

MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 : 2018 (STUDI KASUS: CV. XY)

Krisdana Bima Mahardika¹⁾, Agustinus Fritz Wijaya²⁾, dan Ariya Dwika Cahyono³⁾

^{1,2,3}Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

^{1,2,3}Jalan Diponegoro No. 52-60, Salatiga, 50711

E-mail : 682015046@student.uksw.edu¹⁾, agustinus.wijaya@uksw.edu²⁾, ariya.dc@uksw.edu³⁾

ABSTRAK

CV. XY merupakan salah satu penghasil bus terbesar saat ini di Indonesia. CV. XY menggunakan ISO 9001 : 2008 sebagai pedoman standarisasi mutu perusahaan. Namun, standarisasi tersebut masih mencakup secara keseluruhan dan belum ada standarisasi khusus untuk bagian IT. Maka peneliti tertarik untuk menganalisis manajemen risiko pada bagian IT CV. XY. Manajemen risiko adalah suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Dalam penilaian risiko, ada beberapa tahapan meliputi identifikasi asset, identifikasi risiko, dan analisis risiko. Dari hasil penelitian, didapatkan hasil bahwa ada kemungkinan – kemungkinan risiko dengan berbagai tingkatan. Maka peneliti menyimpulkan bahwa IT CV. XY belum memenuhi syarat standar ISO 31000 : 2018, dikarenakan dari beberapa tahapan pengamatan, wawancara, serta penilaian terhadap risiko itu sendiri masih banyak temuan risiko yang belum bisa terpecahkan oleh perusahaan.

Kata Kunci: Manajemen Risiko, ISO 31000 : 2018, Analisis Risiko, Teknologi Informasi, Penilaian Risiko

1. PENDAHULUAN

Risiko adalah hal yang tidak pasti dan mempunyai dampak negatif terhadap suatu tujuan atau keinginan yang akan dicapai. Risiko dapat menjadi tantangan besar bagi setiap perusahaan, dimana setiap perusahaan harus bisa melakukan manajemen risiko dengan baik. Dengan adanya manajemen risiko yang dikelola dengan baik, perusahaan dapat melindungi nilai (*protecting value*) dan menambah nilai (*creating value*) perusahaan (Yap, 2017). Keberadaan manajemen risiko dalam pengelolaan suatu perusahaan adalah hal yang penting. Mengetahui risiko-risiko serta merencanakan tindakan untuk meminimalisir atas kejadian risiko tersebut hingga membuat kebijakan mengatasi risiko adalah bagian dari manajemen risiko. Penerapan manajemen risiko tidak lepas dari standar yang mengaturnya. Di Indonesia ada beberapa standar yang di kenal seperti *Committee of Sponsoring Organizations of the Treadway Commission*, COSO ERM *integrated framework* 2004, AIRMIC/ALARM/IRM:2002, CAN/CSA-Q850-97(R2009), GRC *Capability Model*, serta ISO 31000:2018.

ISO 31000 adalah panduan penerapan risiko yang terdiri atas tiga elemen, antara lain : prinsip (*principle*), kerangka kerja (*framework*), dan proses (*process*). Prinsip manajemen risiko adalah dasar praktik atau filosofi manajemen risiko. Kerangka kerja adalah pengaturan sistem manajemen risiko secara terstruktur dan sistematis di seluruh organisasi. Proses adalah aktifitas pengelolaan risiko yang sistematis dan saling terkait.

Didirikan pada tahun 1967, CV. XY memulai perjalanan pertama sebagai toko mesin di sebuah kota. Toko tersebut awalnya difokuskan pada mesin otomotif. Dalam tiga tahun pertama, toko tumbuh dengan pesat. Pada tahun 1970, toko ini harus pindah ke lokasi baru yang diperluas. Seiring waktu, beberapa divisi baru didirikan. Akhirnya pada tahun 1977, CV. XY mendirikan divisi auto-manufaktur dan sekaligus pada tahun tersebut CV. XY merintis produk karoseri pertama mereka yaitu: Mitsubishi T – 120 mininya. Pesatnya pertumbuhan divisi auto-manufaktur membutuhkan lokasi yang jauh lebih besar. Pada tahun 1978, divisi ini dipindahkan ke sebuah kabupaten. Dengan lahan seluas 5.000m², bus serta kendaraan komersial lainnya berkumpul. Lokasinya yang berada di Ungaran, Jawa Tengah tersebut kian berkembang di kemudian hari. Tidak terasa, luasnya mencapai 70.000 m² dan akan bertambah luas.

Beberapa inovasi yang telah dihasilkan, mengukuhkan CV. XY sebagai pembangun bus terbesar di Indonesia hingga saat ini. Kapasitas produknya mencapai 1.000 bus per tahun. Kebutuhan pelanggan menjadi hal utama dalam pelayanan CV. Mereka bekerja sangat memperhatikan detail sekecil apapun dalam rangka membantu meningkatkan keselamatan dan kepuasan pelanggan juga penumpang.

Saat ini, kompetisi inti XY adalah bus menengah dan besar. XY memiliki jangkauan terbesar dari produk yang memiliki bus touring, bus antar kota, bus kota dan bus tujuan khusus. XY menempatkan penekanan yang sangat besar pada penyediaan produk berkualitas tertinggi terhadap pelanggan, disaat ini berkisar dari

operator lokal bus kota, operator bus antar kota lokal, operator bus wisatawan lokal dan badan-badan pemerintah untuk *International Corporate*. XY juga sudah mulai mengeksplor bus ke wilayah Asia Pasifik sejak 2009.

Dalam perkembangan teknologi informasi saat ini khususnya di CV. XY telah menjalankan proses bisnisnya dengan baik dan seimbang terutama dalam bidang teknologi informasinya yang dimiliki. XY gencar untuk selalu menjaga sistem yang ada serta melakukan perawatan berkala secara teratur demi mendukung proses bisnis yang sedang berjalan. Seperti *backup* data yang dilakukan setiap hari, perawatan *hardware* setiap minggunya, serta perawatan AC setiap bulannya demi terciptanya suasana kerja yang nyaman dan aman. CV. XY juga telah menjalankan serta berpedoman kepada standar ISO 9001 : 2008 untuk menjadikannya sebagai standarisasi dalam manajemen mutu demi mendukung pelaksanaan proses produksi perusahaan. Semua klausul dalam standar ISO 9001 : 2008 diterapkan dalam pelaksanaan kegiatan produksi karoseri karena semua syarat dalam standar ini bersifat umum dapat diterapkan untuk semua organisasi tanpa melihat jenis, ukuran dan produk yang dihasilkan. Seiring berjalannya serta berkembangnya proses bisnis yang berjalan di CV. XY tidak jauh dengan kendala yang dihadapi pula dalam IT nya. Hal yang sering muncul ketika proses bisnis sedang berjalan yakni seperti listrik yang sering padam secara tiba-tiba dan berdampak kepada *server* yang sedang beroperasi, sehingga berdampak pada kekuatan serta kualitas *server* menjadi menurun. Serta kurangnya sumber daya manusia (SDM) sering menjadi kendala untuk meningkatkan efisiensi dalam proses kinerja. Saat ini IT XY sedang mengembangkan *software development* menggunakan android untuk kemudahan pengaksesan informasi cepat serta meminimalisir kendala yang sering terjadi.

2. RUANG LINGKUP

Penelitian ini merupakan jenis penelitian kualitatif dengan pendekatan studi kasus, dimana peneliti mengeksplorasi IT pada CV. XY.

3. BAHAN DAN METODE

Penelitian ini bertempat di CV. XY yang beralamat di Jl. Raya Ungaran, Km. 24,9 Ungaran, Kec. Bergas, Semarang, Jawa Tengah. Penelitian dilakukan mulai September 2018 sampai Februari 2019. Metode yang digunakan dalam penelitian ini adalah metode Kualitatif, dan peneliti mengumpulkan data melalui observasi dan wawancara (Fitrah, Muh dkk, 2017).

3.1 Kajian Empirik

Risiko selalu berhubungan dengan ketidakpastian sehingga dalam kegiatan apapun pasti tidak akan terhindar dari sebuah risiko. Risiko selalu mengikuti semua kegiatan baik di bidang pengelolaan keuangan, pengelolaan perusahaan maupun dalam kehidupan

sehari-hari. Maka diperlukan suatu cara untuk mengatasi risiko tersebut yang disebut manajemen risiko. Manajemen risiko adalah suatu cara untuk mengelola risiko tersebut agar menjadi sebuah peluang, bahkan bisa menjadi ancaman juga bagi perusahaan lain (Widagdo dkk, 2018).

Penelitian sebelumnya yang berkaitan dengan ISO 31000 dilakukan oleh Stefan Agustinus dengan judul "*Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS*" pada tahun 2017. Penelitian tersebut membahas tentang penilaian risiko terhadap aset-aset yang ada di sekitar perusahaan. Dalam penelitian ini ditemukan 2 kemungkinan risiko memiliki *level of risk* dengan tingkatan *high* dan 18 kemungkinan risiko dengan tingkatan *medium* yang dapat mengganggu kinerja perusahaan. Dengan adanya penilaian risiko, diharapkan mampu meminimalkan kerugian yang dialami perusahaan (Agustinus, 2017).

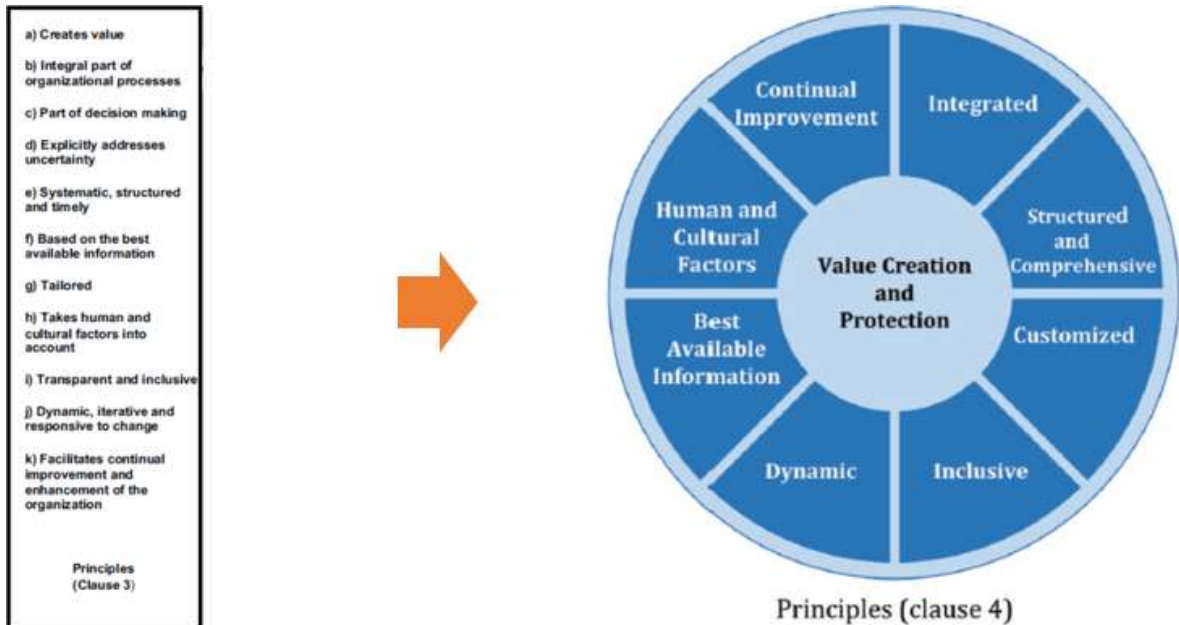
Penelitian lain yang berkaitan dengan ISO 31000 adalah Analisis Risiko Teknologi Informasi Berbasis *Risk Management* Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) oleh Andi Novia Rilyani pada 2015. Penelitian ini berfokus pada i-Gracias (*Integrated Academic Information System*), yaitu sebuah aplikasi yang diakses oleh dosen, mahasiswa, dan staf yang ada di Telkom University. Dari penelitian tersebut didapatkan hasil bahwa risiko yang memiliki nilai risiko paling tinggi adalah risiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran risiko menengah terdapat 30 risiko dan yang berada pada kuadran risiko rendah terdapat 12 risiko. Penanganan risiko difokuskan pada aset yang memiliki risiko tinggi dengan mengidentifikasi penyebab dan mencari solusi yang tepat (Rilyani, 2015).

Selain kedua penelitian diatas, ISO 31000 juga dapat diterapkan di perbankan seperti di jurnal Penerapan ISO 31000 dalam Pengelolaan Risiko Pada Bank Perkreditan Rakyat (Studi Kasus Bank Perkreditan Rakyat X) oleh Tiurma Meilania. Peneliti juga menggunakan metode wawancara dengan analis kredit, supervisor deposito, dan koordinator wilayah. Hasil yang diperoleh kemudian diurutkan menurut prioritasnya dan dicari solusi yang tepat (Melania, 2014).

ISO 31000 adalah panduan penerapan risiko yang terdiri atas tiga elemen: prinsip (*principle*), kerangka kerja (*framework*), dan proses (*process*). Prinsip manajemen risiko adalah dasar praktik atau filosofi manajemen risiko. Kerangka kerja adalah pengaturan sistem manajemen risiko secara terstruktur dan sistematis di seluruh organisasi. Proses adalah aktivitas pengelolaan risiko yang berurutan dan saling terkait. Secara umum, ISO 31000:2018 menyederhanakan versi 2009. Hal itu langsung terlihat antara lain dari nama yang berubah dari "*principles and guidelines*" menjadi hanya "*guidelines*" serta dari jumlah halaman yang menyusut dari 24 halaman menjadi 16 halaman.

Pada versi 2009, prinsip, kerangka kerja, dan proses digambarkan sebagai rangkaian unsur yang berurutan, sedangkan pada versi 2018 ketiga bagian ini digambarkan sebagai sistem terbuka yang saling berkaitan. Prinsip manajemen risiko berubah dari 11 prinsip pada versi 2009 menjadi 1 tujuan (*purpose*) dan 8 prinsip pada versi 2018. Delapan prinsip lain disederhanakan pernyataannya menjadi (1) terintegrasi,

(2) terstruktur dan komprehensif, (3) disesuaikan, (4) inklusif, (5) dinamis, (6) informasi terbaik yang tersedia, (7) faktor manusia dan budaya, serta (8) peningkatan sinambung. Hal tersebut dapat dilihat pada Gambar 1 di bawah ini (Lanin, 2018).



Gambar 1. Perbedaan ISO 31000 Tahun 2009 dan 2018

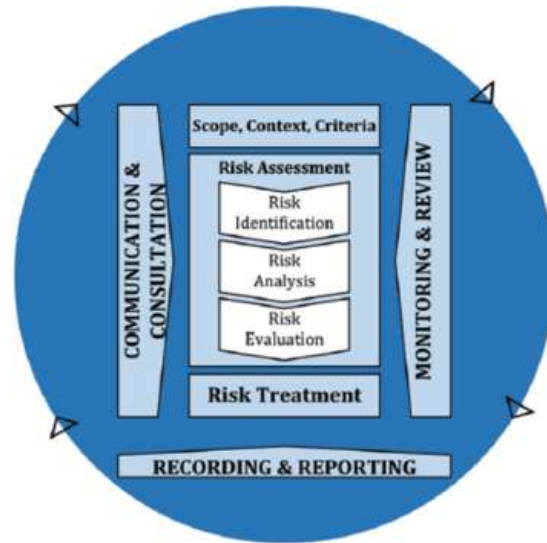
3.2 Tahapan Penelitian

Metode pengumpulan data pada penelitian ini menggunakan metode *Kualitatif* untuk mendapatkan wawasan tentang objek yang diteliti di lain itu, observasi dan analisis dokumen dilakukan untuk mendapatkan gambaran proses kinerja ruang lingkup perusahaan. Wawancara yang dilakukan dengan Supervisor IT di CV. XY bertujuan untuk mengetahui serta menilai suatu masalah atau keadaan tertentu sebagaimana adanya. Tahapan penelitian yang akan dilakukan meliputi:

1. Studi literatur, mempelajari buku dan jurnal untuk mendapatkan pemahaman tentang topik bahasan.
2. Observasi, melakukan pengamatan terhadap objek yang diteliti.
3. Wawancara, melakukan wawancara dengan narasumber terkait objek yang diteliti.
4. Pengolahan data, melakukan pengolahan data keseluruhan dari hasil observasi, maupun wawancara sesuai dengan panduan Standar ISO 31000: 2018.
5. Laporan, melaporkan hasil temuan dan memberikan penilaian terhadap risiko.

Dalam proses penelitian ini akan menggunakan sebuah kerangka kerja The International Organization Standardization (ISO) 31000:2018 yang merupakan sebuah standar internasional yang diterbitkan pada Februari 2018 disusun dan dengan tujuan memberikan prinsip dan panduan generik untuk penerapan manajemen risiko. ISO 31000:2018 sangat membantu dalam manajemen risiko karena menyediakan prinsip, kerangka kerja, dan proses manajemen risiko yang dapat digunakan sebagai arsitektur manajemen risiko dalam usaha menjamin penerapan manajemen risiko TI yang lebih efektif. Selain itu, standar ISO 31000:2018 membantu organisasi atau perusahaan mengimplementasikan penerapan manajemen risiko berdasarkan ISO 31000:2018 yang berlaku secara efektif.

Manajemen risiko adalah suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga dapat memperoleh hasil yang optimal. Proses manajemen risiko meliputi lima kegiatan, yaitu komunikasi dan konsultasi; menentukan konteks; asesmen risiko; perlakuan risiko; serta *monitoring* dan *review*. Proses manajemen risiko dapat ditunjukkan pada Gambar 2 di bawah ini.



Gambar 2. Kerangka Kerja Manajemen Risiko ISO 31000:2018

Di bawah ini terdapat Tabel 1 yang berisikan 25 kemungkinan risiko yang akan terjadi, yang nantinya dilihat melalui frekuensi kejadian dan dampaknya. Penilaian dilakukan dengan memberikan nilai dari angka 1 sampai 5, dimana semakin besar nilainya maka semakin sering pula kemungkinan risiko terjadi dan semakin besar dampak yang ditimbulkan.

Tabel 1. Penilaian Frekuensi dan Dampak

No	Kemungkinan Risiko
1	Kehilangan data
2	Kesalahan yang dilakukan Karyawan (Human Error)
3	Server down
4	Kerusakan pada hardware
5	Kegagalan backup data
6	Overheat
7	Overload
8	Web Service mati tiba-tiba
9	Maintenance tidak terjadwal
10	Pencurian perangkat data
11	Mantan karyawan masih memiliki akses informasi data penting
12	Kebocoran data informasi perusahaan
13	Listrik padam
14	Kebakaran
15	Petir
16	CCTV tidak berfungsi dengan baik
17	Penyalahgunaan hak akses
18	Teknologi tidak terupdate
19	User interface program atau aplikasi susah dipahami
20	Dokumentasi program tidak lengkap
21	Koneksi jaringan terputus
22	Program tidak terselesaikan tepat waktu
23	Pemeliharaan keamanan system
24	Genset tidak berfungsi atau rusak
25	Program crash

Keterangan Tabel 1 :

Frekuensi kejadian :

1. Sangat kecil (Risiko tersebut kecil kemungkinan terjadi bahkan tidak pernah terjadi > 5 tahun).
2. Kecil (Risiko tersebut jarang terjadi 3-5 tahun).
3. Sedang (Risiko tersebut terkadang terjadi 2-4 tahun).
4. Berat (Risiko tersebut sering terjadi 1-2 tahun).

5. Sangat Berat (Risiko tersebut sudah pasti terjadi < 1 tahun).

Dampak :

1. Risiko tidak mengganggu aktivitas proses bisnis perusahaan.
2. Risiko sedikit menghambat proses bisnis perusahaan.
3. Risiko mengganggu proses bisnis perusahaan.
4. Risiko menghambat bagian tertentu proses bisnis perusahaan.
5. Risiko menghambat serta mengganggu seluruh proses bisnis perusahaan.

4. PEMBAHASAN

Proses penilaian risiko didahului dengan beberapa tahap identifikasi dan selanjutnya dilakukan tahap analisis.

4.1 Identifikasi aset

Dalam tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem CV. XY dilihat dari sisi Teknologi Informasi melalui proses *observasi* dan *wawancara* yang telah dilakukan dengan pihak terkait. Berikut ini adalah aset yang dimiliki IT CV. XY:

1. Personal Computer
2. Server Database
3. Server Web Service
4. Data power Logic
5. Data Sytline

4.2 Identifikasi Risiko

Dalam tahap Identifikasi risiko bertujuan untuk mengidentifikasi berbagai kemungkinan risiko yang muncul dan terjadi pada aset melalui proses *studi literature* dan *wawancara*. Identifikasi Risiko merupakan suatu proses dalam menentukan apa, bagaimana, dan mengapa suatu kejadian dapat terjadi. Proses identifikasi risiko harus dilakukan secara komprehensif / menyeluruh agar nantinya risiko dapat dinilai secara sistematis (Husein, 2015). Proses ini dimulai dari mengidentifikasi berbagai kemungkinan risiko yang muncul dan terjadi pada Teknologi Informasi sistem CV. XY. Beberapa kemungkinan risiko yang muncul dapat dilihat pada Tabel 2 di bawah ini. Setelah daftar risiko diperoleh maka mulailah proses analisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari risiko tersebut bagi perusahaan.

Tabel 2. Kemungkinan Risiko

No	Kemungkinan Risiko
1	Kehilangan data
2	Kesalahan yang dilakukan Karyawan (Human Error)
3	Server down
4	Kerusakan pada hardware
5	Kegagalan backup data
6	Overheat
7	Overload
8	Web Service mati tiba-tiba
9	Maintenance tidak terjadwal
10	Pencurian perangkat data
11	Mantan karyawan masih memiliki akses informasi data

	penting
12	Kebocoran data informasi perusahaan
13	Listrik padam
14	Kebakaran
15	Petir
16	CCTV tidak berfungsi dengan baik
17	Penyalahgunaan hak akses
18	Teknologi tidak terupdate
19	User interface program atau aplikasi susah dipahami
20	Dokumentasi program tidak lengkap
21	Koneksi jaringan terputus tidak stabil
22	Program tidak terselesaikan tepat waktu
23	Pemeliharaan keamanan system
24	Genset tidak berfungsi atau rusak
25	Program crash

4.3 Analisis Risiko pada Teknologi Informasi CV. XY

Analisis risiko merupakan upaya untuk memahami risiko lebih dalam. Pada proses ini pula akan dilakukan penilaian terhadap kemungkinan risiko yang sudah teridentifikasi. Analisis risiko ini akan menjadi masukan bagi risiko serta strategi proses pengambilan keputusan mengenai risiko tersebut. Di dalam IT CV. XY sendiri terdapat beberapa temuan risiko yang sering timbul hingga mengganggu berjalannya proses bisnis IT mereka. Risiko pertama yakni diawali dengan kurangnya Sumber Daya Manusia dimana dalam organisasi IT di CV. XY hanya beranggotakan 5 orang, terdiri dari 2 orang pemegang hardware serta 2 orang pemegang software dan 1 orang sebagai staff pembantu. Dari segi keefektifan mereka kurang karena banyaknya aset perusahaan yang belum berjalan dengan baik seperti koneksi jaringan yang buruk, kinerja sistem absensi karyawan yang sering error serta proses marketing dalam era Teknologi Informasi belum terlaksana dengan baik. Ini berdampak pada rutinitas kerja organisasi IT sehingga menjadikan double kerja. Sedangkan dari segi efisiensi mereka sudah efisien karena dengan hanya beranggotakan 5 orang mereka sudah memiliki wewenang masing-masing.

Risiko kedua yakni mengenai lemahnya serta kurangnya pasokan listrik di perusahaan membuat listrik perusahaan sering padam, ini berdampak pada kinerja server yang sedang berjalan yang harus mengalami penurunan kualitas karena sering down secara mendadak dan pada saat listrik menyala server tidaklah menyala dahulu sehingga ini berdampak pada errornya sistem yang sedang berjalan dalam perusahaan tersebut salah satunya sistem absensi karyawan dan marketing. Di samping hal tersebut CV. XY akan segera bekerja sama dengan Android untuk mengembangkan perusahaan mereka demi perbaikan sistem yang lebih baik serta mudah untuk pemantauan dan pengaplikasiannya.

Manajemen risiko dibuat untuk melindungi suatu perusahaan atau organisasi yang juga mencakup karyawan, properti, reputasi dan lainnya dari sebuah bahaya yang sewaktu – waktu dapat terjadi. Dapat kita ketahui bahwa tidak semua risiko dapat dihilangkan atau dihindari, oleh karena itu diperlukan tindakan pencegahan untuk menghadapi risiko yang telah

teridentifikasi tersebut. Tabel 3 di bawah ini menjabarkan 25 kemungkinan risiko di CV. XY dan beberapa dampak yang ditimbulkan.

Tabel 3 Kemungkinan Risiko dan Dampak

No	Kemungkinan Risiko	Dampak
1	Kehilangan data	-Hilangnya data karyawan -Hilangnya Pencatatan gaji karyawan
2	Kesalahan yang di lakukan Karyawan (Human Error)	-menyebabkan kecelakaan kerja -proses kerja terhambat
3	Server down	-Menghambat proses bisnis yang sedang berjalan dalam bidang pemasaran -Aplikasi yang ada di dalam perusahaan menjadi error / tidak dapat berjalan dengan baik
4	Kerusakan pada hardware	-mengurangi jumlah aset perusahaan -mengurangi kinerja
5	Kegagalan backup data	-tidak adanya pembaruan data -kehilangan data-data sebelumnya
6	Overheat	-software aplikasi yang sedang digunakan menjadi lambat / error
7	Overload	-berdampak pada kinerja server yang menjadi lambat
8	Web Service mati tiba-tiba	-kemungkinan hilangnya data
9	Maintenance tidak terjadwal	-melemahnya kapasitas <i>personal computer</i>
10	Pencurian perangkat data	-banyak data penting tentang perusahaan yang hilang -kerugian finansial
11	Mantan karyawan masih memiliki akses informasi data penting	-kemungkinan bocornya data perusahaan
12	Kebocoran data informasi perusahaan	- banyak data penting tentang perusahaan yang hilang -kerugian finansial
13	Listrik padam	-kerugian operasional perusahaan -mengganggu proses kerja server -kualitas server menurun
14	Kebakaran	-kerusakan sarana dan prasarana perusahaan -kerugian materiil -menghambat aktivitas perusahaan
15	Petir	-kerusakan sarana dan prasarana perusahaan
16	CCTV tidak berfungsi dengan baik	-pemantauan proses kerja di perusahaan menjadi kurang efektif -berkurangnya tingkat keamanan
17	Penyalahgunaan hak akses	-bocornya data perusahaan
18	Teknologi tidak terupdate	-proses kerja melambat -perusahaan menjadi sulit untuk berkembang dan tidak mengikuti tren
19	User interface program atau aplikasi susah dipahami	-memperlambat proses kerja di perusahaan
20	Dokumentasi program tidak lengkap	-memperlambat proses kerja di perusahaan

21	Koneksi jaringan terputus tidak stabil	-komunikasi terhambat -proses pemasaran menurun
22	Program tidak terselesaikan tepat waktu	-perusahaan merugi -mengurangi prestasi perusahaan
23	Pemeliharaan keamanan sistem	-data / informasi penting mudah bocor
24	Genset tidak berfungsi atau rusak	-mengganggu aktivitas perusahaan
25	Program crash	-SOP yang ada tidak dapat berjalan dengan baik

Setelah dilakukan tahapan identifikasi kemungkinan risiko selanjutnya masuk pada tahapan penilaian risiko yang bertujuan sebagai pengelompokan kriteria pada risiko yang terjadi berdasarkan range data yang ada. Penilaian ini berguna untuk melihat neraca dalam proses bisnis perusahaan terutama dalam bidang IT CV. XY serta guna untuk penanganan dini untuk kedepannya demi tercapainya proses kinerja yang baik dan seimbang. Hasil penilaian frekuensi dan dampak dapat dilihat di Tabel 4.

Tabel 4 Hasil Penilaian Frekuensi dan Dampak

No	Kemungkinan Risiko	Frekuensi	Dampak
1	Kehilangan data	1	4
2	Kesalahan yang di lakukan Karyawan (Human Error)	3	3
3	Server down	2	5
4	Kerusakan pada hardware	2	5
5	Kegagalan backup data	1	3
6	Overheat	3	3
7	Overload	3	4
8	Web Service mati tiba-tiba	3	4
9	Maintenance tidak terjadwal	1	3
10	Pencurian perangkat data	1	5
11	Mantan karyawan masih memiliki akses informasi data penting	1	5
12	Kebocoran data informasi perusahaan	1	5
13	Listrik padam	4	5
14	Kebakaran	1	5
15	Petir	2	2
16	CCTV tidak berfungsi dengan baik	2	2
17	Penyalahgunaan hak akses	1	5
18	Teknologi tidak terupdate	1	2
19	User interface program atau aplikasi susah dipahami	1	5
20	Dokumentasi program tidak lengkap	1	5
21	Koneksi jaringan terputus	3	5
22	Program tidak terselesaikan tepat waktu	1	5
23	Pemeliharaan keamanan system	3	2
24	Genset tidak berfungsi atau rusak	2	5
25	Program crash	2	5

Pada tahap penilaian frekuensi dan dampak, dilakukan penilaian terhadap kemungkinan risiko yang bisa saja terjadi di CV. XY. Frekuensi dan dampak diisi dengan angka 1 sampai dengan 5 sesuai dengan kondisi yang ada. Semakin besar nilai pada frekuensi kejadian, artinya risiko yang terjadi sangat berat. Begitu pula dengan dampak, nilai yang besar menandakan bahwa

risiko dapat menghambat serta mengganggu seluruh proses bisnis perusahaan.

Setelah melakukan penilaian pada tabel frekuensi dan dampak maka didapatkan angka-angka yang menunjukkan frekuensi kejadian dan seberapa besar dampak yang ditimbulkan. Dari angka tersebut dapat diketahui seberapa besar risiko yang dihasilkan. Tahap inilah yang disebut evaluasi risiko. Tujuan evaluasi risiko adalah untuk membantu proses pengambilan keputusan. Evaluasi risiko meliputi proses membandingkan hasil analisis dari masing-masing risiko terhadap kriteria risiko yang telah ditetapkan dan selanjutnya untuk menetapkan apakah suatu tindakan lebih lanjut diperlukan atau tidak (Susilo, 2018). Tabel 5 di bawah ini akan menjabarkan level risiko yang didapatkan. Level risiko yang dimaksud adalah *low, medium, dan high*.

Tabel 5 Evaluasi Risiko

No	Frekuensi	Dampak	Level Risiko
1	Rare	Major	Medium
2	Possible	Moderate	Medium
3	Unlikely	Catastrophic	Medium
4	Unlikely	Catastrophic	Medium
5	Rare	Moderate	Low
6	Possible	Moderate	Medium
7	Possible	Major	Medium
8	Possible	Major	Medium
9	Rare	Moderate	Low
10	Rare	Catastrophic	Medium
11	Rare	Catastrophic	Medium
12	Rare	Catastrophic	Medium
13	Likely	Catastrophic	High
14	Rare	Catastrophic	Medium
15	Unlikely	Minor	Low
16	Unlikely	Minor	Low
17	Rare	Catastrophic	Medium
18	Rare	Minor	Low
19	Rare	Catastrophic	Medium
20	Rare	Catastrophic	Medium
21	Possible	Catastrophic	High
22	Rare	Catastrophic	Medium
23	Possible	Minor	Medium
24	Unlikely	Catastrophic	Medium
25	Unlikely	Catastrophic	Medium

Dari tabel di atas, dapat kita lihat bahwa ada 5 kemungkinan risiko dengan tingkatan *low*, 18 kemungkinan risiko dengan tingkatan *medium*, dan 2 kemungkinan risiko dengan tingkatan *high*. Baik untuk risiko yang parah maupun signifikan, harus diadakan analisis kelemahan.

5. KESIMPULAN

CV. XY merupakan salah satu karoseri penghasil bus terbesar di Indonesia saat ini. CV. XY juga selalu menjaga sistem yang ada serta melakukan perawatan berkala demi mendukung proses bisnisnya. Karoseri tersebut juga telah berpedoman pada standar ISO 9001 : 2008 sebagai standarisasi dalam manajemen mutu. Namun pedoman tersebut masih digunakan secara menyeluruh, sehingga IT CV. XY belum memiliki

pedoman tersendiri. Berawal dari hal tersebut, peneliti tertarik untuk melakukan penilaian terhadap risiko dalam IT pada CV. XY dengan menggunakan ISO 31000 : 2018.

Setelah dilakukan beberapa tahapan, maka didapatkan hasil bahwa ada 5 kemungkinan risiko dengan tingkatan *low*, 18 kemungkinan risiko dengan tingkatan *medium*, dan 2 kemungkinan risiko dengan tingkatan *high* seperti yang tertera di Tabel 5. Maka peneliti menyimpulkan bahwa IT CV. XY belum memenuhi syarat standar ISO 31000 : 2018, dikarenakan dari beberapa tahapan pengamatan, wawancara, serta penilaian terhadap risiko itu sendiri masih banyak temuan risiko yang belum bisa terpecahkan oleh perusahaan. Walau sebenarnya IT mereka sudah berjalan sendiri dalam artian mempunyai organisasi sendiri serta mencakup pada semua departemen di CV. XY, misalnya saling terintegrasi kepada bagian keuangan, *marketing*, produksi, logistik dan HRD. Rekomendasi solusi yang diperlukan untuk *human error* nya yakni meliputi adanya *training* ulang bagi karyawan, sedangkan untuk meminimalisir pemadaman listrik secara tiba-tiba CV. XY harus memperbaiki sistem regenerasi gensetnya ketika listrik padam haruslah bagian IT terlebih dahulu yang menyala lalu untuk aplikasi absensi karyawan perlu perbaikan ulang agar berjalan dengan baik di lain sisi topangan daya yang harus besar sangatlah mempengaruhi proses bisnis perusahaan.

Ketika ada kelemahan yang bersifat rendah (sistem terkonstruksi dengan baik dan beroperasi dengan benar, maka pengendalian yang ada harus dijaga agar kelemahan tersebut semakin meningkat. Jika kelemahan bersifat menengah, maka sebaiknya pengendalian diimplementasikan. Dan ketika kelemahan mencapai tingkat yang tinggi, maka pengendalian harus diimplementasikan untuk mengurangi kelemahan tersebut.

6. DAFTAR PUSTAKA

- Agustinus, Stefan., 2017, Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS, *Jurnal RESTI* Vol. 1 No.3(2017) 250-258, <http://jurnal.iaii.or.id/>. Diakses tanggal 3 Juli 2018.
- Fitrah, Muh dkk, 2017, *Metodologi Penelitian : Penelitian Kualitatif, Tindakan Kelas dan Studi Kasus*. Jawa Barat: Cv. Jejak.
- Husein, Gilang M., 2015, Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL), *Jurnal Teknik Informatika dan Sistem Informasi* Vol. 1 No. 2 hal. 77, <https://repository.maranatha.edu/>. Diakses tanggal 16 Oktober 2018.
- Lanin, Ivan, 2018, Standar Baru Manajemen Risiko ISO 31000:2018, <https://ibfqi.com/risk-management-31000/>. Diakses tanggal 19 September 2018.

- McLeod, Jr. Raymond dan George P. Schell, 2008, *Sistem Informasi Manajemen*, Jakarta: Penerbit Salemba Empat.
- Meilania A. A. D, Tiurma., 2014, Pengelolaan Risiko Pada Bank Perkreditan Rakyat (Studi Kasus Bank Perkreditan Rakyat X), *Jurnal Administrasi Bisnis* (2014), Vol.10, No.1: hal. 17–32, <http://journal.inpar.ac.id/> . Diakses tanggal 3 Juli 2018.
- Rilyani, Andi Novia., 2015, Analisis Risiko Teknologi Informasi Berbasis *Risk Management* Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University), *e-Proceeding of Engineering* : Vol.2, No.2 Agustus 2015 6201-6208, <http://repository.telkomuniversity.ac.id/> . Diakses tanggal 18 September 2018.
- Susilo, Leo J. dan Victor Riwu Kaho, 2018, *Manajemen Risiko Berbasis ISO 31000:2018 Panduan Untuk Risk Leaders dan Risk Practitioners*, Jakarta: PT. Graasindo.
- Widagdo, Bambang dan Novi Puji Lestari, 2018, *Manajemen Resiko dan Asuransi*, Malang: Penerbit Universitas Muhammadiyah.
- Yap, Pardjo, 2017, *Panduan Praktis Manajemen Risiko Perusahaan*: Growing Publishing.