Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 2, Agustus 2024, pp 1030-1041
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Analisis Manajemen Risiko Pada Aplikasi SAP LOGON 750 di PT. XYZ Berbasis ISO 31000:2018

Marvel Evandi Budiono[1], Endang Haryani[2*]
[1,2]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
Email: 682020007@student.uksw.edu[1], endang_hry@uksw.edu[2]*

Abstract

The SAP LOGON 750 handles production process activities from inputting production data, production scheduling, production processes, to reporting production. There are various possible risks that occur, but PT. XYZ has never managed risks internally. This study aims to analyze risk management for the use of the SAP application. This research focuses on one case study object and applies a qualitative approach based on the ISO 31000: 2018 framework. The results found 18 possible risks. There are 12 medium level risks, among others are dust/dirt, server down, lightning, power outage, lost network connection, dead web service, hardware damage, human error, data theft, fire, earthquake, hacker attack. While there are 6 low level risks, namely backup failure, data corruption, overheat, overload, flooding and virus attacks. Therefore, this study concludes that there are no risks that are very dangerous or have a loss impact on companies related to the use of the SAP LOGON 750 application. Although there are medium-level risks, these can be overcome by technical and systematic risk treatment. Technical risk treatment includes reviewing ventilation and electrical structures, installing lightning rods, providing fire extinguishers, generators and UPS. While systematic risk treatment through periodic maintenance, among others, for servers, web services, networks, hardware and data backups. In addition, there is socialization and training for employees. PT XYZ is expected to always be vigilant and prepared by managing risks and risk treatment properly.

Keywords*: ISO 31000:2018; Information System; Risk; Risk Management*

Abstrak

Aplikasi SAP LOGON 750 menangani kegiatan proses produksi dari penginputan data produksi, penjadwalan produksi, proses produksi, hingga pelaporan hasil produksi. Terdapat berbagai kemungkinan risiko yang terjadi, namun PT. XYZ belum pernah mengelola risiko secara internal. Tujuan dari penelitian ini adalah untuk menganalisis manajemen risiko atas penggunaan aplikasi SAP ini. Penelitian ini berfokus pada satu objek studi kasus dan menerapkan pendekatan kualitatif berbasis framework ISO 31000:2018. Penelitian menemukan adanya 18 kemungkinan risiko. Terdapat 12 risiko tingkat medium/menengah, yaitu debu/kotoran, server down, petir, Listrik padam, koneksi jaringan terputus, web service mati, kerusakan hardware, human error, pencurian data, kebakaran, gempa bumi, serangan hacker. Sedangkan pada tingkat low/rendah ada 6, yaitu kegagalan backup, data corrupt, overheat, overload, banjir dan serangan virus. Oleh karena itu, penelitian ini menyimpulkan bahwa tidak ada risiko yang sangat membahayakan atau memberi dampak kerugian bagi perusahaan terkait penggunaan aplikasi SAP LOGON 750. Meskipun ada risiko level menengah, namun risiko tersebut dapat diatasi dengan tindakan atau perlakuan risiko secara teknis dan sistematis. Perlakuan risiko secara teknis antara lain dengan peninjauan ulang struktur ventilasi dan listrik, pemasangan penangkal petir, penyediaan APAR, genset dan UPS. Sedangkan perlakuan risiko secara sistematis melalui pemeliharaan berkala antara lain untuk server, web service, jaringan, hardware dan backup data. Selain ada sosialisasi dan pelatihan bagi karyawan. Dari semua risiko tersebut, PT. XYZ diharapkan untuk selalu waspada dan siap sedia dengan mengelola risiko dan perlakuan risiko dengan baik.

Kata kunci*: ISO 31000:2018; Sistem Informasi; Risiko; Manajemen Risiko*

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 2, Agustus 2024, pp 1030-1041
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

1. PENDAHULUAN

Keberadaan teknologi informasi dan komunikasi (TIK) saat ini semakin menunjang aktivitas manusia dalam bisnis dan organisasi [1][2]. Dalam perkembangannya, TIK banyak digunakan perusahaan untuk meningkatkan daya saing, seperti meningkatnya produktivitas, menguatkan daya finansial dan menumbuhkan profesionalitas [3][4]. Kehadiran TIK dapat memberikan jalan keluar dan keringanan dalam mendukung hasil dari suatu perusahaan [5][6]. Namun biaya yang dibutuhkan perusahaan untuk pengadaan TIK tersebut tidaklah murah [7]. Investasi ini pun belum tentu berdampak positif bagi perusahaan. Ada ketidakpastian apakah investasi ini benar-benar memberi dampak pada perusahaan, atau bahkan sebaliknya. Oleh karena itu perusahaan perlu melakukan tindakan dan upaya untuk manajemen risiko ini. Selain untuk mencegah kemungkinan masalah yang serupa, dan juga untuk meyakinkan bahwa penggunaan TIK dapat berjalan dengan baik serta perusahaan tidak mengalami kerugian setelah mengeluarkan dana yang tidak sedikit tersebut.

PT. XYZ adalah perusahaan yang berada di Kabupaten Tegal bergerak di bidang produksi teh. Saat ini PT. XYZ sudah menghasilkan berbagai variasi produk dengan merek Botol, Sosro, dan Poci. Untuk kegiatan proses produksi berbagai teh tersebut, PT. XYZ menerapkan aplikasi *System Application and Processing* (SAP) LOGON 750. Aplikasi SAP ini menangani kegiatan proses produksi dari penginputan data produksi, penjadwalan produksi, proses produksi, hingga pelaporan hasil produksi. Risiko yang terjadi dalam melakukan penginputan data produksi salah satunya bisa saja terjadi human error yang menyebabkan salah menginput data dan mengakibatkan data tidak valid, sehingga penjadwalan produksi bisa mengalami keterlambatan. Proses produksi teh memiliki risiko mengalami gangguan listrik mati yang menyebabkan teh yang diproduksi menjadi tidak baik. Hasil teh yang kurang baik akan di reject dan diolah kembali menjadi pupuk kompos. Risiko dari hasil laporan produksi ada kemungkinan bahwa informasi menjadi kurang akurat yang disebabkan data yang tidak valid. Melihat berbagai kemungkinan risiko yang terjadi pada PT. XYZ tersebut, maka manajemen risiko perlu segera dilakukan. Apalagi selama ini PT. XYZ belum pernah mengelola risiko secara internal.

Manajemen risiko sudah banyak dikaji oleh para peneliti. Penelitian sebelumnya yang sudah pernah dilakukan oleh William Frederick Worotikan menggunakan ISO 31000 dan menemukan adanya 33 peluang bahaya pada aplikasi e-Ticketing pada Taman Rekreasi XYZ[8]. Dari 33 peluang bahaya tersebut, 4 diantaranya berada pada risiko tinggi, yaitu jaringan yang terhenti, data pengunjung yang salah input, pengunjung mengajukan uang kembali, dan verifikasi transaksi yang tidak dapat dilakukan oleh sistem; kemudian 17 diantaranya peluang bahaya pada level menengah; dan 12 peluang bahaya lainnya pada level rendah. Penelitian lain dilaksanakan oleh Grialdo Willy Lantang et.al pada aplikasi *System Application and Processing* (SAP). Riset ini menemukan 15 risiko yang mempengaruhi kinerja aplikasi SAP, yaitu 2 risiko level tinggi, meliputi hambatan jaringan *internet* dan koneksi daya listrik; 7 risiko level sedang; dan 6 risiko pada rendah[9]. Kemudian, penelitian dilakukan oleh Aprilia Rahmawati

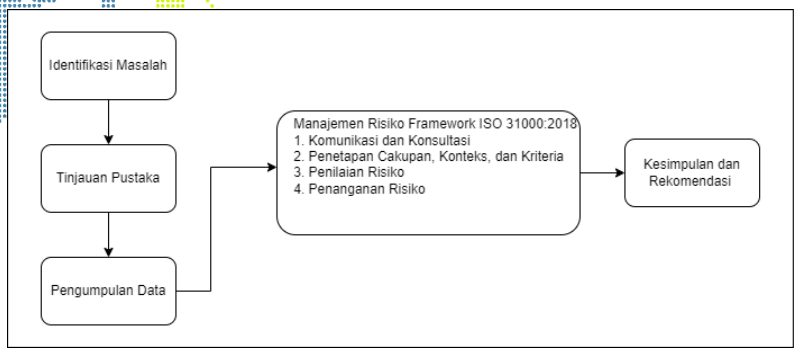
juga menerapkan ISO 31000[10]. Analisis risiko dilakukan terhadap aplikasi iTop, dimana ditemukan 25 kemungkinan ancaman, yaitu 8 ancaman level *medium* dan 17 ancaman level *low*. Sedangkan penelitian oleh Kwee Mey Linda Lole tentang analisis aplikasi Pegadaian Digital Service berdasarkan metode ISO 31000:2018 menemukan adanya 23 kemungkinan risiko yang terdiri dari 1 risiko yang berbahaya atau berada pada level risiko tinggi, yaitu data nasabah yang bocor; 6 risiko yang berbahaya pada tingkatan sedang dan 16 risiko yang berbahaya pada tingkatan rendah[11]. Kemudian penelitian yang dilakukan oleh F. M. Hutabarat dengan menggunakan metode ISO 31000 menjaring 20 peluang ancaman pada aplikasi VCare, yaitu 4 peluang ancaman tingkatan tinggi, 8 peluang ancaman tingkatan sedang, dan 8 peluang ancaman level rendah [12]. Pengkajian yang dilakukan oleh Devara Liko Ivander dan Frederik Samuel Papilaya pada PT. XYZ Bawen juga dengan mengaplikasikan kerangka kerja ISO 31000:2018 bertujuan untuk mendapati, mengukur, dan memperkecil risiko [13]. Riset tersebut menemukan 26 kemungkinan risiko yang bisa mengancam perusahaan, yaitu 15 ancaman berisiko rendah (*low*), 5 ancaman berisiko menengah (*medium*), 5 ancaman berisiko menengah tinggi (*medium high*), dan 1 ancaman berisiko tinggi (*high*). Setelah menerapkan situasi untuk mengatasi risiko, akhirnya perusahaan dapat menerapkan dan mengelola manajemen risiko dengan baik.

Mempertimbangkan bahwa terdapat kesenjangan yang terjadi, yaitu ada kebutuhan manajemen risiko di PT. XYZ atas penggunaan sistem informasi, namun di sisi lain manajemen risiko ini belum pernah diteliti di PT. XYZ, serta berbagai studi yang menunjukkan efektivitas ISO 31000 dalam pengelolaan risiko, maka tujuan penelitian adalah untuk menganalisis manajemen risiko pada penggunaan aplikasi SAP LOGON 750 di PT. XYZ. Berbasis kerangka kerja ISO 31000, riset ini diharapkan dapat membantu PT. XYZ dalam mengelola risiko dengan baik, melalui mengidentifikasi risiko, menganalisis risiko, mengevaluasi dampaknya, dan melakukan upaya-upaya pencegahan risiko serta dampaknya.

2. METODOLOGI PENELITIAN

Prosedur yang dilakukan pada pengkajian saat ini yang berfokus terhadap satu objek studi kasus penelitian serta melakukan metode kualitatif. Data berupa data pokok dari melakukan penelitian secara langsung dan menjalankan wawancara, serta data sekunder dari prosedur dan struktur organisasi[14] Untuk melaksanakan observasi manajemen risiko yang cocok dengan framework ISO 31000:2018[15][16][17]. Metode tahapan dari pengkajian ini dideskripsikan pada Gambar 1.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 2, Agustus 2024, pp 1030-1041
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik



Gambar 1. Tahapan Penelitian[15]

1. Identifikasi masalah untuk menginvestigasi permasalahan yang ada, kemudian merumuskan tujuan penelitian dan memutuskan untuk menggunakan framework ISO 31000:2018 sebagai metode untuk menganalisis risiko dan memperoleh pemahaman tentang subjek studi kasus yang akan diteliti.
2. Tinjauan pustaka yang dilakukan dengan mempelajari peneliti yang sebelumnya yang signifikan dan bisa menjadi dasar dalam melakukan penelitian ini.
3. Pengumpulan data yang dikumpulkan melalui 3 cara, yaitu observasi secara langsung, wawancara tentang proses bisnis yang diimplementasikan ke aplikasi SAP, dan studi pustaka tentang penelitian sebelumnya yang signifikan dan bisa menjadi dasar dalam melakukan analisis penelitian.
4. Analisis manajemen risiko berbasis standar internasional ISO 31000:2018. Versi terbaru standar manajemen risiko ini menyediakan visi yang lengkap dan strategis untuk pengelola atau manajer risiko, termasuk prinsip dan metodologi yang diterapkan, sehingga pengelolaan risiko dapat melindungi nilai perusahaan[18]. Standar menyediakan panduan dengan lingkup yang sangat luas dan tingkat keberhasilan perusahaan berupa faktor internal maupun eksternal[19]. Tahapan manajemen risiko yaitu:
   a. Komunikasi dan Konsultasi Risiko: persepsi yang sama mengenai risiko yang akan ditentukan, dinilai, dan dikaji, termasuk membuat perjanjian tentang rahasia perusahaan dan privasi setiap orang yang terlibat dalam penelitian.
   b. Cakupan, Konteks, dan Kriteria: Fokus riset pada pengelolaan risiko aplikasi SAP di PT. XYZ, berdasarkan kerangka kerja ISO 31000:2018. Adapun kriteria yang digunakan pada risiko tersebut adalah kriteria *likelihood* dan *impact*.
   c. Penilaian Risiko (*Risk Assessment*)
      1. Identifikasi Risiko (*Risk Identification*)
      2. Analisis Risiko (*Risk Analysis*)
      3. Evaluasi Risiko (*Risk Evaluation*) menghasilkan proses penilaian risiko yang tepat dengan dasar hasil temuan analisis risiko[20].
   d. Perlakuan Risiko (*Risk Treatment*): memberikan usulan terkait beberapa pilihan penanganan risiko untuk meminimalisir risiko atau bahaya[21].

5. Kesimpulan dan Rekomendasi merupakan tahap akhir dari penelitian ini, berisi konklusi manajemen risiko pada PT. XYZ dan rekomendasi yang relevan untuk aplikasi SAP.

3. HASIL DAN PEMBAHASAN.

3.1. Komunikasi dan Konsultasi Risiko

Komunikasi dan konsultasi risiko mendukung untuk mengetahui profil perusahaan, mengerti apa saja risiko atau ancaman yang dapat terjadi. Hal ini dilakukan untuk mendapatkan pemahaman dan pengertian yang sama tentang manajemen risiko pada PT. XYZ, khususnya untuk membantu perusahaan meminimalisir risiko yang pernah terjadi tidak terulangi kembali. Proses ini dilakukan dengan teknisi divisi IT.

3.2. Cakupan, Konteks, dan Kriteria

Penetapan cakupan dibuat oleh peneliti adalah untuk menganalisis manajemen risiko aplikasi SAP yang digunakan di PT. XYZ. Konteks yang dipilih yaitu untuk mengetahui apakah setiap divisi di PT. XYZ sudah menggunakan teknologi informasi dengan baik dan mendukung semua infrastruktur.

Tabel 1. Kriteria *Likelihood* [15]

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

Kriteria risiko pertama yang harus ditetapkan adalah kriteria *likelihood*. Pada Tabel 1 diuraikan bahwa terdapat 5 ukuran dari yang nilai likelihood tertinggi yaitu *certain* hingga nilai yang terendah yaitu *rare*. Kelima kriteria tersebut mendeskripsikan frekuensi keterjadian sebuah risiko. Kriteria kedua pada Tabel 2 menjelaskan kriteria *impact*, dimana kriteria dibagi menjadi lima nilai kategori dampak jika sebuah risiko benar-benar terjadi [15].

Tabel 2. Kriteria *Impact* [15]

Impact		**Keterangan**
Nilai	**Kriteria**	
1	*Insignificant*	Tidak merintangi kegiatan perusahaan
2	*Minor*	Kegiatan perusahaan terhalang, namun tidak mengganggu kegiatan yang utama
3	*Moderate*	Menghambat jalannya proses bisnis pada perusahaan, sehingga kegiatan bisnisnya sedikit terlambat
4	*Major*	Kegiatan bisnis mengalami penundaan
5	*Catastrophic*	Kegiatan perusahaan terhenti total

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 2, Agustus 2024, pp 1030-1041
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Selanjutnya, risiko-risiko yang telah ditentukan frekuensi keterjadian (*likelihood*) dan dampaknya jika risiko tersebut benar-benar terjadi (*impact*) dipetakan dalam sebuah matriks evaluasi (Tabel 3). Nilai kedua kriteria dipertemukan untuk mengetahui posisi level risikonya. Matriks terdiri dari 3 tingkatan risiko yaitu *low, medium*, dan *high* yang masing-masing diwakili warna hijau, kuning dan merah.

Tabel 3. Matriks Evaluasi Risiko[15]

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

3.3. Penilaian Risiko

Tahapan selanjutnya yaitu penilaian risiko pada aplikasi SAP LOGON 750, yang terdiri dari identifikasi risiko (*Risk Identification*), analisis risiko (*Risk Analysis*), dan evaluasi risiko (*Risk Evaluation*). Tahapan pertama yaitu identifikasi risiko dimulai dengan melakukan mengenal aset yang dimiliki PT. XYZ seperti terlihat di Tabel 4. Tahapan yang kedua yaitu identifikasi kemungkinan risiko. Pada tahapan ini peneliti akan membagi probabilitas risiko yang muncul ke dalam 3 faktor kelompok (alam atau lingkungan, manusia, serta sistem dan infrastruktur) dan disajikan pada Tabel 5. Tahapan yang ketiga yaitu identifikasi dampak risiko. Pada langkah ini, dari peluang risiko yang sudah ditemukan sebelumnya, maka selanjutnya menemukan dampak risiko dari setiap kemungkinan risiko tersebut. Pengaruh risiko dari setiap kemungkinan risiko terlihat pada Tabel 6.

3.3.1. Identifikasi Risiko

A. Identifikasi Aset

Aplikasi SAP adalah suatu aplikasi yang dipakai untuk membantu dalam memasukan data yang keluar dan yang masuk. Untuk menggunakan aplikasi ini cukup men-*download* aplikasinya, kemudian memasukan data apa yang diperlukan sesuai kolom pilihan yang sudah tersedia di aplikasi SAP. Tahapan ini yang digunakan dalam mengenal aset pada sistem informasi SAP yang terdiri dari aset data, aset perangkat lunak, hingga aset perangkat keras.

Tabel 4. Identifikasi Aset pada Aplikasi SAP

Komponen	Aset
Data	Data User Data Marketing Data Department Data Produksi
Software	Aplikasi SAP Microsoft Office

Komponen	Aset
Hardware	Personal Computer (PC) Laptop Printer Router Proyektor Server UPS

B. Identifikasi Kemungkinan Risiko

Tahap berikutnya adalah melaksanakan identifikasi terhadap kemungkinan risiko yang muncul berdasarkan faktor kelompok, yaitu aspek alam/lingkungan, manusia, sistem dan infrastruktur. Tabel 5 menguraikan 18 risiko yang teridentifikasi, yaitu 5 risiko pada faktor alam dan lingkungan, 3 risiko pada faktor manusia dan 10 risiko pada aspek sistem dan infrastruktur.

Tabel 5. Identifikasi Kemungkinan Risiko

Faktor	ID	Risiko
Alam atau Lingkungan	R01	Banjir
	R02	Gempa Bumi
	R03	Petir
	R04	Kebakaran
	R05	Listrik Padam
Manusia	R06	*Human Error*
	R07	Pencurian data
	R08	*Hacker*
Sistem dan Infrastruktur	R09	Server down
	R10	*Overheat* PC
	R11	*Overload* PC
	R12	Kegagalan *Backup*
	R13	Data *corrupt*
	R14	*Web service* mati
	R15	Serangan virus
	R16	Koneksi jaringan terputus
	R17	Debu/Kotoran
	R18	Kerusakan *hardware*

C. Identifikasi Dampak Risiko

Sesudah melakukan tahap mengenali risiko, ditemukan sejumlah ancaman yang muncul dari beberapa aspek alam atau lingkungan, manusia, serta sistem dan infrastruktur yang mempengaruhi penggunaan dari aplikasi SAP, maka diperlukan kajian pengaruh yang dibentuk dari risiko yang sudah terdeteksi.

Tabel 6. Identifikasi Dampak Risiko

ID	Kemungkinan Risiko	Dampak
R01	Banjir	Aktivitas bisnis terhambat dan mengalami kerusakan fasiltas/infrastruktur
R02	Gempa Bumi	Infrastruktur mengalami kerusakan dan aktivitas bisnis terhambat
R03	Petir	Mengalami kerusakan infrastruktur perusahaan

ID	Kemungkinan Risiko	Dampak
R04	Kebakaran	Aktivitas bisnis terhenti karena infrastruktur yang rusak
R05	Listrik Padam	Seluruh aktivitas bisnis akan terhenti dan terjadi kerugian operasional perusahaan
R06	*Human Error*	Proses layanan memasukkan data tidak berjalan dengan baik
R07	Pencurian data	Akan terjadi kerugian data rahasia dan informasi yang penting
R08	Serangan *Hacker*	Menyebabkan kerugian finansial dan merusak reputasi perusahaan
R09	*Server down*	Gagal melakukan akses ke dalam server
R10	*Overheat*	Hardware akan mengalami kerusakan
R11	*Overload*	Menghambat proses menginput data
R12	Kegagalan Backup	Data yang masuk ke perusahaan tidak lengkap
R13	Data *corrupt*	Tidak menerima data yang valid
R14	*Web service* mati	Aplikasi SAP tidak dapat diakses
R15	Serangan virus	Data dapat dicuri dan menghambat proses bisnis
R16	Koneksi terputus	Tidak dapat mengakses aplikasi SAP
R17	Debu/Kotoran	Dapat merusak komponen komputer
R18	Kerusakan *hardware*	Tidak dapat mengakses aplikasi SAP

3.3.2. Analisis Risiko

Setelah semua kemungkinan risiko dan dampaknya sudah terdeteksi, maka berikutnya adalah melakukan proses analisis risiko pada tabel *likelihood* yang telah dibuat. *Likelihood* dibedakan menjadi 5 kriteria dengan sesuai probabilitas risiko dalam jangka waktu tertentu.

Tabel 7. Nilai Risiko Menurut Kriteria *Likelihood* dan *Impact*

ID	Kemungkinan Risiko	*Likelihood*	*Impact*
R01	Banjir	1	3
R02	Gempa Bumi	1	4
R03	Petir	3	3
R04	Kebakaran	1	5
R05	Listrik Padam	3	3
R06	Human Error	2	4
R07	Pencurian data	2	4
R08	Serangan Hacker	1	4
R09	Server down	3	4
R10	Overheat	2	1
R11	Overload	2	1
R12	Kegagalan Backup	2	2
R13	Data corrupt	2	2
R14	Web service mati	3	2
R15	Serangan virus	1	3
R16	Koneksi jaringan terputus	3	3
R17	Debu/Kotoran	4	3
R18	Kerusakan hardware	3	2

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 9, Nomor 2, Agustus 2024, pp 1030-1041
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

3.3.3. Evaluasi Risiko

Evaluasi risiko adalah langkah terakhir dari asesmen risiko dengan menyusun peta risiko yang diturunkan dari nilai risiko yang telah dievaluasi pada matriks evaluasi risiko (Tabel 8).

Tabel 8. Matriks Evaluasi Risiko

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

Berdasarkan hasil pemetaan seluruh risiko pada tabel matriks evaluasi resiko di Tabel 8, maka dapat diketahui level risiko untuk 18 kemungkinan risiko. Dari 18 risiko yang teridentifikasi, 6 risiko berada pada ruang hijau yaitu level risiko rendah dan 12 risiko pada ruang kuning dengan level risiko menengah. Dengan demikian, tidak ada risiko pada ruang merah atau level risiko tinggi. Hasil proses evaluasi risiko menemukan 12 dari 18 kemungkinan risiko memiliki level risiko tingkat *medium* atau menengah, berturut-turut dari nilai risiko tertinggi, yaitu debu/kotoran (R17), *server down* (R09), petir (R03), listrik padam (R05), koneksi jaringan terputus (R16), web service mati (R14), kerusakan *hardware* (R18), *human error* (R06), pencurian data (R07), kebakaran (R04), gempa bumi (R02), dan serangan *hacker* (R08). Sisanya adalah 6 dari 18 risiko merupakan risiko pada level tingkat *low* atau rendah, yaitu kegagalan *backup* (R12), data *corrupt* (R13), *overheat* (R10), *overload* (R11), banjir (R01) dan serangan virus (R15).

3.4. Perlakuan Pada Risiko

Setelah melakukan evaluasi risiko, maka berikutnya dapat dianalisis perlakuan yang tepat untuk masing-masing risiko sesuai level risikonya. Oleh karena itu, pada tahapan ini akan memberikan masukan yang diharapkan dapat mengatasi atau mengurangi dampak atas kejadian berbagai kemungkinan risiko tersebut. Bahkan dengan masukan yang diberikan, level risiko dapat berkurang, sehingga aplikasi SAP benar-benar dapat bekerja secara maksimal memberikan manfaat bagi Perusahaan.

Tabel 9. Usulan Perlakuan Risiko

ID	Level Risiko	Perlakuan Risiko	Tindakan Risiko
R17	Medium	Turunkan	Meninjau ulang struktur ventilasi sumber debu dan melakukan perawatan komponen secara berkala

ID	Level Risiko	Perlakuan Risiko	Tindakan Risiko
R09	Medium	Turunkan	Memerlukan *maintenance server* secara berkala pada *database*, melakukan *backup server* dan menambah *server*
R03	Medium	Turunkan	Memasang penangkal petir dan menyediakan APAR
R05	Medium	Turunkan	Menyediakan genset listrik dengan SOP yang jelas pengoperasiannya, serta menyiapkan *Uninterruptible Power Supply* (UPS)
R16	Medium	Turunkan	Mengecek jaringan *internet* yang tersedia, dan mengganti *Internet Protocol* (IP) yang lebih baik
R14	Medium	Turunkan	Melakukan *troubleshooting* saat *web service* mati dan perlu adanya jadwal *maintenance*
R18	Medium	Turunkan	Mengganti dengan *hardware* yang baru dan apabila hardware yang rusak masih bisa diperbaiki maka akan dibawa ke *service center* dan melakukan *maintenance*
R06	Medium	Turunkan	Melakukan sosialisasi dan *training* yang terstruktur untuk karyawan baru
R07	Medium	Turunkan	Melakukan *reset password* secara berkala dan memasang CCTV dan melakukan *backup* data berkala
R04	Medium	Turunkan	Menyediakan alat pemadam kebakaran dan pengecekan berkala pada instalasi listrik
R02	Medium	Turunkan	Menyediakan tempat yang aman dan mengantisipasi dengan peninjauan ulang konstruksi bangunan yang lama
R08	Medium	Turunkan	Memasang CCTV dan sering mengganti password dan melakukan *maintenance* berkala
R12	Low	Turunkan	Melakukan *backup* data secara berkala
R13	Low	Turunkan	Melakukan *backup* data dan memasang anti virus
R10	Low	Turunkan	Memasang *Air Conditioner* (AC) pada ruangan supaya hardware tetap dingin dan melakukan maintenance berkala pada PC yang digunakan
R11	Low	Turunkan	Menambah memori dan RAM yang lebih besar dan melakukan *maintenance* berkala
R01	Low	Turunkan	Menempatkan *server* cadangan di lokasi yang lebih aman
R15	Low	Turunkan	Memasang anti virus dan melakukan *scanning* serta mengaktifkan *firewall* dan melakukan *maintenance* berkala

4. SIMPULAN

Penelitian ini mengaplikasikan kerangka kerja ISO 31000:2018 untuk menganalisis risiko/ancaman pada aplikasi SAP LOGON 750 di PT. XYZ. Proses analisis mencakup identifikasi, analisis, evaluasi hingga analisis perlakuan pada risiko. Hasil riset menginvestigasi 18 kemungkinan risiko yang berpotensi mengganggu jalannya aplikasi SAP ini. Penelitian menginvestigasi lebih lanjut dan menemukan bahwa dari 18 risiko tersebut, terdapat 12 kemungkinan risiko dengan tingkat risiko *medium* dan 6 kemungkinan risiko berada pada tingkat risiko *low*. Risiko tingkat *medium*/menengah, yaitu debu/kotoran, *server down*, petir, listrik padam, koneksi jaringan terputus, *web service* mati, kerusakan *hardware*, *human error*, pencurian data, kebakaran, gempa bumi, dan serangan *hacker*. Sedangkan 6 kemungkinan risiko pada level risiko *low*/rendah, yaitu kegagalan *backup*, data *corrupt*, *overheat, overload*, banjir dan serangan virus. Oleh karena itu, penelitian ini menyimpulkan bahwa tidak ada risiko yang sangat membahayakan

atau memberi dampak kerugian bagi perusahaan terkait penggunaan aplikasi SAP LOGON 750. Meskipun ada risiko level menengah, namun risiko tersebut dapat diatasi dengan tindakan atau perlakuan risiko secara teknis dan sistematis. Perlakuan risiko secara teknis yang diusulkan antara lain dengan peninjauan ulang struktur ventilasi dan listrik, pemasangan penangkal petir, penyediaan APAR, genset dan UPS. Sedangkan perlakuan risiko yang disarankan secara sistematis melalui pemeliharaan berkala antara lain untuk *server*, *web service*, jaringan, *hardware* dan *backup* data. Di samping ada tambahan sosialisasi dan pelatihan bagi karyawan. Walau bagaimana pun, dari semua risiko yang sudah ditemukan, PT. XYZ diharapkan untuk selalu waspada dan siap sedia dari setiap risiko yang muncul dengan mengelola risiko dan perlakuan risiko dengan baik.

Penelitian ini juga mengusulkan beberapa rekomendasi. Pertama terkait kerangka kerja atau *framework* yang digunakan pada riset ini yaitu ISO 31000:2018. Penelitian selanjutnya mungkin dapat dikaji dari framework yang lain. Harapannya adalah dengan *framework* lain dapat melengkapi temuan dan analisis yang ada. Keterbatasan lain dari penelitian ini adalah aplikasi SAP LOGON 750 yang menjadi fokus penelitian ini merupakan aplikasi yang menangani produksi. Oleh karena itu, kajian berikutnya diharapkan dapat meneliti proses bisnis lain pada aplikasi lain yang terkait. Dengan demikian, analisis manajemen risiko dapat dilakukan lebih menyeluruh untuk berbagai proses bisnis di perusahaan.

DAFTAR PUSTAKA

[1] T. Lubis, M. Irwan, and P. Nasution, "Peran Teknologi Informasi Dan Komunikasi Dalam Meningkatkan Efisiensi Sistem Pendukung Organisasi," *J. Manaj. dan Ekon. Bisnis*, vol. 4, no. 1, pp. 83–89, 2024, [Online]. Available: https://doi.org/10.55606/cemerlang.v4i1.2246

[2] F. A. Sudirman, "Teknologi Informasi Dan Komunikasi (Tik) Dan Sdgs : Review Literatur Sistematis," *J. Ilmu Komun. UHO J. Penelit. Kaji. Ilmu Komun. dan Inf.*, vol. 8, no. 2, pp. 273–288, 2023, doi: 10.52423/jikuho.v8i2.56.

[3] E. Eskak, "Study of The Information and Communication Technology (ICT) Utilization to Improve The Competitiveness of Creative Crafts And Batik Industries in The 4.0 Industry Era," *Pros. Semin. Nas. Ind. Kerajinan dan Batik*, pp. 1–13, 2020.

[4] E. A. Kadir, A. Syukur, and S. L. Rosa, "Pengembangan Jaringan Internet Untuk Pedesaan Pada Kecamatan Kuala Kampar, Pelalawan, Riau," *J. Pengabdi. Masy. dan …*, vol. 1, no. 2, pp. 11–17, 2020, [Online]. Available: https://journal.uir.ac.id/index.php/jpmpip/article/download/10670/4619

[5] N. Q. Fadillah, M. Amanda, and N. A. Andrelin, "Perancangan Project Base Learning Web Design Kue Pukis Meses," *J. Ilm. Pengabdi. Pada Masy.*, vol. 2, no. 1, pp. 292–301, 2024.

[6] T. G. V Pangemanan, A. S. M. Lumenta, and Y. D. Y. Rindengan, "GMIM Southwest Manado Region," vol. 18, no. 04, pp. 143–152, 2023.

[7] E. Mahmudah, B. Ni'maturahmah, D. Ayu, and M. Dewi, "Seminar Nasional Inovasi Pendidikan Ke-6 (SNIP 2022) SHEs: Conference Series 6 (1) (2023) 358-365 Utilization of Information and Communication Technology as Learning Media to Improve the Quality of Education in Elementary Schools," vol. 6, no. Snip 2022, pp. 358–365, 2023, [Online]. Available: https://jurnal.uns.ac.id/shes

[8] W. F. Worotikan and E. Maria, "KLIK: Kajian Ilmiah Informatika dan Komputer Penerapan ISO 31000:2018 untuk Manajemen Risiko E-Ticketing Taman Rekreasi XYZ," *Media Online*, vol. 3, no. 5, pp. 449–456, 2023, [Online]. Available: https://djournals.com/klik

[9] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000," *Sebatik*, vol. 23, no. 1, pp. 36–43, 2019, doi: 10.46984/sebatik.v23i1.441.

[10] 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.

[11] K. M. Linda Lole and E. Maria, "Analisis Manajemen Risiko Pada Aplikasi Pegadaian Digital Service Menu Tabungan Emas Menggunakan ISO 31000:2018," *J. Sist. Komput. dan Inform.*, vol. 3, no. 3, p. 319, 2022, doi: 10.30865/json.v3i3.3891.

[12] F. M. Hutabarat and A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, pp. 52–65, 2020, doi: 10.33557/binakomputer.v2i1.792.

[13] L. D. Ivander and S. F. Papilaya, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2009," *J. Ekon. Vol. 18, Nomor 1 Maret201*, vol. 2, no. 1, pp. 41–49, 2020, doi: 10.30865/klik.v4i2.1174.

[14] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 3, pp. 546–558, 2020, doi: 10.35957/jatisi.v7i3.525.

[15] G. Vernier, *ISO 31000: Risk Management Guidelines*, vol. 2018. 2018. doi: 10.1007/978-3-031-25984-5_314.

[16] D. B. Vargas, L. Maria, and D. S. Campos, "Risk Management: A Parallel Between ISO 31000 and the PMBOK Guide (2017)," vol. 31000, no. 2018, pp. 1474–1483, 2023, doi: 10.46254/an12.20220285.

[17] Charles R. Vorst, D. S. P. Arif, and Arif Budiman, *Manajemen Risiko Berbasis SNI ISO 31000*, vol. 4, no. 1. 2018.

[18] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 : 2018 (Studi Kasus: Cv. Xy)," *Sebatik*, vol. 23, no. 1, pp. 277–284, 2019, doi: 10.46984/sebatik.v23i1.572.

[19] J. Ecleas, "Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 1, pp. 209–224, 2021, doi: 10.35957/jatisi.v8i1.601.

[20] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus: Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[21] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.