Bit (Fakultas Teknologi Informasi Universitas Budi Luhur) p-ISSN: 1693-9166
Vol. 20, No. 1, April 2023, hlm. 38-43 e-ISSN: 2685-127X

ANALISIS MANAJEMEN RISIKO PADA SISTEM INFORMASI KIMIA FARMA EMPLOYEE SELF TECHNOLOGY

Alya Nur Ramadhani[1], Theresiawati[2*], Sarika[3]

[1,2,3]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta
Email: [1]alyanur@upnvj.ac.id, [2*]theresiawati@upnvj.ac.id, [3]sarika.afrizal@upnvj.ac.id,

(* : corresponding author)

(Naskah masuk: 27 Maret 2023, diterima untuk diterbitkan: 13 Mei 2023)

Abstrak

Hampir semua organisasi sudah menjadikan teknologi informasi sebagai salah satu kebutuhan dan penting bagi organisasi dalam menjalankan berbagai proses bisnisnya, tidak terkecuali PT Kimia Farma Tbk. KIFEST adalah aplikasi sistem informasi pegawai layanan terpadu bagi karyawan internal Kimia Farma yang menampilkan semua aplikasi dalam satu halaman utama aplikasi. Dengan kemudahan dalam pengaksesan aplikasi-aplikasi tersebut tentu saja memungkinkan ancaman dan risiko. Risiko ini akan mengakibatkan kerugian bagi sebuah perusahaan maka penting untuk dilakukan manajemen risiko yang ada dengan diidentifikasi dan diukur. Tujuan penelitian ini adalah untuk menganalisis manajemen risiko Sistem Informasi KIFEST. Untuk melakukan analisis manajemen risiko, menggunakan metode ISO 31000. Hasil dari penelitian ini didapatkan 27 kemungkinan risiko dengan 5 level risiko. Tingkat risiko diurutkan dari yang tertinggi hingga terendah, daftar hasil analisis manajemen risiko dapat dijadikan sebagai patokan dan dasar dalam mengambil keputusan, dengan rekomendasi saran perlakuan berupa mitigasi dan risk sharing.

Kata kunci: *kimia farma employee self technology, manajemen risiko, sistem informasi, ISO 31000*

RISK MANAGEMENT ANALYSIS ON THE KIMIA FARMA EMPLOYEE SELF TECHNOLOGY INFORMATION SYSTEM

Abstract

Almost all organizations have made information technology a necessity and important for organizations in carrying out various business processes, including PT Kimia Farma Tbk. KIFEST is an integrated service employee information system application for Kimia Farma's internal employees that displays all applications on one application main page. With the ease of accessing these applications, of course, it allows threats and risks. This risk will result in a loss for a company, so it is important to carry out existing risk management by identifying and measuring it. The purpose of this research is to analyze the KIFEST Information System risk management. To carry out a risk management analysis, used the ISO 31000 method. The results of this study found 27 possible risks with 5 risk levels. The level of risk is sorted from the highest to the lowest, the list of results of risk management analysis can be used as a benchmark and basis for making decisions, with recommendations for treatment in the form of mitigation and risk sharing

Keywords*: kimia farma employee self technology, risk management, information system, ISO 31000*

1. PENDAHULUAN

KIFEST adalah aplikasi sistem informasi pegawai layanan terpadu bagi karyawan internal Kimia Farma yang menampilkan semua aplikasi dalam satu halaman utama aplikasi. Hal ini tentunya sangat memberikan kemudahan dan juga efisiensi dalam hal penyediaan akses ke beberapa aplikasi hanya dengan menggunakan *Single Sign On* (SSO) atau *Central Authentication Service*[1] dimana pengguna hanya membutuhkan satu akun saja menggunakan *username* dan *password*[2] untuk mendapatkan izin, akses ke semua layanan yang terdapat dalam jaringan [3] serta mengakses aplikasi-aplikasi yang terdapat di dalam *dashboard* aplikasi KIFEST.

Dengan kemudahan dalam pengaksesan aplikasi-aplikasi tersebut tentu saja memungkinkan ancaman dan risiko pada sistem informasi layanan terpadu bagi karyawan internal ini. Risiko ini akan mengakibatkan kerugian bagi sebuah perusahaan maka penting untuk dilakukan manajemen risiko yang ada dengan diidentifikasi dan diukur.

Standar ISO 31000 digunakan sebagai metode dalam analisis manajemen risiko, menganalisis nilai risiko dan nilai dampak yang muncul pada sistem

informasi [4], membantu organisasi atau perusahaan mengimplementasikan penerapan manajemen risiko[5]. ISO 31000 panduan penerapan risiko terdiri dari tiga elemen, kerangka kerja (*framework*), prinsip (*principle*) dan proses (*process*) manajemen risiko sebagai arsitektur manajemen risiko dan menjamin penerapan manajemen risiko yang efektif[6][7] .

Metode ini meliputi proses identifikasi risiko dari aset-aset yang ada, *risk assessment* atau proses penilaian yang digunakan untuk mengetahui tingkat risiko (riskrating)[8], mengidentifikasi potensi bahaya yang dapat terjadi untuk memastikan kontrol risiko dari proses, operasi atau aktivitas yang dilakukan berada pada tingkat yang dapat diterima[9]. Penilaian risiko *atau risk management process*[10] menganalisis dan evaluasi risiko yang telah diidentifikasi, pemeliharaan guna mencegah serta perlakuan risiko kinerja sistem yang mungkin muncul. ISO 31000 juga memberikan pedoman, *framework*, dan proses untuk mengontrol risiko.

Dengan memperhatikan kemungkinan (*likelihood*) dalam proses mencapai sasaran, meningkatkan kemampuan dalam mengidentifikasi peluang dan ancaman, serta menangani risiko (*risk treatment*) dengan memanfaatkan sumber daya yang ada dan dari proses pengumpulan data menggunakan teknik wawancara didapatkan informasi mengenai kemungkinan risiko yang ada pada perusahaan, yaitu ada risiko hilangnya data, *hacking*, data yang tidak valid, *server down*, *human error*, *cybercrime*, dan gagal *update* yang selanjutnya dianalisis lebih lanjut dalam penelitian ini

2. METODE PENELITIAN

Metode penelitian yang digunakan pada analisis risiko ialah kualitatif. Alasan mengapa menggunakan analisis kualitatif adalah analisis dapat dikerjakan dengan cepat dan relatif mudah untuk digunakan pada skala identifikasi kemungkinan dan dampak yang luas serta dapat dijadikan sebagai bahan evaluasi pemeringkatan risiko.

2.1 Penentuan Objek Penelitian

Penelitian ini dilakukan pada sistem informasi pegawai layanan terpadu bagi karyawan internal Kimia Farma bernama Kimia Farma *Employee Self Technology* (KIFEST) menganalisis manajemen risiko dari sistem informasi dengan metode ISO 31000.

2.2 Identifikasi Masalah

Proses identifikasi masalah pada sistem informasi pegawai layanan terpadu bagi karyawan internal Kimia Farma bernama Kimia Farma *Employee Self Technology* (KIFEST) menggunakan metode ISO 31000:2018.

2.3 Studi Literatur

Studi literatur dilakukan dengan mengumpulkan berbagai referensi yang berhubungan dengan informasi yang dibutuhkan untuk penelitian. Sumber studi literatur didapatkan dari e-book untuk mendapatkan landasan teori yang dapat mendukung penelitian, beberapa jurnal ilmiah, dan skripsi yang dijadikan sebagai bahan acuan dalam penelitian ini.

2.4 Pengumpulan Data

Beberapa metode pengumpulan data yang nantinya digunakan untuk identifikasi masalah, antara lain pengumpulan data diantaranya melakukan observasi, wawancara, dan studi pustaka.

2.5 Analisis dan Hasil

Dalam melakukan analisis dan pembahasan menggunakan metode ISO 31000 menggunakan data yang telah dikumpulkan, proses yang dilakukan dari proses komunikasi dan konsultasi hingga proses pemantauan dan tinjauan.

3. HASIL DAN PEMBAHASAN

3.1 Komunikasi dan Konsultasi

Tahapan ini penting dilakukan dari awal proses yaitu menentukan konteks agar memperoleh infornasi-informasi penting demi kelancaran analisis manajemen risiko. Dalam memperoleh informasi yang diperlukan dalam penelitian, melakukan wawancara dengan divisi *human capital*, manajemen risiko, dan *Information Technology*, mengumpulkan informasi mengenai aset dari berbagai divisi yang terhubung dengan Sistem Informasi Kimia Farma *Employee Self Technology*. Dengan menggunakan metode *Responsible Accountable Consulted Informed* (RACI), pemetaan RACI *Chart* identifikasi dibedakan berdasarkan proses kegiatan yang dilakukan, seperti yang terlihat pada Tabel 1.

Tabel 1. Raci Chart

Proses MR	Kepala Divisi HC	Asisten Manajer HC	Kepala Divisi Manaj Risiko	Asisten Manajer Manajemen Risiko	Kepala divisi IT	Admin data dan informasi
Menetapkan lingkup,konteks, dan kriteria	I/C	A/R	C	R	I/C	
Identifikasi risiko	I/C	A/R	C	R	C	C
Analisis Risiko	I/C	A/R	C	R	C	I
Evaluasi Risiko	I/C	A/R	C	R	C	I
Perlakuan risiko	I/C	A/R	C	R	C	I
Pantau dan kaji ulang	I/C	A/R	C	R	C	R
Catat dan Lapor	I/C	A/R	C	R	C	I

3.2 Identifikasi Aset

Pada proses ini, mengumpulkan informasi mengenai aset dari berbagai divisi yang terhubung dengan Sistem Informasi Kimia Farma *Employee Self Technology*, identifikasi ini dilakukan terhadap aset data, *software*, hingga *hardware*, seperti terlihat pada Tabel 2.

Tabel 2. Identifikasi Aset

Komponen Sistem Informasi	Aset KIFEST	Kode Aset	Keterangan
Data	Data Kehadiran Pegawai	A01	Data kehadiran dan absensi pegawai
	Data Lembur Pegawai	A02	Data waktu dan frekuensi lembur pegawai.
	Data Slip gaji (*payslip*) Pegawai	A03	Data terkait gaji, pesangon, dan insentif.
	Data Cuti Pegawai	A04	Data jatah cuti dan daftar ajuan cuti pegawai.
	Data Surat Perintah Perjalanan Dinas (SPPD)	A04	Data perjalanan dinas seperti tujuan perjalanan dinas, tempat, dan informasi terkait lainnya.
	Data tiket WFO	A05	Data jadwal kerja dari rumah pegawai, data pengajuan kerja dari rumah, serta jadwal kerja pegawai.
	Data Arteri	A06	Dokumen dari pegawai masuk sampai saat ini atau saat pensiun milik tiap unit dan divisi
Software	Sistem Informasi KIFEST	A07	Aplikasi milik divisi HC (*Human Capital*), Subdivisi *learning*, subdivisi *talent and organization*, divisi SPI, dan divisi manajemen risiko
Hardware	Laptop	A08	Dipakai oleh setiap *user* di Kimia Farma Tbk. Untuk kegiatan operasional harian.
	Internet	A09	Jaringan wifi kantor yang dapat diakses di semua bagian.
	Server	A10	*Server* khusus menggunakan Google Cloud
	Database	A11	Menggunakan Navicat
	Anti Virus	A12	Menggunakan Imunify
	Domain	A13	Domain co.id
	Handphone	A15	Perangkat pribadi *user*.

Tabel 3. Identifikasi Kemungkinan Risiko

Kode	Kemungkinan Risiko	Dampak
KR01	Kebakaran	Kehilangan aset-aset dan rusaknya infrastruktur ,terhentinya proses bisnis
KR02	Gempa Bumi	Aset IT rusak dan terhentinya proses bisnis
KR03	Petir	Kerusakan infrastruktur, penyediaan data terhambat, proses bisnis terganggu
KR04	Banjir	Terhambatnya aktivitas bisnis
KR05	Debu atau kotoran	Kerusakan perangkat *hardware*
KR06	Listrik padam	Dengan adanya genset aktivitas perusahaan tidak terganggu, namun penggunaan genset tidak untuk semua bagian hanya dinyalakan pada bagian tertentu saja, hal ini bisa berpengaruh pada berjalannya proses bisnis Sistem Informasi KIFEST.
KR07	Human Error	Sulitnya pengaksesan data, aset IT tidak beroperasi dengan baik, terganggunya proses bisnis.
KR08	Kebocoran data atau informasi	Data yang bersifat rahasia seperti *password* dapat dilihat oleh orang yang tidak bertanggung jawab.
KR09	Penyalahgunaan hak akses atau *User* ID	Data pegawai seperti tanggal lahir pegawai, data gaji, pesangon dapat dimanipulasi sehingga dapat merugikan perusahaan.
KR10	Informasi diakses oleh pihak yang tidak berwenang	Informasi kepegawaian apabila diakses oleh pihak yang tidak berwenang dapat menjadi dasar untuk melakukan *cybercrime*
KR11	Data dan informasi tidak sesuai fakta	Data yang tidak valid dapat merugikan perusahaan dan proses bisnis terganggu.
KR12	Mantan *user*/karyawan masih memiliki akses informasi	Data dapat dilihat dan dimanipulasi oleh karyawan yang seharusnya sudah tidak memiliki hak akses.
KR13	Hilangnya data	Aset data pegawai yang hilang dapat mengganggu berjalannya proses bisnis, HC (*Human Capital*) harus melakukan recovery data dan ini merugikan perusahaan dari segi waktu dan finansial.
KR14	Target penggunan sistem perbulan tidak tercapai	Sistem informasi tidak digunakan secara optimal, apabila sistem yang bersifat mandatory tidak terpenuhi target akses nya artinya pegawai tidak menjalankan kewajibannya seperti akses sistem absensi, pengajuan lembur, SF (Sukses Faktor) dan sistem lainnya.
KR15	*Server down*	Kehilangan data, penyediaan data dan penghubungan portal ke aplikasi yang dituju terhambat
KR16	Koneksi jaringan terputus	Penyediaan data dan penghubungan portal ke aplikasi yang dituju terhambat, gagal *update* secara real time, proses bisnis terhenti
KR17	Sistem *Crash*	Sistem tidak dapat dibuka sehingga penyediaan data terhambat, data gagal *update* secara real time dan proses bisnis terhambat..
KR18	*Data Corrupt* / Rusak	Data rusak, data hilang, proses bisnis terganggu
KR19	*Backup Failure* atau gagal melakukan fungsi media penyimpanan.	Data yang diinput tidak tersimpan, data yang diterima perusahaan tidak lengkap,data hilang, proses bisnis terganggu.

Kode	Kemungkinan Risiko	Dampak
KR20	Gagal *Update*	Sistem tidak terbarui, dengan versi yang lama aplikasi tidak berjalan optimal.
KR21	*Database Error*	Sistem tidak bisa menampilkan data yang di-*request user*
KR22	Kurang baiknya kualitas jaringan	Terhambatnya akses ke sistem informasi KIFEST
KR23	Kerusakan *hardware*	Proses bisnis perusahaan terhambat karena harus melakukan setup *hardware* yang baru.
KR24	Notifikasi sistem tidak tampil pada *Operation System* (OS) tertentu	*User* tidak mengetahui berita terkini atau apabila ia menggunakan aplikasi absensi ia tidak tahu apakah terlambat atau tidak.
KR25	*Overheat* Perangkat *Hardware*	*Hardware* mengalami kerusakan, *hardware* tidak berjalan secara optimal, seperti loading yang lama sehingga aktivitas bisnis terganggu.
KR26	Serangan Virus	Data hilang, sistem tidak dapat terbuka secara optimal, aktivitas bisnis terganggu.
KR27	*Hacking*	Sistem diambil alih, dan proses bisnis sistem informasi tidak bisa berjalan.

3.3 Identifikasi Kemungkinan Risiko

Tahap identifikasi risiko dilanjutkan dengan proses identifikasi kemungkinan risiko yang muncul dari aset-aset yang telah diidentifikasi sebelumnya, dimana kemungkinan-kemungkinan ini dilihat dari beberapa faktor, diantaranya faktor alam dan lingkungan, manusia, dan sistem serta infrastruktur, dapat dilihat pada Tabel 3.

3.4 Identifikasi Dampak Resiko

Dari tahap identifikasi risiko ditemukan kemungkinan risiko yang dapat mengganggu penerapan sistem informasi KIFEST. Langkah selanjutnya adalah mengidentifikasi dampak risiko, proses ini mengidentifikasi apa yang akan terjadi oleh sistem informasi KIFEST apabila kemungkinan-kemungkinan ini terjadi. Tabel 4 menunjukkan hasil identifikasi dampak risiko.

Tabel 4. Identifikasi Dampak Risiko

Kode	Kemungkinan Risiko	*Likelihood*	*Impact*	Skala Level Risiko
KR01	Kebakaran	1	2	2
KR02	Gempa Bumi	1	2	2
KR03	Petir	1	2	2
KR04	Banjir	1	1	1
KR05	Debu atau kotoran	1	1	1
KR06	Listrik padam	2	4	8
KR07	Human Error	2	5	10
KR08	Kebocoran data atau informasi	2	4	8
KR09	Penyalahgunaan hak akses atau *User* ID	1	3	3
KR10	Informasi diakses oleh pihak yang tidak berwenang	2	3	6
KR11	Data dan informasi tidak sesuai fakta	2	5	10
KR12	Mantan *user*/karyawan masih memiliki akses informasi	1	2	2
KR13	Hilangnya data	4	5	20
KR14	Target penggunan sistem tidak tercapai	2	4	8
KR15	*Server down*	2	5	10
KR16	Koneksi jaringan terputus	1	4	4
KR17	Sistem *Crash*	2	5	10
KR18	*Data Corrupt* / Rusak	2	5	10
KR19	*Backup Failure* atau gagal melakukan fungsi media penyimpanan.	2	4	8
KR20	Gagal *Update*	2	3	6
KR21	*Database Error*	1	5	5
KR22	Kurang baiknya kualitas jaringan	1	4	4
KR23	Kerusakan *hardware*	1	3	3
KR24	Notifikasi sistem tidak tampil pada OS *(Operation System)* tertentu	4	3	12
KR25	*Overheat* Perangkat *Hardware*	2	3	6
KR26	Serangan Virus	2	4	8
KR27	*Hacking*	3	5	15

Pada tahap penilaian kemungkinan risiko diatas, nilai diberikan pada masing-masing kemungkinan risiko yang bisa saja terjadi di PT. Kimia Farma Tbk. *Likelihood* dan *impact* diberi nilai dengan skala 1 sampai dengan 5 sesuai dengan keadaan pada lingkungan Sistem KIFEST. Semakin besar nilai kemungkinan terjadinya risiko artinya risiko yang terjadi juga semakin besar. Hal ini berlaku juga dengan dampak, semakin besar nilai maka risiko yang terjadi dapat menghambat dan mengganggu proses bisnis pada sistem. Nilai-nilai likelihood dan impact yang telah diidentifikasi kemudian dilanjutkan dalam tahap evaluasi risiko.

3.5 Evaluasi Risiko

Tahap akhir dalam assesmen risiko adalah evaluasi risiko, yaitu proses mengevaluasi penilaian risiko yang telah didapatkan dari proses analisis risiko sebelumnya. Dari nilai tersebut dapat diketahui besar risiko yang dihasilkan. Evaluasi risiko dilakukan untuk membantu dalam mengambil keputusan.

3.5.1 *Probability Impact Matrix*

Hasil penilaian antara *likelihood* dengan *impact* pada tabel 6 dijadikan acuan dalam penentuan *level* risiko yang dibedakan menjadi 5 yaitu rendah (*low*), rendah-sedang (*low to moderate*), sedang (*moderate*), sedang- tinggi (*moderate to high*), dan sangat tinggi (*high*).

Dari penilaian risiko diatas didapatkan 1 kemungkinan risiko dengan level risiko bernilai *high*, 1 kemungkinan risiko dengan level risiko bernilai *moderate* to high, 6 kemungkinan risiko dengan level *moderate*, 8 kemungkinan risiko dengan level risiko *low to moderate*, dan 11 kemungkinan risiko dengan level risiko *low*.

Tabel 5. *Probality Impact Matrix*

			IMPACT				
			1 Tidak signifikan	**2 kecil**	**3 sedang**	**4 besar**	**5 bencana**
LIKELIHOOD	1	Hampir tidak mungkin terjadi	KR04 KR05	KR01 KR02 KR03 KR12	KR09 KR23	KR16 KR22	KR21
	2	Kemungkinan kecil terjadi			KR10 KR20 KR25	KR06 KR08 KR14 KR19 KR26	KR07 KR11 KR15 KR17 KR18
	3	Kemungkinan terjadi dan tidak terjadi sama sekali					KR27
	4	Kemungkinan besar terjadi			KR24		KR13
	5	Hampir pasti terjadi					

3.5.2 Hasil Peringkat Risiko

Setelah kemungkinan risiko dimasukan dalam matriks evaluasi risiko langkah selanjutnya adalah menjabarkan kemungkinan risiko ke dalam Tabel 6 *level of risk* sesuai dengan urutannya dari risiko tertinggi ke risiko yang paling rendah.

Tabel 6. *Level Of Risk*

Kode	Kemungkinan Risiko	Level Risiko	Prioritas
KR13	Hilangnya data	*High*	1
KR27	Hacking	*Moderate to High*	2
KR24	Notifikasi sistem tidak tampil pada OS *(Operation System)* tertentu	*Moderate*	3
KR07	Human Error	*Moderate*	3
KR11	Data dan informasi tidak sesuai fakta	*Moderate*	3
KR15	*Server down*	*Moderate*	3
KR17	Sistem *Crash*	*Moderate*	3
KR18	*Data Corrupt* / rusak	*Moderate*	3
KR06	Listrik padam	*low to moderate*	4
KR08	Kebocoran data atau informasi	*low to moderate*	4
KR14	Target penggunaan sistem per-bulan tidak tercapai	*low to moderate*	4
KR19	*Backup Failure* atau gagal melakukan fungsi media penyimpanan.	*low to moderate*	4
KR26	Serangan Virus	*low to moderate*	4
KR10	Informasi diakses oleh pihak yang tidak berwenang	*low to moderate*	4
KR20	Gagal *Update*	*low to moderate*	4
KR25	*Overheat* Perangkat *Hardware*	*low to moderate*	4
KR21	*Database Error*	*low*	5
KR16	Koneksi jaringan terputus	*low*	5
KR22	Kurang baiknya kualitas jaringan	*low*	5
KR09	Penyalahgunaan hak akses atau *User* ID	*low*	5
KR23	Kerusakan *hardware*	*low*	5
KR01	Kebakaran	*low*	5
KR02	Gempa Bumi	*low*	5
KR03	Petir	*low*	5
KR12	Mantan *user*/karyawan masih memiliki akses informasi	*low*	5
KR04	Banjir	*low*	5
KR05	Debu atau kotoran	*low*	5

Dari penilaian risiko diatas didapatkan kemungkinan risiko dengan *level* tertinggi atau prioritas pertama bernilai *high* yaitu hilangnya data, 1 kemungkinan risiko dengan level risiko bernilai *moderate to high* yaitu *Hacking*, 6 kemungkinan risiko dengan *level moderate* yaitu notifikasi sistem tidak tampil pada *Operation System* (OS) tertentu, *Human Error*, Data dan informasi tidak sesuai fakta, *server down*, sistem *Crash*, data *Corrupt* / rusak, 8 kemungkinan risiko dengan *level* risiko *low to moderate* yaitu listrik padam, kebocoran data atau informasi, target penggunaan sistem per-bulan tidak tercapai, backup Failure atau gagal melakukan fungsi media penyimpanan, serangan *virus*, informasi diakses oleh pihak yang tidak berwenang, gagal *update*, *overheat* perangkat *hardware*, dan 11 kemungkinan risiko dengan level risiko rendah atau *low* yaitu *database error*, koneksi jaringan terputus, kurang baiknya kualitas jaringan, penyalahgunaan hak akses atau *User* ID, kerusakan *hardware*, kebakaran, gempa bumi, petir, mantan *user*/karyawan masih memiliki akses informasi, banjir, dan debu atau kotoran.

3.6 Perlakuan Risiko

Setelah risiko diidentifikasi baik aset, kemungkinan, dan dampaknya. Kemudian dilakukan analisis dengan melakukan penilaian kemungkinan risiko. Tahapan selanjutnya adalah perlakuan risiko. Perlakuan risiko adalah proses mengidentifikasi, menyeleksi, dan melaksanakan respons terhadap risiko yang tidak dapat diterima dan memerlukan tindakan pengendalian (Leo J. Susilo, Victor Riwu Kaho ISO 31000:2018). Pengendalian ini sebagai upaya minimalisir kemungkinan risiko yang ada sehingga sistem informasi dapat berjalan dengan lancar dan tidak mengalami kerugian apabila risiko-risiko tersebut terjadi. Wawancara dilakukan untuk mendiskusikan perlakuan risiko terhadap setiap kemungkinan risiko dengan menyesuaikan keadaan perusahaan PT. Kimia Farma Tbk.Hasil perlakuan risiko dapat dilihat pada tabel 7

Tabel 7. Perlakuan Risiko

Kode	Kemungkinan Risiko	Level	Perlakuan Risiko
KR13	Hilangnya data	*High*	Perlakuan risiko nya adalah mitigasi melalui peningkatan keamanan server dan sistem dan memperhatikan penyimpanan dengan baik. Dengan cara: -Memasang *firewall* -*Reset password* secara berkala -*Backup data* secara berkala
KR27	Hacking	*Moderate to High*	Perlakuan risiko nya adalah mitigasi melalui peningkatan keamanan. Dengan cara: -Memasang dan memonitor *firewall* -*Maintance* Jaringan secara rutin -Reset *password* server berkala
KR24	Notifikasi sistem tidak tampil pada OS *(Operation System)* tertentu	*Moderate*	Perlakuan risiko nya adalah mitigasi atau risk sharing melalui perbaikan sistem. Dengan cara: -Update sistem secara berkala -Melaporkan masalah pada penyedia server (G*oogle Cloud Platform*.)
KR07	Human Error	*Moderate*	Perlakuan risiko nya adalah mitigasi melalui peningkatan pengetahuan atau keterampilan pegawai. Dengan cara : -Mengadakan pelatihan penggunaan sistem secara rutin. Wajib mengikuti bimbingan bagi karyawan baru -Membuat dokumentasi pengetahuan dan Di upload di e-*Learning*.
KR11	Data dan informasi tidak sesuai fakta	*Moderate*	Perlakuan risiko nya adalah mitigasi melalui verifikasi data. Dengan cara: -Data yang di *input* di cek kevalidan nya melalui beberapa tahapan. -Menambah fitur upload bukti.
KR15	*Server down*	*Moderate*	Perlakuan risiko nya adalah mitigasi melalui: -Melakukan pemeriksaan berkala kepada penyedia cloud server.
KR17	Sistem *Crash*	*Moderate*	Perlakuan risiko nya adalah mitigasi melalui peningkatan *bandwidth* dan *maintenance.* Dengan cara: -Meningkatkan *bandwidth* -Memeriksa konfigurasi -*Debugging coding.*
KR18	*Data corrupt* atau rusak	*Moderate*	Perlakuan risiko nya adalah mitigasi melalui meningkatkan proteksi laptop *user*. Dengan cara: -*Backup* secara berkala -Menggunakan anti-virus.

Kode	Kemungkinan Risiko	Level	Perlakuan Risiko
KR06	*List*rik padam	*low to moderate*	Perlakuan risiko nya adalah mitigasi melalui peningkatan penerapan penggunaan *generator set* pada semua bagian terutama untuk menyalakan jaringan internet.
KR08	Kebocoran data atau informasi	*low to moderate*	Perlakuan risiko nya adalah mitigasi melalui peningkatan keamanan penyimpanan data. Dengan cara: -Memasang *firewall* -*Reset password* secara berkala -Membatasi hak akses.
KR14	Target penggunaan sistem per-bulan tidak tercapai	*low to moderate*	Perlakuan risiko nya adalah mitigasi. Bagi sistem yang wajib diakses atau bersifat *mandatory* dapat dilakukan mitigasi dengan adanya notifikasi untuk akses sistem apabila belum akses seperti untuk absensi, mengisi KPI *(Key Performance Indicator)*, dsb, sedangkan untuk aplikasi yang tidak memiliki target atau hanya bersifat sebagai fasilitas dapat mengadakan sosialisasi penggunaan sistem secara berkala khususnya bagi pegawai baru namun hal ini.
KR19	*Backup Failure* atau gagal melakukan fungsi media penyimpanan.	*low to moderate*	Perlakuan risiko nya adalah mitigasi melalui peningkatan monitoring server. Dengan cara: -Pengecekan data secara berkala agar keutuhan data terjaga. -Membuat SOP yang dapat diikuti apabila gagal menyimpan data, sehingga data tidak hilang. -Melakukan *Backup* secara berkala.
KR26	Serangan Virus	*low to moderate*	Perlakuan risiko nya adalah mitigasi melalui pemasangan anti-virus pada laptop dan jaringan.
KR10	Informasi diakses oleh pihak yang tidak berwenang	*low to moderate*	Perlakuan risiko nya adalah mitigasi melalui peningkatan keamanan sistem. Dengan cara: -*Reset password* secara berkala -Memasang Captcha, apabila *user* salah memasukan *user* ID dan *password* sebanyak 5 kali akan muncul capcha.
KR20	Gagal *Update*	*low to moderate*	Perlakuan risiko nya adalah mitigasi melalui: -Melakukan pemeriksaan berkala kepada penyedia hosting.
KR25	*Overheat* Perangkat *Hardware*	*low to moderate*	Perlakuan risiko nya adalah mitigasi melalui: -Memakai kipas laptop tambahan. -Mengatur suhu ruangan agar tetap dingin.
KR21	*Database Error*	*low*	Perlakuan risiko nya adalah mitigasi melalui peningkatan *maintenance.* Dengan cara: -Memeriksa konfigurasi -*Debugging coding.*
KR16	Koneksi jaringan terputus	*low*	Perlakuan risiko nya adalah risk sharing melalui kerja sama dengan penyedia jaringan internet. -Karyawan penyedia jaringan mengontrol langsung koneksi jaringan. Sehingga pemulihan jaringan lebih cepat terurus.
KR22	Kurang baiknya kualitas jaringan	*low*	Perlakuan risiko nya adalah mitigasi melalui cek kualitas internet Dengan cara: -Memilih penyedia layanan internet yang sesuai dengan lingkungan kantor. -Melaporkan tiap kali jaringan tidak stabil agar segera ditangani dan tidak mengganggu berjalannya sistem.
KR09	Penyalahgunaan hak akses atau *User* ID	*low*	Perlakuan risiko nya adalah mitigasi melalui peningkatan keamanan sistem. Dengan cara: -*Reset password* secara berkala -Menambahkan fitur *face recognition* -Membatasi hak akses -Memasang CCTV
KR23	Kerusakan *hardware*	*low*	Perlakuan risiko nya adalah mitigasi dengan cara melakukan *quality control* secara rutin.
KR01	Kebakaran	*low*	Perlakuan risiko nya adalah mitigasi dengan cara menyediakan alat pemadam kebakaran serta memasang pendeteksi api (*fire detector*), karena data sistem berbasis cloud sehingga perlakuan risiko berfokus pada aset fisik seperti laptop dan infrastruktur lainnya. Maka lebih baik kantor menyediakan cadangan infrastruktur baik *hardware* dan perangkat jaringan.

Kode	Kemungkinan Risiko	Level	Perlakuan Risiko
KR02	Gempa Bumi	*low*	Perlakuan risiko nya adalah mitigasi karena data sistem berbasis cloud sehingga perlakuan risiko berfokus pada aset fisik seperti laptop dan infrastruktur lainnya, maka lebih baik kantor menyediakan cadangan infrastruktur baik *hardware* dan perangkat jaringan.
KR03	Petir	*low*	Perlakuan risiko nya adalah mitigasi yaitu dengan mengecek kualitas penangkal secara berkala dan apabila ada kerusakan segera diganti atau diperbaiki.
KR12	Mantan *user*/karyawan masih memiliki akses informasi	*low*	Perlakuan risiko nya adalah mitigasi dengan segera menghapus akses karyawan yang sudah pensiun,
KR04	Banjir	*low*	Perlakuan risiko nya adalah risk acceptance, karena lokasi perusahaan berada di pusat kota yang tidak pernah banjir dan hampir semua perangkat keras serta jaringan juga berada di lantai 2
KR05	Debu atau kotoran	*low*	Perlakuan risiko nya adalah mitigasi dengan cara pembersihan *hardware* secara berkala.

3.7 Pemantauan dan Peninjauan (*Monitoring* and *Review*)

Tahap *monitoring* dan *review* akan dilakukan secara berkala dengan mengadakan rapat guna mengkomunikasikan terkait temuan kemungkinan risiko yang baru dan kendala penerapan manajemen risiko keadaan serta membicarakan terkait penanganannya dan apakah butuh penelitian lebih dalam lagi di kemudian harinya.

4. KESIMPULAN

Setelah dilakukan analisis melalui berbagai tahapan dari tahap komunikasi dan konsultasi hingga *monitoring* dan *review* didapatkan hasil yaitu terdapat 27 kemungkinan risiko dengan 5 *level* risiko yaitu 1 kemungkinan risiko dengan *level* risiko bernilai *high* yaitu hilangnya data, 1 kemungkinan risiko dengan *level* risiko bernilai *moderate to high* yaitu *hacking*, 6 kemungkinan risiko dengan *level moderate* yaitu notifikasi sistem tidak tampil pada *Operation System* (OS) tertentu, *handphone*, data dan informasi tidak sesuai fakta, *server down*, sistem *crash*, data *corrupt* / rusak, 8 kemungkinan risiko dengan *level* risiko *low to moderate* yaitu listrik padam, kebocoran data atau informasi, target penggunaan sistem per-bulan tidak tercapai, *backup failure* atau gagal melakukan fungsi media penyimpanan, serangan *virus*, informasi diakses oleh pihak yang tidak berwenang, gagal *update*, *overheat* perangkat *hardware*, dan 11 kemungkinan risiko dengan *level* risiko *low* yaitu *database error*, koneksi jaringan terputus, kurang baiknya kualitas jaringan, penyalahgunaan hak akses atau *user* ID, kerusakan *hardware*, kebakaran, gempa bumi, petir, mantan *user*/karyawan masih memiliki akses informasi, banjir, dan debu atau kotoran.

Rekomendasi yang dihasilkan untuk kemungkinan risiko hilangnya data, *hacking*, notifikasi sistem tidak tampil pada *Operation System* (OS) tertentu, *human error*, data dan informasi tidak sesuai fakta, *server down*, sistem *crash*, data *corrupt* atau rusak, listrik padam, kebocoran data atau informasi, target penggunaan sistem per-bulan tidak tercapai, *backup failure* atau gagal melakukan fungsi media penyimpanan, serangan *virus*, informasi diakses oleh pihak yang tidak berwenang, gagal *update*, *overheat* perangkat *hardware*, *database error*, kurang baiknya kualitas jaringan, penyalahgunaan hak akses atau *User* ID, kerusakan *hardware*, kebakaran, gempa bumi, petir, mantan *user*/karyawan masih memiliki akses informasi, dan debu atau kotoran diberikan perlakuan risiko Mitigasi (*mitigation*), yaitu melakukan perlakuan risiko untuk mengurangi kemungkinan timbulnya risiko, atau mengurangi dampak risiko bila terjadi, atau mengurangi keduanya, untuk risiko koneksi jaringan terputus diberikan rekomendasi perlakuan risiko berbagi risiko (*risk sharing* / *risk transfer*) yaitu, suatu tindakan untuk mengurangi kemungkinan timbulnya risiko atau dampak risiko dengan berbagi kemungkinan risiko dengan pihak ketiga dalam hal ini yaitu penyedia *hosting* atau *cloud server*. Dan untuk kemungkinan risiko banjir diberikan rekomendasi perlakuan mitigasi (*mitigation*), yaitu penanganan risiko untuk mengurangi kemungkinan timbulnya risiko, atau mengurangi dampak risiko bila terjadi, atau mengurangi keduanya, hal ini diterapkan pada kegiatan harian karyawan.

DAFTAR PUSTAKA

[1] Ardiyah, I., Okra, R., & Musril, H. A, "Perancangan sistem absensi siswa dengan menerapkan SSO (Single sign on) di SMKN 1 Lembah Melintang", *Humantech: Jurnal Ilmiah Multidisiplin Indonesia*, vol. 2, no. 3, p. 572-577, 2022.

[2] Nurhasanah, S., & Harahap, A. A, "Evaluasi Tingkat Kesiapan Pengguna Sistem Single Sign On Pada Portal Universitas Alma Ata Menggunakan Metode Technology Readiness Index (TRI), *Indonesian Journal of Business Intelligence (IJUBI)*, vol. 5, no. 1, p. 1-10, 2022.

[3] Elsera, M, "Implementasi Single Sign On Pada Web Menggunakan Protocol Oauth Facebook", *Buletin Utama Teknik*, vol. 16, no. 3, p. 179-185, 2021.

[4] Fachrezi, M. I, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000: 2018 Diskominfo Kota Salatiga", *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 8, no. 2, p. 764-773, 2021.

[5] Mahardika, K. B., Wijaya, A. F., & Cahyono, A. D, "Manajemen risiko teknologi informasi menggunakan iso 31000: 2018 (studi kasus: cv. xy), *Sebatik*, vol. 23, no. 1, p. 277-284, 2019.

[6] Setiawan, I., Sekarini, A. R., Waluyo, R., & Afiana, F. N, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto", *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, p. 389-396, 2021.

[7] 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. Pengembangan Teknologi Informasi dan Ilmu Komputer., vol. 2, no. 11, pp. 4991–4998, 2018.

[8] Asshaf, M. N. R, "Analysis of Work Accident Risk Factors in Palm Tree Tapping Farmers or Arenga Pinnata Using Hazard Identification Risk Assessment and Risk Control Methods", *Jurnal Penelitian Perawat Profesional*, vol. 2, no. 3, p. 325-336, 2020.

[9] Albar, M. E., Parinduri, L., & Sibuea, S. R, "Analisis Potensi Kecelakaan Menggunakan Metode Hazard Identification and Risk Assessment (HIRA)", *Buletin Utama Teknik*, vol. 17, no. 3, p. 241-245, 2022.

[10] Auliaullah, N. N., Sutari, W., & Salma, S. A, "Perancangan Treatment Risiko Pada Proses Produksi Pipa Baja Di Pt Xyz Menggunakan Pendekatan Risk Management Process Berdasarkan Iso 31000: 2018 Klausul 6.4 Untuk Memenuhi Persyaratan Iso 9001: 2015 Klausul 6.1", *eProceedings of Engineering*, vol. 8, no. 5, 2021.