untuk menyelesaikan masalah pada penelitian yang di angkat peneliti, maka di butuhkan konsep dapat dilihat pada Gambar 1.

https://doi.org/10.36596/jcse.v1i2.76



Gambar 2. Konsep Penelitian

Dari gambar kerangka berikut tersebut, maka dapat di jelaskan sebagai berikut:

1. Identifikasi Masalah

Merupakan langkah awal yang di lakukan untuk mempelajari tentang atau tema yang diangkat oleh peneliti, identifikasi masalah yang di lakukan peneliti adalah sebagai berikut:

a. Menentukan Rumusan Masalah
   Pada tahap ini peneliti menentukan rumusan masalah, yaitu bagaimana melakukan analisis manajemen risiko sistem informasi Ecofo dangan Metode ISO 31000 di Kesatuan Pemangkuan Hutan (KPH) Banyumas Timur

b. Menentukan Batasan Masalah
   Tahap selanjutnya adalah menentikan batasan masalah, yaitu pembuatan difokuskan pada risiko yang terjadi pada sistem informasi Ecofo dan faktor-faktor yang mempengaruhi risiko dari system menggunakan metode ISO 3100 di KPH Banyumas Timur

c. Menentukan Tujuan Penelitian

https://doi.org/10.36596/jcse.v1i2.76

Dalam tahap ini dibuat sebuah sebuah tujuan penelitian, tujuan dari penelitian ini yaitu melakukan tahapan dan proses analisis manajemen risiko pada sistem informasi Ecofo sesuai dengan standar ISO 31000.

d. Menentukan Manfaat Penelitian
Berdasarkan tujuan yang hendak dicapai, maka penelitian ini diharapkan memberikan manfaat bagi KPH Banyumas Timur.

2. Metode Pengumpulan Data
Merupakan cara atau teknik yang digunakan untuk mengumpulkan data maupun informasi yang diperlukan, untuk mendapatkan kebenaran uraian materi pembahasan. Metode pengumpulan data yang digunakan dalam penelitian yaitu studi pustaka, wawancara, observasi dan dokumentasi.

3. Proses Manajemen Risiko ISO 31000
ISO 31000 menyatakan bahwa proses manajemen risiko terdiri dari serangkaian aktivitas sebagai berikut:

a. Komunikasi dan Konsultasi (Communication and Consultation)
Pada penelitian ini komunikasi dan konsultasi dengan pemangku kepentingan sangat penting karena mereka dapat memberikan pertimbangan dan penilaian terhadap risiko yang didasarkan atas persepsi mereka terhadap risiko tersebut.

b. Penetapan konteks (Establishing the Context)
Terdapat empat konteks yang perlu ditentukan dalam penetapan konteks, yaitu konteks internal, konteks eksternal, konteks manajemen risiko, dan kriteria risiko.

c. Assessment Risiko
ISO 31000: 2009 mendefinisikan asesmen risiko sebagai keseluruhan proses identifikasi risiko, analisis risiko, dan evaluasi risiko.

1) Identifikasi Risiko (Risk Identification)
Identifikasi pada penelitian ini menggunakan wawancara langsung dengan pihak yang bertanggung jawab yang mencakup penilaian berdasarkan pengalaman dan pencatatan. Berikut ini adalah proses identifikasi risiko:

a) Identifikasi teknologi informasi yang dimiliki oleh organisasi

b) Identifikasi ancaman pada setiap teknologi informasi

c) Identifikasi kemungkinan risiko yang diakibatkan oleh adanya ancaman

d) Identifikasi dampak yang akan diterima oleh organisasi tersebut

2) Analisis Risiko (Risk Analiysis)

Penelitian ini menerapkan analisis risiko secara kualitatif. Analisis kualitatif merupakan analisis yang cepat dan relatif mudah untuk digunakan untuk jangkauan identifikasi dampak (impact) dan kemungkinan (likelihood) yang luas yang dapat digunakan sebagai bahan evaluasi pemeringkatan risiko. Analisa risiko secara kualitatif merupakan proses penentuan prioritas untuk analisis atau tindakan respon yang lebih jauh dengan mengukur dan mengkombinasikan probabilitas terjadinya risiko serta dampak dari risiko tersebut [11].
Analisa risiko kualitiatif dianggap sebagai tahapan yang paling efektif dan hemat biaya sebab melalui analisa ini, organisasi atau perusahaan dapat melakukan improvisasi terhadap performansi proyek dengan berfokus pada risiko yang memiliki tingkat prioritas tinggi (high-priority risk). Prioritas risiko ini pada akhirnya dapat digunakan pula sebagai dasar dalam melakukan analisa risiko kuantitatif apabila diperlukan. Ketika peluang atau probabilitas (likelihood) serta dampak telah diidentifikasi, maka kemudian akan dilakukan evaluasi untuk mengetahui risiko yang menjadi prioritas untuk ditangani terlebih dahulu [12].

https://doi.org/10.36596/jcse.v1i2.76

Tabel 1. Kriteria *Likelihood*

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

Tabel 2. Kriteria *Impact*

Impact Rating	Kriteria	Keterangan
1	*Insignificant*	Tidak mengganggu operasional dan aktivitas perusahaan
2	*Minor*	Proses bisnis dan aktivitas mengalami gangguan, namun tidak menghambat tugas pokok atau aktivitas inti perusahaan
3	*Moderate*	Proses bisnis mengalami gangguan sehingga sebagian aktivitas terhambat dan mengalami penundaan
4	*Major*	Menghambat hampir seluruh proses bisnis dan aktivitas perusahaan
5	*Catastrophic*	Proses bisnis mengalami gangguan total sehingga aktivitas perusahaan berhenti total dan proses bisnis tidak tercapai

3) Evaluasi Risiko (Risk Evaluation)

Tahap ini melakukan Risk Evaluation atau membandingkan risiko-risiko yang sudah dihitung diatas dengan kriteria risiko yang sudah distandarkan apakah risiko-risiko itu low yang berarti risiko rendah atau dapat diterima, moderate berarti sedanga tau perlu diwaspadai, atau high yang berarti tinggi atau tidak dapat diterima, serta memprioritaskan mitigasi atau penangannya.

Tabel 3. *Matrix* Evaluasi Risiko

LIKELIHOOD						
	Certain / Pasti Terjadi (5)	*Moderate*	*Moderate*	*High*	*High*	*High*
	Likely / Sering (4)	*Low*	*Moderate*	*High*	*High*	*High*
	Possible / Kadang (3)	*Low*	*Low*	*Moderate*	*High*	*High*
	Unlikely / Jarang (2)	*Low*	*Low*	*Moderate*	*Moderate*	*High*
	Rare / Sangat Jarang (1)	*Low*	*Low*	*Low*	*Moderate*	*Moderate*
		Insignificant / Sangat Kecil (1)	*Minor* / Kecil (2)	*Moderate* / Biasa (3)	*Major* / Besar (4)	*Catastrophic* / Sangat Besar (5)
		IMPACT				

Keterangan warna:

H : *High Risiko* (Risiko Tinggi)

M : *Moderate Risk* (Risiko Sedang)

L : *Low Risk* (Risiko Rendah)

https://doi.org/10.36596/jcse.v1i2.76

Tabel 4. Level Risiko

Level Risiko	Keterangan
High Risk - Risiko Tinggi	Risiko yang berbahaya yang harus diatasi secepatnya.
Moderate Risk - Risiko Sedang	Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan.
Low Risk - Risiko Rendah	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil.

d. Perlakuan Risiko (*Risk Treatment*)
Pada tahapan ini beberapa strategi yang digunakan untuk penanganan risiko, yaitu :
1) Membagi (*Transfer*)
Merupakan strategi yang memindahkan dampak negatif dari ancaman risiko, bersamaan dengan tanggung jawabnya, kepada pihak ketiga. Memindahkan risiko hanya berfokus pada pemindahan risiko kepada pihak lain, bukan menghilangkannya.
2) Mengurangi (*Mitigate/Treat*)
Strategi ini bertujuan untuk mengurangi probabilitas dan dampak dari risiko hingga menjadi berada dalam batas yang dapat diterima dan dapat dianalisis melalui 4 tipe kontrol yaitu:
a) Kontrol preventif (pencegahan) kontrol jenis ini diperuntukkan untuk membatasi kemungkinan terjadinya hasil yang tidak diharapkan.
b) Kontrol korektif (perbaikan) kontrol korektif dilaksanakan untuk memperbaiki hasil yang tidak diharapkan yang telah terjadi.
c) Kontrol direktif (pengarahan) kontrol ini diperlukan untuk memastikan hasil yang diinginkan tercapai.
d) Kontrol deteksi kontrol ini digunakan untuk mengidentifikasi waktu terjadinya hasil yang tidak diinginkan. Kontrol ini diterapkan ketika risiko sudah diambil, dan hanya bertujuan untuk mendeteksi hal-hal negatif yang terdapat pada risiko tersebut
3) Menghindari (*Avoidance*)
Strategi ini merupakan langkah untuk menghilangkan kemungkinan terjadinya risiko yang digunakan untuk risiko-risiko yang berdampak sangat besar pada perusahaan, sehingga tidak ada cara lain kecuali untuk menghindari terjadinya risiko tersebut.
4) Menerima (*Tolerate/Acceptance*)
Strategi ini digunakan untuk risiko-risiko yang masih dalam batas kewajaran bagi perusahaan (*risk appetite*), risiko yang tindakan penanganannya masih terbatas, atau risiko yang biaya penanganannya lebih tinggi dibandingkan manfaat yang didapat perusahaan.

e. *Monitoring dan Review*
Monitoring dan Review dilaksanakan terhadap seluruh proses manajemen risiko termasuk konteksnya (lingkungan, proses, organisasi, strategi, *stakeholder* dsb). Catatan-catatan hasil pemantauan dan pengkajian ulang disimpan sebagai bukti dan laporan bahwa aktifitas itu telah dilaksanakan dan sebagai masukan bagi *Risk Management Framework* yang telah disiapkan sebelumnya.

4) Hasil dan Pembahasan

4.1Analisis Hasil

Metode yang digunakan dalam penelitian ini menggunakan ISO 31000:2009 *risk management*. Terdapat lima kegiatan risiko yang termasuk dalam proses manajemen risiko yaitu komunikasi dan konsultasi, menentukan konteks, *risk assessment* yang terdiri dari identifikasi risiko, analisis risiko dan evaluasi risiko. Kemudian perlakuan risiko serta *monitoring* dan *review* [13].

1. Komunikasi dan Konsultasi

Tahap pertama dalam proses manajeman risiko pada ISO 31000 yaitu melakukan observasi dan wawancara kepada pihak yang terkait di KPH Banyumas Timur. Tahap ini dilakukan kepada kepala bidang divisi bisnis yaitu Bapak Sugito, untuk membahas izin melakukan manajemen risiko sehingga ada bukti yang kuat secara hukum, yang digunakan sebagai dasar pertanggung jawaban untuk apa dilakukan manajemen risiko di KPH Banyumas Timur.

https://doi.org/10.36596/jcse.v1i2.76

Proses komunikasi dan konsultasi menjadi tahap pertama pengelolaan risiko karena merupakan proses tukar-menukar informasi dan pendapat mengenai risiko dan pengelolaannya oleh para pemangku kepentingan (*stakeholder*). Proses komunikasi dan konsultasi dari para stakeholder harus dapat diidentifikasi dan dipertimbangkan dalamproses pengambilan keputusan. Proses komunikasi dan konsultasi harus berjalan selama proses manajemen risiko berlangsung baik dari *stakeholder* internal maupun eksternal.

KPH Banyumas Timur telah telah melakukan komunikasi dan konsultasi secara dua arah baik dari pihak eksternal yaitu *vendor*, *investor* dan Lembaga Masyarakat Desa Hutan (LMDH), serta dari pihak internal yaitu karyawan pada sub bidang, terutama pada bidang divisi bisnis yang berkaitan langsung dengan pengimplementasian teknologi informasi berbasis *website* Ecofo. Divisi bisnis di KPH Banyumas Timur melakukan proses komunikasi dengan mengadakan rapat dan pertemuan berkala dengan para *stakeholder* internal dan eksternal untuk membahas dan mengkomunikasikan permasalahan yang ditemui. Salah satu permasalahanya yaitu terkait dengan risiko teknologi informasi yang diterapkan.

2. Menentukan konteks

a. Menentukan Konteks Eksternal

Konteks eksternal pada KPH Banyumas Timur adalah lingkungan eksternal dimana organisasi mengupayakan pencapaian sasaran tujuan yang diterapkanya. Pihak eksternal meliputi:

1) *Vendor*: Divisi bisnis memerlukan *vendor* terkait dengan pemberian solusi dan membantu terkait pengadaan kebutuhan teknologi informasi yang dibutuhkaan perusahaan untuk memperlancar proses bisnis perusahaan.
2) *Investor*: Bagian divisi bisnis di KPH Banyumas Timur bekerjasama dengan investor terkait dengan pemanfaatan hutan sebagai kawasan wisata untuk memperoleh investasi baik jangka pendek maupun jangka panjang untuk membentuk dan meningkatkan keuntungan.
3) Lembaga Masyarakat Desa Hutan (LMDH): Bagian divisi bisnis di KPH Banyumas Timur bekerjasama dengan lembaga yang dibentuk oleh masyarakat desa yang berada didalam atau disekitar hutan untuk mengatur dan memenuhi kebutuhannya melalui pemanfaatan hutan salah satunya sebagai kawasan wisata untuk memperoeh keuntungan bersama.

b. Menentukan Konteks Internal

Konteks internal pada KPH Banyumas Timur adalah lingkungan internal dimana organisasi mengupayakan pencapaian sasaran tujuan yang diterapkanya. Pihak internal meliputi:

1) Visi dan Misi : Visi dan misi perusahaan telah disebutkan sebelumnya, KPH Banyumas Timur merupakan perusahaan umum dibawah naungan Perum Perhutani yang merupakan Badan Usaha bergerak dibidang pengelolaan dan pengembangan fungsi hutan dan pemanfataan hutan Milik Negara (BUMN) sebagaimana diatur dalam Undang – Undang Nomor 9 tahun 1969 dan berupaya memberdayakan masyarakat sekitar hutan melalui industri pariwisata[3].
2) Struktur organisasi: Struktur organisasi menjelaskan gambaran yang jelas berkaitan dengan posisi dan wewenang di dalam perusahaan.
3) Karyawan / SDM : Merupakan hal yang sangat penting di KPH Banyumas Timur. Sehingga perusahaan berupaya untuk melakukan perekrutan dan training dengan baik. Serta memberikan *awards* bagi karyawan yang berprestasi.

c. Menetapkan Konteks Proses Manajemen Risiko

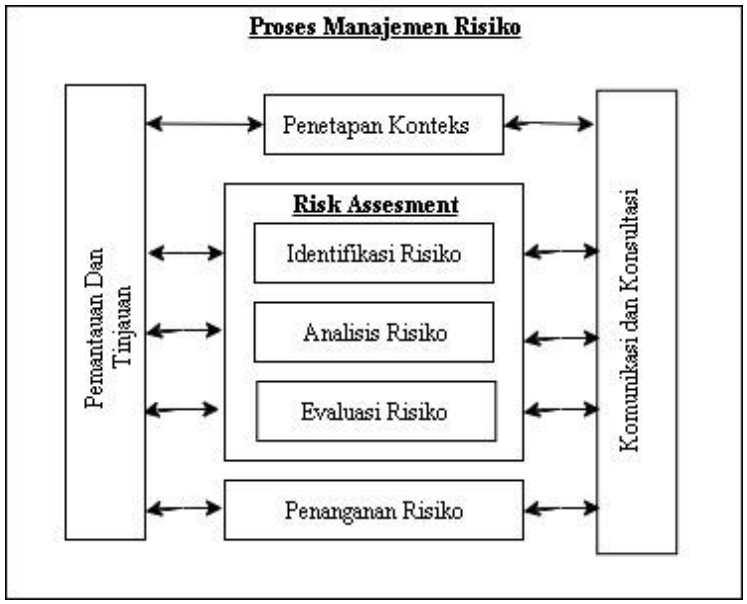
Tujuan disusunnya penelitian ini yaitu untuk menganalisa manajemen risiko teknologi informasi pada KPH Banyumas Timur. Yang menjadi objek penelitian yaitu berupa implementasi sistem informasi berbasis *website* yang diterapkan yaitu Ecofo, yang merupakan sistem informasi berbasis *website* yang digunakan untuk melakukan pengelolaan tiket yang dikelola oleh divisi bidang bisnis di KPH Banyumas Timur. Risiko berfokus pada teknologi yang diterapkan. TI tidak lagi dipandang sebagai sebuah tool yang terpisah (*separated*) dari perangkat organisasi, tetapi sudah dianggap sebagai salah satu sumber daya (*resources*) yang memiliki peran yang sama penting dengan sumber daya lain seperti finansial, aset, dan SDM.

Konteks *website* Ecofo antara lain:

https://doi.org/10.36596/jcse.v1i2.76

1) Software : software yang digunakan yaitu sistem informasi berbasis *website* "ECOFO", yang merupakan *website* pengolahan tiket yang tersistem untuk memudahkan proses bisnis pada divisi bagian bisnis di KPH Banyumas Timur.
2) Informasi : informasi merupakan data-data yang telah diolah untuk kepentingan manajemen guna sebagai pengambilan keputusan dalam menjalankan proses bisnis. Data yang diolah untuk menghasilkan informasi berupa data transaksi, data pengguna, data laporan dan data mitra.
3) Infrastruktur : mencakup *hardware*, sistem operasi, sistem manajemen *database*, jaringan (*networking*), multimedia, dan fasilitas-fasilitas lainnya yang mendukung akses terhadap *website* Ecofo.
4) *People* : merupakan sumber daya yang paling penting bagi organisasi dalam pengelolaan dan operasionalisasi bisnis organisasi. Kesadaran dan produktivitasnya dibutuhkan untuk merencanakan, mengorganisasikan, melaksanakan, memperoleh, menyampaikan, mendukung, dan memantau layanan TI organisasi.

   Proses manajemen risiko akan dilakukan berfokus pada website Ecofo menggunakan ISO 31000:2009 yang memiliki 5 tahapan proses yaitu komunikasi dan konsultasi, menentukan konteks, *risk assessment*, penanganan risiko, dan pemantauan dan tinjauan.



Gambar 3. Konteks Proses Manajemen Risiko

Tahap komunikasi dan konsultasi dimana dilakukan komunikasi yang baik antara pihak internal dan eksternal dengan bidang divisi bisnis. Selanjutnya tahap menentukan konteks dimana akan ditentukan pihak yang terkait dari pihak internal maupun pihak eksternal, konteks manajemen risiko dan kriteria risiko. Tahap Risk assessment dibagi menjadi tiga yaitu identifikasi risiko, analisis risiko dan evaluasi risiko. Dalam melakukan analisis risiko dilakukan dengan menggunakan metode pemeringkatan risiko dengan memerhatikan prioritas kemungkinan (likelihood) dan dampak (impact). Tahap selanjutnya yaitu perlakuan risiko yang terdiri dari empat macam yaitu penerimaan risiko, menghindari risiko, berbagi risiko, dan mitigasi risiko yang digunakan untuk penenganan risiko yang telah teridentifikasi. Langkah selanjutnya yaitu pemantauan dan tinjauan yang digunakan untuk penanganan risiko dimasa yang akan datang.

d. Kriteria Risiko

Tabel 5. Kriteria *Likelihood*

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

https://doi.org/10.36596/jcse.v1i2.76

Tabel 6. Level Risiko

Level Risiko	Keterangan
Risiko Tinggi	Risiko yang berbahaya yang harus diatasi secepatnya.
Risiko Sedang	Risiko ini harus dimonitor dan membutuhkan penangananyang berkelanjutan.
Risiko Rendah	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh palingkecil.

3. Penilaian Risiko

Pada tahap penilaian risiko pada *website* Ecofo terdiri dari 3 tahapan yaitu identifikasi risiko (*risk identification*), analisis risiko (*risk analiysis*) dan evaluasi risiko (*risk evaluate*).

a. Identifikasi Risiko

1) Identifikasi Aset

Tahapan identifikasi aset yang terkait dengan *website* Ecofo dilakukan melalui proses studi pustaka, wawancara, observasi dan dokumentasi. Pada tahap ini dilakukan identifikasi aset dari data, *software* hingga *hardware* yang berkaitan dengan *website* Ecofo. Detail aset-aset yang terkait dengan *website* Ecofo dapat dilihat pada Tabel 7.

Tabel 47. Identifikasi Aset *Website* ECOFO [4]

Identifikasi Aset Website ECOFO	
Data	1. Data Transaksi 2. Data Pengguna 3. Data Mitra 4. Data Laporan Perolehan
Software	Sistem Informasi Berbasis *Website* ECOFO
Hardware	1. Komputer 2. Keyboard 3. Printer 4. CPU 5. Perangkat Jaringan *6. Wifi* 7. Android Pos 8. Handphone

2) Identifikasi Kemungkinan Risiko

Setelah melakukan identifikasi aset terhadap *website* Ecofo, hal yang selanjutnya dilakukan yaitu identifikasi kemungkinan risiko untuk mengidentifikasi berbagai kemungkinan risiko yang muncul terhadap aset-aset *website* Ecofo yang terdiri dari berbagai faktor seperti alam atau lingkungan, manusia serta sistem dan infrastruktur.

Tabel 4.5 Identifikasi Kemungkinan Risiko [4]

Faktor	**ID**	**Kemungkinan Risiko**
Alam & Lingkungan	KR01	- Gempa bumi
	KR02	- Banjir
	KR03	- Petir
	KR04	- Kebakaran
	KR05	- Debu atau kotoran
	KR06	- Listrik padam
Manusia(SDM)	KR07	- *Human Error*
	KR08	- Penyalagunaan hak akses/ *user ID*
	KR09	- Pencurian Perangkat
	KR10	- Data dan Informasi yang tidak sesuai dengan fakta
	KR11	- *Cybercrime*
	KR12	- Kesalahan teknis
	KR13	- Pengunduran diri
	KR14	- Pegawai yang sakit atau cidera
	KR15	- Petugas tidak mengikuti keseluruhan SOP

https://doi.org/10.36596/jcse.v1i2.76

Sistem & Infrastruktur	KR16	- Kegagalan sistem jaringan/jaringan terputus
	KR17	- Kegagalan/rusaknya *Software*
	KR18	- Kegagalan/rusaknya *Hardware*
	KR19	- Gagal melakukan fungsi media penyimpanan seperti *disk error, disk Full.*
	KR20	- *Data Corrupt/*Rusak
	KR21	- *Overload Database*
	KR22	- *Server down*
	KR23	- *Overheat* Perangkat Komputer
	KR24	- Serangan Virus, *Malware, Malicious* Program

3) Identifikasi Dampak Risiko

Setelah melakukan tahapan identifikasi kemungkinan risiko, langkah selanjutnya adalah melakukan identifikasi dampak risiko. Proses ini akan mengidentifikasi dampak seperti apa yang akan dialami oleh *website* Ecofo jika kemungkinan-kemungkinan yang sudah diidentifikasi sebelumnya terjadi.

Tabel 8. Identifikasi Dampak Risiko [4]

ID	Kemungkinan Resiko	Dampak Risiko
R1	Gempa Bumi	Aset-aset IT rusak, proses bisnis terhenti.
R2	Banjir	Alat rusak, ketersedian data terhambat, instansi mengalami kerugian secara financial
R3	Petir	Alat rusak, ketersedian data terhambat, instansi mengalami kerugian secara finansial, proses bisnis terganggu.
R4	Kebakaran	Kehilangan data, instansi mengalami kerugian secara finansial, kehilangan aset-aset dan mengganggu proses bisnis instansi tersebut.
R5	Debu Atau Kotoran	Alat mengalami kerusakan.
R7	*Human Error*	Aset-aset IT tidak beroperasi dengan baik, data sulit untuk di akses, mengganggu proses bisnis.
R8	Penyalagunaan Hak Akses/*User ID*	Manipulasi data, kebocoran informasi atau data penting.
R9	Pencurian Perangkat	Kehilangan perangkat, kehilangan data, kerugian finansial dan proses bisnis terganggu.
R10	Data Dan Informasi Yang Tidak Sesuai Dengan Fakta	Manipula si data, proses bisnis terganggu.
R11	*Cybercrime*	Manipulasi data, pencurian data.
R12	Kesalahan Teknis	Pekerjaan terhambat, alat rusak, proses bisnis terganggu.
R13	Pengunduran Diri	Sulit mencari penganti staff yang ahli dan berpengalaman dibidang pekerjaan, proses bisnis terganggu.
R14	Pegawai Yang Sakit Atau Cidera	Sulit mencari penganti staff yang ahli dan berpengalaman dibidang pekerjaan.
R15	Pegawai IT tidak mengikuti keseluruhan SOP	Alat rusak, kerja tidak optimal.
R16	Kegagalan Sistem Jaringan	Gagal update data, kehilangan data.Pekerjaan terganggu
R17	Kegagalan/ Rusaknya *Software*	Kehilangan data, proses bisnis sangat terganggu. Kerugian secara finansial.
R18	Kegagalan/Rusaknya *Hardware*	Kehilangan data, proses bisnis sangat terganggu. Kerugian secara finansial.
R19	Gagal Melakukan Fungsi Penyimpanan Seperti *Disk Error, Disk Full.*	Gagal menyimpan data. kehilangan data. Proses bisnis terganggu.
R20	*Data Corrupt/*Rusak	Data rusak, kehilangan data. proses bisnis terganggu.
R21	*Overload Database*	Kehilangan data, lambat *loading*.
R22	*Server Down*	Kehilangan data, proses bisnis terhenti. kerugian besar.
R23	*Overheat* Perangkat Komputer	Alat mengalami kerusakan, loading lambat proses bisnis terganggu.
R-24	Serangan Virus, *Malware, Malicious Program.*	Kehilangan data, proses bisnis terganggu, data corrupt.

https://doi.org/10.36596/jcse.v1i2.76

b. Analisis Risiko

Setelah melakukan tahap identifikasi risiko, tahap selanjutnya yaitu melakukan tahapan analisis risiko. Pada proses ini akan dilakukan penilaian terhadap kemungkinan risiko yang telah diidentifikasi. Penentuan nilai berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*) pada Tabel 9.

Tabel 9. Penilaian Kemungkinan Risiko dengan *Likelihood* dan *impact.*

ID	Kemungkinan Risiko	*Likelihood*	*Impact*
R1	Gempa Bumi	1	5
R2	Banjir	1	3
R3	Petir	1	3
R4	Kebakaran	1	5
R5	Debu Atau Kotoran	4	1
R6	Listrik Padam	2	3
R7	*Human Error*	3	2
R8	Penyalagunaan Hak Akses/*User ID*	2	3
R9	Pencurian Perangkat	2	2
R10	Data Dan Informasi Yang Tidak Sesuai Dengan Fakta	3	2
R11	*Cybercrime*	1	3
R15	Pegawai IT tidak mengikuti keseluruhan SOP	3	3
R16	Kegagalan Sistem Jaringan/jaringan terputus	3	4
R17	Kegagalan/ Rusaknya *Software*	3	3
R18	Kegagalan/Rusaknya *Hardware*	3	3
R19	Gagal Melakukan Fungsi Penyimpanan Seperti *Disk Error, Disk Full.*	2	3
R20	*Data Corrupt*/Rusak	3	3
R21	*Overload Database*	5	3
R22	*Server Down*	5	3
R23	*Overheat*Perangkat Komputer	4	2
R-24	Serangan *Virus, Malware, Malicious Program.*	1	3

c. Evaluasi Risiko

Tahap terakhir dalam *risk assesment* adalah tahap evaluasi risiko. Dalam tahap ini menggunakan acuan berupa matriks risiko, dimana dalam matriks tersebut dibedakan kedalam 3 *risk level* yaitu *low, medium dan high*. Kemungkinan risiko yang telah ditentukan nilai *likehood* dan nilai *impact* pada proses sebelumnya akan dibedakan lagi menysuaikan matriks yang ada.

Tabel 10. Matriks Evaluasi Risiko

LIKELIHOOD						
	Certain/ Pasti Terjadi (5)			R21 R22		
	Likely / Sering (4)	R5	R23			
	Possible / Kadang (3)		R7 R10 R12	R15 R17 R18 R20	R16	
	Unlikely / Jarang (2)		R9 R13 R14	R6 R8 R19		
	Rare Hampir Tidak Pernah (1)			R2 R3 R11 R24		R1 R4
		Insignificant /	*Minor* /	*Moderate* /	*Major* /	*Catastrophic* /

https://doi.org/10.36596/jcse.v1i2.76

		Sangat Kecil (1)	Kecil (2)	Biasa (3)	Besar (4)	Sangat Besar (5)
IMPACT						

Keterangan warna:

H :*High Risiko* (Risiko Tinggi)

M :*Moderate Risk* (Risiko Sedang)

L :*Low Risk* (Risiko Rendah)

Tabel 11. Level Risiko

Level Risiko	Keterangan
High Risk - Risiko Tinggi	Risiko yang berbahaya yang harus diatasi secepatnya.
Moderate Risk - Risiko Sedang	Risiko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan.
Low Risk - Risiko Rendah	Risiko ini dapat diabaikan dengan kebijakan tertentu karena risiko ini merupakan risiko dengan tingkat pengaruh paling kecil

Setelah kemungkinan-kemungkinan risiko dimasukan ke dalam matriks evaluasi berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*), kemudian akan dijabarkan dari 24 kemungkinan risiko ke dalam *level of risk* dengan tingkatan *high, medium dan low*.

Tabel 12. Risk Level Kemungkinan Risiko [8]

ID	Kemungkinan Risiko	*Likelihood*	*Impact*	*Risk Level*
R16	Kegagalan Sistem Jaringan	3	4	*High*
R21	*Overload Database*	5	3	*High*
R22	*Server Down*	5	3	*High*
R1	Gempa Bumi	1	5	*Medium*
R4	Kebakaran	1	5	*Medium*
R6	Listrik Padam	2	3	*Medium*
R8	Penyalagunaan Hak Akses/*User ID*	2	3	*Medium*
R15	Pegawai IT tidak mengikuti keseluruhan SOP	3	3	*Medium*
R17	Kegagalan/ Rusaknya *Software*	3	3	*Medium*
R18	Kegagalan/Rusaknya *Hardware*	3	3	*Medium*
R19	Gagal Melakukan Fungsi Penyimpanan Seperti *Disk Error, Disk Full.*	2	3	*Medium*
R20	*Data Corrupt*/Rusak	3	3	*Medium*
R23	*Overheat*Perangkat Komputer	4	2	*Medium*
R2	Banjir	1	3	*Low*
R3	Petir	1	3	*Low*
R5	Debu Atau Kotoran	4	1	*Low*
R7	*Human Error*	3	2	*Low*
R9	Pencurian Perangkat	2	2	*Low*
R11	*Cybercrime*	1	3	*Low*
R12	Kesalahan Teknis	3	2	*Low*
R13	Pengunduran Diri	2	2	*Low*
R14	Pegawai Yang Sakit Atau Cidera/meninggal	2	2	*Low*
R-24	Serangan Virus, *Malware, Malicious Program.*	1	3	*Low*

Pada Tabel 12. merupakan hasil dari *risk evaluation* dimana dari 24 kemungkinan risiko terdapat 3 (Kegagalan Sistem Jaringan/jaringan terputus, *Overload, Server Down*) merupakan *level of risk* dengan tingkatan *high*, tardapat risiko lainya sejumlah 10 (gempa bumi, kebakaran, listrik padam, penyalagunaan hak akses/*user ID*, pegawai IT tidak mengikuti keseluruhan SOP, kegagalan/ rusaknya *software*, kegagalan/rusaknya *hardware*, gagal melakukan fungsi penyimpanan seperti *disk error, disk full, data*

https://doi.org/10.36596/jcse.v1i2.76

corrupt, overheat) merupakan *level of risk* tingkatan *medium*, serta risiko berjumlah 11 (banjir, petir, debu atau kotoran, *human error*, pencurian perangkat, data dan informasi yang tidak sesuai dengan fakta, *cybercrime*, kesalahan teknis, pengunduran diri, pegawai yang sakit atau cidera, serangan virus, malware, malicious program) merupakan *level of risk* tingkatan *low*.

4. Perlakuan Risiko

Setelah melakukan tahap identifikasi risiko, langkah selanjutnya yaitu perlakuan risiko. Pada tahap ini penulis memberikan saran mengenai perlakuan risiko untuk kemungkinan risiko yang ada pada website Ecofo. Diharapkan dapat mengurangi dan digunakan untuk pencegahan terhadap kemungkinan risiko yang mungkin akan muncul.

Tabel 13. Usulan Perlakuan Risiko [8]

ID	Kemungkinan Risiko	*Risk Level*	Perlakuan Risiko
R16	Kegagalan Sistem Jaringan/jaringan terputus	High	Kendala yang sering dialami yaitu tidak tersediaanya jaringan di lokasi tertentu. Jaringan yang diterapkan menggunakan jasa *service provider*. Oleh karena itu diperlukanya pengecekan jaringan secara berkala dan menambahkan router penguat sinyal agar sistem dapat diakses.
R21	*Overload*	High	Penerapan *website* Ecofo menggunakan *server hosting*, dimana sering terjadi *overload* yang terjadi ketika yang sibuk. Masalah lain juga Sering terjadinya masalah pada data *center* penyedia *server hosting* sehinggga: - Perusahaan perlu melakukan *monitoring* berkala kepada penyedia jasa *hosting*. - Mengingat pentingnya *website* Ecofo, maka perusahaan perlu mempunyai *server* tersendiri yang lebih handal dan lebih menjaga keamanan data
R22	*Server Down*	High	*Server down* merupakan risiko yang sangat sering terjadi. *Server down* terjadi ketika proses transaksi data yang sibuk dan terjadinya masalah pada penyedia *server hosting* sehingga: - Perusahaan perlu melakukan monitoring berkala kepada penyedia jasa *hosting*. - Mengingat pentingnya *website* Ecofo, maka perusahaan perlu mempunyai *server* tersendiri yang lebih handal dan lebih menjaga keamanan data
R1	Gempa Bumi	Medium	Gempa bumi merupakan fakor yang ditimbulkan oleh kondisi alam yang tidak dapat terduga. Untuk mengurangi kerugian, perusahaan harus melakukan perawatan dan menyiapkan perencanaan penyediaan cadangan infrastruktur baik *hardware* maupun perangkat jaringan.
R4	Kebakaran	Medium	- Perusahaan harus menyediakan alat pemadam kebakaran yang dapat digunakan ketika hal tersebut terjadi. - Jika kebakaran terjadi perusahaan harus menyiapkan perencanaan penyediaan cadangan infrastruktur baik *hardware* maupun perangkat jaringan.
R6	Listrik Padam	Medium	Ketika terjadi listrik padam tentunya akan menghambat sebagian aktivitas. Untuk menghindarinya perusahaan harus menyediakan genset yang dapat digunakan ketika terjadinya listrik padam
R8	Penyalagunaan Hak Akses/User ID	Medium	- Untuk mencegah penggunaan hak akses maka harus mengganti *password* secara periodik ataupun berkala. - Memanajemen hak akses.
R15	Pegawai IT tidak mengikuti keseluruhan SOP	Medium	- Melakukan teguran lisan, apabila masih malakukan kesalahan yang sama maka akan diberikan teguran secara tertulis. - Membuat dokumen SOP untuk setiap bidang pekerjaan supaya lebih jelas aturannya.

https://doi.org/10.36596/jcse.v1i2.76

R17	Kegagalan/rusaknya *software*	Medium	- Ketika terjadi kerusakan pada *software*, maka harus melakukan instal ulang *software* dan melakukan *update* antivirus secara periodik
R18	Kegagalan/rusaknya *hardware*	Medium	- Untuk mencegah risiko kerusakan *hardware* maka perlunya melakukan perawatan terhadap *hardware* secara berkala. - Memilih *hardware* dengan kualitas yang sudah terjamin. - Menyediakan cadangan *hardware* yang baru jika sewaktu-waktu *hardware* memang tidak bisa digunakan lagi
R19	Gagal melakukan fungsi penyimpanan seperti *disk error, disk full*.	Medium	- Untuk menghindari masalah ini, perlu melakukan penyediaan dan cadangan hardisk dengan kapasitas sesuai kebutuhan
R20	*Data Corrupt*	Medium	- Untuk mencegah hal ini, pegawai harus melakukan proses penyimpanan data dengan baik. - Melakukanpengecakan data secara berkala dan melakukan back up
R23	*Overheat* pada perangkat	Medium	- Untuk menghindari overheat atau panas yang berlebih pada perangkat, maka perlu melakukan perawatan perangkat dan melakukan penggunaan sesuai kebutuhan. - Melakukan pengecekan terhadap perangkat.
R2	Banjir	Low	- Tempatkan infrastruktur perangkat dan jaringan yang aman dan jauh dari kemungkinan banjir. - Perusahaan harus menyiapkan perencanaan penyediaan cadangan infrastruktur baik hardware maupun perangkat jaringan.
R3	Petir	Low	Petir merupakan risiko yang ditimbulkan oleh alam yang tentunya dapat menjadi risiko terhadap perangkat. Oleh sebab itu perlu memasang alat penangkal petir. Menyiapkan cadangan dan penggantian perangkat jika terjadi risiko karena petir terjadi.
R5	Debu Atau Kotoran	Low	perlu melakukan perawatan kebersihan untuk meminimalisir risiko kerusakan.
R7	*Human Error*	Low	- Untuk meminimalisir hal ini maka perlu dilakukan teguran lisan, apabila masih malakukan kesalahan yang sama maka akan diberikan teguran secara tertulis. - Melakukan pelatihan terhadap karyawan dan melakukan pemetaan kemampuan masing-masing individu. - Melakukan pembagian tugas sesuai dengan kemampuan masing-masing individu. - Membuat dan menjalankan SOP agar tahu lebih jelas peraturan di bidang kerjanya.
R9	Pencurian Perangkat	Low	- Untuk mencegah hal ini terjadi maka perlu memperbanyak tenaga security terlatih - Memperbanyak titik-titik pemasangan CCTV. - Melakukan penjagaan yang ketat terhadap infrastruktur terutama hardware.
R10	Data dan Informasi yang tidak sesuai dengan fakta	Low	- Data dan informasi tidak sesuai dengan fakta ditemukan di bagian loket. Untuk mencegah hal ini terjadi, petugas loket harus melakukan pengecekan/*scan barcode* terhadap tiket
R11	*Cybercrime*	Low	- Untuk melindungi data perlu dilakukan privasi datadengan perlindungan *security software* yang *up to date, install software* antivirus dan menggunakan fitur keamanan untuk *website* seperti layanan SSL/HTTPs.
R12	Kesalahan Teknis	Low	- Untuk mencegah risiko kesalahan teknis perlu melakukan pelatihan terhadap sumber daya manusia. - Membuat dan menjalankan SOP agar tahu lebih jelas peraturan di bidang kerjanya.
R13	Pengunduran Diri	Low	- Untuk mencegah pegawai melakukan pengunduran diri, diperlukanya pemetaan terhadap kemampuan dan melakukan pembagian tugas sesuai dengan kemampuan.

https://doi.org/10.36596/jcse.v1i2.76

			Jika terjadi pengunduran pegawai maka perusahaan harus mencari dan melatih pegawai baru.
R14	Pegawai Yang Sakit Atau Cidera	Low	- Pegawai/karyawan yang terdapat pada loket bekerja dengan sistem shift, sehingga jika ada pegawai sakit maka akan digantikan pegawai lain. - Untuk mencegah risiko cidera, maka diperlukan pelatihan terhadap karyawan dan pemetaan terhadap kemampuan karyawan.
R-24	Serangan Virus, Malware, Malicious Program.	Low	- Menyediakan antivirus, melakukan update dan monitoring software dan database antivirus

5. Monitoring dan *Review*

Hasil yang diperoleh dari proses *monitoring dan review* yaitu berupa kritik dan saran yang membangun dari pihak-pihak yang terlibat langsung dengan pengelolaan website Ecofo. Proses pelaksanaan manajemen risiko dikelola dan di *monioring* oleh bagian divisi bisnis KPH Banyumas Timur. Seluruh proses kegiatan dilakukan oleh para pihak yang terlibat yaitu kepala pimpinan divisi dan karyawan serta semua pihak lain yang terkait baik internal maupun eksternal perusahaan. Semua pihak yang terkait.

Pelaksanaan proses *monitoring dan review* dilakukan dengan mengadakan pertemuan daan rapat berkala yang dilaksanakan guna mengkomunikasikan dan melaporkan terkait implementasi teknologi informasi termasuk kendala/kemungkinan risiko yang berpotensi menghambaat proses bisnis perusahaan. Termasuk membahas bagaimana melakukan penanganan dan pencegahan risiko yang muncul yang bertujuan untuk meminimalisir risiko di masa yang akan datang.

5) Conclusion

Berdasarkan dari penelitian yang sudah dilakukan, analisis risiko teknologi informasi menggunakan ISO 31000 pada website Ecofo di KPH Banyumas timur dijalankan dengan menggunakan tahapan-tahapan yang dimulai dari tahap komunikasi dan konsultasi, menentukan konteks, penilaian risiko yang terdiri dari tahap identifikasi risiko, tahap analisis risiko, tahap evaluasi risiko, tahap perlakuan risiko serta monitoring dan review dan dari hasil analisis risiko yang telah dilakukan terdapat 24 kemungkinan risiko dimana terdapat 3 risiko level high yaitu (Kegagalan Sistem Jaringan/jaringan terputus, Overload Database, Server Down). 10 risiko level medium yaitu (gempa bumi, kebakaran, listrik padam, penyalagunaan hak akses/user ID, pegawai IT tidak mengikuti keseluruhan SOP, kegagalan/ rusaknya software, kegagalan/rusaknya hardware, gagal melakukan fungsi penyimpanan seperti disk error, disk full, data corrupt/rusak, overheat perangkat), serta risiko berjumlah 11 merupakan level of risk tingkatan low (banjir, petir, debu atau kotoran, human error, pencurian perangkat, data dan informasi yang tidak sesuai dengan fakta, cybercrime, kesalahan teknis, pengunduran diri, pegawai yang sakit atau cidera/meninggal, serangan virus, malware, malicious program).

References

[1] Pramanda, R., Astuti, E., dan Azizah, D. (2018). Pengaruh kemudahan dan kemanfaatan penggunaan teknologi informasi terhadap kinerja karyawan. Jurnal Administrasi Bisnis. 39(2), 117-126.

[2] Sutabri, T. (2014). Pengantar teknologi informasi. Yogyakarta: Andi Offset.

[3] Undang-Undang Nomor 9 Tahun 1969 tentang Penetapan Undang-Undang Nomor 1 Tahun 1969 tentang Bentuk-Bentuk Usaha Negara

[4] Nice, F., dan Imbar, R. (2016). Analisis risiko teknologi informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada website Swifts menggunakan ISO 31000. Jurnal JUISI. 2(2), 1-11.

https://doi.org/10.36596/jcse.v1i2.76

[5] Susilo, L., dan Kaho, V. (2011). Manajemen risiko berbasis ISO 31000. Jakarta: Penerbit PPM.

[6] Pramana, T. (2011). Manajemen risiko bisnis. Jakarta: Sinar Ilmu.

[7] Lantang, G., Cahyono, A., dan Sitokdana, M. (2019). Analisis risiko teknologi informasi pada aplikasi sap di pt serasi autoraya menggunakan iso 31000. Jurnal Sebatik. 23

[8] Agustinus, S., Nugroho, A., dan Cahyono, A. (2017). Analisis risiko teknologi informasi menggunakan ISO 31000 pada program HRMS. Jurnal Resti. 1(3), 250-238.

[9] Rahmawati, A., dan Wijaya, A. (2019). Analisis risiko teknologi informasi menggunakan ISO 31000 pada Aplikasi ITOP. Jurnal SITECH. 2(1), 14-20.

[10] Kurniawan, A. (2012). Audit internal nilai tambah bagi organisasi. Yogyakarta: BPFE. (1), 36-43.

[11] Project Management Institute (2008), A Guide to the Project Management Body of

[12] Knowledge (PMBOK Guide) Fourth Edition, Project Management Institute, Pennsylvania.

[13] Ajeng Retna Maharani (2018). Perancangan Manajemen Risiko Operasional Di Pt.X dengan Menggunakan Metode House of Risk. Tesis Pm-147501. Institut Teknologi Sepuluh Nopember.

[14] Susilo, L. J. dan Kaho, V.R (2011). Manajemen Risiko Berbasis ISO 31000 untuk Industri Non Perbankan. Jakarta: PPM

[15] Valery, K. (2011). Internal audit. Jakarta: Penerbit Erlangga.

[16] Mulyani, S. (2016). Sistem informasi manajemen. Bandung: Abdi Sistematika.

https://doi.org/10.36596/jcse.v1i2.76