Infotekmesin
Vol.14, No.02, Juli 2023
p-ISSN: 2087-1627, e-ISSN: 2685-9858
DOI: 10.35970/infotekmesin.v14i2.1877, pp.237-243

Manajemen Risiko Teknologi Informasi Aplikasi *E-Office* ASN Menggunakan ISO 31000:2018

Fathoni Mahardika[1*], Muhammad Agreindra H[2], Siti Ainun Fatimah[3] , Lusi Tsulutsiah Nur F[4]
[1, 2,3,4]Program Studi Informatika, Fakultas Teknologi Informasi Universitas Sebelas April
[1,2,3,4]Jln. Angkrek Situ No.19 Sumedang, Jawa Barat 45323
E-mail: fathoni@unsap.ac.id[1], agreindra@unsap.ac.id[2] , a2.1900168@mhs.stmik-sumedang.ac.id[3], a2.1900097@mhs.stmik-sumedang.ac.id[4]

Info Naskah:
Naskah masuk: 27 April 2023
Direvisi : 23 Juni 2023
Diterima: 24 Juni 2023

Abstrak

Dalam melaksanakan tugas urusan pemerintahan pada Diskominfosanditik Kabupaten Sumedang, maka diterapkan sistem *E-Government* yaitu aplikasi *E-Office* ASN yang merupakan aplikasi berbasis *website* dan berbasis *mobile* dengan spesifikasi minimal android 4 yang digunakan oleh seluruh ASN (Aparatur Sipil Negara) yang terdiri dari PNS (Pegawai Negeri Sipil) dan PPPK (Pegawai Pemerintah dengan Perjanjian Kerja) yang ada di Kabupaten Sumedang. Dengan adanya aplikasi tersebut memungkinkan adanya ancaman dan serangan meliputi *vulnerability* yang menimbulkan risiko, dimana hal tersebut mengganggu proses penggunaan aplikasi tersebut. Oleh karena itu peneliti memutuskan untuk melakukan penelitian manajemen risiko teknologi informasi sebagai penanganan dan perlindungan terhadap aplikasi tersebut dengan menerapkan proses manajemen risiko dari *ISO* 31000:2018 di mana setiap informasi yang dibutuhkan dalam penelitian ini didapatkan dari sumber-sumber internal yang ada di Diskominfosanditik Kabupaten Sumedang. Penelitian ini dilakukan pada bagian bidang informatika dengan menghasilkan terdapat 14 kemungkinan risiko yang terdiri dari 3 risiko dengan *level high*, 2 risiko dengan *level medium*, dan 9 risiko dengan *level low*. Dari pengukuran *GAP* terdapat selisih bahwa perlunya manajemen risiko sebagai langkah awal untuk pengelolaan risiko.

Keywords:
risk management;
e-office;
asn;
ISO 31000;

Abstract

In carrying out the task of government affairs at Diskominfosanditik Sumedang Regency, an E-Government system is implemented, namely the ASN E-Office application which is a website-based and mobile-based application with a minimum specification of Android 4 which is used by all ASN (State Civil Apparatus) consisting of PNS (Civil Servants) and PPPK (Government Employees with Work Agreements) in Sumedang Regency. With this application, there may be threats and attacks including vulnerabilities that pose a risk, which disrupt the process of using the application. Therefore, the researcher decided to conduct information technology risk management research as a handling and protection of the application by applying the risk management process from ISO 31000:2018 where any information needed in this research was obtained from internal sources at Diskominfosanditik Sumedang Regency. This research was conducted in the informatics section and resulted in 14 possible risks consisting of 3 risks with high levels, 2 risks with medium levels, and 9 risks with low levels. From the GAP measurement, there is a difference that the need for risk measurement as the first step for risk management.

***Penulis korespondensi:**
Fathoni Mahardika
E-mail: fathoni@unsap.ac.id

1. Pendahuluan

Dinas Komunikasi dan Informatika, Persandian, dan Statistik (Diskominfosanditik) Kab Sumedang merupakan instansi pemerintahan yang bertugas menjalankan kegiatan pemerintahan kewenangan daerah dalam bidang komunikasi dan informatika, bidang statistik, dan bidang persandian serta tugas pembantuan yang diberikan kepada daerah. Pada pelaksanaan tugasnya, Diskominfosanditik didukung dengan teknologi informasi pada dinas tersebut yaitu diterapkannya sistem *E-Government*. *E-Office (Elektronik Office)* adalah salah satu penerapan dari penggunaan teknologi informasi untuk memudahkan ASN dalam tata kelola kegiatan sehari-harinya.

E-Office yang diterapkan di Diskominfosanditik yaitu *E-Office* ASN (Aparatur Sipil Negara). *E-Office* ASN merupakan aplikasi berbasis website dan berbasis mobile dengan spesifikasi minimal android 4 yang digunakan oleh seluruh pegawai pemerintah ASN (Aparatur Sipil Negara) yang terdiri dari PNS (Pegawai Negeri Sipil) dan PPPK (Pegawai Pemerintah dengan Perjanjian Kerja) yang ada di Kabupaten Sumedang. Pada dasarnya aplikasi ini digunakan untuk surat menyurat, absensi, dan manajemen kinerja dari para ASN. Namun seiring berjalannya waktu, di dalam aplikasi *E-Office* ASN tersebut terdapat beberapa Sistem Informasi mengenai tata naskah surat, kegiatan dan agenda, manajemen kinerja, tata pemerintahan, informasi lembaga, web SKPD/Kecamatan, dan aplikasi kedinasan lainnya.

Penggunaan aplikasi tersebut menimbulkan beberapa masalah yang menjadikan kemungkinan adanya ancaman dan serangan berupa *vulnerability* yang menimbulkan risiko serta bisa mengganggu dalam proses penggunaan aplikasi tersebut. Oleh karena itu, begitu pentingnya manajemen risiko sebagai alat untuk melakukan penanganan terhadap kemungkinan ancaman yang muncul suatu saat nanti, selain itu manajemen risiko dilakukan untuk meminimalisir risiko-risiko yang ada dan bisa terjadi kapan saja tanpa diketahui. Selain itu Aplikasi *E-Office* menyimpan beberapa data penting yang berhubungan dengan privasi pegawai maka hal ini bisa kemungkinan mengundang ancaman baik dari internal atau eksternal yang bisa muncul suatu saat. Maka dengan adanya permasalahan diatas, dibutuhkan sebuah mekanisme atau aturan yang bisa melindungi para pengguna *E-Office* dalam hal menjaga keamanan data atau privasi data. *ISO* (*International Organization for Standardization*) sebagai salah satu badan yang mengeluarkan standarisasi internasional, mengeluarkan sebuah standarisasi untuk Manajemen Risiko, yaitu *ISO* 31000:2018, dengan standar *ISO* ini setidaknya memberikan penegasan bahwa untuk pengelolaan risiko dibutuhkan standar yang jelas karena berhubungan dengan proses pengamanan atau manajemen keamanan informasi. *ISO* 31000:2018 merupakan sebuah standar internasional yang disusun dengan tujuan memberikan prinsip dan panduan generik untuk penerapan manajemen risiko. Proses manajemen risiko melibatkan penerapan sistematis dari kebijakan, prosedur dan praktik pada aktivitas komunikasi dan konsultasi, penetapan konteks, serta penilaian, peninjauan hingga pelaporan risiko [1][2][3].

Berdasarkan penjelasan di atas, maka peneliti akan melakukan sebuah kajian dan studi ilmiah tentang Manajemen Risiko Teknologi Informasi Aplikasi *E-Office* ASN pada Diskominfosanditik Kabupaten Sumedang dengan menggunakan metode *ISO* 31000:2018. Penulis telah melakukan studi literatur di mana ada beberapa penelitian yang menjadi acuan serta perbandingan dalam penelitian ini. Manajemen Risiko Teknologi Informasi pada Penerapan *E-Recruitment* berbasis *ISO* 31000:2018 dengan *FMEA* (Studi Kasus PT Pertamina) oleh Hanafi Indra Pribadia dan Ernastuti menghasilkan sebanyak 3 jenis potensial risiko dan 28 atribut resiko, setelah dilakukan penilaian risiko maka didapatkan hasil bahwa 7 atribut risiko memerlukan perhatian khusus dalam proses penerapan sistem agar dapat berjalan dengan baik untuk kedepannya. Kemudian terdapat penelitian yang berjudul Sistem Manajemen Risiko Keamanan Aset Teknologi Informasi menggunakan *ISO* 31000:2018 oleh Reski Mai Candra at., al menghasilkan 45 risiko secara keseluruhan untuk aset, terdapat 14 risiko *level* rendah, 16 risiko *level* menengah, dan 15 risiko level tinggi. Manajemen Risiko Teknologi Informasi menggunakan ISO 31000:2018 (Studi Kasus: CV. XY) oleh Krisdana Bima Mahardika at., al menghasilkan kemungkinan–kemungkinan risiko dengan berbagai tingkatan. Maka peneliti menyimpulkan bahwa IT CV. XY belum memenuhi syarat standar ISO 31000:2018, dikarenakan dari beberapa tahapan pengamatan, wawancara, serta penilaian terhadap risiko itu sendiri masih banyak temuan risiko yang belum bisa terpecahkan oleh perusahaan [4].

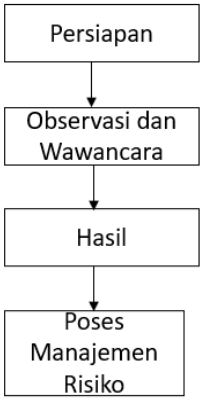
Adapun tujuan utama penelitian ini adalah untuk menerapkan manajemen risiko teknologi informasi menggunakan standar ISO 31000:2018 dalam rangka penanganan dan perlindungan terhadap aplikasi *E-Office* ASN yang digunakan oleh ASN (Aparatur Sipil Negara) di Kabupaten Sumedang. Tujuan tersebut dijabarkan melalui beberapa langkah. Pertama, tujuan penelitian ini adalah untuk mengidentifikasi dengan cermat kemungkinan risiko yang dapat terjadi dalam penggunaan aplikasi *E-Office* ASN oleh para PNS (Pegawai Negeri Sipil) dan PPPK (Pegawai Pemerintah dengan Perjanjian Kerja) di Kabupaten Sumedang. Selanjutnya, penelitian ini bertujuan untuk menentukan tingkat risiko dari setiap risiko yang diidentifikasi, berdasarkan kriteria yang relevan dan mengacu pada standar ISO 31000:2018.

Selain itu, penelitian ini juga bertujuan untuk mengukur kesenjangan (GAP) antara kondisi resiko aktual yang terdapat dalam penggunaan aplikasi *E-Office* ASN dan kondisi risiko yang diinginkan atau yang sesuai dengan standar ISO 31000:2018. Dengan melakukan pengukuran GAP ini, diharapkan dapat diidentifikasi kebutuhan akan manajemen risiko sebagai langkah awal dalam pengelolaan risiko yang terkait dengan aplikasi *E-Office* ASN. Terakhir, penelitian ini memiliki tujuan untuk memberikan rekomendasi konkret mengenai tindakan pengelolaan risiko yang dapat diimplementasikan oleh pihak berwenang untuk mengurangi risiko dan meningkatkan keamanan penggunaan aplikasi *E-Office* ASN di Kabupaten Sumedang. Tujuan kenapa harus menggunakan *framework* tersebut karena kebutuhan instansi berkaitan dalam pengelolaan risiko yang lebih lengkap dan teratur.

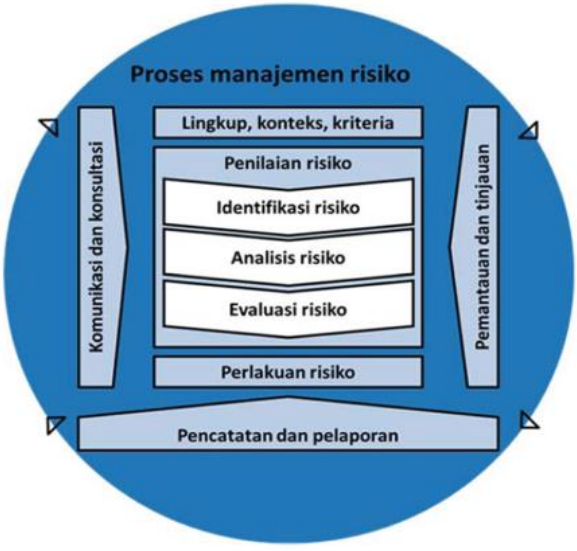
2. Metode

Penelitian ini dilakukan dengan cara pendekatan kualitatif, dimana proses pengumpulan data yang ada berupa pernyataan-pernyataan yang berisikan isu-isu, kajian, persoalan atau masalah yang ada disesuaikan dengan situasi, kondisi serta realita yang ada pada Diskominfosanditik. Hasil dari penelitian ini nantinya digunakan sebagai landasan untuk bahan evaluasi atau perbaikan yang ada pada aplikasi *E-Office* ASN pada Diskominfosanditik Kabupaten Sumedang [5][6][7].

Teknik pengumpulan data yang digunakan yaitu metode wawancara. Metode wawancara ini sasarannya adalah bagian bidang informatika yaitu admin aplikasi *E-Office* ASN dengan tujuan mencari data berupa risiko-risiko yang timbul dari aplikasi tersebut. Selain menggunakan teknik pengumpulan data menggunakan metode wawancara, metode yang digunakan adalah metode analisis manajemen risiko yang mengacu kepada *ISO* 31000:2018 [8]. Tahapan metode penelitian yang dilakukan dalam penyusunan paper ini dapat dilihat pada gambar 1:



Gambar 1. Metode Penelitian



Gambar 2. Proses *Risk Management ISO 31000:2018*

Gambar 2 merupakan proses manajemen risiko menggunakan ISO 31000:2018 yang terdiri dari:

a) Komunikasi dan Konsultasi
b) Lingkup, Konteks, dan Kriteria
c) Penilaian Risiko
d) Perlakuan Risiko
e) Pemantauan dan Tinjauan

Setelah melakukan beberapa tahapan diatas tentang manajemen risiko, penulis akan menentukan *level* dari tiap risiko yang ada pada area yang diteliti [5] [9][4]

3. Hasil dan Pembahasan

3.1 Komunikasi dan Konsultasi

Pada tahap ini, peneliti melakukan pengajuan penelitian terkait manajemen risiko teknologi informasi ke instansi Diskominfosanditik Kabupaten Sumedang yang diawali dengan menghubungi Staf Bagian Umum dan kemudian setelah itu peneliti melakukan diskusi dan wawancara kepada staff bagian informatika [10][11].

3.2 Lingkup, Konteks, dan Kriteria

Peneliti memastikan penelitian dengan menghubungi Staf Bagian Umum kembali yang kemudian diarahkan pada Staf Bagian Informatika. Berdasarkan hasil diskusi dan rekomendasi dan kajian yang ada maka peneliti melakukan riset pada aplikasi *E-Office* ASN yang memiliki pengguna banyak dan hal ini berdasarkan laporan dari user atau admin bahwa aplikasi tersebut memiliki risiko yang tinggi dari adanya bug, serangan atau ancaman dan lain sebagainya.

3.3 Penilaian Risiko

Tabel 1 adalah proses penilaian risiko, sama seperti tahapan yang ada pada beberapa artikel/jurnal kegiatan penilaian ini didasari dari proses yang dihasilkan Identifikasi Risiko (*Risk Identification*), Analisis Risiko (*Risk Analysis*), dan Evaluasi Risiko (*Risk Evaluation*) [12] [13][14][15]. Setelah dilakukan penilaian risiko, selanjutnya dilakukan evaluasi risiko berdasarkan matriks evaluasi risiko yang dapat dilihat dan dipetakan pada gambar 3. Hasil dari evaluasi risiko dapat dilihat pada tabel 2, di mana pada tabel tersebut dapat diketahui level dari setiap risiko yang sudah diidentifikasi sebelumnya.

Tabel 1. Penilaian Identifikasi Risiko

NO	*IT Resources*	Identifikasi Risiko	Frekuensi Kejadian	Dampak yang Diakibatkan
(1)	(2)	(3)	(4)	(5)
1.	*Application*	Aplikasi Mengalami *crash* (down) atau sering *Force Close* **(A1)**	2	1
		Aplikasi *Bug* ketika digunakan **(A2)**	4	3
		Aplikasi mengalami *error* ketika digunakan **(A3)**	3	3
2.	*Information*	Data *corrupt* **(Inf1)**	2	2

NO	*IT Resources*	Identifikasi Risiko	Frekuensi Kejadian	Dampak yang Diakibatkan
(1)	(2)	(3)	(4)	(5)
		Penyalahgunaan hak akses **(Inf2)**	1	1
		Kegagalan dalam *Backup* Data **(Inf3)**	2	1
3.	Infrastruktur	Kerusakan *Hardware* **(IN1)**	2	2
		Koneksi jaringan bermasalah **(IN2)**	3	3
		Gangguan Server **(IN3)**	2	2
		Listrik Padam **(IN4)**	1	1
4.	People	Dokumentasi pengguna aplikasi yang kurang lengkap **(P1)**	2	2
		Kelalaian dalam memasukkan data **(P2)**	3	4
		Maintenance tidak terjadwal **(P3)**	4	4
		Keterbatasan SDM **(P4)**	1	1

5					
4			**A2**	**P3**	
3			**A3, IN2**	**P2**	
2	**A1, Inf3**	**Inf1, IN1, IN3, P1**			
1	**Inf2, IN4, P4**				
	1	**2**	**3**	**4**	**5**

Gambar 3. Matrix Evaluasi Risiko

Tabel 2. Evaluasi Risiko menurut Frekuensi dan Dampak

Kode Identifikasi Risiko	Identifikasi Risiko	Frekuensi Kejadian	Dampak yang Diakibatkan	Evaluasi
(1)	(2)	(3)	(4)	(5)
A1	Aplikasi Mengalami *crash* (down) ering *Force Close*.	2	1	*Low*
A2	Aplikasi *Bug* ketika digunakan	4	3	*High*
A3	Aplikasi mengalami *error* ketika digunakan	3	3	*Medium*
Inf1	*Data corrupt*	2	2	*Low*
Inf2	Penyalahgunaan hak akses	1	1	*Low*
Inf3	Kegagalan dalam *Backup Data*	2	1	*Low*
IN1	Kerusakan *Hardware*	2	2	*Low*
IN2	Koneksi jaringan bermasalah	3	3	*Medium*
IN3	Gangguan Server	2	2	*Low*
IN4	Listrik Padam	1	1	*Low*
P1	Dokumentasi pengguna aplikasi yang kurang lengkap	2	2	*Low*
P2	Kelalaian dalam memasukkan data	3	4	*High*
P3	*Maintenance* tidak terjadwal	4	4	*High*
P4	Keterbatasan SDM	1	1	*Low*

3.4 Perlakuan Risiko

Pada tabel 3 merupakan penjelasan tahapan perlakuan risiko, prosesnya dilakukan dengan cara melakukan strategi perlakuan risiko, dimana proses yang paling tepat dalam mengatasi permasalahan yang sesuai dengan pembahasan ini adalah dengan melakukan proses *Risk Reduction* (Mengurangi Risiko atau Mitigasi risiko meliputi proses kegiatan tahapan pengurangan *likelihood*, pengurangan dampak, dan pengurangan *likelihood* dan dampak sekaligus) [11][12][13][14][15].

Tabel 3. Program Penanganan Risiko

NO	*IT Resources*	Identifikasi Risiko	Program Penanganan Risiko
(1)	(2)	(3)	(4)
1.	*Application*	Aplikasi Mengalami *crash* (down) atau sering *force close*. **(A1)**	Melakukan perbaikan sistem aplikasi dan membuat peraturan pencegahan instalasi aplikasi lain yang bisa menyebabkan aplikasi utama mengalami *crash* atau *force close*. Atau dengan cara membuat user akses untuk proses instalasi aplikasi.
		Aplikasi *Bug* ketika digunakan **(A2)**	Melakukan peningkatan kembali dalam pembuatan dan pengembangan aplikasi.
		Aplikasi mengalami *error* ketika digunakan **(A3)**	Melakukan *refresh* (muat ulang) dan periksa koneksi internet.
2.	*Information*	*Data corrupt* **(Inf1)**	Lakukan *disk check* secara manual dan *back up data* secara rutin.

NO	*IT Resources*	Identifikasi Risiko	Program Penanganan Risiko
(1)	(2)	(3)	(4)
		Penyalahgunaan hak akses **(Inf2)**	Membatasi beberapa user dalam mengakses aplikasi atau membuat hak akses tertentu, hal ini dilakukan supaya memberikan akses kepada user yang benar-benar bertanggungjawab dan dipercaya atau user saja.
		Kegagalan dalam *Backup Data* **(Inf3)**	Penggunaan *password* untuk aplikasi dan media harus memiliki enkripsi yang sangat baik. Menggunakan media penyimpanan secara *online*, harus dari *provider cloud computing* yang benar-benar terpercaya, memiliki alamat kantor yang jelas dan memiliki *support* selama 24 jam penuh.
3.	Infrastruktur	Kerusakan *Hardware* **(IN1)**	Melakukan perawatan *hardware* secara rutin.
		Koneksi jaringan bermasalah **(IN2)**	Mengganti ISP (*Internet Service Provider*) ke yang lebih baik atau Dinas melakukan Kerjasama dengan ISP khusus.
		Gangguan *Server* **(IN3)**	Ada kebijakan/aturan tentang pengecekan *server* secara berkala dan adanya jadwal maintenance *server* atau update *server* yang jelas
		Listrik Padam **(IN4)**	Menyediakan listrik cadangan/*generator set* dan UPS (*Uninterruptible Power Supply*) dengan daya sesuai dengan kebutuhan.
4.	People	Dokumentasi pengguna aplikasi yang kurang lengkap **(P1)**	Setiap ada perubahan menu atau fitur baru yang ada di aplikasi *E-Office* ASN, harus langsung dikoordinasikan ke bagian dokumentasi sehingga bagian di dokumentasi langsung membuat dokumen penggunaan aplikasi yang paling *update*. Selain itu, harus senantiasa mengadakan sosialisasi setiap ada perubahan pada aplikasi tersebut.
		Kelalaian dalam memasukkan data **(P2)**	Data-data yang akan dimasukkan dalam aplikasi *E-Office* ASN di cek terlebih dahulu dan meningkatkan fokus saat memasukkan data.
		Maintenance tidak terjadwal **(P3)**	Perlu adanya jadwal *maintenance* secara berkala sehingga aplikasi tersebut dapat terpantau dengan baik. Selain itu juga harus membuat jadwal untuk adanya program *maintenance* tersebut.
		Keterbatasan SDM **(P4)**	Memanfaatkan SDM yang ada, apabila kekurangan maka menambah karyawan baru.

3.5 Pemantauan dan Tinjauan

Tahapan terakhir meliputi pemantauan dan tinjauan, pada proses ini menunjukan bahwa penelitian sudah selesai dilaksanakan, seluruh proses manajemen risiko dari aplikasi yang diteliti sudah dilakukan dan menghasilkan beberapa kemungkinan risiko [16][17]. Hasil penelitian ini berupa dokumentasi aturan yang berisikan dokumentasi terkait penanganan risiko yang ada di aplikasi *E-Office* ASN Diskominfosanditik Kabupaten Sumedang. Selain itu juga, akan mengkomunikasikan dan melaporkan *progress* manajemen risiko dari Aplikasi *E-Office* ASN. Hasil penelitian diharapkan, dapat memberikan masukan berupa kritik dan saran yang bisa membangun untuk pihak-pihak yang terlibat secara langsung dalam pengelolaan aplikasi yang ada di Diskominfosanditik. Pada tabel 4 dan tabel 5 dapat dilihat terdapat penilaian kondisi sebelum dan sesudah melakukan manajemen risiko pada aplikasi *E-office* ASN.

Tabel 4. Aplikasi *E-Office* ASN Kondisi Saat Ini dan Kondisi yang Diharapkan

No	Pertanyaan	Kondisi Saat Ini (As is)						Kondisi yang Diharapkan (To be)					
		0	1	2	3	4	5	0	1	2	3	4	5
1	Sejauh mana Diskominfosanditik Kabupaten Sumedang mendefinisikan upaya analisis risiko yang sesuai, mengingat semua faktor-faktor risiko dalam aplikasi *E-Office* ASN.		√								√		
2	Sejauh mana Diskominfosanditik Kabupaten Sumedang membangun dan menambah skenario risiko aplikasi *E-Office* ASN secara teratur, termasuk dari jenis risiko yang tidak terduga.		√							√			
3	Sejauh mana Diskominfosanditik Kabupaten Sumedang memperkirakan frekuensi dan besarnya untung rugi terhadap risiko aplikasi *E-Office* ASN.	√								√			
4	Sejauh mana Diskominfosanditik Kabupaten Sumedang menerima toleransi risiko dan mengidentifikasi hal yang memerlukan tindakan risiko pada aplikasi *E-Office* ASN.	√								√			
5	Sejauh mana Diskominfosanditik Kabupaten Sumedang menganalisis untung rugi dari kemungkinan pilihan seperti menghindari, mengurangi, memindahkan, mengambil, serta mengusulkan tindakan yang optimal.		√								√		
6	Sejauh mana Diskominfosanditik Kabupaten Sumedang menentukan *high-level requirements*	√									√		

No	Pertanyaan	Kondisi Saat Ini (As is)						Kondisi yang Diharapkan (To be)					
		0	1	2	3	4	5	0	1	2	3	4	5
	terhadap aplikasi *E-Office* ASN dalam melakukan tanggapan terhadap risiko yang terpilih												
7	Sejauh mana Diskominfosanditik Kabupaten Sumedang memvalidasi hasil analisis risiko sebelum digunakan untuk pengambilan keputusan, memastikan bahwa analisis sejajar dengan persyaratan perusahaan dan memverivikasi perkiraan itu benar.			√								√	

Tabel 5. Rekapitulasi Jawaban Kuesioner

No	Pertanyaan	Status	Distribusi Jawaban					
			0	1	2	3	4	5
1	Sejauh mana Diskominfosan ditik Kabupaten Sumedang mendefinisikan upaya analisis risiko yang sesuai, mengingat semua faktor-faktor risiko dalam aplikasi *E-Office* ASN.	*As is*		100				
		To be				100		
2	Sejauh mana Diskominfosan ditik Kabupaten Sumedang membangun dan menambah skenario risiko aplikasi *E-Office* ASN secara teratur, termasuk dari jenis risiko yang tidak terduga.	*As is*		100				
		To be			100			
3	Sejauh mana Diskominfosan ditik Kabupaten Sumedang memperkirakan frekuensi dan besarnya untung rugi terhadap risiko aplikasi *E-Office* ASN.	*As is*	100					
		To be			100			
4	Sejauh mana Diskominfosan ditik Kabupaten Sumedang menerima toleransi risiko dan mengidentifikasi hal yang memerlukan tindakan risiko pada aplikasi *E-Office* ASN.	*As is*	100					
		To be			100			
5		*As is*		100				
	Sejauh mana Diskominfosan ditik Kabupaten Sumedang menganalisis untung rugi dari kemungkinan pilihan seperti menghindari, mengurangi, memindahkan, mengambil, serta mengusulkan tindakan yang optimal.	*To be*				100		
6	Sejauh mana Diskominfosan ditik Kabupaten Sumedang menentukan *high-level requirements* terhadap aplikasi *E-Office* ASN dalam melakukan tanggapan terhadap risiko yang terpilih	*As is*	100					
		To be				100		
7	Sejauh mana Diskominfosan ditik Kabupaten Sumedang memvalidasi hasil analisis risiko sebelum digunakan untuk pengambilan keputusan, memastikan bahwa analisis sejajar dengan persyaratan perusahaan dan memverifikasi perkiraan itu benar.	*As is*			100			
		To be					100	
	Total	*As is*	42,85	42,85	14,28	0	0	0
		To be	0	0	42,85	42,85	14,28	0

Rumus menentukan GAP yaitu:

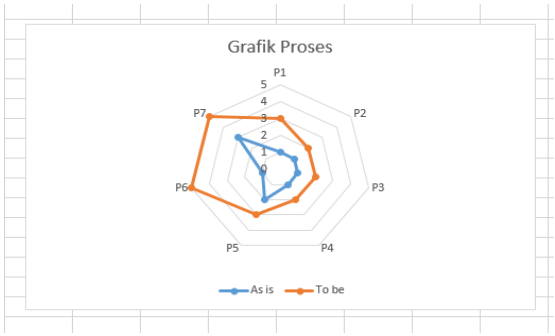
$$R_{xy} = \frac{\sum x}{\sum y} \quad (1)$$

Keterangan:

R_{xy} = Hasil GAP

$\sum x$ = Jumlah jawaban

$\sum y$ = Jumlah pertanyaan



Gambar 3. GAP Keadaan Sebelum dan Sesudah

Berdasarkan rumus perhitungan GAP didapatkan GAP (selisih) yang dapat dilihat pada gambar 3 di mana kondisi sebelum dan sesudah dilakukan penilaian risiko terlihat bahwa penilaian risiko diperlukan sebagai dasar untuk pengambilan keputusan lembaga dalam hal ini Diskominfosanditik Sumedang.

4. Kesimpulan

Kesimpulan yang dihasilkan dari penelitian ini didapatkan sebanyak 14 kemungkinan resiko yang ada pada Diskominfosanditik yang terdiri dari: 3 risiko dengan level *high* (tinggi), yaitu Aplikasi *bug* ketika digunakan **(A2)**, Kelalaian dalam memasukkan data **(P2)**, dan Maintenance tidak terjadwal **(P3)**. 2 risiko dengan level *medium*, yaitu Aplikasi mengalami *error* ketika digunakan **(A3)** dan Koneksi jaringan bermasalah **(IN2)**. 9 risiko dengan level *low*, yaitu Aplikasi Mengalami *Crash (down)* **(A1)**, Data *corrupt* **(Inf1)**, Penyalahgunaan hak akses **(Inf2)**, Kegagalan dalam *Backup Data* **(Inf3)**, Kerusakan *Hardware* **(IN1)**, Gangguan Server **(IN3)**, Listrik padam **(IN4)**, Dokumentasi pengguna aplikasi yang kurang lengkap **(P1)**, dan Keterbatasan SDM **(P4)**. Adanya GAP kondisi risiko sebelum dan sesudah menggambarkan bahwa risiko ini perlu dikelola, dengan *framework ISO* 31000 setidaknya risiko bisa dikelola dan ditangani sesuai dengan hasil perlakuannya yang sudah ditentukan sebelumnya.

Saran untuk penelitian selanjutnya tidak hanya sebatas melakukan manajemen risiko atau pengelolaan risiko dengan *framework ISO* 31000:2018, akan tetapi bisa menggabungkan dengan beberapa *framework* lain seperti *FISMA, NIST, COBIT* sehingga bisa menghasilkan dokumentasi kebijakan yang lebih lengkap tentang pengelolaan Manajemen Keamanan Informasi di instansi tersebut.

Ucapan Terimakasih

Terimakasih yang kepada pihak Diskominfosanditik Kab. Sumedang yang telah memberikan kesempatan untuk melakukan kajian atau riset tentang manajemen risiko pada instansi tersebut.

Daftar Pustaka

[1] Y. H. Akbar and L. Nurhayati, "Information System Risk Management Analysis Using Octave-S Method," *J-Sin's-Jurnal Sist. Inf.*, vol. 3, no. 2, 2019.

[2] F. A. Hardianto and Y. S. Dharmawan, "Manajemen Risiko TI ISO 31000 Dengan Cobit 5 Dan FMEA (PT. XYZ)," *J. SITECH Sist. Inf. dan Teknol.*, vol. 4, no. 2, pp. 133–146, 2021.

[3] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," vol. 02, no. 02, 2017.

[4] 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.

[5] R. M. Candra, Y. N. Sari, I. Iskandar, and F. Yanto, "Sistem Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000: 2018," *J. CoreIT*, vol. 5, no. 1, pp. 19–28, 2019.

[6] M. I. Fachrezi, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000: 2018 Diskominfo Kota Salatiga," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 2, pp. 764–773, 2021.

[7] 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.

[8] H. I. Pribadi and E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000: 2018 Dengan FMEA (Studi Kasus PT Pertamina)," *JSINBIS (Jurnal Sist. Inf. Bisnis)*, vol. 10, no. 1, pp. 28–35, 2020.

[9] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, pp. 91–96, 2020.

[10] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analisis manajemen risiko keamanan data sistem informasi (Studi kasus: RSUD XYZ)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, pp. 282–287, 2018.

[11] I. P. A. E. Pratama and M. T. S. Pratika, "Manajemen risiko teknologi informasi terkait manipulasi dan peretasan sistem pada Bank XYZ tahun 2020 menggunakan ISO 31000: 2018," *J. Telemat.*, vol. 15, no. 2, pp. 63–70, 2020.

[12] R. Budiarto, "Manajemen risiko keamanan sistem informasi menggunakan metode fmea dan iso 27001 pada organisasi xyz," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 2, no. 2, pp. 48–58, 2017.

[13] W. Harefa and K. D. Hartomo, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000: 2018 Pada Sistem Informasi Gudang," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 1, pp. 407–420, 2022.

[14] E. Saputra, C. Rudianto, and P. F. Tanaem, "Analisis Resiko Sistem Informasi Penjualan Berbasis ISO 31000: Study Kasus PT XYZ," *J. Pengemb. Sist. Inf. dan Inform.*, vol. 3, no. 1, pp. 1–10, 2022.

[15] H. Hardjomidjojo, C. Pranata, and G. Baigorria, "Rapid assessment model on risk management based on ISO 31000: 2018," in *IOP Conference Series: Earth and Environmental Science*, 2022, vol. 1063, no. 1, p. 12043.

[16] H. Qinthara, W. Sutari, and S. A. Salma, "Design of Risk Management System on Material Handling Services to Fulfill ISO 9001: 2015 Requirements Clause 6.1 Based on ISO 31000: 2018," *JKIE (Journal Knowl. Ind. Eng.*, vol. 8, no. 3, pp. 154–166, 2021.

[17] D. Hendarwan, "Penerapan Manajemen Resiko (Risk Management) Dengan Pendekatan Iso 31000: 2018 Dalam Pelaksanaan Strategi Perusahaan," *Adminika*, vol. 8, no. 1, pp. 58–72, 2022.