JURNAL SISTEM INFORMASI DAN TENOLOGI

http://www.jurnal.umk.ac.id/sitech

ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI ITOP

Aprilia Rahmawati[1], **Agustinus Fritz Wijaya**[2]

[1,2] Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga

Article Info:
Dikirim: 15 Maret 2019
Direvisi: 04 April 2019
Diterima: 04 Mei 2019
Tersedia Online: 29 Juni 2019

Penulis Korespondensi:
Aprilia Rahmawati
Fakultas Teknologi Informasi,
Universitas Kristen Satya Wacana,
Salatiga, Indonesia
Email:
aprilia_rahmawati@outlook.co.id

Abstrak: *Aplikasi IT Operation Support (iTop) merupakan support system yang membantu PT. ABCD menerima customer incident. Keberadaan aplikasi iTop ini membantu perusahaan untuk mengetahui kualitas layanan kepada customer. Kualitas layanan customer ditentukkan oleh aplikasi ini sehingga dibutuhkan analisis risiko untuk mencegah risiko yang mungkin terjadi. Analisis risiko dengan menggunakan ISO 31000 pada PT. ABCD diharapkan dapat meminimalisir kemungkinan-kemungkinan risiko di sekitar aplikasi iTop. Hasil analisis risiko dengan ISO 31000 berupa dokumentasi kemungkinan risiko yang ada di sekitar aplikasi iTop, prioritas risiko dari tiap kemungkinan risiko yang telah diidentifikasi serta penanganan dari kemungkinan-kemungkinan risiko yang ada. Sehingga hasil analisis risiko ini dapat digunakan untuk membantu perusahaan mencegah, meminimalisir risiko serta memperlakukan risiko tersebut sesuai prioritasnya sebelum kemungkinan risiko-risiko tersebut menghambat kinerja perusahaan.*

Kata kunci: *manajemen analisis risiko; ISO 31000; IT operation support (iTop).*

Abstract: *iTop application is a support system that help PT. ABCD to receive customer incident. The exixtence of iTop application is help company to know their service quality to customer. Their customer service quality decided by this application that needed risk analysis to prevent possible risk that maybe happened. A risk analysis using ISO 31000 to PT. ABCD expected can minimize the emergence of the possible risk. The result of risk analysis using ISO 31000 is documentation of possible risk around iTop application, risk priority of the possible risk that already identified and handle the existing possible risk. The results of risk analysis can used to help company prevent, minimize risk and treat the risk by thir priority before the possible risk hamper company performance.*

Keywords: *risk analysis management; ISO 31000; IT operation suport (iTop).*

1. PENDAHULUAN

PT. ABCD merupakan perusahaan yang bergerak di bidang IT yang melayani jasa Total IT *Managed Service* di Indonesia. Dalam memberikan layanan terkelola bagi kliennya PT. ABCD memiliki 7 pilar utama yaitu *product solution, field services, operation command center, data center, security services, developer, dan contact center*. Layanan terkelola yang diberikan bertujuan agar klien dapat berfokus pada bisnis perusahaan mereka tanpa mengkhawatirkan permasalahan IT di dalam perusahaan.

Namun permasalahan IT dapat terjadi dimana saja dan kapan saja. Saat terjadi permasalahan IT pada klien PT. ABCD dibutuhkan penanganan segera dari staff operational IT untuk memperbaiki insiden yang terjadi. Untuk menerima laporan mengenai permasalahan IT yang dihadapi oleh klien, PT. ABCD menggunakan aplikasi iTop.

iTop adalah aplikasi *open source* CMDB (*Configuration Management Data Base*) yang berfungsi untuk menghubungkan proses operational IT PT. ABCD. Berbagai fitur yang ada di aplikasi iTop yaitu *incident and user request management, transparent SLA, problem management, customizable* CMDB dan *chat messenger*. Aplikasi iTop membantu perusahaan untuk mendapatkan laporan mengenai kualitas layanan yang diberikan oleh perusahaan kepada klien. Aplikasi iTop sangat penting bagi *staff operational* IT dalam membuat laporan kepada perusahaan.

Setiap aplikasi pasti memiliki berbagai kemungkinan risiko yang dapat menggangu sehingga aplikasi tidak dapat berjalan optimal. Kemungkinan risiko yang ada dapat muncul dari berbagai faktor baik dari internal atau eksternal aplikasi tersebut. Tidak terkecuali aplikasi iTop, apikasi tersebut juga dapat mengalami kemungkinan-kemungkinan risiko yang muncul di sekitarnya. Berdasarkan permasalahan tersebut, maka dibutuhkan penelitian untuk mendokumentasikan berbagai macam kemungkinan risiko serta prioritas risiko-risiko tersebut terhadap perusahaan. Sehingga dengan tujuan tersebut dapat dilakukan analisis manajemen risiko menggunakan ISO 31000.

Penelitian manajemen risiko di Bandara Soekarno Hatta mengacu pada ISO 31000 dilakukan pada tahun 2013 oleh Terry George Abisa. Analisis risiko yang dilakukan meliputi 3 tahapan ISO 31000. Hasil dari penelitian tersebut menunjukkan adanya 7 peristiwa risiko yang berpotensi bahaya dan perancangan sistem pengendalian risiko yang ada sudah dibuat dengan baik. [1]

Analisis risiko menggunakan ISO 31000 juga dilakukan pada sistem i-Gracias di Universitas Telkom oleh Andi Novia Rilyani pada tahun 2015. Analisis risiko pada penelitian berfokus pada *hardware* dan infrastruktur jaringan sistem i-Gracias. Dari hasil penelitian didapatkan dokumentasi tingkatan risiko pada sistem i-Gracias serta rekomendasi untuk menangulangi risiko yang sudah teridentifikasi. [2]

Pada tahun 2107, Stefan Agustinus melakukan analisis risiko teknologi informasi menggunakan ISO 31000 pada program Human Resources Management System (HRMS). Analisis risiko dilakukan degan tujuan mendokumentasikan kemungkinan risiko di sekitar program HRMS dan memberikan perlakukan risiko untuk meminimalisir kemungkinan risiko tersebut. Dari hasil penelitian ditemukan 26 kemungkinan risiko program HRMS beserta tingkatan level risiko yang ada. [3]

Berdasarkan penelitian-penelitian tersebut dapat dilihat bahwa terdapat hubungan dengan penelitian yang akan dilakukan penulis yaitu analisis risiko menggunakan ISO 31000 yang bertujuan untuk mengidentifikasi kemungkinan risiko yang muncul, dampak dari risiko tersebut, level risiko, dan perlakuan risiko terhadap kemungkinan-kemungkinan risiko yang ada. Peneitian yang akan penulis lakukan adalah analisis risiko aplikasi iTop pada PT. ABCD. Yang mampu menghasilkan dokumentasi kemungkinan risiko yang dapat muncul beserta level dampak risiko tersebut terhadap aplikasi iTop serta rekomendasi terhadap perlakukan risiko yang dapat dilakukan untuk meminimalisir risiko yang ada.

Manajemen risiko mencakup proses identifikasi, pengukuran risiko dan membuat strategi untuk pengelolaan sumber daya yang ada, Tujuan dari manajaemen risiko adalah mengelola risiko-risko yang ada sehingga perusahaan mendapatkan hasil yang optimal. [4]

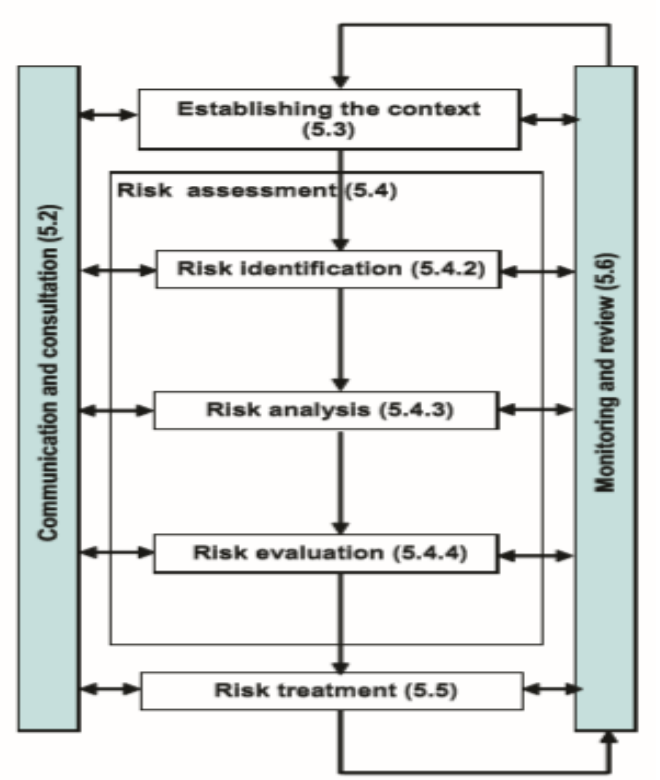
Beberapa prinsip dasar dalam manajemen risiko untuk diterapkan di dalam binis, yaitu :

a. Memahami *business goal*.
b. Mengidentifikasi hal yang menghambat tercapainya *business goal*.
c. Menentukan pengendalian untuk meminimalisir risiko-risiko yang ada.

Perusahaan perlu melakukan analisis risiko terhadap aset-aset teknologi informasi dikarenakan risiko dapat muncul dimana saja dan kapan saja, jika tidak dianalisa sebelumnya maka tidak dapat dilakukan pengendalian terhadap risiko yang ada dan dapat menggangu kinerja perusahaan. Sehingga dengan penelitian yang akan penulis lakukan dapat membantu perusahaan menangulangi risiko terhadap aset-aset aplikasi iTop. Serta dengan adanya dokumentasi risiko serta rekomendasi perlakukan risiko tersebut dapat menjadi acuan perusahaan dalam memperlakukan risiko sebelum risiko-risiko tersebut menghambat kinerja perusahaan.

2. METODOLOGI PENELITIAN

International Organization for Standardization (ISO) 31000 seperti yang ditunjukkan pada gambar 1, merupakan standar yang disusun dengan tujuan memberikan prinsip dan pedoman manajemen risiko secara universal. Di dalam *International Organization for Standardization* (ISO 31000:2009) terdapat 2 tahapan dalam proses manajemen risiko. Tahapan pertama adalah *risk assesment* yang merupakan proses menentukan risiko yang berpotensi menanggu perusahaan mmencapai *business goal*. Di dalam tahapan *risk assessment* terdapat 3 proses yaitu *risk identification*, *risk analysis*, dan *risk evaluation*. *Risk identification* yaitu proses mengidentifikasi kemungkinan-kemungkinan risiko yang dapat menghambat perusahaan, *risk analyst* yaitu proses menentukan risiko yang berpotensi menghambat perusahaan mencapai *business goal*, *risk evaluation* yaitu proses evaluasi setiap kemungkinan risiko berdasarkan tingkat kegawatan berdasarkan kriteria yang telah dibuat. Tahapan selanjutnya yaitu *risk treatment* dimana peneliti melakukan penyeleksian terhadap kemungkinan-kemungkinan risiko sebelumnya. Sehingga kemungkinan-kemungkinan risiko dan dampak risiko dapat bertambah atau berkurang. [5]



Gambar 1. ***Risk Management – Principles and Guidelines***

Metode yang akan penulis gunakan dalam penelitian ini adalah metode *case study research*.. Metode ini berfokus pada satu kasus serta sample yang digunakan berupa individu atau kelompok. Sehingga dengan metode ini penulis dapat mengumpulkan data lebih pada objek yang diteliti untuk menjawab permaslahan yang ada. Data pada penelitian ini berupa data primer, dimana sumber data dikumpulkan dalam bentuk dokumen yang sudah divalidasi dan diverifikasi oleh narasumber. Sumber data yang berasal dari tesis atau disertasi tidak dapat digunakan karena termasuk data tertier. [6]

Teknik pengumpulan data berupa wawancara. Penulis melakukan wawancara dengan *IT Operation Support & Biz Deputy Head* dari PT. ABCD sebagai sumber internal. Sebagai narasumber beliau memiliki kompetensi berupa pengetahuan mengenai ISO 20000 dan mempunyai sertifikat ITIL (minimal *foundation*).

3. HASIL DAN PEMBAHASAN

3.1 Risk Assesment

Tahap *risk assessment* atau penilaian risiko merupakan tahap pertama yang dilakukan sesuai dengan pedoman analisis manajemen risiko ISO 31000. Dimana pada tahap ini akan terdapat 3 proses yang dilakukan yaitu *risk identification, risk analysis*, dan *risk evaluation.* Ketiga proses tersebut harus dilalui untuk ke tahap yang selanjutnya.

3.1.1 Identifikasi Risiko

Proses pertama dalam tahap *risk assessment* adalah proses *risk identification* atau identifikasi aset terkait aplikasi iTop dilakukan melalui proses wawancara dengan *IT Operation Support & Biz Deputy Head* dari PT. ABCD. Pada tahap ini dilakukan identifikasi aset dari data, software hingga hardware yang berakaitan dengan aplikasi iTop.

Tabel 1. Identifikasi aset iTop

Komponen Sisitem Informasi	*Aset iTop*
Data	Data User Client, Data Aset
Software	IT Operational Portal (iTop)
Hardware	Personal Computer (PC), Server Database, Server Web Service

Setelah dilakukan identifiksi aset dari data, software hingga hardware yang berkaitan dengan aplikasi iTop. Selanjutnya adalah mengidentifikasi kemungkinan-kemungkinan risiko yang terkait dengan aset aplikasi iTop yang dapat muncul dari berbagai faktor seperti alam/lingkungan, manusia, sistem dan infrastruktur. Serta tidak lupa diberikan identitas untuk setiap kemungkinan risiko yang ditemukan.

Tabel 2. Identifikasi kemungkinan risiko

Faktor	*ID*	*Kemungkinan Risiko*
Alam / Lingkungan	R01	Banjir
	R02	Gempa bumi
	R03	Kebakaran
	R04	Petir
Manusia	R05	Pencurian perangkat/data
	R06	*Human Error*
	R07	Informasi diakses oleh pihak yang tidak berwenang
	R08	Data dan informasi tidak sesuai fakta
	R09	Kerusakan akibat ulah manusia (*cybercrime* dan vandalism)
Sistem dan Infrastruktur	R10	*Server Down*
	R11	*Data corrupt*
	R12	*Backup failure*
	R13	Web service mati secara tiba-tiba
	R14	Hacking terhadap jaringan
	R15	Memori penuh
	R16	Koneksi jaringan terputus
	R17	Kerusakan hardware
	R18	*Overheat*
	R19	*Overload*
	R20	Kurang baiknya kualitas jaringan
	R21	Listrik padam

Dari hasil proses identifikasi risiko ditemukan terdapat 21 kemungkinan risiko yang berasal dari faktor alam/lingkungan, manusia, sistem dan infrastruktur yang berpotensi mempengaruhi perusahaan. Kemudian kemungkinan-kemungkinan risiko yang telah teridentifikasi tersebut diidentifikasi dampaknya terhadap perusahaan. Sehingga di dalam proses ini dampak dari setiap kemungkinan risiko yang ada dapat teridentifikasi.

Tabel 3. Identifikasi dampak risiko

ID	*Kemungkinan Risiko*	*Dampak*
R01	Banjir	Terhambatnya aktivitas bisnis perusahaan.
R02	Gempa bumi	Terjadi kerusakan infrastruktur dan jalannya perusahaan terhenti.
R03	Kebakaran	Terjadi kerusakan infrastruktur dan jalannya perusahaan terhenti.
R04	Petir	Terjadi kerusakan infrastruktur.
R05	Pencurian perangkat/data	Kerugian finansial/ informasi data perusahaan.
R06	Human Error	User request tertunda.
R07	Informasi diakses oleh pihak yang tidak berwenang	Tidak mempengaruhi perusahaan karena data iTop berupa *customer incident*.
R08	Data dan informasi tidak sesuai fakta	Laporan insiden *customer* tidak valid.
R09	Kerusakan akibat ulah manusia (*cybercrime* dan vandalism)	Kerugian finansial/ informasi data perusahaan.
R10	*Server down*	Tidak dapat melakukan akses ke iTop dan *database*.
R11	*Data corrupt*	Perusahaan tidak dapat menerima laporan yang valid mengenai kualitas layanan kepada *customer*.
R12	*Backup failure*	Data laporan insiden customer tidak lengkap.
R13	*Web service* mati secara tiba-tiba	Customer tidak dapat mengakses iTop dan perusahaan tidak dapat menerima laporan insiden *customer*.
R14	*Hacking* terhadap jaringan	Pencurian data-data perusahaan dan aktivitas penerimaan insiden customer terganggu.
R15	Memori penuh	Insiden customer yang baru gagal ditampung.
R16	Koneksi jaringan terputus	Gagal melakukan akses ke iTop.

ID	*Kemungkinan Risiko*	*Dampak*
R17	Kerusakan hardware	Aktivitas perusahaan terhambat karena harus *setup* data ke hardware yang baru.
R18	*Overheat*	Kinerja hardware tidak maksimal dan hardware dapat mengalami kerusakan jika menanggung suhu yang panas terus-menerus.
R19	*Overload*	*Log database* dan *log temp database* penuh. Terjadinya *bottleneck*.
R20	Kurang baiknya kualitas jaringan	Akses ke iTop terhambat.
R21	Listrik padam	Aktivitas perusahaan tidak tergangu karena memiliki genset

3.1.2 Risk Analysis

Setelah kemungkinan- kemungkinan risiko beserta dampaknya telah teridentifikasi, langkah selanjutnya adalah proses analisis risiko. Pada proses ini terdapat tabel kriteria *likelihood* dan tabel kriteria *impact* yang digunakan sebagai acuan untuk proses analisis risiko. Tabel 4 merupakan tabel kriteria *likelihood* atau nilai kemungkinan yang telah ditentukan. Dalam penilaiannya *likelihood* dibedakan di dalam 5 kriteria yang dibedakan melalui seberapa banyak kemungkinan risiko tersebut dapat terjadi dalam kurun waktu tertentu.

Tabel 4. Kriteria likelihood

Likelihood		*Keterangan*	*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

Tabel 5 merupakan tabel nilai *impact* atau dampak jika kemungkinan-kemungkinan risiko tersebut terjadi di perusahaan. Di dalam penilaiannya terdapat 5 kriteria dampak yang mungkin terjadi. Dari kelima kriteria tersebut dibedakan dari dampak yang tidak berpengaruh hingga dampak yang paling mempengaruhi kinerja perusahaan. Dari setiap dampak kemungkinan risiko yang telah diidentifikasi akan dimasukan satu per satu di dalam nilai *impact* yang telah ditentukan.

Tabel 5. Kriteria impact

Impact		*Keterangan*
Nilai	*Kriteria*	
1	*Insignificant*	Tidak mengganggu aktivitas perusahaan.
2	*Minor*	Aktivitas perusahaan sedikit terhambat namun aktivitas inti perusahaan tidak terganggu.
3	*Moderate*	Menyebabkan ganguan pada proses bisnis sehingga sebagian jalannya aktivitas perusahaan terhambat.
4	*Major*	Menghambat hampir seluruh aktivitas perusahaan.
5	*Catastrophic*	Aktivitas perusahaan berhenti karena proses bisnis mengalami gangguan total.

Setelah nilai kemungkinan dan dampak ditentukan, langkah selanjutnya adalah melakukan penilaian satu per satu terhadap kemungkinan risiko yang ada. Dari 21 kemungkinan risiko yang ada ditentukn satu per satu nilai *likelihood* dan nilai *impact* berdasarkan acuan tabel yang dibuat sebelumnya yang dapat dilihat detailnya pada tabel 6.

Tabel 6. Penilaian kemungkinan risiko dengan *likelihood* dan *impact*

ID	*Kemungkinan Risiko*	*Likelihood*	*Impact*
R01	Banjir	1	3
R02	Gempa bumi	1	5
R03	Kebakaran	1	5
R04	Petir	1	3
R05	Pencurian perangkat/data	2	2
R06	*Human Error*	3	2
R07	Informasi diakses oleh pihak yang tidak berwenang	2	1
R08	Data dan informasi tidak sesuai fakta	3	2
R09	Kerusakan akibat ulah manusia (*cybercrime* dan *vandalism*)	1	2
R10	Server Down	3	2
R11	Data corrupt	2	2
R12	Backup failure	2	2
R13	Web service mati secara tiba-tiba	2	2
R14	Hacking terhadap jaringan	1	3
R15	Memori penuh	1	2
R16	Koneksi jaringan terputus	3	4

ID	*Kemungkinan Risiko*	*Likelihood*	*Impact*
R17	Kerusakan *hardware*	2	1
R18	*Overheat*	2	1
R19	*Overload*	2	2
R20	Kurang baiknya kualitas jaringan	3	3
R21	Listrik padam	2	3

3.1.3 Risk Evaluation

Proses terkahir untuk menyelesaikan tahap *risk assesment* adalah proses *risk evaluation.* Dalam proses ini menggunakan acuan berupa matrix evaluasi risiko. Diamana dalam matrix tersebut dibedakan ke dalam 3 *risk level* yaitu *low, medium* dan *high.* Kemungkinan risiko yang telah ditentukan nilai *likelihood* dan nilai *impact* pada proses sebelumnya akan dibedakan lagi menyesuaikan matrix yang ada. Tabel 7 telah memetakan *risk level* berdasarkan *likelihood* dan *impact*.

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

Setiap kemungkinan risiko berdasrkan *likelihood* dan *impact* akan dimasukkan ke dalam matrix evaluasi risiko dengan melihat pemetaan pada tabel matrix evaluasi risiko sebelumnya. Di dalam tabel matrix evaluasi risiko identitas setiap kemungkinan risiko dimasukkan kedalam parameter yang sesuai dengan kriteria *likelihood* dan kriteria *impact* yang dilakukan sebelumnya.

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

Likelihood	**Certain**	**5**					
	Likely	**4**					
	Possible	**3**		R06 R08 R10	R20	R16	
	Unlikely	**2**	R07 R17 R18	R05 R11 R12 R13 R19	R21		
	Rare	**1**		R09 R15	R01 R04 R14		R02 R03
Impact			***1***	***2***	***3***	***4***	***5***
			Insignificant	***Minor***	***Moderate***	***Major***	***Catastrophic***

Kemudian setelah semua kemungkinan risiko yang ada dimasukkan ke dalam matrix evaluasi risiko pada tabel 9 akan dijabarkan dari 21 kemungkinan risiko yang ada termasuk kedalam *level of risk* dengan tingkatan *high, medium* atau *low* berdasarkan kriteria *likelihood* dan *impact.*

Tabel 9. *Risk level* dari kemungkinan risiko

ID	*Kemungkinan Risiko*	*Likelihood*	*Impact*	*Risk Level*
R16	Koneksi jaringan terputus	3	4	Medium
R20	Kurang baiknya kualitas jaringan	3	3	Medium
R06	*Human Error*	3	2	Medium
R08	Data dan informasi tidak sesuai fakta	3	2	Medium
R10	*Server Down*	3	2	Medium
R21	Listrik padam	2	3	Medium
R02	Gempa bumi	1	5	Medium
R03	Kebakaran	1	5	Medium
R05	Pencurian perangkat/data	2	2	Low
R11	*Data corrupt*	2	2	Low
R12	*Backup failure*	2	2	Low
R13	*Web service* mati secara tiba-tiba	2	2	Low
R19	*Overload*	2	2	Low
R07	Informasi diakses oleh pihak yang tidak berwenang	2	1	Low
R17	Kerusakan hardware	2	1	Low
R18	*Overheat*	2	1	Low

ID	*Kemungkinan Risiko*	*Likelihood*	*Impact*	*Risk Level*
R01	Banjir	1	3	Low
R04	Petir	1	3	Low
R14	*Hacking* terhadap jaringan	1	3	Low
R09	Kerusakan akibat ulah manusia (*cybercrime* dan *vandalism*)	1	2	Low
R15	Memori penuh	1	2	Low

Hasil dari proses *risk evaluation* dapat dilihat pada tabel 9 yaitu dari 21 kemungkinan terdapat 8 (koneksi jaringan terputus, kurang baiknya kualitas jaringan, *human error*, data dan informasi tidak sesuai fakta, *server down*, listrik padam, gempa bumi, kebakaran) yang termasuk kedalam *level of risk* tingkatan *medium*. Serta 13 (pencurian perangkat/data, *data corrupt, backup failure*, web service mati secara tiba-tiba, *overload*, informasi diakses oleh pihak yang tidak berwenang, kerusakan *hardware, overheat*, banjir, petir, hacking terhadap jaringan, risiko kerusakan akibat ulah manusia seperti *cybercrime* dan *vandalism*, memori penuh) yang termasuk kedalam *level of risk* tingkatan *low*.

3.2 Risk Treatment

Tahap setelah identifikasi risiko adalah tahap perlakuan risiko. Pada tahap ini, penulis akan memberikan saran-saran mengenai perlakuan untuk semua kemungkinan risiko yang ada pada aplikasi iTop. Saran perlakukan yang diberikan penulis diharapkan dapat mengurangi arau meminimalisr kemungkinan risiko yang ada. Serta dapat digunakan perusahaan untuk melakukan pencegahan terhadap kemungkinan risiko yang ada.

Tabel 10. Usulan tindakan risiko

ID	*Kemungkinan Risiko*	*Risk Level*	*Tindakan Risiko*
R16	Koneksi jaringan terputus	Medium	Ketika koneksi jaringan terputus segera lapor ke bagian jaringan. Melakukan *maintenance* jaringan di perusahaan secara berkala.
R20	Kurang baiknya kualitas jaringan	Medium	Ketika koneksi jaringan menghambat perusahaan segera lapor ke bagian jaringan. Mengganti ISP (*Internet Service Provider*) jika jaringan yang dipakai menggangu aktivitas peprusahaan.
R06	*Human Error*	Medium	Melakukan pelatihan sebelumnya terhadap karyawan baru. Membuat *knowledge management system* sebagai dokumentasi pengetahuan bagi karyawan baru agar tidak melakukan kesalahan yang sama.
R08	Data dan informasi tidak sesuai fakta	Medium	Memastikan kembali data *customer incident* yang diterima sesuai dengan fakta yang ada.
R10	*Server Down*	Medium	Melakukan pengecekan secara berkala dalam 1 hari terhadap database dari aplikasi iTop dan database utama perusahaan. Melakukan *refresh* terhadap penggunan log, temp, dan RAM dari aplikasi iTop dan database utama untuk mencegah *server down.* Memasang *antivirus* yang terpercaya.
R21	Listrik padam	Medium	Menggunakan sumber listrik yang berbeda.
R02	Gempa bumi	Medium	Memasang server cadangan di lokasi yang berbeda. Melakukan *mirroring database*.
R03	Kebakaran	Medium	Memasang *server* cadangan di lokasi yang berbeda. Melakukan *mirroring database*. Memasang *fire hydran* di dalam gedung perusahaan untuk mencegah terjadinya kebakaran. Menyediakan peralatan pemadam kebakaran di dalam gedung.
R05	Pencurian perangkat/data	Low	Mengadakan *maintenance password* secara berkala. Memasang CCTV di gedung perusahaan.
R11	*Data corrupt*	Low	Melakukan *backup data* secara berkala. Melakukan permbersihan pada PC secara berkala agar mencegah munculnya virus/ malware.
R12	*Backup failure*	Low	Memperhatikan penggunaan memori penyimpaan yang digunakan secara berkala. Melakukan *backup data* yang terdapat di aplikasi iTop dan database utama secara berkala. Membuat *maintenance plan* yang sesuai kebutuhan.
R13	*Web service* mati secara tiba-tiba	Low	Segera melakukan perbaikan saat *web service* mati. Memberikan pengumuman kepada *customer*.
R19	*Overload*	Low	Melakukan pengecekan secara berkala terhadap *databas*e dari aplikasi iTop dan *database* utama perusahaan. Melakukan *refresh* terhadap penggunan log, temp, dan RAM dari aplikasi iTop dan database utama sebelum server down.
R07	Informasi diakses oleh pihak yang tidak berwenang	Low	Mengadakan *maintenance password* secara berkala. Memasang CCTV di gedung perusahaan.

ID	*Kemungkinan Risiko*	*Risk Level*	*Tindakan Risiko*
R17	Kerusakan *hardware*	Low	Membersihkan hardware setiap hari agar tidak berdebu. Segera melaporkan kepada bagian teknisi jika ditemukan hardware yang bermasalah .
R18	*Overheat*	Low	Memastikan *air conditioner* sudah mampu membuat *hardware* tetap dingin.
R01	Banjir	Low	Memasang server cadangan di lokasi yang berbeda. Melakukan mirroring database. Menyediakan tempat tinggi untuk menyimpan asset perusahaan.
R04	Petir	Low	Memasang server cadangan di tempat yang berbeda. Melakukan mirroring database . Memasang alat penangkal petir di gedung perusahaan.
R14	*Hacking* terhadap jaringan	Low	Mengganti password server secara berkala. Mengadakan *maintenance* jaringan secara berkala.
R09	Kerusakan akibat ulah manusia (*cybercrime* dan *vandalism*)	Low	Mengganti password server secara berkala. Memasang CCTV di gedung perusahaan.
R15	Memori penuh	Low	Mengecek penggunaan memori ecara berkala. Menambah kapasitas memori sebelum penuh. Menghapus data-data perusahaan yang sudah lebih dari 10 tahun

4. KESIMPULAN

Tahapan analisis manajemen risiko pada aplikasi iTop di PT. ABCD yang berpedoman pada *International Organization for Standardization* (ISO 31000:2009) telah dilaksanakan. Proses analisis risiko yang dilaksanakan dari tahapan *risk assesment* yang melalui 3 langkah yaitu *risk identification, risk analysis,* dan *risk evaluation*. Dan tahap *risk treatment* untuk membuat saran-saran perlakukan risiko untuk kemungkinan risiko yang ada pada aplikasi iTop.

Dari hasil analisis risiko dapat dilihat, terdapat 21 kemungkinan risiko yang berpotensi menganggu kinerja aplikasi iTop. Terdapat 8 kemungkinan risiko yang termasuk kedalam *level of risk* tingkat *medium*, yaitu koneksi jaringan terputus, kurang baiknya kualitas jaringan, *human error*, data dan informasi tidak sesuai fakta, *server down*, listrik padam, gempa bumi, dan kebakaran. Serta terdapat 17 kemungkinan risiko yang termasuk kedalam *level of risk* tingkat *low*, yaitu pencurian perangkat/data, *data corrupt, backup failure, web service* mati secara tiba-tiba, *overload*, informasi diakses oleh pihak yang tidak berwenang, kerusakan *hardware, overheat*, banjir, petir, *hacking* terhadap jaringan, risiko kerusakan akibat ulah manusia seperti *cybercrime* dan *vandalism*, dan memori penuh.

Sebenarnya proses mengatasi risiko yang dilakukan oleh perusahaan sudah terlaksana, karena PT. ABCD merupakan perusahaan yang berfokus di bidang IT. Namun kemungkinan tidak dilaksanakannya pengangulangan risiko tersebut secara berkala dapat terjadi, sehingga diharapkan hasil penelitian ini dapat digunakan perusahaan untuk dapat menyusun kebijakan dan meminimalisir kemungkinan-kemungkinan risiko yang dapat terjadi pada perushaan dikemudian hari.

DAFTAR PUSTAKA

[1] N. Terry George Abisay, "Manajemen Risiko pada Bandara Soekarno Hatta Berbasis Iso 31000," pp. 116 - 129, 2013.

[2] D. D. J. Andi Novia Rilyani. Yanuar Firdaus, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University)," *e-Proceeding of Engineering*, pp. 6201-6208, 2015.

[3] A. N. A. D. C. Stefan Agustinus, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *RESTI (Rekayasa Sistem dan Teknologi Informasi)*, pp. 250-258, 2017.

[4] R. V. I. Francisca Lady Nice, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," *JUISI*, pp. 1-11, 2016.

[5] "Risk management—Principles and guidelines," *Standards Australia/Standards New Zealand* , pp. 1-35, 2009.

[6] P. Zainal A. Hasibuan, "Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi," pp. 1-194, 2007.

[7] R. A. K. Tri Ramdhany, "Analisis Risiko Sistem Informasi Penjualan Berbasis ISO 31000 - Risk Management di PT. Remaja Rosdakarya," pp. 1-7.

[8] D. J. P. K. A. S. S. Paulus Sukapto, "Integration of Risk Engineering by ISO 31000 and Safety Engineering: A Case Study in a Production Floor of Sport Footwear Industry in Indonesia," *International Journal of Simulation*, pp. 22.1-22.12, 2018.

[9] I. D. P. Angraini, "Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000," *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi*, pp. 70-76, 2017.