Perancangan Pengelolaan Risiko Keamanan Informasi di Dinas Komunikasi dan Informatika Kabupaten Bogor Menggunakan ISO 27005:2022

Zhillan Andru Atharsad
Department of Information System
Telkom University
Bandung, Indonesia
zhillanathar@student.telkomuniversity.ac.id

Ryan Adhitya Nugraha
Department of Information System
Telkom University
Bandung, Indonesia
ranugraha@telkomuniversity.ac.id

Widyatasya Agustika Nurtrisha
Department of Information System
Telkom University
Bandung, Indonesia
nurtrisha@telkomuniversity.ac.id

Keamanan informasi merupakan aspek krusial dalam era digital, terutama bagi instansi pemerintah seperti Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Bogor. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), serangan siber di Indonesia meningkat signifikan, dengan sektor pemerintahan sebagai salah satu target utama. Penelitian ini bertujuan untuk merancang pengelolaan risiko keamanan informasi di Diskominfo Kabupaten Bogor menggunakan standar ISO/IEC 27005:2022. Penelitian ini menggunakan metode kualitatif dengan pendekatan Design Science Research (DSR). Data dikumpulkan melalui wawancara, analisis dokumen, dan studi literatur. Proses manajemen risiko mengikuti kerangka kerja ISO/IEC 27005:2022, meliputi context establishment, risk assessment, dan risk treatment. Hasil penelitian menunjukkan terdapat 119 risiko, terdiri dari 3 risiko sangat tinggi, 2 risiko tinggi, 18 risiko sedang, 16 risiko rendah, dan 80 risiko sangat rendah. Risiko dengan tingkat sangat tinggi hingga sedang yaitu sebanyak 23 risiko kemudian diberi rekomendasi kontrol sesuai ISO/IEC 27001:2022.

Kata kunci— manajemen risiko, keamanan informasi, SNI ISO/IEC 27005:2022

I. PENDAHULUAN

Keamanan informasi merupakan aspek yang sangat penting pada era digitalisasi saat ini, terutama terhadap instansi atau organisasi yang menggunakan teknologi informasi [1]. Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Bogor merupakan sebuah instansi pemerintah yang berperan penting dalam pemanfaatan teknologi informasi dan komunikasi (TIK) [2]. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber di Indonesia pada tahun 2022 meningkat sebesar 22% dibandingkan tahun sebelumnya. Untuk menghadapi berbagai ancaman keamanan siber, Diskominfo Kabupaten Bogor menerapkan manajemen risiko keamanan informasi secara sistematis. Namun, efektivitas pengelolaan ini masih memerlukan penguatan, agar keamanan informasi yang ada semakin kuat.

Hingga saat ini, Diskominfo Kabupaten Bogor belum sepenuhnya menerapkan standar yang mengatur Manajemen Risiko Keamanan Informasi seperti ISO 27005:2022. Upaya yang dapat dilakukan oleh Diskominfo Kabupaten Bogor adalah mengimplementasikan standar internasional seperti ISO 27005:2022 menjadi pedoman yang sangat relevan [3]. ISO/IEC 27005:2022 memberikan panduan komprehensif untuk manajemen risiko keamanan informasi. Standar ini mendukung penerapan persyaratan dalam Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan ISO/IEC 27001:2022 dengan menyediakan kerangka kerja untuk mengidentifikasi, menilai, dan mengelola risiko yang berkaitan dengan keamanan informasi [4].

Berdasarkan permasalahan yang dihadapi Diskominfo Kabupaten Bogor, penelitian ini bertujuan untuk mengidentifikasi dan menganalisis risiko keamanan informasi yang ada di instansi terkait. Penelitian ini juga bertujuan untuk memberikan rekomendasi yang berbasis pada kerangka kerja ISO 27005:2022 dalam rangka meningkatkan perlindungan terhadap aset TI dan memitigasi potensi ancaman yang dapat mengganggu operasional maupun kepercayaan publik terhadap layanan Diskominfo.

II. KAJIAN TEORI

Pada bagian ini disajikan konsep-konsep teoretis dan standar yang relevan sebagai landasan penelitian.

A. Sistem Manajemen Keamanan Informasi (SMKI)

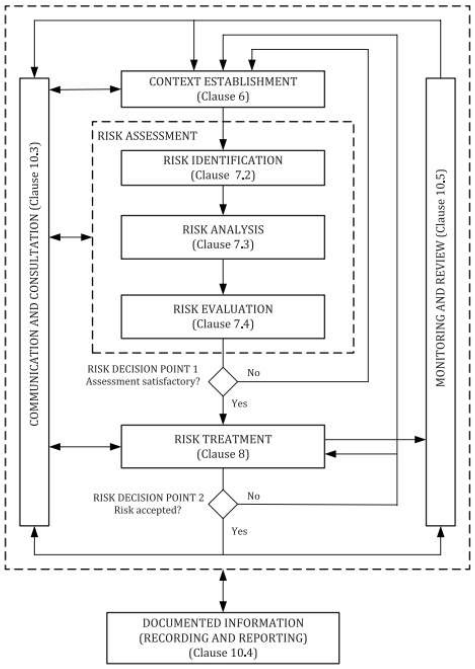
"Sistem Manajemen Keamanan Informasi (SMKI) adalah kerangka proses yang dirancang berdasarkan pendekatan risiko bisnis. SMKI mencakup perencanaan (*Plan*), implementasi dan operasional (*Do*), pemantauan dan peninjauan (*Check*), serta pemeliharaan dan pengembangan (*Act*) untuk melindungi keamanan informasi perusahaan secara menyeluruh" [5]. SMKI meliputi serangkaian kebijakan, prosedur, praktik, serta teknologi yang diterapkan untuk mengelola dan menjaga keamanan informasi dalam suatu organisasi [6].

B. Manajemen Risiko

"Manajemen risiko adalah proses sistematis yang melibatkan identifikasi, pengukuran, analisis, evaluasi, dan pengelolaan risiko yang dapat memengaruhi pencapaian tujuan organisasi" [6]. Proses ini mencakup penyusunan strategi untuk mengelola risiko secara efektif dengan memanfaatkan sumber daya yang tersedia guna meminimalkan dampak negatif dan mendukung keberhasilan organisasi. Manajemen risiko juga menjadi salah satu strategi yang penting untuk mencegah kerugian besar yang dapat mengancam kelangsungan hidup perusahaan. Tujuan utama dari penerapan manajemen risiko adalah untuk memberikan gambaran mengenai potensi peristiwa yang dapat terjadi, sehingga perusahaan dapat merencanakan langkah-langkah pencegahan dan mengevaluasi risiko yang ada [7].

C. ISO/IEC 27005:2022

ISO/IEC 27005 adalah standar internasional yang memberikan panduan untuk manajemen risiko keamanan informasi. ISO 27005:2022 membantu organisasi dalam menerapkan proses manajemen risiko yang disesuaikan dengan kebutuhan spesifik mereka, yang juga mendukung penerapan standar ISO/IEC 27001. Proses manajemen risiko keamanan informasi mencakup beberapa langkah penting, yaitu penetapan konteks (*context establishment*), penilaian risiko (*risk assessment*), penanganan risiko (*risk treatment*), komunikasi (*risk communication*), pemantauan dan peninjauan (*risk monitoring and review*) [8].



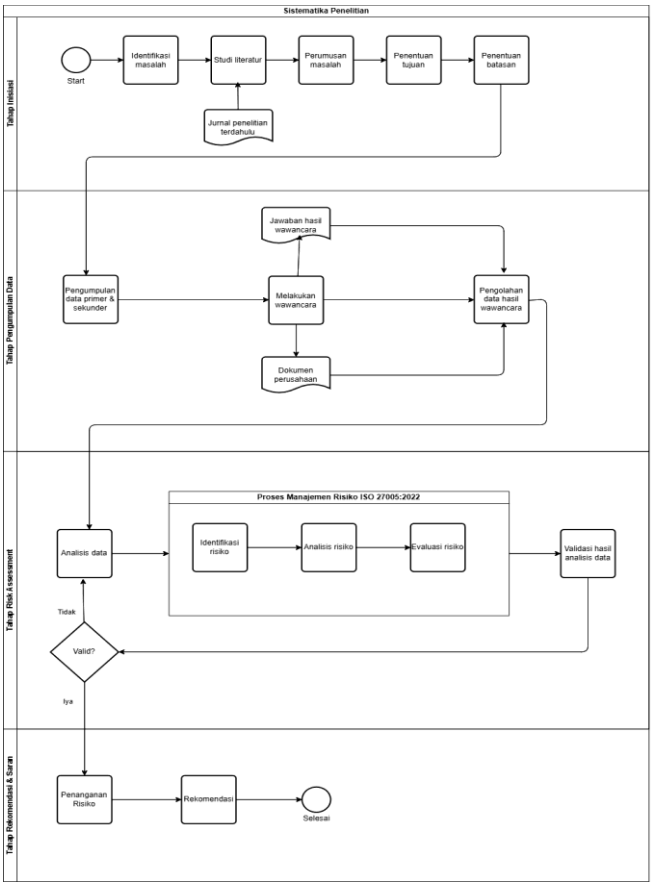
GAMBAR 1
(A)

III. METODE

Penelitian ini menggunakan metode kualitatif dengan pendekatan *Design Science Research* (DSR) untuk menghasilkan artefak berupa rancangan pengelolaan risiko. Tahapan penelitian mengacu pada ISO/IEC 27005:2022: *Context Establishment* (penetapan kriteria risiko), *Risk Assessment* (identifikasi, analisis, evaluasi), serta *Risk Treatment* (penanganan risiko).

A. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah adalah langkah-langkah terstruktur yang digunakan untuk memahami pola pikir dalam setiap tahap penelitian. Proses ini bertujuan untuk mencapai tujuan penelitian dan memberikan rekomendasi terkait pengurangan risiko.



GAMBAR 2
(A)

1. Tahap Inisiasi, tahap ini dimulai dengan mengidentifikasi masalah yang dihadapi oleh organisasi, yang kemudian dianalisis melalui studi literatur menggunakan jurnal penelitian terdahulu. Berdasarkan hasil analisis ini, dilakukan perumusan masalah yang dilanjutkan dengan penentuan tujuan penelitian. Untuk memastikan penelitian memiliki ruang lingkup yang jelas, ditentukan pula batasan penelitian yang akan menjadi acuan pada tahap-tahap selanjutnya.
2. Tahap Pengumpulan Data, pada tahap ini, dilakukan pengumpulan data primer dan sekunder. Data primer diperoleh melalui wawancara dengan pihak terkait, sedangkan data sekunder dikumpulkan dari dokumen perusahaan yang relevan. Jawaban hasil wawancara kemudian diolah menjadi data yang dapat digunakan untuk analisis. Tahap ini bertujuan untuk memastikan bahwa informasi yang dikumpulkan mencakup seluruh aspek yang relevan dengan risiko keamanan informasi yang ada.
3. Tahap *Risk Assessment*, data yang telah dikumpulkan dianalisis menggunakan kerangka kerja ISO/IEC 27005:2022, yang meliputi tiga proses utama:
    a. Identifikasi risiko, dilakukan dengan mengumpulkan aset TI yang penting, mencatat potensi ancaman seperti serangan siber atau kehilangan data, serta menganalisis kerentanan yang ada di dalam sistem. Data dikumpulkan melalui wawancara dengan bidang terkait, observasi langsung terhadap infrastruktur

TI, dan peninjauan insiden keamanan sebelumnya.

b. Analisis risiko, melibatkan penghitungan tingkat risiko dengan menghubungkan kemungkinan terjadinya ancaman dan dampaknya terhadap organisasi. Analisis dilakukan menggunakan pendekatan kualitatif maupun kuantitatif, termasuk membuat matriks risiko.

c. Evaluasi risiko, risiko yang telah dianalisis diprioritaskan berdasarkan tingkatannya, dan dibandingkan dengan kriteria risiko yang ditetapkan oleh Diskominfo. Hasil analisis ini kemudian divalidasi melalui diskusi dengan bagian terkait untuk memastikan keakuratan data, dan jika ditemukan ketidaksesuaian, proses analisis diulang hingga hasilnya sesuai dengan kondisi sebenarnya.

4. Tahap Rekomendasi & Saran, Berdasarkan hasil validasi yang dilakukan pada tahap *Risk Assessment*, disusun rencana penanganan risiko yang spesifik dan sesuai dengan kebutuhan organisasi. Rekomendasi ini dirancang secara komprehensif dengan mempertimbangkan tiga aspek utama, yaitu *people*, *process*, dan *technology*. Aspek *people* mencakup penyusunan dokumen rekomendasi terkait peran, penambahan tanggung jawab, serta pengembangan keterampilan dan kesadaran. Hal ini bertujuan untuk meningkatkan kompetensi individu dalam perusahaan secara efektif. Dari aspek *process*, dirancang kebijakan dan prosedur yang terstandar untuk pengelolaan risiko keamanan informasi, termasuk pengelolaan insiden, mitigasi risiko, serta tindakan preventif. Aspek *technology* mencakup penyusunan dokumen rekomendasi terkait alat *tools* dan fitur teknologi yang dapat diimplementasikan untuk meningkatkan produktivitas dan efisiensi sistem dalam perusahaan.

B. Pengumpulan Data

Penelitian ini bertujuan untuk menganalisis dan mengelola risiko keamanan informasi di Dinas Komunikasi dan Informatika Kabupaten Bogor menggunakan standar ISO 27005:2022. Data yang dikumpulkan terdiri dari data primer dan data sekunder.

1. Data Primer, diperoleh melalui wawancara terstruktur dengan pihak-pihak terkait, seperti Kepala Bidang Persandian dan Statistik, Kasie Persandian, Ketua Tim Infrastuktur Pusat Data untuk memahami kebijakan dan strategi keamanan informasi, Staf Operasional dari bidang-bidang terkait untuk mengidentifikasi ancaman dan kerentanan yang sering dihadapi, serta untuk memperoleh informasi terkait pengelolaan aset TI dan prosedur mitigasi risiko.

2. Data Sekunder, diperoleh dari berbagai sumber, termasuk dokumen internal seperti kebijakan keamanan informasi, laporan insiden keamanan, dan prosedur operasional standar (SOP), serta referensi eksternal berupa jurnal ilmiah dan buku panduan ISO yang relevan. Data ini diperoleh melalui studi dokumen dan studi literatur untuk mendukung analisis yang lebih mendalam.

C. Pengolahan Data

Setelah data dan informasi yang relevan dikumpulkan melalui metode yang telah dijelaskan sebelumnya, langkah berikutnya adalah mengolah data tersebut menjadi sebuah analisis yang komprehensif. Langkah selanjutnya adalah menggunakan matriks risiko untuk menilai dan memetakan tingkat risiko pada setiap aset TI yang telah diidentifikasi. Matriks risiko ini merupakan alat analisis yang menggabungkan dua parameter utama, yaitu kemungkinan terjadinya ancaman (*likelihood*) dan dampak yang ditimbulkan apabila ancaman tersebut terjadi (*consequence*). Berdasarkan hasil kuesioner yang diberikan peneliti, nilai kemungkinan dan dampak diberikan pada setiap potensi ancaman. Skor risiko diperoleh dengan mengalikan nilai kemungkinan dengan dampak risiko, menghasilkan skor risiko [9]. Setelah itu potensi ancaman dapat diklasifikasikan masuk ke dalam kategori mana. Matriks risiko ini dibagi menjadi beberapa kuadran, di mana risiko dengan prioritas tinggi memerlukan tindakan segera dan pengawasan ketat, sedangkan risiko dengan prioritas rendah hanya membutuhkan pemantauan rutin.

Langkah selanjutnya adalah mengevaluasi tingkat risiko yang telah dipetakan untuk menentukan tindakan mitigasi yang paling tepat. Tindakan mitigasi ini melibatkan pengembangan kebijakan dan prosedur yang bertujuan untuk mengurangi dampak atau kemungkinan risiko tersebut. Dengan melalui pendekatan ini, diharapkan Diskominfo Kabupaten Bogor tetap aman dan bisa mempersiapkan risiko yang akan terjadi.

D. Metode Evaluasi

Penelitian ini menggunakan metode evaluasi Uji *Credibility*, Uji *Transferability*, Uji *Dependability*, dan Uji *Confirmability* (Shenton, 2004)[10].

1. Uji *Credibility*, proses evaluasi ini mencakup triangulasi data dari wawancara, dokumen internal Diskominfo, dan literatur terkait ISO/IEC 27005:2022. Kredibilitas data diverifikasi dengan diskusi bersama *stakeholder* terkait.

2. Uji *Transferability*, untuk mengevaluasi transferabilitas, hasil penelitian dibandingkan dengan studi kasus lain di sektor pemerintah atau organisasi yang mengadopsi standar keamanan informasi yang sama.

3. Uji *Dependability*, dokumentasi langkah-langkah penelitian, seperti metode pengumpulan data, analisis risiko, dan pembuatan mitigasi, menjadi acuan untuk memastikan proses penelitian dapat diulang dan menghasilkan hasil yang sama.

4. Uji *Confirmability*, semua data yang digunakan dalam penelitian, termasuk catatan wawancara dan dokumen pendukung, disimpan dalam sistem yang terstruktur untuk memungkinkan *stakeholder* penilai memberikan penilaian.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini diuraikan hasil analisis risiko keamanan informasi di Diskominfo Kabupaten Bogor sesuai tahapan

ISO/IEC 27005:2022. Risiko-risiko diidentifikasi berdasarkan aset, ancaman, dan kerentanan, kemudian dianalisis tingkat risikonya menggunakan nilai *likelihood* dan *consequence* dari data kuesioner. Evaluasi risiko dilakukan untuk memprioritaskan risiko sesuai levelnya, sehingga rekomendasi kontrol yang disusun relevan dan sesuai kebutuhan.

A. Context Establishment

Gambar dinomori

1. Penetapan Kemungkinan Risiko (*Likelihood*)

   Kemungkinan risiko merupakan peluang atau frekuensi suatu ancaman dapat terjadi terhadap suatu aset. Kemungkinan risiko harus dinilai dan diungkapkan dengan menggunakan kriteria kemungkinan yang telah ditetapkan.

Kemungkinan	*Level*	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
Hampir tidak terjadi	1	X < 2 kali
Jarang terjadi	2	2 ≤ X ≤ 5 kali
Kadang-kadang terjadi	3	6 ≤ X ≤ 9 kali
Sering terjadi	4	10 ≤ X ≤ 12 kali
Hampir pasti terjadi	5	> 12 kali

GAMBAR 3

(A)

2. Penetapan Konsekuensi Risiko (*Consequence*)
   Konsekuensi risiko merupakan tingkat dampak apabila risiko tersebut benar-benar terjadi terhadap aset informasi. Konsekuensi risiko yang timbul akibat kegagalan dalam menjaga kerahasiaan, integritas, atau ketersediaan informasi dengan baik harus diidentifikasi dan dievaluasi.

Area Konsekuensi	Level Konsekuensi				
	1	2	3	4	5
	Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Reputasi	Keluhan Stakeholder secara langsung lisan/tertulis ke organisasi jumlahnya ≤ 3 dalam satu periode	Keluhan Stakeholder secara langsung lisan/tertulis ke organisasi jumlahnya ≥ 3 dalam satu periode	Pemberitaan negatif di media massa lokal	Pemberitaan negatif di media massa nasional	Pemberitaan negatif di media massa internasional
Kinerja	Penurunan Kinerja < 20%	Penurunan Kinerja 20% s.d < 40%	Penurunan Kinerja 40% s.d < 60%	Penurunan Kinerja 60% s.d < 80%	Penurunan Kinerja ≥ 80%
Layanan Organisasi	Pelayanan tertunda ≤ 1 hari	Pelayanan tertunda diatas 1 hari s.d 5 hari	Pelayanan tertunda diatas 5 hari s.d 15 hari	Pelayanan tertunda diatas 15 hari s.d 30 hari	Pelayanan tertunda lebih dari 30 hari
Operasional dan Aset TIK	Terganggunya operasional dan penurunan kinerja aset TIK <20%	Terganggunya operasional dan penurunan kinerja aset TIK <20% s.d <40%	Terganggunya operasional dan penurunan kinerja aset TIK <40% s.d <60%	Terganggunya operasional dan penurunan kinerja aset TIK <60% s.d <80%	Terganggunya operasional dan penurunan kinerja aset TIK ≥80%

GAMBAR 4

(A)

3. Matriks risiko merupakan kombinasi dari skor kemungkinan dan dampak, yang digunakan untuk menentukan tingkat risiko secara kuantitatif dan kualitatif. Matriks risiko berfungsi sebagai alat bantu untuk memprioritaskan penanganan dan strategi mitigasi risiko dengan mengelompokkan risiko berdasarkan tingkat kemungkinan dan dampaknya.

Level Kemungkinan	Level Konsekuensi				
	Tidak Signifikan (1)	Kurang Signifikan (2)	Cukup Signifikan (3)	Signifikan (4)	Sangat Signifikan (5)
Hampir Pasti Terjadi (5)	Rendah (9)	Sedang (15)	Tinggi (18)	Sangat Rendah (23)	Sangat Tinggi (25)
Sering Terjadi (4)	Rendah (6)	Sedang (12)	Tinggi (16)	Tinggi (19)	Sangat Tinggi (24)
Kadang-Kadang Terjadi (3)	Sangat Rendah (4)	Rendah (10)	Sedang (14)	Tinggi (17)	Sangat Tinggi (22)
Jarang Terjadi (2)	Sangat Rendah (2)	Rendah (7)	Sedang (11)	Sedang (13)	Sangat tinggi (21)
Hampir Tidak Terjadi (1)	Sangat Rendah (1)	Sangat Rendah (3)	Sangat Rendah (5)	Rendah (8)	Sangat Tinggi (20)

GAMBAR 5

(A)

4. Penanganan risiko (*risk treatment*) ditentukan berdasarkan hasil evaluasi terhadap level risiko yang diperoleh dari matriks risiko. Pendekatan Penanganan risiko dalam penelitian ini merujuk pada ISO 27005:2022 dan mencakup 4 respon.

No	Penanganan Risiko	Deskripsi
1	*Risk Avoidance*	Tindakan ini dilakukan dengan menghindari aktivitas atau proses yang berisiko tinggi
2	*Risk Modification*	Tindakan ini bertujuan untuk mengurangi kemungkinan terjadinya risiko atau menurunkan dampaknya
3	*Risk Retention*	Tindakan ini organisasi menyadari dan menerima adanya risiko, baik secara eksplisit maupun implisit, karena risiko dianggap tidak signifikan atau biaya pengendaliannya terlalu besar dibandingkan dampaknya.
4	*Risk Sharing*	Tindakan ini mengalihkan sebagian atau seluruh konsekuensi risiko kepada pihak ketiga

GAMBAR 6

(A)

B. Risk Identification

Identifikasi risiko merupakan tahap awal dalam proses penilaian risiko, yang bertujuan untuk mengenali dan mendokumentasikan risiko-risiko potensial yang dapat memengaruhi aset informasi di organisasi. Dalam penelitian ini, identifikasi risiko dilakukan dengan pendekatan berbasis aset (*asset-based approach*) sebagaimana diatur dalam ISO/IEC 27005:2022, yang mencakup identifikasi aset-aset penting, potensi ancaman (*threats*) yang mungkin terjadi terhadap aset tersebut, serta kerentanan (*vulnerabilities*) yang ada di dalamnya. Dalam penelitian ini, identifikasi aset dilakukan berdasarkan dokumen resmi Kartu Inventaris Barang (KIB) yang diberikan oleh Diskominfo Kabupaten Bogor. Berdasarkan hasil identifikasi, teridentifikasi

sebanyak 40 aset TI, 16 ancaman, 22 kerentanan yang menjadi objek dalam penelitian ini. Setiap kerentanan dikaitkan dengan aset dan ancaman yang sesuai, membentuk dasar bagi analisis risiko dan penentuan tingkat risiko dalam konteks pengelolaan keamanan informasi di Diskominfo Kabupaten Bogor.

C. Risk Analysis

Analisis risiko dilakukan untuk mengetahui tingkat risiko dari setiap kombinasi aset, ancaman, dan kerentanan yang telah diidentifikasi sebelumnya. Nilai *likelihood* dan *consequence* diperoleh melalui pengisian kuesioner yang disebarkan oleh peneliti dalam bentuk Google Form kepada bagian-bagian Diskominfo yang relevan. Nilai-nilai tersebut kemudian dikalikan untuk menghasilkan nilai tingkat risiko (*level of risk*) kemudian disesuaikan dengan matriks risiko. Berdasarkan analisis, diperoleh total 119 risiko yang berhasil diidentifikasi dan dianalisis.

D. Risk Evaluation

Evaluasi risiko dilakukan untuk menentukan risiko-risiko mana saja yang perlu mendapatkan prioritas penanganan berdasarkan tingkat risikonya. Proses ini mengacu pada kriteria penerimaan risiko (*risk acceptance criteria*), dan digunakan untuk membandingkan hasil analisis risiko dengan tingkat toleransi organisasi terhadap ancaman keamanan informasi. Berdasarkan hasil analisis, diperoleh total 119 risiko yang diklasifikasikan ke dalam lima kategori, yaitu 3 risiko dengan tingkat sangat tinggi, 2 risiko tinggi, 18 risiko sedang, 16 risiko rendah, dan 80 risiko sangat rendah. Risiko yang berada pada kategori rendah dan sangat rendah ditangani dengan pendekatan *retention*, yaitu risiko diterima karena dinilai tidak berdampak signifikan. Sementara itu, risiko pada kategori sangat tinggi, tinggi, dan sedang ditangani dengan penanganan aktif berupa *modification, avoidance*, atau *sharing*, disesuaikan dengan karakteristik dan konteks masing-masing risiko.

TABEL 1

Risk ID	Aset	Ancaman	Kerentanan	*Risk Level*	*Level of Risk*	*Risk Treatment*
R116	A39	T15	V17	Sangat Tinggi	25	*Modification*
R21	A7	T12	V4	Sangat Tinggi	24	*Modification*
R8	A3	T10	V3	Sangat Tinggi	20	*Modification*

E. Risk Treatment

Penanganan risiko dilakukan terhadap seluruh risiko yang berada pada tingkat sangat tinggi, tinggi, dan sedang berdasarkan hasil evaluasi sebelumnya. Risiko-risiko tersebut diprioritaskan untuk ditindaklanjuti karena dinilai dapat berdampak signifikan terhadap keamanan informasi dan kelangsungan operasional Diskominfo Kabupaten Bogor apabila tidak segera dikendalikan. Setiap risiko yang ditangani dilengkapi dengan rekomendasi kontrol keamanan informasi yang disusun berdasarkan referensi kontrol-kontrol yang relevan di Annex A ISO/IEC 27001:2022. Rekomendasi kontrol juga dikategorikan berdasarkan aspek penanganan, yaitu *people, process,* dan *technology*. Dengan pembagian ini, kontrol dirancang lebih komprehensif agar mampu mencakup pengembangan kapabilitas sumber daya manusia, pembaruan prosedur operasional, hingga penerapan perangkat teknis. Selain itu, kontrol juga diklasifikasikan berdasarkan jenisnya ke dalam kategori *preventive, detective*, dan *corrective*, sesuai kebutuhan pengendalian risiko agar lebih efektif.

TABEL 2

Aspek	Jenis Kontrol	Referensi ISO/IEC 27001:2022	Rekomendasi Kontrol	*Risk Owner*	*Risk ID*
People, Process	*Preventive, Corrective*	5.2 Peran dan tanggung jawab keamanan informasi 6.3 Kesadaran keamanan informasi, pendidikan, dan pelatihan 6.4 Proses penegakan disiplin	1. Menetapkan prosedur backup personel dan definisi tanggung jawab secara jelas agar proses kerja tidak terhambat ketika ada personel yang tidak hadir. 2. Melakukan perencanaan jadwal kerja yang fleksibel agar dapat mengantisipasi ketidakhadiran personel secara mendadak. 3. Implementasi kebijakan rotasi tugas dan pengembangan multi-skill bagi pegawai agar mereka dapat saling menggantikan peran dalam	Umum & Kepegawaian	R116

			kondisi mendesak.		
Process, Technology	*Preventive*	7.13 Pemeliharaan peralatan 5.9 Inventarisasi informasi dan aset terkait lainnya 7.8 Penempatan dan perlindungan peralatan	1. Menetapkan prosedur pemeliharaan perangkat keras secara berkala dan terdokumentasi. 2. Menjaga persediaan suku cadang printer agar selalu tersedia.	Umum & Kepegawaian	R21
People, Technology	*Preventive, Detective, Corrective*	8.7 Perlindungan terhadap malware 8.12 Pencegahan kebocoran data 8.24 Penggunaan kriptografi	1. Mengimplementasikan perlindungan terhadap malware dengan menggunakan perangkat lunak antivirus terkini dan memberikan pelatihan kepada pengguna mengenai ancaman malware. 2. Menerapkan enkripsi pada data yang disimpan untuk mencegah kebocoran.	Infrastruktur Jaringan	R8

V. KESIMPULAN

Berdasarkan proses *risk assessment*, penelitian ini mengidentifikasi 40 aset TI beserta potensi ancaman, kerentanan, dan area dampaknya. Proses ini menghasilkan 119 risiko, dengan klasifikasi tingkat risiko sebagai berikut: 3 risiko sangat tinggi, 2 risiko tinggi, 18 risiko sedang, 16 risiko rendah, dan 80 risiko sangat rendah. Proses *risk treatment* disusun berdasarkan kontrol dari ISO/IEC 27001:2022 untuk 23 risiko yang berada di luar batas toleransi, dimana sebanyak 20 risiko dilakukan *risk modification* dan 3 risiko dilakukan *risk modification/sharing.*

REFERENSI

[1] M. Utomo, A. H. Noor, and I. Affandi, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I," 2012.

[2] N. Diva Ramadhani, W. Hayuhardhika Nugraha Putra, and A. Dwi Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[3] F. Nasher, "Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (LPSE)," *Media Jurnal Informatika*, vol. 10, no. 1, pp. 1–16, 2018, [Online]. Available: http://jurnal.unsur.ac.id/mjinformatika

[4] M. L. B. Hikam, F. Dewi, and D. Praditya, "Analisis Manajemen Risiko Informasi Menggunakan ISO/IEC 27005:2018 (Studi Kasus: PT.XYZ)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 728–734, May 2024, doi: 10.29100/jipi.v9i2.4709.

[5] T. Hartati, "Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013," vol. 01, no. 02, pp. 63–70, 2017.

[6] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 (Studi Kasus: PT Global Infotech)," 2020.

[7] R. S. P. Abiyoga, "Manajemen Risiko Aset Aplikasi pada Diskominfo Statistik dan Persandian Kota XYZ Menggunakan Standar ISO/IEC 27005: 2008," 2020.

[8] ISO/IEC 27005, "Information security, cybersecurity and privacy protection-Guidance on managing information security risks," 2022.

[9] A. Aminudin and A. Supriyanto, "Kematangan Risiko Keamanan Informasi Layanan TI Menggunakan Pendekatan NIST dan Standar ISO 27001:2013 (Studi Kasus: Bapenda Provinsi Jawa Tengah)," *AITI: Jurnal Teknologi Informasi*, vol. 21, no. 2, pp. 210–229, 2024.

[10] A. K. Shenton, "Strategies For Ensuring Trustworthiness In Qualitative Research Projects," *Education for Information*, vol. 22, no. 2, pp. 63–75, 2004, doi: 10.3233/EFI-2004-22201.