ANALISIS MANAJEMEN RESIKO PROYEK MENGGUNAKAN FRAMEWORK ISO 31000 (STUDI KASUS : WEBSITE RENTAL MOBIL)

Jonathan Pratama Dinatha, Rangga
Teknik Informatika, Universitas Palangka Raya
Jalan Yos Sudarso Kota Palangka Raya, Indonesia
jonathanpratamad@mhs.eng.upr.ac.id

ABSTRAK

Website rental mobil merupakan sistem informasi berbasis internet yang digunakan untuk memfasilitasi layanan pemesanan dan penyewaan kendaraan secara daring. Penggunaan *website* ini rentan terhadap berbagai resiko seperti ancaman keamanan sistem, gangguan infrastruktur teknis, dan kesalahan proses pemesanan serta pembayaran yang dapat mengganggu aktivitas bisnis. Penelitian ini bertujuan untuk menganalisis resiko yang mungkin terjadi pada proyek *website* rental mobil. Penelitian dilakukan menggunakan metode ISO 31000 yang merupakan pedoman dalam analisis manajemen resiko dengan memiliki 3 tahapan besar yaitu identifikasi resiko (*Risk Identification*), analisis resiko (*Risk Analysis*), dan evaluasi resiko (*Risk Evaluation*). Penelitian ini menggunakan metode *Case Study Research* dengan pendekatan kualitatif, yaitu pendekatan yang dilakukan dengan mendeskripsikan atau menguraikan data dan fakta yang terjadi di dalam objek studi kasus ke dalam bentuk kata-kata. Adapun hasil dari analisis resiko ini berupa analisis kemungkinan resiko, mengelompokkan kemungkinan resiko berdasarkan dampaknya sehingga menghasilkan usulan atau perlakuan tindakan resiko terhadap kemungkinan resiko yang terdapat pada *website*. Dengan begitu, resiko yang ada dapat ditangani sesuai dengan prioritas level resikonya dan dapat dicegah serta diminimalisasi sehingga tidak mengganggu aktivitas bisnis pada proyek *website* rental mobil.

Kata kunci : *Manajemen Resiko, ISO 31000, Analisis Resiko, Website Rental Mobil.*

1. PENDAHULUAN

Kemajuan teknologi yang begitu pesat telah memberikan dampak signifikan pada kehidupan manusia, tujuannya adalah membantu manusia dalam pencapaian tujuan mereka [1]. Seiring dengan laju perkembangan teknologi yang begitu cepat, hampir seluruh aspek kehidupan manusia telah mengalami perubahan yang cukup drastis. Mulai dari cara berkomunikasi, berinteraksi, berbelanja, hingga bekerja, semua itu kini telah dipengaruhi dan diubah oleh kemajuan di bidang teknologi. Salah satu dampak kemajuan tersebut adalah penggunaan *website rental* mobil [2].

Website rental mobil merupakan contoh sistem informasi berbasis internet yang memungkinkan terjadinya berbagai resiko karena menawarkan layanan pemesanan dan penyewaan kendaraan secara daring. Berbagai aktivitas transaksi *online* yang dilakukan melalui *website* menjadikannya rentan terhadap berbagai ancaman keamanan sistem, gangguan infrastruktur teknis, hingga kesalahan proses pemesanan dan pembayaran. Oleh karena itu, analisis manajemen resiko perlu dilakukan agar berbagai resiko tersebut dapat dikelola secara tepat.

Beberapa penelitian terdahulu telah menganalisis manajemen resiko pada sistem informasi dengan menggunakan kerangka ISO 31000 yang merupakan standar pengelolaan resiko yang diterbitkan oleh *Internasional Organization for Standardization* (ISO) untuk memfasilitasi proses identifikasi, analisis, evaluasi, dan penanganan resiko [3]. Namun demikian, belum ada penelitian khusus yang menganalisis tentang manajemen resiko pada *website* rental mobil, sehingga perlu adanya analisis sekaligus penelitian yang ditulis dalam artikel dengan memanfaatkan kerangka ISO 31000 guna mengidentifikasi dan mitigasi berbagai resiko potensial yang mungkin timbul pada proyek tersebut [4]. sehingga hasil analisis ini diharapkan dapat mendukung pengelolaan resiko secara tepat sehingga proyek dapat terlaksana dengan baik dan tanpa terkendala resiko yang fatal.

2. TINJAUAN PUSTAKA

2.1. Penelitian Sebelumnya

Devara Liko Ivander dan Frederik Samuel Papilaya dalam penelitiannya yang berjudul "*Analisis Manajemen Resiko Teknologi Informasi Menggunakan Framework ISO 31000:2018*" pada tahun 2023, menenukan 26 kemungkinan resiko yang dapat terjadi di dalam perusahaan manufaktur kemasan karton *box* dan karton *sheet* PT XYZ cabang Bawen. Dari 26 kemungkinan resiko tersebut, terdapat 15 resiko dengan tingkat resiko rendah (*low*), 5 resiko dengan tingkat resiko menengah (*medium*), 5 resiko dengan tingkat resiko menengah tinggi (*medium high*), dan 1 resiko dengan tingkat resiko tinggi (*high*). Hasil dari penelitian ini adalah rekomendasi bagi perusahaan untuk secara cermat menilai dan mengatasi resiko yang terkait dengan adopsi teknologi informasi, agar dapat meminimalisir resiko dan merasakan manfaat dari penerapan teknologi informasi [3].

Ridho Fahlepi, Afdal Afdal, dan Surya Darma dalam penelitiannya yang berjudul "*Analisis Manajemen Resiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000*" pada tahun 2023, menemukan masalah mengenai resiko-resiko yang mungkin terjadi pada Sistem Informasi Akademik (SIAKAD) di Sekolah Tinggi Teknologi Pekanbaru. Penelitian ini mengidentifikasi resiko *human error*, listrik padam, jaringan tidak stabil, dan kebakaran sebagai kategori resiko *medium*, sedangkan resiko *server down*, data *corrupt*, *overheat*, gagal *update*, kerusakan *hardware*, dan petir sebagai kategori resiko rendah. Hasil dari penelitian ini adalah rekomendasi mitigasi resiko untuk memastikan bahwa resiko-resiko tersebut dapat dikelola dengan baik [4].

Fathoni Mahardika, Muhammad Agreindra H, Siti Ainun Fatimah, dan Lusi Tsulutsiah Nur F dalam penelitiannya yang berjudul "*Manajemen Resiko Teknologi Informasi Aplikasi E-Office ASN Menggunakan ISO 31000:2018*" pada tahun 2023, menemukan masalah mengenai ancaman dan serangan, termasuk kerentanan yang menimbulkan resiko, yang mengganggu proses penggunaan aplikasi *E-Office* ASN di Diskominfosanditik Kabupaten Sumedang. Penelitian ini mengidentifikasi 14 kemungkinan resiko, yang terdiri dari 3 resiko dengan level *high*, 2 resiko dengan level *medium*, dan 9 resiko dengan level *low*. Hasil dari penelitian ini adalah rekomendasi perlunya manajemen resiko sebagai langkah awal untuk pengelolaan resiko pada aplikasi *E-Office* ASN di Diskominfosanditik Kabupaten Sumedang [5].

Dengan referensi dari berbagai penelitian sebelumnya, artikel ini mengadopsi pendekatan yang sama dalam menggunakan *framework* ISO 31000 untuk analisis manajemen resiko pada proyek *Website* Rental Mobil. *Framework* ini dianggap tepat karena fleksibilitas dan penerapannya yang luas di berbagai bidang serta kemampuannya dalam memberikan panduan yang komprehensif untuk manajemen resiko.

2.2. Framework ISO 31000

Framework ISO 31000 merupakan sebuah standar pengelolaan resiko yang dibuat oleh *International Organization for Standardization* (ISO) [1], [6]. Standar ini merupakan rancangan yang digunakan untuk membantu organisasi mengidentifikasi, mengevaluasi, dan mengelola resiko dengan cara yang sistematis. Dalam penerapannya, ISO 31000 dapat digunakan pada berbagai jenis usaha publik atau swasta serta mampu menyiapkan prinsip dan tahapan mengelola resiko sehingga dapat digunakan sebagai gambaran dalam manajemen resiko guna menerapkan manajemen resiko yang lebih efektif [7]. Tujuan dari ISO adalah untuk memberikan prinsip-prinsip dan pedoman untuk manajemen resiko yang diakui secara universal atau global [8].

2.3. Resiko

Resiko adalah kemungkinan terjadinya bahaya yang dapat timbul dari beberapa penerapan proses pada saat ini atau dari beberapa peristiwa di masa depan [9]. Resiko merupakan bagian yang tidak terpisahkan dari aktifitas manusia, ibarat seperti tidak ada kehidupan tanpa adanya resiko[4]. Resiko dapat dihadapi dengan menyusun suatu manajemen resiko yang baik sebagai pertimbangan kepada Perusahaan agar dapat mengambil keputusan dengan tepat[9]. Proses tersebut bertujuan untuk mengantisipasi dan memitigasi potensi masalah, sehingga langkah-langkah pencegahan yang tepat dapat diambil untuk mengurangi dampak negatif yang mungkin terjadi. Oleh sebab itu diperlukan suatu cara untuk mengatasi resiko tersebut yang disebut manajemen resiko [7].

2.4. Identifikasi Resiko

Identifikasi Resiko adalah sebuah proses yang menentukan apa, bagaimana, dan mengapa suatu kejadian dapat terjadi [7]. Hal ini bertujuan untuk mengantisipasi dan mengurangi potensi masalah yang mungkin muncul, sehingga tindakan pencegahan yang tepat dapat diambil untuk mengurangi dampak negatif yang mungkin terjadi. Dalam manajemen proyek, identifikasi resiko merupakan langkah krusial untuk memastikan proyek berjalan dengan sukses dan lancar.

2.5. Manajemen Resiko

Manajemen merupakan sebuah kegiatan praktis yang berhubungan dengan identifikasi, penilaian, pengontrolan dan peminimalisiran resiko [10]. Manajemen resiko diperlukan untuk mengurangi kemungkinan dan dampak dari potensi resiko berdasarkan potensi tingkat resiko tersebut [4].

Proses ini melibatkan serangkaian langkah yang sistematis dan terstruktur, dimulai dengan mengenali potensi resiko yang dapat mempengaruhi tujuan organisasi atau proyek. Setelah potensi resiko teridentifikasi, langkah selanjutnya adalah melakukan penilaian resiko untuk memahami dan mengukur sifat serta tingkat resiko tersebut, termasuk dampaknya terhadap operasional dan keberlanjutan proyek. Manajemen resiko ini diperlukan untuk melindungi aset yang dimiliki oleh suatu organisasi dan digunakan untuk mengelola resiko menjadi sebuah peluang bagi organisasi[6].

Peran dari manajemen Resiko yaitu dapat mengantisipasi lingkungan cepat berubah, mengembangkan *corporate governance*, mengoptimalkan *strategic management*, mengamankan sumber daya dan asset yang dimiliki organisasi, serta mengurangi reactive decision making dari manajemen puncak [7].

2.6. Proses Manajemen Resiko

Proses manajemen resiko merupakan sebuah rangkaian langkah-langkah yang berhubungan dengan identifikasi, penilaian, pengontrolan dan peminimalisiran resiko[10]. Proses manajemen resiko

ini memiliki tiga proses besar, yang meliputi menentukan konteks *(establishing the context)*, penilaian resiko *(risk assessment)*, dan pengelolaan resiko *(Risk treatment)* [8].

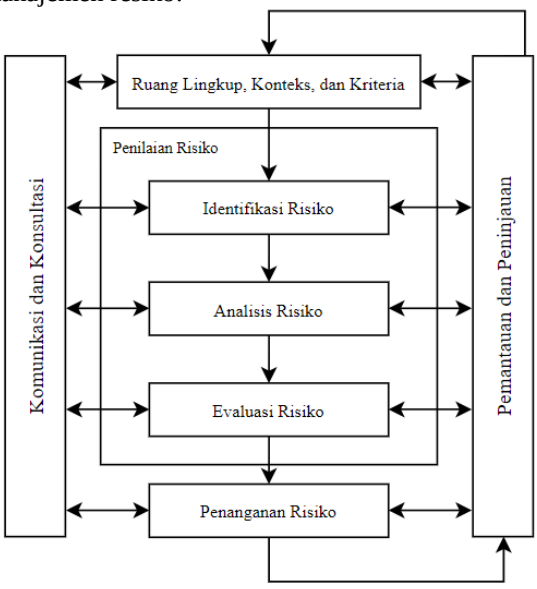
2.7. Website

Website adalah sekumpulan halaman *web* yang saling terkait satu sama lain mengenai topik tertentu. Halaman-halaman tersebut biasanya disimpan di *server web* untuk dapat diakses oleh para pengguna internet atau hanya jaringan lokal saja (LAN). *Website* juga dapat diartikan sebagai kumpulan halaman informasi digital berbentuk multimedia yang menampilkan unsur seperti gambar, suara, musik, serta animasi [11].

3. METODE PENELITIAN

Metode penelitian yang digunakan adalah *Case Study Research* dengan pendekatan kualitatif. Pendekatan ini dilakukan dengan mendeskripsikan atau menguraikan data dan fakta yang terjadi di dalam suatu objek studi kasus kedalam bentuk kata-kata. Salah satu jenis pendekatan kualitatif yaitu metode penelitian *Case Study Research*, dimana metode tersebut hanya berfokus pada satu objek tertentu [7], [12]. Metode ini memiliki karakteristik yang cukup unik, di mana peneliti berfokus secara mendalam pada satu objek atau kasus tertentu untuk memperoleh pemahaman yang komprehensif.

Metode tersebut digunakan dalam kasus Analisis Manajemen Resiko Proyek *Website* Rental Mobil Menggunakan *Framework* ISO 31000. Standar internasional ini menyediakan prinsip-prinsip dan pendoman dalam manajemen resiko. Dalam manajemen resiko, Langkah-langkah yang dilakukan meliputi identifikasi resiko, analisis resiko, dan evaluasi resiko [13]. Berikut adalah prinsip dan pedoman untuk mengidentifikasi serta mengelola manajemen resiko:



Gambar 1. Prinsip dan Pedoman Manajemen Resiko [13]

Pada tahap pertama dilakukan penilaian resiko secara sistematis untuk menentukan apakah *website* rental mobil ini memiliki resiko yang dapat diterima atau tidak [12].

Terdapat beberapa tahapan yang harus dilalui dalam melakukan penilaian resiko ini. Tahapan-tahapan tersebut melibatkan proses yang menyeluruh dan terperinci untuk memastikan bahwa setiap aspek resiko diidentifikasi, dianalisis, dan dievaluasi dengan baik. Berikut adalah tahapan-tahapan tersebut:

a. Risk Identification (Identifikasi Resiko)
   Langkah pertama dalam proses ini adalah identifikasi resiko, yang bertujuan untuk mencari dan mengetahui resiko-resiko yang memiliki kemungkinan muncul dalam kegiatan- kegiatan yang dilakukan oleh situs web rental mobil [7], [10], [12]. Resiko-resiko tersebut dapat berasal dari berbagai sumber, seperti ancaman keamanan siber, kerentanan sistem, masalah operasional, atau bahkan resiko reputasi.
b. Risk Analyst (Analisis Resiko)
   Setelah resiko diidentifikasi, tahap kedua adalah melakukan analisis mendalam terhadap masing-masing resiko tersebut. Metode analisis resiko ini meliputi faktor penilaian seberapa besar dampak yang mungkin akan timbulkan dan seberapa sering resiko tersebut dapat terjadi., karakterisasi, manajemen dan kebijakan yang berkaitan dengan resiko [7], [10], [12]
   Hal tersebut dapat membantu dalam memahami tingkat keparahan dan frekuensi dari setiap resiko.
c. Risk Evaluation (Evaluasi Resiko)
   Pada tahap terakhir, hasil analisis resiko dievaluasi untuk menentukan tingkat resiko keseluruhan. Evaluasi tersebut bertujuan untuk membantu proses pengambilan resiko berdasarkan hasil analisis resiko [7], [10], [12]. Evaluasi dilakukan dengan membandingkan tingkat resiko dengan kriteria yang telah ditentukan sebelumnya untuk menentukan apakah resiko tersebut dapat diterima atau memerlukan tindakan lebih lanjut.

3.1. Pengumpulan Data

Proses pengumpulan data pada kasus Analisis Manajemen Resiko Proyek *Website* Rental Mobil Menggunakan *Framework* ISO 31000, diperoleh dengan melakukan studi literatur [5].

Studi literatur ini melibatkan pengumpulan dan analisis data dari berbagai sumber tertulis yang relevan, meliputi artikel, jurnal, laporan penelitian, dan sumber-sumber terpercaya. Manfaat studi literatur ini adalah membantu dalam mendapatkan pemahaman terkait rental mobil berdasarkan resiko dan tantangan yang mungkin dihadapi dalam pembuatan *website* tersebut [14].

Kemudian untuk pengumpulan data sekunder diperoleh dengan melakukan pendekatan kuantitatif yaitu, dengan melakukan wawancara terhadap *Developer Website* untuk mengetahui nilai dari

frekuensi dan nilai dari dampak resiko yang akan terjadi pada *Website* Rental Mobil ini.

4. HASIL DAN PEMBAHASAN

4.1. Penilaian Resiko

Pada tahap ini, merupakan tahap penilaian resiko pada *Website* Rental Mobil. Proses penilaian resiko pada *Website* Rental Mobil ini terdiri dari 3 tahap, yaitu: Identifikasi resiko (*risk identification*), analisis resiko (*risk analysis*), dan evaluasi resiko (*risk evaluation*) [1].

4.2. Identifikasi Aset

Dalam melakukan identifikasi resiko pada *Website* Rental Mobil, dimulai dengan mengenali aset-aset pada sisi teknologi dan infrastruktrur yang ada untuk menunjang penggunaan *Website* Rental Mobil tersebut, yaitu terdapat aset data, aset perangkat lunak (*software*), dan aset perangkat keras (*hardware*) [13].

Tabel 1. Aset terkait *Website* Rental Mobil

Elemen Sistem Informasi	Aset Organisasi
Data	Data pelanggan, data kendaraan, data pembayaran, data riwayat rental mobil
Software	Sistem operasi, aplikasi website rental mobil, *database*, API pembayaran, sistem manajemen pemesanan, CMS (*Content Management System*)
Hardware	*Server* fisik, *router* dan *switch* jaringan, komputer admin, perangkat *backup* (*tape* drive), perangkat keamanan (*firewall*), perangkat mobile untuk administrasi lapangan, *power supply unit*, modem

Dari proses identifikasi aset pada tabel 1 diatas, telah teridentifikas aset-aset yang dimiliki untuk menunjang penggunaan *Website* Rental Mobil ini yang terdiri dari data, *software*, dan *hardware*. Dari tabel tersebut, dapat dilihat ada beberapa aset penting yang terdapat pada *Website* Rental Mobil seperti data pelanggan, data kendaraan, data pembayaran, data riwayat rental mobil, aplikasi *website* rental mobil, sistem operasi, *database*, API pembayaran, sistem manajemen pemesanan, CMS, perangkat *backup* (*tape drive*), *server* fisik, *router* dan *switch* jaringan, komputer admin, perangkat keamanan (*firewall*), perangkat *mobile* untuk administrasi lapangan, *power supply unit*, dan modem.

4.3. Identifikasi Kemungkinan Resiko

Setelah melakukan identifikasi aset dan mengetahui daftar aset yang ada pada *Website* Rental Mobil, langkah selanjutnya adalah melakukan identifikasi kemungkinan resiko yang mengancam keberadaanan setiap aset tersebut. Identifikasi dilakukan dengan mengelompokkan resiko berdasarkan faktor-faktor yang sering muncul, seperti faktor alam atau lingkungan, faktor manusia, serta faktor sistem dan infrasturuktur [13].

Tabel 2. Identifikasi Kemungkinan Resiko

Asal Resiko	Bentuk Resiko
Alam/Lingkungan	Kebakaran
	Petir
	Banjir
	Gempa Bumi
	Badai
Manusia	*Human error*
	Penyalahgunaan hak akses sistem
	Kelalaian dalam memasukan data
	Cybercrime
Sistem dan Infrastruktur	Server *down*
	Koneksi Jaringan bermasalah
	Kerusakan *hardware*
	Gagal *backup*
	Kegagalan *update*
	Overload *server*
	Overheat *server*
	System crash
	Serangan *virus* atau *malware*
	Data *corrupt*
	Listrik padam

Dari proses identifikasi resiko pada tabel 2 diatas, telah teridentifikasi tiga sumber resiko utama, yaitu resiko yang berasal dari alam atau lingkungan, manusia, serta sistem dan infrasturuktur. Dari ketiga sumber resiko tersebut, telah ditemukan total 20 resiko spesifik yang mengancam penggunaan dan keamanan *Website* Rental Mobil tersebut.

4.4. Identifikasi Dampak Resiko

Setelah proses identifikasi resiko dilakukan, beberapa kemungkinan resiko yang dapat berpotensi mengancam kinerja *Website* Rental Mobil telah teridentifikasi, termasuk faktor alam atau lingkungan, faktor manusia, serta faktor sistem dan infrasturuktur. Oleh karena itu, diperlukan analisis dampak yang dihasilkan dari masing-masing resiko yang telah teridentifikasi tersebut [13].

Tabel 3. Identifikasi Dampak Resiko

Asal Resiko	ID	Bentuk Resiko	Dampak
Alam/Lingkungan	R01	Kebakaran	Menyebabkan kerusakan pada server dan perangkat keras, kehilangan data, serta gangguan layanan. Pemulihan memerlukan biaya tinggi.
	R02	Petir	Merusak elektronik, menyebabkan gangguan akses ke *website*, dan hilangnya data.
	R03	Banjir	Merusak infrastruktur dan perangkat keras, mengganggu layanan, dan membutuhkan biaya pemulihan tinggi.
	R04	Gempa Bumi	Merusak pusat data dan *server*, menyebabkan gangguan layanan

Asal Resiko	ID	Bentuk Resiko	Dampak
			dan hilangnya data.
	R05	Badai	Mengganggu listrik dan telekomunikasi, merusak infrastruktur, dan mengakibatkan *website* tidak dapat diakses.
Manusia	R06	*Human error*	Mengakibatkan kesalahan data dan logika pemrograman, *downtime website*, dan membutuhkan waktu serta sumber daya untuk melakukan perbaikan *website*.
	R07	Penyalahgunaan hak akses sistem	Kebocoran data sensitif, gangguan operasional, dan kerugian finansial.
	R08	Kelalaian dalam memasukan data	Kesalahan data, gangguan proses pemesanan, dan ketidakpuasan pelanggan.
	R09	*Cybercrime*	Pencurian data, gangguan operasional, Peretasan system, kerugian finansial, dan biaya pemulihan tinggi.
Sistem dan Infrastruktur	R10	*Server down*	Gangguan layanan, kehilangan pendapatan, dan ketidakpuasan pelanggan.
	R11	Koneksi Jaringan bermasalah	Gangguan akses, penurunan produktivitas, dan biaya perbaikan.
	R12	Kerusakan *hardware*	Hilangnya data, gangguan operasional, dan biaya penggantian tinggi.
	R13	Gagal *backup*	Kehilangan data penting, gangguan operasional, dan kerugian finansial.
	R14	Kegagalan *update*	Kerentanan keamanan, gangguan operasional, dan biaya perbaikan.
	R15	*Overload server*	Penurunan performa *website*, gangguan layanan, dan kehilangan pendapatan.
	R16	*Overheat server*	Kerusakan *hardware*, gangguan operasional, dan biaya pendinginan tinggi
	R17	*System crash*	Gangguan operasional, hilangnya data, dan biaya pemulihan tinggi.
	R18	Serangan *virus* atau *malware*	Kebocoran data, gangguan layanan, kerugian finansial, dan biaya pemulihan.
	R19	Data *corrupt*	Kehilangan data penting, gangguan operasional, dan biaya pemulihan data.
	R20	Listrik *padam*	Gangguan operasional, hilangnya data, dan biaya tambahan untuk pemulihan serta *backup* data.

4.5. Analisis Resiko

Setelah dipetakan resiko beserta dampaknya, tahapan selanjutnya adalah menganalisis resiko. Dalam tahap ini, dilakukan penilaian terhadap resiko dengan mengacu pada tabel kriteria *likelihood*, yang mengukur frekuensi atau seberapa sering resiko tersebut terjadi, dan tabel kriteria impact, yang mengukur besaran efek atau seberapa besar dampak dari resiko tersebut [1]. Penilaian kemungkinan resiko berdasarkan pada tabel 4 (kriteria *Likelihood*) dan tabel 5 (kriteria *Impact*) akan dilakukan sebagai acuan dalam memberikan penilaian pada kemungkinan resiko yang telah teridentifikasi.

Tabel 4. Kriteria *Likelihood*

Likelihood		Deskripsi	Frekuensi per Tahun
Rating	Kriteria		
1	*Rare*	Resiko yang ada hampir tidak pernah terjadi	> 2 tahun
2	*Unlikely*	Resiko yang ada punya kemungkinan terjadi tetapi kecil (jarang)	1 – 2 tahun
3	*Possible*	Resiko yang ada mungkin saja terjadi (kadang-kadang)	7 – 12 bulan
4	*Likely*	Resiko yang ada kemungkinan besarterjadi (sering)	4 – 6 bulan
5	*AlmostCertain*	Resiko yang ada hampir selalu terjadi	1 – 3 bulan

Pada tahap ini dilakukan penilaian terhadap kemungkinan resiko pada tahap identifikasi resiko sebelumnya, dengan menggunakan tabel *Likelihood*. Pada tabel 4 diatas, terdapat 5 kriteria yang berdasarkan frekuensi kejadian kemungkinan resiko terjadi [1], [7].

Tabel 5. Kriteria *Impact*

Impact		Deskripsi
Rating	**Kriteria**	
1	*Insignificant*	Resiko yang terjadi tidak mengganggu aktivitas instansi dan pengoperasian aplikasi.
2	*Minor*	Resiko yang terjadi sedikitmengambat pengoperasianaplikasi, namun aktivitas sentral instansi tidak terganggu
3	*Moderate*	Resiko yang terjadi mengakibatkan gangguan terhadap jalannya sebagian aktivitas instansi dan pengoperasian aplikasi
4	*Major*	Resiko yang terjadi menahan nyaris semua aktivitas instansi dan pengoperasian aplikasi.
5	*Catastrophic*	Resiko yang terjadi menghentikan aktivitas instansi pengoperasian aplikasi karena mengalami gangguan total.

Pada tabel 5 di atas, terdapat lima kriteria yang berdasarkan keterangan dampak resiko tersebut terjadi dan rating dari setiap kriteria dampak nya [1], [7]. Setelah mendapatkan kriteria kemungkinan (*Likelihood*) di tabel 4, dan kriteria dampak (*Impact*) di tabel 5, maka selanjutnya penilaian terhadap kemungkinan resiko berdasarkan tabel 4 dan 5. Berikut penilaian resiko berdasarkan *likelihood* dan *impact* pada tabel 6.

Tabel 6. Penilaian Resiko *Likelihood* dan *Impact*

ID	Bentuk Resiko	Likelihood	Impact
R01	Kebakaran	2	5
R02	Petir	3	4
R03	Banjir	1	3
R04	Gempa bumi	2	5
R05	Badai	2	3
R06	*Human error*	4	3
R07	Penyalahgunaan hak akses sistem	2	4
R08	Kelalaian dalam memasukan data	4	2
R09	*Cybercrime*	5	5
R10	*Server down*	4	4
R11	Koneksi jaringan bermasalah	3	3
R12	Kerusakan *hardware*	3	4
R13	Gagal *backup*	2	4
R14	Kegagalan *update*	2	3
R15	Overload *server*	5	3
R16	Overheat *server*	5	4
R17	*System crash*	3	4
R18	Serangan *virus* atau *malware*	3	4
R19	Data *corrupt*	3	4
R20	Listrik padam	4	3

4.6. Evaluasi Resiko

Selesai mengidentifikasi resiko dan segala dampaknya, tahapan akhir dari *Risk Assessment* adalah *Risk Evaluation* atau Evaluasi Resiko. Pada tahap ini bertujuan untuk tingkatan resiko yang berdasarkan temuan analisis resiko yang telah dilakukan pada tahap sebelumnya. Proses mengevaluasi resiko akan menggunakan *Matrix* evaluasi resiko, yakni penggabungan indikator *Likelihood* dan *Impact* sebagai acuan. Pada tabel matriks evaluasi resiko terdiri dari tiga tingkatan yaitu *low*, *medium* dan *high* [2], [15].

Tabel 7. *Matrix* Evaluasi Resiko

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

Tabel 8. *Matrix* Hasil Evaluasi Resiko Berdasarkan *Likelihood* dan *Impact*

AlmostCertain			R15	R16	R09
Likely		R08	R20, R06,	R10	
Possible			R11	R12, R17, R18, R19, R02	
Unlikely			R05, R14	R07, R13	R01, R04
Rare			R03		
	Insignificant	Minor	Moderate	Major	Catastrophic

Setelah melakukan perhitungan *likelihood* dan *impact* terhadap 20 kemungkinan resiko pada tabel 8 diatas, resiko-resiko tersebut dikelompokkan berdasarkan rasio. Resiko-resiko ini kemudian diklasifikasikan ke dalam tingkat resiko tinggi (*high*), sedang (*medium*), dan rendah (*low*) sesuai dengan tingkatannya.

Tabel 9. Pengelompokan Resiko Berdasarkan Tingkatan

ID	Daftar Resiko	Likeli hood	Impact	Risk Level
R09	*Cybercrime*	5	5	HIGH
R15	*Overload server*	5	3	HIGH
R16	*Overheat server*	5	4	HIGH
R10	*Server down*	4	4	HIGH
R12	Kerusakan *hardware*	3	4	MEDIUM
R17	*System crash*	3	4	MEDIUM
R18	Serangan *virus* atau *malware*	3	4	MEDIUM
R19	Data *corrupt*	3	4	MEDIUM
R20	Listrik Padam	4	3	MEDIUM
R06	*Human error*	4	3	MEDIUM
R02	Petir	3	4	MEDIUM
R01	Kebakaran	2	5	MEDIUM
R04	Gempa bumi	2	5	MEDIUM
R05	Badai	2	3	MEDIUM
R07	Penyalahgunaan hak akses sistem	2	4	MEDIUM
R08	Kelalaian dalam memasukan data	4	2	MEDIUM
R11	Koneksi jaringan bermasalah	3	3	MEDIUM
R13	Gagal *backup*	2	4	MEDIUM
R14	Kegagalan *update*	2	3	MEDIUM
R03	Banjir	1	3	LOW

Untuk mendapatkan hasil dari evaluasi resiko dan *risk level* pada tabel 8 dan 9, maka dilakukan perhitungan dengan perkalian antara *rating likehood* dan *rating impact* yang sesuai dengan data pada tabel 6 dan mengkategorikan *risk level* dari setiap resiko tersebut sesuai dengan tabel 7. Sehingga diperoleh kriteria dari *risk level* pada masing-masing resiko adalah sebagai berikut: yang pertama untuk kategori resiko tinggi (*level of risk* tingkat *high*) memiliki kriteria dengan nilai *risk score*-nya 15 hingga 25 dengan ditandai dengan warna merah, selanjutnya untuk kategori resiko sedang (*level of risk* tingkat *medium*) memiliki kriteria dengan nilai *risk score*-nya 5 hingga 12 dengan ditandai dengan warna kuning, kemudian yang terakhir untuk kategori resiko rendah (*level of risk* tingkat *low*) memiliki kriteria dengan *risk score*-nya 1 hingga 4 dengan ditandai dengan warna hijau [15].

4.7. Perlakuan Resiko

Setelah dilakukan analisis resiko, langkah selanjutnya adalah tahap perlakuan resiko atau *Risk Treatment*. Pada tahapan ini, diberikan rekomendasi mengenai perlakuan resiko yang telah dikelompokkan berdasarkan *risk level* yang teridentifikasi dalam *Website* Rental Mobil. Tujuannya adalah mengurangi resiko dan mencegah kemungkinan resiko di masa depan [13]. Tahap perlakuan resiko dilakukan dengan memberikan saran atau rekomendasi penanganan resiko oleh peneliti, diharapkan dapat ditangani atau meminimalisir dampak dari setiap resiko yang ada pada *Website* Rental Mobil.

Tabel 10. Penanganan Resiko

ID	Daftar Resiko	Level Resiko	Tindak Lanjut
R09	*Cybercrime*	HIGH	Implementasi langkah-langkah keamanan siber yang lebih kuat, termasuk penggunaan *firewall* tingkat lanjut, enkripsi data, dan meningkatkan kemampuan untuk mengatasi ancaman siber.
R15	*Overload server*	HIGH	Mengurangi beban kerja server dengan menerapkan teknik *load balancing* dan melakukan pemantauan performa *server* secara rutin.
R16	*Overheat server*	HIGH	Menggunakan sistem pendinginan yang dapat beroperasi secara efektif dan melakukan pemantauan rutin terhadap suhu *server* untuk mencegah terjadinya *overheating*.
R10	*Server down*	HIGH	Menambah kapasitas *server* dengan menyiapkan *server* cadangan serta memonitor kinerja *server* secara *real-time* untuk mendeteksi dan menangani masalah sebelum terjadi *downtime*.
R12	Kerusakan *hardware*	MEDIUM	Melakukan pemeliharaan rutin pada perangkat keras serta menyiapkan suku cadang untuk komponen yang rentan mengalami kerusakan.
R17	*System crash*	MEDIUM	Menyusun rencana pemulihan yang komprehensif dan melakukan *monitoring* sistem secara *real-time* untuk mencegah dan mengatasi *crash* dengan cepat.
R18	Serangan *virus* atau *malware*	MEDIUM	Menggunakan perangkat lunak seperti *antivirus* dan *anti-malware* terbaru, serta melakukan *update* secara rutin dan menambah keamanan terhadap data pada *website*.
R19	Data *corrupt*	MEDIUM	Melakukan *backup* data secara rutin dan menggunakan teknik validasi data untuk mencegah dan mendeteksi kerusakan data.
R20	Listrik padam	MEDIUM	Menyediakan UPS (*Uninterruptible Power Supply*) dan generator cadangan untuk memastikan operasional tetap berjalan meskipun terjadi pemadaman listrik.
R06	*Human error*	MEDIUM	Memberikan peringatan kepada *programmer* serta melakukan pengecekan ulang secara teliti terhadap logika pemrograman sesuai dengan prosedur operasi standar (SOP) untuk meminimalkan kesalahan manusia.
R02	Petir	MEDIUM	Memasang penangkal petir dan perangkat *surge protector* untuk melindungi

ID	Daftar Resiko	Level Resiko	Tindak Lanjut
			peralatan dari kerusakan akibat sambaran petir.
R01	Kebakaran	MEDIUM	Menginstal sistem pemadaman kebakaran otomatis di seluruh area operasional dan melakukan latihan evakuasi kebakaran secara berkala.
R04	Gempa Bumi	MEDIUM	Merancang serta memperkuat struktur bangunan untuk tahan terhadap gempa, dan melakukan simulasi gempa secara rutin untuk memastikan kesiapan..
R05	Badai	MEDIUM	Melindungi bangunan dan infrastruktur dengan cara memperkuat strukturnya dan memberikan perlindungan terhadap faktor eksternal.
R07	Penyalahgunaan hak akses sistem	MEDIUM	Menerapkan kebijakan akses yang ketat, melakukan audit secara berkala, dan memantau aktivitas pengguna untuk mencegah penyalahgunaan akses ke sistem.
R08	Kelalaian dalam memasukan data	MEDIUM	Membuat sistem yang dapat menangani data dengan menerapkan validasi data otomatis untuk mengurangi kesalahan.
R11	Koneksi Jaringan bermasalah	MEDIUM	Meningkatkan infrastruktur jaringan dengan menambahkan redundansi dan memantau konektivitas secara berkelanjutan.
R13	Gagal *backup*	MEDIUM	Menetapkan sistem backup yang ketat dan melakukan pemulihan data secara rutin untuk memastikan backup data berfungsi dengan baik.
R14	Kegagalan *update*	MEDIUM	Mengevaluasi *update* di lingkungan *staging* sebelum mengaplikasikannya ke lingkungan produksi adalah langkah yang penting untuk memastikan kelancaran *update* tersebut.
R15	*Overload server*	MEDIUM	Mengurangi beban kerja server dengan menerapkan teknik *load balancing* dan melakukan pemantauan performa *server* secara rutin.
R16	*Overheat server*	MEDIUM	Menggunakan sistem pendinginan yang dapat beroperasi secara efektif dan melakukan pemantauan rutin terhadap suhu *server* untuk mencegah terjadinya *overheating*.
R03	Banjir	LOW	Memilih lokasi yang aman dari resiko banjir dan menerapkan tindakan mitigasi seperti meningkatkan ketinggian ruang *server* dan melindungi area yang rentan dengan *waterproofing*.

Melalui isi pada tabel 10 di atas, dapat dilihat bahwa rekomendasi diberikan terutama pada resiko-resiko dari tingkat *low* hingga tingkat *high*. Tujuan utama dari penanganan ini adalah untuk lebih memperhatikan resiko-resiko yang dapat menggangg atau mengancam kinerja atau proses yang berjalan dalam *Website* Rental Mobil tersebut. Dengan demikian, diharapkan rekomendasi dan saran tersebut mampu meminimalisir dan mencegah kemungkinan terjadinya resiko-resiko tersebut di masa mendatang.

5. KESIMPULAN DAN SARAN

Tahap analisis manajemen resiko pada proyek *website* rental mobil menggunakan *framework* ISO 31000 telah dilakukan. Proses analisis resiko ini melalui tiga langkah dalam tahapan evaluasi resiko yaitu identifikasi resiko, analisis resiko, dan evaluasi resiko. Setelah itu dilanjutkan dengan tahapan penanganan resiko (*risk treatment*) untuk memberikan saran tindakan yang perlu dilakukan guna mengatasi kemungkinan resiko pada proyek *website* rental mobil.

Hasil dari penelitian analisis manajemen resiko menggunakan ISO 31000 yang telah dilakukan pada proyek *website* rental mobil menunjukkan adanya 20 kemungkinan resiko yang terbagi kedalam tiga jenis asal resiko yaitu, oleh alam/lingkungan, oleh manusia, serta oleh sistem dan infrastruktur sehingga dapat menghambat proses bisnis pada proyek tersebut. Terdapat 4 kemungkinan resiko yang masuk ke dalam kategori resiko tinggi (*level of risk* tingkat *high*), Selanjutnya, terdapat 15 kemungkinan resiko yang masuk ke dalam kategori resiko sedang (*level of risk* tingkat *medium*), lalu terakhir terdapat 1 kemungkinan resiko yang masuk ke dalam kategori resiko rendah (*level of risk* tingkat *low*).

Hasil penelitian ini diharapkan dapat memberikan panduan bagi pengelola proyek *website* rental mobil dalam mengurangi kemungkinan resiko yang dapat terjadi akibat faktor-faktor yang telah teridentifikasi. Dengan menerapkan rekomendasi penanganan resiko yang diajukan, diharapkan resiko-resiko tersebut dapat diatasi.

DAFTAR PUSTAKA

[1] G. Moleong and A. R. Tanaamah, "ANALISIS RESIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI INLISLITE DI DINAS KEARSIPAN DAN PERPUSTAKAAN PROVINSI NUSA TENGGARA TIMUR," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 6, no. 2, pp. 501–506, Aug. 2022, doi: 10.36040/jati.v6i2.4840.

[2] G. Gioferi and Y. Yulhendri, "Penilaian Resiko TI Pada Website DosenIT Dengan Framework ISO 31000 Dan ISO 27002," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 5, no. 4, pp. 409–419, Oct. 2023, doi: 10.47233/jteksis.v5i4.897.

[3] D. Liko Ivander and F. S. Papilaya, "Analisis Manajemen Resiko Teknologi Informasi Menggunakan Framework ISO 31000:2018,"

Kajian Ilmiah Informatika dan Komputer, vol. 4, no. 2, pp. 1042–1051, 2023, doi: 10.30865/klik.v4i2.1174.

[4] R. Fahlepi, M. Fronita, E. Saputra, M. Luthfi Hamzah, A. Marsal, and S. Daulay, "Analisis Manajemen Resiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000," *Jurnal Sains Komputer & Informatika (J-SAKTI)*, vol. 7, no. 2, pp. 663–674, 2023.

[5] F. Mahardika, M. Agreindra H, S. A. Fatimah, and L. T. Nur F, "Manajemen Resiko Teknologi Informasi Aplikasi E-Office ASN Menggunakan ISO 31000:2018," *Infotekmesin*, vol. 14, no. 2, pp. 237–243, Jul. 2023, doi: 10.35970/infotekmesin.v14i2.1877.

[6] M. I. Fachrezi, A. Dwika Cahyono, and P. F. Tanaem, "Manajemen Resiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 2, 2021, [Online]. Available: http://jurnal.mdp.ac.id

[7] J. N. Utamajaya, A. Afrina, and A. N. Fitriah, "ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI PADA PERUSAHAAN TOKO UJUNG PANDANG GROSIR PENAJAM PASER UTARA MENGGUNAKAN FRAMEWORK ISO 31000:2018," *Sebatik*, vol. 25, no. 2, pp. 326–334, Dec. 2021, doi: 10.46984/sebatik.v25i2.1430.

[8] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Resiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 7, no. 3, pp. 546–558, Dec. 2020, doi: 10.35957/jatisi.v7i3.525.

[9] H. I. Pribadi and E. Ernastuti, "Manajemen Resiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," *JURNAL SISTEM INFORMASI BISNIS*, vol. 10, no. 1, pp. 28–35, May 2020, doi: 10.21456/vol10iss1pp28-35.

[10] H. C. Suawa and H. P. Chernovita, "ANALISIS MANAJEMEN RESIKO APLIKASI SRIKANDI PADA KANTOR DISKOMINFO KOTA MANADO MENGGUNAKAN ISO 31000," *Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 3, no. 5, pp. 604–616, 2023.

[11] R. Irfani, "PERANCANGAN USER INTERFACE WEBSITE 'Si Dimas' UNTUK MENINGKATKAN USER EXPERIENCE MENGGUNAKAN METODE HUMAN CENTERED DESIGN," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 3, pp. 2084–2087, Dec. 2023, doi: 10.36040/jati.v7i3.7106.

[12] D. Andika and A. Wijaya, "MANAJEMEN RESIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK ISO 31000:2018 PADA PT. TRUST LERINVITAL TIMUR," *Jurnal Mnemonic*, vol. 5, no. 2, pp. 111–118, Aug. 2022, doi: 10.36040/mnemonic.v5i2.4778.

[13] K. C. D. Jayonata and M. N. N. Sitokdana, "ANALISIS RESIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI CUPK MOBILE (STUDI KASUS : KSP ABC)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 1, pp. 16–25, Feb. 2024, doi: 10.29100/jipi.v9i1.4291.

[14] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "MANAJEMEN RESIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 : 2018 (STUDI KASUS: CV. XY)," *Sebatik*, vol. 23, no. 1, pp. 277–284, Jun. 2019, [Online]. Available: https://jurnal.wicida.ac.id/index.php/sebatik/article/view/572

[15] D. P. Natalie and A. D. Manuputty, "Analisis Manajemen Resiko Teknologi Informasi dengan ISO 31000:2018 pada PT Bayu Buana Tbk," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 5, pp. 1290–1301, Oct. 2022, doi: 10.30865/jurikom.v9i5.4797