ANALISIS RISIKO TEKNOLOGI INFORMASI PADA APLIKASI SAP DI PT SERASI AUTORAYA MENGGUNAKAN ISO 31000

Grialdo Willy Lantang [1)], Ariya Dwika Cahyono[2)], dan **Melkior Nikolar Ngalumsine Sitokdana[3)]**

[1,3] Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
[2] Program Studi Komputerisasi Akuntansi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
[1,2,3] Jl. Blotongan, Sidorejo Lor, Sidorejo, Kota Salatiga, Jawa Tengah 50714
E-mail: 682015048@student.uksw.edu[1)], ariyadc@uksw.edu[2)], melkior.sitokdana@uksw.edu[3)]

ABSTRAK

Program *System Application and Processing* (SAP) merupakan *software* utama yang digunakan di PT. Serasi Autoraya. Analisis risiko yang digunakan pada PT. Serasi Autoraya adalah ISO 31000. 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. Proses ini melakukan 3 tahapan yaitu, Identifikasi Risiko (*Risk Identification*), Analisis Risiko (*Risk Analyst*), Evaluasi Risiko (*Risk Evaluation*). Kemudian Tahap yang kedua adalah perlakuan pada risiko *(Risk Treatment*). Serangkaian proses yang berdasarkan pada ISO 31000, didapatkan hasil tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi yaitu listrik dan koneksi internet. Dua hal tersebut harus mendapat perhatian khusus karena sangat mengganggu aktivitas yang ada. Kemudian tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang menengah yaitu, data corrupt, *overheat*, kerusakan perangkat keras, gempa bumi, kebakaran, petir, peretasan terhadap jaringan. Terakhir tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang rendah yaitu *web service* mati, pencurian perangkat keras, pencurian data, memori penuh, kurangnya Sumber Daya Manusia dan banjir.

Kata Kunci: *Risiko, Teknologi Informasi, ISO 31000*

1. PENDAHULUAN

Teknologi Informasi dan Sistem Informasi yang berkembang sangat pesat dan canggih merupakan peluang yang dapat diandalkan untuk mendukung berbagai aktivitas organisasi. Peran aplikasi teknologi informasi saat ini sudah menjadi suatu kebutuhan yang tidak dapat dipisahkan, sekaligus menjadi tempat bergantung para penggunanya untuk menyelesaikan berbagai permasalahan. Salah satu organisasi yang memanfaatkan teknologi informasi adalah PT. Serasi Autoraya.

PT. Serasi Autoraya adalah perusahaan yang bergerak dibidang jasa transportasi yang beralamat di Kawasan Candi Kota Semarang, Jawa Tengah. Kini PT. Serasi Autoraya memiliki 34 cabang dan 68 autlet yang tersebar di seluruh wilayah nusantara. PT. Serasi Autoraya mengunakan Teknologi Informasi berupa aplikasi *System Application and Processing* (SAP) untuk menunjang segala kegiatan administrasi. Namun tidak dapat dipungkiri bahwa ada beberapa ancaman-ancaman risiko yang muncul dan menggangu aktifitas dalam sistem SAP, seperti fasilitas perangkat komputer yang belum memadai, pasokan listrik dan sumber daya manusianya yang dapat menyebabkan aktifitas tidak berjalan secara optimal, dan sebagainya. Oleh karena itu, dilakukan penelitian untuk menganalisis Manajemen Risiko pada aplikasi SAP dengan mengidentifikasi kemungkin risiko yang ada, dampak yang mungkin terjadi, penilaian dan evaluasi risiko serta apa yang akan dilakukan untuk mengantisipasi risiko dan permasalahan yang ada.

Penelitian tentang Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 bukan merupakan penelitian terbaru, maka beberapa penelitian terdahulu dijadikan sebagai acuan dalam penelitian ini, yaitu:

Penelitian tentang Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS. 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 (Agustinus, Nugroho and Cahyono, 2017).

Penelitian tentang Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) Pada Website SWIFTS Menggunakan ISO 31000. Penerapan dari analisis risiko meliputi identifikasi risiko, penilaian risiko dan pemeliharaan risiko. Berdasarkan hasil analisis didapatkan nilai risiko yang telah terdokumentasi, sehingga LAPAN dapat melakukan pencegahan, penanganan dan pemeliharaan terhadap sistem dan aset pendukung kinerja sistem di masa depan. Aset memiliki nilai kemungkinan dan nilai dampak yang tinggi, baik data perangkat lunak, perangkat keras, sumber daya manusia dan prosedur yang terkait pada sistem SWIFtS yang dinilai dapat mengganggu proses bisnis LAPAN itu sendiri. Sehingga diperlukan peninjauan kembali dan penerapan pada perlakuan risiko yang disarankan (Nice and Imbar, 2016).

Penelitian tentang Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus: Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square). Pada penelitian ini mencoba mengimplementasikan suatu analisis manajemen risiko menggunakan ISO 31000 yang dapat digunakan untuk mengelola risiko secara keseluruhan pada suatu area kegiatan sehingga perusahaan dapat melakukan pencegahan, penanganan, serta perbaikan kedepannya. Analisis risiko menggunakan ISO 31000 terlihat nilai risiko dengan tiga tingkatan yaitu rendah, sedang, dan tinggi. Berdasarkan hasil analisis, rekomendasi pengendalian yang tepat seperti risk reduction untuk risiko *human error* (kesalahan dalam mengoperasikan sistem), *risk avoidance* untuk risiko pencurian *password* otorisasi, serta *risk reduction* untuk risiko koneksi yang tidak stabil (Talitha, Driantami and Perdanakusuma, 2018).

Berdasarkan beberapa penelitian yang terdahulu, maka dilakukan penelitian tentang risiko teknologi informasi, khususnya risiko terhadap *System Application and Processing* (SAP). Penelitian tentang hal tersebut belum pernah dilakukan oleh peneliti sebelumnya, maka penelitian ini masih baru dan tentunya memberikan sumbangsih positif karena mengevaluasi aplikasi utama yang digunakan perusahaan. Dalam penelitian ini dilakukan identifikasi aset teknologi informasi yang ada dan mengidentifikasi kemungkin risiko yang ada, dampak yang mungkin terjadi, penilaian dan evaluasi risiko serta apa yang akan dilakukan untuk mengantisipasi risiko tersebut. Penelitian ini bertujuan untuk mendokumentasikan risiko yang mungkin terjadi dan mengusulkan perlakuan risiko untuk semua kemungkinan risiko yang akan bermunculan, baik yang sudah pernah terjadi maupun yang belum pernah terjadi.

2. RUANG LINGKUP

Ruang lingkup penelitian ini adalah sebagai berikut:

1. Cakupan permasalahannya adalah: terdapat berbagai risiko yang dapat menganggu aktivitas PT. Serasi Autoraya, terutama risiko penggunaan *System Application and Processing* (SAP). Oleh karena itu, dilakukan analisis Risiko Teknologi Informasi Berbasis *Risk Management* Menggunakan ISO 31000.
2. Batasan penelitian ini adalah hanya fokus menganalisis risiko pada *System Application and Processing* (SAP)
3. Rencana hasil yang didapatkan dari penelitian ini adalah mengidentifikasi risiko yang mengganggu implementasi *System Application and Processing* dan memberikan rekomendasikan perlakuan setiap risiko

3. BAHAN DAN METODE

Berikut disajikan bahan kajian, metode dan tahapan penelitian yang dilakukan

3.1 Risiko Sistem informasi

Risiko adalah kemungkinan terjadinya peristiwa yang dapat merugikan perusahaan. Risiko pada hakikatnya merupakan kejadian yang mempunyai dampak negatif terhadap sasaran dan strategi perusahaan. Kemungkinan terjadinya risiko dan akibatnya terhadap bisnis merupakan hal mendasar untuk diidentifikasi dan diukur. Menurut Sutanto (2012), risiko merupakan kombinasi dari kemungkinan dan keparahan dari suatu kejadian. Besarnya risiko ditentukan oleh berbagai faktor, seperti besarnya paparan, lokasi, pengguna, kuantitas serta kerentanan unsur yang terlibat (Sirait and Susanty, 2016).

. Sedangkan menurut Hanggraeni (2010) dalam Suhendra dkk (2013), manajemen risiko merupakan suatu rangkaian prosedur dan metodologi yang digunakan untuk mengidentifikasi, mengukur, memonitor dan mengontrol risiko yang timbul dari bisnis operasional perusahaan(Suhendra, Oswari and Setiawan, 2013). Sasaran dari pelaksanaan manajemen risiko adalah mengurangi risiko yang berbeda-beda yang berkaitan dengan bidang yang telah dipilih pada tingkat yang dapat diterima oleh masyarakat. Hal ini dapat berupa berbagai jenis ancaman yang disebabkan oleh lingkungan, teknologi, manusia, organisasi dan politik. Di sisi lain pelaksanaan manajemen risiko melibatkan segala cara yang tersedia bagi manusia, khususnya, bagi entitas manajemen risiko (manusia, staf, dan organisasi)(Sirait and Susanty, 2016).

Teknologi Informasi memiliki risiko yang mengakibatkan kerugian bagi organisasi. Menurut Jakaria, dkk (2013), ada dua risiko, yaitu risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam *(natural disaster)*,pencurian *(theft)*, kebakaran

(fires), lonjakan arus listrik *(power surge)*, dan perusakan *(vandalism)*. Hal ini tentunya akan berpengaruh terhadap perangkat keras yang ada. Sedangkan risiko kerusakan yang lainnya adalah risiko kerusakan logik yang mengacu pada proses yang terjadi dalam sistem informasi dan data (Ernawati and Santoso, 2017).

Pengertian Sistem informasi menurut Bodnar dan Hopwood (1993) adalah kumpulan perangkat keras dan perangkat lunak yang dirancang untuk mentransformasikan data ke dalam bentuk informasi yang berguna. Sedangkan pengertian teknologi informasi menurut Alter (1992), mencakup perangkat keras dan perangkat lunak untuk melaksanakan satu atau sejumlah tugas pemrosesan data seperti menangkap, mentransmisikan, menyimpan, mengambil, memanipulasi, atau menampilkan data (Kadir, 2014).

3.2 ISO 31000

ISO 31000 adalah suatu standar implementasi manajemen risiko yang diterbitkan oleh International Organization for Standardization pada tanggal 13 November 2009. Standar ini ditujukan untuk dapat diterapkan dan disesuaikan untuk semua jenis organisasi dengan memberikan struktur dan pedoman yang berlaku generik terhadap semua operasi yang terkait dengan manajemen risiko. Menurut ISO 31000, manajemen risiko suatu organisasi harus mengikuti 11 prinsip dasar agar dapat dilaksanakan secara efektif. Berikut penjabaran prinsip-prinsip tersebut. Yaitu : Manajemen risiko menciptakan nilai tambah, Manajemen risiko adalah bagian integral proses dalam organisasi, Manajemen risiko adalah bagian dari pengambilan keputusan, Manajemen risiko secara eksplisit menangani ketidakpastian Manajemen risiko bersifat sistematis, terstruktur, dan tepat waktu, Manajemen risiko berdasarkan informasi terbaik yang tersedia, Manajemen risiko dibuat sesuai kebutuhan, Manajemen risiko memperhitungkan faktor manusia dan budaya, Manajemen risiko bersifat transparan dan inklusif, Manajemen risiko bersifat dinamis, iteratif, dan responsif terhadap perubahan, Manajemen risiko memfasilitasi perbaikan dan pengembangan berkelanjutan organisasi (Qintharah, 2019).

3.3 Metode Penelitian

Penelitian ini menggunakan metode kualitatif, menurut Trumbull & Watson (2010) adalah suatu metode dengan beraneka segi fokus yang meliputi suatu interpretif, konstruktif, pendekatan naturalistik pada subjeknya. Hal ini bermakna penelitian kualitatif mempelajari sesuatu pada sudut pandang alamiahnya, menerjemahkannya, dan melihat fenomena dalam hal makna yang dipahami manusia (Azmi, Nasution and Wardayani, 2018). Pengertian lainnya adalah suatu cara yang digunakan untuk menjawab masalah penelitian yang berkaitan dengan data berupa narasi yang bersumber dari aktivitas wawancara, pengamatan dan pengalian dokumen (Wahidmurni, 2017)

Penelitian ini terdiri dari beberapa tahap, yaitu:

1. Identifikasi Masalah

   Tahap tersebut adalah proses dimana peneliti mendapatkan suatu gambaran tentang suatu permasalahan yang ada untuk memberikan solusi.
2. Studi Literatur.

   Pada tahap ini dilakukan kajian penelitian terdahulu yang relevan dan teori yang menjadi landasan dalam penelitian ini.
3. Pengumpulan Data

   Pada tahap ini dilakukan pengambilan data dengan beberapa pendekatan, yaitu: (1) Melakukan wawancara dengan GS OFFICER dan 6 staff yang menggunakan aplikasi SAP. (2) Melakukan Observasi selama 3 bulan di PT. Serasi Autoraya untuk melihat dan mengamati proses bisnis dan pemanfaatan aplikasi SAP. (3) Menggunakan data historis aplikasi SAP yang ada di PT. Serasi Autoraya untuk melihat apa saja proses-proses yang telah terjadi.
4. Analisis Risiko

   Pada tahap ini dilakukan analisis risiko menggunakan *International Organization For Standardization* (ISO) 31000. Tahapan analisis risiko terdiri dari tiga tahap yaitu:

   1) Identifikasi risiko (*Risk Identification*)

      Pada tahap ini meliputi identifikasi risiko yang mungkin terjadi dalam suatu aktivitas. Identifikasi dilakukan secara akurat dan komplit sangatlah vital dalam manajemen risiko. Merupakan salah satu aspek penting dalam manajemen risiko. Teknik yang dapat digunakan adalah wawancara, survei, informasi historis dan lainnya.
   2) Analisis Risiko (*Risk Analyst*)

      Pahap ini melihat potensial terjadinya risiko, seberapa besar terjadi kerusakan dalam risiko tersebut. Probabilitas dalam suatu *event* sangatlah subjektif dan lebih didasarkan pada pengalaman dan nalar.
   3) Evaluasi Risiko (*Risk Evaluation*).

      Pada tahap ini dilakukan untuk menentukan manajemen risiko dengan membandingkan tingkat risiko terhadap standar yang telah ditentukan. Tujuan dari evaluasi risiko adalah mengetahui tingkat prioritas tinggi hingga rendah dan mengetahuhi tingkat risiko mana yang harus ditindaklanjuti dan mana yang di pantau.
5. Perlakuan pada Risiko (*Risk Treatment*),

   Tahap ini dilakukan upaya menyelesaikan pilihan yang dapat mengurangi atau bahkan meniadakan kemungkinan serta dampak dari risiko yang terjadi dan menerapkan perlakuan.
6. Kesimpulan dan Saran.

   Pada tahap ini akan ditarik kesimpulan berdasarkan hasil analisis risiko dan saran penelitian lebih lanjut.

4. PEMBAHASAN

Penelitian ini akan dilakukan dengan dua tahapan, yaitu Penilaian Risiko dan Perlakuan Terhadap Risiko.

4.1 Penilaian Risiko

Tahap ini merupakan tahap penilayan Risiko pada program SAP yang terdiri dari 3 tahap yaitu Identifikasi Risiko, Analisis Risiko, Eveluasi Risiko.

1. Identifikasi Risiko

Pada bagian ini dilakukan identifikasi aset, kemungkinan risiko dan dampaknya yang terjadi, adalah sebagai berikut:

1) Identifikasi Aset

Tahapan Identifikasi pada aset yang dimiliki oleh PT. Serasi Autoraya yang terkait dengan program *SAP*. Tahapan ini dilakukan melalui wawancara dengan Susilo Wibowo (GS OFFICER) dan observasi langsung ke PT. Serasi Autoraya. Detail aset-asetnya adalah sebagai berikut: Data (Data Mobil, Data Penyewaan, Data Transaksi dan Data Karyawan), Software (SAP), hardware dan jaringan (*Personal Computer (pc)*, Kabel UTP, RJ45, Server Database, Kabel Fiber Optik, Server Web Service dan Server Load Balancer). Selain itu, terdapat berbagai macam aset perusahaan.

2) Identifikasi Kemungkinan Risiko

Setelah melakukan identifikasi aset yang terakit dengan program *SAP*, maka hal yang perlu diidentifikasi selanjutnya adalah kemungkinan kemungkinan risiko yang berada di sekitar program *SAP*. Berikut adalah Tabel identifikasi kemungkinan risiko.

Tabel 1. Tabel Identifikasi Kemungkinan Risiko

Kode	Risiko
R001	Banjir
R002	Data Corrupt
R003	Gempa Bumi
R004	Kebakaran
R005	Kerusakan perangkat keras
R006	Koneksi *Internet* terputus
R007	Kurangnya SDM secara kualitas dan kuantitas
R008	Listrik Mati
R009	Memori penuh
R010	*Overheat*
R011	Petir
R012	Pencurian data
R013	Pencurian perangkat keras
R014	Peretasan terhadap jaringan
R015	Web Service Mati

3) Identifikasi Dampak Risiko

Tahapan selanjutnya adalah identifikasi dampak risiko. Tahapan ini mengidentifikasi dampak risiko seperti apa yang akan terjadi pada program *SAP*. Detail dampak risiko dapat dilihat pada Tabel 2.

Tabel 2. Identifikasi Dampak Risiko

Kode	Risiko	Dampak
R001	Banjir	Kerusakan Infrastruktur dan prasarana yang mengganggu aktifitas bisnis.
R002	Data Corrupt	Tidak dapat mangakses dan menjalankan program *SAP*.
R003	Gempa Bumi	Kerusakan Infrastruktur dan/atau menghentikan aktivitas bisnis.
R004	Kebakaran	Kerusakan Infrastruktur dan menghentikan aktivitas bisnis.
R005	Kerusakan perangkat keras	Tidak dapat mengakses program *SAP*.
R006	Koneksi *Internet* terputus	Tidak dapat mengakses program *SAP*.
R007	Kurangnya SDM secara kualitas dan kuantitas	Proses penyelesaian data tidak tepat waktu.
R008	Listrik Mati	Seluruh aktivitas terhenti.
R009	Memori penuh	Data baru yang diinput akan menggalami keterlambatan dalam proses penyajian.
R010	*Overheat*	Kinerja perangkat keras kurang maksimal. Rusaknya hardware karena harus menanggung suhu panas terus-menerus.
R011	Petir	Kerusakan pada perangkat digital.
R012	Pencurian data	Penyalahgunaan informasi yang berkaitan dengan kerahasiaan organisasi.
R013	Pencurian perangkat keras	Tidak dapat mengakses program *SAP* dan kerugian secara finansial.
R014	Peretasan terhadap jaringan	Pencurian data penting terhadap organisasi.
R015	Web Service Mati	Tidak dapat mengakses program *SAP*.

2. Analisis Risiko

Jika sudah menyelesaikan tahap identifikasi, berikutnya adalah tahap analisis risiko. Proses ini dilakukan penilaian terhadap kemungkinan risiko yang sudah diidentifikasi sebelumnya. Penentuan nilai ini berdasarkan pada Kemungkinan (Tabel 3) dan Dampak (Tabel 5).

Tabel 3. Tabel Nilai Kemungkinan

Kemungkinan		Deskripsi	Frekuensi
Nilai	Kriiteria		
1	Rare	Risiko hampir tidak pernah terjadi	>5 kali per tahun
2	Unlikely	Risiko jarang terjadi	2-5 kali per tahun
3	Possible	Risiko kadang terjadi	1-2 kali per tahun
4	Likely	Risiko sering terjadi	7-12 kali per bulan
5	Certain	Risiko pasti terjadi	1-6 kali per bulan

Nilai kemungkinan pada Tabel 3. memiliki 5 nilai yaitu pertama *Rare*, *Unlikely*, *Possible*, *Likely*, dan *Certain*. *Rare* merupakan nilai kemungkinan yang paling kecil dan hampir tidak pernah terjadi. Nilai kemungkinan yang paling tinggi adalah *Certain* yaitu risiko yang paling sering terjadi.

Tabel 4. Tabel Nilai Dampak

Dampak		Deskripsi
Nilai	Kriiteria	
1	Insignficant	Risiko tidak mengganggu proses bisnis yang ada dan jalannya aktivitas perusahaan
2	Minor	Risiko sedikit menghambat jalannya aktivitas perusahaan
3	Moderate	Risiko menghambat sebagian aktivitas perusahaan
4	Major	Risiko mulai mengganggu proses bisnis dan menghambat hampir seluruh aktivitas perusahaan
5	Catastrophic	Risiko sangat mengganggu proses bisnis dan mengentikan aktivitas perusahaan

Tabel Nilai Dampak diatas juga memiliki 5 nilai yaitu *Insignficant*, *Minor*, *Moderate Major* dan *Catastrophic*. *Insignficant* merupakan nilai dampak terendah dan *Catastrophic* merupakan nilai dampak tertinggi karena sangat menganggu kegiatan bisnis yang ada.

Setelah menentukan nilai Kemungkinan (Tabel 3) dan Dampak (Tabel 4), selanjutnya adalah penilaian terhadap kemungkinan risiko yang terikat dengan program *SAP* yang telah teridentifikasi.

Tabel 5. Tabel Penilaian Kemungkinan dan Dampak pada Kemungkinan Risiko

Kode	Risiko	Kemungkinan	Dampak
R001	Banjir	1	1
R002	Data Corrupt	2	4
R003	Gempa Bumi	1	5
R004	Kebakaran	1	5
R005	Kerusakan perangkat keras	2	4
R006	Koneksi *Internet* terputus	4	4
R007	Kurangnya SDM secara kualitas dan kuantitas	2	2
R008	Listrik Mati	4	4
R009	Memori penuh	1	3
R010	*Overheat*	3	4
R011	Petir	1	4
R012	Pencurian data	1	3
R013	Pencurian perangkat keras	1	3
R014	Peretasan terhadap jaringan	1	4
R015	Web Service Mati	2	2

3. Evaluasi Risiko

Pada tahap evaluasi risiko ini, penulis telah mengidentifikasi dan menganalisis risiko-risiko yang ada kemudian langkah selanjutnya adalah memasukkan dalam sebuah matriks evaluasi risiko berdasarkan kemungkinan dan dampak. Menggunakan parameter evaluasi risiko yang telah ditentukan didapatkan pembentukan matriks evaluasi. Parameter evaluasi risiko dapat dilihat di Tabel 6 dan matriks evaluasi risiko dapat dilihat pada Tabel 7.

Tabel 6. Tabel Parameter Evaluasi Risiko

Kemungkinan	Dampak	Level Risiko
Rare	Insignficant	Rendah
Rare	Minor	
Rare	Moderate	
Unlikely	Insignficant	
Unlikely	Minor	
Possible	Moderate	
Rare	Major	Menengah
Rare	Catastrophic	
Unlikely	Moderate	
Unlikely	Major	
Unlikely	Catastrophic	
Possible	Minor	
Possible	Moderate	
Possible	Major	
Likely	Insignficant	
Likely	Minor	
Likely	Moderate	
Certain	Insignficant	
Certain	Minor	
Possible	Catastrophic	Tinggi
Likely	Major	
Likely	Catastrophic	
Certain	Moderate	
Certain	Major	
Certain	Catastrophic	

Tabel 6 menampilkan parameter evaluasi dari kemungkinan, dampak dan level dari setiap dampak yang dihasilkan oleh perusahaan ketika kemungkinan risiko terjadi. Berikut adalah Tabel matriks evaluasi risiko.

Tabel 7. Matriks Evaluasi Risiko Berdasarkan Pada Kemungkinan dan Dampak

Kemungkinan						
	Certain(5)					
	Likely(4)				R006 R008	
	Possible(3)				R010	
	Unlikely (2)		R007 R015		R002 R005	
	Rare(1)	R001		R009 R012 R013	R014 R011	R004 R003
		Insignficant (1)	Minor(2)	Moderate(3)	Major (4)	Catastrophic (5)

Tabel 8. Matriks Evaluasi Risiko Berdasarkan Pada Kemungkinan, Dampak dan Level Risiko

Kode	Risiko	Kemungkinan	Dampak	Level Risiko
R001	Banjir	1	1	Rendah
R002	Data Corrupt	2	4	Menengah
R003	Gempa Bumi	1	5	Menengah
R004	Kebakaran	1	5	Menengah
R005	Kerusakan perangkat keras	2	4	Menengah
R006	Koneksi *Internet* terputus	4	4	Tinggi
R007	Kurangnya SDM secara kualitas dan kuantitas	2	2	Rendah
R008	Listrik Mati	4	4	Tinggi
R009	Memori penuh	1	3	Rendah
R010	*Overheat*	3	4	Menengah
R011	Petir	1	4	Menengah
R012	Pencurian data	1	3	Rendah
R013	Pencurian perangkat keras	1	3	Rendah
R014	Peretasan terhadap jaringan	1	4	Menengah
R015	Web Service Mati	2	2	Rendah

Berdasarkan Tabel 8 di atas bahwa risiko yang memiliki level tinggi *(high*) ada 2 dari 15 kemungkinan yaitu, Listrik Mati dan Koneksi Internet Terputus. Kemudian ada 7 kemungkinan yang memiliki level menengah (*medium*) yaitu *Data Corrupt*, *Overheat*, Kerusakan perangkat keras, Gempa Bumi, Kebakaran, Petir, Peretasan terhadap jaringan. Sedangkan yang terakhir mempunyai 6 level Rendah (*low)* yaitu *Web Service* Mati, Pencurian perangkat keras, Pencurian data, Memori Penuh, Kurangnya SDM secara kualitas dan kuantitas, Banjir.

3. Perlakuan Risiko

Pada tahap perlakuan risiko, akan diberikan saran dan usulan dalam memperlakukan risiko-risiko yang telah teridentifikasi dengan harapan dapat meminimalisir munculnya risiko-risiko tersebut sehingga semua aktivitas dapat berjalan secara optimal. Berikut adalah Tabel saran perlakuan terhadap risiko.

Tabel 9. Saran Perlakuan terhadap Risiko

Kode	Risiko	Level Risiko	Perlakuan Risiko
R006	Koneksi *Internet* terputus	Tinggi	Cek jaringan internet yang ada. Segera melapor pihak ISP jika tidak bisa ditangani sendiri.
R008	Listrik Mati	Tinggi	Menyediakan generator set listrik dengan daya yang sesuai dengan kebutuhan. Kemudian menyiapkan Uninterruptible Power Supply (UPS).
R002	Data Corrupt	Menengah	Melakukan backup data secara berkala, melakukan *scan* dengan menggunakan anti virus yang *berlisensi* secara berkala dan melakukan permbersihan pada PC agar mencegah munculnya *virus/malware* yang dapat menyebabkan data *corrupt.*
R010	*Overheat*	Menengah	Menyediakan ruangan yang cukup luas dengan mesin pendingin ruangan dan menjaga suhu ruangannya agar

			tidak panas.
R005	Kerusakan perangkat keras	Menengah	Memperbaiki perangkat keras yang rusak. Jika tidak dapat diperbaiki secepatnya diganti dengan yang baru agar tidak mengganggu aktivitas, serta melakukan pencadangan perangkat keras.
R003	Gempa Bumi	Menengah	Menyediakan tempat yang cukup aman untuk menempatkan perangkat-perangkat yang mendukung program *SAP*.
R004	Kebakaran	Menengah	menyediakan alat-alat pemadam kebakaran di sekitar gedung yang mudah dilihat dan dijangkau.
R011	Petir	Menengah	Menyediakan penangkal petir, orde pada instalasi listrik dan mempersiapkan tempat yang diperkirakan cukup aman untuk menempatkan perangkat-perangkat yang mendukung program *SAP*.
R014	Peretasan terhadap jaringan	Menengah	Memasang *password* yang rumit untuk setiap bagian penting dari komputer server.
R015	Web Service Mati	Rendah	Memberitahukan kepada user yang akan mengakses program *SAP* agar tidak terjadi gagal input data dan sebagainya.
R013	Pencurian perangkat keras (PC, hardisk)	Rendah	Melalukan backup data secara berkala.
R012	Pencurian data	Rendah	Pembatasan akses (*data, hardware*) serta monitoring data dan melalukan backup data secara berkala.
R009	Memori penuh	Rendah	Selalu memonitoring penggunaan memori dan *Phishing* yang ada. Bersihkan memori jika terdapat data yang tidak dibutuhkan dan melakukan pembesaran kapasitas memori.
R007	Kurangnya SDM secara kualitas dan kuantitas	Rendah	Perekrutan staff baru sesuai kebutuhan. Melalukan penelitian dan bimbingan (*training*) kepada staff baru.
R001	Banjir	Rendah	Mempersiapkan tempat yang diperkirakan cukup aman untuk menempatkan perangkat-perangkat yang mendukung program *SAP*.

Berdasarkan Tabel 9. dapat dilihat risiko yang mungkin akan terjadi beserta level risiko dan solusi yang dapat dilakukan untuk meminimalisir risiko. Dalam penanganan risiko-risiko tersebut direkomendasikan agar dilakukan skali prioritas, yaitu pertama diutamakan yang level risiko tertinggi, yaitu mengantisipasi risiko koneksi internet terputus dan listrik mati. Kemudian yang level menangah yaitu data corrupt, overheat, kerusakan perangkat keras, gempa bumi, kebakaran, petir dan peretasan terhadap jaringan. Selanjutnya mengantisipasi risiko yang paling rendah, yaitu: web service mati, pencurian perangkat keras (pc, hardisk), pencurian data, memori penuh, kurangnya SDM dan banjir.

5. KESIMPULAN

Dalam penelitian ini dilakukan analisis terhadap program *SAP* menggunakan ISO 31000, terdiri dari penilaian risiko dan perlakuan pada risiko. Dalam penilaian risiko ada tiga tahap yaitu Identifikasi Risiko (*Risk Identification*), Analisis Risiko (*Risk Analyst*) dan Evaluasi Risiko (*Risk Evaluation*). Setelah itu dilakukan perlakuan pada risiko *(Risk Treatment*). Serangkaian proses yang berdasarkan pada ISO 31000, didapatkan hasil tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi adalah listrik dan koneksi internet. Dua hal tersebut harus mendapat perhatian khusus karena sangat mengganggu aktivitas yang ada dikarenakan segala aktivitas administrasi TRAC harus terhubung dengan koneksi internet dan apabila terjadi listris mati secara otomatis koneksi internet terputus. Oleh sebab itu, TRAC harus menyediakan pasokan listrik yang memadai sesuai dengan kebutuhan. Kemudian tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang menengah yaitu, *data corrupt*, *overheat*, kerusakan perangkat keras, gempa bumi, kebakaran, petir, peretasan terhadap jaringan. Terakhir tingkatan risiko yang memiliki nilai kemungkinan dan nilai dampak yang rendah yaitu *web service* mati, pencurian perangkat keras, pencurian data, memori penuh, kurangnya SDM secara kualitas dan kuantitas, banjir. Untuk mengatasi risiko tersebut maka telah diusulkan beberapa solusi, yaitu Menyediakan generator set listrik, Menyiapkan *Uninterruptible Power*

Supply (UPS), Melakukan backup data secara berkala, memasang antivirus melakukan scan dengan menggunakan anti virus, Menyiapkan ruangan yang cukup luas dengan mesin pendingin ruangan dan menjaga suhu ruangannya agar tidak panas, Memperbaiki perangkat keras yang rusak, Menyiapkan alat-alat pemadam kebakaran di sekitar gedung yang mudah dilihat dan dijangkau, Mempersiapkan penangkal petir, orde pada instalasi listrik dan mempersiapkan tempat yang diperkirakan cukup aman untuk menempatkan perangkat-perangkat yang mendukung program SAP, mengelolah sistem keamanan dengan tertib.

6. SARAN

Penelitian ini hanya terbatas pada analisis risiko program *System Application and Processing* (SAP) sehingga masih perlu dikaji secara holisitik dan komprehensif tentang tata kelola SI/TI pada PT. Serasi Autoraya. Sebab analisis risiko merupakan salah bagian dari Tata Kelola SI/TI, sehingga apabila hanya fokus pada manajemen risiko tentu tidak akan berdampak pada perusahaan, maka diharapkan kajian lebih lanjut dilakukan secara menyeluruh agar perusahaan benar-benar menyelaraskan teknologi informasi dengan strategi perusahaan serta realisasi dari keuntungan-keuntungan TI (*Benefit Realisation*), memaksimalkan sumber daya TI (*Resource Optimisation*) dan manajemen risiko yang dilakukan secara tepat dan terukur (*Risk Optimisation*).

7. DAFTAR PUSTAKA

Agustinus, Nugroho and Cahyono. 2017. '*Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS'*, Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 1(3), pp. 250–258. doi: 10.29207/resti.v1i3.94.

Azmi, Nasution and Wardayani. 2018. '*Memahami Penelitian Kualitatif dalam Akuntansi',* Akuntabilitas, 11(1), pp. 159–168. doi: 10.15408/akt.v11i1.6338.

Ernawati and Santoso. 2017. *'Identifikasi dan Analisa Risiko Penerapan Teknologi Informasi di Lingkungan PerguruanTinggi',* in. Yogyakarta: SEMINAR NASIONAL Dinamika Informatika 2017 Universitas PGRI, pp. 21–28. Available at: http://senadi.upy.ac.id/prosiding/index.php/sndi/article/viewFile/32/31.

Kadir, A. 2014. *Pengenalan Sistem Informasi Edisi Revisi*. Yogyakarta: Andi Offset.

Nice and Imbar. 2016. '*Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000',* Jurnal Informatika dan Sistem Informasi (JUISI) Universitas Ciputra, 02(02). Available at: https://journal.uc.ac.id/index.php/JUISI/article/view/237/220.

Qintharah, Y. N. 2019. '*Perancangan Penerapan Manajemen Risiko (Studi Kasus Pada Umkm Saripakuan CV. Jarwal Maega Buana)',* JRAK, 10(1), pp. 67–86. Available at: jurnal.unismabekasi.ac.id/index.php/jrak/article/download/1645/1420/%0A%0A.

Sirait and Susanty. 2016. '*Analisis Risiko Operasional Berdasarkan Pendekatan Enterprise Risk Management (ERM) Pada Perusahaan Pembuatan Kardus di CV Mitra Dunia Palletindo',* Industrial Enginerering Online Journal, 5(4). Available at: https://ejournal3.undip.ac.id/index.php/ieoj/article/view/14043/13578.

Suhendra, E. S., Oswari, T. and Setiawan, S. 2013. *'Peran Business Continuity Plan dan Contingency Plan Dalam Meminimalisir Risiko Teknologi Informasi pada Industri Asuransi.'*, Jurnal Asuransi dan Manajemen Risiko, 1(1), pp. 42–52.

Talitha, Driantami and Perdanakusuma. 2018. '*Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)',* Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2(11), pp. 4991–4998. Available at: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3159.

Wahidmurni. 2017. *Pemaparan Metode Penelitian Kualitatif*. Malang. Available at: http://repository.uin-malang.ac.id/1984/2/1984.pdf.