

## Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000

Felisia Meini Hutabarat<sup>1</sup>, Augie David Manuputty<sup>2,\*</sup>  
Program Studi Sistem Informasi, Fakultas Teknologi Informasi,  
Universitas Kristen Satya Wacana, Salatiga  
<sup>1</sup> [682016003@student.uksw.edu](mailto:682016003@student.uksw.edu), <sup>2</sup> [augiemanuputty@gmail.com](mailto:augiemanuputty@gmail.com)

### Abstract

*VCare is a BITS (Branch IT Service) application that is applied to support businesses at PT Visionet Data Internasional. The VCare application is used for client registration that will use machine procurement services, service contracts (full managed services, managed services), merchant registration, repairment, and withdrawal of EDC (Electronic Data Capture) machines from PT Visionet Data Internasional's clients. The VCare application is very important for the company in running its business as a service provider company. In order for this application to run optimally, a risk analysis is needed to document a variety of possible risks around the VCare application, and risk treatments are also needed to minimize the possible risks that may occur. The framework used to analyze risks in PT Visionet Data Internasional is ISO 31000. The first stage used in this study is the risk assessment stage which consists of 3 stages: risk identification, risk analysis, and risk evaluation. The second stage is the risk treatment stage. So the results of the risk analysis that has been done can be used to assist companies in preventing, minimizing risks, and treating these risks according to priority risk levels, before the possibility of these risks hamper existing business in the company.*

**Keywords-** management risk analysis; ISO31000; VCare application

### Abstrak

VCare merupakan aplikasi BITS (Branch IT Service) yang di terapkan untuk menunjang bisnis yang berjalan di PT Visionet Data Internasional. Aplikasi VCare digunakan untuk pendaftaran klien yang akan menggunakan layanan pengadaan mesin, kontrak layanan (full managed service, managed service), pendafaran merchant, perbaikan, dan penarikan mesin EDC (Electronic Data Capture) dari klien PT Visionet Data Internasional. Aplikasi VCare sangat penting bagi perusahaan dalam menjalankan bisnis nya sebagai perusahaan penyedia layanan. Agar aplikasi ini dapat berjalan secara optimal maka diperlukan sebuah analisa resiko untuk mendokumentasikan berbagai macam kemungkinan resiko yang ada di sekitar aplikasi VCare, serta perlakuan resiko juga diperlukan untuk meminimalisir kemungkinan – kemungkinan resiko yang akan muncul. Kerangka kerja yang digunakan untuk menganalisa resiko pada PT Visionet Data Internasional adalah ISO 31000. Tahap pertama yang digunakan dalam penelitian ini adalah tahap penilaian resiko yang terdiri dari 3 tahapan yaitu identifikasi resiko, analisis resiko, dan evaluasi resiko. Tahap kedua adalah tahap perlakuan resiko. Sehingga hasil dari analisa resiko yang sudah di lakukan dapat digunakan untuk membantu perusahaan dalam mencegah, meminimalisir resiko, serta memperlakukan resiko – resiko tersebut sesuai prioritas level resikonya, sebelum kemungkinan resiko tersebut menghambat bisnis yang ada di perusahaan.

**Kata kunci:** analisis manajemen resiko; ISO 31000; Aplikasi VCare

\* Penulis Korespondensi

## 1. PENDAHULUAN

PT Visionet Data Internasional adalah perusahaan total *IT Managed Services* di Indonesia. PT Visionet Data Internasional menawarkan layanan *outsourcing* terkelola dari 7 pilar utama layanannya yaitu *product solution, field services, operation command center, data center, security services, developer, dan contact center*. Berbagai layanan yang ditawarkan tersebut bertujuan agar klien dapat fokus menjalankan bisnis nya tanpa harus memikirkan permasalahan IT pada perusahaannya. Perusahaan ini memiliki cakupan yang luas dengan memiliki lebih dari 155 titik layanan yang tersebar di seluruh Indonesia.

Salah satu aplikasi yang di gunakan PT Visionet Data Internasional adalah VCare. VCare merupakan aplikasi BITS (*Branch IT Service*) yang di terapkan untuk menunjang bisnis yang berjalan di PT Visionet Data Internasional. Aplikasi VCare digunakan untuk pendaftaran klien yang akan menggunakan layanan pengadaan mesin, kontrak layanan (*full managed service, managed service*), pendafaran *merchant*, perbaikan, dan penarikan mesin EDC (*Electronic Data Capture*) dari klien PT Visionet Data Internasional. Aplikasi VCare sangat penting bagi perusahaan dalam menjalankan bisnis nya sebagai perusahaan penyedia layanan.

Dalam penerapan aplikasi pasti memiliki berbagai kemungkinan resiko yang dapat mengganggu sehingga aplikasi yang dijalankan tidak berjalan secara optimal. Resiko yang dapat muncul bisa terjadi dari berbagai faktor yang ada di sekitarnya. Begitupun dalam pemanfaatan aplikasi VCare, berbagai kemungkinan resiko dapat muncul. Pada tahun 2013 dilakukan penelitian menggunakan ISO 31000 di Bandara Soekarno Hatta oleh Terry George Abisa. Analisa resiko yang di lakukan pada penelitian ini melalui 3 tahapan yang terdapat pada ISO 31000. Hasil penelitian tersebut menunjukkan adanya 7 peristiwa resiko yang berpotensi membahayakan proses yang berjalan di Bandara Soekarno Hatta. Perancangan dan sistem pengendalian resiko yang ada di Bandara Soekarno Hatta sudah di jalankan dengan baik.[1] Penelitian menggunakan ISO 31000 juga dilakukan oleh Aprilia Rahmawati pada tahun 2018. Dari analisa tersebut di dapat 21 kemungkinan resiko yang berpotensi mengganggu kinerja aplikasi iTop yang di klasifikasikan berdasarkan level resiko. Pada penelitian tersebut, perusahaan sudah melakukan manajemen resiko dengan baik, karena perusahaan tersebut merupakan perusahaan yang berfokus di bidang IT.[2]

Resiko adalah kemungkinan terjadinya peristiwa yang akan mengakibatkan kerugian bagi sebuah perusahaan. Resiko merupakan kejadian yang akan berdampak negatif terhadap tujuan dan strategi yang ingin di capai perusahaan. Kemungkinan terjadinya resiko dan akibat terhadap jalan nya bisnis merupakan hal mendasar untuk diidentifikasi dan diukur.[3]

ISO 31000 merupakan standart yang di publikasikan oleh ISO yang mengatur pengelolaan resiko. ISO 31000-2009 memberikan panduan, kerangka kerja, dan proses untuk mengatur resiko. Standart ini dapat digunakan oleh berbagai organisas atau perusahaan untuk membantu meningkatkan kemungkinan (*likelihood*) didalam proses mencapai tujuan, meningkatkan performa didalam mengidentifikasi peluang (*opportunity*) dan ancaman (*threat*) serta dilakukan untuk memanfaatkan sumber daya yang ada dalam menangani resiko (*risk treatment*).[4]

Pada tahun 2016 dilakukan penelitian analisis resiko teknologi informasi menggunakan ISO 31000 di Lembaga Penerbangan dan Antariksa Nasional (LAPAN). Dari penelitian tersebut dilakukan tahapan dan proses analisa resiko teknologi informasi terhadap *website Space Weather*

*Information and Forecast Services (SWIFTS)*. Penggunaan ISO 31000 terhadap website SWIFTS menghasilkan dokumentasi tingkat resiko dan perlakuan resiko dari pemanfaatan website tersebut.[5]

Analisis resiko teknologi informasi menggunakan ISO 31000 pada *program Human Resources Management System (HRMS)* juga di lakukan oleh Stefan Agustinus pada tahun 2017. Tujuan dilakukannya analisis resiko untuk melakukan dokumentasi kemungkinan resiko yang muncul dalam pemanfaatan program HRMS dan memberikan perlakuan resiko dengan tujuan meminimalisir kemungkinan resiko tersebut. Dari hasil analisa tersebut menemukan 26 kemungkinan resiko aplikasi HRMS beserta tingkatan level resikonya.[6]

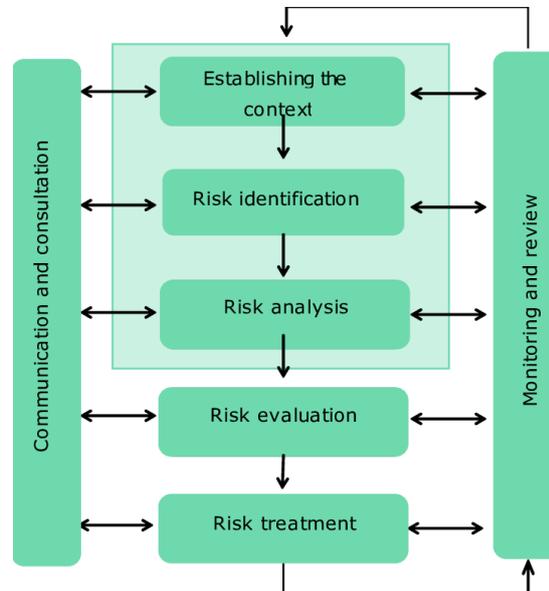
Penelitian manajemen resiko menggunakan *International Organization for Standardization (ISO) 31000* yang dilakukan untuk menganalisis aplikasi iTop pada suatu perusahaan dilakukan oleh Aprilia Rahmawati pada tahun 2018. Dari analisa tersebut di dapat 21 kemungkinan resiko yang berpotensi mengganggu kinerja aplikasi iTop yang di klasifikasikan berdasarkan level resiko.[2]

Berdasarkan penelitian-penelitian yang sudah dilakukan, dapat dinilai bahwa analisis manajemen resiko dengan ISO 31000 bertujuan untuk mengidentifikasi kemungkinan-kemungkinan resiko yang akan muncul, dampak resiko, level resiko dan perlakuan resiko terhadap kemungkinan-kemungkinan resiko yang ada pada sebuah perusahaan. Oleh sebab itu analisa manajemen resiko pada suatu perusahaan merupakan hal penting dilakukan untuk melindungi aset dan aplikasi yang digunakan agar tidak mengganggu jalannya bisnis dari sebuah perusahaan. Oleh sebab itu tujuan penulis melakukan penelitian ini adalah untuk membantu perusahaan dalam menganalisis resiko yang akan muncul. Sehingga perusahaan dapat melakukan pencegahan resiko yang akan muncul pada aset-aset yang dimiliki aplikasi VCare. Dengan adanya penelitian ini, diharapkan dapat menjadi acuan bagi perusahaan dalam memperlakukan resiko yang akan muncul dan mengganggu jalannya bisnis.

## 2. METODOLOGI PENELITIAN

*International Organization for Standardization (ISO) 31000* merupakan standar internasional yang berkaitan dengan manajemen resiko. Tujuan dari diterapkannya ISO adalah untuk memberikan pedoman dan prinsip manajemen resiko yang di akui dengan lingkup universal. Seperti yang ditunjukkan pada gambar 1 tersebut, merupakan susunan standar yang bertujuan memberikan prinsip dan manajemen resiko. Berdasarkan *International Organization for Standardization (ISO 31000:2009)*, maka penelitian ini akan dilakukan menggunakan 2 tahap yaitu pencarian informasi yang dibutuhkan didapatkan melalui proses wawancara terhadap narasumber internal dari PT Visionet Data Internasional dan tahapan kedua adalah mengolah data wawancara yang di dapat untuk kemudian di analisa berdasarkan tahapan yang ada pada kerangka kerja ISO 31000. Tahap pertama yang dilakukan untuk menganalisa adalah *Risk Assesment (Penilaian Resiko)*. Dalam proses ini memiliki 3 tahap yaitu *Risk Identification (Identifikasi Resiko)*, *Risk Analys (Analisis Resiko)*, dan *Risk Evaluation (Evaluasi Resiko)*. Tahap *Risk Assesment (Penilaian Resiko)* merupakan proses untuk menentukan potensi resiko yang akan mempengaruhi perusahaan untuk mencapai tujuan bisnis. Proses analisis resiko merupakan proses evaluasi terhadap tingkat kepentingan resiko berdasarkan kriteria yang akan ditentukan.[5]

Tahap kedua dari manajemen resiko adalah *Risk Treatment* (Perlakuan Resiko). Tahap ini dilakukan peneliti untuk menyeleksi kemungkinan-kemungkinan resiko, mengurangi, bahkan menghilangkan dampak serta kemungkinan terjadinya resiko yang akan muncul.[5]



**Gambar 1.** Prinsip dan Kerangka Kerja Manajemen Resiko

Metode yang akan di gunakan dalam penelitian ini adalah *case study research*, Metode ini berfokus pada satu objek studi kasus serta bahan penelitiannya menggunakan suatu individu atau kelompok.[7] Dengan menggunakan metode *case study research* peneliti dapat lebih fokus kepada objek penelitiannya untuk mencari dan mengumpulkan data yang dibutuhkan untuk menjawab permasalahan yang terjadi. Data yang digunakan pada penelitian ini adalah data primer yang didapatkan dari dokumen yang sudah divalidasi dan terverifikasi oleh narasumber. Hasil dari penelitian ini berupa data kualitatif yang di dapatkan melalui hasil wawancara dengan narasumber terkait. Data yang di dapatkan dari sumber tesis dan disertasi tidak dapat digunakan karena termasuk data tertier.[2]

Narasumber dari penelitian ini adalah *Business Analyst* yang melakukan perancangan, analisa pada proses dan sistem yang berjalan pada aplikasi VCare. Juga *Application Developer* yang membuat, mengembangkan, dan memperbaiki saat aplikasi VCare mengalami kendala dan gangguan. Kedua narasumber tersebut sebagai sumber internal dari penelitian yang di lakukan di PT Visionet Data Internasional.

### 3. HASIL DAN PEMBAHASAN

#### 1. Tahap Penilaian Resiko (Risk Assesment)

Pada tahap proses penilaian resiko pada aplikasi VCare ini akan dilakukan 3 tahap sesuai dengan pedoman analisis manajemen resiko ISO 31000. 3 tahap penilaian tersebut adalah tahap identifikasi resiko, tahap analisis resiko, dan tahap evaluasi resiko.

### 1.1 Identifikasi Resiko (*risk identification*)

Tahap pertama yang dilakukan dalam tahap penilaian resiko (*risk assessment*) adalah proses identifikasi resiko (*risk identification*) atau identifikasi aset yang berhubungan dengan aplikasi VCare. Dalam proses ini dilakukan wawancara dengan *business analyst* dan *developer* dari aplikasi ini. Pada tahap ini dilakukan identifikasi terhadap aset data, *software* hingga *hardware* yang berhubungan dengan aplikasi VCare.

**Tabel 1. Identifikasi Aset VCare**

Komponen Sistem Informasi	Aset VCare
Data	<i>Data Merchant, Data Aset, Data SPK (Surat Perintah Kerja), Data Informasi, Data User</i>
Software	Aplikasi VCare
Hardware	<i>Personal Computer (PC), Server Database, Server Web Service</i>

Setelah melakukan tahap identifikasi aset yang dimiliki aplikasi VCare melalui proses wawancara maka di dapat informasi berupa data, *software*, hingga *hardware*, selanjutnya perlu dilakukan identifikasi kemungkinan-kemungkinan resiko yang ada di sekitar aset aplikasi VCare. Identifikasi ini dilakukan dengan melihat resiko yang akan muncul dari beragam faktor yang akan mengancam aplikasi seperti alam/lingkungan, manusia, sistem dan infrastruktur yang akan mengancam aplikasi VCare. Kemungkinan-kemungkinan resiko tersebut dapat dilihat pada Tabel 2.

**Tabel 2. Identifikasi Kemungkinan Resiko**

Faktor	ID	Kemungkinan Resiko
Alam/Lingkungan	KR01	Kebakaran
	KR02	Banjir
	KR03	Gempa Bumi
	KR04	Petir
Manusia	KR05	Penyalahgunaan hak akses
	KR06	<i>Human error</i>
	KR07	<i>User interface</i> aplikasi sulit di pahami
	KR08	Pencurian perangkat/Data
	KR09	Kerusakan akibat ulah manusia ( <i>cybercrime</i> )
Sistem dan Infrastruktur	KR10	<i>Server Down</i>
	KR11	<i>Overload</i>
	KR12	<i>Overheat</i>
	KR13	Koneksi jaringan terputus

KR14	<i>Web service</i> mati secara tiba-tiba
KR15	Memori penuh
KR16	<i>Data corrupt</i>
KR17	<i>Backup failure</i>
KR18	Kerusakan <i>hardware</i>
KR19	Koneksi jaringan tidak stabil
KR20	Listrik padam

Dari tahap identifikasi resiko, ditemukan 20 kemungkinan resiko yang berasal dari faktor alam/lingkungan, manusia, serta sistem dan infrastruktur yang mengganggu penerapan aplikasi VCare. Pada tahap ini di lakukan identifikasi dampak seperti apa yang akan dialami oleh aplikasi VCare setelah di ketahui kemungkinan-kemungkinan resiko yang sudah diidentifikasi sebelumnya. Detail identifikasi dampak resiko dapat di lihat pada Tabel 3.

**Tabel 3. Identifikasi Dampak Resiko**

ID	Kemungkinan Resiko	Dampak
KR01	Kebakaran	Kerusakan insfrastruktur perusahaan dan aktivitas bisnis berhenti
KR02	Banjir	Aktivitas bisnis perusahaan terhambat
KR03	Gempa Bumi	Kerusakan insfrastruktur perusahaan dan aktivitas bisnis berhenti
KR04	Petir	Kerusakan infrastuktur perusahaan
KR05	Penyalahgunaan hak akses	Tidak berpengaruh karena dalam aplikasi VCare tidak menyimpan data finansial
KR06	<i>Human error</i>	Proses layanan tidak berjalan dengan optimal
KR07	<i>User interface</i> aplikasi sulit di pahami	<i>User</i> sulit memahami cara penggunaan aplikasi
KR08	Pencurian perangkat/Data	Perusahaan mengalami kerugian finansial karena kehilangan asetnya
KR09	Kerusakan akibat ulah manusia ( <i>cybercrime</i> )	Bocornya informasi data <i>merchant</i>
KR10	<i>Server Down</i>	Tidak dapat mengakses aplikasi VCare dan database sehingga pekerjaan enginner terhambat dan mengakibatkan kerugian secara finansial
KR11	<i>Overload</i>	<i>Log database</i> dan <i>log temp database</i> penuh sehingga terjadi <i>bottleneck</i>
KR12	<i>Overheat</i>	Hardware tidak bekerja secara optimal dan menyebabkan kerusakan pada <i>hardware</i> jika mengalami suhu yang panas terus menerus
KR13	Koneksi jaringan terputus	Gagal melakukan <i>update</i> secara <i>real time</i> pada aplikasi VCare <i>mobile</i>

KR14	<i>Web service</i> mati secara tiba-tiba	Aplikasi VCare tidak dapat di akses
KR15	Memori penuh	Akan terjadi proses <i>deadlock</i> pada fungsi post data API
KR16	<i>Data corrupt</i>	Perusahaan tidak dapat menerima data yang valid
KR17	<i>Backup failure</i>	Data yang akan di terima perusahaan tidak lengkap
KR18	Kerusakan <i>hardware</i>	Aktivitas perusahaann terhambat karena harus melakukan setup data ke <i>hardware</i> yang baru
KR19	Koneksi jaringan tidak stabil	Terhambatnya akses ke aplikasi VCare
KR20	Listrik padam	Aktivitas perusahaan tidak terganggu karena memiliki genset

### 1.2 Tahap Analisa Resiko (*risk analysis*)

Setelah selesai melakukan proses identifikasi, maka tahap selanjutnya adalah melakukan analisis resiko. Pada proses ini dilakukan penilaian terhadap kemungkinan-kemungkinan resiko yang sudah diidentifikasi pada proses sebelumnya dengan menggunakan tabel kriteria *likelihood* dan tabel kriteria *impact* sebagai acuan untuk proses menganalisis resiko. Pada tabel kriteria *likelihood* yang terdapat pada Tabel 4, penilaian *likelihood* dibagi menjadi 5 kriteria berdasarkan banyaknya kemungkinan resiko yang terjadi dalam waktu tertentu.

**Tabel 4. Tabel Nilai pada *Likelihood***

<i>Likelihood</i>		Deskripsi	Frekuensi Kejadian
Nilai	Kriteria		
1	<i>Rare</i>	Resiko tersebut hampir tidak pernah terjadi	>2 tahun
2	<i>Unlikely</i>	Resiko tersebut jarang terjadi	1 – 2 tahun
3	<i>Possible</i>	Resiko tersebut kadang terjadi	7 – 12 bulan
4	<i>Likely</i>	Resiko tersebut sering terjadi	4 – 6 bulan
5	<i>Certain</i>	Resiko tersebut pasti terjadi	1 – 3 bulan

Tabel 5 di bawah ini merupakan tabel penilaian *impact* atau dampak yang akan terjadi jika kemungkinan-kemungkinan resiko terjadi di perusahaan. Pada tabel ini terapat 5 kriteria dampak yang mungkin terjadi. Kriteria tersebut di bedakan berdasarkan dampak yang tidak berpengaruh dan dampak yang paling berpengaruh bagi jalanya aktivitas di perusahaan. Setelah kemungkinan resiko diidentifikasi, proses selanjutnya adalah memasukanya ke dalam tabel *impact* sesuai kriteria yang sudah didapatkan.

**Tabel 5. Tabel Kriteria *Impact***

<i>Impact</i>		Keterangan
Nilai	Kriteria	
1	<i>Insignificant</i>	Resiko tersebut tidak meganggu aktivitas perusahaan.

2	<i>Minor</i>	Resiko tersebut sedikit menghambat namun aktivitas inti perusahaan tidak terganggu.
3	<i>Moderate</i>	Resiko tersebut menyebabkan gangguan pada proses bisnis yang ada sehingga sebagian jalannya aktivitas perusahaan terhambat.
4	<i>Major</i>	Resiko tersebut hampir menghambat seluruh jalannya aktivitas perusahaan
5	<i>Catastrophic</i>	Resiko tersebut membuat aktivitas perusahaan berhenti karena proses bisnis mengalami gangguan total.

Setelah menemukan nilai kemungkinan (*likelihood*) di Tabel 4 dan dampak (*impact*) di Tabel 5 yang sudah ditentukan, maka selanjutnya akan dilakukan penilaian terhadap kemungkinan – kemungkinan resiko yang ada di sekitar aset – aset yang terkait dengan aplikasi Vcare yang sudah teridentifikasi pada proses sebelumnya. Penilaian kemungkinan – kemungkinan resiko tersebut dapat di lihat pada Tabel 6 berikut.

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

ID	Kemungkinan Resiko	<i>Likelihood</i>	<i>Impact</i>
KR01	Kebakaran	1	5
KR02	Banjir	1	3
KR03	Gempa Bumi	3	5
KR04	Petir	2	2
KR05	Penyalahgunaan hak akses	2	1
KR06	<i>Human error</i>	4	2
KR07	<i>User interface</i> aplikasi sulit di pahami	4	2
KR08	Pencurian perangkat/Data	2	2
KR09	Kerusakan akibat ulah manusia ( <i>cybercrime</i> )	2	2
KR10	<i>Server Down</i>	5	3
KR11	<i>Overload</i>	4	2
KR12	<i>Overheat</i>	3	1
KR13	Koneksi jaringan terputus	5	3
KR14	<i>Web service</i> mati secara tiba-tiba	3	3
KR15	Memori penuh	3	2
KR16	<i>Data corrupt</i>	1	2
KR17	<i>Backup failure</i>	1	1
KR18	Kerusakan <i>hardware</i>	3	2
KR19	Koneksi jaringan tidak stabil	5	3
KR20	Listrik padam	2	3

### 1.3 Tahap Evaluasi Resiko (*risk evaluation*)

Pada tahap ini dilakukan evaluasi resiko dari kemungkinan – kemungkinan resiko yang sudah diidentifikasi serta di analisis sebelumnya. Hasil dari identifikasi tersebut akan di masukan ke dalam matrix evaluasi resiko berdasarkan pedoman yang ada dalam kerangka kerja ISO 31000. Matrix evaluasi resiko tersebut di bedakan berdasarkan 3 level resiko (*risk level*) yaitu *low*,

medium, dan high. Kemungkinan resiko yang telah ditentukan dengan nilai *likelihood* dan nilai *impact* pada proses sebelumnya akan di sesuaikan dengan matrix yang ada. Pemetaan level resiko berdasarkan *likelihood* dan *impact* dapat di lihat pada Tabel 7 berikut.

**Tabel 7. Matrix evaluasi resiko**

<b>Likelihood</b>	<b>Certain</b>	5	Medium	Medium	High	High	High
	<b>Likely</b>	4	Medium	Medium	Medium	High	High
	<b>Possible</b>	3	Low	Medium	Medium	Medium	High
	<b>Unlikely</b>	2	Low	Low	Medium	Medium	Medium
	<b>Rare</b>	1	Low	Low	Low	Medium	Medium
<b>Impact</b>			<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
			<i>Insignificant</i>	<i>Minor</i>	<i>Moderate</i>	<i>Major</i>	<i>Catastrophic</i>

Setiap kemungkinan resiko yang didapat berdasarkan likelihood dan impact akan di evaluasi ke dalam tabel matrix evaluasi resiko. Pada tabel ini akan dilakukan evaluasi resiko berdasarkan dari identitas yang dimiliki oleh kemungkinan resiko, untuk di masukan ke dalam parameter sesuai kriteria *likelihood* dan kriteria *impact*.

**Tabel 8. Matrix evaluasi resiko berdasarkan *likelihood* dan *impact***

<b>Likelihood</b>	<b>Certain</b>	5			KR10 KR13 KR19		
	<b>Likely</b>	4		KR06 KR07 KR11			
	<b>Possible</b>	3	KR12	KR15 KR18	KR14		KR03
	<b>Unlikely</b>	2	KR05	KR04 KR08 KR09	KR20		
	<b>Rare</b>	1	KR17	KR16	KR02		KR01
<b>Impact</b>			<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
			<i>Insignificant</i>	<i>Minor</i>	<i>Moderate</i>	<i>Major</i>	<i>Catastrophic</i>

Setelah kemungkinan–kemungkinan resiko di masukan ke dalam matrix evaluasi berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*) maka pada Tabel 9 akan dijabarkan 20 kemungkinan resiko tersebut ke dalam level resiko dengan tingkatan *high*, *medium* hingga *low*

**Tabel 9. Level resiko dari kemungkinan resiko**

<b>ID</b>	<b>Kemungkinan Resiko</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Level</b>
KR03	Gempa Bumi	3	5	High
KR10	Server Down	5	3	High
KR13	Koneksi jaringan terputus	5	3	High

KR19	Koneksi jaringan tidak stabil	5	3	High
KR01	Kebakaran	1	5	Medium
KR06	<i>Human error</i>	4	2	Medium
KR07	<i>User interface</i> aplikasi sulit di pahami	4	2	Medium
KR11	<i>Overload</i>	4	2	Medium
KR14	<i>Web service</i> mati secara tiba-tiba	3	3	Medium
KR15	Memori penuh	3	2	Medium
KR18	Kerusakan <i>hardware</i>	3	2	Medium
KR20	Listrik padam	2	3	Medium
KR02	Banjir	1	3	Low
KR04	Petir	2	2	Low
KR05	Penyalahgunaan hak akses	2	1	Low
KR08	Pencurian perangkat/Data	2	2	Low
KR09	Kerusakan akibat ulah manusia ( <i>cybercrime</i> )	2	2	Low
KR12	<i>Overheat</i>	3	1	Low
KR16	<i>Data corrupt</i>	1	2	Low
KR17	<i>Backup failure</i>	1	1	Low

Dari hasil proses evaluasi resiko, dapat dilihat pada Tabel 9 terdapat 20 kemungkinan resiko yang sudah di analisis berdasarkan level resikonya. Terdapat 4 kemungkinan resiko yang masuk ke dalam *level of risk* tingkatan *high* yaitu gempa bumi, *server down*, koneksi jaringan terputus, dan koneksi jaringan tidak stabil. Berikutnya ada 8 kemungkinan resiko yang masuk ke dalam *level of risk* tingkatan *medium* yaitu kebakaran, *human error*, *user interface* aplikasi sulit dipahami, *overload*, *web service* mati secara tiba – tiba, memori penuh dan listrik padam. Serta terdapat 8 kemungkinan resiko yang masuk ke dalam *level of risk* tingkatan *low* yaitu banjir, petir, penyalahgunaan hak akses, pencurian perangkat/data, kerusakan akibat ulah manusia (*cybercrime*), *overheat*, *data corrupt* dan *backup failure*.

## 2. Perlakuan Resiko (*risk treatment*)

Setelah di lakukan proses identifikasi resiko disekitar aset – aset yang dimiliki oleh aplikasi VCare, selanjutnya akan dilakukan proses perlakuan resiko. Pada tahap ini akan di berikan usulan – usulan yang dapat digunakan untuk memperlakukan kemungkinan-kemungkinan resiko tersebut. Dengan adanya usulan yang diberikaan tersebut, penulis berharap resiko yang akan muncul dapat diminimalisir dengan baik agar aplikasi dapat bekerja secara optimal sehingga proses bisnis berjalan dengan lancar dan tidak mengalami kerugian ketika resiko – resiko tersebut muncul.

Tabel 10. Usulan perlakuan resiko

ID	Kemungkinan Resiko	Risk Level	Tindakan Resiko
KR03	Gempa Bumi	High	Menyediakan <i>server</i> cadangan di lokasi yang lebih aman.

KR10	<i>Server Down</i>	High	<p>Menerapkan teknik <i>mirroring</i> database pada database yang digunakan aplikasi VCare.</p> <p>Melakukan pengecekan berkala dalam 1 hari terhadap database aplikasi VCare dan database utama milik perusahaan.</p> <p>Melakukan <i>refresh</i> penggunaan db log, temp, dan RAM yang digunakan oleh aplikasi VCare</p> <p>Mengaplikasikan antivirus yang terpercaya agar tidak terinfeksi <i>malicious code</i>.</p>
KR13	Koneksi jaringan terputus	High	Melapor kebagian jaringan ketika koneksi jaringan terputus.
KR19	Koneksi jaringan tidak stabil	High	<p>Mengganti ISP (<i>Internet Service Provider</i>) yang lebih baik.</p> <p>Melapor kebagian jaringan ketika koneksi jaringan terputus dan menghambat aktivitas perusahaan.</p>
KR01	Kebakaran	Medium	<p>Menyediakan <i>server</i> cadangan di lokasi yang lebih aman.</p> <p>Menerapkan teknik <i>mirroring</i> database pada database yang digunakan aplikasi VCare.</p> <p>Memasang <i>fire detector</i> didalam gedung untuk mencegah terjadinya kebakaran.</p> <p>Memasang <i>fire hydrant system</i> dalam gedung perusahaan untuk mencegah terjadinya kebakaran.</p>
KR06	<i>Human error</i>	Medium	<p>Melakukan <i>training</i> untuk karyawan baru.</p> <p>Melakukan bimbingan dan <i>mentoring</i> untuk karyawan baru.</p> <p>Membuat <i>konwledge management system</i> untuk mendokumentasikan pengetahuan yang dimiliki karyawan baru agar tidak melakukan kesalahan yang sama.</p>
KR07	<i>User interface</i> aplikasi sulit di pahami	Medium	<p>Membuat tampilan yang lebih <i>user friendly</i> agar mudah di pahami.</p> <p>Membuat <i>manual book</i> aplikasi, sebagai petunjuk untuk <i>user</i>.</p>
KR11	<i>Overload</i>	Medium	<p>Melakukan <i>refresh</i> penggunaan db log, temp, dan RAM yang digunakan oleh aplikasi VCare.</p> <p>Melakukan pengecekan berkala terhadap database aplikasi VCare dan database utama milik perusahaan</p>

KR14	Web service mati secara tiba-tiba	Medium	Memberikan pemberitahuan kepada <i>user</i> saat <i>web service</i> mati. Melakukan <i>troubleshooting</i> saat <i>web service</i> mati.
KR15	Memori penuh	Medium	Menambah kapasitas memori yang lebih besar agar daya tampungnya lebih optimal. Melakukan cek memori secara berkala. Menghapus data – data perusahaan yang sudah tidak penting.
KR18	Kerusakan hardware	Medium	Melakukan perawatan <i>hardware</i>
KR20	Listrik padam	Medium	Menyediakan <i>generator set</i> dan UPS ( <i>Uninterruptible Power Supply</i> ) dengan daya yang disesuaikan dengan kebutuhan perusahaan. Menggunakan sumber listrik dari gardu listrik yang berbeda.
KR02	Banjir	Low	Menyimpan aset perusahaan ditempat yang lebih tinggi. Memasang <i>server</i> cadangan di lokasi berbeda yang lebih aman. Menerapkan teknik <i>mirroring</i> database pada database yang digunakan aplikasi VCare.
KR04	Petir	Low	Memasang alat penangkal petir di gedung perusahaan.
KR05	Penyalahgunaan hak akses	Low	Melakukan <i>reset password</i> secara berkala. Memasang dan memantau CCTV di gedung perusahaan.
KR08	Pencurian perangkat/Data	Low	Melakukan <i>reset password</i> secara berkala. Memasang dan memantau CCTV di gedung perusahaan.
KR09	Kerusakan akibat ulah manusia ( <i>cybercrime</i> )	Low	Mengganti <i>password server</i> secara berkala. Memasang dan memantau CCTV di gedung perusahaan.
KR12	Overheat	Low	Memastikan suhu ruangan tetap dalam suhu yang dingin Melakukan <i>service AC (air conditioner)</i> pada ruangan secara berkala.
KR16	Data corrupt	Low	Memproteksi PC dengan antivirus secara berkala untuk mencegah munculnya virus/ <i>malware</i> . Melakukan <i>backup data</i> secara berkala.

KR17	<i>Backup failure</i>	Low	Memperhatikan penggunaan memori yang digunakan database agar jangan sampai penuh. Membuat <i>maintenance plan</i> yang tepat. Melakukan <i>backup data</i> secara berkala.
------	-----------------------	-----	--

#### 4. KESIMPULAN

Berdasarkan penelitian analisis resiko teknologi informasi menggunakan ISO 31000 yang sudah dilakukan pada aplikasi VCare di PT Visionet Data Internasional melalui semua tahapan yang dimulai dari proses penilaian resiko, identifikasi resiko (*risk identification*), tahap analisis resiko (*risk analyst*), dan tahap evaluasi resiko (*risk evaluation*) hingga tahap perlakuan resiko (*risk treatment*) maka hasil analisis resiko yang sudah dilakukan, terdapat 20 kemungkinan resiko yang berpotensi mengganggu kinerja aplikasi VCare. Terdapat 4 kemungkinan resiko yang masuk ke dalam *level of risk* tingkatan *high* yaitu gempa bumi, *server down*, koneksi jaringan terputus, dan koneksi jaringan tidak stabil. Berikutnya ada 8 kemungkinan resiko yang masuk ke dalam *level of risk* tingkatan medium yaitu kebakaran, *human error*, *user interface* aplikasi sulit dipahami, *overload*, *web service* mati secara tiba – tiba, memori penuh dan listrik padam. Serta terdapat 8 kemungkinan resiko yang masuk ke dalam *level of risk* tingkatan *low* yaitu banjir, petir, penyalahgunaan hak akses, pencurian perangkat/data, kerusakan akibat ulah manusia (*cybercrime*), *overheat*, *data corrupt* dan *backup failure*.

Dengan melihat situasi di perusahaan dalam mengatasi resiko, sebenarnya perusahaan sudah menerapkan manajemen resiko dengan baik karena PT Visionet Data Internasional merupakan perusahaan yang berfokus pada bisnis di bidang IT. Namun terdapat kemungkinan proses penanggulangan resiko secara berkala belum dilakukan secara optimal, sehingga dari penelitian ini diharapkan dapat digunakan perusahaan dalam menyusun kebijakan untuk meminimalisir kemungkinan – kemungkinan resiko yang akan muncul dan mengganggu jalannya bisnis perusahaan di kemudian hari.

#### DAFTAR PUSTAKA

- [1] T. George, “MANAJEMEN RISIKO PADA BANDARA SOEKARNO HATTA.”
- [2] A. Rahmawati, “Jurnal sistem informasi dan teknologi,” *Sitech*, vol. Vol 1, No, pp. 1–6, 2018.
- [3] G. W. Lantang, A. D. Cahyono, and N. Ngalumsine, “Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000,” *Sebatik 2621-069X*, vol. 23 No. 1, pp. 36–43, 2019.
- [4] I. G. Bagus and W. Putra, “Pemerintahan Dengan Menggunakan Framework Iso 31000 : 2009 of Software Analysis Implementation on Government Environment By Using Iso 31000 : 2009,” 2015.
- [5] Nice and Imbar, “Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000,” *J. Inform. dan Sist. Inf. Univ. Ciputra*, vol. 02, no.

- 02, 2016.
- [6] S. Agustinus, A. Nugroho, and A. D. Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 3, pp. 250–258, 2017.
- [7] Z. A. Hasibuan, *METODOLOGI PENELITIAN PADA BIDANG ILMU KOMPUTER DAN TEKNOLOGI INFORMASI*. 2007.