Journal of Information Systems and Informatics
Vol. 3, No. 1, March 2021 e-ISSN: 2656-4882 p-ISSN: 2656-5935

http://journal-isi.org/index.php/isi Published By DRPM-UBD

Analisis Risiko Teknologi Informasi Pada Perusahaan Toko Surabaya Cabang Surakarta

Nico Vicky Richardo[1], Melkior N.N. Sitokdana[2]

[1,2] Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
Email: [1]682017017@student.uksw.edu, [2]melkior.sitokdana@uksw.edu

Abstract

Toko Surabaya cabang Surakarta merupakan sebuah perusahaan yang bergerak dalam bidang penjualan pakaian, toko tersebut sudah menggunakan penerapan SI/TI dalam menunjang aktivitas bisnis yang dijalankan. Toko tersebut menggunakan aplikasi *SmartConsole* yang digunakan untuk menunjang penjualan, mendata stok barang, serta mendata pengeluaran sehari-hari yang dibutuhkan. Namun dalam dunia manajemen pasti selalu ada kemungkinan risiko yang mungkin dapat terjadi dan dapat mengganggu aktivitas bisnis dalam penggunaan sistem tersebut. Dengan begitu analisis risiko sangat diperlukan terhadap sumber daya SI/TI yang terdapat pada toko tersebut. Dengan menggunakan ISO 31000 diharapkan dapat meminimalisir risiko yang terdapat pada aplikasi *SmartConsole*. Hasil dari analisis risiko ini berupa analisis kemungkinan risiko, mengelompokkan kemungkinan – kemungkinan risiko berdasarkan dampak nya sehingga menghasilkan usulan tindakan risiko terhadap kemungkinan risiko yang terdapat pada aplikasi *SmartConsole*, dengan begitu toko tersebut dapat memperlakukan kemungkinan risiko yang ada sesuai dengan prioritas level risikonya dan dapat mencegah serta meminimalisir sehinga tidak mengganggu aktivitas bisnis di Toko Surabaya cabang Surakarta..

Keywords: ISO 31000, risk analysis, risk management

1. PENDAHULUAN

Perkembangan teknologi saat ini sangat cepat dan pesat sehingga teknologi menjadi kebutuhan yang sangat intim dalam kehidupan sehari hari terutama dalam dunia bisnis. Teknologi mempunyai peranan yang sangat penting bagi kemajuan sebuah organisasi atau perusahaan untuk dapat bersaing dengan para kompetitornya, terlebih lagi dengan mengoptimalkan pemanfaatkan pengelolaan SI/TI yang baik bagi organisasi atau perusahaan akan menjadikan sebuah organisasi atau perusahaan menjadi lebih efektif dan efesien dalam menjalankan setiap proses bisnis yang ada di dalam sebuah organisasi atau perusahaan tersebut[1]. Tidak sedikit organisasi atau perusahaan yang rela mengeluarkan dana yang sangat besar untuk investasi sistem informasi tersebut. Bagi perusahaan yang sukses, mereka pasti menyadari pentingnya manfaat dari SI/TI dan menggunakan SI/TI untuk mendorong (*drive*) nilai-nilai stakeholder (*stakeholder value*), serta

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

menyadari dan melakukan pengelolaan risiko (*risk management*) terhadap risiko-risiko yang terkait dengan perencanaan dan implementasi SI [2].
Pengelolaan SI/TI di suatu perusahaan memang penting begitu pula dengan Toko Surabaya Cabang Surakarta, toko baju yang sudah mengoptimalkan pengelolaan SI/TI di setiap aktifitas manajemen perusahaanya, hal ini dapat dibuktikan dengan adanya Aplikasi *SmartConsole*. Namun tidak dapat dipungkiri walaupun pengelolaan SI/TI di Toko Surabaya Cabang Surakarta sudah optimal, pasti memiliki beberapa kemungkinan ancaman dan risiko yang dapat mengganggu aktivitas proses bisnis yang berjalan terutama masih dapat dilihat secara visual dengan jelas terdapat beberapa risiko di perusahaan Toko Surabaya cabang Surakarta yang belum mendapatkan perlakuan risiko seperti *Human Error, Overheat,* dan *Server Down* sehingga diperlukan analisis dan evaluasi manajemen risiko terhadap Toko Surabaya Cabang Surakarta dengan mengidentifikasi kemungkin risiko dan potensial risiko yang ada, seberapa besar dampak dari risiko yang mungkin terjadi, penilaian dan evaluasi risiko serta apa yang harus dilakukan untuk mengantisipasi risiko dan permasalahan yang ada. Oleh karena itu diperlukan tindakan untuk mengelola risiko yang ada, tindakan mengelola risiko ini telah diatur dalam ISO 31000:2018 tentang *risk management.* Manajemen risiko adalah upaya manajemen untuk mengendalikan risiko kegiatan operasional perusahaan dengan melakukan analisis risiko, evaluasi risiko dan rencana mitigasinya [3].

Dalam hal ini tentang analisis risiko teknologi informasi aplikasi *SmartConsole* di Toko Surabaya Cabang Surakarta ini dengan pendekatan menggunakan metode ISO 31000:2018. Pada bulan Februari 2018, Organisasi Standar Nasional (ISO) memperkenalkan ISO 31000:2018 kepada public. ISO ini berisikan mengenai Standar Manajemen Risiko. Dengan diterbitkannya ISO 31000 versi terbaru ini maka diharapkan dapat menggantikan standar yang banyak berbeda yang saat ini banyak digunakan perusahaan. ISO 31000:2018 merupakan pedoman standar, instruksi, dan tuntutan bagi sebuah organisasi atau perusahaan untuk membangun sebuah pondasi dan kerangka kerja bagi suatu program manajemen risiko [4]. Pondasi tersebut meliputi aturan, tujuan, dan komitmen untuk membangun suatu program manajemen risiko yang komprehensif. Kerangka kerja meliputi perencanaan, akuntabilitas dari para karyawan, proses dan aktivitas yang digunakan untuk mengelola risiko dalam kinerja perusahaan. Untuk mengelola risiko di Toko Surabaya Cabang Surakarta ini diperlukan *risk assessment* yang diatur dalam ISO 31000:2018. Analisis risiko menggunakan ISO 31000:2018 dapat terlihat *risk value* atau nilai risiko dengan tiga tingkatan yaitu risiko dengan tingkatan rendah, sedang, dan tinggi [5].

Dengan menggunakan metode ISO 31000:2018 dimana standar dari metode ini memiliki pandangan yang lebih luas dan dapat diterapkan di berbagai ruang lingkup organisasi serta lebih konseptual dibandingkan standar lainya[6]. Fokus dari metode penilitian ini adalah untuk melakukan identifikasi dari beberapa aset

teknologi informasi di Toko Surabaya Cabang Surakarta dan mengidentifikasi kemungkinan-kemungkinan risiko yang ada, berapa besar dampak yang ditimbulkan risiko tersebut, serta memberikan rekomendasi kepada Toko Surabaya Cabang Surakarta terhadap risiko-risiko yang ada maupun risiko-risiko yang sewaktu-waktu bisa muncul. Dengan begitu kinerja dari aktivitas SI/TI maupun proses bisnis di Toko Surabaya Cabang Surakarta dapat dioptimalkan oleh pihak organisasi atau perusahaan.

Dalam dunia Manajemen, setiap hal yang dijalankan dalam suatu organisasi atau perusahaan pasti selalu diiringi dengan ancaman dan risiko. Risiko selalu membayangi setiap kegiatan yang dijalani untuk menghambat organisasi atau perusahaan untuk mencapai tujuan maupun visi dan misi mereka, maka dari itu diperlukan suatu pengendalian risiko agar mampu membantu suatu organisasi atau perusahaan untuk menangani setiap risiko yang ada dan mampu mewujudkan tujuan dari organisasi atau perusahaan tersebut.

Penelitian sebelumnya yang membahas pula tentang ISO 31000 dilakukan oleh Andi Novia Rilyani dengan judul "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000" pada tahun 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. Pada penelitian tersebut membahas tentang analisis risiko mengenai aset-aset yang berhubungan dengan sistem *i-Gracias* dilihat dari sisi Teknologi dan Infrastrukturnya. Dalam penelitian ini mendapatkan hasil bahwa risiko yang memiliki nilai risiko paling tinggi adalah 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 [7].

Penelitian lainya yang berkaitan tentang ISO 31000 di tulis oleh Francisca Lady Nice dengan judul "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada website SWIFTS menggunakan ISO 31000" pada tahun 2016. Pada penelitian ini di fokuskan pada website SWIFTS. Dari penelitian tersebut maka didapatkan hasil tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi adalah asset, baik data perangkat lunak, perangkat keras, sumber daya manusia dan prosedur yang terkait pada sistem SWIFtS yang dinilai dapat mengganggu proses bisnis LAPAN itu sendiri. Sehingga diperlukan peninjauan kembali oleh pihak kepala Divisi IT LAPAN dan penerapan pada perlakuan risiko yang disarankan[8]. Pada tahun 2017, Stefan Agustinus juga melakukan penilitian dengan judul "Analisis Risiko Teknologi Informasi pada program HRMS". Penelitian tersebut membahas tentang penilaian risiko terhadap aset-aset yang ada di sekitar perusahaan. Dalam

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

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[9].

Dari ketiga penelitian diatas keduanya sama-sama memakai ISO 31000, namun mereka masih berpedoman pada ISO 31000:2009, dimana pada Februari 2018, organisasi standar internasional ISO menerbitkan *ISO 31000:2018 Risk management — Guidelines*. Standar ini menggantikan *ISO 31000:2009 Risk management — Principles and guidelines* yang diterbitkan pada November 2009. Revisi ini merupakan bagian dari proses peninjauan sistematis yang diterapkan pada semua standar ISO. Tulisan ini secara ringkas mengulas perubahan yang diterapkan ISO 31000 versi 2018 terhadap versi 2009.

2. METODE

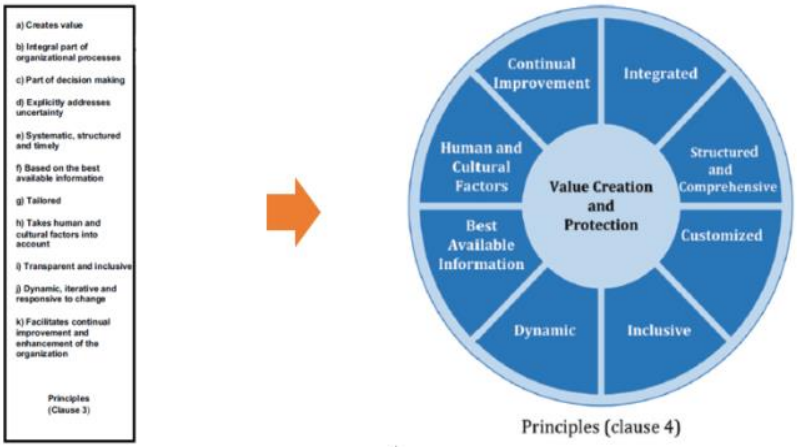
2.1. Metode Penelitian

Penilitian di Toko Surabaya Cabang Surakarta ini tentang manajemen risiko menggunakan framework ISO 31000:2018. Dimana ISO 31000:2018 memiliki prinsip-prinsip dan pedoman untuk manajemen risiko yang diakui secara internasional. Manajemen Risiko merupakan proses mengidentifikasi risiko, menganalisis serta mengevaluasi risiko yang dimana mampu untuk membentuk suatu strategi untuk mengelola risiko pada aplikasi *SmartConsole* yang ada di Toko Surabaya Cabang Surakarta. 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. Diagram yang menggambarkan hubungan prinsip, kerangka kerja, dan proses manajemen proses pun berubah. 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 [4].

Prinsip manajemen risiko berubah dari 11 prinsip pada versi 2009 menjadi 1 tujuan (*purpose*) dan 8 prinsip pada versi 2018. Satu prinsip, yaitu "penciptaan dan pelindungan nilai", diubah menjadi tujuan manajemen risiko. Dua prinsip, yaitu "bagian pengambilan keputusan" dan "secara eksplisit menangani ketidakpastian", dihapus. Delapan prinsip lain disederhanakan pernyataannya menjadi (1)

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

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. Gambar lebih detail proses manajemen risiko ISO 31000:2018 dapat dilihat pada gambar 2.



Gambar 1. Perbedaan ISO 31000:2009 dan ISO 31000:2018

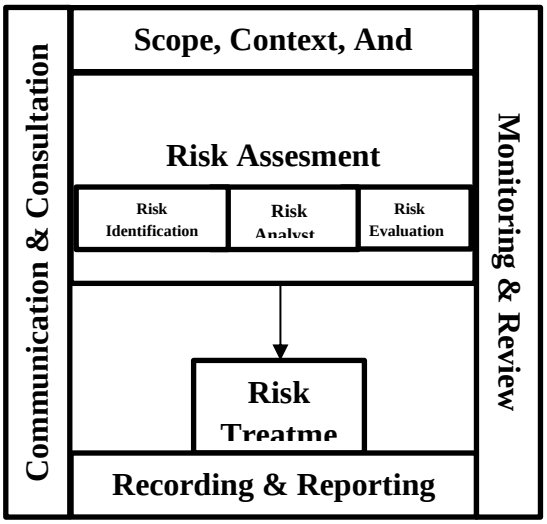
Dalam Penelitian ini, peneliti menggunakan metode penelitian *Case Study Research* dengan pendekatan kualitatif. Pendekatan ini dilakukan dengan mendiskripsikan atau menguraikan data dan fakta yang terjadi di dalam objek studi kasus kedalam bentuk kata-kata. Salah satu jenis pendekatan kualitatif ini adalah metode penelitian *Case Study Research*, dimana metode ini hanya berfokus pada satu objek tertentu, dengan metode ini peneliti akan dengan mudah mendapatkan data-data yang dibutuhkan untuk menyelesaikan permasalahan yang terjadi pada objek studi kasus. Dalam metode *Case Study Research* ini dilakukan dengan beberapa tahapan dimana tahapan-tahapan ini sesuai dengan manajemen risiko dari *framework* ISO 31000:2018. Dimana untuk melakukan riset ini dalam mencari segala informasi yang dibutuhkan guna menunjang penelitian terhadap aplikasi *SmartConsole* di Toko Surabaya Cabang Surakarta. Data yang didapatkan ini berupa data primer yang didapatkan melalui wawancara dengan pihak internal terkait penelitian ini[10].

2.2. Metode Pengambilan Data

Metode pengambilan data merupakan teknik yang digunakan peneliti untuk pengumpulan data guna mendapatkan segala informasi yang digunakan oleh peneliti sebagai bahan penelitian untuk mencapai tujuan penelitian[11]. Dalam penelitian ini peneliti mengambil data dengan melakukan wawancara terhadap narasumber internal dari perusahaan Toko Surabaya cabang Surakarta, yaitu salah satu *stakeholder* perusahaan yang merupakan sumber internal dari penelitian ini.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

2.3. Metode Analisis Data



Gambar 2. Metode Analsis Data

Pada gambar 2 menjelaskan metode yang digunakan peneliti dalam menganalisis data, tahapan-tahapan yang dimulai dari *Risk Assesment* sampai *Risk Treatment*, dengan cara-cara yang digunakan agar penelitian berjalan dengan baik antara lain memperhitungkan *scope, context*, dan *criteria* dari risiko, lalu melakukan konsultasi dan komunikasi dengan pihak terkait, kemudian melihat *track record* sera *reporting*. Dan terakhir melakukan *monitoring* dan *review*[12]. Seperti pada gambar 1, tahapan pertama adalah *Risk Assesment* (Penilaian Risiko). Penilaian risiko merupakan metode yang sistematis dalam menentukan apakah dalam aplikasi *SmartConsole* di Toko Surabaya Cabang Surakarta memiliki risiko yang dapat diterima atau tidak. Dalam Penilaian Risiko ini terdiri dari beberapa tahapan.

1. *Risk Identification* (Identifikasi Risiko)
   Merupakan usaha untuk mencari dan mengetahui risiko – risiko yang memiliki kemungkinan muncul dalam kegiatan – kegiatan yang dilakukan oleh perusahaan.
2. *Risk Analyst* (Analisis Risiko)
   Dalam metode analisis risiko ini meliputi daktor penilaian, karakterisasi, manajemen dan kebijakan yang berkaitan dengan risiko dalam perusahaan
3. *Risk Evaluation* (Evaluasi Risiko)
   Evaluasi risiko ini merupakan proses untuk membandingkan antara level risiko mulai dari risiko terendah hingga risiko yang paling tinggi yang ditemukan selama proses analisis. Dalam evaluasi ini bertujuan untuk membantu proses pengambilan risiko berdasarkan hasil analisis risiko.

Pada tahapan selanjutnya yaitu *Risk Treatment* (Perlakuan Risiko) dalam tahapan ini melibatkan pemilihan satu atau lebih pilihan untuk menanggulangi risiko dan

menerapkan penanganan risiko. Setelah diimplementasikan, penanganan risiko dapat dilakukan maupun dimodifikasi dalam kontrol penanganan risiko [13] Dalam proses ini melibatkan.

1. Menilai penanganan risiko
2. Memutuskan apakah tingkat risiko dapat ditoleransi atau tidak
3. Jika tidak dapat ditoleransi berarti akan menghasilkan penanganan risiko baru
4. Menilai efektivitas dari penanganan tersebut

3. HASIL DAN PEMBAHASAN

3.1. Penilaian Risiko

Pada tahap ini merupakan tahap penilaian risiko di Toko Surabaya Cabang Surakarta. Pada Proses penilaian risiko aplikasi *SmartConsole* ini terdiri dari 3 tahap yaitu : Identifikasi risiko (*risk identification*), analisis risiko (*risk analysis*), evaluasi risiko (*risk evaluation*).

3.2. Identifikasi Risiko

3.2.1. Identifikasi Aset

Pada tahap pertama, dilakukan identifikasi aset yang berhubungan dengan aplikasi *SmartConsole* seperti aset data, aset perangkat lunak (*Software*), dan aset perangkat keras (*Hardware*). Dan dalam identifikasi ini mewawancarai Pemilik Toko Surabaya dan Staff IT atau bagian yang mengurusi sistem *SmartConsole*. Pada tahap ini memfokuskan pada aset data, *software* dan *hardware*-nya.

Tabel 1. Identifikasi Aset

KOMPONEN SISTEM INFORMASI	ASET
DATA	Data barang, data *supplier*, data karyawan
SOFTWARE	Aplikasi *Smart Console*
HARDWARE	Personal computer, database server

Pada tabel 1 memperlihatkan aset dari komponen sistem informasi yang berupa data, *software,* dan *hardware* yang mendukung perkembangan aplikasi *SmartConsole*.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3.2.2 Identifikasi Kemungkinan Risiko

Setelah melakukan identifikasi aset yang menghasilkan informasi dari data, *software*, dan *hardware* yang berkaitan dengan aplikasi *SmartConsole*. Selanjutnya perlu dilakukan identifikasi kemungkinan risiko yang dapat menjadi ancaman bagi aplikasi *SmartConsole*. Kemungkinan risiko dapat dikelompokkan berdasarkan 3 faktor yaitu; faktor alam/lingkungan, faktor manusia dan faktor *system* dan infrastruktur. Yang bisa dilihat pada tabel 2. dibawah ini.

Tabel 2. Identifikasi Kemungkinan Risiko

FAKTOR	ID	KEMUNGKINAN RISIKO
ALAM	R001	Banjir
	R002	Gempa Bumi
	R003	Kebakaran
	R004	Petir
MANUSIA	R005	Human Error
	R006	Penyalahgunaan hak akses
	R007	Pencurian dan kebocoran data
	R008	Pencurian hardware
	R009	Hacking
	R010	User Interface yang sulit dipahami
	R011	*Vandalism*
	R012	Pegawai baru yang belum mengerti betul alur kerja sistem
SISTEM DAN INFRASTRUKTUR	R013	Koneksi jaringan yang buruk
	R014	Kerusakan hardware
	R015	Server down
	R016	Data korup
	R017	Overheat
	R018	Touble Backup
	R019	Sistem error
	R020	Listrik padam

Dari tahapan identifikasi risiko, ditemukan ada 20 kemungkinan – kemungkinan risiko yang berasal dari ketiga faktor tadi yaitu: alam/lingkungan, manusia, *system* dan infrastruktur.

3.2.3 Identifikasi Dampak Kemungkinan Risiko

Setelah mengetahui identifikasi dari kemungkinan risiko, pada tahap berikutnya melakukan identifikasi dampak risiko dari kemungkinan – kemungkinan risiko yang ada. Dapat dilihat pada tabel 3.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Tabel 3. Identifikasi Dampak Kemungkinan Risiko

FAKTOR	ID	KEMUNGKINAN RISIKO	DAMPAK
ALAM	R001	Banjir	kerusakan pada infrastruktur dan mengganggu jalannya proses bisnis
	R002	Gempa Bumi	mengganggu jalannya proses bisnis
	R003	Kebakaran	kerusakan pada infrastruktur dan mengganggu jalannya proses bisnis
	R004	Petir	kerusakan pada infrastruktur
MANUSIA	R005	Human Error	Data yang diinput tidak sesuai
	R006	Penyalahgunaan hak akses	Hak akses user dapat disalahgunakan
	R007	Pencurian dan kebocoran data	Data dapat disalahgunakan oleh pihak lain
	R008	Pencurian Hardware	Kerugian finansial
	R009	Hacking	Sistem dapat disadap dan mengalamii gangguan
	R010	User Interface yang sulit dipahami	User dapat mengalami kesulitan dalam memahami dan menjalankan sistem
	R011	*Vandalism* (merusak fasilitas seperti perangkat komputer)	Kerugian finansial dan menyebabkan perangkat menjadi rusak
	R012	Pegawai baru yang belum mengerti betul alur kerja sistem	Proses penyelesaian data tidak tepat waktu

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

FAKTOR	ID	KEMUNGKINAN RISIKO	DAMPAK
SISTEM DAN INFRASTRUKTUR	R013	Koneksi jaringan yang buruk	User akan kesulitan dalam mengakses sistem
	R014	Kerusakan hardware	Menghambat proses bisnis dan user akan kesulitan dalam mengakses sistem
	R015	Server down	Tidak dapat mengakses sistem dan database
	R016	Data korup	User tidak dapat melihat data yang valid
	R017	Overheat	Dapat menyebabkan kerusakan hardware karena suhu meningkat
	R018	Touble Backup	Dapat menyebabkan kehilangan data
	R019	Sistem error	User akan mengalami kesulitan dalam menjalankan sistem
	R020	Listrik padam	Aktivitas proses bisnis tidak dapat berjalan

Dari tabel 3 tentang identifikasi dampak kemungkinan risiko diatas maka dapat dilihat dampak yang ditimbulkan dari kemungkinan risiko yang terjadi.

3.2.4 Analisis Risiko

Selanjutnya masuk dalam tahap analisis risiko. Pada tahap ini dilakukan penilaian terhadap kemungkinan risiko pada tahap identifikasi risiko sebelumnya, dengan menggunakan tabel kriteria *Likelihood*. Pada tabel *Likehood* terdapat 5 kriteria yang berdasarkan frekuensi kejadian kemungkinan risiko terjadi.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Tabel 4. Kriteria *Likelihood*

LIKELIHOOD		**DESKRIPSI**	**FREKUENSI KEJADIAN**
NILAI	Kriteria		
1	Rare	Risiko tersebut hampir tidak pernah terjadi	>2 Tahun
2	Unlikely	Risiko tersebut jarang terjadi	1 – 2 Tahun
3	Possible	Risiko tersebut kadang terjadi	7 – 12 Bulan
4	Likely	Risiko tersebut sering terjadi	4 – 6 Bulan
5	Certain	Risiko tersebut pasti terjadi	1 – 3 Bulan

Kemudian pada tabel 5 dibawah ini merupakan tabel nilai *impact* atau dampak yang terjadi dari kemungkinan risiko di Toko Surabaya Cabang Surakarta. Pada tabel penilaian dampak ini dikelompokkan kedalam 5 kriteria dan dikelompokkan berdasarkan mulai dari dampak yang paling tidak berpengaruh sampai dampak yang paling berpengaruh.

Tabel 5. Kriteria Impact

IMPACT		**KETERANGAN**
NILAI	Kriteria	
1	Insignificant	Tidak mengganggu aktifitas
2	Minor	Aktifitas perusahaan sedikit terhambat
3	Moderate	Menyebabkan gangguan pada proses bisnis
4	Major	Menghambat hampir seluruh aktifitas
5	Catasirophic	Aktifitas perusahaan berhenti

Setelah mendapatkan kriteria kemungkinan (*Likelihood*) di tabel 4, dan kriteria dampak (*Impact*) di tabel 5. Maka selanjutnya penilaian terhadap kemungkinan risiko berdasarkan tabel 4 dan 5.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Tabel 6. Penilaian Likelihood dan Impact

FAKTOR	ID	KEMUNGKINAN RISIKO	LIKELIHOOD	IMPACT
ALAM	R001	Banjir	1	4
	R002	Gempa Bumi	2	2
	R003	Kebakaran	1	5
	R004	Petir	2	3
MANUSIA	R005	Human Error	4	3
	R006	Penyalahgunaan hak akses	2	2
	R007	Pencurian data	1	2
	R008	Pencurian hardware	1	3
	R009	Hacking	1	3
	R010	User Interface yang sulit dipahami	2	1
	R011	*Vandalism* (merusak fasilitas seperti perangkat komputer)	1	3
	R012	Pegawai baru yang belum mengerti betul alur kerja sistem	4	2
SISTEM DAN INFRASTRUKTUR	R013	Koneksi jaringan yang buruk	4	4
	R014	Kerusakan hardware	2	4
	R015	Server down	4	4
	R016	Data korup	1	4
	R017	Overhead	4	1

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

FAKTOR	ID	KEMUNGKINAN RISIKO	LIKELIHOOD	IMPACT
	R018	Touble Backup	1	2
	R019	Sistem error	3	4
	R020	Listrik padam	3	3

Dari tabel 6 diatas dapat menemukan nilai dari kemungkinan risiko yang ada pada tabel *Likelihood* dan *Impact*. Setelah menemukan nilai dari *Likelihood* dan *Impact*, kemudian masuk pada tahap evaluasi risiko.

3.3 Evaluasi Risiko

Pada tahapan terakhir yaitu evaluasi risiko akan dilakukan proses evaluasi risiko dari kemungkinan - kemungkinan risiko yang sudah di analisis pada tahapan sebelumnya. Dari hasil analisis tersebut akan dimasukkan ke dalam matrix evaluasi risiko berdasarkan pedoman yang ada di dalam kerangka kerja ISO 31000. Matrix evaluasi dibedakan menjadi 3 level risiko yaitu : *Low*, *Medium*, dan *High*.

Tabel 7. Matrix Evaluasi Risiko

Likelihood	Certain	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Possible	3	Low	Medium	Medium	Medium	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	rare	1	Low	Low	Low	Medium	Medium
	Impact		1	2	3	4	5
			Insigficant	Minor	Moderate	Major	Catastrophic

Pada tabel 7 menjelaskan tentang rasio pengelompokan berdasarkan level risiko dari yang tertinggi (*high*), hingga terendah (*low*). Tahap selanjutnya yaitu memasukkan setiap identitas kemungkinan risiko kedalam matrix evaluasi risiko sesuai dengan kriteria *Likelihood* dan kriteria *Impact*.

Journal of Information Systems and Informatics
Vol. 3, No. 1, March 2021
p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Tabel 8. Matrix Evaluasi Risiko Berdasarkan *Likelihood* dan *Impact*

Likelihood							
	Certain	5					
	Likely	4	R017	R012	R005	R013 R015	
	Possible	3			R020	R019	
	Unlikely	2	R010	R002 R006	R004	R014	
	rare	1		R007 R018	R008 R009 R011	R001 R016	R003
	Impact		1	2	3	4	5
			Insigficant	Minor	Moderate	Major	Catastrophic

Berdasarkan *Likelihood* dan *Impact* beberapa kemungkinan risiko dapat dikategorikan dengan rasio yang sesuai seperti pada tabel 8. Setelah memasukan kemungkinan risiko ke dalam matrix evaluasi berdasarkan *Likelihood* dan *Impact*, pada tahapan berikutnya akan di dikelompokkan 20 kemungkinan risiko diatas kedalam tingkatan level *high*, *medium* dan *low*.

Tabel 9. Pengelompokkan Risiko Berdasarkan Tingkatan

ID	Kemungkinan Risiko	Likehood	Impact	Risk Level
R013	Koneksi jaringan yang buruk	4	4	High
R015	Server down	4	4	High
R001	Banjir	1	4	Medium
R003	Kebakaran	1	5	Medium
R004	Petir	2	3	Medium
R005	Human Error	4	3	Medium
R012	Pegawai baru yang belum mengerti betul alur kerja sistem	4	2	Medium
R014	Kerusakan hardware	2	4	Medium
R016	Data korup	1	4	Medium
R017	Overhead	4	1	Medium
R019	Sistem error	3	4	Medium
R020	Listrik padam	3	3	Medium
R002	Gempa Bumi	2	2	Low

R006	Penyalahgunaan hak akses	2	2	Low
R007	Pencurian data	1	2	Low
R008	Pencurian hardware	1	3	Low
R009	Hacking	1	3	Low
R010	User Interface yang sulit dipahami	2	1	Low
R011	*Vandalism* (merusak fasilitas seperti perangkat komputer)	1	3	Low
R018	Touble Backup	1	2	Low

Dalam tabel 9 tahapan proses evaluasi risiko diatas, terdapat 20 kemungkinan risiko yang sudah di analisis serta di kelompokkan berdasarkan level risikonya. Terdapat 2 kemungkinan risiko yang dikategorikan ke dalam level risiko dengan tingkatan *high*, yaitu: R013 dan R015. Kemudian terdapat 10 kemungkinan risiko yang dikategorikan ke dalam level risiko tingkatan *medium*, yaitu: R001, R003, R004, R005, R012, R014, R016, R017, R019 dan R020. Dan juga terdapat 8 kemungkinan risiko yang dikategorikan kedalam level risiko tingkatan *low*, yaitu: R002, R006, R007, R008, R009, R010, R011, dan R018.

3.4 Perlakuan Risiko

Setelah melakukan proses identifikasi risiko mengenai asset yang berada dalam lingkungan aplikasi SmartConsole, maka selanjutnya akan dilakukan tahap *Risk Treatment* atau perlakuan risiko. Dalam tahap ini memberikan tindakan risiko terhadap kemungkinan risiko yang sudah di kelompokkan berdasarkan *risk level* pada tabel 9. Dalam tabel 10 ini diharapkan dapat meminimalisir kemungkinan risiko yang dapat terjadi bagi aplikasi SmartConsole yang dimiliki Toko Surabaya.

Tabel 10. Usulan Perlakuan Risiko

ID	Kemungkinan Risiko	Risk Level	Tindakan Risiko
R013	Koneksi jaringan yang buruk	High	Mengganti dengan ISP (Internet Service Proider) yang baru
R015	Server down	High	Melakukan pengecekan berskala pada database
R001	Banjir	Medium	Meletakkan alat alat infrastruktur di tempat yang aman dari banjir
R003	Kebakaran	Medium	Menyiapkan alat pemadam kebakaran
R004	Petir	Medium	Memasang alat penangkal petir
R005	Human Error	Medium	Melakukan training kepada user

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

ID	Kemungkinan Risiko	Risk Level	Tindakan Risiko
R012	Pegawai baru yang belum mengerti betul alur kerja sistem	Medium	Membuat SOP kerja sistem dan melakukan training kepada pegawai baru
R014	Kerusakan hardware	Medium	Memberikan asuransi terhadap aset hardware yang ada
R016	Data korup	Medium	Melakukan backup secara berkala
R017	Overheat	Medium	Menyediakan ruang yang memiliki AC (Air Conditioner) dan menambah fan pada semua hardware
R019	Sistem error	Medium	Menambah bandwidth, melakukan pembaharuan sistem, dan melakukan update antivirus.
R020	Listrik padam	Medium	Menyediakan generator set listrik dengan daya yang sesuai dengan kebutuhan. Kemudian menyiapkan Uninterruptible Power Supply (UPS)
R002	Gempa Bumi	Low	Menyediakan tempat yang cukup aman untuk menempatkan perangkat-perangkat
R006	Penyalahgunaan hak akses	Low	Memberikan batasan akses pada setiap device
R007	Pencurian data	Low	Memasang CCTV, alarm, dan alat sensor di setiap ruangan
R008	Pencurian hardware	Low	Memasang CCTV, alarm, dan alat sensor di setiap ruangan
R009	Hacking	Low	Menggunakan jaringan private dan meningkatkan keamanan sistemnya
R010	User Interface yang sulit dipahami	Low	Mengubah tampilan user interface agar lebih simple dan fungsional
R011	*Vandalism* (merusak fasilitas seperti perangkat komputer)	Low	Memberikan peringatan ganti rugi kepada setiap user
R018	Touble Backup	Low	Membuat SOP backup dan melakukan backup secara berskala.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Pada tabel 10 mendapatkan tindakan yang perlu dilakukan Toko Surabaya untuk meminimalisir risiko yang ada pada Toko Surabaya sesuai dengan rasio lategori *Likelihood* dan *Impact*-nya.

4 KESIMPULAN

Berdasarkan penelitian analisis risiko SI/TI menggunakan ISO 31000:2018 pada aplikasi *SmartConsole* yang dimiliki Toko Surabaya mulai dari tahapan penilaian risiko, identifikasi risiko, analisis risiko, evaluasi risiko, hingga tahap perlakukan risiko. Dari tahapan - tahapan tersebut, analisis risiko ini mendapatkan 20 kemungkinan risiko yang dapat sewaktu-waktu bisa menganggu kinerja dari aplikasi SmartConsole maupun mengganggu proses bisnis yang terdapat di Toko Surabaya Cabang Surakarta. Terdapat 2 kemungkinan risiko dengan tingkat *High* meliputi koneksi jaringan yang buruk dan server down. Kemudian terdapat 10 kemungkinan risiko dengan tingkat *Medium* meliputi banjir, kebakaran, petir, *human error*, pegawai baru yang belum mengerti alur kerja sistem, kerusakan *hardware*, data korup, *overheat*, sistem error, dan listrik padam. Kemudian juga terdapat 8 kemungkinan risiko dengan tingkat *Low* yang meliputi gempa bumi, penyalahgunaan hak akses, pencurian data, pencurian hardware, *hacking*, *user interface* yang sulit dipahami, *vandalism*, serta *trouble backup*.

Setelah penelitian ini dilakukan, diharapkan penelitian ini dapat digunakan Toko Surabaya Cabang Surakarta sebagai pedoman atau kebijakan untuk meminimalisir kemungkinan - kemungkinan risiko yang dapat terjadi dengan menggunakan usulan tindakan risiko yang sudah tersedia dalam tabel 10 seperti melakukan pengecekan berskala pada database, menggunakan ISP terbaru, membuat SOP, memasang CCTV. Terutama pada kemungkinan risiko dengan tingkat *High*, supaya tidak menganggu sistem aplikasi SmartConsole.

DAFTAR PUSTAKA

[1] A. R. Tampubolon and Suhardi, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 : 2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010," *J. Telemat.*, vol. 7, no. 2, pp. 1–10, 2011.

[2] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[3] D. E. Adi and N. Susanto, "Analisis Manajemen Risiko Aktivitas Pengadaan pada Percetakan Surat Kabar," *J. Metris*, vol. 18, pp. 113–118, 2017.

[4] I. Lanin, "Standar Baru Manajemen Risiko ISO 31000:2018," *IBFG Institute*, 2018. https://ibfgi.com/risk-management-31000/ (accessed Apr. 12, 2018).

[5] Angraini and I. D. Pertiwi, "Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 3, no. 2, pp. 70–76, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/4317.

[6] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.

[7] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)," *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6201–6208, 2015.

[8] F. L. Nice and R. V. Imbar, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," *J. Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 1–11, 2017.

[9] 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, doi: 10.29207/resti.v1i3.94.

[10] F. M. Hutabarat and A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, pp. 52–65, 2020, doi: 10.33557/binakomputer.v2i1.792.

[11] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.

[12] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech)," *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, 2020, doi: 10.33557/binakomputer.v2i1.799.

[13] M. Monica, didik Kurniawan, and R. Prabowo, "Analisis Manajemen Risiko Sistem Informasi Pengelolaaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan Metode ISO 31000," *J. Komputasi*, vol. 8, no. 1, pp. 83–90, 2020, doi: 10.23960/komputasi.v8i1.2351.