Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO *Office*

Sukma Arta Atmojo *[1], Augie David Manuputty[2]
[1,2]Universitas Kristen Satya Wacana;
Jl. Diponegoro No.52-60, Salatiga, Kec. Sidorejo, Kota Salatiga, Jawa Tengah 50711, (0298) 321212
[3]Jurusan Sistem Informasi, FTI UKSW, Salatiga
e-mail: *[1]atmojosukmaarta@gmail.com, [2]augiemanuputty@gmail.com

Abstrak

Penelitian ini memiliki tujuan untuk mengetahui dan mengidentifikasi kemungkinan-kemungkinan risiko teknologi informasi pada aplikasi AHO Office yang digunakan PT. SAT. Peneliti ingin mendokumentasi jenis-jenis risiko serta mengetahui cara penanganan terhadap risiko yang ada, menggunakan framework ISO 31000. Terdapat 3 proses besar didalamnya, ketiga proses tersebut yaitu menentukan konteks, penilaian risiko dan pengelolaan risiko. Untuk mengetahui jenis-jenis risiko dan cara penanganan risiko yang ada, peneliti menggunakan metode kualitatif, dengan cara melakukan wawancara dan observasi secara langsung untuk mengumpulkan data yang dibutuhkan. Setelah melakukan wawancara ditemukan 19 risiko yang berada di sekitar aset terkait aplikasi AHO Office, terdapat 3 risiko yang memiliki level of risk dengan tingkatan extreme risk, terdapat 7 risiko memiliki level of risk dengan tingkatan high risk, kemudian terdapat 7 risiko memiliki level of risk dengan tingkatan moderate risk, dan terdapat 2 risiko memiliki level of risk dengan tingkatan low risk. Hasil tersebut dapat digunakan sebagai alat bantu bagi pemangku kebijakan untuk menyusun dokumentasi terkait manajemen risiko perusahaan.

Kata kunci—Risiko, Proses Manajemen Risiko, ISO 31000

Abstract

This study aims to identify and identify possible information technology risks in the AHO Office application used by PT. SAT. Researchers want to document the types of risks and know how to handle existing risks, using the ISO 31000 framework. There are 3 major processes in it, the three processes are determining context, risk assessment and risk management. To find out the types of risks and ways of handling existing risks, researchers used qualitative methods, by conducting interviews and direct observation to collect the required data. After conducting the interview, it was found that 19 risks were found around the assets related to the AHO Office application, there were 3 risks that had a level of risk with an extreme risk level, there were 7 risks having a level of risk with a high risk level, then there were 7 risks having a level of risk moderate risk level, and there are 2 risks of having a level of risk with a low risk level. These results can be used as a tool for policy makers to prepare documentat on related to corporate risk management.

Keywords—*Risk, Risk Management Process, ISO 31000*

1. PENDAHULUAN

PT. Sumber Alfaria Trijaya, Tbk (SAT) merupakan salah satu perusahaan retail yang sudah terkenal di Indonesia. Perusahaan retail yang dimaksud ialah sebuah *brand minimarket*. *Brand minimarket* disini menjual segala macam jenis produk mulai dari *food*, *non-food* dan *grocery*. Perusahaan ini sudah memiliki banyak sekali gerai yang tersebar hampir di seluruh kota di Indonesia, kurang lebih memiliki 13.726 gerai dan untuk sekarang memiliki kurang lebih 32 cabang. Tentu saja perusahaan tersebut tidak terlepas dari adanya peran teknologi informasi. Penggunaan teknologi informasi apabila dapat dimaksimalkan akan menjadi nilai plus untuk perusahaan tersebut, tetapi tetap saja teknologi yang diterapkan di dalam perusahaan memiliki kekurangan. Kekurangan dari teknologi informasi tersebut dapat menimbulkan kemungkinan-kemungkinan ancaman maupun risiko, risiko tersebut tentu saja dapat mengganggu bisnis perusahaan. Tidak hanya teknologi informasi saja yang berperan penting dalam jalannya suatu perusahaan tetapi perlu adanya sumber daya manusia (SDM) yang kompeten, sistem dan infrastuktur yang ada di perusahaan juga harus memadai. PT. Sumber Alfaria Trijaya, Tbk (SAT) sendiri memiliki 12 divisi untuk menjalankan segalam macam jenis proses bisnis yang ada, pada penelitian ini peneliti lebih berfokus kepada divisi IT dan pada aplikasi AHO Office. Terdapat beberapa kendala di dalam divisi IT dan aplikasi AHO office antara lain kurangnya sumber daya manusia dari segi kuantitas, server yang digunakan untuk menjalankan aplikasi AHO office mengalami *down* dan kerusakan *hardware* yang digunakan untuk menajalankan aplikasi AHO office. Berdasarkan kendala yang ada, maka perlu adanya dokumentasi atas kemungkinan risiko dan memprioritas risiko tersebut dari tingkatan rendah, sedang kemudian tinggi. Pendokumentasian dan memprioritaskan risiko tersebut untuk acuan pemangku kebijakan dalam mengambil sebuah keputusan yang tepat sehingga tidak merugikan perusahaan kedepannya.

Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa pemanfaatan teknologi informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat. Tidak dapat dipungkuri lagi peran teknologi informasi sangat besar serta berdampak bagi perusahaan maupun bagi kehidupan bermasyarakat. Menurut *Oxford English Dictionary* (dalam Aziz, 2012) mendefinisikan Teknologi Informasi yaitu *hardware*, *software*, jaringan dan telekomunikasi yang biasanya dalam konteks bisnis. Teknologi informasi merupakan bagian dari usaha yang memanfaatkan perangkat elektronik komputer. Intinya istilah teknologi informasi merupakan teknologi yang memanfaatkan komputer sebagai perangkat utama untuk mengolah data menjadi informasi yang bermanfaat (dalam Aziz, 2012). [1]

2. METODE PENELITIAN

2.1 Penelitian Terdahulu

Penelitian oleh Aprilia Rahmawati pada tahun 2019 mengenai Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi iTop. Penelitian yang dilakukan memiliki tujuan untuk mendokumentasi kemungkinan risiko yang muncul, level dampak risiko serta rekomendasi terhadap perlakuan risiko yang dapat dilakukan. Dari hasil penelitian yang dilakukan pada aplikasi iTop menghasilkan analisis risiko yaitu 21 kemungkinan risiko yang mengganggu kinerja aplikasi iTop, 8 kemungkinan risiko termasuk dalam *level of risk* tingkat *medium*, serta terdapat 17 kemungkinan risiko termasuk dalam *level of risk* tingkat *low*. [2]

Stefan Agustinus juga melakukan penelitian mengenai Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program *Human Resources Management System* pada tahun 2017. Penelitian ini memiliki tujuan dapat mendokumentasikan risiko-risiko yang

dihadapai serta tindakan yang dapat dilakukan untuk meminimalisir risiko terhadap program HRMS. Penelitian yang telah dilakukan menghasilkan terdapat 26 kemungkinan risiko, 2 risiko memiliki *level of risk* dengan tingkatkan *high*, 18 kemungkinan risiko memiliki *level of risk* dengan tingkatan *medium*, serta 6 kemungkinan risiko memiliki *level of risk* dengan tingkatan *low*.[3]

Penelitian Analisis Risiko Teknologi Informasi menggunakan ISO 31000 juga dilakukan oleh Fransisca Lady Nice pada tahun 2016, studi kasus yang digunakan ialah *Website* SWIFTS pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN). Memiliki beberapa tujuan antara lain melaksanakan tahapan dan proses analisis risiko teknologi informasi berbasis *risk management* sesuai dengan standar dan kerangka kerja ISO 31000 pada *website* SWIFTS, serta mendokumentasi tingkat risiko dan perlakuan terhadap risiko teknologi informasi *website* SWIFTS. Penelitian yang dilakukan mendapatkan beberapa hasil diantaranya Analisis terhadap *website* SWIFTS dilakukan dalam beberapa tujuan antara lain komunikasi dan konsultasi, menetapkan konteks, *asesmen* risiko dan perlakuan risiko, Tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi adalah *asset*, baik data perangkat lunak, perangkat keras, sumber daya manusia dan prosedur yang terkait.[4]

2. 2 Landasan Teori

2. 2.1 Risiko

Definisi Risiko menurut Idroes (2008:4) (dalam Nurochman, 2014) merupakan bahaya, risiko yaitu suatu ancaman atau kemungkinan dari suatu tindakan yang akan memicu dampak yang bertolak belakang dengan tujuan yang akan dicapai.[5]

2. 2.2 Manajemen Risiko

Manajemen Risiko adalah aktivitas manajemen yang dilakukan berdasarkan tingkatan pada tingkat pimpinan pelaksana. Kegiatan penemuan serta analisis sistematis terhadap kerugian yang mungkin dihadapai oleh perusahaan atau organisasi. Dampak dari suatu risiko dan metode yang paling tepat untuk mengatasi kerugian tersebut dihubungkan terhadap tingkat keuntungan perusahaan atau organisasi (Harimurti, 2006). Stoneburner (2002:4) (dalam Nurochman 2014) melihat bahwa manajemen risiko dalam penerapan teknologi informasi di sebuah perusahaan atau organisasi ialah sebuah proses yang memungkinkan manajer teknologi informasi untuk menyetarakan biaya operasional dan biaya ekonomi sebagai langkah pengamanan dalam usaha melindungi sistem teknologi informasi dan data yang mendukung misi perusahaan atau organisasi.[5]

2. 2.3 Proses Manajemen Risiko

Menurut ISO 31000:2009, proses manajemen risiko adalah aktivitas kritikal dalam manajemen risiko, karena merupakan penerapan prinsip dan kerangka kerja yang sudah ada[6]. Proses manajemen risiko memiliki tiga proses besar, yaitu:

1. Menentukan konteks (*establishing the context)*
2. Penilaian risiko (*risk assessment*)
3. Pengelolaan risiko (*Risk treatment*)

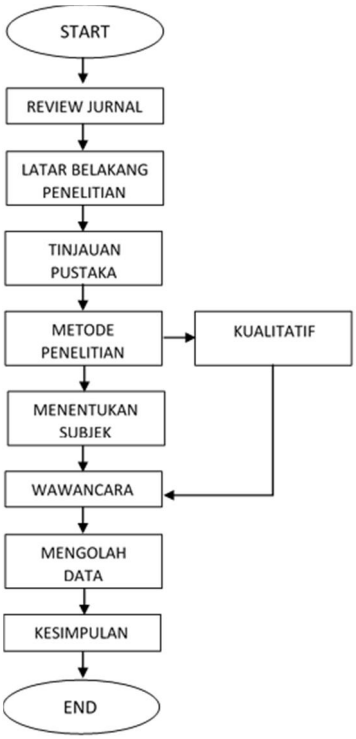
2. 2.4 Framework ISO 31000

ISO 31000 merupakan *standart* 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.

2.3 Metodologi Penelitian

Peneliti kali ini akan menggunakan metode kualitatif. Metode ini ialah memahami kejadian-kejadian apa saja yang dialami oleh subjek penelitian misalnya tingkah laku, presepsi, dan tindakan. Dapat disimpulkan metode kualitatif berakar dari latar alamiah sebagai keutuhan, menjadikan manusia sebagai alat penelitian. Sumber data utama metode kualitatif ialah kata-kata dan tindakan, keduanya berasal dari wawancara baik melalui rekaman *audio tapes, video recorder* dan kuesioner, sumber data tertulis (majalah ilmiah, sumber dari arsip, dokumen-dokumen resmi dan dokumen-dokumen pribadi), dapat juga berupa data statistik dan foto (misalnya data dari perusahaan, data dari kantor pemerintahan serta data statistik yang ada di dalam BPS) .(dalam Hasibuan, 2007).[7]

Peneliti mendapatkan data yang ada dengan cara melakukan observasi lapangan secara langsung dan wawancara. Wawancara dilakukan secara langsung, narasumber dari divisi IT bagian *Quality Assurance Analyst* dan divisi IT bagian *Website Programmer Analyst*. Peneliti melakukan beberapa tahap penelitian guna membantu selama proses pengerjaan penelitian, Gambar 1 di bawah ini merupakan alur tahap penelitian dari awal penelitian hingga akhir penelitian.



Gambar 1. Tahap Penelitian

3. HASIL DAN PEMBAHASAN

3.1 Penilaian Risiko (Risk Assessment)

Proses awal yang dilakukan oleh peneliti ialah penialain risiko karena dasar dari analisis manajemen risiko ISO 31000. Pada proses penilaian risiko ini memiliki 3 tahapan yang akan dilakukan peneliti antara lain identifikasi risiko, analisis risiko dan evaluasi risiko. Ketiga tahapan tersebut harus dilakukan agar dapat melangkah ke tahap selanjutnya.

3.1.1 Identifikasi Risiko

3.1.1.1 Identifikasi Aset AHO Office

Tahap pertama dalam penilaian risiko yaitu tahap identifikasi risiko aset-aset yang terkait dengan aplikasi AHO *office*. dapat berupa data, *hardware* dan *software*. Peneliti melakukan wawancara dan observasi agar mendapat data mengenai aset terkait aplikasi AHO *office*. Proses dilakukan dengan cara wawancara dan observasi kepada karyawan divisi IT bagian *Website Programmer Analyst* dan IT bagian *Quality Assurance Analyst*.

"Data yang ada di dalam aplikasi AHO office itu ada beberapa sih mas,antara lain data awal report problem, data awal report problem itu data problem yang diinputkan oleh pengguna aplikasi. Data solusi, di dalam aplikasi AHO office juga terdapat data solusi, yaitu data yang berisi solusi-solusi untuk menyelesaikan problem yang ada. Data list problem, Data departemen tujuan di data yang ini cuma ada (Divisi IT, Divisi Maintenance & Building, dan Divisi Learning & Development), terus ada data list aplikasi sama yang terakhir itu data history problem, di data history problem kita bisa lihat problem apa aja yang pernah ada selama ini." (IT Quality Assurance)

"Kalau di tempat kita hardware yang digunakan ada PC atau Laptop. Selama ini saya menggunakan PC untuk kerjaan saya, ada juga karyawan yang menggunakan laptop. Semuanya itu fasilitas dari kantor, selain PC juga terdapat UPS, switch, Pick to Light (PTL) sebagai penunjang. Kita juga memiliki ruang server sendiri, terpisah dari kantor utama, penempatan ruang server yang kita miliki menurut saya sudah bagus dan memiliki aturan yang ketat apabila ingin mengunjungi server utama." (IT Website Programmer)

Berikut rincian aset-aset terkait aplikasi AHO office berdasarkan percakapan dengan narasumber, dapat dilihat di "Tabel 1" di bawah ini:

Tabel 1. Identifikasi Aset AHO *Office*

Komponen Sistem Informasi	Aset AHO Office
Data	a. Data awal Report Problem b. Data List Aplikasi c. Data List Problem d. Data Departemen Tujuan e. Data Solusi Problem f. Data History Problem
Software	✓ Aplikasi AHO Office
Hardware	a. Personal Computer (PC) b. PTL (Pick to Light) c. UPS d. Switch e. Server Database f. Server Web Service

3.1.1.2 Identifikasi Risiko AHO Office

Tahap kedua dalam penilaian risiko yaitu tahap identifikasi risiko, tahap kedua peneliti melakukan identifikasi risiko terkait aplikasi AHO *office*. Penyebab risiko dapat muncul dari beberapa faktor, faktor tersebut antara lain dari lingkungan atau alam, manusia, sistem dan infrastruktur. Peneliti melakukan wawancara dan observasi agar mendapat data mengenai risiko terkait aplikasi AHO *office*. Proses dilakukan dengan cara wawancara dan observasi kepada karyawan divisi IT bagian *Website Programmer Analyst* dan IT bagian *Quality Assurance Analyst*.

"Ooo risiko ya mas, kalau itu ada mas. Risiko yang terdapat di aplikasi AHO office, antara lain tampilan aplikasi kurang user friendly, ada user yang bilang tampilan aplikasi kurang menarik tetapi ada juga user yang bilang kalau tampilaan aplikasi sudah bagus. Kalau itu balik lagi ke pribadi masing-masing sih mas. Disini juga sudah menerapkan pendokumentasian penggunaan aplikasi, tapi ya gitu mas ada beberapa dokumen yang belum dibuat karena satu dan lain hal. Penyalahgunaan hak akses, pencurian perangkat atau data, informasi penting diakses oleh pihak yang tidak bertanggung jawab, Ini sih mas kalau disini menurut saya kurang SDM terutama di bagian Quality Assurance soalnya yang pegang cuma saya. Kalau ada masalah langsung ke saya, saya koordinasinya sama developer. Ya cuma kita berdua aja yang paham sama alur penggunaan AHO office ini, untuk bagian Quality Assurance sendiri belum ada penerusnya sih mas pengennya ada yang nerusin selain saya. Butuh temen gitu lah mas, soalnya aplikasi ini cukup penting di perusahaan, Selama ini hardware yang saya pakai beberapa kal rusak, kalu disini rusak langsung lapor aja mas ke bagian teknisi tapi disini belum ada penjadwalan khusus buat maintenance hardware sih mas. Saya berharapnya ada jadwal maintenance hardware gitu mas biar lebih teratur. Selama ini jarang banget ada bencana alam yang sampai mengganggu proses bisnis perusahaan sih mas dari banjir maupun gempa bumi, tapi pernah kejadian kebakaran di gedung yang terdapat di server utama mas, tapi untungnya bukan ruang yang terdapat server utama kita, jadi di ruangan lain mas untungnya api cepet padam ga menjalar ke ruangan lain" (IT Quality Assurance)

"Selama saya kerja disini untuk komunikasi antar divisi bagus mas, yang penting disini tuh aktif tanya mas kalau semisal kurang paham sama kerjaan. Jangan diem aja kalau cuma diem aja ya kita nggaggepnya udah paham mas. Server utama kita pernah down mas setahun beberapa kali, kalau lagi down kita berhenti total mas ga bisa kerja juga buat proses di aplikasi AHO office." (IT Website Programmer)

Berdasarkan kutipan wawancara diatas, terdapat risiko yang berasal dari faktor manusia, lingkungan, sistem dan infrastruktur. Tetapi dari risiko - risiko tersebut belum adanya pendokumentasian yang digunakan sebagai acuan perusahaan untuk mengambil keputusan dalam jangka pendek maupun jangka panjang. Berikut rincian risiko-risiko terkait aplikasi AHO *office*, sebagaimana yang dapat dilihat di "Tabel 2" di bawah ini.

Tabel 2. Identifikasi Risiko AHO *Office*

ID	Risiko	Faktor
IR01	Penyalahgunaan hak akses	Manusia
IR02	Tampilan aplikasi kurang user friendly	
IR03	Dokumentasi penggunaan aplikasi yang kurang lengkap	
IR04	Penyelesaian program yang tidak sesuai jadwal	
IR05	Kurangnya SDM dari segi kuantitas	
IR06	Pencurian perangkat atau data	
IR07	Kurangnya komunikasi antar divisi yang terkait	
IR08	Informasi penting diakses oleh pihak yang tidak bertanggung jawab	
IR09	Kesalahan saat membuat fungsi pada program	
IR10	Kelalaian memasukan data pada program	
IR11	Gempa bumi	Lingkungan/Alam
IR12	Kebakaran	
IR13	Banjir	
IR14	Server down	Sistem dan Infrastruktur
IR15	Web service mati secara tiba-tiba	
IR16	Data corrupt	
IR17	Backup failure	
IR18	Kerusakan hardware	
IR19	Tidak ada maintenance hardware secara berkala	

3.1.1.3 Identifikasi Dampak Risiko

Tahap ketiga dalam penilaian risiko yaitu tahap identifikasi dampak risiko. Pada tahap ini peneliti mengidentifikasi dampak apa yang akan terjadi di aplikasi AHO *office* apabila risiko yang sebelumnya terjadi dan akan berdampak pada kinerja perusahaan. Berikut rincian dari dampak risiko - risiko aplikasi AHO *office*, terdapat di "Tabel 3".

Tabel 3. Identifikasi Dampak Risiko

ID	Risiko	Dampak
IR01	Penyalahgunaan hak akses	Data di dalam aplikasi AHO office dapat dihapus atau dirubah oleh pihak yang tidak bertanggung jawab.
IR02	Tampilan aplikasi kurang user friendly	Pengguna aplikasi AHO office mengalami kesulitan untuk pengoperasian aplikasi.
IR03	Dokumentasi penggunaan aplikasi yang kurang lengkap	Pengguna baru aplikasi AHO office sulit untuk memahami alur proses yang ada di dalam aplikasi.
IR04	Penyelesaian program yang tidak sesuai jadwal	Penyelesaian program tidak tepat waktu atau mundur dari jadwal yang sudah ada.
IR05	Kurangnya SDM dari segi kuantitas	Tidak ada penerus yang memahami alur kerja aplikasi AHO office secara keseluruhan
IR06	Pencurian perangkat atau data	Perusahaan rugi dari segi informasi dan segi finansial.
IR07	Kurangnya komunikasi antar divisi yang terkait	Sulit dalam pengambilan keputusan yang didasarkan kedua belah pihak.
IR08	Informasi penting diakses oleh pihak yang tidak bertanggung jawab	Data dapat dimanipulasi kemudian disebarkan untuk umum tetapi tidak sesuai data *real* yang ada.
IR09	Kesalahan saat membuat fungsi pada program	Menu/fitur yang terdapat di aplikasi AHO office tidak berjalan semestinya.
IR10	Kelalaian memasukan data pada program	Data yang dimasukan di aplikasi tidak sesuai dengan data yang ada di lapangan.
IR11	Gempa bumi	Infrastruktur perusahaan rusak dan aktivitas bisnis perusahaan terhenti.
IR12	Kebakaran	Infrastruktur perusahaan rusak dan aktivitas bisnis perusahaan terhenti
IR13	Banjir	Aktivitas bisnis perusahaan tersendat.
IR14	Server down	Tidak dapat mengakses database utama dan aplikasi AHO office.
IR15	Web service mati secara tiba-tiba	Tidak dapat mengakses database utama dan aplikasi AHO office.
IR16	Data corrupt	Proses aplikasi AHO office terhambat karena tidak ada data yang dapat diolah.
IR17	Backup data gagal	Tidak ada data cadangan apabila sewaktu-waktu diperlukan.
IR18	Kerusakan hardware	Menghambat dalam proses pengoperasian aplikasi AHO office.
IR19	Tidak ada maintenance hardware secara berkala	Tidak dapat mengetahui penyebab dari rusaknya hardware.

3.1.2 Analisis Risiko

Proses kedua atau proses setelah selesainya identifikasi risiko adalah proses analisis risiko. Proses analisis risiko adalah proses mengukur risiko dengan cara melihat dua aspek yaitu kemungkinan seberapa besar kerusakan yang terjadi (*impact*) dan seberapa sering risiko tersebut terjadi (*likelihood*). Hasil dari proses analisis risiko dapat digunakan sebagai saran dalam proses evaluasi risiko dan dalam proses mengelola risiko yang ada. Di dalam proses ini terdapat dua

tabel yaitu tabel *impact* dan tabel *likelihood*. Tabel *impact* terdapat di "Tabel 4" sedangkan tabel *likelihood* terdapat di "Tabel 5"[8]

Tabel 4. *Likelihood*

Likelihood		Keterangan	Frekuensi Kejadian
Nilai	Kriteria		
1	Rare	Risiko yang ada hampir tidak pernah terjadi	> 18 bulan
2	Unlikely	Risiko yang ada jarang terjadi	12-17 bulan
3	Possible	Risiko yang ada kadang terjadi	9-11 bulan
4	Likely	Risiko yang ada sering terjadi	5-8 bulan
5	Almost Certain	Risiko yang ada tidak diragukan lagi akan terjadi	1-4 bulan

Tabel 5. *Impact*

Impact		Keterangan
Nilai	Kriteria	
1	Negligible	Risiko yang terjadi tidak mengganggu aktivitas bisnis perusahaan dan jalannya pengoperasian aplikasi.
2	Minor	Risiko yang terjadi mulai sedikit mengganggu aktivitas bisnis perusahaan dan sedikit menghambat jalannya pengoperasian aplikasi.
3	Moderate	Risiko yang terjadi mulai mengganggu sebagian aktivitas bisnis perusahaan dan menghambat sebagian jalannya pengoperasian aplikasi.
4	Major	Risiko yang terjadi mulai mengganggu aktivitias bisnis perusahaan dan mengganggu jalannya pengoperasian aplikasi sehingga menyebabkan hambatan.
5	Catastrophic	Risiko yang terjadi benar-benar mengganggu dan menhambat aktivitas bisnis perusahaan menyebabkan aktivitas bisnis perusahaan berhenti secara menyeluruh.

Proses analisi risiko kali ini berdasarkan risiko-risiko yang telah diidentifikasi pada aplikasi AHO *office* dengan menggunakan metode wawancara dan observasi lapangan. Proses dilakukan dengan cara wawancara dan observasi kepada karyawan divisi IT bagian *Website Programmer Analyst* dan *Quality Assurance Analyst*.

"*Kalau dilihat dari frekuensi kejadiannya ya mas, ada beberapa risiko yang jarang sekali terjadi atau tidak pernah kejadian selama saya kerja disini mas. Contohnya pencurian perangkat atau data, informasi penting bocor atau disebarkan sama pihak tidak bertanggung jawab, dan penyalahgunaan hak akses. Disini akses ke suatu aplikasi sudah diatur mas, ada grade tertentu mas dalam mengakses aplikasi tersebut. Kalau dari bencana alam yang sampai mengganggu perusahaan atau meliburkan karyawan, saya belum pernah ngalamin sih mas, selama ini masih aman mas. Tapi ada juga beberapa risiko yang kadang-kadang kejadian tuh mas malah ada yang sering terjadi disini, antara lain ini mas. Pendokumentasian penggunaan aplikasi yang kurang lengkap, soalnya kan aplikasi ada tambahan fitur atau fitur yang dirubah tetapi belum sempat membikin dokumennya mas. Kalau buat orang lama yang udah sering pakai aplikasi masih paham mas tapi kalau orang baru pasti bingung mas. Ooo iya mas kalau risiko yang pasti terjadi itu ada server down setahun bisa 2 atau 3 kali mas, karena satu dan lain hal. Dari segi kuantitas SDM menurut saya kurang mas, terutama di bagian Quality Assurance, dari awal masuk sampai sekarang belum ada partner buat bantuin mengelola aplikasi AHO office ini mas, kalau buat koordinasi saya langsung ke bagian Website Programmer aja mas..*" *(IT Quality Assurance)*

"Salah bikin fungsi dan lalai memasukan data sering terjadi mas, apa lagi pas kondisi badan kurang fit atau sakit tapi deadline udah deket mau gamau harus cepet selesai malah banyak salahnya pas ngoding mas. Sekarang kita ngomongin soal hardware ya mas, disini hardware yang digunakan udah bagus mas, udah sesuai kebutuhan juga, missal hardware yang kita pakai rusak langsung lapor bagian teknisi mas untuk minta tolong dibenerin ya kalau udah ga bisa dibenerin ya harus nunggu hardware baru mas. Disini belum nerapin penjadwalan buat hardware mas, jadi kita by request aja." (IT Website Programmer)

Berdasarkan kutipan wawancara diatas perlu adanya tindak lanjut untuk risiko - risiko tersebut, sehingga risiko tersebut tidak mengganggu aktivitas jalannya aplikasi dan menyebabkan aktivitas perusahaan berhenti secara sementara maupun berhenti total. Berikut rincian dari penilaian risiko dengan *Impact* dan *Likelihood*, dapat dilihat di "Tabel 6".

Tabel 6. Penilaian Risiko Dengan *Impact* dan *Likelihood*

ID	Risiko	Impact	Likelihood
IR01	Penyalahgunaan hak akses	2	2
IR02	Tampilan aplikasi kurang user friendly	1	3
IR03	Dokumentasi penggunaan aplikasi yang kurang lengkap	2	4
IR04	Penyelesaian program yang tidak sesuai jadwal	3	3
IR05	Kurangnya SDM dari segi kuantitas	4	5
IR06	Pencurian perangkat atau data	3	2
IR07	Kurangnya komunikasi antar divisi yang terkait	3	2
IR08	Informasi penting diakses oleh pihak yang tidak bertanggung jawab	2	2
IR09	Kesalahan saat membuat fungsi pada program	3	3
IR10	Kelalaian memasukan data pada program	3	4
IR11	Gempa bumi	5	1
IR12	Kebakaran	5	1
IR13	Banjir	2	1
IR14	Server down	4	4
IR15	Web service mati secara tiba-tiba	3	4
IR16	Data corrupt	5	2
IR17	Backup data gagal	2	2
IR18	Kerusakan hardware	5	3
IR19	Tidak ada maintenance hardware secara berkala	2	5

3.1.3 Evaluasi Risiko

Proses ketiga yang ada didalam proses penilaian risiko adalah evaluasi risiko. Evaluasi risiko adalah proses dimana peneliti mulai menentukan risiko mana yang perlu diprioritaskan dan membutuhkan perlakuan secara khusus. Disini peneliti menggunakan tabel matriks risiko untuk mendukung dalam penentuan pengambilan risiko.

Tabel matriks risiko berisi gabungan dari seberapa besar kerusakan yang terjadi (*impact*) dan seberapa sering risiko terjadi (*likelihood*) didasarkan pada hasil identifikasi risiko yang sudah dilakukan sebelumnya. Peringkat risiko merupakan hasil perkalian dari *impact* dan *likelihood*, didalam peringkat risiko dibagi kedalam empat tingkatan yaitu *low risk, moderate risk, high risk, extreme risk.* Tabel matriks evaluasi risiko terdapat di tabel "Tabel 7". [9]

Keterangan tabel matriks risiko:

1-3	Low risk
4-6	Moderate risk
8-12	High risk
15-25	Extreme risk

Tabel 7. Matriks Evaluasi Risiko

Impact	Likelihood				
	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Catastrophic (5)	IR11 IR12	IR16	IR18		
Major (4)				IR14	IR05
Moderate (3)		IR06 IR07	IR04 IR09	IR10 IR15	
Minor (2)	IR13	IR01 IR08 IR17		IR03	IR19
Negligible (1)			IR02		

Risiko-risiko yang ada di sekitar AHO *office* sudah dimasukan ke dalam tabel matriks evaluasi risiko didasarkan pada seberapa besar kerusakan yang terjadi (*impact*) dan seberapa sering risiko terjadi (*likelihood*). Risiko tersebut kemudian di klasifikasikan berdasarkan *risk level* yang paling atas sampai yang paling bawah (*extreme risk, high risk, moderate risko*, dan *low risk*).[10] Detail *risk level* terdapat di "Tabel 8" berikut ini.

Tabel 8. Tingkatan Risiko

ID	Risiko	Impact	Likelihood	Risk level
IR05	Kurangnya SDM dari segi kuantitas	4	5	Extreme risk
IR14	Server down	4	4	Extreme risk
IR18	Kerusakan hardware	5	3	Extreme risk
IR03	Dokumentasi penggunaan aplikasi yang kurang lengkap	2	4	High risk
IR04	Penyelesaian program yang tidak sesuai jadwal	3	3	High risk
IR09	Kesalahan saat membuat fungsi pada program	3	3	High risk
IR10	Kelalaian memasukan data pada program	3	4	High risk
IR15	Web service mati secara tiba-tiba	3	4	High risk
IR16	Data corrupt	5	2	High risk
IR19	Tidak ada maintenance hardware secara berkala	2	5	High risk
IR01	Penyalahgunaan hak akses	2	2	Moderate risk
IR06	Pencurian perangkat atau data	3	2	Moderate risk
IR07	Kurangnya komunikasi antar divisi yang terkait	3	2	Moderate risk
IR08	Informasi penting diakses oleh pihak yang tidak bertanggung jawab	2	2	Moderate risk
IR11	Gempa bumi	5	1	Moderate risk
IR12	Kebakaran	5	1	Moderate risk
IR17	Backup data gagal	2	2	Moderate risk
IR02	Tampilan aplikasi kurang user friendly	1	3	Low risk
IR13	Banjir	2	1	Low risk

3.2 Pengelolaan Risiko (Risk Treatment)

Proses akhir yang dilakukan dalam penelitian ini adalah proses pengelolaan risiko, peneliti sudah melalui beberapa proses sehingga dapat sampai di proses ini. Peneliti akan memberikan usulan - usulan mengenai pengelolaan risiko terkait risiko yang sudah diidentifikasi sebelumnya, peneliti berharap dengan adanya usulan-usulan pengelolaan risiko dapat berdampak ke aplikasi AHO *office* sehingga pengoperasian aplikasi dan aktivitas proses bisnis berjalan secara optimal serta kerugian atas risiko - risiko tersebut dapat diminimalisir. Usulan pengelolaan risiko diurutkan dari *risk level* yang tertinggi yaitu *extreme risk* kemudian turun sampai risk level terendah yaitu *low risk*. Rincian dari usulan pengelolaan risiko dapat dilihat pada "Tabel 9" di bawah ini.

Tabel 9. Usulan Pengelolaan Risiko

ID	Risiko	Risk Level	Pengelolaan Risiko
IR05	Kurangnya SDM dari segi kuantitas	Extreme risk	Menambah karyawan baru berdasrkan standar yang sudah ditentukan sebelumnya, sehingga ada *partner* dan penerus yang memahami proses kerja aplikasi AHO office secara menyeluruh.
IR14	Server down	Extreme risk	Perlu adanya pengecekan server secara berkala dan adanya jadwal *maintenance* server yang jelas, sehingga semua *user* aplikasi AHO office dapat mengetahui jauh - jauh hari.
IR18	Kerusakan hardware	Extreme risk	*Hardware* yang rusak segera dilaporkan ke bagian teknisi apabila *hardware* tidak dapat diperbaiki maka pengguna mengurus permintaan barang baru sehingga tidak menghambat kinerja.
IR03	Dokumentasi penggunaan aplikasi yang kurang lengkap	High risk	Setiap ada menu/fitur baru di aplikasi AHO office langsung dikoordinasikan ke bagian dokumentasi sehingga bagian dokumentasi langsung membuat dokumen penggunaan aplikasi yang paling *update*.
IR04	Penyelesaian program yang tidak sesuai jadwal	High risk	Perlu adanya pemantauan terhadap programmer yang bertanggung jawab atas program tersebut dan diberlakukannya sistem *punishment* dan *reward* kepada programmer sehingga motivasi meningkat.
IR09	Kesalahan saat membuat fungsi pada program	High risk	Setiap penjelasan masalah yang ada harus lebih rinci, menyerahkan tanggung jawab kepada *programmer* yang benar - benar menguasai hal tersebut menghidari teradinya *miss communication* antar divisi yang terkait.
IR10	Kelalaian memasukan data pada program	High risk	Sebelum menyelesaikan program dicek terlebih dahulu dan meningkatkan fokus saat membuat program, mengurangi hal - hal yang tidak berangkutan dengan program.
IR15	Web service mati secara tiba-tiba	High risk	Memberikan info terlebih dahulu kepada semua *user* sebelum adanya *maintenance*, sebaiknya 1 atau 2 hari sebelum *maintenance*. Perlu adanya jadwal *maintenance* server secara berkala.
IR16	Data corrupt	High risk	Membuat jadwal backup data secara berkala.

IR19	Tidak ada maintenance hardware secara berkala	High risk	Perlu adanya jadwal *maintenance hardware* secara berkala, dengan adanya jadwal *maintenance hardware* teknisi dapat memantau *hardware* mana saja yang perlu diperbaik dan diganti dengan *hardware* yang baru.
IR01	Penyalahgunaan hak akses	Moderate risk	Membatasi beberapa *user* dalam mengakses aplikasi, memberikan akses kepada *user* yang benar - benar bertanggung jawab dan dipercaya.
IR06	Pencurian perangkat atau data	Moderate risk	*Password* dirubah secara berkala, menghindari *user* yang tidak bertanggung jawab. Mempercayakan data penting kepada *user* yang bertanggung jawab dan dapat dipercaya.

4. KESIMPULAN

Penelitian yang sudah dilakukan peneliti kali ini merupakan analisis risiko teknologi informasi di PT. Sumber Alfaria Trijaya, Tbk (SAT) pada aplikasi AHO *office* menggunakan ISO 31000. Peneliti melalui beberapa proses. Proses awal yang dilakukan peneliti adalah penilaian risiko di dalam penilaian risiko terdapat beberapa proses yaitu identifikasi risiko, analisis risiko dan evaluasi risiko, kemudian proses kedua adalah pengelolaan risiko. Peneliti mendapat beberapa hasil temuan yang telah dilakukan melalui proses - proses yang ada. Ditemukan 19 risiko yang berada di sekitar aset terkait aplikasi AHO *office*, dari ke-19 risiko terdapat 3 risiko memiliki *level of risk* dengan tingkatan *extreme risk*. Ketiga risiko tersebut adalah kurangnya SDM dari segi kuantitas, server down dan kerusakan *hardware*. Terdapat 7 risiko memiliki *level of risk* dengan tingkatan *high risk*. Ketujuh risiko tersebut adalah dokumentasi penggunaan aplikasi yang kurang lengkap, penyelesaian program yang tidak sesuai jadwal, kesalahan saat membuat fungsi pada program, kelalaian memasukan data pada program, *web service* mati secara tiba-tiba, *data corrupt* dan tidak ada *maintenance hardware* secara berkala. Selanjutnya terdapat 7 risiko yang memiliki *level of risk* dengan tingkatan *moderate risk*. Risiko tersebut yaitu penyalahgunaan hak akses, pencurian perangkat atau data, kurangnya komunikasi antar divisi yang terkait, informasi penting diakses oleh pihak yang tidak bertanggung jawab, gempa bumi, kebakaran dan *backup* data gagal. Serta terdapat 2 risiko memiliki *level of risk* dengan tingkatan *low risk*, kedua risiko tersebut yaitu tampilan aplikasi kurang *user friendly* dan banjir.

Proses pengelolaan risiko terhadap risiko - risiko yang ada di sekitar aset aplikasi AHO *office* sudah berjalan, tetapi proses pengelolaan risiko tersebut berdasarkan pengalaman saja tanpa adanya dokumentasi yang jelas terkait manajemen risiko perusahaan. Peneliti melakukan penelitian ini diharapkan dapat berguna sebagai alat bantu untuk pengambilan keputusan kebijakan perusahaan dan dapat membuat dokumentasi terkait dengan manajemen risiko untuk jangka panjang.

5. SARAN

Setelah peneliti menyelesaikan penelitian analisis manajemen risiko teknologi informasi menggunakan ISO 31000 pada aplikasi AHO office di PT.SAT, untuk peneliti di kemudian hari dapat melakukan penelitian dengan cakupan lebih luas sehingga temuan-temuan yang ada dapat digunakan oleh pemangku kebijakan untuk menyusun dokumentasi terkait dengan manajemen risiko perusahaan.

UCAPAN TERIMA KASIH

Penulis mengucapkan banyak terima kasih kepada Tuhan Yang Maha Esa atas penyertaan dan kekuatan yang telah diberikan sehingga penulis dapat menyelesaikan jurnal ini. Penulis juga mengucapkan terima kasih kepada keluarga, dosen pembinbing, mentor di kantor, narasumber yang bersedia menyediakan waktunya untuk melakukan wawancara dan teman-teman terdekat. Sekali lagi terima kasih yang sebesar-besarnya kepada semua yang terlibat dalam penulisan yang selalu memberikan dukungan kepada penulis.

DAFTAR PUSTAKA

[1] A. Aziz, "*Pemanfaatan Teknologi Informasi Dalam Pengembangan Bisnis Pos*," *Bul. Pos dan Telekomun.*, Vol. 10, No. 1, p. 35, 2015, doi: 10.17933/bpostel.2012.100104.

[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] 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.

[5] A. Nurochman, "*Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan Universitas Gadjah Mada)*," *Berk. Ilmu Perpust. dan Inf.*, Vol. 10, No. 2, p. 1, 2016, doi: 10.22146/bip.8830.

[6] A. N. Rilyani, Y. AW Firdaus, and D. D. Jatmiko, "*Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000*," *e-Proceeding Eng.*, Vol. 2, No. 2, pp. 1–8, 2015.

[7] Z. A. Hasibuan, "*Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi," Konsep, Tek. dan Apl.*, No. Universitas Indonesia, p. 194, 2007.

[8] I. G. Bagus and W. Putra, "*Pemerintahan Dengan Menggunakan Framework Iso 31000 : 2009 of Software Analysis Implementation on Government Environment By Using Iso 31000 : 2009*," 2015.

[9] 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.

[10] NPSA, "*A Risk Matrix for Risk Managers*," *Npsa*, No. January, pp. 1–18, 2008.