

ABSTRAK

Tujuan dari penelitian ini adalah mengidentifikasi dan mengukur resiko-resiko yang sewaktu-waktu dapat terjadi dalam penerapan teknologi informasi pada perusahaan, serta memberikan informasi mengenai resiko-resiko yang berkaitan dengan keamanan sistem teknologi informasi pada perusahaan. Metode yang digunakan yaitu: teknik pengumpulan data dan teknik analisis. Teknik pengumpulan data terdiri dari studi pustaka, studi lapangan, dimana studi lapangan dilakukan dengan wawancara dan pengamatan. Teknik analisis yang digunakan dalam pengukuran resiko adalah ISO 31000. Hasil yang dicapai yaitu ditemukannya resiko-resiko yang berkaitan dengan manajemen resiko, rencana *contingency*, serta desain dan arsitektur keamanan. Simpulan dari penelitian ini adalah masih terdapat berbagai resiko yang dapat mengancam perusahaan seperti tidak adanya rencana *contingency* dan *disaster recovery plan*.

Kata kunci: ISO 31000, Manajemen resiko.

ABSTRACT

The purpose of this study is to identify and quantify risks that may occur any time in the application of information technology in a company, as well as to provide information on the risks associated with the security of information technology system of the company. The methods used are: data collection and analysis techniques. Data collection includes: literature and field studies, in which the field study is conducted by interview and observation. Analytical technique used in the measurement of risk is ISO 31000. The results found the risks associated with risk management, contingency planning, as well as design and security architecture. It is concluded from this study that there are still a lot of risks that can threaten companies such as lack of contingency and disaster recovery plan.

Keyword: ISO 31000, Risk Management.

DAFTAR ISI

LEMBAR PENGESAHAN	Error! Bookmark not defined.
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN	ii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iii
PRAKATA	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR LAMPIRAN	xii
DAFTAR SINGKATAN	xiii
DAFTAR ISTILAH	xv
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup Kajian	2
1.5 Sumber Data	2
1.6 Sistematika Penyajian	3
BAB 2. KAJIAN TEORI	5
2.1 Manajemen Resiko	6
2.1.1 Resiko dalam Manajemen Resiko	6
2.2 <i>Risk Assessment</i>	7
2.2.1 Informasi adalah Aset	8
2.2.2 Fungsi dan Pelaksanaan <i>Risk Assessment</i>	11
2.2.3 Mempersiapkan <i>Risk Assessment</i>	12
2.2.4 Proses <i>Risk Assessment</i>	13
2.3 Mitigasi	26
BAB 3. ANALISIS DAN RANCANGAN SISTEM	30
3.1 Rancangan Analisis	30

3.1.1	Melakukan Kajian Literatur.....	31
3.1.2	Pengumpulan Data.....	31
3.1.3	<i>Risk Identification</i>	31
3.1.4	<i>Risk Assessment</i>	32
3.1.5	Risk Treatment.....	33
3.1.6	Pelaporan.....	34
3.2	Profil Pusat Penelitian dan Pengembangan Sumber Daya Air	34
3.2.1	Sejarah Puslitbang SDA diawali dari	34
3.2.2	Tugas dan Fungsi.....	35
3.2.3	Visi dan Misi Perusahaan.....	36
3.2.4	Lingkup Kegiatan.....	36
3.2.5	Struktur Organisasi Perusahaan	37
3.2.6	Struktur Organisasi Kegiatan Sistem Informasi dan Jaringan Internet40	
3.2.7	Tugas, tanggung jawab dan wewenang	41
3.3	OPEN KM (<i>Open Knowledge Management</i>)	43
3.4	Proses Alur Data dan Topologi Jaringan	44
3.5	<i>IT Risk Assesment</i>	46
3.5.1	<i>Risk Identification</i>	47
3.5.2	<i>Risk Analysis</i>	48
3.5.3	<i>Risk Evaluation</i>	50
3.6	<i>Risk Treatment</i>	53
BAB 4.	SIMPULAN DAN SARAN	61
4.1	Simpulan.....	61
4.2	Saran.....	61
	DAFTAR PUSTAKA.....	62

DAFTAR GAMBAR

Gambar 2.1 Proses menyusun manajemen resiko dengan ISO 31000	13
Gambar 3.1 Rancangan Analisis	30
Gambar 3.2 Struktur Organisasi Perusahaan	37
Gambar 3.3 Struktur Organisasi Program dan Kerjasama.....	41
Gambar 3.4 Alur Data <i>Software</i>	44
Gambar 3.5 Topologi Jaringan OPEN KM	46
Gambar 3.6 Sebaran Resiko IT berdasarkan kategori frekuensi dan kategori dampak.....	51

DAFTAR TABEL

Tabel 2-1 <i>Review Element Definitions</i>	10
Tabel 2-2 Contoh sederhana matriks probabilitas	19
Tabel 2-3 Contoh dampak sederhana.....	20
Tabel 2-4 Tabel penentuan peringkat resiko.....	22
Tabel 2-5 Contoh peringkat resiko	24
Tabel 2-6 Mengendalikan Resiko.....	28
Tabel 3-1 Dasar nilai/bobot frekuensi	48
Tabel 3-2 Dasar nilai/bobot dampak yang diakibatkan	48
Tabel 3-3 Penilaian identifikasi resiko menurut frekuensi dan dampak.....	49
Tabel 3-4 Matriks Evaluasi Resiko.....	50
Tabel 3-5 Matriks Evaluasi Resiko IT berdasarkan kategori frekuensi dan kategori dampak	51
Tabel 3-6 Evaluasi Resiko berdasarkan penilaian identifikasi dengan tabel matriks	52
Tabel 3-7 Penanggulangan Resiko dalam Perusahaan.....	53
Tabel 3-8 Hasil Usulan Mitigasi.....	55

DAFTAR LAMPIRAN

LAMPIRAN A.	PROFIL PERUSAHAAN	64
LAMPIRAN B.	USER MANUAL.....	76
LAMPIRAN C.	WAWANCARA AWAL	225
LAMPIRAN D.	HASIL KESEPAKATAN FREKUENSI DAN DAMPAK	252
LAMPIRAN E.	WAWANCARA.....	253
LAMPIRAN F.	QUISIONER.....	261
LAMPIRAN G.	PERHITUNGAN IDENTIFIKASI RESIKO	268

DAFTAR SINGKATAN

DDR3	<i>Double Data Rate type 3</i>
DPMA	Direktorat Penyelidikan Masalah Air
DRP	<i>Disaster Recovery Planning</i>
FO	<i>Fiber Optic</i>
GB	<i>Giga Byte</i>
HaKi	Hak Kekayaan Intelektual
HDD	<i>Hard Disk Drive</i>
HSE	<i>Health, Safety, Environment</i>
IIX	<i>Indonesia Internet Exchange</i>
IKMN	Inventarisasi Kelompok Milik Negara
ISO	<i>International Organization for Standardization</i>
IT	<i>Information Technology</i>
Kimbangwil	Pemukiman dan Pengembangan Wilayah
Litbang	Penelitian dan Pengembangan
LPMA	Lembaga Penyelidikan Masalah Air
MBPS	<i>Megabytes Per Second</i>
NAS	<i>Network Attached Storage</i>
NEPA	<i>National Environmental Policy Act</i>
OPEN KM	<i>OPEN Knowledge Management</i>
PNPB	Penerimaan Negara Bukan Pajak
Puslitbang	Pusat Penelitian dan Pengembangan
RAM	<i>Random Access Memory</i>
RENSTRA	Rencana Strategi
RKAKL	Rencana Kerja Anggaran Kementerian/Lembaga
SAS	<i>Statistical Analysis System</i>
SDA	Sumber Daya Air
SDM	Sumber Daya Manusia
SOP	<i>Standard Operational Procedure</i>
UK	<i>United Kingdom</i>

V en W	<i>Verkeer en Waterstaat</i>
WBS	<i>Work Breakdown Structure</i>

DAFTAR ISTILAH

<i>Akreditasi</i>	Pengakuan terhadap lembaga pendidikan yang diberikan oleh badan yang berwenang setelah dinilai bahwa lembaga itu memenuhi syarat kebakuan atau kinerja tertentu.
<i>Analisis</i>	Penyelidikan terhadap suatu peristiwa (karangan, perbuatan, dsb) untuk mengetahui keadaan yang sebenarnya.
<i>Arsitektur</i>	Seni ilmu merancang serta membuat konstruksi bangunan, jembatan, dsb.
<i>Aset</i>	Sesuatu yang mempunyai nilai tukar, modal, kekayaan.
<i>Asuransi</i>	Pertanggungan (perjanjian antara dua pihak, pihak yang satu berkewajiban membayar iuran dan pihak yang lain berkewajiban memberikan jaminan sepenuhnya kepada pembayar iuran apabila terjadi sesuatu yang menimpa pihak pertama atau barang miliknya sesuai dengan perjanjian yang dibuat).
<i>Auditor</i>	Seseorang yang memiliki kualifikasi tertentu dalam melakukan audit atas laporan keuangan dan kegiatan suatu perusahaan atau organisasi.
<i>Bandwith</i>	Nilai hitung atau perhitungan konsumsi transfer data telekomunikasi yang dihitung dalam satuan bit per detik atau yang biasa disingkat bps yang terjadi diantara computer server dan komputer server dan komputer klient dalam waktu tertentu dalam sebuah jaringan komputer.
<i>Brownout</i>	<i>Under-voltage</i> adalah tegangan listrik rendah dalam waktu lama.

<i>Chace</i>	Mekanisme penyimpanan data sekunder berkecepatan tinggi yang digunakan untuk menyimpan data/instruksi yang sering diakses.
<i>Chassis</i>	Sebuah rangka yang berfungsi sebagai penopang berat dan beban kendaraan, mesin serta penumpang.
<i>Contingency plan</i>	Suatu tindakan yang sudah dipersiapkan, untuk mengatasi kemungkinan terjadinya kondisi terhentinya produksi pada proses produksi yang terlalu lama.
<i>Cores</i>	Working part dari processor – CPU atau Central Processing Unit
<i>Crash</i>	Suatu keadaan dimana sebuah komputer atau program, baik aplikasi atau bagian dari suatu system operasi berhenti berfungsi.
<i>Cybercrime</i>	Istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, saran atau tempat terjadinya kejahatan.
<i>Defragmentasi</i>	Sebuah proses untuk menangani berkas-berkas yang mengalami fragmentasi internal.
<i>Diseminasi</i>	Suatu kegiatan yang ditunjukan kepada kelompok atau target individu agar mereka memperoleh informasi, timbul kesadaran, menerima, dan akhirnya memanfaatkan informasi tersebut.
<i>Deviden</i>	Pembagian laba kepada pemegang saham berdasarkan banyaknya saham yang dimiliki.
<i>Due dilligence</i>	Istilah yang digunakan untuk penyelidikan penilaian kinerja perusahaan atau seseorang, ataupun kinerja dari suatu kegiatan guna memenuhi standar baku yang diterapkan.

<i>Ethernet</i>	Keluarga teknologi jejaring komputer untuk jaringan wilayah setempat (LAN).
<i>File Permission</i>	Hak akses bagi user untuk membaca, menulis dan mengeksekusi sebuah file.
<i>File Server</i>	Layanan penyimpanan file secara terpusat pada suatu mesin.
<i>Firewall</i>	Suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dengan mencegah lalu lintas jaringan yang dianggap tidak aman.
<i>Finansial</i>	Ilmu keuangan dan <i>asset</i> lainnya, pengelolaan atau manajemen <i>asset</i> tersebut, dan bagaimana menghitung dan mengatur resiko proyeknya.
<i>Fluktasi</i>	Ketidak tetapan atau guncangan salah satunya terhadap harga barang atau jasa atas segala yang bisa dilihat didalam sebuah grafik.
<i>Guidance</i>	Pedoman/petunjuk untuk mengantisipasi sebelum masalah kesehatan/tumbuh kembang terjadi.
<i>Hedging</i>	Tindakan yang dilakukan untuk mengurangi atau bahkan menghilangkan resiko yang terkait dari langkah tertentu yang diambil seseorang.
<i>Hot-plug</i>	Merupakan kemampuan untuk menghapus dan menggantikan komponen pada PC ketika beroperasi.
<i>Information (Informasi)</i>	Data yang telah diolah menjadi sesuatu yang berarti bagi penerimanya dan bermanfaat bagi pengambilan keputusan saat ini atau saat mendatang.
<i>Injeksi Script</i>	Istilah umum untuk menjelaskan jenis serangan yang terdiri dari kode kode program yang kemudian dimasukan melalui celah keamanan tertentu untuk

	tujuan yang tidak baik. Jenis serangan ini biasanya terjadi karena kurangnya validasi input / output data.
<i>Investor</i>	Orang perorangan atau lembaga baik <i>domestic</i> atau <i>non domestic</i> yang melakukan sesuatu investasi (bentu penanaman modal sesuai dengan jenis investasi yang dipilihnya) baik dalam jangka pendek atau jangka panjang.
<i>Implementasi</i>	Suatu tindakan atau pelaksanaan dari sebuah rencana yang sudah disusun secara matang dan terperinci.
<i>ISO 31000</i>	Suatu standar implementasi manajemen resiko yang diterbitkan oleh <i>International Organization for Standardization</i> pada tanggal 13 November 2009.
<i>Job Description</i>	Rincian pekerjaan yang berisi informasi menyeluruh tentang tugas/kewajiban, tanggung jawab, dan kondisi-kondisi yang diperlukan apabila pekerjaan tersebut dikerjakan.
<i>Komprehensif</i>	Bersifat mampu menangkap (menerima) dengan baik, luas dan lengkap (tentang ruang lingkup atau isi).
<i>Konfigurasi</i>	Pengaturan atau proses pembuatan pengaturan dari bagian yang membentuk keseluruhan
<i>Korporasi</i>	Badan usaha yang sah, badan hukum, perusahaan atau badan usaha yang sangat besar atau beberapa perusahaan yang dikelola dan dijalankan sebagai suatu perusahaan besar.
<i>Kredibilitas</i>	Kualitas, kapabilitas, atau kekuatan untuk menimbulkan kepercayaan.
<i>Kualitatif</i>	Data yang dinyatakan dalam bentuk kata-kata atau bukan dalam bentuk angka.
<i>Kuantitatif</i>	Data yang dinyatakan dalam bentuk angka.

<i>Maintenance</i>	Segala kegiatan yang bertujuan untuk menjaga peralatan dalam kondisi terbaik.
<i>Malware</i>	Aplikasi komputer yang khusus dibuat dengan tujuan mencari celah dan kelemahan <i>software</i> .
<i>Matching</i>	Sebuah teknik dalam pengolahan citra digital untuk menemukan bagian kecil dari gambar yang cocok dengan template gambar.
<i>Metodologi</i>	Ilmu/cara yang digunakan untuk memperoleh kebenaran menggunakan penelusuran dengan tata cara tertentu dalam menemukan kebenaran, tergantung dari realitas yang sedang dikaji.
<i>Milestones</i>	Suatu bagian item pekerjaan yang dibuat seolah-olah menjadi <i>temporary finish</i> atau selesai sementara atas sekelompok atau serangkaian pekerjaan-pekerjaan yang menjadi bagian dari <i>schedule</i> besar.
<i>Nulled</i>	Suatu <i>script</i> yang berbayar yang digunakan untuk web, untuk memodifikasi <i>script</i> yang ada dan disebarluaskan dengan gratis.
<i>Obligasi</i>	Surat berharga atau sertifikat yang berisi kontrak pengakuan hutang atas pinjaman yang diterima oleh penerbit obligasi dari pemberi pinjaman (pemodal).
<i>Patch</i>	<i>Software</i> yang biasanya berukuran kecil yang didesain untuk memperbaiki, atau memperbaharui suatu program komputer ataupun data-data yang didukungnya.
<i>Plugin</i>	Sebuah program komputer yang menambah fungsionalitas sebuah program utama (suatu web atau klien).
<i>Power Supply</i>	Sebuah piranti elektronika yang berguna sebagai sumber daya untuk piranti lain terutama daya listrik.

<i>Premi</i>	Sejumlah uang yang harus dibayarkan setiap bulannya sebagai kewajiban dari tertanggung atas keikutsertaannya di asuransi.
<i>Prioritas</i>	Sebuah pilihan yang dipilih dari sekian banyak pilihan yang ada dalam pikiran, pilihan ini pada umumnya bersifat kecenderungan dalam menentukan pilihan yang lebih penting.
<i>Probabilitas</i>	Cara untuk mengungkapkan pengetahuan atau kepercayaan bahwa suatu kejadian akan berlaku atau telah terjadi.
<i>Processor</i>	Sebuah <i>chip</i> yang berupa <i>Integrated Circuit</i> (IC) yang mengontrol keseluruhan sistem komputer dan digunakan sebagai pusat atau otak dari kegiatan komputer dalam melakukan perhitungan dan menjalankan tugas <i>input</i> dan <i>output</i> .
<i>Proksimat</i>	Suatu metoda analisis kimia untuk mengidentifikasi kandungan nutrisi seperti protein, karbohidrat, lemak dan serat pada suatu zat makanan dari bahan pakan atau pangan.
<i>Rackmount</i>	Merupakan <i>casing</i> berbentuk tipis, pipih horizontal dan dapat disusun layaknya sebuah rak pada sebuah lemari khusus.
<i>Sistematis</i>	Segala usaha untuk menguraikan dan merumuskan sesuatu dalam hubungan yang teratur dan logis sehingga membentuk suatu sistem yang berarti secara utuh, menyeluruh, terpadu, mampu menjelaskan rangkaian sebab akibat menyangkut objeknya.
<i>Spesifikasi</i>	Perincian jenis dan level komponen yang akan dipakai.

<i>Terabytes</i>	1 terabytes = 1000 gigabytes (satuan kuantitas memori)
<i>Troubleshooting</i>	Sebuah bentuk penyelesaian sebuah masalah
Verifikasi	Pemeriksaan tentang kebenaran laporan, pernyataan, perhitungan uang, dsb.
<i>Watt</i>	Satuan turunan untuk daya listrik.
WBS	(<i>Work Breakdown Structure</i>) Merupakan proses awal dari <i>project</i> management yang membagi dalam fase-fase <i>project</i> .
<i>Web Browser</i>	Perangkat lunak yang berfungsi untuk menerima dan menyajikan sumber informasi di Internet.
<i>Web Server</i>	Sebuah perangkat yang menyediakan sebuah layanan bagi para penggunanya agar dapat mengakses segala jenis berkas atau file yang terdapat di sebuah halaman situs website, melalui protokol-protokol komunikasi tertentu, dengan menggunakan sebuah program atau aplikasi.