ANALISIS RISIKO MENGGUNAKAN ISO 31000 : 2018 DALAM PENGELOLAAN APLIKASI PADA KECAMATAN DAN OPD KABUPATEN SIDOARJO

Ardicca Citra S, Ilham, M.Andik Izzudin
Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Ampel Surabaya
Jl. Ahmad Yani No.177, Jemur Wonosari, Kec. Wonocolo, Surabaya, Indonesia
ardiccabila9307@gmail.com)

ABSTRAK

Penelitian ini bertujuan untuk menganalisis risiko dalam pengelolaan aplikasi di Organisasi Perangkat Daerah (OPD) dan kecamatan di Kabupaten Sidoarjo menggunakan kerangka kerja ISO 31000:2018. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan melakukan identifikasi, analisis, dan evaluasi risiko berdasarkan pengumpulan data melalui studi pustaka, wawancara, dan observasi langsung. Hasil penelitian mengungkapkan bahwa terdapat sembilan risiko utama yang teridentifikasi, di mana satu risiko dikategorikan sangat tinggi, yaitu serangan siber/hacking (R01). Selain itu, terdapat lima risiko yang termasuk dalam kategori sedang, yaitu gangguan layanan/downtime (R02), tidak adanya kontrol penuh terhadap aplikasi dan database (R03), pembengkakan biaya pengadaan, pengembangan, dan pemeliharaan aplikasi (R06), serta perubahan atau pemutusan kontrak dengan pihak ketiga (R09). Tiga risiko terakhir berada pada level rendah, termasuk penurunan kepercayaan masyarakat (R05), hilangnya kredibilitas dan transparansi pemerintah (R04), serta tidak adanya kontrak yang jelas dengan pihak ketiga (R08). Penelitian ini memberikan rekomendasi mitigasi yang mencakup penggunaan domain resmi, pengelolaan source code dan database oleh Diskominfo, serta evaluasi berkala terhadap aplikasi yang digunakan. Implementasi rekomendasi ini diharapkan dapat mengurangi risiko dan meningkatkan efektivitas pengelolaan aplikasi di lingkungan pemerintah Kabupaten Sidoarjo.

Kata kunci : *Manajemen Risiko, ISO 31000, Aplikasi, OPD, Diskominfo.*

1. PENDAHULUAN

Pada era digital yang semakin berkembang pesat, pengelolaan teknologi informasi memiliki peran yang sangat krusial dalam menunjang efektivitas operasional dan optimalisasi layanan publik. Pemerintah diharapkan mampu mengadopsi sistem teknologi yang terintegrasi untuk meningkatkan kinerja dan efisiensi dalam berbagai aspek administrasi dan pelayanan kepada masyarakat[1].

Selain itu, penerapan teknologi informasi yang tepat juga berperan penting dalam menjaga keamanan data serta mendorong keterbukaan informasi, sehingga transparansi kinerja pemerintah dapat lebih mudah diakses oleh masyarakat [2].

Melalui pengelolaan teknologi yang baik, pemerintah dapat membangun kepercayaan publik sekaligus mendorong partisipasi aktif dalam program-program pemerintah yang dijalankan.

Sebagai instansi yang bertanggung jawab atas pengelolaan teknologi informasi dan komunikasi di Kabupaten Sidoarjo, Dinas Komunikasi dan Informatika (Diskominfo) memiliki peran strategis dalam memastikan seluruh aplikasi yang digunakan kecamatan oleh dan Organisasi Perangkat Daerah (OPD) telah dikelola dengan baik dan sesuai dengan standar keamanan yang ditetapkan [3].

Tugas ini mencakup pengelolaan aplikasi, sistem keamanan data, dan infrastruktur server yang mendukung keberlangsungan layanan publik secara digital. Untuk itu, Diskominfo Kabupaten Sidoarjo melakukan monitoring dan evaluasi (MONEV) terhadap semua aplikasi yang digunakan oleh kecamatan dan OPD [4].

Berdasarkan data hasil MONEV Aplikasi Diskominfo Kabupaten Sidoarjo pada bulan Januari hingga Maret 2024, teridentifikasi beberapa permasalahan terkait pengelolaan 199 aplikasi di lingkungan Kecamatan dan OPD di Kabupaten Sidoarjo. Pertama, aplikasi masih terdapat aplikasi yang dikelola oleh server Diskominfo namun tidak lagi digunakan oleh Kecamatan dan OPD. Hal ini dapat membebani server Diskominfo dan perlu dilakukan penghapusan aplikasi yang tidak aktif [5]. Kedua, banyak Kecamatan dan OPD yang mengembangkan aplikasi dengan memanfaatkan server dan URL dari pihak ketiga, seperti .com,. Hal ini tidak diperkenankan karena seluruh aplikasi seharusnya dikelola oleh Diskominfo dengan menggunakan server dan URL "sidoarjokab.go.id" agar lebih terjaga keamanannya dan sesuai dengan identitas sebagai aplikasi resmi Pemerintah [6].

Melihat permasalahan yang ada pada pengelolaan aplikasi tersebut, maka Penelitian ini Penelitian ini mengkaji berbagai risiko yang muncul dalam pengelolaan aplikasi di Kecamatan dan OPD. fokus pada perspektif pengguna utama, yaitu administrator atau pegawai yang bertanggung jawab atas operasional website [7].

Analisis ini mencakup identifikasi potensi masalah teknis, keamanan, serta efisiensi operasional yang mungkin dihadapi dalam pengelolaan aplikasi.

Penelitian ini akan menggunakan framework ISO 31000:2018 sebagai landasan untuk manajemen risiko dalam pengelolaan aplikasi di Kecamatan dan OPD Kabupaten Sidoarjo. Dengan menerapkan framework ini, diharapkan penelitian ini dapat memberikan

rekomendasi yang komprehensif dan tepat kepada Diskominfo Kabupaten Sidoarjo dalam upaya mengurangi atau meminimalkan potensi risiko yang mungkin terjadi dalam pengelolaan aplikasi di lingkungan pemerintahan.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian serupa pernah dilakukan oleh Pangestu dan rekan mengenai manajemen risiko aplikasi Sistem Penelusuran Perkara (SIIPP). Dalam analisis risiko yang mengikuti standar ISO 31000 mengidentifikasi 14 risiko, dengan 5 dikategorikan sebagai risiko sedang, 9 risiko lainnya dianggap sebagai risiko rendah [8].

Penelitian selanjutnya dilakukan oleh Moleong dan Tanaamah dalam menganalisis risiko pada aplikasi Integrated Library System (INSLITE) di dinas kearsipan dan perpustakaan provinsi Nusa Tenggara Timur menggunakan framework ISO 31000 : 2018. Penelitian tersebut berhasil mengidentifikasi 19 risiko, dengan rincian 1 risiko pada level tertinggi, 16 risiko pada level sedang dan 2 risiko pada level rendah [9].

2.2. Manajemen Risiko

Manajemen Risiko merupakan proses identifikasi, pengelolaan, dan pengembangan strategi yang tepat dalam mengelola sumber daya organisasi atau perusahaan. Beberapa Strategi dalam manajemen risiko pertama yaitu mentransfer risiko kepada pihak lain, Kedua ialah menghindari risiko, dan yang terakhir mengurangi dampak buruk yang disebabkan dari risiko [10].

Berbagai pendekatan dapat diambil dalam manajemen risiko, termasuk penyaluran risiko kepada pihak ketiga, penghindaran terhadap potensi risiko, pengurangan dampak yang tidak diinginkan, serta penerimaan sebagian atau seluruh konsekuensi dari risiko yang ada [11].

Oleh karena itu, organisasi perlu mengembangkan kerangka kerja manajemen risiko yang lebih holistik, dengan melibatkan pemangku kepentingan dari berbagai fungsi, serta memanfaatkan teknologi analitik untuk mengidentifikasi, mengukur, dan memitigasi risiko.

2.3. ISO 31000 : 2018

ISO 31000:2018 merupakan panduan internasional yang menyediakan prinsip-prinsip dan kerangka kerja untuk mengelola risiko secara efektif di dalam suatu organisasi. Salah satu kelebihan utama dari ISO 31000:2018 adalah sifatnya yang komprehensif dan fleksibel, sehingga dapat diterapkan pada berbagai jenis organisasi, ukuran, dan kompleksitas [12].

Proses manajemen risiko menggunakan kerangka kerja ISO 31000 : 2018 mencakup penerapan sistematis dari kebijakan, prosedur, dan berbagai pendekatan untuk menjelaskan komunikasi dan konsultasi, membangun konteks, serta menilai risiko. Proses menilai risiko juga termasuk pemberian perlakuan terhadap risiko, pemantauan, peninjauan ulang, pencatatan, dan pelaporan kepada pihak yang berkepentingan. Dalam proses menilai risiko terdapat beberapa kriteria tertentu yaitu, kriteria kemungkinan risiko, kriteria dampak, dan kriteria level risiko. berikut ini adalah kriteria kriteria yang diterapkan pada penelitian ini.

2.4. Kriteria Level Risiko

Kriteria level risiko dalam penelitian ini ditentukan berdasarkan analisis probabilitas dan dampak dari setiap risiko yang mungkin terjadi. Setiap level risiko didefinisikan untuk memberikan gambaran yang jelas mengenai frekuensi dan besarnya potensi kerugian yang dapat timbul akibat suatu peristiwa risiko. Berikut adalah penjelasan mengenai kriteria level risiko yang digunakan.

Tabel 1. Kriteria Level Risiko

Level Kemungkinan	Kriteria
1 (Hampir Tidak Terjadi)	1.Kemungkinan terjadinya sangat jarang (kurang dari 2 kali dalam 5 tahun) 2.Persentase Kemungkinan terjadinya kurang dari 5% dari volume transaksi dalam 1 periode
2 (Jarang Terjadi)	1.Kemungkinan terjadinya jarang (2 kali s.d 10 kali dalam 5 tahun) 2.Persentase kemungkinan terjadinya 5% s.d 10% dari volume transaksi dalam 1 periode
3 (Kadang Kadang Terjadi)	1.Kemungkinan terjadinya cukup sering (di atas 10 kali s.d 18 kali dalam 5 tahun) 2.Persentase kemungkinan terjadinya di atas 10% s.d 20% dari volume transaksi dalam 1 periode
4 (Sering Terjadi)	1.Kemungkinan terjadinya sering (di atas 18 kali s.d 26 kali dalam 5 tahun) 2.Persentase kemungkinan terjadinya di atas 20% s.d 50% dari volume transaksi dalam 1 periode
5 (Hampir Selalu Terjadi)	1.Kemungkinan terjadinya sangat sering (di atas 26 kali dalam 5 tahun) 2.Persentase kemungkinan terjadinya lebih dari 50% dari volume transaksi dalam 1 periode

Sumber : Sitanggang & Sitanggang, 2022.

Tabel ini menjelaskan lima tingkat probabilitas risiko yang dinilai berdasarkan frekuensi kejadian atau kemungkinan terjadinya dalam periode waktu tertentu.

2.5. Kriteria Dampak Risiko

Dampak dinilai berdasarkan besarnya kerugian atau gangguan yang dapat ditimbulkan oleh suatu risiko. Berikut adalah penjelasan mengenai kategori dampak risiko yang diterapkan dalam penelitian ini.

Tabel 2 kriteria Dampak Risiko.

Dampak	Tingkat	Deskripsi
Sangat Kecil	1	Dampak yang sangat kecil atau tidak penting atau sangat sedikit perlu perhatian atau bahkan tidak butuh perhatian.
Kecil	2	Tidak terlalu penting atau bernilai, tidak terlalu serius, tidak menyebabkan banyak masalah atau kerusakan.
Sedang	3	Cukup besar atau punya pengaruh untuk mendapat perhatian.
Besar	4	Sangat buruk, serius, atau kerusakan yang tidak dikehendaki.
Sangat Besar	5	Dampak yang menggagalkan pencapaian sasaran.

Sumber: Taufik dkk, 2022.

Tabel ini menguraikan lima tingkat dampak risiko, yang diukur berdasarkan seberapa besar pengaruh atau kerugian yang mungkin ditimbulkan oleh suatu risiko terhadap tujuan, aset, atau operasional organisasi.

2.6. Matrix Level Risiko

Kriteria level risiko menggabungkan dua aspek utama, yaitu kemungkinan terjadinya risiko dan besarnya dampak yang ditimbulkan. Kombinasi dari kedua faktor ini menghasilkan tingkat risiko yang bervariasi, mulai dari sangat rendah hingga sangat tinggi. Penilaian level risiko ini bertujuan untuk memprioritaskan tindakan mitigasi berdasarkan urgensi dan besarnya potensi ancaman. Berikut adalah penjelasan mengenai tingkatan level risiko yang digunakan dalam penelitian ini.

Tabel 3. Matrix Level Risiko

Probabilitas	Hampir pasti terjadi	5	9	15	18	23	25
	Sering terjadi	4	6	12	16	19	24
	Kadang kadang terjadi	3	4	10	14	17	22
	Jarang terjadi	2	2	7	11	13	21
	Hampir tidak terjadi	1	1	3	5	8	20
	Dampak		1	2	3	4	5
			SR	R	S	B	SB

Sumber: Taufik dkk, 2022.

Tabel ini menggambarkan bagaimana risiko dinilai dengan menggabungkan dua elemen utama, yaitu kemungkinan terjadinya risiko (probabilitas) dan tingkat dampak yang ditimbulkan (konsekuensi). Dengan mengalikan kedua elemen ini, didapatkan level risiko yang membantu mengidentifikasi tingkat keparahan risiko secara keseluruhan. Rumus yang digunakan untuk menghitung level risiko adalah:

$$R_{(risiko)} = D_{(dampak)} \times K_{(kejadian)} \quad (1)$$

Rumus ini menunjukkan bahwa tingkat risiko dihitung dengan mengalikan tingkat dampak (D) dari suatu risiko dengan kemungkinan terjadinya (K). Dampak mengukur seberapa besar kerugian atau gangguan yang diakibatkan oleh risiko, sedangkan kemungkinan mengukur seberapa sering risiko tersebut diperkirakan terjadi.Hasil perhitungan dari rumus tersebut akan dikelompokkan ke dalam beberapa level risiko, yang digambarkan dalam tabel berikut:

Tabel 4. Tingkat Prioritas Penanganan risiko

Level Risiko	Level Risiko	Besaran Risiko
Merah	5 (Sangat Tinggi)	20-25
Jingga	4 (Tinggi)	16-15
Kuning	3 (Sedang)	12-15
Hijau	2 (Rendah)	6-11
Biru	1 (Sangat Rendah)	1-5

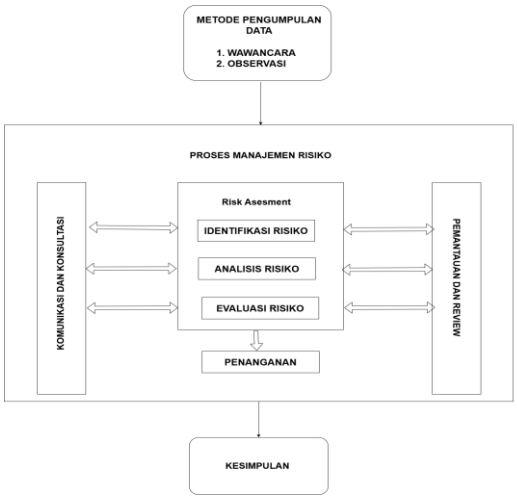
Tabel ini menjelaskan bagaimana hasil perhitungan risiko dapat diklasifikasikan ke dalam kategori yang berbeda, mulai dari sangat rendah hingga sangat tinggi. Kategori ini membantu menentukan prioritas dalam penanganan risiko, di mana risiko dengan level tinggi atau sangat tinggi memerlukan perhatian dan tindakan mitigasi segera.

3. METODE PENELITIAN

3.1. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dalam menganalisis risiko. Pendekatan ini dianggap efisien dan relatif sederhana untuk mengidentifikasi serta menilai dampak dan kemungkinan terjadinya risiko[8].

Penelitian ini juga menerapkan kerangka kerja ISO 31000, yang merupakan standar dalam manajemen risiko. Proses manajemen risiko meliputi identifikasi, analisis, dan evaluasi risiko untuk memberikan rekomendasi terkait pengelolaannya[9]. Gambar berikut menggambarkan konsep yang digunakan dalam penelitian ini.



Gambar 1. Konsep Penelitian
Sumber : Lole & Maria, 2022.

3.2. Metode Pengumpulan data

Penelitian ini menggunakan beberapa metode pengumpulan data, yaitu studi pustaka, wawancara, dan observasi. Studi pustaka dilakukan dengan mengakses berbagai literatur tentang manajemen risiko yang menggunakan standar ISO 31000:2018. Wawancara dilakukan dengan pegawai yang bertanggung jawab di Kecamatan dan OPD, sementara observasi dilakukan dengan mengamati langsung proses pengelolaan aplikasi dan interaksi yang terjadi.

4. HASIL DAN PEMBAHASAN

4.1. Identifikasi Risiko

Untuk mengidentifikasi risiko dalam pengelolaan aplikasi di Kecamatan dan OPD Kabupaten Sidoarjo, peneliti bersama tim MONEV Diskominfo melakukan observasi langsung serta wawancara dengan pranata komputer atau pihak yang bertanggung jawab di setiap Kecamatan dan OPD. Tujuan dari kegiatan ini adalah untuk mendapatkan gambaran menyeluruh mengenai potensi risiko dalam pengelolaan aplikasi di pemerintah daerah Kabupaten Sidoarjo.

4.2. Identifikasi Aset

Langkah pertama dalam mengidentifikasi risiko pada pengelolaan aplikasi di Kabupaten Sidoarjo adalah dengan mendata seluruh aset terkait pengelolaan aplikasi. Hasil monitoring Diskominfo Kabupaten sidoarjo menunjukkan bahwa aset-aset tersebut dapat dikelompokkan menjadi tiga kategori, yaitu : aset *software*, aset sumber daya IT, dan aset data.

Tabel 4. Identifikasi Aset

Komponen SI/TI	Aset
Software	Seluruh aplikasi yang ada pada Kecamatan dan OPD
Sumber Daya	Server
	Jaringan
	Database
Data	Data kependudukan
	Data kesehatan
	Data kepegawaian
	Data keuangan

Sumber : data diolah, 2024.

Tabel identifikasi aset dalam pengelolaan aplikasi di Kecamatan dan OPD Kabupaten Sidoarjo mendata tiga kategori aset utama, yaitu software (seluruh aplikasi yang digunakan), sumber daya IT (server, jaringan, dan database), serta data (kependudukan, kesehatan, kepegawaian, dan keuangan), untuk mempermudah manajemen risiko sesuai kerangka ISO 31000:2018.

4.3. Identifikasi Kemungkinan Risiko

Setelah mengidentifikasi terkait aset pengelolaan aplikasi, Tahapan berikutnya adalah mengenali potensi risiko, yang kemudian akan dikelompokkan sesuai dengan faktor yang mempengaruhinya[10].

Seperti keamanan, yang melibatkan ancaman terhadap kerahasiaan, integritas, dan ketersediaan data; reputasi, terkait dampak negatif pada citra pemerintah jika layanan terganggu. Keuangan, yang mencakup risiko pembengkakan anggaran dan biaya tambahan akibat perbaikan sistem. Integrasi data, yang menyangkut keselarasan antar sistem yang dapat memicu ketidaksesuaian data. serta kontrak, yang melibatkan potensi masalah dalam perjanjian dengan penyedia layanan atau pihak ketiga.

Tabel 5. Identifikasi Kemungkinan Risiko

Faktor	ID	Risiko
Keamanan	R01	Serangan siber/hacking
Operasional	R02	Gangguan layanan/downtime
	R03	Tidak adanya kontrol penuh terhadap aplikasi dan database
Risiko Reputasi	R04	Hilangnya kredibilitas dan transparansi pemerintah
Penurunan kepercayaan masyarakat	R05	Penurunan kepercayaan masyarakat
Keuangan /Biaya	R06	Pembengkakan Biaya pengadaan,pengembangan,dan pemeliharaan aplikasi
Data	R07	Kegagalan sinkronisasi data antara aplikasi pihak ketiga dan sistem utama
Risiko Kontrak	R08	Tidak adanya kontrak yang jelas dan mengikat dengan pihak ketiga
	R09	Perubahan atau pemutusan kontrak

Tabel Identifikasi Kemungkinan Risiko memetakan berbagai risiko dalam pengelolaan aplikasi di Kecamatan dan OPD Kabupaten Sidoarjo, termasuk risiko serangan siber, gangguan operasional, hilangnya reputasi, pembengkakan biaya, kegagalan sinkronisasi data, serta masalah kontrak dengan pihak ketiga, untuk menentukan prioritas mitigasi berdasarkan potensi dampaknya.

4.4. Identifikasi Dampak Risiko

Setelah mengidentifikasi potensi risiko dari berbagai aspek seperti keamanan, reputasi, keuangan, integrasi data, dan kontrak. Berikutnya adalah mengidentifikasi dampak akibat dari risiko yang berpotensi mengganggu kinerja aplikasi di seluruh Kecamatan dan OPD dan. Setiap risiko diberi label dengan ID tertentu dan memiliki dampak yang relevan.

Tabel 6. Identifikasi Dampak Risiko

Risiko	ID	Dampak
Serangan siber/hacking	**R01**	Aplikasi yang tidak berada dalam domain resmi pemerintah mengakibatkan terganggunya ketersediaan sistem, serta potensi manipulasi atau pencurian data
Gangguan layanan/downtime	**R02**	Tertundanya pelayanan publik dan terhambatnya aktivitas organisasi.
Tidak adanya kontrol penuh terhadap aplikasi dan database	**R03**	Kesulitan melakukan pemantauan, perbaikan, dan pengembangan sistem sesuai kebutuhan.
Hilangnya kredibilitas dan transparansi pemerintah	**R04**	Menurunnya citra dan reputasi pemerintah daerah.
Penurunan kepercayaan masyarakat	**R05**	Partisipasi masyarakat dalam kegiatan dan program pemerintah dapat menurun
Pembengkakan biaya pengadaan, pengembangan, dan pemeliharaan aplikasi	**R06**	Pemborosan anggaran daerah.
Kegagalan sinkronisasi data antara aplikasi pihak ketiga dan sistem utama	**R07**	Inkonsistensi informasi
Tidak adanya kontrak yang jelas dan mengikat dengan pihak ketiga	**R08**	Permasalahan terkait hukum dan operasional.
Perubahan atau pemutusan kontrak	**R09**	Pengelolaan Sistem Informasi Pemerintahan Daerah dapat mengganggu keberlangsungan layanan publik.

Tabel Identifikasi Dampak Risiko menjelaskan bahwa risiko serangan siber, gangguan layanan, kurangnya kontrol aplikasi, hilangnya kredibilitas pemerintah, penurunan kepercayaan masyarakat, pembengkakan biaya, kegagalan sinkronisasi data, serta masalah kontrak dengan pihak ketiga dapat mengganggu layanan publik, memicu inkonsistensi data, dan membebani anggaran

4.5. Evaluasi Risiko

Dalam konteks pengelolaan aplikasi di Kecamatan dan OPD Kabupaten Sidoarjo digunakan untuk mengukur tingkat risiko berdasarkan kombinasi antara dampak dan kemungkinan terjadinya setiap risiko yang telah diidentifikasi.

Tabel 7. Marix Risiko Berdasarkan Probabilitas dan dampak

Probabilitas	**Hampir pasti terjadi**	5	9	15 R03 R06	18	23	25
	Sering terjadi	4	6	12 R02 R09	16	19	24
	Kadang kadang terjadi	3	4 R04	10	14	17	22
	Jarang terjadi	2	2	7	11	13	21
	Hampir tidak terjadi	1	1	3 R05 R08	5	8 R07	20 R01
	Dampak		1	2	3	4	5
			SR	R	S	B	SB

Tabel evaluasi risiko mengelompokan dalam pengelolaan aplikasi di Kecamatan dan OPD Kabupaten Sidoarjo. Risiko-risiko ini kemudian akan dikelompokkan berdasarkan rasionya. Setelah itu, risiko-risiko tersebut akan dikelompokkan sesuai dengan tingkatan risiko yang tinggi, sedang, dan rendah.

Tabel 9. Pengelompokan Level Risiko

ID	Kemungkinan Risiko	Level Risiko
R01	Serangan siber/hacking	**SANGAT TINGGI**
R03	Tidak adanya kontrol penuh terhadap aplikasi dan database	SEDANG
R06	Pembengkakan biaya pengadaan, pengembangan, dan pemeliharaan aplikasi	SEDANG
R09	Perubahan atau pemutusan kontrak	SEDANG
R02	Gangguan Layanan / Down Time	SEDANG
R07	Kegagalan sinkronisasi data antara aplikasi pihak ketiga dan sistem utama	SEDANG
R08	Tidak adanya kontrak yang jelas dan mengikat dengan pihak ketiga	SANGAT RENDAH
R05	Penurunan kepercayaan masyarakat	SANGAT RENDAH
R04	Hilangnya kredibilitas dan transparansi pemerintah	SANGAT RENDAH

Dari tabel ini dapat disimpulkan bahwa dari 9 risiko yang telah teridentifikasi, terdapat 2 risiko yang tinggi) yakni ; R 01. lalu terdapat juga risiko dengan tingkat sedang sebanyak 3 risiko yaitu; R09, R02, R03. Sisanya risiko yang dengan level sangat rendah sebanyak 3 yaitu; R06, R05. dan R04.

4.6. Perlakuan Risiko

Langkah selanjutnya adalah mitigasi risiko. Pada tahap ini, dilakukan penentuan rekomendasi tindakan untuk menangani risiko-risiko yang telah diidentifikasi dan dikelompokkan berdasarkan tingkat risikonya sesuai dengan tabel evaluasi risiko sebelumnya [15].

Tabel 10. Rekomendasi Perlakuan Risiko

ID	Risiko	Level	Mitigasi
R01	Serangan Ciber/ Hacking	**SANGAT TINGGI**	1. URL wajib Sidoarjo.kab karena stabil dan terjamin 2. Source Code dan database wajib dititipkan kominfo Sidoarjo
R03	Tidak adanya kontrol penuh terhadap aplikasi dan database	**SEDANG**	1. Siapkan rencana pemeliharaan, backup, dan pemulihan 2. source code dan database wajib dititipkan kominfo Sidoarjo 3. Siapkan rencana kontingensi untuk migrasi aplikasi
R06	Pembengkakan biaya pengadaan, pengembangan, dan pemeliharaan aplikasi	**SEDANG**	1. Perencanaan matang sebelum pengadaan aplikasi 2. Evaluasi dan penghentian penggunaan aplikasi
R09	Perubahan atau pemutusan kontrak	**SEDANG**	1. Siapkan rencana kontingensi untuk migrasi
R02	Gangguan Layanan / Down Time	**SEDANG**	1. Pertimbangkan untuk menggunakan domain resmi Sidoarjo.kab 2. Memastikan bahwa tim IT Anda memiliki kapabilitas yang memadai untuk mengelola aplikasi-aplikasi tersebut. 3. Pantau kinerja pihak ketiga secara berkala dan pastikan ada
R07	Kegagalan sinkronisasi data antara aplikasi pihak ketiga dan sistem utama	**SEDANG**	1. Memastikan ada perjanjian yang jelas terkait sinkronisasi data. 2. Source Code dan database wajib dititipkan kominfo Sidoarjo guna memastikan ada backup dan keamanan yang memadai.
R08	Tidak adanya kontrak yang jelas dan mengikat dengan pihak ketiga	**SANGAT RENDAH**	1. Membuat kontrak yang jelas dan mengikat 2. Memastikan hak kepemilikan dan penggunaan
R05	Penurunan kepercayaan masyarakat	**SANGAT RENDAH**	1. Branding dan identitas aplikasi 2. Evaluasi dan perbaikan berkelanjutan dengan Pertimbangkan untuk menggunakan domain resmi Sidoarjo
R04	Hilangnya kredibilitas dan transparansi pemerintah	**SANGAT RENDAH**	1. Komunikasi dan transparansi kepada masyarakat 2. Koordinasi dan penghapusan aplikasi tidak aktif

Tabel 10 memberikan rekomendasi mitigasi untuk risiko-risiko yang dihadapi dalam pengelolaan aplikasi di OPD dan kecamatan Kabupaten Sidoarjo. Untuk risiko sangat tinggi seperti serangan siber (R01), disarankan menggunakan URL resmi sidoarjokab.go.id dan menyerahkan pengelolaan source code serta database ke Diskominfo untuk memastikan kontrol dan keamanan. Risiko sedang, seperti kurangnya kontrol aplikasi (R03) dan pembengkakan biaya (R06), membutuhkan rencana pemeliharaan, backup, serta evaluasi berkala, sementara untuk gangguan layanan (R02), penting memastikan kompetensi tim IT dan memantau kinerja pihak ketiga. Masalah sinkronisasi data (R07) dan pemutusan kontrak (R09) memerlukan rencana kontingensi serta perjanjian yang jelas. Untuk risiko sangat rendah seperti penurunan kepercayaan masyarakat (R05) dan hilangnya kredibilitas pemerintah (R04), disarankan memperkuat branding, komunikasi, dan menghapus aplikasi yang tidak aktif.

5. KESIMPULAN

Terdapat 9 risiko yang teridentifikasi pada Penelitian ini mengidentifikasi sembilan risiko utama dalam pengelolaan aplikasi di OPD dan Kecamatan Kabupaten Sidoarjo menggunakan ISO 31000:2018, dengan satu risiko sangat tinggi, yaitu serangan siber/hacking, yang membutuhkan pengelolaan source code dan database oleh Diskominfo untuk meningkatkan keamanan. Empat risiko sedang, seperti gangguan layanan, kurangnya kontrol aplikasi, pembengkakan biaya, dan pemutusan kontrak, dapat diatasi melalui perencanaan matang, evaluasi berkala, dan sinkronisasi data. Risiko sangat rendah seperti penurunan kepercayaan masyarakat ,e,erlukan peningkatan branding, komunikasi, serta kontrak yang jelas. Penelitian ini menyarankan pemerintah Kabupaten Sidoarjo untuk segera mengimplementasikan mitigasi yang telah direkomendasikan, khususnya dengan cara memprioritaskan penggunaan URL resmi dan

pengelolaan aplikasi yang lebih baik aman serta efisien dengan tetap mempertahankan kepercayaan masyarakat terhadap pelayanan pemerintah.

DAFTAR PUSTAKA

[1] Wuryan Andayani, Dahlia, Eka Putrianti, Oktavima Wisdaningrum, Panji Putranto, and Yesika Yanuarisa, "Penguatan Good Governance: Pengalaman Penerapan Electronic Government Pemerintah Daerah Di Indonesia," *J. Akt. Ris. Akunt. Dan Keuang.*, vol. 6, no. 2, pp. 116–131, Jul. 2024, doi: 10.52005/aktiva.v6i2.240.

[2] B. A. Iswandari, "Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance," *J. Huk. Ius Quia Iustum*, vol. 28, no. 1, Jan. 2021, doi: 10.20885/iustum.vol28.iss1.art6.

[3] D. Prayogi and A. Prawijaya, "Strategi Media Relations Dinas Komunikasi dan Informatika Kabupaten Luwu Timur dalam Peningkatan Sarana Informasi Publik," *J. Terap. Pemerintah. MINANGKABAU*, vol. 2, no. 2, pp. 115–131, Dec. 2022, doi: 10.33701/jtpm.v2i2.2824.

[4] R. Hardiansyah and Y. T. Mursityo, "Evaluasi Proses Tata kelola Keamanan Informasi Menggunakan COBIT 5 Dengan Proses APO13, DSS04 dan DSS05 (Studi Pada DISKOMINFO Kabupaten Sidoarjo)".

[5] M. Reza Maulana, E. Budi Susanto, and S. Sattriedi, "ANALISIS KINERJA WEBSITE PEMERINTAH KOTA PEKALONGAN," *J. LITBANG KOTA PEKALONGAN*, vol. 20, Jun. 2021, doi: 10.54911/litbang.v20i.144.

[6] R. Achmad, "Kualitas Pelaksanaan Online Public Relation Pemerintah Provinsi Bangka Belitung melalui babelprov.go.id ditinjau dari Penerapan Prinsip The 7C's Framework," 2022.

[7] K. Y. Indira, "PENERAPAN IEC/ISO 31010:2018 DALAM MANAJEMEN RISIKO APLIKASI SMARD DISDUKCAPIL KABUPATEN SEMARANG," vol. 27, no. 2, 2023.

[8] R. H. Pangestu, A. D. Cahyono, and P. F. Tanaem, "Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Mengunakan ISO 31000," *J. Comput. Inf. Syst. Ampera*, vol. 2, no. 1, pp. 43–57, Jan. 2021, doi: 10.51519/journalcisa.v2i1.59.

[9] G. Moleong and A. R. Tanaamah, "ANALISIS RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 PADA APLIKASI INLISLITE DI DINAS KEARSIPAN DAN PERPUSTAKAAN PROVINSI NUSA TENGGARA TIMUR," *JATI J. Mhs. Tek. Inform.*, vol. 6, no. 2, pp. 501–506, Aug. 2022, doi: 10.36040/jati.v6i2.4840.

[10] Hastin Nuraini, "Manajemen Risiko Untuk Meminimalisir Masalah Perusahaan," *Optim. J. Ekon. Dan Manaj.*, vol. 2, no. 3, pp. 339–350, Sep. 2022, doi: 10.55606/optimal.v2i3.1366.

[11] E. Evinia and M. N. N. Sitokdana, "Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama)," *J. Inf. Syst. Inform.*, vol. 5, no. 1, pp. 380–390, Mar. 2023, doi: 10.51519/journalisi.v5i1.420.

[12] N. L. Putri and A. F. Wijaya, *"Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework," J. Inf. Syst. Inform.*, vol. 5, no. 2, pp. 630–649, May 2023, doi: 10.51519/journalisi.v5i2.468.