Terbit online pada laman web jurnal : **http://jurnal.iaii.or.id**

JURNAL RESTI

(Rekayasa Sistem dan Teknologi Informasi)

Vol. 1 No. 3 (2017) 250 – 238 ISSN Media Elektronik : 2580-0760

Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS

Stefan Agustinus[a], Adi Nugroho[b], Ariya Dwika Cahyono[c]

[a]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, s14agustinus@gmail.com

[b]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, adi.nugroho@staff.uksw.edu

[c]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, ariyadc@staff.uksw.edu

Abstract

The HRMS program is the central database of all matters relating to Human Resources Development of PT. XYZ. The existence of HRMS program is very important for the sustainability of the company, especially in the employment sector. Therefore, this HRMS program should be able to run optimally and consistently. A risk analysis is required to obtain documentation of the various possible risks that are in the vicinity of the HRMS program and the risk treatment required to minimize the likelihood of these risks arising. Risk analysis used at PT. XYZ is ISO 31000. The first stage used in this research is the stage of risk assessment which consisting of 3 stages, namely risk identification, risk analysis, and risk evaluation. The second stage is the stage of risk treatment. The results of this research are used as a tool for the stakeholders of the company to be able to arrange documentation related to company risk management in the future.

Keywords: Risk Analysis, International Organization for Standardization (ISO) 31000, Human Resources Management System (HRMS)

Abstrak

Program HRMS merupakan database pusat dari segala hal yang berkaitan dengan Human Resources Development dari PT. XYZ. Keberadaan program HRMS ini tentu saja sangat penting bagi keberlangsungan perusahaan, terutama di sektor kepegawaian. Maka dari itu program HRMS ini harus bisa berjalan secara optimal dan konsisten. Dibutuhkan sebuah analisis risiko untuk mendapatkan dokumentasi terhadap berbagai macam kemungkinan risiko yang berada di sekitar dari program HRMS serta perlakuan risiko yang diperlukan untuk meminimalisir kemungkinan-kemungkinan risiko tersebut muncul. Analisis risiko yang digunakan pada PT. XYZ adalah ISO 31000. Tahapan pertama yang digunakan dalam penelitian ini adalah tahap penilaian risiko yang terdiri dari 3 tahapan, yaitu identifikasi risiko, analisis risiko, dan evaluasi risiko. Tahapan kedua adalah tahap perlakuan risiko. Hasil dari penelitian ini digunakan sebagai alat bantu bagi pemangku kebijakan dari perusahaan untuk dapat menyusun dokumentasi terkait dengan manajemen risiko perusahaan di kemudian hari.

Kata kunci: Analisis Risiko, International Organization for Standardization (ISO) 31000, Human Resources Management System (HRMS)

1. Pendahuluan

PT. XYZ merupakan sebuah perusahaan yang bergerak di bidang usaha retail. Sebagai salah satu perusahaan yang cukup besar, PT. XYZ kemudian masih dibagi-bagi kembali ke dalam cabang-cabang berdasarkan beberapa kota besar yang ada di Indonesia. Salah satu cabang yang ada di PT. XYZ adalah cabang *Head Office* (HO). HO PT. XYZ berkedudukan di dua lokasi yang berbeda di Jakarta, yaitu yang pertama berlokasi di Kemayoran (HO Kemayoran) dan yang kedua berlokasi di Ancol (HO Ancol).

Sebagai kantor pusat, baik HO Kemayoran maupun HO Ancol tentu saja menjadi pusat dari aktivitas PT. XYZ itu sendiri. Di dalam HO ini juga masih dibagi-bagi kembali ke dalam 14 direktorat yang berbeda, salah satunya ialah direktorat *Information Technology* (IT) yang tentu saja adalah direktorat yang menangani semua persoalan yang berkaitan dengan teknologi informasi dari PT. XYZ.

Salah satu program yang digunakan PT. XYZ ialah HRMS (*Human Resources Managemet System*). Program ini dikembangkan oleh direktorat IT, divisi *Software Development and Support* 4, bagian *Software Development* II dan *Software Support* 2. Fungsi dari

program HRMS ialah sebagai *database* pusat dari segala hal yang berkaitan dengan *Human Resources Development* (HRD). Keberadaan program HRMS ini tentu saja sangat penting bagi keberlangsungan perusahaan, terutama untuk sektor kepegawaian. Maka dari itu program HRMS ini harus bisa berjalan secara optimal dan konsisten.

Namun sama halnya dengan program atau sistem lainnya, HRMS tentu saja juga memiliki berbagai macam kemungkinan risiko yang bisa saja muncul setiap saat dan tentu saja dapat mengganggu bahkan hingga melumpuhkan kinerja sistem sehingga program tidak dapat berjalan secara optimal dan konsisten. Kemungkinan-kemungkinan risiko tersebut bisa saja datang dari beberapa macam faktor yang berada di sekitarnya. Berdasarkan dari permasalahan di atas inilah, maka dirasa perlu untuk melakukan sebuah penelitian yang berkaitan dengan analisis manajemen risiko dengan menggunakan ISO 31000. Tujuannya ialah dengan hasil penelitian ini nantinya dapat mendokumentasikan risiko-risiko yang dihadapi serta tindakan yang dilakukan untuk meminimalisir risiko terhadap program HRMS di PT. XYZ yang bisa saja muncul setiap saat pada aset-aset yang merupakan kesatuan dari program HRMS untuk dapat dilakukan pengendaliannya secara menyeluruh di masa yang akan datang.

2. Tinjauan Pustaka

Penelitian di Lembaga Penerbangan dan Antariksa Nasional (LAPAN) terkait dengan analisis risiko teknologi informasi menggunakan ISO 31000 ini dapat melaksanakan tahapan dan proses analisis risiko teknologi informasi *website Space Weather Information and Forecast Services* (SWIFTS). Penggunaan ISO 31000 terhadap teknologi informasi *website* SWIFTS ini dapat membantu mendokumentasikan tingkat risiko dan perlakuan terhadap risiko teknologi informasi *website* SWIFTS. [1]

Analisis risiko teknologi informasi menggunakan ISO 31000 dilakukan pada *Document Management System* (DMS) di PT. Jabar Telematika (JATEL) ini juga menganalisis risiko yang terjadi pada DMS arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE). Penggunaan ISO 31000 ini menghasilkan analisis manajemen risiko teknologi informasi pada DMS arsip elektronik ADEL dan NADINE [2]

Penelitian analisis risiko teknologi informasi menggunakan ISO 31000 juga dilakukan pada lembaga penelitian perguruan tinggi. Hasil dari penelitian tersebut adalah tersedianya sebuah katalog mengenai risiko teknologi informasi yang terdiri dari daftar risiko dan faktor-faktor yang berkontribusi atau memicu terjadinya peristiwa tertentu yang mengancam penggunaan teknologi informasi pada lembaga penelitian perguruan tinggi. [5]

Berdasarkan dari 3 penelitian sebelumnya ini menunjukan adanya hubungan dengan penelitian yang penulis lakukan mengenai kerangka serta metode untuk mengidentifikasi aset-aset teknologi informasi, kemungkinan-kemungkinan risiko yang ada, dampak yang dapat dimunculkan, penilaian dan pengevaluasian risiko, serta perlakuan risiko yang dapat dilakukan. Penulis akan melakukan sebuah penelitian yang berfokus untuk memberikan usulan perlakuan risiko untuk semua kemungkinan-kemungkinan risiko yang sewaktu-waktu bisa muncul, baik itu risiko yang sudah pernah dialami oleh perusahaan maupun risiko yang belum pernah dialami oleh perusahaan.

Analisis manajemen risiko adalah suatu kegiatan yang dilakukan pada tingkat pimpinan pelaksana, yaitu berupa kegiatan penemuan dan analisis sistematis atas kerugian yang mungkin saja dapat dihadapi oleh sebuah perusahaan, akibat suatu risiko serta cara pengendalian yang paling tepat untuk menangani kerugian yang dihubungkan dengan tingkat keuntungan perusahaan. [3]

Analisis risiko mempunyai beberapa tujuan, yaitu:

a. Tujuan sebelum mengalami kerugian, berupa efisiensi, meningkatkan kepercayaan, menanggulangi tanggung jawab pihak luar.
b. Tujuan setelah mengalami kerugian, berupa keberlangsungan operasi, mampu untuk tetap terus *survive*, stabilitas pendapatan dan pertumbuhan. [3]

Melakukan analisis manajemen risiko terhadap aset-aset teknologi informasi pada sebuah perusahaan merupakan suatu hal yang penting. Karena setiap aset yang dimiliki hingga semua aktivitas yang ada di dalam suatu perusahaan pasti memiliki risiko yang bisa saja muncul setiap saat tanpa bisa diprediksi sebelumnya jika tidak dianalisis oleh perusahaan yang berkaitan.

3. Metodologi Penelitian

ISO 31000 merupakan standar yang berkaitan dengan manajemen risiko yang dikodifikasi oleh *International Organization for Standardization* (ISO). Tujuan dari ISO sendiri adalah untuk memberikan prinsip-prinsip dan pedoman untuk manajemen risiko yang diakui secara universal. [1]

Penelitian ini akan dilakukan dengan menggunakan 2 tahapan yang telah disesuaikan dengan proses menejemen risiko dari *International Organization for Standardization* (ISO 31000:2009) di mana setiap informasi yang dibutuhkan dalam penelitian ini didapatkan dengan cara melalui wawancara terhadap sumber-sumber internal dari PT. XYZ.

Tahapan yang pertama adalah *Risk Assesment* (Penilaian Risiko). Proses ini terdiri dari 3 tahapan, yaitu *Risk Identification* (Identifikasi Risiko), *Risk Analyst* (Analisis Risiko), dan *Risk Evaluation* (Evaluasi Risiko). *Risk assesment* atau penilaian risiko merupakan proses penentuan risiko yang berpotensi mempengaruhi organisasi dalam mencapai tujuannya. *Risk analyst* atau analisis risiko merupakan upaya untuk memahami risiko secara lebih mendalam. Sementara *Risk Evaluation* atau evaluasi risiko merupakan proses melakukan evaluasi terhadap tingkat kegawatan masing-masing risiko menggunakan kriteria yang telah ditentukan. [1]

Untuk tahapan yang kedua adalah *Risk Treatment* (Perlakuan Risiko). Tahapan ini meliputi upaya untuk menyeleksi pilihan-pilihan yang dapat mengurangi atau bahkan meniadakan dampak serta kemungkinan terjadinya risiko kemudian menerapkan pilihan-pilihan tersebut. [1]

Penelitian ini juga akan menggunakan metode *Case Studies Research*. Zainal A. Hasibuan, PhD (2007) mengemukakan bahwa metode *Case Studies Research* merupakan penelitian yang memusatkan perhatian pada suatu kasus tertentu dengan menggunakan individu atau kelompok sebagai bahan studinya. Penggunaan metode *Case Studies Research* ini biasanya difokuskan untuk menggali mengumpulkan data yang lebih dalam terhadap obyek yang diteliti untuk dapat menjawab permasalahan yang sedang terjadi. [4]

Penggunaan individu atau kelompok sebagai objek studi ini bertujuan agar peneliti bisa mendapatkan data yang peneliti butuhkan dan data penelitian yang didapatkan tersebut adalah data primer. Penelitian *Case Studies Research* datanya harus berupa data primer. Data ini dapat dikumpulkan dalam bentuk dokumen-dokumen yang telah divalidasi dan dilakukan verifikasi konfirmasi data ke *primary source*-nya. Zainal A. Hasibuan, PhD (2007) juga menambahkan bahwa sumber data yang diambil dari tesis atau disertasi tidak dapat digunakan karena data tersebut bukan data primer melainkan data tertier karena diambil dari data lain yang kemudian diolah. [4]

4. Hasil dan Pembahasan

4.1 Tahap Penilaian Risiko

Proses tahap penilaian risiko pada program HRMS ini akan terdiri 3 tahapan, yaitu tahap identifikasi risiko, tahap analisis risiko, dan tahap evaluasi risiko.

4.1.1 Identifikasi Risiko

Identifikasi aset HRMS

Tahapan identifikasi aset-aset yang terkait dengan HRMS dilakukan dengan melalui proses wawancara serta observasi kepada karyawan dari bagian *Software Development* II dan *Software Support* 2. Detail aset-aset yang terkait dengan HRMS dapat dilihat pada Tabel 1.

Tabel 1. Tabel Identifikasi Aset HRMS

Komponen Sistem Informasi	Aset HRMS
Data	a) Data Recruiting b) Data Hiring c) Data Administration and Benefits d) Data Time and Attendance e) Data Training and Administration f) • Data Leave and Permission
Software	• Human Resource Management System (HRMS)
Hardware	a) Personal Computer (PC) b) Server Database c) Server Web Service d) Server Remote Desktop Protocol (RDP) e) Server Load Balancer f) Server Compelant g) Switch Bokade 300 h) Kabel Fiber Optik i) Kabel Unshielded Twisted Pair (UTP) j) RJ 45

Identifikasi kemungkinan risiko

Setelah melakukan identifikasi aset, hal yang perlu diidentifikasi selanjutnya adalah kemungkinan-kemungkinan risiko yang berada di sekitar dari aset-aset yang terkait dengan program HRMS. Kemungkinan-kemungkinan risiko tersebut dapat dilihat pada Tabel 2.

Tabel 2. Tabel Identifikasi Kemungkinan Risiko

ID	Kemungkinan Risiko
KR01	Data corrupt
KR02	Kegagalan backup/generate data
KR03	Kegagalan proses pemeliharaan dan continue development
KR04	Software tidak dapat meningkatkan kualitas kinerja perusahaan
KR05	Web service mati secara tiba-tiba
KR06	Kesalahan pembuatan fungsi pada program
KR07	Hacking terhadap jaringan
KR08	Memori penuh
KR09	Server down
KR10	Koneksi jaringan terputus
KR11	Kerusakan hardware
KR12	Listrik padam
KR13	Overheat
KR14	Overload
KR15	Penyelesaian program yang tidak tepat waktu
KR16	Dokumentasi program yang tidak lengkap
KR17	Petunjuk penggunaan program yang susah dipahami
KR18	Penyelesaian program yang tidak tepat waktu
KR19	User interface rumit dan susah dipahami
KR20	Muncul anomali proses di lapangan yang tidak dapat diatasi oleh program
KR21	Kurangnya SDM secara kualitas/kuantitas
KR22	Pencurian perangkat/data
KR23	Banjir
KR24	Gempa bumi
KR25	Kebakaran
KR26	Petir

Identifikasi dampak risiko

Tahapan identifikasi selanjutnya adalah identifikasi dampak risiko. Proses ini mencoba untuk mengidentifikasi dampak seperti apa yang akan dialami oleh program HRMS jika kemungkinan-kemungkinan risiko yang sudah diidentifikasi sebelumnya terjadi. Detail dari identifikasi dampak risiko terdapat pada Tabel 3.

Tabel 3. Tabel Identifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak
KR01	Data corrupt	Data kepegawaian PT. XYZ rusak dan tidak dapat diakses. Terjadi masalah terkait dengan presensi kehadiran, lembur, dan gaji dari karyawan.
KR02	Kegagalan backup/generate data	Maintenance plan tidak dapat berjalan.
KR03	Kegagalan proses pemeliharaan dan continue development	Program mengalami penurunan performa secara perlahan-perlahan. Teknologi yang digunakan pada program tidak berkembang.
KR04	Program tidak dapat meningkatkan kualitas kinerja perusahaan	Kualitas kinerja HRD perusahaan tidak dapat berkembang secara optimal.
KR05	Web service mati secara tiba-tiba	Gagal melakukan akses ke program HRMS dan database utama.
KR06	Proses maintenance tidak terjadwal	Mengganggu aktifitas pada program HRMS dan database utama.
KR07	Hacking terhadap jaringan	Pencurian data-data penting perusahaan. Penyalahgunaan sumber daya pada jaringan.
KR08	Overcapacity	Inputan data baru yang berkaitan dengan kepegawaian PT. XYZ gagal ditampung oleh database utama.
KR09	Server down	Sulit/gagal melakukan akses ke program HRMS dan database utama.
KR10	Koneksi jaringan terputus	Gagal melakukan akses ke program HRMS dan database utama.
KR11	Kerusakan hardware	Tidak dapat melakukan akses ke program HRMS dan database utama.
KR12	Listrik padam	Aktifitas perusahaan tidak dapat berjalan.
KR13	Overheat	Kinerja hardware tersendat dan tidak maksimal. Rusaknya hardware karena harus menanggung suhu ekstrim secara terus-menerus.
KR14	Overload	Log database dan Log temp database penuh. Terjadinya bottleneck.
KR15	Dokumentasi program yang tidak lengkap	Menyulitkan programmer dalam pengembangan program. Kesalahan pembuatan fungsi pada program.
KR16	Kesalahan pembuatan fungsi pada program	Program tidak tepat guna.
KR17	Tampilan program tidak user friendly	Menyulitkan user dalam memahami cara penggunaan program.
KR18	Penyelesaian program yang tidak tepat waktu	Penyelesaian permasalahan tidak tepat waktu.
KR19	Petunjuk penggunaan program yang susah dipahami	Menyulitkan user dalam memahami cara penggunaan program.
KR20	Muncul anomali proses di lapangan yang tidak dapat diatasi oleh program	Anomali proses yang muncul harus dijalankan secara manual.
KR21	Kurangnya SDM secara kualitas/kuantitas	Penyelesaian program pendukung yang tidak tepat waktu. Kesulitan dalam pembagian kerja.
KR22	Pencurian perangkat/data	Kerugian secara finansial/informasi berkaitan dengan kerahasiaan perusahaan.
KR23	Banjir	Kerusakan infrastruktur dan menghambat aktivitas bisnis perusahaan.
KR24	Gempa bumi	Kerusakan infrastruktur dan menghentikan aktivitas bisnis perusahaan.
KR25	Kebakaran	Kerusakan infrastruktur dan menghentikan aktivitas bisnis perusahaan.
KR26	Petir	Kerusakan infrastruktur perusahaan.

4.1.2 Analisis Risiko

Setelah menyelesaikan tahap identifikasi, tahap selanjutnya adalah tahap analisis risiko. pada proses ini akan dilakukan penilaian terhadap kemungkinan-kemungkinan risiko yang sudah teridentifikasi. Penentuan nilai ini akan dilakukan berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*) yang terdapat pada Tabel 4 dan Tabel 5.

Tabel 4. Tabel Nilai pada Likelihood

Likelihood		Deskripsi	Frekuensi per kejadian
Nilai	Kriteria		
1	Rare	Risiko tersebut hampir tidak pernah terjadi	> 5 tahun
2	Unlikely	Risiko tersebut jarang terjadi	2 – 5 tahun
3	Possible	Risiko tersebut kadang terjadi	1 – 2 tahun
4	Likely	Risiko tersebut sering terjadi	7 – 12 bulan
5	Certain	Risiko tersebut pasti terjadi	1 – 6 bulan

Tabel 5. Tabel Nilai pada Impact

Impact		Deskripsi
Nilai	Kriteria	
1	Insignificant	Risiko tersebut tidak mengganggu proses bisnis yang ada dan jalannya aktivitas perusahaan.
2	Minor	Risiko tersebut mulai sedikit menghambat jalannya aktivitas perusahaan.

Impact		
Nilai	Kriteria	Deskripsi
3	Moderate	Risiko tersebut menghambat sebagian jalannya aktivitas perusahaan.
4	Major	Risiko tersebut mulai mengganggu proses bisnis yang ada dan menghambat hampir seluruh jalannya aktivitas perusahaan.
5	Catastrophic	Risiko tersebut sangat mengganggu proses bisnis yang ada dan menghentikan jalannya aktivitas perusahaan secara menyeluruh.

Setelah melakukan penentuan nilai pada kemungkinan (*likelihood*) di Tabel 4 dan pada dampak (*impact*) di Tabel 5, selanjutnya adalah memulai penilaian terhadap kemungkinan-kemungkinan risiko yang berada di sekitar dari aset-aset yang terkait dengan program HRMS yang sudah teridentifikasi sebelumnya. Detail dari penilaian kemungkinan-kemungkinan risiko dapat dilihat pada Tabel 6.

Tabel 6. Tabel Penilaian Likelihood dan Impact pada Kemungkinan Risiko

ID	Kemungkinan Risiko	Likelihood	Impact
KR01	Data corrupt	1	5
KR02	Kegagalan backup/generate data	2	2
KR03	Kegagalan proses pemeliharaan dan continue development	1	3
KR04	Program tidak dapat meningkatkan kualitas kinerja perusahaan	1	4
KR05	Web service mati secara tiba-tiba	5	2
KR06	Proses maintenance tidak terjadwal	5	1
KR07	Hacking terhadap jaringan	1	4
KR08	Overcapacity	1	3
KR09	Server down	5	2
KR10	Koneksi jaringan terputus	2	5
KR11	Kerusakan hardware	1	4
KR12	Listrik padam	4	5
KR13	Overheat	1	1
KR14	Overload	5	3
KR15	Dokumentasi program yang tidak lengkap	5	2
KR16	Kesalahan pembuatan fungsi pada program	3	3
KR17	Tampilan program tidak user friendly	4	2
KR18	Penyelesaian program yang tidak tepat waktu	2	3
KR19	Petunjuk penggunaan program yang susah dipahami	1	2
KR20	Muncul anomali proses di lapangan yang tidak dapat diatasi oleh program	4	1
KR21	Kurangnya SDM secara kualitas/kuantitas	5	1
KR22	Pencurian perangkat/data	1	3
KR23	Banjir	4	3
KR24	Gempa bumi	1	5
KR25	Kebakaran	1	5
KR26	Petir	1	4

4.1.3 Evaluasi Risiko

Pada tahapan evaluasi risiko ini, kemungkinan-kemungkinan risiko yang sudah diidentifikasi serta dianalisis sebelumnya akan dimasukan ke dalam sebuah matrik evaluasi risiko berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*).

Pembentukan matrik evaluasi risiko didapat berdasarkan dari parameter evaluasi risiko yang sudah ditentukan. Secara lebih detail, parameter evaluasi risiko dapat dilihat pada Tabel 7 sementara untuk matrik evaluasi risiko berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*) dapat dilihat pada Tabel 8.

Tabel 7. Tabel Parameter Evaluasi Risiko

Likelihood	Impact	Level of risk
Rare	Insignificant	Low
Rare	Minor	
Rare	Moderate	
Unlikely	Insignificant	
Unlikely	Minor	
Possible	Insignificant	
Rare	Major	Medium
Rare	Catastrophic	
Unlikely	Moderate	
Unlikely	Major	
Unlikely	Catastrophic	
Possible	Minor	
Possible	Moderate	
Possible	Major	
Likely	Insignificant	
Likely	Minor	
Likely	Moderate	
Certain	Insignificant	
Certain	Minor	
Possible	Catastrophic	High
Likely	Major	
Likely	Catastrophic	
Certain	Moderate	
Certain	Major	
Certain	Catastrophic	

Tabel 8. Tabel Matrik Evaluasi Risiko Berdasarkan Likelihood dan Impact

Likelihood						
	Certain (5)	KR06 KR21	KR05 KR09 KR15	KR14		
	Likely (4)	KR20	KR17	KR23		KR12
	Possible (3)			KR16		
	Unlikely (2)		KR02	KR18		KR10
	Rare (1)	KR13	KR19	KR03 KR08 KR22	KR04 KR07 KR11 KR26	KR01 KR24 KR25
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
	Impact					

Setelah kemungkinan-kemungkinan risiko dimasukan ke dalam matrik evaluasi berdasarkan kemungkinan (*likelihood*) dan dampak (*impact*), baru kemudian

dievaluasi seperti pada Tabel 9 di bawah. Kemungkinan risiko disusun berdasarkan dari *level of risk* dengan tingkatan *high* hingga *low*.

Tabel 9. Tabel Evaluasi Kemungkinan Risiko Berdasarkan Likelihood dan Impact serta Level of Risk

ID	Kemungkinan Risiko	Likelihood	Impact	Level of risk
KR12	Listrik padam	4	5	High
KR14	Overload	5	3	High
KR01	Data corrupt	1	5	Medium
KR04	Program tidak dapat meningkatkan kualitas kinerja perusahaan	1	4	Medium
KR05	Web service mati secara tiba-tiba	5	2	Medium
KR06	Proses maintenance yang tidak terjadwal	5	1	Medium
KR07	Hacking terhadap jaringan	1	4	Medium
KR09	Server down	5	2	Medium
KR10	Koneksi jaringan terputus	2	5	Medium
KR11	Kerusakan hardware	1	4	Medium
KR15	Dokumentasi program yang tidak lengkap	5	2	Medium
KR16	Kesalahan pembuatan fungsi pada program	3	3	Medium
KR17	User interface rumit dan susah dipahami	4	2	Medium
KR18	Penyelesaian program yang tidak tepat waktu	2	3	Medium
KR20	Muncul anomali proses di lapangan yang tidak dapat diatasi oleh program	4	1	Medium
KR21	Kurangnya SDM secara kualitas/kuantitas	5	1	Medium
KR23	Banjir	4	3	Medium
KR24	Gempa bumi	1	5	Medium
KR25	Kebakaran	1	5	Medium
KR26	Petir	1	4	Medium
KR02	Kegagalan backup/generate data	2	2	Low
KR03	Kegagalan proses pemeliharaan dan continue development	1	3	Low
KR08	Memori penuh	1	3	Low
KR13	Overheat	1	1	Low
KR19	Petunjuk penggunaan program yang susah dipahami	1	2	Low
KR22	Pencurian perangkat/data	1	3	Low

Berdasarkan dari Tabel 9 di atas, dapat dilihat jika 2 (listrik padam dan *overload*) dari 26 kemungkinan risiko yang ada memiliki *level of risk* dengan tingkatan *high*, 18 (data *corrupt*, program tidak dapat meningkatkan kualitas kinerja perusahaan, *web service* mati secara tiba-tiba, proses *maintenance* yang tidak terjadwal, *hacking* terhadap jaringan, *server down,* koneksi jaringan terputus, kerusakan *hardware,* dokumentasi program yang tidak lengkap, kesalahan pembuatan fungsi pada program, *user interface* rumit dan susah dipahami, penyelesaian program yang tidak tepat waktu, muncul anomali proses di lapangan yang tidak dapat diatasi oleh program, kurangnya SDM secara kualitas/kuantitas, banjir, gempa bumi, kebakaran, dan petir) dari 26 kemungkinan risiko yang ada memiliki *level of risk* dengan tingkatan *medium*, dan 6 (kegagalan *backup/generate* data, kegagalan proses pemeliharaan dan *continue development*, memori penuh, *overheat,* petunjuk penggunaan program yang susah dipahami, dan pencurian perangkat/data) dari 26 kemungkinan risiko yang ada memiliki *level of risk* dengan tingkatan *low*.

4.2 Tahap Perlakuan Risiko

Pada tahapan ini, semua kemungkinan-kemungkinan risiko yang berada di sekitar dari aset-aset yang terkait dengan program HRMS akan diberikan usulan-usulan dalam memperlakukan kemungkinan-kemungkinan risiko tersebut dengan harapan bahwa usulan-usulan berikut ini dapat meminimalisir kemungkinan munculnya risiko-risiko tersebut sehingga program HRMS dapat berjalan secara optimal atau meminimalisir kerugian yang akan didapat oleh perusahaan ketika risiko-risiko tersebut muncul. Usulan perlakuan risiko disusun berdasarkan dari *level of risk* dengan tingkatan *high* hingga *low*. Detail dari usulan-usulan perlakuan risiko dapat dilihat pada Tabel 10.

Tabel 10. Tabel Usulan perlakuan risiko

ID	Kemungkinan Risiko	Level resiko	Perlakuan Risiko
KR05	Listrik padam	High	Penyediaan generator set dan UPS (Uninterruptible Power Supply) dengan daya yang disesuaikan terhadap kebutuhan seluruh perusahaan. Menggunakan 2 (dua) atau lebih sumber listrik dari gardu listrik yang dibedakan.
KR08	Overload	High	Menyusun jadwal pengecekan dalam 1 hari secara berkala terhadap db log, temp db log, CPU usage, dan RAM usage dari program HRMS dan database utama. Melakukan refresh terhadap db log, temp db log, CPU usage, dan RAM usage dari program HRMS dan database utama. Menambah personil di bagian database analyst agar dapat lebih sigap dalam mengatasi risiko tersebut.

KR01	Data corrupt	Medium	Melakukan backup data yang terdapat pada program HRMS dan database utama secara berkala. Selalu melakukan permbersihan pada PC agar mencegah munculnya virus/ malware yang dapat menyebabkan data corrupt.
KR04	Program tidak dapat meningkatkan kualitas kinerja perusahaan	Medium	Melakukan peningkatan kualitas dalam pendefinisian masalah dan pendesainan sistem sebelum diimplementasikan menjadi sebuah program. Melakukan pendokumentasian dan testing program secara lengkap dan menyeluruh sebelum program mulai dioperasikan.
KR05	Web service mati secara tiba-tiba	Medium	Memberikan pengumuman kepada user sebelum mengadakan maintenance. Pengumuman diinformasikan paling lambat 30 hingga 60 menit sebelum maintenance dimulai. Menyusun jadwal maintenance program secara berkala. Maintenance sebaiknya dijadwalkan pada saat jam istirahat karyawan.
KR06	Proses maintenance yang tidak terjadwal	Medium	Menyusun jadwal maintenance program secara berkala. Maintenance sebaiknya dijadwalkan pada saat jam istirahat karyawan. Memberikan pengumuman kepada user sebelum mengadakan maintenance. Pengumuman diinformasikan paling lambat 30 hingga 60 menit sebelum maintenance dimulai.
KR07	Hacking terhadap jaringan	Medium	Memasang password unik untuk setiap bagian penting dari komputer server. Selalu mengadakan maintenance terhadap jaringan secara berkala.
KR09	Server down	Medium	Melakukan pengecekan secara berkala dalam 1 hari terhadap db log, temp db log, CPU usage, dan RAM usage dari program HRMS dan database utama. Melakukan refresh terhadap db log, temp db log, CPU usage, dan RAM usage dari program HRMS dan database utama sebelum server down. masang antivirus yang berkualitas agar tidak terinfeksi malicious code.
KR10	Koneksi jaringan terputus	Medium	Segera melaporkan kepada bagian jaringan jika dirasa koneksi jaringan mengalami masalah.
KR11	Kerusakan hardware	Medium	Menjaga kebersihan dan penggunaan hardware-hardware yang ada. Segera melaporkan kepada bagian teknisi jika ditemukan hardware yang bermasalah agar bisa langsung ditanggulangi.
KR15	Dokumentasi program yang tidak lengkap	Medium	Menghilangkan stigma bahwa pendokumentasian sebuah program akan membuang banyak waktu dan tidak terlalu bermanfaat bagi perusahaan. Memberikan tanggung jawab pendokumentasian program kepada karyawan yang benar-benar menguasai mengenai hal tersebut.
KR16	Kesalahan pembuatan fungsi pada program	Medium	Melakukan peningkatan kualitas dalam pendefinisian masalah dan pendesainan sistem sebelum diimplementasikan menjadi sebuah program. Melakukan pendokumentasian dan testing program secara lengkap dan menyeluruh sebelum program mulai dioperasikan. Memberikan tanggung jawab pendesainan sebuah sistem kepada karyawan yang benar-benar menguasai mengenai hal tersebut supaya memudahkan bagi programmer dalam memahami desain yang telah dirancangkan shingga dapat mengimplementasikannya sesuai dengan keinginan user.
KR17	User interface rumit dan susah dipahami	Medium	Menyederhanakan pembuatan desain user interface supaya user bisa lebih cepat dalam memahami program tersebut. Memberikan pelatihan dan petunjuk penggunaan program kepada user.
KR18	Penyelesaian program yang tidak tepat waktu	Medium	Meningkatkan kualitas kontrol dan pengawasan ketika proses implementasi program berjalan. Mengadakan sistem reward and punishment kepada karyawan untuk meningkatkan motivasi

			dalam menyelesaikan tanggung jawab pekerjaannya tepat waktu.
KR20	Muncul anomali proses di lapangan yang tidak dapat diatasi oleh program	Medium	Merancangkan pembuatan program pendukung baru untuk mengatasi anomali proses yang tidak dapat diatasi oleh program sebelumnya. Memperbarui program yang ada agar dapat mengatasi anomali proses tersebut.
KR21	Kurangnya SDM secara kualitas/kuantitas	Medium	Melakukan perekrutan karyawan baru dengan menentukan standar-standar yang sesuai dengan kebutuhan perusahaan. Melakukan pelatihan kepada keryawan. Melakukan bimbingan kepada karyawan baru.
KR23	Banjir	Medium	Menyiapkan server cadangan di lokasi yang berbeda dengan server utama kemudian melakukan teknik mirroring database terhadap database HRMS sehingga data yang tersimpan di server utama juga otomatis tersimpan di server cadangan. Melakukan penyimpanan seluruh aset-aset perusahaan di tempat yang tinggi atau jauh dari jangkauan banjir.
KR24	Gempa bumi	Medium	Menyiapkan server cadangan di lokasi yang berbeda dengan server utama kemudian melakukan teknik mirroring database terhadap database HRMS sehingga data yang tersimpan di server utama juga otomatis tersimpan di server cadangan.
KR25	Kebakaran	Medium	Menyiapkan server cadangan di lokasi yang berbeda dengan server utama kemudian melakukan teknik mirroring database terhadap database HRMS sehingga data yang tersimpan di server utama juga otomatis tersimpan di server cadangan. Selalu mempesiapkan berbagai macam perlengkapan pemadam kebakaran di dalam gedung dan memperbarui perlengkapan-perlengkapan tersebut secara berkala.
KR26	Petir	Medium	Menyiapkan server cadangan di lokasi yang berbeda dengan server utama kemudian melakukan teknik mirroring database terhadap database HRMS sehingga data yang tersimpan di server utama juga otomatis tersimpan di server cadangan. Menyiapkan penangkal petir.
KR02	Kegagalan backup/generate data	Low	Selalu memperhatikan penggunaan memori penyimpanan yang dibutuhkan oleh database secara berkala agar jangan sampai penuh. Melakukan backup data yang terdapat di program HRMS dan database utama secara berkala. Membuat maintenance plan yang tepat guna.
KR03	Kegagalan proses pemeliharaan dan continue development	Low	Meningkatkan kinerja dalam kontrol dan pengawasan terhadap program setelah program dijalankan. Mencatat dan memperbaiki setiap permasalahan yang timbul.
KR08	Memori penuh	Low	Selalu memperhatikan penggunaan memori penyimpanan yang dibutuhkan oleh database secara berkala agar jangan sampai penuh. Menambah kapasitas memori sebelum penuh.
KR13	Overheat	Low	Menyiapkan mesin pendingin ruangan yang sesuai dengan kebutuhan agar hardware tidak mengalami overheat.
KR19	Petunjuk penggunaan program yang susah dipahami	Low	Menyederhanakan penggunaan bahasa pada petunjuk penggunaan program agar dapat dengan cepat dipahami oleh user.
KR22	Pencurian perangkat/data	Low	Memasang password unik untuk akses data penting dari bagian Software Development II dan Software Support 2. Password bisa dibuat dengan kombinasi huruf besar, huruf kecil, angka, dan tanda baca dengan minimal karakter untuk sebuah password adalah 10 karakter. Selalu mengadakan maintenance terhadap password untuk akses data penting dari bagian Software Development II dan Software Support 2 dengan cara mengganti password secara berkala.

	Menyiagakan security selama 24 jam. Gedung hanya dapat dimasuki dengan menggunakan kartu akses karyawan perusahaan. Merekam semua sudut gedung perusahaan dengan menggunakan CCTV.

5. Kesimpulan

5.1 Simpulan

Berdasarkan dari penelitian yang sudah dilakukan, analisis risiko teknologi informasi menggunakan ISO 31000 pada program *Human Resource Management System* (HRMS) di perusahaan retail di Indonesia dijalankan dengan menggunakan tahapan-tahapan yang dimulai dari tahap penilaian risiko yang terdiri dari tahap identifikasi risiko, tahap analisis risiko, dan tahap evaluasi risiko hingga tahap perlakuan risiko.

Dari hasil penelitian yang telah dilakukan, ditemukan terdapat 26 kemungkinan risiko yang berada di sekitar dari aset-aset yang terkait dengan program HRMS. Dari ke-26 kemungkinan risiko tersebut diketahui jika 2 kemungkinan risiko memiliki *level of risk* dengan tingkatan *high*, yaitu risiko listrik padam dan *overload*, 18 kemungkinan risiko yang memiliki *level of risk* dengan tingkatan *medium*, yaitu risiko data *corrupt*, program tidak dapat meningkatkan kualitas kinerja perusahaan, *web service* mati secara tiba-tiba, proses *maintenance* yang tidak terjadwal, *hacking* terhadap jaringan, *server down,* koneksi jaringan terputus, kerusakan *hardware,* dokumentasi program yang tidak lengkap, kesalahan pembuatan fungsi pada program, *user interface* rumit dan susah dipahami, penyelesaian program yang tidak tepat waktu, muncul anomali proses di lapangan yang tidak dapat diatasi oleh program, kurangnya SDM secara kualitas/kuantitas, banjir, gempa bumi, kebakaran, dan petir, serta 6 kemungkinan risiko yang memiliki *level of risk* dengan tingkatan *low*, yaitu risiko kegagalan *backup/generate* data, kegagalan proses pemeliharaan dan *continue development*, memori penuh, *overheat,* petunjuk penggunaan program yang susah dipahami, dan pencurian perangkat/data.

Sebenarnya proses penanggulangan yang dilakukan oleh perusahaan terhadap kemungkinan-kemungkinan risiko sudah berjalan, tapi proses penanggulangan yang dilakukan tersebut hanya berdasarkan dari pengalaman saja tanpa dilengkapi dengan dokumentasi yang baik terkait dengan manajemen risiko perusahaan. Dengan adanya penelitian ini diharapkan dapat digunakan sebagai alat bantu bagi pemangku kebijakan dari perusahaan untuk dapat menyusun dokumentasi-dokumentasi terkait dengan manajemen risiko perusahaan di kemudian hari.

5.2 Saran

Setelah melakukan penelitian analisis risiko teknologi informasi menggunakan ISO 31000 pada program Human Resource Management System (HRMS) di perusahaan retail di bagian *Software Development* II dan *Software Support* 2 ini, untuk peneliti di kemudian hari bisa melaksanakan penelitian dengan cakupan penelitian yang lebih luas sehingga temuan-temuan analisis risiko yang ada nantinya bisa dimanfaatkan oleh pemangku kebijakan untuk menyusun dokumentasi terkait dengan manajemen risiko perusahaan dan dokumentasi tersebut bisa diaplikasikan tidak hanya pada bagian-bagian tertentu saja melainkan bisa diaplikasikan untuk ke seluruh bagian dari perusahaan yang ada.

6. Daftar Rujukan

[1] Nice, F. L., Imbar, R. V., 2016, Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Mengunakan ISO 31000, *http://journal.uc.ac.id/index.php/JUISI/article/view/237*, diakses tanggal 22 September 2017.

[2] Husein, G. M., Imbar, R. V., 2015, Analisis Manajemen Risiko Teknologi Informasi Penerapan pada Document Management System di PT. Jabar Telematika (JATEL), *http://jutisi.maranatha.edu/index.php/jutisi/article/view/368*, diakses tanggal 22 September 2017.

[3] Harimurti, F., 2006, Manajemen Risiko, Fungsi dan Mekanismenya, *Jurnal Ekonomi dan Kewirausahaan*, no. 1, vol. 6, hal 105-112.

[4] Hasibuan, Z. A., 2007, Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi, *http://mhs.uks.ac.id/.../BUKU-METODE-PENELITIAN-PADA-BIDANG-IKOM-TI-ZAINA...*, diakses tanggal 22 September 2017.

[5] Amriani, Selvi, 2012, Analisis Risiko Teknologi Informasi Berbasis ISO 31000/31010 Studi Kasus: Lembaga Penelitian Perguruan Tinggi, *http://majour.maranatha.edu/index.php/jurnal-sistem-informasi/article/view/996*, diakses tanggal 13 November 2017.

[6] Joint Australian New Zealand International Standard, 2009, AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.

[7] Dali. Alex, 2012, "ISO 31000 Risk Management" The Golden Standard, vol. 45, no. 5.

[8] Knight, K. W., 2012, ISO 31000:2009; ISO/IES 31010 & ISO Guide 73:2009 International Standards for the Management of Risk, Presentation.

[9] Putra, I Gusti B. W., Muqtadiroh, F. A., Nisafani, A. S., 2016, Analisis Risiko pada Implementasi Perangkat Lunak di Lingkungan Pemerintahan dengan Menggunakan Framework ISO 31000:2009, http://*repository.its.ac.id/48855*, diakses tanggal 16 November 20