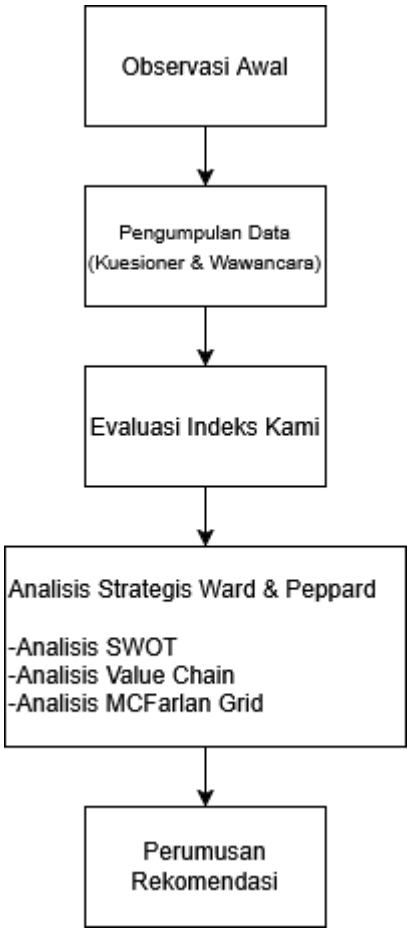
BAB III

METODOLOGI

3.1 Diagram Alur Penelitian

Diagram alur penelitian yang dilakukan dapat dilihat pada Gambar 3.1.



Gambar 3.1 Diagram Alur Penelitian

3.2 Observasi Awal

Observasi awal dilakukan untuk memperoleh pemahaman menyeluruh mengenai kondisi aktual penerapan keamanan informasi di lingkungan Dinas PUTRLH. Kegiatan observasi mencakup pengamatan terhadap kebijakan internal,

prosedur operasional, infrastruktur teknologi informasi, serta pola kerja pegawai yang berkaitan dengan pengelolaan data dan sistem informasi.

Kondisi fisik dan administratif yang dapat memengaruhi keamanan informasi dicatat, seperti akses kontrol ruang *server*, pengelolaan dokumen digital, serta penggunaan perangkat dan jaringan internal. Perangkat lunak keamanan juga diperhatikan dalam penerapannya, serta kesadaran pegawai terhadap pentingnya perlindungan data turut diamati.

Hasil dari kegiatan observasi digunakan sebagai dasar dalam penyusunan instrumen penelitian, seperti kuesioner dan panduan wawancara, agar selaras dengan konteks operasional di lingkungan Dinas. Observasi ini juga menjadi pijakan awal dalam menentukan arah analisis strategi menggunakan pendekatan *Ward and Peppard*, sehingga proses evaluasi dan perumusan rekomendasi dapat dilakukan secara lebih kontekstual dan tepat sasaran.

3.3 Pengumpulan Data

Pengumpulan data dilakukan untuk memperoleh informasi yang relevan mengenai tingkat kematangan keamanan informasi di Dinas PUTRLH. Proses ini dilakukan menggunakan dua metode utama, yaitu kuesioner dan wawancara, yang saling melengkapi untuk memperoleh data kuantitatif dan kualitatif secara seimbang.

Kuesioner disebarkan dengan mengacu pada instrumen Indeks KAMI versi 5.0 kepada responden yang telah ditentukan. Instrumen ini terdiri dari sejumlah pernyataan yang mewakili tujuh domain utama pengelolaan keamanan informasi, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi,

Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi, Pelindungan Data Pribadi, serta Suplemen. Tingkat implementasi menjadi dasar evaluasi pernyataan, yang diberi skor sesuai kategori mulai dari "tidak dilakukan" hingga "diterapkan secara menyeluruh".

Wawancara semi-terstruktur juga dilakukan untuk menggali informasi yang tidak dapat diperoleh melalui kuesioner. Panduan wawancara disusun berdasarkan temuan dari observasi awal dan hasil sementara pengisian kuesioner. Wawancara dilaksanakan secara langsung kepada responden yang memiliki pengetahuan dan pengalaman teknis maupun manajerial terkait keamanan informasi.

Kombinasi antara data kuesioner dan wawancara memberikan pemahaman yang utuh terhadap situasi keamanan informasi di Dinas PUTRLH. Data tersebut menjadi dasar utama dalam proses evaluasi Indeks KAMI dan akan digunakan pada tahapan selanjutnya, yaitu analisis strategis menggunakan pendekatan *Ward and Peppard*.

3.4 Evaluasi Indeks Kami 5.0

Indeks Keamanan Informasi (KAMI) versi 5.0 digunakan sebagai instrumen untuk mengevaluasi tingkat kematangan keamanan informasi di Dinas PUTRLH. Indeks KAMI dipilih karena telah dirancang khusus oleh Badan Siber dan Sandi Negara (BSSN) untuk mengukur kesiapan pengelolaan keamanan informasi pada instansi pemerintah, sesuai dengan standar ISO/IEC 27001.

Evaluasi dilakukan terhadap enam domain utama, yaitu: Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi, Pelindungan Data Pribadi. Domain

dinilai berdasarkan pernyataan-pernyataan yang mencerminkan tingkat implementasi kebijakan dan prosedur yang berlaku.

Tahapan pertanyaan tersebut disesuaikan dengan alat evaluasi yang digunakan yaitu Indeks KAMI versi 5.0. Selain proses pengumpulan data dengan menggunakan kuisioner, data juga dapat diperoleh dengan menggunakan lisan (wawancara) terhadap narasumber terkait jika memang terdapat beberapa data hasil dari kuisioner kurang jelas atau kurang detail sesuai dengan kebutuhan penelitian.

Pertanyaan dikelompokkan untuk 2 keperluan. Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2022. Dalam pengelompokan ini responden diminta untuk memberi tanggapan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan diberi label "1"), efektifitas dan konsistensi penerapannya (label "2"), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label "3"). Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2022.

Setiap jawaban diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka indeks sekaligus digunakan untuk menampilkan hasil evaluasi dalam dashboard di akhir proses ini. Skor yang diberikan untuk jawaban pertanyaan sesuai tingkat kematangannya mengacu pada tabel 3.1

Tabel 3.1 Status pengamanan dan kategori pengamanan

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan/ Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

Pengisian pertanyaan dengan label '3' hanya dapat dilakukan jika seluruh pertanyaan dengan label '1' telah berstatus 'Diterapkan Menyeluruh' dan/atau paling banyak dua pertanyaan berstatus 'Diterapkan Sebagian' dalam satu area pengamanan.

Pengelompokan pertanyaan kedua dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh keangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga.

Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai berikut :

a. Tingkat I - Kondisi Awal
b. Tingkat II - Penerapan Kerangka Kerja Dasar

c. Tingkat III - Terdefinisi dan Konsisten

d. Tingkat IV - Terkelola dan Terukur

e. Tingkat V - Optimal

Untuk membantu memberikan uraian yang lebih detil, tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar ISO/IEC 2700:2013, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

Tabel 3.2 batasan nilai skor Indeks KAMI

Area	**Maks**	**Rendah (<33%)**	**Menengah (33–65%)**	**Tinggi (≥66%)**
Tata Kelola	126	< 42	42 – 82	≥ 83
Risiko	72	< 24	24 – 47	≥ 48
Kerangka Kerja	192	< 64	64 – 126	≥ 127
Aset	258	< 86	86 – 169	≥ 170
Teknologi	186	< 62	62 – 122	≥ 123
PDP (Perlindaungan Data Pribadi)	84	< 28	28 – 55	≥ 56

Tabel 3.2 menunjukkan batas nilai untuk mengklasifikasikan skor Indeks KAMI ke dalam tiga kategori: rendah, menengah, dan tinggi. Klasifikasi ini dihitung berdasarkan persentase dari skor maksimum tiap area, yang mencerminkan sejauh mana kontrol keamanan informasi telah diterapkan dalam organisasi.

Kedua pengelompokan tersebut dapat dipetakan (gambar 3.2) untuk memberikan dua sudut pandang yang berbeda: tingkat kelengkapan pengamanan dan tingkat kematangan pengamanan. Instansi responden dapat menggunakan metrik ini sebagai target program keamanan informasi

Gambar 3.2 Pemetaan kelengkapan dan kematangan

Evaluasi ini tidak hanya digunakan untuk menilai kondisi saat ini, tetapi juga menjadi dasar dalam menyusun analisis strategis menggunakan pendekatan *Ward and Peppard*. Hasil dari Indeks KAMI berperan sebagai fondasi dalam merancang strategi peningkatan keamanan informasi yang sesuai dengan kebutuhan dan kondisi organisasi.

3.5 Analisis Strategis dengan *Ward and Peppard*

Pendekatan perencanaan strategis dari *Ward and Peppard* digunakan untuk menganalisis kondisi keamanan informasi berdasarkan hasil evaluasi Indeks KAMI 5.0. Pendekatan ini dipilih karena mampu menjembatani antara kebutuhan bisnis dan pengelolaan teknologi informasi dalam suatu organisasi, khususnya dalam konteks sektor publik.

Pendekatan *Ward and Peppard* menekankan pentingnya pemahaman terhadap lingkungan internal dan eksternal organisasi sebelum merumuskan strategi sistem informasi dan teknologi informasi (SI/TI). Proses analisis menggunakan tiga alat bantu utama yang terdapat dalam pendekatan ini, yaitu: analisis *SWOT*, analisis *Value chain*, dan analisis *RH McFarlan Strategic Grid*.

3.5.1 Analisis *SWOT*

Analisis *SWOT* digunakan untuk mengidentifikasi faktor kekuatan (*Strengths*), kelemahan (*Weaknesses*), peluang (*Opportunities*), dan ancaman (*Threats*) yang memengaruhi kondisi keamanan informasi di Dinas PUTRLH. Hasil analisis *SWOT* dimanfaatkan untuk merancang strategi yang memanfaatkan kekuatan dan peluang, serta mengatasi kelemahan dan ancaman yang ada.

3.5.2 Analisis Value chain

Analisis *Value chain* diterapkan untuk mengidentifikasi aktivitas utama dan aktivitas pendukung dalam operasional Dinas PUTRLH yang berkaitan dengan pengelolaan keamanan informasi. Aktivitas dianalisis kontribusinya terhadap perlindungan informasi, sehingga dapat ditemukan titik lemah yang perlu diperkuat dalam rantai nilai organisasi.

3.5.3 Analisis McFarlan Strategic Grid

Analisis *McFarlan Strategic Grid* digunakan untuk mengklasifikasikan sistem informasi yang digunakan oleh Dinas PUTRLH berdasarkan tingkat kritikalitas dan dampaknya terhadap operasional. Hasil klasifikasi ini menjadi dasar dalam menentukan prioritas pengembangan atau peningkatan sistem informasi untuk mendukung keamanan data secara strategis.

3.6 Perumusan Rekomendasi

Rekomendasi strategi peningkatan keamanan informasi dirumuskan berdasarkan hasil evaluasi Indeks KAMI 5.0 dan analisis strategis menggunakan pendekatan *Ward and Peppard*. Proses perumusan dilakukan dengan mengintegrasikan temuan dari tiga alat bantu utama, yaitu analisis *SWOT*, *Value chain*, dan *RH McFarlan Strategic Grid.*

Hasil analisis *SWOT* digunakan untuk mengidentifikasi isu strategis yang perlu segera ditangani. Strategi yang dihasilkan dari matriks *SWOT* menjadi dasar awal dalam membentuk arah rekomendasi yang terfokus.

Hasil analisis *Value chain* digunakan untuk menentukan titik-titik aktivitas organisasi yang berkontribusi langsung terhadap keamanan informasi. Aktivitas-aktivitas tersebut, baik utama maupun pendukung, dianalisis untuk mengetahui bagian yang perlu diperkuat, dipertahankan, atau diperbaiki.

Analisis *RH McFarlan Strategic Grid* diterapkan untuk memetakan sistem informasi yang ada berdasarkan dampaknya terhadap operasional. Hasil pemetaan ini digunakan untuk menetapkan prioritas pengembangan sistem informasi yang mendukung keamanan data dan layanan publik secara lebih efektif.

Ketiga pendekatan tersebut digunakan secara terintegrasi untuk menghasilkan rekomendasi yang komprehensif dan realistis. Rekomendasi disusun agar sesuai dengan kondisi aktual organisasi, sumber daya yang tersedia, serta ancaman yang mungkin dihadapi.