ANALISIS RISIKO TEKNOLOGI INFORMASI DI ORGANISASI XYZ CABANG SALATIGA MENGGUNAKAN ISO 31000

Sermon Paskah Zagoto[1], Melkior N.N. Sitokdana[2]
[1,2] Sistem Informasi S1 Universitas Kristen Satya Wacana
682017089@student.uksw.edu

ABSTRAK

Organisasi XYZ Cabang Salatiga merupakan organisasi yang bergerak di bidang jasa pengiriman barang. Organisasi tersebut telah menggunakan teknologi informasi untuk menunjang aktivitas bisnis. TIKI KU merupakan aplikasi yang digunakan untuk mendata setiap pengiriman barang yang dilakukan oleh konsumen mulai dari data pengirim barang, data barang, dan data penerima barang. Namun tidak dapat dipungkiri, setiap risiko yang terjadi dapat mengganggu kinerja aplikasi TIKI KU. Oleh karena itu diperlukan analisis risiko terhadap teknologi informasi yang digunakan. Pada penelitian ini, peneliti mencoba mengimplementasikan kerangka kerja manajemen risiko *ISO 31000* untuk melihat setiap kemungkinan risiko yang terdapat pada aplikasi TIKI KU. Hasil akhir dari penelitian ini diharapkan membantu organisasi dalam melihat serta mengetahui tindakan-tindakan apa saja yang harus dilakukan terhadap setiap kemungkinan risiko atau ancaman yang terjadi disekitar aplikasi TIKI KU berdasarkan level risikonya.

Keyword : *analisis risiko, ISO 31000, risiko teknologi informasi, manajemen risiko.*

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) dari tahun ke tahun semakin berkembang. Perkembangan tersebut disebabkan oleh semakin meningkatnya kebutuhan organisasi. Setiap komponen yang ada didalam teknologi informasi harus mampu berjalan dengan baik sesuai dengan tugas dan fungsinya masing-masing sehingga dapat membantu organisasi menjalankan proses bisnis serta tercapainya visi misi organisasi.

Organisasi XYZ merupakan organisasi yang bergerak dibidang jasa pengiriman barang dan telah berdiri sejak tahun 1970. Hingga saat ini, Organisasi XYZ telah memiliki 65 kantor cabang yang tersebar di kota-kota besar di Indonesia. Sejak berdirinya Organisasi XYZ Cabang Salatiga, kantor cabang tersebut telah menggunakan Sistem Informasi/Teknologi Informasi (SI/TI) untuk menjalankan proses bisnis organisasi. Salah satu aplikasi yang digunakan yaitu aplikasi TIKI KU. TIKI KU merupakan aplikasi yang digunakan untuk mendata pengiriman barang yang dilakukan oleh konsumen seperti data pengirim barang, data barang, dan data penerima barang. Namun tidak dapat dipungkiri, kemungkinan ancaman dan risiko yang muncul disekitar aplikasi bisa saja terjadi. Risiko atau ancaman bisa saja terjadi pada aplikasi TIKI KU, maka dampak yang dihasilkan dapat mengganggu bahkan menghentikan aktivitas bisnis organisasi. Oleh karena itu pentingnya mengetahui risiko yang bisa berdampak terhadap kinerja aplikasi TIKI KU. Manfaat dari audit manajemen risiko yaitu memberikan gambaran risiko-risiko yang dapat muncul dari berbagai faktor yang berdampak buruk terhadap kinerja teknologi informasi organisasi kepada pihak *stakeholder* sehingga dapat mengambil keputusan dalam mengantisipasi risiko-risiko yang bisa saja terjadi.

Salah satu *tools* berstandar internasional mengenai manajemen risiko yaitu *ISO 31000*. *ISO 31000* merupakan pedoman standar, instruksi, dan tuntutan bagi sebuah organisasi untuk membangun sebuah pondasi dan kerangka kerja bagi suatu program manajemen risiko. Tujuan dari standarisasi ini adalah menyediakan prinsip-prinsip dan acuan dari program manajemen risiko kepada organisasi.

Tujuan penelitian ini adalah untuk mengetahui kemungkinan risiko atau ancaman yang terjadi di aplikasi TIKI KU dan dampak terjadinya risiko terhadap aktivitas bisnis serta memberikan rekomendasi terhadap setiap dampak yang timbul.

2. TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian sebelumnya digunakan sebagai bahan referensi terhadap penelitian yang dilakukan saat ini. Terdapat beberapa penelitian tentang manajemen risiko atau analisis risiko menggunakan kerangka kerja *ISO 31000*, antara lain penelitian analisis risiko teknologi informasi F. Hutabarat dan A. Manuputty (2020) terhadap aplikasi VCare di PT. Visionet Data Internasional [1]. Penelitian tersebut dilakukan untuk melihat setiap kemungkinan risiko terhadap aplikasi VCare. Aplikasi tersebut digunakan untuk pendaftaran klien yang akan menggunakan layanan dari PT Visionet Data Internasional. Hasil akhir penelitian menghasilkan 20 kemungkinan risiko yang terbagi kedalam 4 kemungkinan risiko tergolong *High*, 8 kemungkinan risiko tergolong *Medium*, serta 8 kemungkinan risiko tergolong *Low* yang berpotensi menghambat kinerjasi aplikasi.

Selanjutnya penelitian analisis risiko teknologi informasi yang dilakukan oleh A. Rahmawati dan A. Wijaya (2019) di aplikasi *IT Operation Support (iTop)* pada PT. ABCD menghasilkan sebuah risiko teknologi informasi yang terdiri dari daftar dan

faktor sehingga dapat menyebabkan terjadinya risiko yang mengancam kinerka aplikasi iTop [2]. Faktor-faktor tesebut antara lain, alam/lingkungan, kesalahan yang disengaja oleh manusia, dan dari sistem itu sendiri.

Penelitian analisis risiko teknologi informasi menggunakan kerangka kerja *ISO 31000* juga dilakukan oleh S. Agustinus, A. Nugroho, dan A. Cahyano (2017) terhadap program HRMS. Program HRMS merupakan *database* pusat dari segala hal yang berkaitan dengan *Human Resources Development* dari PT. XYZ [3]. Penelitian tersebut bertujuan melakukan analisa risiko untuk mendapatkan dokumentasi terhadap berbagai macam kemungkinan risiko yang berada disekitar program HRMS. Dari penelitian yang dilakukan, ditemukan 26 kemungkinan risiko dan terbagi kedalam tiga level. Untuk level *High* terdapat 2 kemungkinan risiko, untuk level *Medium* terdapat 18 kemungkinan risiko, serta untuk level *Low* terdapat 6 kemungkinan risiko.

Penelitian terakhir yang digunakan sebagai bahan referensi terhadap penelitian yang dilakukan saat ini yaitu penelitian analisis risiko teknologi yang dilakukan oleh H. Driantami, Suprapto, dan A. Perdanakusuma (2018) di PT Matahari Department Store Cabang Malang Town Square menggunakan *ISO 31000* [4]. Tujuan penelitian tersebut yaitu untuk mengetahui risiko IT terhadap sistem penjualan Alphapos yang dimana sistem itu digunakan untuk membantu seluruh kegiatan baik *back office* maupun *front office*. Yang mana untuk metodologi penelitian dibantu dengan menggunakan NIST *800-300* untuk menentukan peringkat risiko yang dihasilkan dari sistem penjualan Alphapos dan menentukan rekomendasi pengendalian *cost-benefit analysis* untuk setiap risiko yang termasuk kedalam daftar prioritas risiko.

2.2 Landasan Teori

Teknologi informasi merupakan sekumpulan alat yang saling terhubung yang akan membantu manusia dalam melakukan pekerjaannya. Teknologi informasi meliputi perangkat keras (*hardware*) dan perangkat lunak (*software*). Teknologi informasi membantu manusia mulai dari mengolah data menjadi informasi yang berguna bagi pengguna sehingga bisa menghasilkan keputusan yang baik berdasarkan data dan informasi yang tepat.

Manajemen risiko adalah suatu proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mengelolanya menjadi sumber daya yang tersedia. Manajemen risiko bertujuan untuk mengelola risiko sehingga memperoleh hasil yang optimal [5].

Untuk mengetahui kemungkinan risiko, maka diperlukan proses identifikasi risiko pada aktivitas yang dilakukan oleh organisasi. Menurut D. Ramadhan, R. Febriansyah, dan R. Dewi (2020), identifikasi risiko adalah usaha untuk menemukan atau mengetahui risiko-risiko yang timbul yang ada di proses bisnis perusahaan [6]. Identifikasi risiko biasanya dilakukan di semua proses bisnis. Hal ini bertujuan untuk mengetahui semua risiko-risiko yang timbul yang mana berasal dari berbagai faktor.

Faktor-faktor yang dapat menimbulkan risiko bisa saja berasal dari alam, manusia, dan sistem/infrastruktur. Pertama faktor dari alam atau biasa disebut bencana alam. Faktor ini disebabkan oleh peristiwa alam seperti gempa bumi, *tsunami*, dan sebagainya. Kedua yaitu faktor dari manusia. Faktor ini disebabkan oleh adanya upaya merubah aplikasi/program secara sengaja. Hal ini dapat menimbulkan risiko seperti penyalahgunaan hak akses, *cybercrime*, pencirian data. Yang ketiga yaitu faktor dari sistem/infrastruktur. Faktor ini disebabkan oleh kegagalan saat sistem atau infrastruktur sedang berjalan.

Upaya untuk meminimalisir terjadinya risiko-risiko yang tidak diinginkan yaitu dengan menerapkan manajemen risiko pada organisasi. Tujuan dari manajemen risiko adalah mengurangi risiko yang mungkin terjadi (ancaman), mengukur dampak dari potensi ancaman, dan menentukan kerugian yang diderita akibat hilangnya potensi bisnis [7].

Pada tanggal 13 November 2009 *ISO 31000* standar internasional diterbitkan oleh *The International Organization for Standarization*. Standar tersebut dapat digunakan di segala jenis organisasi untuk menghadapi risiko yang berada pada aktivitas organisasi [4]. *ISO 31000* adalah panduan penerapan risiko yang terdiri atas tiga elemen yaitu prinsip (*principle*), kerangka kerja (*framework*), dan proses (*process*). Salah satu hal yang membedakan *ISO 31000* dengan standar manajemen risiko yang lain yaitu perspektif *ISO 31000* yang lebih luas dan lebih konseptual dibandingkan dengan yang lainnya. Hal ini ditandai dengan adanya kerangka kerja manajemen risiko yang merupakan implementasi prinsip manajemen mutu dan dikenal dengan "*Plan-Do-Chek-Action*" [4].

Dengan menggunakan kerangka kerja *ISO 31000*, maka kita dapat melakukan proses manajemen risiko di suatu organisasi. Kemudian membantu organisasi untuk meminimalisir kemungkinan risiko yang dapat ditimbulkan. Dengan begitu aktivitas bisnis organisasi dapat terus berjalan.

3. METODE PENELITIAN

3.1 Metode Penelitian

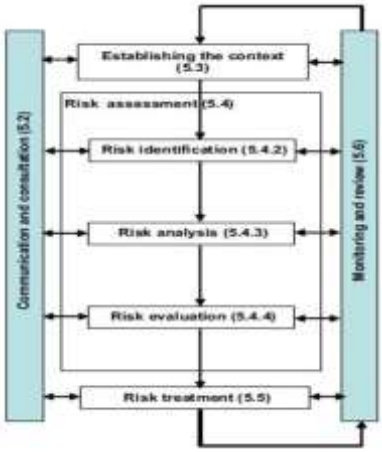
Metode penelitian yang akan digunakan penulis yaitu metode penelitian kualitatif. Menurut Zainal. A. Hasibuan, Ph.D (2007), penelitian kualitatif adalah penelitian yang bermaksud untuk memahami fenomena tentang apa yang akan dialami oleh subjek penelitian misalnya perilaku, persepsi, motivasi, tindakan, dan lain-lain, secara holistik dan

deskripsi kata-kata dan bahasa, pada suatu konteks khusus yang alamiah dan dengan memanfaatkan berbagai metode alamiah [8]. Salah satu jenus penelitian kualitatif adalah berupa penelitian dengan metode atau pendakatan studi kasus (*case study*). Metode tersebut berfokus terhadap satu objek dengan menggunakan individu atau kelompok sebagai bahan studinya. Dengan metode ini, peneliti dengan mudah mengumpulkan data untuk menjawab permasalahan yang terjadi. Data yang digunakan dalam penelitian ini berupa data primer yang bersumber dari hasil wawancara bersama narasumber. Data yang didapatkan juga sudah diverifikasi dan divalidasi oleh narasumber. Sumber data diluar data primer tidak dapat digunakan karena tergolong kedalam data tersier [8].

3.2 Metode Pengambilan Data

Metode pengambilan data untuk penelitian ini yaitu dengan melakukan wawancara terhadap dua narasumber. Narasumber pertama yaitu *Sales Counter* yang bertugas mengisi data barang dari konsumen ke dalam aplikasi TIKI KU. Narasumber kedua yaitu Koordinatir TI yang bertugas menangani masalah pada saat aplikasi TIKI KU mengalami gangguan. Kedua narasumber tersebut sebagai sumber internal dari penelitian.

3.3 Metode Analisis Data



Gambar 1. *Risk Management – Principles and Guidelines* [9]

Penelitian ini menggunakan *International Organization for Standarization (ISO 31000)*. Pada gambar diatas, terdapat 2 tahapan besar yaitu *risk assessment* (penilaian risiko) dan *risk treatment* (perlakuan risiko).

Tahap pertama yaitu tahap *risk assessment* (penilaian risiko). Pada tahap penilaian risiko, terdapat 3 proses yang dilakukan yaitu identifikasi risiko, analisis risiko, dan terakhir evaluasi risiko. *Risk Identification* (identifikasi risiko) adalah usaha untuk menemukan risiko-risiko yang timbul yang ada di proses bisnis perusahaan. Identifikasi risiko biasanya dilakukan di semua proses bisnis. Hal ini bertujuan untuk mengetahui semua risiko yang timbul yang mana berasal dari berbagai faktor [6]. *Risk analysis* (analisis risiko) yaitu proses melihat dampak/kerusakan yang ditimbulkan oleh risiko-risiko sehingga menghambat jalannya proses bisnis. *Risk evaluation* (evaluas risiko) dilakukan untuk menentukan manajemen risiko dengan membandingkan tingkat risiko terhadap standar yang telah ditetapkan. Tujuannya yaitu untuk mengetahui tingkat prioritas tinggi hingga rendah dan mengetahui tingkat risiko mana yang harus ditindaklanjuti dan mana yang dipantau [10].

Tahap kedua yaitu tahap *risk treatment* (perlakuan risiko). Tahap ini dilakukan untuk menyeleksi kemungkinan-kemungkinan risiko, mengurangi bahkan menghilangkan dampak serta kemungkinan terjadinya risiko yang akan muncul [5].

4. HASIL DAN PEMBAHASAN

4.1 Penilaian Risiko

Tahap ini merupakan tahap penilaian risiko terhadap aplikasi TIKI KU yang terdiri dari identifikasi risiko, analisis risiko, dan evaluasi risiko.

4.1.1 Identifikasi Risiko

a) Identifikasi Aset

Pada tahap ini dilakukan identifikasi aset yang terdapat pada aplikasi TIKI KU mulai dari identifikasi aset data, perangkat lunak (*software*) dan perangkat keras (*hardware*). Proses identifikasi aset dilakukan dengan melakukan wawancara terhadap *Sales Counter* dan Koordinator TI.

Tabel 1. Identifikasi Aset

Komponen Sistem Informasi	Aset TIKI KU
Data	Data User, Data Pengirim, Data Barang, Data Penerima
Software	TIKI KU
Hardware	*Personal Computer* (PC), *Server Database*

Sumber: Hasil Analisis Uji Coba Penelitian

Dari hasil analisis yang dilakukan untuk mengidentifikasi aset, didapatkan tiga komponen sistem informasi atau tiga aset. Pertama aset Data dengan isi data user, data pengirim barang, data barang, dan data penerima barang. Kedua aset perangkat lunak (*software*) yaitu TIKI KU. Aplikasi TIKI KU merupakan aplikasi yang digunakan untuk mendata setiap pengiriman barang yang dilakukan oleh konsumen. Aplikasi tersebut berjalan di atas *Operating System* (*OS*) Windows. Ketiga aset perangkat keras (*hardware*) yaitu *Personal Computer* (*PC*) dan *Server Database*. Setiap *Personal Computer* (*PC*) memiliki jumlah *Random*

Acces Memory (*RAM*) sebesar 2GB dan Server Database juga memiliki jumlah RAM sebesar 8GB.

b) Identifikasi Kemungkinan Risiko

Setelah identifikasi aset terhadap aplikasi TIKI KU, maka selanjutnya identifikasi kemungkinan risiko yang ada disekitar aplikasi. Identifikasi kemungkinan risiko terbagi kedalam 3 faktor.

Tabel 2. Identifikasi Kemungkinan Risiko

Faktor	ID	Kemungkinan Risiko
Alam	R001	Gempa Bumi
	R002	*Tsunami*
	R003	Banjir
	R004	Petir
	R005	Kebakaran
Manusia	R006	*Human Error*
	R007	Penyalahgunaan Hak Ases
	R008	User Interface sulit dipahami
	R009	*Hacking* terhadap jaringan
	R010	Pencurian Data
Sistem	R011	Listrik Padam
	R012	*Server Down*
	R013	Koneksi internet tiba-tiba putus
	R014	Data korup
	R015	*Web Server* bermasalah
	R016	Memori penuh
	R017	*Overheat*
	R018	Kerusakan *hardware*
	R019	*Backup failure*
	R020	Tidak adanya sistem *Automatic Logout System*

Sumber: Hasil Analisis Uji Coba Penelitian

Dari hasil identifikasi kemungkinan risiko, ditemukan 20 kemungkinan risiko atau ancaman yang berasal dari faktor alam, manusia, dan sistem.

c) Identifikasi Dampak Kemungkinan Risiko

Setelah mengidentifikasi kemungkinan risiko, selanjutnya menentukan dampak dari setiap kemungkinan risiko yang sudah diidentifikasi.

Tabel 3. Dampak Kemungkinan Risiko

ID	Kemungkinan Risiko	Dampak
R001	Gempa Bumi	Kerusakan terhadap infrastruktur dan aktivitas bisnis berhenti.
R002	*Tsunami*	Kerusakan terhadap infrastruktur dan aktivitas bisnis berhenti.
R003	Banjir	Aktivitas pengiriman barang tergganggu.
R004	Petir	Aktivitas pengiriman barang tergganggu.
R005	Kebakaran	Proses layanan pengiriman barang terganggu.
R006	*Human Error*	Data yang diinputkan tidak *valid*.
R007	Penyalahgunaan Hak Ases	Hak akses *user* disalahgunakan.
R008	User Interface sulit dipahami	*User* tidak memahami penggunaa aplikasi TIKI KU.
R009	*Hacking* terhadap jaringan	Aplikasi TIKI KU akan mengalami gangguan.
R010	Pencurian Data	Data klien dan data informasi barang akan disalahgunakan.
R011	Listrik Padam	Tidak berpengaruh karena Organisasi XYZ Cabang Salatiga memiliki cadangan listrik.
R012	*Server Down*	Aplikasi TIKI KU dan *database* tidak bisa diakses.
R013	Koneksi internet tiba-tiba putus	Tidak dapat mengakses aplikasi TIKI KU.
R014	Data korup	Data pengirim, data barang, dan data penerima rusak.
R015	*Web Server* bermasalah	Tidak bisa akses ke aplikasi TIKI KU.
R016	Memori penuh	Data baru tidak dapat masuk ke aplikasi TIKI KU.
R017	*Overheat*	Kerusakan pada *hardware* karena suhu meningkat dan akses ke *database* terganggu.
R018	Kerusakan *hardware*	Menghambat aktivitas penginputan data barang karena harus melakukan konfigurasi ke *hardware* baru.
R019	*Backup failure*	Data pengirimbarang dan data barang hilang.
R020	Tidak adanya sistem *Automatic Logout System*	*User* meninggalkan akses aplikasi TIKI KU dalam keadaaan *login* sehingga pengguna selain *user* menggunakan aplikasi TIKI KU secara bebas dan berpotensi terjadinya pencurian data.

Sumber: Hasil Analisis Uji Coba Penelitian

4.1.2 Analisis Risiko

Kemudian tahap selanjutnya yaitu analisis risiko. Pada tahap ini dilakukan penilaian terhadap kemungkinan risiko yang sudah diidentifikasi sebelumnya. Tabel 4 merupakan tabel kriteria *likelohood*. Dalam penelaian *likelihood* dibedakan kedalam 5 kriteria dengan kriteria laninya memiliki frekuensi kejadian yang berbeda.

Tabel 4. Kriteria Likelihood [2]

Likelihood		**Deskripsi**	**Frekuensi Kejadian**
Nilai	**Kriteria**		
1	*Rare*	Risiko hampir tidak pernah terjadi	>2 tahun
2	*Unlikely*	Risiko jarang terjadi	1-2 tahun
3	*Posibble*	Risiko kadang terjadi	7-12 bulan
4	*Likely*	Risiko sering terjadi	4-6 bulan
5	*Certain*	Risiko pasti terjadi	1-3 bulan

Tabel 5 merupakan tabel nilai *impact* atau dampak jika kemungkinan risiko terjadi di Organisasi XYZ Cabang Salatiga. Tabel penilaian dampak dibedakan kedalam 5 kriteria dan dikelompokkan mulai dari dampak yang paling tidak berpengaruh sampai dampak yang paling berpengaruh.

Tabel 5. Kriteria Impact [2]

Impact		**Deskripsi**
Nilai	**Kriteria**	
1	Insignificant	Tidak mengganggu aktivitas bisnis perusahaan
2	Minor	Aktivitas perusahaan sedikit terhambat namun aktivitas utama tidak tergganggu
3	Moderate	Menghambat proses bisnis sehingga sebagian aktivitas terganggu
4	Major	Menghambat hampir seluruh aktivitas perusahaan
5	Catastrophic	Aktivitas perusahaan terhenti karena aktivitas bisnis mengalami gangguan total

Selanjutnya dilakukan penilaian terhadap kemungkinan risiko berdasarkan tabel 4 dan tabel 5.

Tabel 6. Penilaian Likelihood dan Impact

Faktor	**ID**	**Kemungkinan Risiko**	**Likelihood**	**Impact**
Alam	R001	Gempa Bumi	3	5
	R002	*Tsunami*	1	5
	R003	Banjir	2	4
	R004	Petir	3	4
	R005	Kebakaran	1	5
Manusia	R006	*Human Error*	3	3
	R007	Penyalahgunaan Hak Ases	2	3
	R008	User Interface sulit dipahami	4	4
	R009	*Hacking* terhadap jaringan	1	4
	R010	Pencurian Data	1	4
Sistem	R011	Listrik Padam	3	3
	R012	*Server Down*	4	4
	R013	Koneksi internet tiba-tiba putus	4	4
	R014	Data korup	1	3
	R015	*Web Server* bermasalah	4	3
	R016	Memori penuh	2	2
	R017	*Overheat*	1	1
	R018	Kerusakan *hardware*	1	2
	R019	*Backup failure*	2	1
	R020	Tidak adanya sistem *Automatic Logout System*	2	1

Sumber: Hasil Analisis Uji Coba Penelitian

4.1.3 Evaluasi Risiko

Tahap terakhir yaitu tahap evaluasi risiko. Tahap ini menggunakan acuan berupa matrix evaluasi risiko, dimana dilakukan pemetaan terhadap level risiko berdasarkan penilaian terhadap kemungkinan risiko dan ancaman di sekitar aplikasi TIKI KU.

Tabel 7. Matrix Evaluasi Risiko [1]

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
	Impact	**1**	Low	Low	Low	Medium	Medium
Impact			**1**	**2**	**3**	**4**	**5**
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**

Pada tabel matrix evaluasi risiko diatas terdapat tiga warna yaitu Merah, Kuning, dan Hijau. Warna Merah diartikan sebagai level risiko *High*, yang artinya kemungkinan risiko tersebut sering terjadi dan memiliki dampak besar terdapat aktivitas bisnis organisasi. Untuk warna Kuning diartikan sebagai level risiko *Medium*, yang artinya kemungkinan risiko tersebut jarang terjadi dan memiliki dampak sedikit terhadap aktivitas bisnis organisasi. Sedangkan untuk warna Hijau diartikan sebagai level risiko *Low*, yang artinya kemungkinan risiko tesebut hampir tidak pernah terjadi dan tidak memiliki dampak sama sekali terhadap aktivitas bisnis organisasi.

Tahap selanjutnya yaitu mengevaluasi risiko berdasarkan identitas kemungkinan risiko kedalam parameter sesuai dengan kriteria *Likelihood* dan kriteria *Impact*.

Tabel 8. Matrix Evaluasi Risiko Berdasarkan Likelihood dan Impact

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

Sumber: Hasil Analisis Uji Coba Penelitian

Setelah kemungkinan risiko telah dimasukkan kedalam matrix evaluasi risiko, maka selanjutnya mengelompokkan 20 kemungkinan risiko berdasarkan tingkatan level mulai dari *High*, *Medium*, dan *Low*.

Tabel 9. Pengelompokkan Risiko Berdasarkan Tingkatan

ID	Kemungkinan Risiko	Likelihood	Impact	Risk Level
R001	Gempa Bumi	3	5	High
R008	*User Interface* sulit dipahami	4	4	High
R012	*Server down*	4	4	High
R013	Koneksi internet tiba-tiba terputus	4	4	High
R002	Tsunami	1	5	Medium
R005	Kebakaran	1	5	Medium
R004	Petir	3	4	Medium
R003	Banjir	2	4	Medium
R009	*Hacking* terhadap jaringan	1	4	Medium
R010	Pencurian data	1	4	Medium
R015	*Web Server* bermasalah	4	3	Medium
R006	Human Error	3	3	Medium
R007	Penyalahgunaan hak akses	2	3	Medium
R011	Listrik Padam	3	3	Medium
R020	Tidak adanya *Automatic Logout System*	5	1	Medium
R014	Data korup	1	3	Low
R016	Memori penuh	2	2	Low
R018	Kerusakan *hardware*	1	2	Low
R019	*Backup failure*	2	1	Low
R017	*Overheat*	1	1	Low

Sumber: Hasil Analisis Uji Coba Penelitian

Dari hasil proses evaluasi risiko, terlihat pada tabel 9 terdapat 20 kemungkinan risiko yang sudah dianalisa dan diurutkan berdasarkan level risikonya.

Terdapat 4 kemungkinan risiko tergolong *High* mulai dari gempa bumi, *user inteface* sulit dipahami, *server down*, serta koneksi internet tiba-tiba terputus. 11 kemungkinan risiko tergolong *Medium* seperti *tsunami*, kebakaran, petir, banjir, *hacking* terhadap jaringan, pencurian data, *web server* bermasalah, *human error*, penyalahgunaan hak akses, listrik mati, dan tidak adanya *automatic logout system*. Dan terakhir 5 kemungkinan risiko tergolong *Low* mulai dari data korup, kerusakan *hardware*, *backup failure*, dan *overheat*.

4.2 Perlakuan Risiko

Setelah melalui tahap identifikasi risiko, maka tahap terakhir yaitu tahap perlakukan risiko. Pada tahap ini, diberikan usulan tindakan risiko untuk setiap kemungkinan risiko. Dengan adanya usulan tindakan risiko, diharapkan dapat mengurangi atau meminimaliris setiap kemungkinan-kemungkinan risiko yang terjadi disekitar aplikasi TIKI KU.

Tabel 10. Usulan Perlakuan Risiko

ID	Kemungkinan Risiko	Risk Level	Tindakan Risiko
R001	Gempa Bumi	*High*	Menyediakan cadangan server ditempat yang aman
R008	*User Interface* sulit dipahami	*High*	Menyediakan buku panduan tentang penggunaan aplikasi TIKI KU kepada setiap karyawan. Memberikan pelatihan dan petunjuk penggunaan aplikasi TIKI KU kepada *user*.
R012	*Server down*	*High*	Melakukan pengecekan secara berkala terhadap *dblog*, *temp dblog*, *CPU usage*, dan *RAM usage* pada *server*
R013	Koneksi internet tiba-tiba terputus	*High*	Segera melaporkan ke pihak *Internet Service Provider* (*ISP*)
R002	Tsunami	*Medium*	Menyediakan cadangan server dilokasi yang berbeda dan memindahkan aset kantor yaitu *hardware* ke tempat yang lebih tinggi
R005	Kebakaran	*Medium*	Menyediakan alat pemadam kebakaran agar tidak terjadi kerusakan pada *hardware*
R004	Petir	*Medium*	Memasang alat penangkal petir di gedung
R003	Banjir	*Medium*	Menyediakan cadangan server dilokasi yang berbeda dan memindahkan aset kantor yaitu *hardware* ke tempat yang lebih tinggi
R009	*Hacking* terhadap jaringan	*Medium*	Menggunakan jaringan *private* agar sulit diretas
R010	Pencurian data	*Medium*	Memasang alat *CCTV* disetiap ruangan
R015	*Web Server* bermasalah	*Medium*	Memberitahu kepada *user* bahwa akses ke aplikasi TIKI KU akan gagal. Memperbaiki *web server* agar kembali normal.
R006	*Human Error*	*Medium*	Melakukan pelatihan kepada karyawan/calon karyawan dalam menggunakan aplikasi TIKI KU
R007	Penyalahgunaan hak akses	*Medium*	Memberi konfirmasi *login* saat *user login* ke aplikasi TIKI KU
R011	Listrik Padam	*Medium*	Menyediakan *generator set* dan UPS (*Uninterruptible Power Supply*) dengan daya yang disesuaikan dengan kondisi organisasi
R020	Tidak adanya *Automatic Logout System*	*Medium*	Membuat sistem *automatic logout system*, agar ketika *user login* ke aplikasi TIKI KU dan lupa untuk *logout*, maka sistem otomatis akan *logout*. Hal ini perlu dilakukan untuk menghindari orang-orang yang tidak memiliki hak akses terhadap aplikasi TIKI KU.
R014	Data korup	*Low*	Melakukan *backup data* terhadap aplikasi TIKI KU.

			Selalu memperhatikan file yang telah di *download*/unduh dari internet. Hal ini diperlukan untuk melihat apalah file yang telah di undah merupakan virus atau bukan sehingga menegah kehilangan dan kerusakan data.
R016	Memori penuh	*Low*	Memperhatikan penggunaan memori penyimpanan pada *database* secara berkala agar jangan sampai penuh
R018	Kerusakan *hardware*	*Low*	Melakukan perawatan dan memberikan asuransi terhadap aset *hardware* yang dimiliki
R019	*Backup failure*	*Low*	Melakukan pengecekan secara berkalan. Melakukan *backup data* yang terdapat pada aplikasi TIKI KU.
R017	*Overheat*	*Low*	Menyediakan AC (air conditioner) pada ruangan agar suhu tetap stabil

Sumber: Hasil Analisis Uji Coba Penelitian

5. KESIMPULAN

Berdasarkan dari peneltian yang sudah dilakukan, analisis risiko teknologi informasi aplikasi TIKI KU di Organisasi XYZ Cabang Salatiga dijalankan melalui dua tahapan besar. Tahap pertama yaitu tahap penilaian risiko meliputi identifikasi risiko, analisis risiko, dan evaluasi risiko. Dan tahap kedua yaitu tahap perlakuan risiko.

Dari hasil penelitian yang telah dilakukan, terdapat 4 kemungkinan risiko dengan level risiko *High*, 11 kemungkinan risiko dengan level risiko *Medium*, dan 5 kemungkinan risiko dengan level risiko *Low*. Level risiko *High* merupakan level risiko yang pasti terjadi dan memiliki dampak langsung terhadap aktivitas bisnis organisasi. Untuk itu perlu dilakukan tindakan risiko untuk meminimalisir hal tesebut. Solusi yang dilakukan yaitu dengan menyediakan *server* cadangan jika terjadi gempa bumi, menyediakan buku panduan penggunaan aplikasi TIKI KU kepada karyawan, melakukan pengecekan secara berkala terhadap *server* untuk menghindari *server down*, serta melaporkan kepada ISP jika koneksi internet tiba-tiba terputus.

Setelah dilakukan penelitian ini, diharapkan setiap kemungkinan-kemungkinan risiko yang terjadi di sekitar aplikasi TIKI KU dapat diminimalisir agar aktivitas Organisasi XYZ Cabang Salatiga dapat terus berjalan.

DAFTAR PUSTAKA

[1] 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.

[2] A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP," *J. SITECH Sist. Inf. dan Teknol.*, vol. 2, no. 1, pp. 13–20, 2019, doi: 10.24176/sitech.v2i1.3122.

[3] 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.

[4] 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.

[5] 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.

[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] Z. A. Hasibuan, "Metodologi Penelitian Pada Bidang Ilmu Komputer Dan Teknologi Informasi," *Konsep, Tek. Dan Apl.*, no. Universitas Indonesia, p. 194, 2007.

[9] ISO 31000, "International Organization for Standardization ISO 31000: Risk management - Principles and guidelines," vol. 2009, p. 36, 2009.

[10] 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, doi: 1410-3737.