ARSITEKTUR TARGRET SPBE

Pemerintah Kabupaten Murung Raya

Daftar Isi

Bab I Konsep Solusi SPBE

1.1. Kondisi Ideal Tata Kelola SPBE

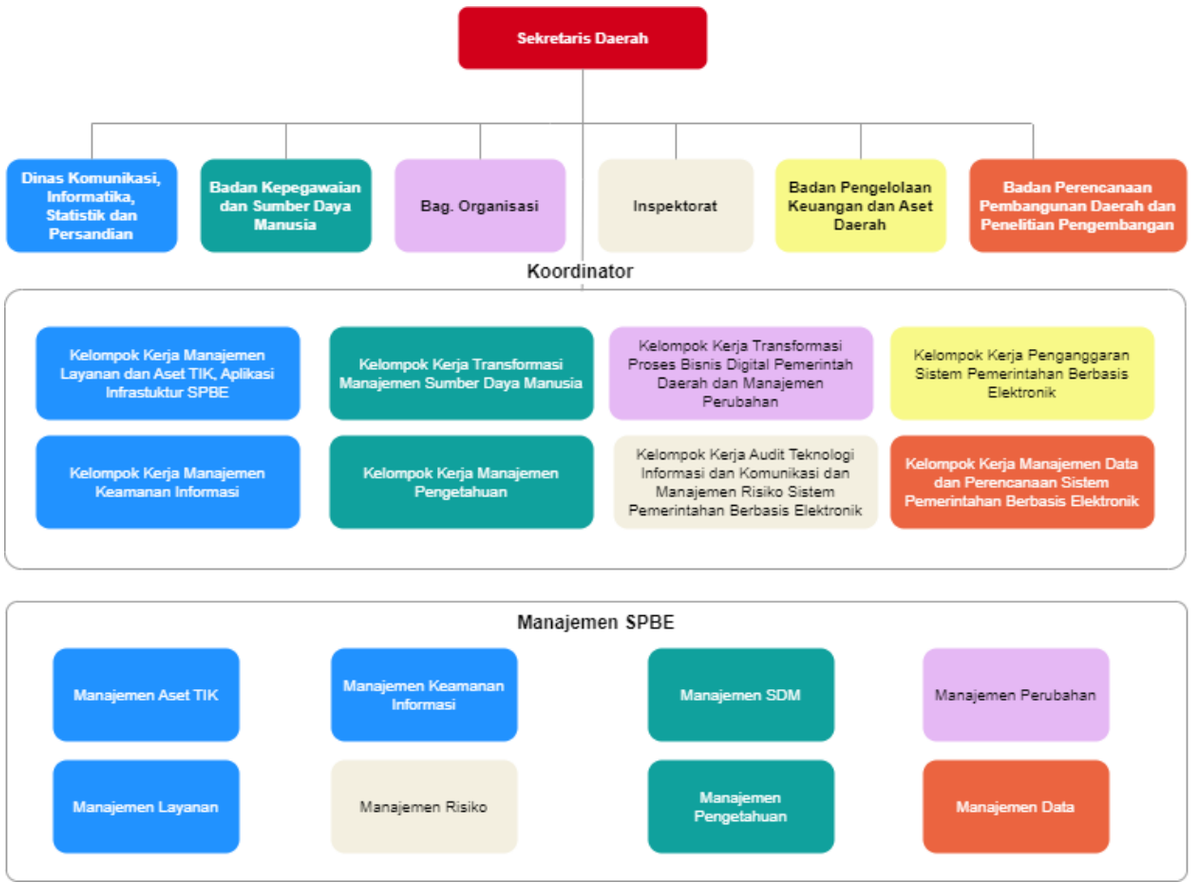
Analisa kondisi ideal dimaksudkan untuk melihat sejauh mana kondisi yang dapat dicapai dari penerapan teknologi informasi dalam mendukung kinerja pemerintahan daerah. Analisa kondisi ideal ini disusun berdasarkan peraturan yang berlaku, tren teknologi informasi saat ini, dan tren teknologi informasi yang akan datang. Sesuai dengan amanat Perpres 95/2018 tentang Sistem Pemerintahan Berbasis Elektronik dalam paragraf tujuan pengembangan SPBE, tiga tujuan utama SPBE, yaitu:

1. **Mewujudkan tata kelola pemerintahan yang bersih, efektif, efisien, transparan, dan akuntabel;**
2. **Mewujudkan pelayanan publik yang berkualitas dan terpercaya; dan**
3. **Mewujudkan sistem pemerintahan berbasis elektronik yang terpadu.**

Kerangka fungsi teknologi informasi tidak sekedar sebagai penunjang manajemen pemerintahan yang ada, tetapi justru merupakan *driver of change* atau agen yang memicu terjadinya perubahan-perubahan mendasar sehubungan dengan proses penyelenggaraan pemerintahan. Pencapaian semua tujuan tersebut merupakan perwujudan dari kondisi ideal di mana pemerintah dengan dukungan teknologi informasi mampu memberikan pelayanan yang responsif dan berkualitas pada masyarakat, dunia usaha, maupun layanan antar lembaga pemerintahan. Tidak terkecuali Pemerintah Kabupaten Murung Raya, secara umum, pemanfaatan Teknologi Informasi dan Komunikasi perlu menganut prinsip-prinsip dasar sebagai pemicu kesuksesan implementasi SPBE.

1.1.1. Kondisi Ideal Kelembagaan

Model kelembagaan yang ideal dalam pengelolaan sumber daya SPBE di lingkungan Pemerintah Kabupaten Murung Raya merupakan sebuah perpaduan model sentralisasi. Model sentralisasi kewenangan diperlukan guna mengontrol penerapan SPBE di masing-masing Perangkat Daerah. Selain itu, dalam penerapan SPBE perlu dibentuk sebuah Tim Koordinasi SPBE, dimana Tim Koordinasi terdiri dari Tim Pengarah dan Tim Pelaksana Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Murung Raya. Adapun tugas dan tata kerja Tim Koordinasi SPBE mengacu pada Keputusan Menteri Negara Pendayagunaan Aparatur Negara dan Reformasi Birokrasi No 965 Tahun 2021 tentang Tugas dan Tata Kerja Tim Koordinasi Sistem Pemerintahan Berbasis Elektronik Nasional.



Gambar 1.1.1.1. Struktur Tim Koordinasi SPBE Ideal (rekomendasi)

Berdasarkan gambar di atas menjelaskan bahwa kondisi ideal dalam struktur Tim Koordinator SPBE Pemerintah Kabupaten Murung Raya terdiri atas Koordinator dan Anggota. Koordinator Tim Koordinasi SPBE Pemerintah Kabupaten Murung Raya mempunyai tugas:

a. Memberikan arahan dan validasi terhadap seluruh inisiatif program dan kegiatan SPBE di lingkungan Pemerintah Kabupaten Murung Raya, khususnya yang bersifat kebijakan dan anggaran/investasi;
b. Memfasilitasi proses koordinasi, kerja sama, atau integrasi penerapan SPBE antar unit;
c. Memfasilitasi penerapan tata kelola dan manajemen SPBE;
d. Melakukan pemantauan dan evaluasi berkala atas penerapan SPBE; dan
e. Melakukan perbaikan dan pengembangan atas hasil rekomendasi pemantauan dan evaluasi penerapan SPBE.

Anggota Tim Koordinasi SPBE Pemerintah Kabupaten Murung Raya terdiri dari seluruh perangkat daerah yang mempunyai tanggung jawab terhadap layanan, data, aplikasi, infrastruktur maupun keamanan informasi. Anggota Tim Koordinasi SPBE Pemerintah Kabupaten Murung Raya mempunyai tugas:

a. Melaksanakan arahan program dan kegiatan SPBE yang telah diputuskan oleh Koordinator;
b. Melakukan optimalisasi proses bisnis;
c. Melakukan integrasi data dalam aplikasi dalam rangka penerapan SPBE yang optimal;

d. Mengelola jaringan teknologi informasi serta pengembangan sistem informasi dan keamanan informasi yang berkelanjutan; dan
e. Menerapkan manajemen SPBE sebagai budaya kerja.

1.1.1.1. Kelompok Kerja (Pokja) SPBE

Pemerintah Kabupaten Murung Raya juga perlu membentuk Tim Koordinasi SPBE dan membaginya ke dalam delapan kelompok kerja SPBE. Delapan kelompok kerja SPBE ini merupakan kepanjangan tangan dari kelompok kerja Tim Koordinasi SPBE Nasional. Adapun kedelapan kelompok kerja dijelaskan sebagai berikut.

1. Kelompok Kerja Transformasi Proses Bisnis Digital, Manajemen Risiko, Manajemen Perubahan, dan Manajemen Sumber Daya Manusia diketuai oleh Bagian Organisasi yang mempunyai tugas melakukan perencanaan strategis pemenuhan kebijakan internal dalam penerapan SPBE, melaksanakan penyiapan perumusan dan sinkronisasi kebijakan SPBE, melakukan koordinasi dan sinkronisasi pelaksanaan kebijakan SPBE, melakukan pemantauan, analisis dan evaluasi penerapan SPBE secara berkala, serta melaporkan hasil penerapan SPBE kepada ketua tim koordinasi SPBE lingkungan Pemerintah Kabupaten Murung Raya.
2. Kelompok Kerja Transformasi Proses Bisnis Digital Pemerintah Daerah diketuai oleh Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian yang mempunyai tugas melakukan koordinasi, sinkronisasi, dan konsultasi penyusunan proses bisnis SPBE, serta melakukan koordinasi, sinkronisasi, dan konsultasi penerapan layanan SPBE dalam pelaksanaan SPBE di lingkungan Pemerintah Kabupaten Murung Raya.
3. Kelompok Kerja Penganggaran SPBE diketuai oleh Badan Pengelolaan Keuangan dan Aset Daerah yang mempunyai tugas merumuskan serta melaksanakan kebijakan dan standardisasi teknis di bidang penganggaran belanja SPBE, serta menyelenggarakan fungsi koordinasi, sinkronisasi, dan konsultasi penyusunan anggaran SPBE dalam pelaksanaan SPBE di lingkungan Pemerintah Daerah Kabupaten Murung Raya.
4. Kelompok Kerja Manajemen Layanan dan Aset TIK, Aplikasi dan Infrastruktur SPBE diketuai oleh Dinas Komunikasi, Informatika, Statistik dan Persandian yang mempunyai tugas melaksanakan kebijakan, pemberian bimbingan teknis dan supervisi, serta pemantauan, evaluasi, dan pelaporan di bidang layanan aplikasi informatika pemerintahan, melakukan koordinasi dan sinkronisasi penyiapan pembangunan dan pengembangan infrastruktur SPBE, melakukan koordinasi dan sinkronisasi penyiapan pengelolaan infrastruktur SPBE, melakukan perumusan standar interoperabilitas antar layanan SPBE dalam pelaksanaan SPBE, melakukan perumusan kebijakan standar interoperabilitas data dan informasi antar layanan SPBE, melakukan koordinasi, sinkronisasi, dan asistensi penerapan kebijakan standar interoperabilitas data dan informasi antar layanan SPBE, melakukan koordinasi, sinkronisasi, dan asistensi keterpaduan pembangunan dan pengembangan aplikasi SPBE di lingkungan Pemerintah Kabupaten Murung Raya dan pada Instansi Pusat dan Pemerintah Daerah dalam pelaksanaan SPBE, merumuskan pemberian pertimbangan pembangunan dan pengembangan aplikasi SPBE yang menggunakan kode sumber

tertutup, merumuskan kebijakan standar teknis dan prosedur pembangunan dan pengembangan aplikasi dalam SPBE, melakukan koordinasi penyiapan pembangunan repositori aplikasi SPBE dalam pelaksanaan SPBE, merumuskan kebijakan standar teknis dan prosedur pengembangan aplikasi dalam pelaksanaan SPBE, merumuskan kebijakan pedoman manajemen aset teknologi informasi dan komunikasi dalam pelaksanaan SPBE, melakukan koordinasi, sinkronisasi dan konsultasi penerapan manajemen aset teknologi informasi dan komunikasi dalam pelaksanaan SPBE, merumuskan pedoman manajemen layanan dalam pelaksanaan SPBE, serta koordinasi, sinkronisasi, dan konsultasi penerapan manajemen layanan dalam pelaksanaan SPBE di lingkungan Pemerintah Kabupaten Murung Raya.

5. Kelompok Kerja Audit Teknologi Informasi dan Komunikasi diketuai oleh Inspektorat yang mempunyai tugas melaksanakan perumusan kebijakan, penyusunan norma, standar, prosedur, dan kriteria, pemberian bimbingan teknis dan supervisi, pemantauan, evaluasi, dan pelaporan di bidang penatakelolaan aplikasi informatika, merumuskan kebijakan umum penyelenggaraan audit teknologi informasi dan komunikasi dalam pelaksanaan SPBE, serta koordinasi, sinkronisasi, dan konsultasi pemantauan, evaluasi, dan pelaporan audit TIK dalam pelaksanaan SPBE di lingkungan Pemerintah Kabupaten Murung Raya.
6. Kelompok Kerja Perencanaan SPBE diketuai oleh Badan Perencanaan Pembangunan Daerah, Penelitian dan Pengembangan yang mempunyai tugas melaksanakan pengoordinasian, perumusan dan pelaksanaan kebijakan, serta pemantauan, evaluasi, dan pengendalian perencanaan pembangunan daerah, melakukan koordinasi dan sinkronisasi perencanaan SPBE, melakukan koordinasi dan sinkronisasi pelaksanaan reviu arsitektur dan peta rencana SPBE Daerah dalam pelaksanaan SPBE, melakukan koordinasi dan sinkronisasi pelaksanaan pemantauan dan evaluasi reviu arsitektur dan peta rencana SPBE Daerah dalam pelaksanaan SPBE, serta melakukan koordinasi dan sinkronisasi terkait integrasi layanan perencanaan, layanan penganggaran, layanan pengadaan, layanan akuntabilitas kinerja, dan layanan pemantauan dan evaluasi dalam pelaksanaan SPBE di Instansi Pusat dan Pemerintah Daerah.
7. Kelompok Kerja Manajemen Data diketuai oleh Dinas Komunikasi, Informatika, Statistik dan Persandian yang mempunyai tugas melaksanakan penetapan domain data dan informasi dalam penyusunan arsitektur SPBE daerah dalam pelaksanaan SPBE, melakukan koordinasi dan sinkronisasi penyelenggaraan tata kelola data dan informasi, koordinasi dan sinkronisasi penerapan manajemen data dalam pelaksanaan SPBE, serta penetapan kebijakan pedoman manajemen data dalam pelaksanaan SPBE pada Instansi Pusat dan Pemerintah Daerah di lingkungan Pemerintah Kabupaten Murung Raya.
8. Kelompok Kerja Manajemen Keamanan Informasi diketuai oleh Dinas Komunikasi, Informatika, Statistik dan Persandian yang mempunyai tugas melaksanakan penyusunan, koordinasi, pelaksanaan, pengendalian, evaluasi, dan pelaporan kebijakan teknis di bidang jaminan keamanan informasi pemerintah, merumuskan

domain keamanan SPBE dalam penyusunan arsitektur SPBE, merumuskan pemberian pertimbangan keamanan jaringan intra pemerintah dalam pelaksanaan SPBE, merumuskan pemberian pertimbangan keamanan sistem penghubung layanan pemerintah dalam pelaksanaan SPBE, melakukan koordinasi, sinkronisasi, dan konsultasi penerapan keamanan, penyelesaian permasalahan keamanan SPBE, merumuskan standar teknis dan prosedur keamanan SPBE, melakukan konsultasi dan asistensi penerapan standar teknis dan prosedur keamanan SPBE dalam pelaksanaan SPBE pada Instansi Pusat, Pemerintah Daerah lain dan lingkungan Pemerintah Kabupaten Murung Raya, merumuskan kebijakan pedoman manajemen keamanan informasi dalam pelaksanaan SPBE, serta melakukan konsultasi dan asistensi penerapan manajemen keamanan informasi dalam pelaksanaan SPBE pada Instansi Pusat, Pemerintah Daerah lain dan lingkungan Pemerintah Kabupaten Murung Raya.

9. Kelompok Kerja Manajemen Pengetahuan diketuai oleh Badan Kepegawaian dan Pengembangan Sumber Daya Manusia yang mempunyai tugas melaksanakan pengkajian dan penerapan di bidang teknologi informasi dan komunikasi, merumuskan kebijakan internal tentang pedoman manajemen pengetahuan dalam pelaksanaan SPBE, serta melakukan koordinasi, sinkronisasi, dan konsultasi penerapan SPBE di lingkungan Pemerintah Kabupaten Murung Raya.

1.1.1.2. Tim *Developer* Internal

Berikut ini dijelaskan kebutuhan tim *developer* internal untuk mendukung pengembangan aplikasi di Pemerintah Kabupaten Murung Raya setiap tahunnya.

Tabel 1.1.1.1. Kebutuhan Anggaran Tim *Developer* Internal

Kebutuhan Anggaran SDM			Tahun									
No	Posisi	Gaji/Bulan	2024		2025		2026		2027		2028	
			Orang	Gaji Setahun	Orang	Gaji Setahun	Orang	Gaji Setahun	Orang	Gaji Setahun	Orang	Gaji Setahun
1	Project Manager	Rp4.000.000	1	Rp48.000.000	1	Rp 48.000.000	1	Rp 48.000.000	2	Rp 96.000.000	2	Rp 96.000.000
2	System Analyst	Rp6.000.000	1	Rp72.000.000	1	Rp 72.000.000	1	Rp 72.000.000	2	Rp 144.000.000	2	Rp 144.000.000
3	Data Scientist/Engineer	Rp7.000.000	1	Rp84.000.000	1	Rp 84.000.000	1	Rp 84.000.000	1	Rp 84.000.000	1	Rp 84.000.000
4	UI/UX Designer	Rp4.500.000	1	Rp54.000.000	2	Rp 108.000.000	2	Rp 108.000.000	2	Rp 108.000.000	2	Rp 108.000.000
5	Front-End Web Developer	Rp5.000.000	1	Rp60.000.000	2	Rp 120.000.000	3	Rp 180.000.000	4	Rp 240.000.000	4	Rp 240.000.000
6	Front-End Mobile Developer	Rp5.000.000	1	Rp60.000.000	2	Rp 120.000.000	3	Rp 180.000.000	4	Rp 240.000.000	4	Rp 240.000.000
7	Back-End Developer	Rp6.000.000	1	Rp72.000.000	2	Rp 144.000.000	3	Rp 216.000.000	4	Rp 288.000.000	4	Rp 288.000.000
8	Application Support	Rp4.000.000	1	Rp48.000.000	2	Rp 96.000.000	3	Rp 144.000.000	3	Rp 144.000.000	3	Rp 144.000.000
	Budget Need / Year		**8**	**Rp498.000.000**	**13**	**Rp 792.000.000**	**17**	**Rp 1.032.000.000**	**22**	**Rp 1.344.000.000**	**22**	**Rp 1.344.000.000**
	Total	**Rp 5.010.000.000**										
	Note : Standard Salary Menyesuaikan UMR Murung Raya (Rp. 3.594.095) dan Standar Perusahaan IT Swasta											

Adapun kompetensi minimum yang dibutuhkan dalam Tim *Developer* Internal Pemerintah Kabupaten Murung Raya mengadopsi standar dari bursa kerja yang dijelaskan sebagai berikut:

A. *System Analyst*

1. Persyaratan
   - Memiliki *background* pendidikan TI/Ilmu Komputer;
   - Menguasai *SDLC* dan *Agile* dalam pengembangan aplikasi;
   - Memahami logika pemrograman dan *business process modelling*;
   - Mampu menganalisis *DFD, Use Case*, dan *ERD*;
   - Berpengalaman dalam *programming* dan integrasi data menggunakan API serta mendokumentasikannya; dan
   - Berpengalaman dalam mendesain *mockup* dan *functional specification document.*
2. Deskripsi Pekerjaan
   - Melakukan analisis kebutuhan aplikasi dalam mengembangkan aplikasi berbasis *cloud* pada *platform* dan aplikasi di dalam Tim *Developer* Pemerintah Kabupaten Murung Raya dengan menghitung dan mengidentifikasi kerentanan atau potensi kegagalan dan ketidaklayakan implementasi aplikasi;
   - Berkoordinasi dengan Tim *Programmer*, Tim Data, Tim Produk, Tim Operasional dan *Stakeholder* dalam proses identifikasi dan analisis kebutuhan pengembangan aplikasi berbasis *Cloud* pada *platform* dan aplikasi yang ada di Pemerintah Kabupaten Murung Raya; dan
   - Mendokumentasikan hasil identifikasi dan analisis kebutuhan pengembangan aplikasi berbasis *cloud* pada *platform* dan aplikasi dalam bentuk dokumentasi teknis yang menjelaskan *flowchart*, *database* dan spesifikasi teknis lainnya yang dapat dipahami oleh Tim *Programmer*, sebagai acuan untuk proses pengembangan aplikasi.

B. Data *Scientist/Engineer*

1. Persyaratan
   - Lulusan gelar sarjana di bidang teknik, matematika, statistik, riset operasi, atau disiplin terkait lainnya;
   - Membuat dan memelihara *data pipeline Architecture* yang optimal;
   - Mengotomatiskan proses manual, mengoptimalkan pengiriman data, mendesain ulang;
   - Membangun infrastruktur yang diperlukan untuk pemuatan data yang optimal dari berbagai sumber data menggunakan teknologi *SQL* dan *NOSQL*;
   - Bekerja sama dengan Tim *Developer* Internal dalam pengembangan aplikasi untuk membantu masalah teknis terkait data dan mendukung kebutuhan infrastruktur data; dan
   - Menguasai *Python, Bigquery, MySQL, PostgreSQL,* dan *Airflow*. Opsional: *MongoDB, elasticSearch, Cloud Platform (eg: GCP),* dan *Gitlab*.

2. Deskripsi Pekerjaan
    - Identifikasi sumber data yang berkualitas dan otomatisasi proses pengumpulan;
    - Melakukan *preprocessing* data terstruktur dan tidak terstruktur;
    - Menganalisis keperluan data untuk pengembangan aplikasi;
    - Menyajikan informasi menggunakan teknik visualisasi data;
    - Mengusulkan solusi dan strategi untuk tren pengembangan aplikasi; dan
    - Berkolaborasi dengan Tim Internal *Developer*.

C. UI/UX Designer

1. Persyaratan
    - Berpengalaman dalam *basic design process: research, ideation, user journey*;
    - Mampu mempresentasikan *wireframe, prototype* ataupun *UI/UX*;
    - Berpengalaman dalam melakukan *testing* terhadap UI/UX;
    - Mampu mengikuti perkembangan teknik dan *tools design UI/UX*;
    - Familiar dengan *tools Figma, Adobe XD, Sketch* atau *tools design* lainnya;
    - Menguasai *flow, wireframe* dan *prototype*; dan
    - Mengelola *knowledge sharing* para UI/UX *designer*.
2. Deskripsi Pekerjaan
    - Menciptakan desain yang berpusat pada pengguna untuk memahami persyaratan dan kebutuhan bisnis, serta umpan balik yang pengguna berikan;
    - Merancang *user flows, wireframes, prototypes, dan mockups;*
    - Menunjukan persyaratan ke dalam *style guides,* aplikasi, pola desain, serta *interface* yang menarik dan nyaman;
    - Merancang elemen, seperti: *input controls*, navigasi, dan komponen informasi lainnya;
    - Membuat desain grafis yang original;
    - Mengidentifikasi dan memecahkan masalah terkait pengalaman pengguna;
    - Bekerja secara kolaboratif dengan tim produksi, *developer*, dan manajemen; dan
    - Mengevaluasi *feedback* pengguna, metrik penggunaan, serta *usability finding* ke dalam hasil desain untuk meningkatkan pengalaman pengguna.

D. Front-End Developer (Web & Mobile)

1. Persyaratan
    - Lulusan minimum S1 Ilmu Komputer atau Teknik Informatika;
    - Menguasai pengembangan *front end* dengan *javascript*;
    - Memahami konsep *DOM, HoC, Promise, Async/Await, Event Delegation,* dan *Event Bubbling*;
    - Menguasai konsep *UI/UX design pattern* dan responsif desain pada *web* dan *mobile*;
    - Familiar menggunakan *code repository management,* seperti: *Git/Gitlab;*
    - Memahami penggunaan HTML sesuai *best practice;*
    - Memiliki kemampuan untuk membangun aplikasi dengan bahasa pemrograman *javascript* atau *typescript*;
    - Memiliki kemampuan dalam menggunakan *CSS/Less/Sass* dengan baik;

- Memiliki kemampuan pengembangan produk menggunakan *Bootstrap/Tailwind/Vuetify/MUI/Framework7/Ant Design*;
- Memiliki kemampuan dalam membangun produk menggunakan *ReactJS,NextJS/Gatsby,* dan *library/framework* berbasis *ReactJS* lainnya;
- Memiliki kemampuan dalam membangun produk menggunakan *VueJS,NuxJS/Gridsome,* dan *Library/framework* berbasis *VueJS*; dan
- Memiliki kemampuan yang baik dalam memahami konsep, dasar, dan cara menggunakan beberapa jenis *web service/API*, khususnya *REST API*.

2. Deskripsi Pekerjaan
   - Membangun dan merancang aplikasi *front end* sebuah aplikasi/fitur;
   - Memastikan kelayakan teknis desain *UI/UX*;
   - Memastikan semua *input user* tervalidasi dan terkirim ke *backend*;
   - Mengatasi berbagai *bug* dan *error* pada sisi *front end*;
   - Menerapkan prinsip pengembangan *front end* yang sesuai (*best practice*) dan memastikan bahwa *front end* dapat berjalan dengan baik di semua perangkat;
   - Melakukan *maintenance* dan pembaharuan aplikasi *front end* yang sudah ada;
   - Mendukung siklus pengembangan (konsep, desain, pengujian, rilis, operasional);
   - Bekerja sama dengan tim untuk berinovasi dalam meningkatkan kualitas dan performa aplikasi;
   - Berkolaborasi dengan tim infrastruktur dan tim *programmer* yang berspesialisasi dalam *DevOps, Backend, QA, System Analyst, Product Owner, UI/UX Designer*; dan
   - Berkontribusi dalam membantu pembuatan dokumentasi teknis atau secara manual.

E. Back-End Developer

1. Persyaratan
   - Merupakan lulusan S1 Teknik Informatika;
   - Memiliki minimum 2 tahun pengalaman terkait bidang pemrograman atau pembangunan aplikasi;
   - Memiliki pemahaman yang kuat terkait konsep OOP dan MVC;
   - Berpengalaman dalam penggunaan PHP dan *framework* yang relevan *(Laravel, Yii, CI, dll)/C# .Net/ASP.Net;*
   - Memahami bahasa pemrograman *SQL (SQL pusat data/PostgreSQL/MySQL);*
   - Memahami konsep manajemen *source code* seperti *Git*;
   - Memahami dan dapat mengimplementasikan *web service/API*;
   - Bersedia untuk belajar *framework*, teknologi, atau bahasa pemrograman yang berbeda;
   - Dapat membaca dokumen kebutuhan aplikasi; dan
   - Memiliki jiwa yang kreatif, berorientasi pada detail dan memiliki *skill* komunikasi yang baik.
2. Deskripsi Pekerjaan
   - Melakukan perancangan *database;*

- Melakukan *update* atau pembaharuan struktur data yang telah ada;
- Membuat perancangan alur aplikasi;
- Melakukan pembangunan aplikasi dan *testing* di sisi *backend;*
- Mengatur keamanan aplikasi dan memastikan aplikasi memiliki tingkat keamanan yang baik;
- Melakukan *maintenance*/menemukan *bug* pada aplikasi dan memperbaikinya; dan
- Berkoordinasi dengan tim *frontend* untuk melakukan riset dan evaluasi terkait tampilan desain aplikasi agar sesuai dengan struktur *database* yang dibangun.

F. Application Support

1. Persyaratan
   - Minimal S1 jurusan Sistem Informasi/ Teknik Informatika;
   - Mempunyai Pengalaman dalam bidang *Application Support;*
   - Memiliki pengalaman di *ERP System* (Nilai tambah jika memiliki pengalaman di SAP);
   - Memiliki pengalaman dalam implementasi *project* aplikasi;
   - Memiliki pengalaman dalam dokumentasi aplikasi; dan
   - Memiliki pengalaman dalam membuat *user* manual aplikasi.
2. Deskripsi Pekerjaan
   - Melakukan instalasi dan konfigurasi aplikasi;
   - Memastikan aplikasi informasi dapat berjalan;
   - Monitoring terhadap permintaan bantuan penanganan insiden yang di *submit* melalui *Web Ticketing System (SLA dan troubleshoot);*
   - Menerima *Issue* dari *user* melalui *Web Ticketing System* maupun *Non Ticketing;* dan
   - Monitoring Laporan *Daily Log* dari *Team Application Support.*

1.1.1.3. Kebijakan SPBE

Reviu kebijakan perlu dilakukan untuk mendukung pengembangan, penggunaan, maupun pemeliharaan sumber daya TIK. Daftar kebijakan yang perlu direviu, yaitu:

a. Kebijakan internal arsitektur SPBE;
b. Kebijakan internal peta rencana SPBE;
c. Kebijakan internal manajemen data SPBE;
d. Kebijakan internal pembangunan aplikasi SPBE;
e. Kebijakan internal layanan pusat data;
f. Kebijakan internal layanan jaringan intra Pemerintah;
g. Kebijakan internal penggunaan sistem penghubung layanan Pemerintah;
h. Kebijakan internal manajemen keamanan informasi;
i. Kebijakan internal audit teknologi informasi dan komunikasi; dan
j. Kebijakan internal tim koordinasi SPBE.

1.1.2. Penganggaran SPBE

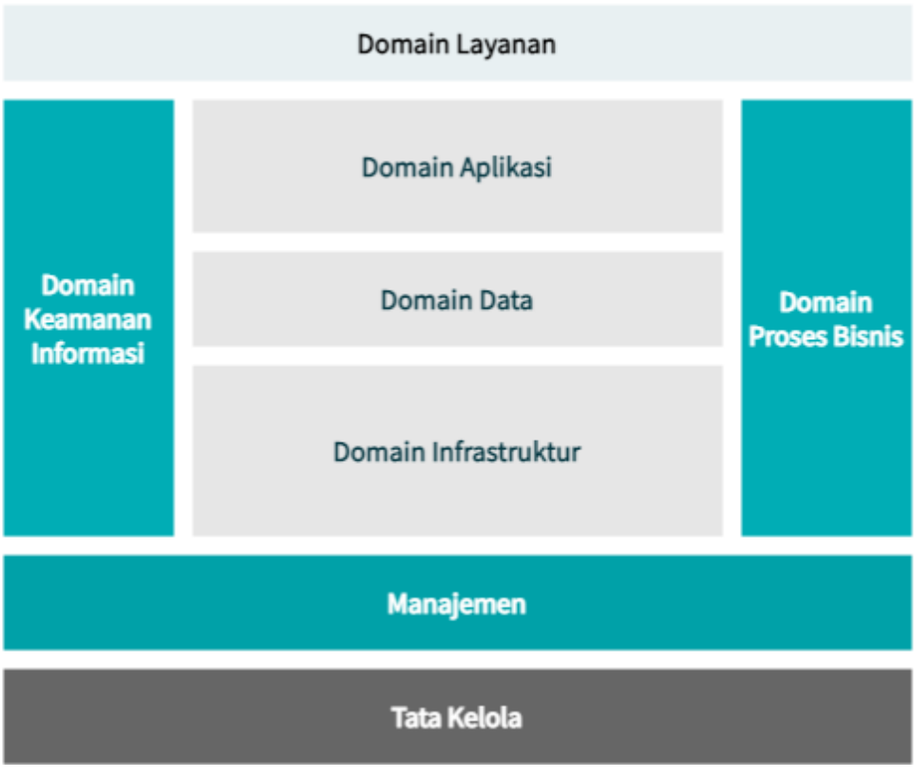
Anggaran dan belanja SPBE disusun dengan berpedoman pada arsitektur SPBE Pemerintah Kabupaten Murung Raya yang kemudian dituangkan dalam Peta Rencana SPBE. Anggaran dan belanja SPBE kemudian disusun dalam bentuk inventarisasi kebutuhan anggaran dan belanja perangkat daerah. Penyusunan anggaran dan belanja SPBE dikoordinasikan oleh Bappeda dan dibantu dengan Diskominfo. Koordinasi dalam proses penyusunan anggaran dan belanja SPBE dilakukan dengan cara melakukan peninjauan terhadap rencana anggaran dan belanja SPBE untuk memastikan keterpaduan perencanaan anggaran dan belanja SPBE di seluruh perangkat daerah.

Selain itu, Tim Anggaran Pemerintah Daerah (TAPD) bertugas untuk memastikan kesesuaian rencana anggaran dan belanja SPBE dengan perencanaan yang tertuang dalam rencana kerja Pemerintah Kabupaten Murung Raya. Anggaran dan belanja SPBE harus mendapatkan persetujuan oleh Tim Koordinasi SPBE Pemerintah Kabupaten Murung Raya yang melakukan peninjauan terhadap realisasi penggunaan anggaran dan belanja SPBE secara berkala. Lebih jauh, hasil peninjauan digunakan sebagai pertimbangan dalam penyusunan rencana anggaran dan belanja SPBE periode selanjutnya.

1.2. Tata Kelola SPBE

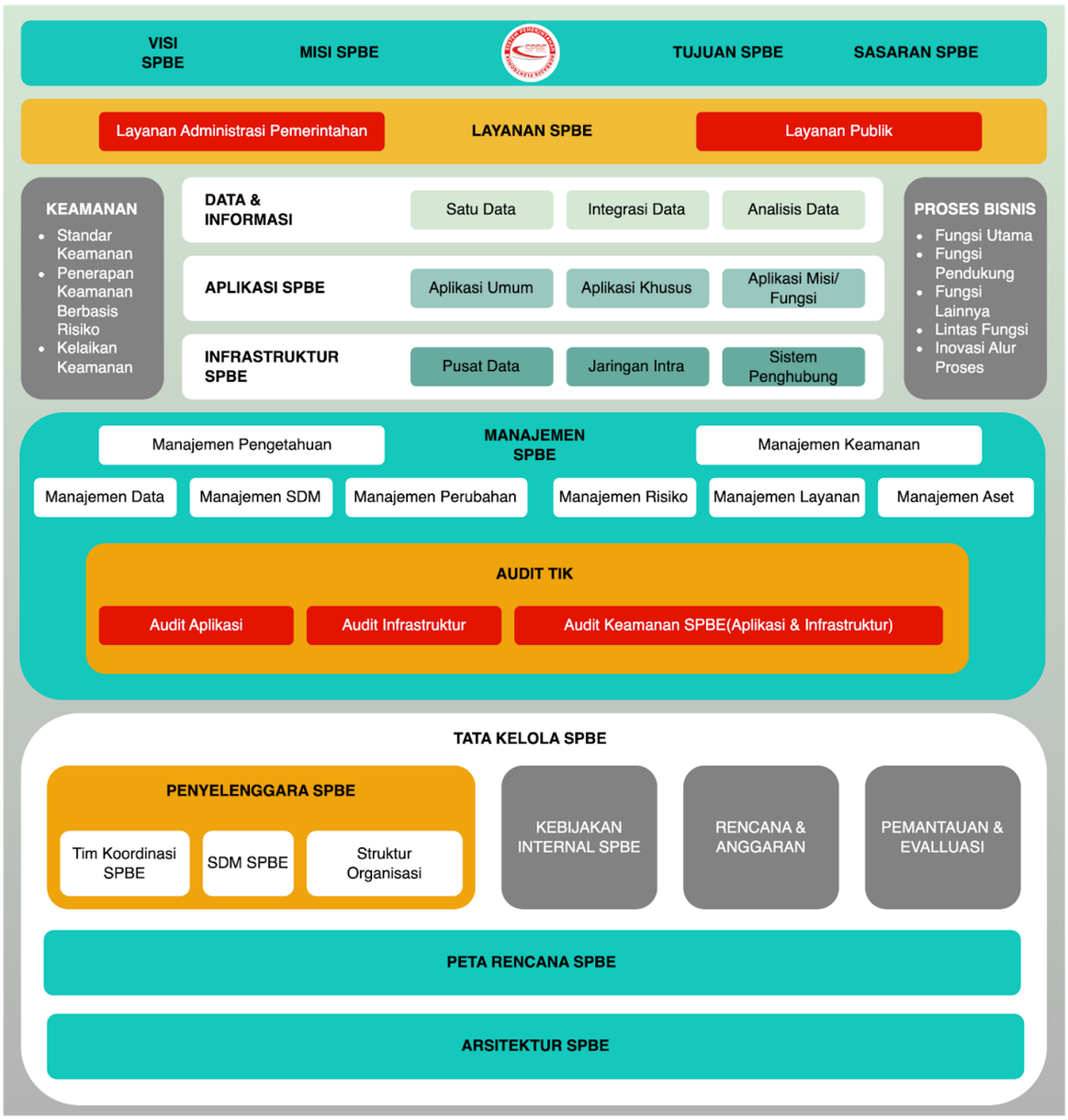
1.2.1. Tata Kelola Arsitektur SPBE

Arsitektur dan Peta Rencana SPBE merupakan panduan dalam pelaksanaan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terpadu. Arsitektur memuat beberapa domain yang dijelaskan sebagai berikut:



Gambar 1.2.1.1. Domain Arsitektur SPBE (i)

Berdasarkan gambar di atas dapat disimpulkan bahwa Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terintegrasi. Pengembangan dari kelima aspek tersebut didukung oleh manajemen yang dikelola dengan baik dan tata kelola yang disusun secara rinci serta terarah. Setiap domain yang disebutkan dalam kerangka SPBE memiliki detail masing-masing yang saling terkait dan dapat mendorong keberhasilan domain-domain lainnya. Detail dari masing-masing domain dijelaskan dalam Gambar 1.2.1.2. Domain Arsitektur SPBE (ii).



Gambar 1.2.1.2. Domain Arsitektur SPBE (ii)

Proses penyusunan dokumen arsitektur SPBE diawali dengan domain tata kelola. Tata kelola adalah rangkaian proses, kebiasaan, kebijakan, aturan, dan institusi yang mempengaruhi pengarahan, pengelolaan, serta pengontrolan kegiatan dalam Pemerintah Kabupaten Murung Raya. Tata kelola juga mencakup hubungan antara para pemangku kepentingan yang terlibat serta tujuan pengelolaan dari institusi. Dalam hal ini, pengembangan arsitektur SPBE bidang tata kelola dimulai dengan membentuk tim koordinasi, menentukan kebijakan, dan menyusun rencana serta anggaran.

Langkah kedua dalam membangun arsitektur SPBE adalah dengan menentukan bentuk-bentuk manajemen yang akan dilakukan dalam proses pengembangan SPBE di Pemerintah Kabupaten Murung Raya. Manajemen adalah sebuah cara untuk mengarahkan Tim Koordinasi SPBE untuk mencapai tujuan utama melalui proses perencanaan, pengorganisasian, pengelolaan, dan pengawasan sumber daya dengan cara yang efektif dan efisien. Adapun 8 (delapan) proses manajemen dalam SPBE mencakup:

1. Manajemen Resiko;

2. Manajemen Perubahan;
3. Manajemen Data;
4. Manajemen SDM;
5. Manajemen Aset TIK;
6. Manajemen Layanan;
7. Manajemen Pengetahuan; dan
8. Manajemen Keamanan Informasi.

Lebih jauh, arsitektur SPBE pada domain SPBE yang perlu dikelola pertama adalah domain proses bisnis. Proses bisnis dikelola sedemikian rupa sehingga dapat memberikan alur organisasi internal serta pelayanan paling efektif dan efisien. Domain proses bisnis selanjutnya dapat menjadi acuan dalam pembangunan aplikasi pada domain aplikasi. Dalam hal ini, aplikasi dapat berupa portal yang mendukung layanan dan telah terintegrasi dengan aplikasi lain. Beberapa portal layanan yang dapat dibangun antara lain:

1. Portal layanan administrasi pemerintahan; dan
2. Portal layanan publik.

Berdasarkan penggunaannya, aplikasi dapat dibagi menjadi aplikasi yang bersifat khusus dan aplikasi yang bersifat umum. Setiap pembangunan aplikasi tidak lepas dari adanya integrasi data antar perangkat daerah di lingkungan Pemerintah Kabupaten Murung Raya. Integrasi data tidak hanya antar perangkat daerah saja tetapi juga dapat dilakukan integrasi ke portal data nasional. Selain itu, domain lain yang dikembangkan dalam proses pembangunan SPBE adalah domain infrastruktur. Domain ini dikembangkan sebagai bentuk penanganan alat yang digunakan dalam pelayanan yang ada di Pemerintah Kabupaten Murung Raya. Domain infrastruktur dibagi menjadi 2 (dua) jenis, yaitu: infrastruktur jaringan dan infrastruktur pusat data. Infrastruktur jaringan adalah hal-hal mengenai pengelolaan koneksi yang ada pada instansi, termasuk didalamnya pusat pengendalian dan jaringan, jaringan intra instansi pusat, jaringan intra instansi pemda, dan jaringan pita lebar. Selanjutnya untuk pusat data nasional didalamnya terdapat *cloud services* dan repositori aplikasi/data. Domain terakhir yang digunakan dalam peningkatan layanan instansi adalah domain keamanan informasi. Aspek keamanan informasi adalah aspek-aspek yang dilingkupi dan melingkupi keamanan informasi dalam sebuah aplikasi informasi. Aspek-aspek ini meliputi privasi/kerahasiaan khususnya dalam menjaga kerahasiaan informasi dari semua pihak, kecuali yang memiliki kewenangan.

Arsitektur SPBE Pemerintah Kabupaten Murung Raya disusun oleh Tim Koordinasi SPBE dan mengacu pada Arsitektur SPBE Nasional. Arsitektur SPBE dan peta rencana perlu ditinjau secara berkala minimal satu tahun sekali dan perlu dilakukan perubahan ketika terjadi perubahan terhadap arsitektur SPBE Nasional, dokumen perencanaan pembangunan dan kondisi penerapan SPBE di Pemerintah Kabupaten Murung Raya. Berdasarkan hasil pemantauan dan evaluasi pelaksanaan SPBE di Pemerintah Kabupaten Murung Raya ditahun 2022 menyatakan perlu adanya perubahan substansi kondisi arsitektur SPBE agar disesuaikan dengan Arsitektur SPBE Nasional. Peninjauan tersebut dilakukan oleh Tim Koordinator SPBE. Hasil peninjauan tersebut dijadikan sebagai dasar dalam mengubah arsitektur SPBE dan peta rencana di Tahun 2023 ini.

1.2.2. Tata Kelola Kebijakan SPBE

Penyusunan kebijakan perlu dilakukan untuk mendukung pengembangan dan operasional SPBE. Rekomendasi kebijakan yang perlu dibuat mengacu pada Perpres 95/2018 dan pembuatan kebijakan berdasarkan analisis domain, aspek, dan indikator untuk peningkatan nilai indeks evaluasi SPBE. Adapun rekomendasi kebijakan terkait tata kelola dan manajemen SPBE di Pemerintah Kabupaten Murung Raya sebagai berikut :

A. Kebijakan internal arsitektur SPBE

1. Menetapkan kebijakan internal arsitektur SPBE yang memuat secara lengkap pengaturan mengenai referensi arsitektur dan domain arsitektur SPBE (proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, keamanan SPBE, serta layanan SPBE); dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal arsitektur SPBE.

B. Kebijakan internal peta rencana SPBE

1. Menetapkan kebijakan internal terkait peta rencana SPBE yang telah mengatur seluruh muatan peta rencana SPBE secara lengkap (tata kelola SPBE, manajemen SPBE, layanan SPBE, infrastruktur SPBE, aplikasi SPBE, keamanan SBE, dan audit TIK); dan
2. Membuat jadwal reviu dan melakukan evaluasi secara periodik pada kebijakan internal peta rencana SPBE.

C. Kebijakan internal manajemen data SPBE

1. Menetapkan kebijakan manajemen data yang mengatur seluruh rangkaian proses pengelolaan arsitektur data, data induk, data referensi, basis data, kualitas data, dan interoperabilitas data; dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal manajemen data.

D. Kebijakan internal pembangunan aplikasi SPBE

1. Menetapkan kebijakan internal pembangunan aplikasi SPBE yang mengatur siklus pembangunan aplikasi SPBE dengan perangkat daerah yang menjalankan fungsi pengelolaan TIK; dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal pembangunan aplikasi SPBE.

E. Kebijakan internal layanan pusat data

1. Menetapkan konsep kebijakan internal terkait layanan pusat data yang mengatur interkoneksi layanan pusat data dengan pusat data Nasional dan/atau mengatur penggunaan layanan pusat data Nasional; dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal Layanan Pusat Data.

F. Kebijakan internal layanan jaringan intra Pemerintah

1. Menetapkan konsep kebijakan internal terkait layanan jaringan intra yang mengatur interkoneksi layanan jaringan intra Pemerintah; dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan jaringan intra Pemerintah.

G. Kebijakan internal penggunaan sistem penghubung layanan Pemerintah

1. Menetapkan konsep kebijakan internal terkait Sistem Penghubung Layanan yang mengatur penggunaan Sistem Penghubung Layanan untuk seluruh perangkat daerah & keterhubungan dengan Sistem Penghubung Layanan Pemerintah; dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan sistem penghubung layanan Pemerintah.

H. Kebijakan internal manajemen keamanan informasi

1. Menetapkan kebijakan internal terkait Manajemen Keamanan Informasi yang mengatur penerapan untuk seluruh perangkat daerah; dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan manajemen keamanan informasi.

I. Kebijakan internal audit teknologi informasi dan komunikasi

1. Menetapkan kebijakan internal terkait audit TIK yang telah mengatur pelaksanaan seluruh audit TIK (audit infrastruktur SPBE audit aplikasi SPBE, dan audit keamanan SPBE); dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan audit teknologi informasi dan komunikasi.

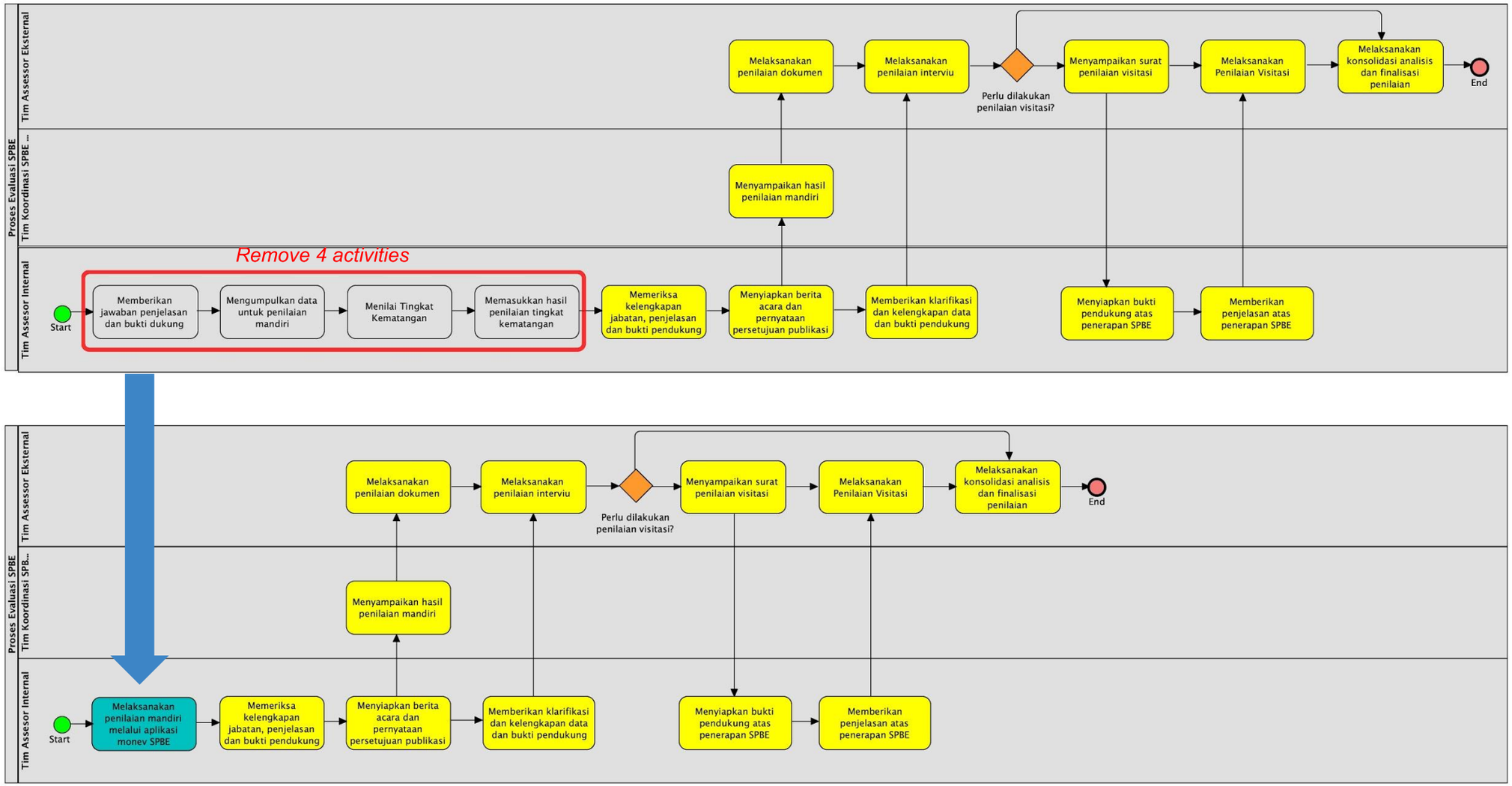
J. Kebijakan internal tim koordinasi SPBE

1. Menetapkan kebijakan internal terkait Tim Koordinasi SPBE yang telah mencakup pengaturan tugas-tugas Tim Koordinasi SPBE yang mendukung penerapan SPBE pada seluruh perangkat daerah; dan
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal tim koordinasi SPBE.

1.2.3. Tata Kelola Proses Bisnis

Proses bisnis pemerintahan perlu dipetakan secara berkala minimal 5 tahun sekali ke dalam bentuk peta proses bisnis yang penyusunannya mengacu pada Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 19 tahun 2018 tentang Penyusunan Peta Proses Bisnis Instansi Pemerintah.

Dewasa ini, digitalisasi dapat membantu mengoptimalkan proses bisnis pemerintah yang kompleks menjadi lebih efisien dan efektif, sebagai contoh proses evaluasi SPBE yang yang didalamnya terdapat 10 aktivitas dan dilakukan secara manual. Selanjutnya ketika dilakukan digitalisasi dalam proses evaluasi SPBE tersebut terdapat beberapa aktivitas yang bisa di simplifikasi dari 10 aktivitas menjadi 7 aktivitas. Adapun ilustrasi digitalisasi untuk simplifikasi proses bisnis ditunjukkan pada gambar berikut:



Gambar 1.2.3.1. Ilustrasi Simplifikasi Proses Evaluasi SPBE

1.2.4. Tata Kelola Data

Satu Data Indonesia adalah kebijakan tata kelola data pemerintah untuk menghasilkan data yang akurat, mutakhir, terpadu, dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antara Instansi Pusat dengan Instansi Daerah, melalui pemenuhan standar data, metadata, interoperabilitas data, dan menggunakan kode referensi dan data induk (Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019). Satu Data Indonesia harus dilakukan berdasarkan prinsip sebagai berikut:

1. Data yang dihasilkan oleh produsen data harus memenuhi standar data;
2. Data yang dihasilkan oleh produsen data harus memiliki metadata;
3. Data yang dihasilkan oleh produsen data harus memenuhi kaidah Interoperabilitas data; dan
4. Data yang dihasilkan oleh produsen data harus menggunakan kode referensi dan/atau data induk.

Standar data statistik dan data geospasial ditetapkan oleh pembina data yang merupakan salah satu perangkat daerah yang diberi kewenangan melakukan pembinaan terkait data sebagaimana diatur dalam Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia. Secara khusus, Pemerintah Kabupaten Murung Raya harus menetapkan standar data yang pemanfaatannya ditujukan untuk memenuhi kebutuhan perangkat daerah sesuai dengan tugas dan fungsinya yang telah ditetapkan oleh pembina data. Data yang dihasilkan oleh produsen data harus dilengkapi dengan metadata yang informasinya mengikuti struktur dan format baku yang merujuk pada bagian informasi serta spesifikasi atau standar teknis dari metadata. Adapun standar metadata Pemerintah Kabupaten Murung Raya, yaitu:

Tabel 1.2.4.1 Standar Metadata

Elemen	Keterangan
Sumber	Nama instansi pemilik data
Author	Bidang di perangkat daerah selaku produsen data
Last Updated	Tanggal data di *update*
Created	Tanggal data dibuat
Nama Berkas	Nama berkas digital
Ekstensi	Format file (*xls, doc, ppt, pdf)*

Pemerintah Kabupaten Murung Raya dapat menetapkan struktur dan format yang baku untuk data yang pemanfaatannya memenuhi kebutuhan perangkat daerah sesuai dengan tugas dan fungsi yang telah ditetapkan oleh pembina data. Data dari produsen data

harus memenuhi kaidah interoperabilitas data. Adapun kaidah interoperabilitas data harus memenuhi kriteria sebagai berikut:

1. Konsisten dalam sintak/bentuk, struktur/skema/komposisi penyajian, dan semantik/artikulasi keterbacaan; dan
2. Disimpan dalam format terbuka yang dapat dibaca sistem elektronik.

Panduan dasar yang merujuk pada Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia bertujuan untuk mengatasi berbagai permasalahan berkaitan dengan data. Adapun panduan data yang dapat diikuti untuk Pemerintah Kabupaten Murung Raya sebagai berikut:

A. Forum Satu Data Indonesia

Mengacu pada Perpres 39 Tahun 2019 tentang Satu Data Indonesia Pasal 10 Ayat (3) huruf a, Forum Satu Data Indonesia akan menyepakati:

1. Kode referensi dan/atau data induk; dan
2. Perangkat daerah yang menjadi produsen data atas kode referensi dan/atau data induk tersebut.

B. Penyelenggara Satu Data Indonesia

Penyelenggara Satu Data Indonesia dilaksanakan oleh:

1. Pembina Data Tingkat Kabupaten;
2. Walidata Tingkat Kabupaten;
3. Walidata Pendukung Tingkat Kabupaten; dan
4. Produsen Data Tingkat Kabupaten.

C. Dewan Pengarah Satu Data Indonesia

Tugas Dewan Pengarah Satu Data Indonesia, yaitu:

1. Mengkoordinasikan dan menetapkan kebijakan terkait Satu Data Indonesia;
2. Mengkoordinasikan pelaksanaan Satu Data Indonesia;
3. Melakukan pemantauan dan evaluasi pelaksanaan Satu Data Indonesia; dan
4. Mengkoordinasikan penyelesaian permasalahan dan hambatan pelaksanaan Satu Data Indonesia.

D. Komposisi Dewan Pengarah Satu Data Indonesia

Dewan Pengarah Satu Data Indonesia terdiri dari:

1. Ketua merangkap anggota, yaitu Sekda; dan
2. Anggota, terdiri atas Kepala Dinas dari masing-masing perangkat daerah.

E. Pembina Data Tingkat Daerah

Tugas Pembina Data Tingkat Daerah, yaitu:

1. Menetapkan Standar Data yang berlaku lintas Instansi Daerah;
2. Menetapkan struktur yang baku dan format yang baku dari Metadata yang berlaku lintas Instansi Daerah;
3. Memberikan rekomendasi dalam proses perencanaan pengumpulan data;
4. Melakukan pemeriksaan ulang terhadap data prioritas; dan
5. Melakukan pembinaan penyelenggaraan Satu Data Indonesia sesuai dengan ketentuan peraturan perundang-undangan.

F. Produsen Data

Tugas produsen data tingkat daerah, yaitu:

1. Mengumpulkan, memeriksa kesesuaian data, dan mengelola data yang disampaikan oleh produsen data sesuai dengan prinsip Satu Data Indonesia;
2. Menyebarluaskan data, metadata, kode referensi, dan data induk di Portal Satu Data Indonesia;
3. Membantu pembina data dalam membina produsen data;
4. Memberikan masukan kepada pembina data dan Kepala Dinas mengenai standar data, metadata, dan interoperabilitas data;
5. Menghasilkan data sesuai dengan prinsip Satu Data Indonesia; dan
6. Menyampaikan data dan metadata kepada produsen data.

Produsen Data melakukan pengumpulan data sesuai dengan:

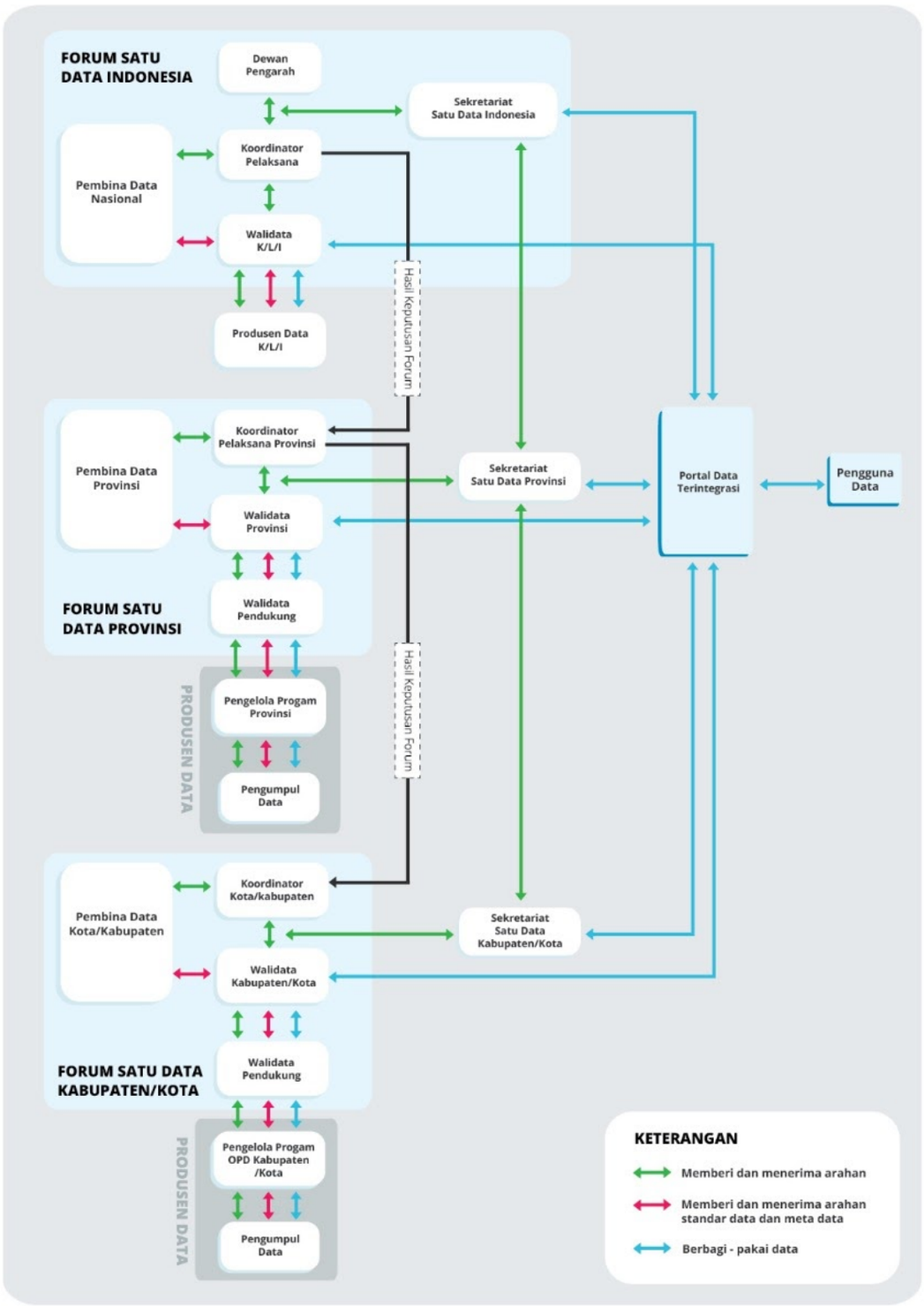
1. Standar data;
2. Daftar data yang telah ditentukan dalam Forum Satu Data Indonesia; dan
3. Jadwal pemutakhiran data atau rilis data yang selanjutnya disampaikan kepada produsen data.

G. Pelaksana Penyelenggaraan Satu Data Indonesia

Pelaksana Penyelenggaraan Satu Data Indonesia dilakukan oleh:

1. Pembina data tingkat daerah;
2. Produsen data tingkat daerah;
3. Produsen data pendukung; dan
4. Produsen data tingkat daerah.

Dari panduan dasar untuk implementasi Satu Data Indonesia di atas, maka didapatkan alur koordinasi aktor yang dapat dilihat pada Gambar berikut ini :



Gambar 1.2.4.1. Alur Koordinasi Aktor Forum Satu Data

1.2.5. Tata Kelola Layanan

Proses transformasi digital atau tata kelola layanan dalam SPBE merupakan salah satu upaya pemerintah dalam mendigitalkan layanan yang ada untuk mendukung visi, misi dan tujuan SPBE. Layanan SPBE terbagi menjadi 2 kategori yaitu Layanan Administrasi Pemerintahan dan Layanan Publik. Berikut merupakan gambaran layanan yang perlu ada dalam SPBE.

Layanan Administrasi Pemerintah	Layanan Publik	
Layanan Perencanaan	Pengaduan Publik	Kesejahteran Ekonomi
Layanan Penganggaran	Dokumentasi dan Informasi	Pertanian dan Peternakan
Layanan Keuangan	Kependudukan	Ketenagakerjaan
Layanan Pengadaan Barang dan Jasa	Perizinan Usaha	Agama
Layanan Kepegawaian	Kebudayaan	Pemukiman
Layanan Kearsipan Dinamis	Pendidikan	Perlindungan Sosial
Layanan Pengelolaan Barang Milik Daerah	Lingkungan Hidup	Perdagangan
Layanan Pengawasan Internal	Industri	Pariwisata
Layanan Akuntabilitas Kinerja Organisasi	Kesehatan	Transportasi
Layanan Kinerja Pegawai	Portal Data	

Gambar 1.2.5.1 Tata Kelola Layanan SPBE

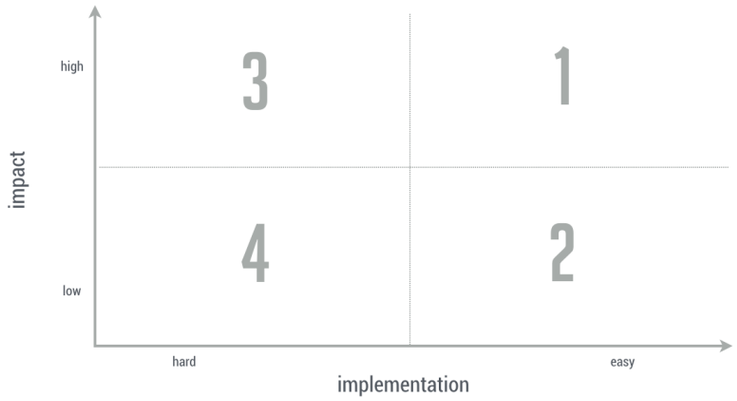
Berdasarkan hasil *assessment* mengenai kondisi *eksisting* layanan SPBE di Pemerintah Kabupaten Murung Raya, seluruh layanan SPBE telah didukung oleh pemanfaatan aplikasi informasi, hanya saja perlu adanya integrasi antar aplikasi di Pemerintah Kabupaten Murung Raya, baik integrasi dengan aplikasi internal daerah maupun dengan aplikasi instansi pusat.

1.2.6. Tata Kelola Aplikasi

Secara umum, saat ini Pemerintah Kabupaten Murung Raya membangun solusi TI dalam beberapa aplikasi yang terpisah / silo, bukan dalam satu kesatuan aplikasi. Hal ini dikarenakan usulan aplikasi biasanya terbagi berdasarkan perangkat daerah, atau berdasarkan proses bisnis yang ada. Hal ini tentunya dapat menimbulkan beberapa masalah ketika terjadi perubahan pada proses bisnis maka perlu menyesuaikan pada beberapa aplikasi terkait. Kedepan, alternatif digitalisasi proses bisnis harus dapat meminimalisir banyaknya aplikasi internal yang ada di Pemerintah Kabupaten Murung Raya. Sebagai contoh praktik terbaik yaitu adanya sebuah aplikasi layanan kepegawaian milik BKPSDM yang dapat mengakomodir berbagai kebutuhan kepegawaian, seperti: *profiling* pegawai, presensi, izin cuti-sakit, kinerja pegawai, dan lain sebagainya.

Selain itu, masifnya pembangunan aplikasi yang akan dibangun menjadi tantangan di Pemerintah Kabupaten Murung Raya. Oleh karena itu, diperlukan sebuah metode untuk menentukan prioritas aplikasi yang akan diakomodasi. Pemilihan prioritas salah satunya dapat menggunakan *matrix impact-implementation*. Cara membaca tabel prioritas yaitu dimulai dari kanan atas (aplikasi yang mudah diimplementasikan dan memiliki *impact* tinggi) ke bawah, dilanjutkan dengan aplikasi dengan implementasi dan *impact* sedang

menuju ke bagian *impact* tinggi. Aplikasi-aplikasi yang akan dibangun, baik usulan dari perangkat daerah, maupun inisiatif dari Diskominfo dipetakan dalam matriks sebagai berikut.



Gambar 1.2.6.1. *Matrix Easy Implementation*

Pengembangan aplikasi dikategorikan mudah (*easy*) jika:

1. Aplikasi telah ada/pernah digunakan di perangkat daerah lain sebelumnya;
2. Biaya pengembangan aplikasi sama dengan atau lebih kecil dari rata-rata biaya pengembangan aplikasi;
3. *Platform* aplikasi relevan dengan kualifikasi SDM TIK di Diskominfo/perangkat daerah; dan
4. Proses kerja aplikasi tidak terlalu kompleks.

Aplikasi dikategorikan memiliki *impact* yang besar (*high impact*) jika:

1. Aplikasi yang langsung dapat dirasakan manfaatnya bagi masyarakat (G2C);
2. Aplikasi diusulkan oleh lebih dari satu perangkat daerah;
3. Aplikasi dapat digunakan oleh lebih dari satu perangkat daerah; dan
4. Aplikasi pesanan langsung dari pimpinan (*strategic decision maker*).

Selain menggunakan *matrix impact-implementation* di atas, proses penentuan prioritas pengembangan aplikasi juga dilakukan dengan menggunakan strategi yang digambarkan dalam diagram sebagai berikut:

Gambar 1.2.6.2. Bagan Strategi Prioritasisasi Pengembangan Aplikasi

Aplikasi yang sifatnya mendukung pelayanan publik dan menyentuh jajaran eksekutif/pimpinan perlu diprioritaskan pengembangannya. Jika hal tersebut telah terpenuhi, prioritas selanjutnya ditujukan untuk aplikasi-aplikasi yang mengefisiensikan proses kolaborasi antar perangkat daerah. Terakhir, aplikasi yang diprioritaskan merupakan aplikasi yang sifatnya untuk kalangan bisnis dan investor. Prioritas pengembangan aplikasi tersebut mempertimbangkan kesiapan internal perangkat daerah dari sisi SDM dan anggaran, serta adanya dukungan pimpinan perangkat daerah terhadap pengembangan Layanan SPBE.

Pengembangan aplikasi dapat diinisiasi melalui berbagai kegiatan seperti: 1) penyusunan panduan integrasi antar aplikasi perangkat daerah, 2) pengembangan dan pemeliharaan *platform* integrasi aplikasi (*web services*), 3) pengembangan dan pemeliharaan *data warehouse* dan aplikasi *dashboard*, 4) pengembangan dan pemeliharaan aplikasi, dan 5) *penetration testing* aplikasi. Secara keseluruhan, kebutuhan pengembangan dan pemeliharaan aplikasi dilakukan berdasarkan perkembangan kesiapan proses bisnis.

Gambar 1.2.6.3. Inisiatif Pengembangan Aplikasi

Sebagai langkah untuk mengembangkan dan mengintegrasikan aplikasi, terdapat 4 (empat) inisiatif utama sebagai berikut:

1. Penguatan aplikasi *eksisting* untuk meningkatkan reliabilitas aplikasi dan akuntabilitas data;
2. Pengembangan *platform* integrasi berbasis layanan *(services)* guna memastikan tiap perangkat daerah memiliki rujukan untuk interoperabilitas aplikasi maupun data;
3. Kolaborasi bersama dengan inisiatif pengembangan aplikasi di perangkat daerah agar bisa dimanfaatkan pada level nasional; dan
4. Pengembangan *mobile applications* untuk menyajikan layanan publik yang transparan dan akuntabel bagi masyarakat.

1.2.6.1. Prinsip Pengembangan Aplikasi

Prinsip-prinsip pengembangan aplikasi di Pemerintah Kabupaten Murung Raya harus meliputi aspek: *Sustainable, Mobile, Agile, Reliability, Transparency* (SMART).

A. *Sustainability*

Aplikasi yang dikembangkan dapat ditingkatkan secara terus menerus (*continuous improvement*) dan berkembang menyesuaikan kebutuhan. Konsep ini dikenal dengan istilah *System Development Life Cycle* (SDLC).

B. *Mobile*

Aplikasi yang dikembangkan di Pemerintah Kabupaten Murung Raya harus dapat meningkatkan fleksibilitas pemanfaatan teknologi dan kemudahan bagi masyarakat.

C. *Agile*

Pemerintah Kabupaten Murung Raya cepat tanggap dalam merespon kebutuhan maupun permasalahan dalam implementasi SPBE.

D. *Reliability*

Aplikasi yang akan dikembangkan harus bisa diandalkan, dalam hal ketepatan proses dan ketepatan informasi.

E. *Transparency*

Aplikasi yang dikembangkan harus dapat mendukung budaya transparansi di Pemerintah Kabupaten Murung Raya agar tercipta pelayanan prima kepada masyarakat.

1.2.6.2. Pilihan Teknologi

A. Ragam Teknologi (Bahasa Pemrograman dan *Tools*)

Terdapat banyak ragam teknologi yang digunakan dalam pengembangan perangkat lunak saat ini. Beberapa di antaranya termasuk:

Gambar 1.2.6.2.1. Ragam Bahasa Pemrograman

1. Bahasa Pemrograman Umum:
   - Python
   - Java
   - C#
   - JavaScript
   - Ruby
   - Go
   - Swift
   - Kotlin
   - Rust
2. Bahasa Pemrograman untuk Aplikasi *Web*:
   - HTML
   - CSS
   - JavaScript
   - PHP
   - Ruby on Rails
   - ASP.NET

- Node.js

3. Bahasa Pemrograman untuk Aplikasi Mobile:
    - Java (untuk Android)
    - *Swift* (untuk iOS)
    - Kotlin (untuk Android)
    - *React Native* (JavaScript *framework* untuk pengembangan aplikasi mobile lintas *platform*)
4. *Relational Database Management System* (RDBMS):
    - Oracle Database
    - Microsoft SQL Server
    - MySQL/MariaDB
    - PostgreSQL.

Berdasarkan hasil survei aplikasi internal di Pemerintah Kabupaten Murung Raya menunjukkan bahwa mayoritas aplikasi merupakan berbasis *web* yang berjumlah 109 aplikasi (94%). Pemilihan *platform web* merupakan hal yang umum mengingat *platform* ini dapat diakses dari *personal* komputer maupun *smartphone* sehingga memberikan kemudahan bagi para pengguna aplikasi dalam mengakses sebuah layanan pemerintah.

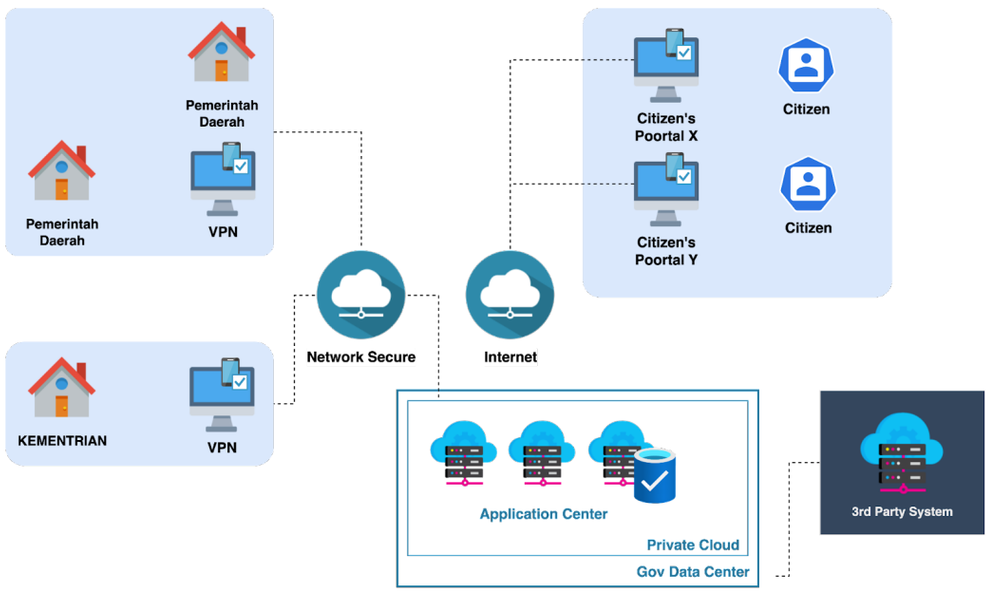
Aplikasi internal di lingkungan Pemerintah Kabupaten Murung Raya, tentunya akan terus diarahkan dan diproyeksikan menjadi sebuah aplikasi yang mampu mendukung bisnis proses dasar dan pendukung yang ada. Teknologi yang terus berkembang dapat menjawab tantangan kompleksitas bisnis proses agar lebih efisien dengan adanya otomasi. Namun dibalik pesatnya perkembangan teknologi terdapat tantangan yang dihadapi yaitu banyaknya ragam teknologi yang ada perlu didukung dengan SDM yang menguasai teknologi tersebut. Melihat kondisi riil aplikasi internal Pemerintah Kabupaten Murung Raya saat ini terhadap penggunaan teknologi yang marak digunakan dan kompetensi programmer yang ada maka perlu ditetapkan standar teknologi yang dapat digunakan di lingkungan Pemerintah Kabupaten Murung Raya.

Tabel 1.2.6.2.1. Pilihan Teknologi Pemerintah Kabupaten Murung Raya

No	Platform	Teknologi
1	*Front End Web*	HTML, CSS, Js, Vue JS
	Back End Web	PHP
2	*Front End Mobile*	Flutter, Kotlin
	Back End Mobile	PHP
3	*Desktop*	C#, Java
4	RDBMS	MySQL, PostgreSQL
5	*Interoperability*	JSON

B. Integrasi *Data dengan Platform Interoperabilitas*

WSO2 merupakan *platform* interoperabilitas berlisensi terbuka (*open source*) yang mendukung berbagai jenis layanan integrasi. WSO2 menawarkan keuntungan *platform middleware* berbasis *Service Oriented Architecture* (SOA) yang mudah untuk diintegrasikan dan mendukung layanan berbasis *cloud* serta menyediakan *helpdesk* di dalam produknya. Republik Moldova merupakan salah satu negara yang telah menerapkan WSO2 di dalam penyelenggaraan layanan pemerintah berbasis e-Government guna keperluan *identity management, authentication* dan *authorization transaction* untuk berbagai *electronic devices* dan *mobile apps*.



Gambar 1.2.6.2.2. Integrasi Data dengan Platform Interoperabilitas

Gambar di atas mengilustrasikan integrasi data dan pertukaran informasi antar perangkat daerah di dalam mengelola layanannya melalui *secure network* dan menyediakan media penyampaian informasi publik melalui portal masyarakat berdasarkan pusat data pemerintahan.

1.2.7. Tata Kelola Infrastruktur

Infrastruktur SPBE terdiri dari Pusat Data Nasional yang bertujuan untuk meningkatkan efisiensi dalam memanfaatkan sumber daya Pusat Data nasional oleh Instansi Pusat dan Pemerintah Daerah. Pusat Data Kementerian atau Lembaga dapat menjadi Pusat Data Nasional jika memenuhi SNI: 9799-1: 2019 tentang Panduan Spesifikasi Teknis Pusat Data dan SNI: 9799-2: 2019 tentang Panduan Manajemen Pusat Data. Pada Pusat Data terdapat beberapa komponen antara lain *pusat data, storage*, perangkat pendukung pusat data, dan teknologi yang digunakan untuk pengembangan aplikasi.

1.2.7.1. Pusat Data

Gambar 1.2.7.1.1. SNI No: 8799-1:2019 tentang Panduan Spesifikasi Teknis Pusat Data

A. SNI No: 8799-1:2019 tentang Panduan Spesifikasi teknis pusat data.

1. Spesifikasi gedung

   Pemilihan lokasi gedung pusat data tidak boleh terletak di wilayah rawan bencana. Referensi wilayah rawan bencana dapat mengacu pada Katalog BMKG melalui *https://cdn.bmkg.go.id/Web/Katalog-Gempabumi-Signifikan-dan-Merusak-1821-2018.pdf* serta Dokumen Risiko Bencana Indonesia (RBI) dari BNPB melalui *https://bnpb.go.id/uploads/24/buku-rbi-1.pdf.*

   - Ketahanan gempa;
   - Ketahanan beban gempa;
   - Pembagian ruangan;
   - Ketahanan material gedung; dan
   - Sistem monitoring gedung.

2. Spesifikasi sistem kelistrikan:
   - Catu daya listrik;
   - Sistem kelistrikan berkesinambungan;
   - Persediaan bahan bakar;
   - *Uninterruptible Power Supply* (UPS);
   - Analisis sistem listrik;
   - Konstruksi panel listrik;
   - Jalur kabel listrik;
   - Pembumian; dan
   - Efisiensi pemakaian listrik pada pusat data (*Power Usage Effectiveness*).

3. Spesifikasi sistem pendinginan:
   - Spesifikasi sistem jaringan data;
   - Spesifikasi sistem pemadam kebakaran;
   - Spesifikasi sistem monitoring lingkungan pusat data; dan
   - Spesifikasi sistem keamanan akses fisik.

B. SNI-No: 8799-2:2019 tentang Panduan Manajemen Pusat data.

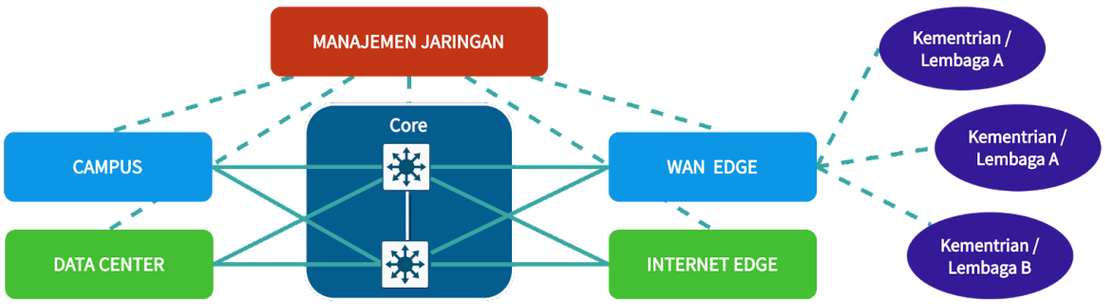
Gambar 1.2.7.1.2. SNI-No 8799-1:2019 tentang Panduan Manajemen Pusat Data

1. Perencanaan
   - Analisis kebutuhan
   - Manajemen risiko dan kesesuaian
2. Operasional
   - Organisasi penyelenggara pusat data
   - Sistem manajemen layanan operasional pusat data
   - Infrastruktur
3. Manajemen layanan
   - Sistem manajemen layanan tingkat lanjut (STML)
   - Manajemen keselamatan
   - Manajemen keamanan
   - Manajemen proyek
4. Manajemen SDM
   - Pengelolaan kompetensi
   - Pelatihan
   - Manajemen kinerja
5. *Monitoring*, pelaporan dan pengendalian
6. Manajemen keberlangsungan
   - Manajemen keberlangsungan kegiatan
   - Manajemen keberlangsungan lingkungan

C. SNI No: 8799-3:2019 beserta amandemennya tentang Panduan Audit Pusat Data
   1. Program audit.
   2. Kegiatan audit.
   3. Penyiapan, pengesahan dan penyampaian laporan audit.
   4. Kompetensi auditor.

1.2.7.2. Jaringan Intra Pemerintah

Jaringan intra pemerintah adalah jaringan yang digunakan oleh pemerintah untuk berbagi informasi dan komunikasi antar *stakeholder*. Jaringan ini umumnya tersedia untuk layanan basis data, berbagi dokumen, dan berbagi informasi dari satu perangkat daerah ke perangkat daerah lainnya. Jaringan intra pemerintah juga dapat digunakan untuk mengatur akses ke layanan administratif, seperti akses ke layanan kesehatan, pendidikan, dan keuangan.

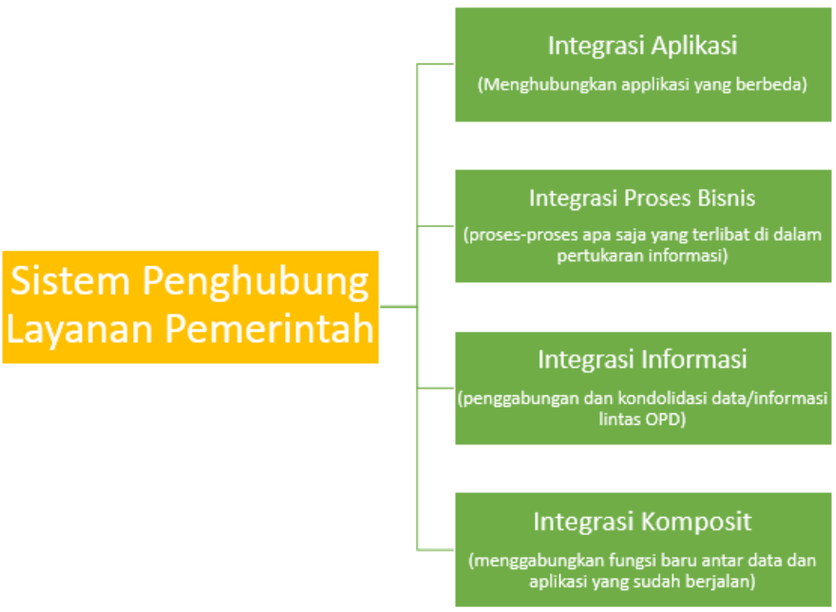


Gambar 1.2.7.2.1. Arsitektur Jaringan Intra Pemerintah Kabupaten Murung Raya

Dari gambar arsitektur di atas diperoleh informasi bahwa untuk koneksi jaringan intra pemerintah antara jaringan Pemerintah Kabupaten Murung Raya dengan Kementerian/Lembaga Negara/Pemerintah Daerah Provinsi, Kota/Kabupaten melalui *WAN Edge* dengan menggunakan koneksi yang aman dan terenkripsi. *WAN Edge* di dukung oleh perangkat *router WAN* dan *Next-Generation Firewall WAN.*

1.2.7.3. Sistem Penghubung Layanan Pemerintah

Sistem penghubung layanan pemerintah adalah sistem yang menyediakan akses ke berbagai layanan pemerintah dari satu tempat. Sistem ini dapat berupa portal layanan pemerintah atau antarmuka berbasis *web* yang dapat digunakan untuk mengakses berbagai layanan pemerintah, seperti pelayanan fiskal, sosial, pengawasan, dan lainnya. Sistem ini menyediakan berbagai fitur seperti verifikasi, pelaporan, dan pemantauan untuk memastikan bahwa layanan yang ditawarkan oleh pemerintah dapat diakses oleh masyarakat,

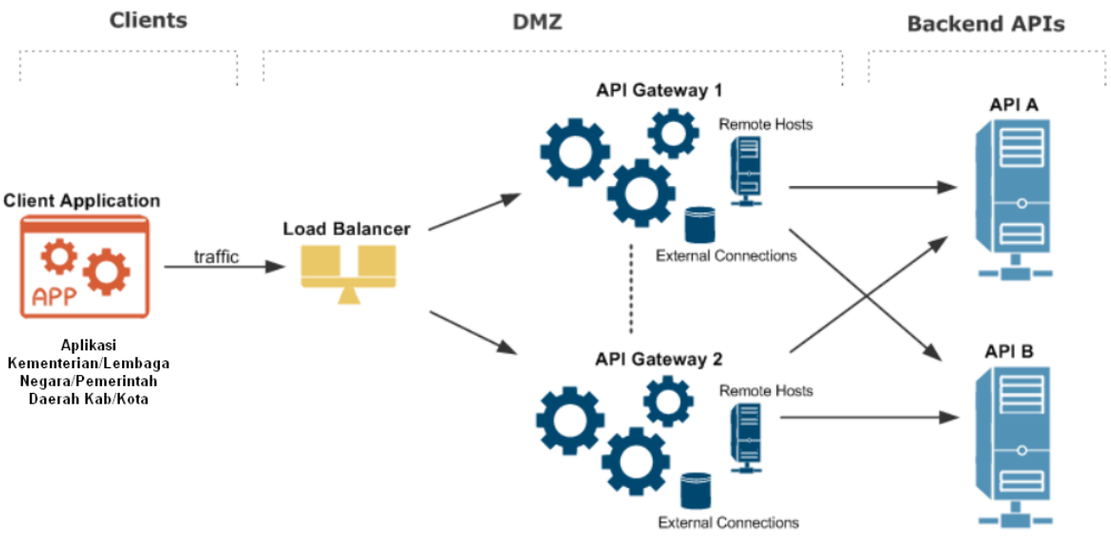


Gambar 1.2.7.3.1. Sistem Penghubung Layanan Pemerintah

A. *Application Programming Interface (API)*

API adalah sekumpulan kode pemrograman yang membantu *developer* melakukan integrasi data antara dua aplikasi berbeda secara bersamaan. API memungkinkan developer untuk membuat aplikasi dengan berbagai elemen seperti

function, protocols dan *tools* lain. API dapat digunakan untuk berkomunikasi dengan berbagai bahasa pemrograman.



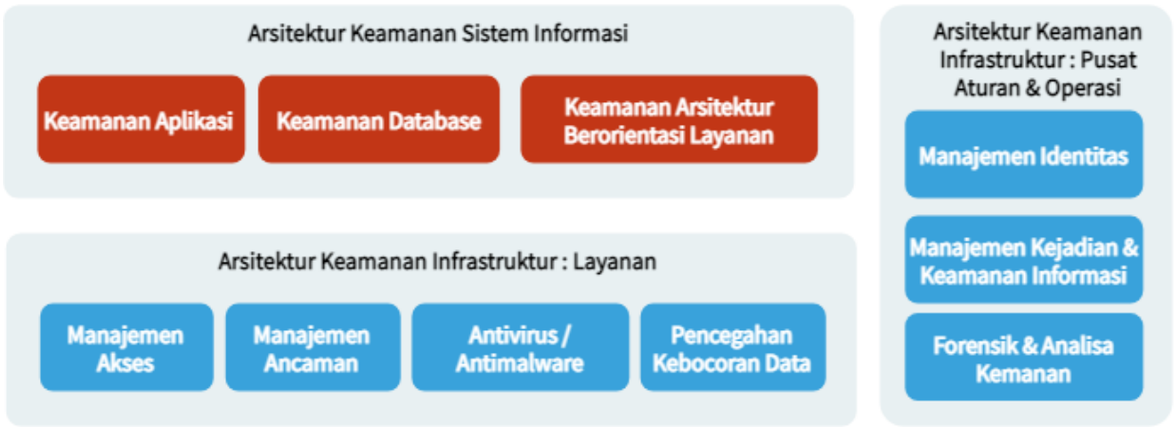
Gambar 1.2.7.3.2. Arsitektur API *Gateway* dengan konfigurasi *High Availability*

Berikut ini adalah penjelasan dari gambar Arsitektur API *Gateway* diatas dengan *konfigurasi High Availability* (HA) sebagai berikut.

1. Aplikasi klien eksternal membuat panggilan masuk melalui protokol pengangkutan pesan tertentu (misalnya, *HTTP, JMS*, atau *FTP*) ke penyeimbang beban.
2. Penyeimbang beban melakukan pemeriksaan pada setiap *instance* API *Gateway*, dan mendistribusikan beban pesan ke *port* di setiap instance API *Gateway* (*default*-nya adalah 8080).
3. Setiap *instance* API *Gateway* harus memiliki Koneksi Eksternal ke sistem pihak ketiga. Termasuk *database* seperti *Oracle* dan *MySQL*, dan *Authentication Repositories seperti CA SiteMinder, Oracle Access Manager, pusat data Local Directory Access Protocol (LDAP)*, dan sebagainya.
4. Setiap *instance* API *Gateway* direplikasi menggunakan sistem *caching* berdasarkan Ehcache.
5. Setiap *instance* API *Gateway* memiliki antarmuka *Host* Jarak Jauh yang menentukan koneksi keluar sistem API *backend*.
6. Setiap *instance* API *Gateway* berisi *database Apache Cassandra* yang disematkan dan digunakan oleh fitur-fitur tertentu untuk penyimpanan data persisten, dimana setiap *instance* API *Gateway* memiliki kemampuan HA-nya sendiri.
7. Setiap *instance* API *Gateway* berisi sistem pesan *Apache ActiveMQ* tertanam, yang dapat dikonfigurasi untuk HA dalam sistem file bersama.
8. Setiap API *backend* juga direplikasi untuk memastikan tidak ada kegagalan di tingkat pusat data.

9. *Traffic* manajemen yang digunakan oleh *Admin Node Manager, API Gateway Manager,* dan *Policy Studio* ditangani secara terpisah di *port* yang berbeda (*default* 8090).

1.2.8. Tata Kelola Keamanan



Gambar 1.2.8.1 Keamanan SPBE

Tata Kelola Keamanan SPBE terdapat beberapa komponen yang mencakup didalamnya, seperti Arsitektur Keamanan Sistem Informasi yang terdiri atas keamanan aplikasi, keamanan *database,* dan keamanan arsitektur berorientasi layanan. Selain itu, juga terdapat arsitektur keamanan infrastruktur: layanan yang didalamnya mencakup manajemen akses, manajemen ancaman, antivirus/antimalware dan pencegahan kebocoran data.

1.2.8.1. Arsitektur Keamanan Sistem Informasi

Terdiri dari keamanan aplikasi, keamanan *database*, dan keamanan arsitektur berorientasi layanan. Setiap data dan informasi yang dikelola oleh satuan kerja wajib dilakukan *backup* secara terpusat dan berkala sesuai dengan frekuensi dan tingkat keamanan data dan informasi. Pusat Data dan Informasi melakukan pengujian secara teratur terhadap mekanisme *backup* dan *restore* data dan informasi untuk memastikan integritas dan validitas prosedur. Tata cara *backup* dan *restore* data dan informasi telah tertuang dalam SOP dan ditetapkan. Kepastian keamanan data dan informasi, perlu dilakukan manajemen keamanan informasi melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE. Manajemen keamanan informasi dilaksanakan berdasarkan pedoman manajemen keamanan informasi SPBE yang ditetapkan oleh Badan Siber Sandi Negara.

1.2.8.2. Arsitektur Keamanan Infrastruktur Layanan

Meliputi manajemen akses, manajemen ancaman, antivirus/anti malware, dan pencegah kebocoran data. Dalam memastikan keamanan Infrastruktur SPBE, dilakukan audit keamanan Infrastruktur SPBE. Audit keamanan Infrastruktur SPBE dilaksanakan minimal 1 kali dalam setahun dengan berdasarkan standar dan tata cara pelaksanaan audit keamanan infrastruktur SPBE yang ditetapkan oleh Badan Siber Sandi Negara.

1.2.8.3. Arsitektur Keamanan Infrastruktur: Aturan Pusat dan Operasi

Terdiri dari manajemen identitas, manajemen kejadian dan keamanan informasi, dan forensik dan analisa keamanan. Pelaksanaan terhadap Keamanan SPBE mencakup:

1. Penjaminan kerahasiaan.
2. Penjaminan keutuhan.
3. Penjaminan ketersediaan.
4. Penjaminan kenirsangkalan.

Penjaminan kerahasiaan dilakukan melalui penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan lainnya. Penjaminan keutuhan dilakukan melalui pendeteksian modifikasi. Penjaminan ketersediaan dilakukan melalui penyediaan mekanisme verifikasi dan validasi. Penjaminan kenirsangkalan dilakukan melalui penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.

1.3. Manajemen SPBE

Perlu adanya manajemen dalam implementasi SPBE dan mengakomodir proses operasional SPBE yang mengacu dari Perpres 95/2018. Secara keseluruhan dalam manajemen SPBE terdapat beberapa lingkup yang diuraikan sebagai berikut :

Tabel 1.3.1. Lingkup Manajemen SPBE

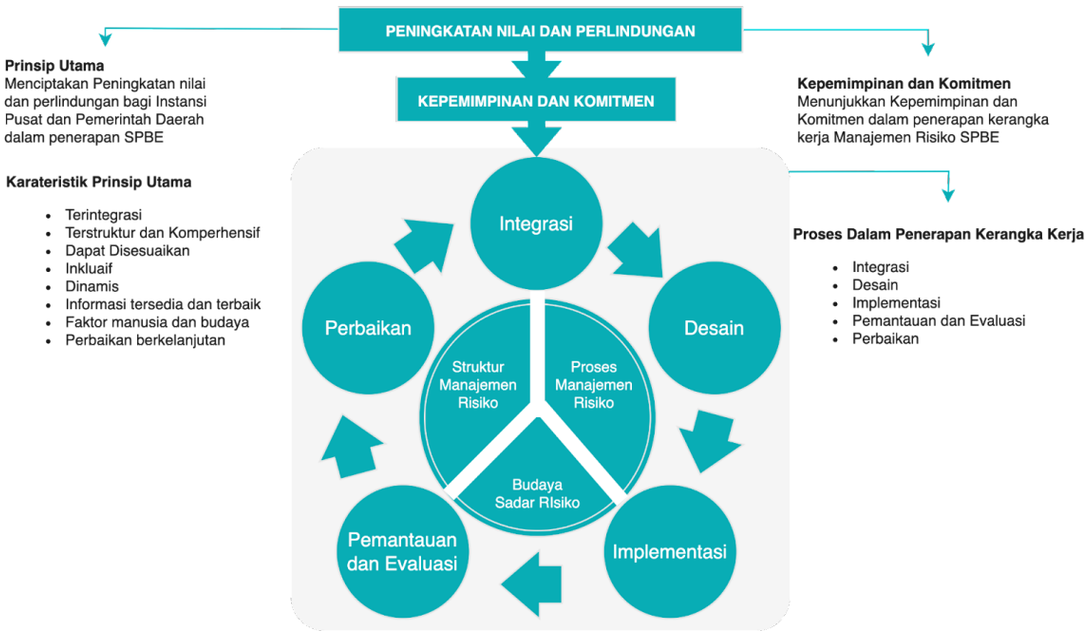
No	Lingkup	Referensi	Kegiatan	Penanggung Jawab
a.	Manajemen Risiko	PermenpanRB 05/2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik, International Standardization Organization (ISO) 31000 tentang *Risk Management*, 27005 tentang I*nformation technology– Security techniques – Information security risk management*	1. Pembentukan komite manajemen risiko 2. Penyusunan dan penetapan kebijakan manajemen risiko SPBE 3. Penyusunan pedoman manajemen risiko SPBE yang berisi kerangka manajemen risiko SPBE, proses manajemen risiko SPBE, struktur manajemen risiko SPBE, budaya risiko SPBE 4. Penyusunan dan pelaksanaan rencana program dan kegiatan pelaksanaan manajemen risiko 5. Pelaksanaan sosialisasi, pelatihan, bimbingan, dan supervisi risiko SPBE oleh inspektorat 6. Penerapan manajemen risiko melalui komunikasi dan konsultasi melalui rapat berkala, rapat insidental, fgd 7. Penetapan konteks risiko SPBE 8. Penyusunan identifikasi risiko SPBE dengan menguraikan jenis risiko SPBE, penyebab, kategori, dampak, dan area dampak 9. Penyusunan analisis risiko SPBE dengan menguraikan kemungkinan dan dampak yang ditimbulkan seta level risiko SPBE & penyusunan evaluasi risiko SPBE 10. Penyusunan rencana penanganan risiko SPBE dengan menguraikan opsi, rencana aksi penanganan risiko, output, jadwal implementasi, dan penanggung jawabnya 11. Penyusunan laporan evaluasi manajemen risiko SPBE secara periodik dan insidental	Inspektorat dan Dinas Komunikasi, Informatika, Statistik dan Persandian
b.	Manajemen Keamanan Informasi	ISO 27001 tentang Sistem Manajemen Keamanan Informasi, Indeks Keamanan Informasi (KAMI)	1. Pembentukan tim keamanan informasi 2. Penyusunan SOP keamanan informasi mengacu pada Peraturan BSSN No. 4 Tahun 2021 3. Membuat postingan keamanan informasi pada media informasi 4. Pelaksanaan sosialisasi, pelatihan, bimbingan, dan supervisi keamanan SPBE 5. Evaluasi dan perbaikan manajemen keamanan informasi	Dinas Komunikasi, Informatika, Statistik dan Persandian
c.	Manajemen Data	Perpres 39/2019 tentang Satu Data Indonesia, Permen PPN 16/2020 tentang Manajemen Data Sistem Pemerintahan Berbasis Elektronik, SNI 8799:2019	1. Pembentukan tim satu data 2. Penyusunan pedoman manajemen data 3. Pembaharuan arsitektur data 4. Pengumpulan data sektoral di masing-masing unit kerja 5. Pemeriksaan pemenuhan data sektoral 6. Penyebarluasan data sektoral 7. Pembaruan data sektoral secara berkala 8. Penyimpanan data pada portal open data	Dinas Komunikasi, Informatika, Statistik dan Persandian dan Badan Perencanaan Pembangunan Daerah dan

No	Lingkup	Referensi	Kegiatan	Penanggung Jawab
		tentang Pusat Data, International Standardization Organization (ISO) 11179 tentang *Metadata Registry*	9. Penjaminan kualitas data meliputi daftar data, data prioritas, dan jadwal pemutakhiran data	Penelitian Pengembangan
d.	Manajemen Aset TIK	International Standardization Organization (ISO) 19770-5 tentang Sistem Manajemen Aset TIK	1. Menginventarisasi aset SPBE (aplikasi dan infrastruktur) 2. Penyusunan SOP perencanaan aset TIK 3. Penyusunan SOP pengadaan aset TIK 4. Penyusunan SOP atas penghapusan aset TIK 5. Evaluasi dan perbaikan manajemen aset TIK	Dinas Komunikasi, Informatika, Statistik dan Persandian
e.	Manajemen SDM	PermenPANRB 38/2017 tentang Standar Kompetensi Jabatan Aparatur Sipil Negara, *Skills Framework for the Information Age* (SFIA) *Framework*, ISO 30400 tentang *Human Resource Management*	1. Analisis jabatan dan analisis beban kerja terhadap jabatan TIK 2. Analisis kebutuhan pelatihan bagi SDM TIK 3. Evaluasi pelaksanaan pengembangan kompetensi SDM TIK	Bagian Organisasi, Badan Kepegawaian dan Sumber Daya Manusia, dan Dinas Komunikasi, Informatika, Statistik dan Persandian
f.	Manajemen Pengetahuan	International Standardization Organization (ISO) 30401 tentang *Knowledge Management System*	1. Pembentukan komite manajemen pengetahuan 2. Penyusunan pedoman manajemen pengetahuan (kebijakan dan SOP manajemen pengetahuan) 3. Pelaksanaan manajemen pengetahuan dengan aplikasi 4. Evaluasi dan perbaikan manajemen pengetahuan	Dinas Komunikasi, Informatika, Statistik dan Persandian
g.	Manajemen Perubahan	*Change Management* (ITIL) COBIT 2019	1. Pembentukan komite manajemen perubahan 2. Penyusunan pedoman / SOP manajemen perubahan SPBE 3. Penyusunan form log manajemen perubahan 4. Pelaksanaan manajemen perubahan SPBE 5. Evaluasi dan perbaikan manajemen perubahan	Dinas Komunikasi, Informatika, Statistik dan Persandian dan Bagian Organisasi
h.	Manajemen Layanan	*Information Technology Infrastructure Library* (ITIL)	1. Pembentukan tim helpdesk TIK 2. Pengembangan aplikasi ticketing layanan TIK 3. Evaluasi & perbaikan kinerja tim helpdesk TIK	Dinas Komunikasi, Informatika, Statistik dan Persandian

1.3.1. Manajemen Risiko SPBE

Manajemen Risiko SPBE merupakan sebuah langkah strategis dalam rangka membangun pondasi kebijakan manajemen SPBE yang digunakan sebagai acuan pelaksanaan manajemen risiko SPBE pada instansi pemerintah. Manajemen risiko SPBE mengidentifikasi, memahami, mengukur, mengelola, dan memantau risiko yang dihadapi dalam implementasi SPBE. Selain itu, dalam manajemen risiko juga dilakukan untuk

mengidentifikasi risiko yang mungkin terjadi, menilai tingkat risiko, mencari cara untuk mengurangi risiko, serta mengawasi risiko secara terus-menerus untuk memastikan bahwa kegiatan yang dilakukan sudah sesuai. Agar proses dan pengukuran dalam Manajemen Risiko SPBE dapat dilaksanakan dengan baik, maka diperlukan tata kelola Manajemen Risiko SPBE yang mengatur tugas dan tanggung jawab dari struktur Manajememen Risiko SPBE.



Gambar 1.3.1.1. Manajemen Risiko SPBE

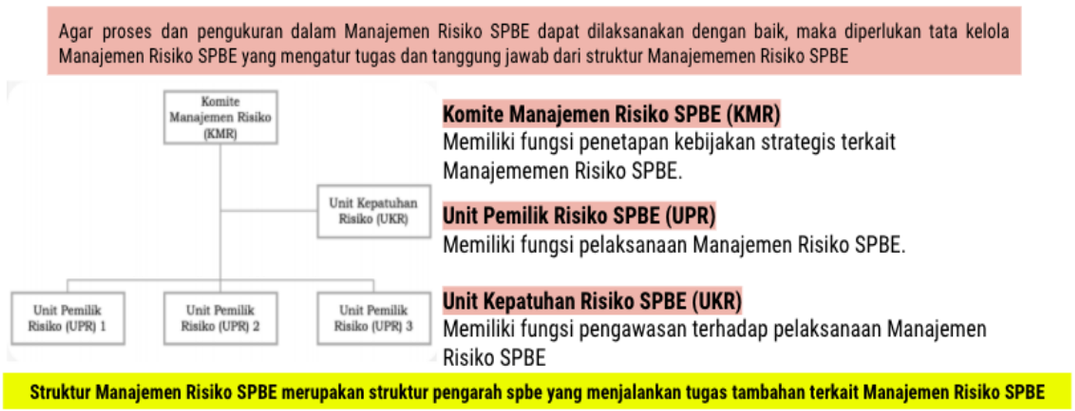
Manajemen risiko saat ini telah menjadi rujukan utama dalam penerapan sistem pemerintahan berbasis elektronik. Hal ini bisa berupa upaya dalam mengidentifikasi, menilai, dan mengurangi risiko terkait SPBE secara terus-menerus dalam tingkat toleransi yang ditetapkan oleh Kepala Daerah. Mengacu pada Permen PAN RB 05/2020 tentang pedoman Manajemen Risiko SPBE, tujuan dari Manajemen Risiko SPBE adalah :

1. Meningkatkan kemungkinan pencapaian tujuan penerapan SPBE di Pemerintah Daerah.
2. Memberikan dasar yang kuat untuk perencanaan dan pengambilan keputusan melalui penyajian informasi Risiko SPBE yang memadai di Pemerintah Daerah dalam penerapan SPBE.
3. Meningkatkan optimalisasi pemanfaatan sumber daya SPBE di Instansi Pemerintah Daerah dalam penerapan SPBE.
4. Meningkatkan kepatuhan kepada peraturan dalam penerapan SPBE.
5. Menciptakan budaya sadar Risiko SPBE bagi pegawai ASN di lingkungan Pemerintah Daerah dalam penerapan SPBE.

Manfaat dari penerapan Manajemen Risiko SPBE dalam penerapan SPBE adalah :

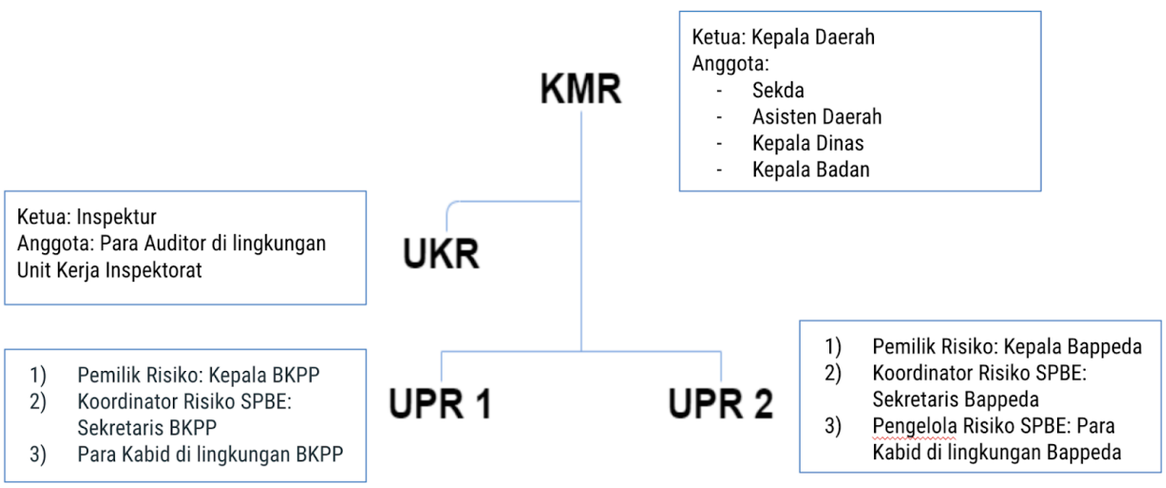
1. Mewujudkan tata kelola pemerintahan yang efektif, efisien, transparan, dan akuntabel melalui penerapan SPBE di Instansi Pemerintah Daerah.
2. Mewujudkan penerapan SPBE yang terpadu di Instansi Pemerintah Daerah.
3. Meningkatkan kinerja pemerintahan di Instansi Pemerintah Daerah.
4. Meningkatkan reputasi dan kepercayaan pemangku kepentingan kepada Pemerintah Daerah.
5. Mewujudkan budaya kerja yang profesional dan berintegritas di Pemerintah Daerah.

Dalam menerapkan Manajemen Risiko SPBE, Pemerintah Kabupaten Murung Raya perlu menyusun struktur manajemen risiko SPBE sebagaimana yang telah tertuang dalam PermenpanRB No. 05/2020 dan dijelaskan sebagai berikut :



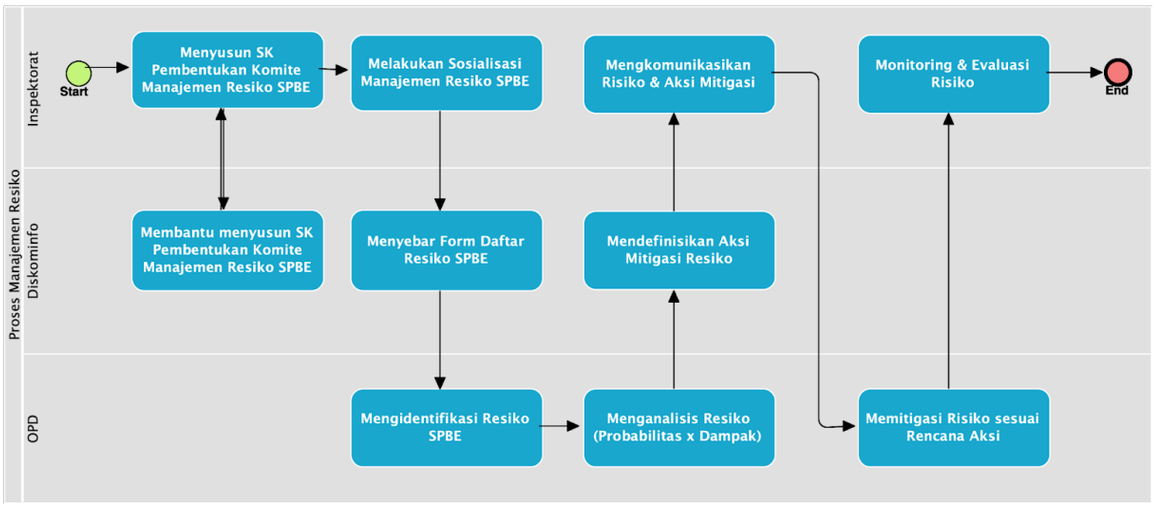
Gambar 1.3.1.2. Pedoman Struktur Manajemen Risiko SPBE Daerah

Mengacu pada gambar di atas maka susunan untuk struktur manajemen risiko SPBE di Pemerintah Kabupaten Murung Raya dijelaskan sebagai berikut :



Gambar 1.3.1.3. Struktur Manajemen Risiko SPBE Pemerintah Kabupaten Murung Raya

Merujuk pada *best practices* yang ada dalam PermenpanRB 05/2020 terdapat beberapa aktivitas yang dapat dilakukan oleh pemerintah daerah dalam upaya menjalankan manajemen risiko SPBE yang dijelaskan sebagai berikut :



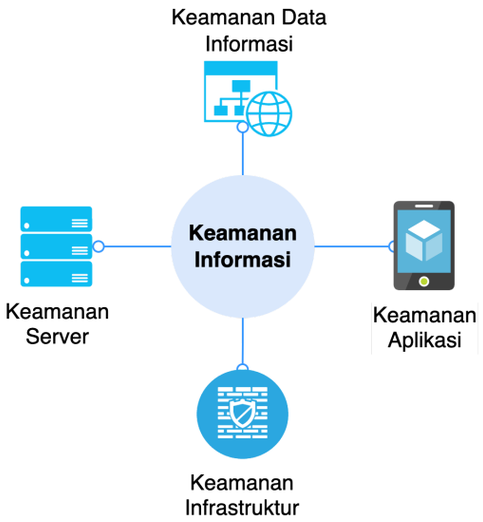
Gambar 1.3.1.4. Alur Proses Manajemen Risiko SPBE

Secara teknis pemerintah daerah perlu menyusun SOP dan dokumen terkait manajemen risiko dengan lingkup sebagai berikut :

1. SOP Manajemen Risiko SPBE oleh setiap perangkat daerah; dan
2. Kajian Manajemen Risiko.

1.3.2. Manajemen Keamanan Informasi

Manajemen keamanan informasi merupakan kegiatan pengelolaan yang menyediakan pelindungan keamanan informasi pada SPBE. Manajemen keamanan informasi termasuk dalam identifikasi, penetapan, implementasi, dan pemeliharaan kontrol dan prosedur keamanan yang menyediakan perlindungan terhadap penggunaan, distribusi, dan perlindungan informasi yang tersimpan dalam SPBE. Secara umum, ruang lingkup dalam manajemen keamanan informasi meliputi: data/informasi SPBE, aplikasi SPBE, infrastruktur SPBE, dan jaringan SPBE di setiap instansi pemerintah.



Gambar 1.3.2.1. Domain Keamanan Informasi

Secara umum terdapat empat domain keamanan SPBE yaitu :

1. Keamanan Data/Informasi

   Keamanan data atau informasi adalah proses memastikan bahwa data atau informasi yang disimpan, diproses, atau ditransmisikan melalui sistem informasi dapat diakses, dirahasiakan, dan digunakan hanya oleh orang-orang yang berwenang. Tujuannya adalah untuk melindungi data atau informasi dari ancaman keamanan seperti kebocoran, peningkatan, pencurian, dan sabotase. Ini bisa dilakukan dengan berbagai cara termasuk penyimpanan data, enkripsi data dan akses yang diatur.

2. Keamanan Aplikasi

   Seperangkat prinsip, standar, prosedur, dan operasi yang digunakan untuk melindungi data dan informasi pada aplikasi dari ancaman keamanan. Kontrol keamanan aplikasi bertujuan untuk mencegah atau mereduksi risiko. Secara umum, kontrol keamanan aplikasi, meliputi: enkripsi data, *authentication*, *authorization*, *access control*, *logging* & *monitoring*, *and code review & testing.*

3. Keamanan Jaringan

   Suatu proses yang dimaksudkan untuk melindungi jaringan komputer dari serangan yang berbahaya dengan mengatur akses ke sistem informasi dan jaringan komputer. Secara umum, *software* keamanan jaringan digunakan untuk melakukan autentikasi *user* dan pengguna yang akan mengakses jaringan melalui sistem enkripsi.

4. Keamanan Infrastruktur

   Keamanan infrastruktur mengacu pada *best practices* COBIT 2019. Berikut aktivitas-aktivitas yang perlu dilakukan dalam manajemen keamanan informasi yaitu:

   a. Menentukan ruang lingkup dan batas-batas manajemen keamanan informasi dalam hal karakteristik organisasi, lokasi, aset dan teknologi.
   b. Menetapkan manajemen keamanan informasi sesuai dengan kebijakan instansi dan konteks dimana instansi beroperasi.
   c. Menyelaraskan manajemen keamanan informasi dengan pendekatan organisasional secara keseluruhan pada manajemen keamanan.

d. Mendapatkan otorisasi dari pejabat struktural untuk menerapkan dan mengoperasikan atau mengubah manajemen keamanan informasi.
e. Mempersiapkan dan memelihara pernyataan penerapan yang menggambarkan ruang lingkup manajemen keamanan informasi.
f. Menetapkan serta mengkomunikasikan peran dan tanggung jawab pengelola keamanan informasi.
g. Mengkomunikasikan pendekatan manajemen keamanan informasi.

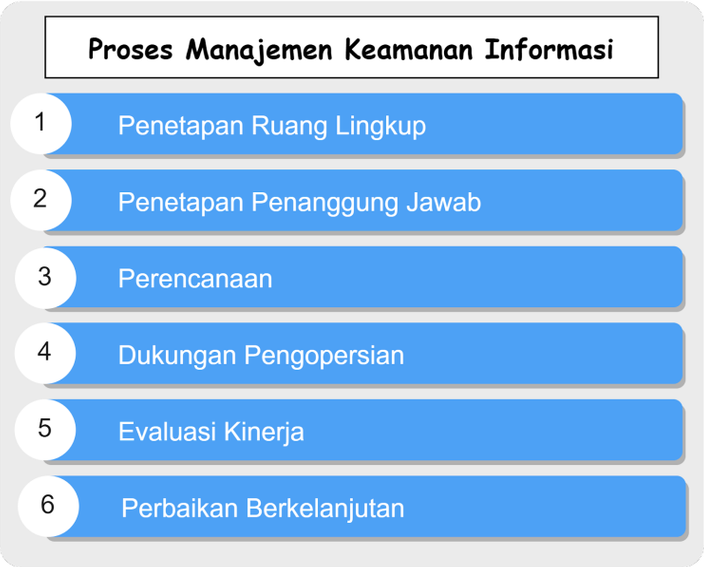
1.3.2.1. Urgensi Keamanan

Gambar 1.3.2.1.1. Manajemen Keamanan Informasi

Setiap instansi pemerintahan baik pusat maupun daerah diwajibkan menyelenggarakan SPBE. Transformasi digital pada setiap layanan menjadi salah satu bentuk penerapan SPBE oleh pemerintah. Namun demikian, penyelenggaraan SPBE tidak terlepas dari berbagai tantangan baru salah satunya pada keamanan informasi. Beberapa masalah yang muncul dalam keamanan informasi antara lain: tingginya risiko penyerangan siber dan minimnya penerapan keamanan SPBE yang didasari pada rendahnya kemampuan SDM pemerintah dalam menangani keamanan informasi SPBE. Berdasarkan kondisi yang ada, BSSN menyusun strategi dan menetapkan kebijakan manajemen serta standar teknis terkait keamanan SPBE agar dapat menjadi panduan dan acuan instansi pemerintah dalam mengimplementasikan keamanan SPBE. Dengan adanya kebijakan manajemen keamanan SPBE menjadikan teknologi yang digunakan lebih aman serta selaras dengan proses bisnis sesuai dengan persyaratan tugas pekerjaan.

1.3.2.2. Manajemen Keamanan SPBE

Dalam Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, terdapat pedoman dalam melakukan manajemen keamanan informasi SPBE. Manajemen keamanan informasi SPBE dilakukan oleh instansi pusat dan daerah. Adapun proses manajemen keamanan informasi meliputi:



Gambar 1.3.2.2.1. Proses Manajemen Keamanan Informasi

1. Penetapan ruang lingkup

   Penetapan ruang lingkup manajemen keamanan SPBE dilakukan oleh setiap pimpinan instansi pusat atau Kepala Daerah. Dalam menetapkan ruang lingkup keamanan *cyber* dapat dilakukan berdasarkan 2 hal yaitu isu internal keamanan informasi SPBE dalam organisasi dan isu eksternal keamanan informasi SPBE. Isu internal keamanan informasi SPBE adalah area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE. Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE setidaknya meliputi:

   - Data dan informasi SPBE;
   - Aplikasi SPBE;
   - Aset Infrastruktur SPBE; dan
   - Kebijakan keamanan informasi SPBE yang telah dimiliki.

   Sedangkan isu eksternal menyesuaikan dengan ketentuan peraturan perundang-undangan.

2. Penetapan penanggung jawab

   Penetapan penanggung jawab pada manajemen keamanan SPBE dilakukan oleh kepala daerah. Penanggung jawab Kelompok Kerja Manajemen Keamanan Informasi dalam Tim Koordinasi SPBE adalah Sekretaris Daerah. Dalam pelaksanaannya, Kelompok Kerja Manajemen keamanan informasi akan menetapkan pelaksana teknis keamanan SPBE yang terdiri dari:

   a. Pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan Informasi ~~TIK~~; dan
   b. Pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE.

3. Perencanaan

   Perencanaan dalam manajemen keamanan SPBE dilakukan oleh pelaksana teknis keamanan SPBE. Tahap perencanaan terdiri dari dua bagian yaitu program kerja

keamanan SPBE dan target realisasi program kerja keamanan SPBE. Adapun program kerja yang dilakukan meliputi:

a. Edukasi Kesadaran Keamanan SPBE

Gambar 1.3.2.2.2. Contoh Sosialisasi dan Pelatihan

Gambar 1.2.2.4. merupakan salah satu contoh dari sosialisasi atau *spread awareness* yang dilakukan di pemda lain sebagai bentuk dari manajemen keamanan informasi melalui berbagai kegiatan seperti: informasi tips menghindari serangan *man in the middle attack* di *wifi public* dan tips menghindari penipuan atau *scam* melalui sosial media.

b. Pengukuran Nilai Kerentanan Keamanan SPBE.

Adapun tahapan pengukuran nilai kerentanan keamanan SPBE dapat dilakukan dengan cara:

- Menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
- Mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
- Mengukur tingkat risiko Keamanan SPBE.

c. Peningkatan Keamanan SPBE

Adapun upaya dalam peningkatan keamanan SPBE dapat dilakukan dengan cara:

- Menerapkan standar teknis dan prosedur Keamanan SPBE; dan
- Menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE

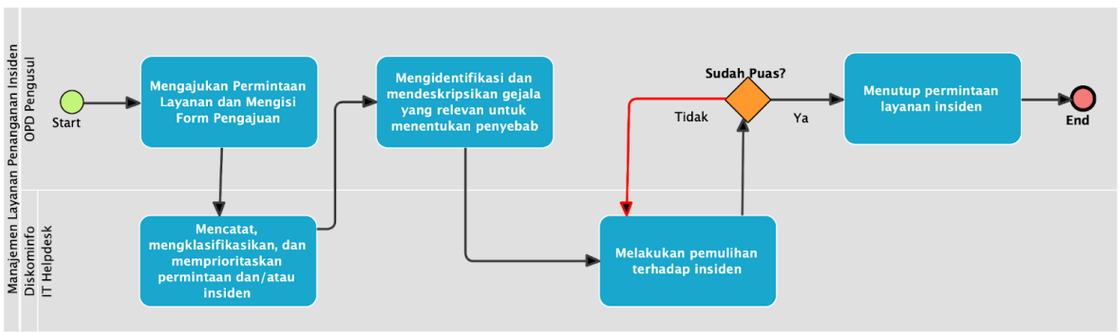
Secara teknis pemerintah daerah perlu menyusun kebijakan/SOP terkait manajemen keamanan informasi dengan lingkup sebagai berikut:

1. SOP Akses Ruang pusat data.
2. SOP Backup dan Restore Data.

3. SOP Hak Akses TIK.
4. SOP Penanganan Gangguan TIK.
5. SOP Pengajuan Jaringan Baru.
6. SOP Pengembangan Sistem Informasi.
7. SOP Penitipan dan Pengembalian pusat data.
8. SOP Evaluasi Keamanan SPBE.

d. Penanganan Insiden Keamanan SPBE

1. Mengidentifikasi sumber serangan;
2. Menganalisis informasi yang berkaitan dengan insiden selanjutnya;
3. Memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
4. Mendokumentasi bukti insiden yang terjadi; dan
5. Memitigasi atau mengurangi dampak risiko Keamanan SPBE.



Gambar 1.3.2.2.3. Alur Proses Penanganan Insiden SPBE

e. Audit Keamanan SPBE.

Audit keamanan SPBE perlu dilakukan 2 tahun sekali sesuai dengan Peraturan Badan Siber dan Sandi Negara nomor 4 tahun 2021 tentang manajemen keamanan informasi, sedangkan untuk target realisasi program kerja ditetapkan oleh masing-masing instansi.

4. Dukungan Pengoperasian

Dukungan pengoperasian dalam kelompok kerja manajemen keamanan informasi harus menyediakan SDM yang berkompeten dan anggaran keamanan SPBE. Kelompok kerja manajemen keamanan informasi harus menyediakan SDM keamanan SPBE yang memiliki kompetensi dalam bidang infrastruktur TIK dan juga keamanan aplikasi. Diperlukan pelatihan atau bimtek untuk SDM yang belum kompeten. Selain itu, anggaran keamanan SPBE yang akan disediakan harus didasarkan pada perencanaan yang telah disusun.

5. Evaluasi Kinerja

Evaluasi dilakukan paling sedikit satu kali dalam setahun oleh kelompok kerja manajemen keamanan informasi. Evaluasi kinerja keamanan SPBE dapat mencakup hal-hal berikut ini.

a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan SPBE;

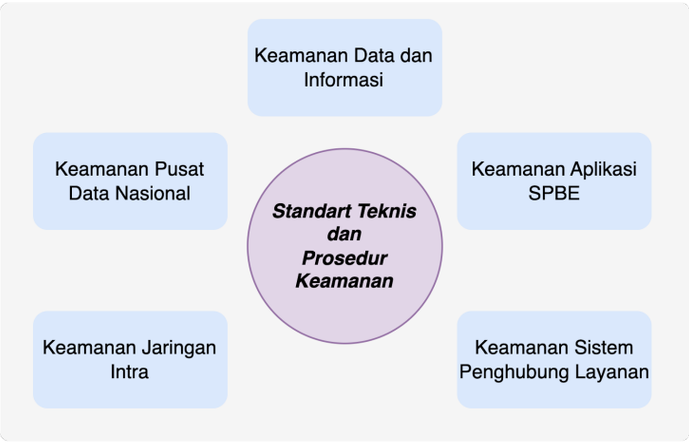
b. menetapkan indikator kinerja pada setiap area proses;
c. memformulasi pelaksanaan keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
d. menganalisis efektifitas pelaksanaan keamanan SPBE; dan
e. mendukung dan merealisasikan program audit keamanan SPBE.

6. Perbaikan Berkelanjutan

Perbaikan berkelanjutan dilakukan oleh pelaksana teknis keamanan SPBE. Perbaikan berkelanjutan merupakan bentuk tindak lanjut dari hasil evaluasi kinerja. Perbaikan berkelanjutan mencakup:

a. solusi permasalahan dalam pelaksanaan keamanan SPBE; dan
b. Perbaikan pelaksanaan keamanan SPBE secara periodik.

Setiap instansi pemerintahan baik Instansi Pusat maupun Instansi Daerah berkewajiban untuk menyelenggarakan SPBE termasuk didalamnya dalam hal keamanan informasi. Dalam penerapannya, keamanan SPBE juga harus memenuhi standar teknis dan prosedur keamanan SPBE yang diatur melalui Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.



Gambar 1.3.2.2.4. Standar Teknis dan prosedur keamanan

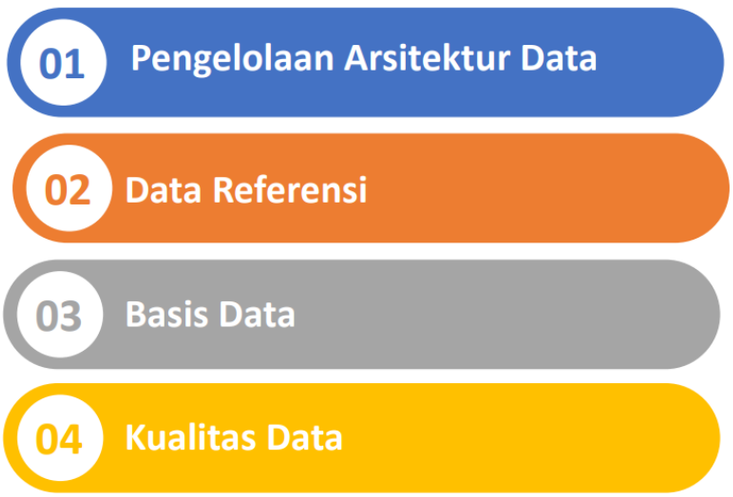
1.3.3. Manajemen Data

Manajemen data merupakan serangkaian proses pengelolaan arsitektur data, data induk, data referensi, basis data, kualitas data dan interoperabilitas data. Manajemen data SPBE memungkinkan pemerintah untuk menyimpan, menganalisis, dan memanfaatkan data sehingga memudahkan pemerintah untuk mengakses dan mengelola data secara efektif, serta untuk meningkatkan transparansi dan akuntabilitas. Manajemen data SPBE bertujuan untuk menjamin terwujudnya data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan nasional. Adapun sasaran manajemen data SPBE bagi instansi pusat maupun pemerintah daerah yaitu :

1. memahami kebutuhan data;
2. mendapatkan, menyimpan, melindungi, dan memastikan integritas data;
3. meningkatkan kualitas data secara terus menerus; dan
4. memaksimalkan penggunaan data dan memberikan hasil yang efektif.

Tujuan Satu Data Indonesia untuk mewujudkan ketersediaan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan menjadi dasar dalam perencanaan, pelaksanaan, evaluasi, dan pengendalian manajemen data SPBE. Secara umum, penyelenggaraan Satu Data Indonesia merupakan bagian dari penyelenggaraan manajemen data SPBE. Hal tersebut tertuang dalam Permen PPN Nomor 18 Tahun 2020 tentang Tata Kerja Penyelenggaraan Satu Data Tingkat Pusat.

Menurut Permen PPN Nomor 18 Tahun 2020 tentang Tata Kerja Penyelenggaraan Satu Data Tingkat Pusat, terdapat empat komponen utama yang harus dilakukan dalam melakukan manajemen data khususnya manajemen data SPBE. Komponen tersebut adalah manajemen arsitektur data, manajemen data induk dan data referensi, manajemen basis data, dan manajemen kualitas data.



Gambar 1.3.3.1. Manajemen Basis Data

1. Manajemen arsitektur data

Arsitektur data didefinisikan sebagai model yang mengatur dan menentukan jenis data yang dikumpulkan, disimpan, dikelola, dan diintegrasikan dalam SPBE. Sedangkan, manajemen arsitektur data merupakan rangkaian proses untuk menetapkan dan menyebarluaskan komponen arsitektur data. Manajemen arsitektur data memungkinkan pemerintah untuk membangun dan mengelola data untuk mengakses informasi, serta mengintegrasikan data dan informasi antar aplikasi yang diperlukan untuk menyediakan layanan yang bermanfaat bagi warga. Selain itu, manajemen arsitektur data juga bermanfaat dalam mengelola pemeliharaan dan peningkatan serta keamanan data.

Arsitektur data sangat penting untuk manajemen data. Data pemerintahan perlu direpresentasikan pada tingkat abstraksi yang berbeda sehingga mudah dipahami dan dapat digunakan dalam pengambilan keputusan. Artefak Arsitektur Data mencakup spesifikasi yang digunakan untuk menggambarkan keadaan yang ada, menentukan

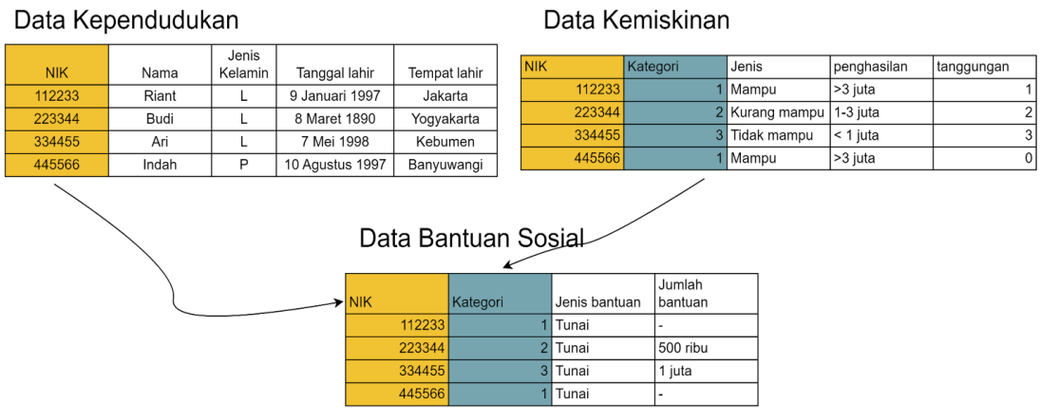
persyaratan data, memandu integrasi data, dan mengontrol aset data seperti yang dituangkan dalam strategi data. Arsitektur Data organisasi dijelaskan melalui kumpulan dokumen desain induk yang terintegrasi pada berbagai tingkat abstraksi, termasuk standar yang mengatur bagaimana data dikumpulkan, disimpan, diatur, digunakan, dan dihapus. Arsitektur data juga diklasifikasikan berdasarkan deskripsi semua wadah dan jalur yang diambil data melalui sistem Pemerintah Daerah.

Manajemen arsitektur data terdiri atas komponen utama berupa spesifikasi data (format dan struktur baku untuk data induk dan referensi) dan ketentuan data (tata perencanaan, pengumpulan, pemeriksaan, dan penyebarluasan spesifikasi data). Tujuan manajemen arsitektur data untuk menyediakan data berkualitas tinggi, mengidentifikasi, merancang struktur dan rencana untuk memenuhi kebutuhan data. Kegiatan manajemen arsitektur data meliputi penyusunan dan penetapan, penyebarluasan, dan reviu.

2. Manajemen Data referensi

Data referensi merupakan komponen yang mendeskripsikan substansi data yang berupa spesifikasi dan kategorisasi, dan ketentuan mengenai data, serta mengintegrasikannya dengan domain arsitektur SPBE yang lain. Lebih jauh, manajemen data referensi didefinisikan sebagai rangkaian proses perencanaan, pengumpulan, pemeriksaan dan penyebarluasan data referensi. Manajemen data referensi SPBE memungkinkan pengguna untuk mengakses informasi yang relevan, memperbarui informasi yang ada, dan berbagi informasi secara efisien. Data referensi SPBE juga dapat berfungsi sebagai sarana untuk meningkatkan efisiensi dan keefektifan operasional pemerintahan. Data referensi dapat mencakup hal-hal seperti undang-undang, peraturan, program pemerintah, dan lain sebagainya.

Tujuan manajemen data data referensi adalah menyediakan data yang sesuai struktur dan format baku, dijadikan acuan untuk menghasilkan data yang akurat, mutakhir dan dapat dibagi pakaikan, serta menghindari duplikasi. Kegiatan dalam manajemen data referensi, meliputi: perencanaan, pengumpulan, pemeriksaan, penyebarluasan, dan pembaruan data.



Gambar 1.3.3.2. Ilustrasi Manajemen Data

Gambar di atas merupakan contoh dari data bantuan sosial. Data bantuan sosial diperoleh dari data kependudukan dan data kemiskinan. Data kependudukan dan data kemiskinan merupakan data referensi yang diambil oleh data bantuan sosial. Data kependudukan untuk mengetahui data diri penerima bantuan sosial dan data kemiskinan untuk mengetahui kategori dan penghasilan penerima bantuan sosial. Adapun beberapa Kegiatan manajemen data yaitu :

1. Memenuhi persyaratan data Kabupaten Murung Raya. Beberapa area dalam Pemerintah Kabupaten Murung Raya memerlukan akses ke kumpulan data yang sama, dengan keyakinan bahwa kumpulan data tersebut lengkap, terkini, dan konsisten. Data induk sering menjadi dasar kumpulan data (misalnya, menentukan apakah suatu analisis mencakup semua perangkat daerah bergantung pada penerapan definisi perangkat daerah secara konsisten).
2. Mengelola kualitas data: inkonsistensi data, masalah kualitas, dan kesenjangan, menyebabkan keputusan yang salah atau kehilangan peluang, Manajemen data induk mengurangi risiko kurangnya kualitas data dengan mengaktifkan representasi yang konsisten dari entitas penting di Pemerintah Kabupaten Murung Raya.
3. Mengelola biaya integrasi: Biaya integrasi sumber data baru ke dalam lingkungan yang sudah kompleks menjadi lebih tinggi tanpa adanya data induk. Hal ini mengurangi variasi dalam menentukan dan mengidentifikasi entitas penting.
4. Mengurangi risiko: data induk dapat memungkinkan penyederhanaan arsitektur berbagi data untuk mengurangi biaya dan risiko yang terkait dengan lingkungan yang kompleks.

3. Manajemen basis data

Manajemen basis data didefinisikan sebagai proses pengelolaan kumpulan data yang disimpan di pusat data nasional. Manajemen basis data SPBE merupakan sebuah cara untuk mengelola dan menyimpan data yang dibutuhkan untuk menjalankan sistem informasi pemerintahan. Hal ini termasuk membangun dan mengatur struktur data, membuat kebijakan dan prosedur untuk memastikan data tersedia untuk pembuatan keputusan, mengatur hak akses pengguna, dan memantau kinerja sistem.

Tujuan manajemen basis data adalah menjamin penyimpanan data yang akurat, mutakhir dapat dibagi pakaikan, menjamin ketersediaan akses data yang terus menerus, dan menjaga keamanan data. Kegiatannya meliputi mendefinisikan kebutuhan walidata dan produsen data untuk basis data, mengelola basis data di Pusat Data Nasional serta menyebarluaskan basis data melalui portal SDI. Ketentuan penyimpanan data diatur oleh Menteri yang menyelenggarakan urusan pemerintahan bidang komunikasi dan informatika.

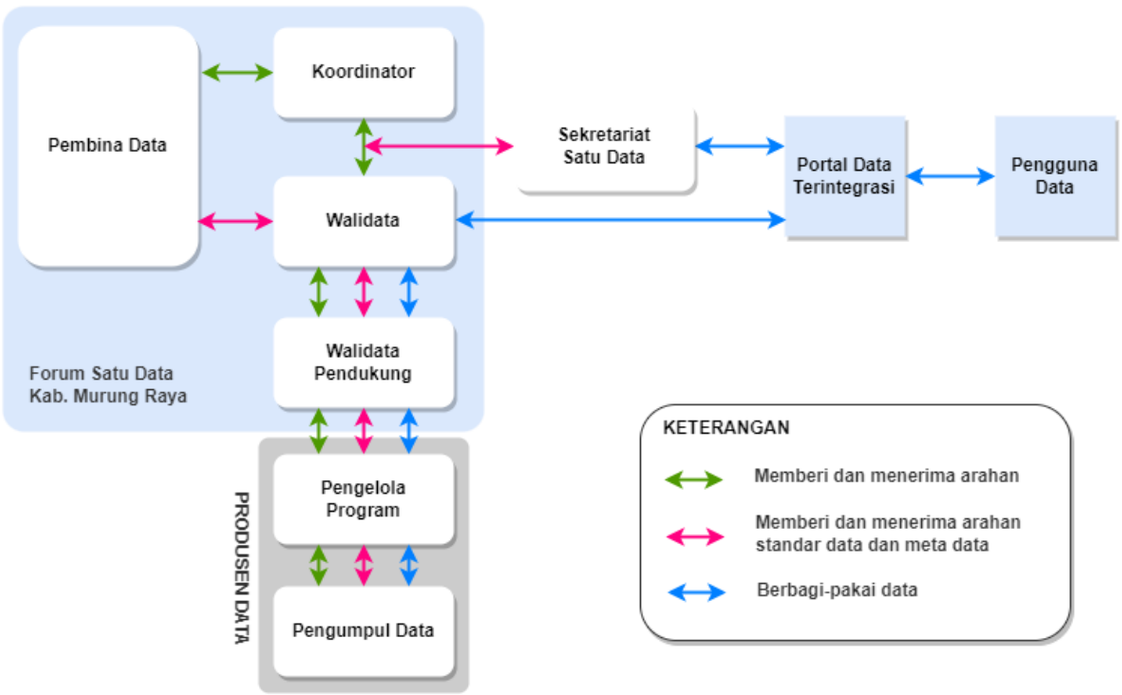
4. Manajemen kualitas data

Manajemen kualitas data didefinisikan sebagai proses untuk memastikan data yang dihasilkan dan dikelola secara elektronik memenuhi prinsip Satu Data Indonesia. Manajemen kualitas data SPBE merupakan sebuah proses untuk menentukan dan memenuhi kebutuhan kualitas data yang diterima oleh sistem, termasuk dalam hal ini penilaian data, memeriksa konsistensi data, mengevaluasi standar data, memverifikasi integritas data, melacak dan menganalisis masalah kualitas data, dan mengidentifikasi tren kualitas data. Selain itu, proses manajemen kualitas data termasuk dalam mengidentifikasi sumber data dan memahami kontribusi yang diberikan oleh sumber data tersebut.

Tujuan dari manajemen kualitas data adalah untuk menjamin bahwa data yang dihasilkan oleh produsen data memenuhi prinsip SDI dan diperbarui sesuai dengan jadwal pemutakhiran data. Kegiatan manajemen kualitas data meliputi pengembangan dan promosi kesadaran kualitas, menentukan persyaratan kualitas data, menetapkan profil, menganalisis, dan menilai kualitas data serta menentukan matriks kualitas data.
Kualitas data dapat dideskripsikan menjadi 6 bagian yaitu :

- Kelengkapan : Proporsi data yang disimpan terhadap potensi 100%.
- Keunikan : Tidak ada instance entitas (benda) yang akan direkam lebih dari satu kali berdasarkan bagaimana benda tersebut diidentifikasi.
- Ketepatan Waktu : Sejauh mana data mewakili kenyataan dari titik waktu yang diperlukan.
- Validitas : Data valid jika sesuai dengan sintaks (format, type, range) definisinya.
- Akurasi : Sejauh mana data dengan benar menggambarkan objek atau peristiwa "dunia nyata" yang dijelaskan.
- Konsistensi : Tidak adanya perbedaan, ketika membandingkan dua atau lebih representasi dari suatu hal terhadap definisi.

Mengacu pada Perpres 39/2019 tentang Satu Data Indonesia, dalam Penerapan Manajemen Data Kabupaten Murung Raya perlu menyusun struktur forum satu data seperti berikut :



Gambar 1.3.3.3. Kelembagaan Forum Satu Data Kabupaten Murung Raya

Penugasan:

Koordinator	SEKDA
Pembina Data	BPS & Badan Perencanaan Pembangunan Daerah dan Penelitian Pengembangan
Walidata	Dinas Komunikasi, Informatika, Statistik dan Persandian
Walidata Pendukung	Unsur perangkat daerah/instansi
Produsen Data	Unsur perangkat daerah/instansi

Tugas Pembina Data:

1. memberikan rekomendasi dalam proses perencanaan pengumpulan data; dan
2. bertanggung jawab dalam pelaksanaan pembinaan penyelenggaraan Satu Data Indonesia tingkat kabupaten sesuai dengan ketentuan peraturan perundang-undangan.

Tugas Wali Data Tingkat Kabupaten:

1. bertanggung jawab dalam pengelolaan simpul jaringan;
2. membangun, memelihara, dan menjamin keberlangsungan sistem akses Informasi Geospasial (IG);
3. bertanggung jawab dalam penyimpanan, pengamanan dan penyebarluasan Data Geospasial (DG) dan IG;
4. mengoordinasikan simpul jaringan dalam hal penyelenggaraan jaringan IG;
5. bertanggung jawab dalam pemeriksaan kesesuaian data yang disampaikan oleh

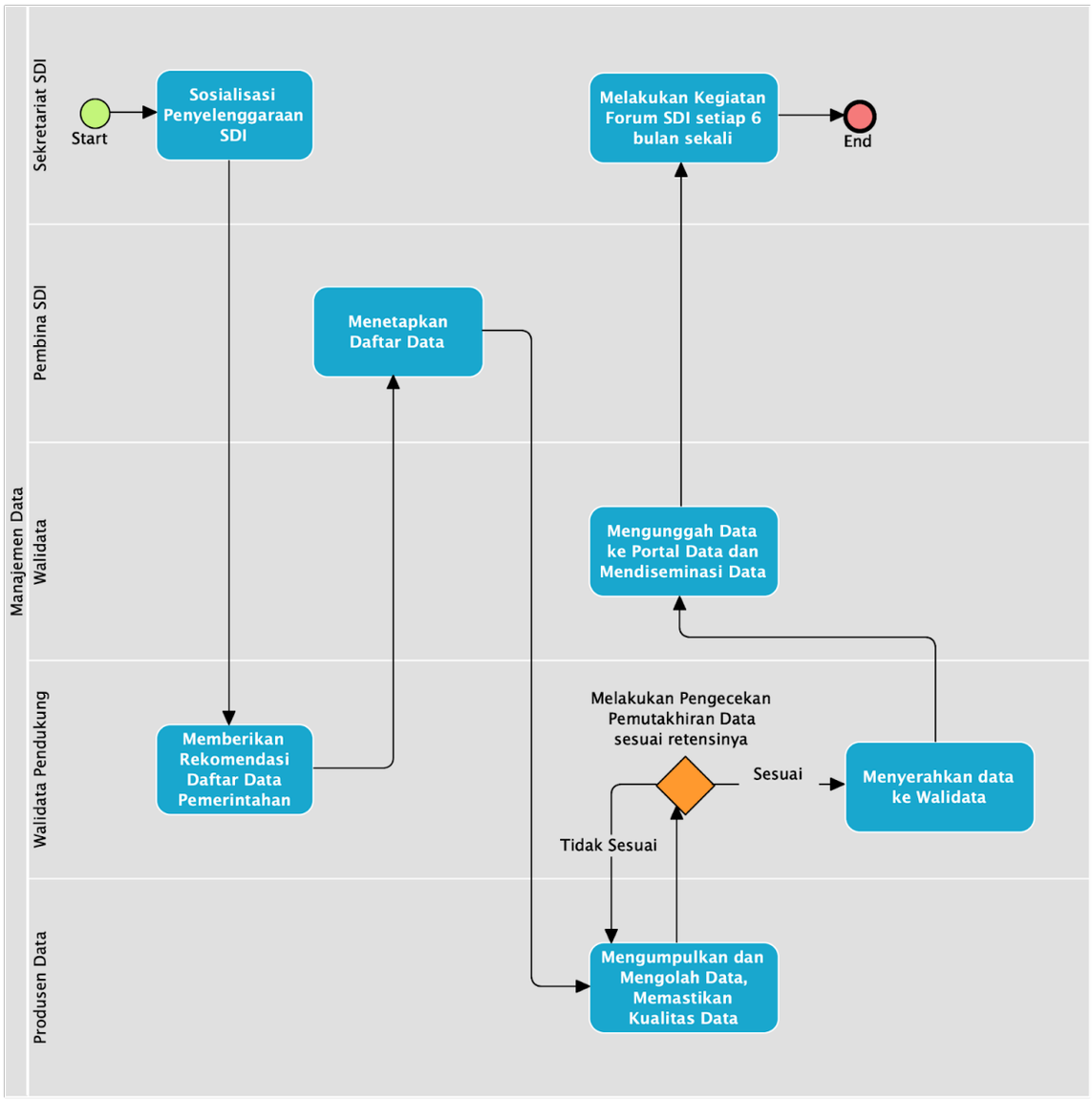
produsen data tingkat Kabupaten sesuai dengan prinsip Satu Data Indonesia;

6. bertanggung jawab dalam penyebarluasan data dan metadata melalui portal Satu Data Indonesia tingkat Kabupaten;
7. membantu Pembina Data tingkat Kabupaten dalam membina produsen data tingkat Kabupaten; dan
8. berperan aktif dalam simpul jaringan, Forum Satu Data Pembangunan dan Satu Data Indonesia tingkat Kabupaten.

Tugas Produsen Data Tingkat Kabupaten:

1. memberikan masukan kepada Pembina Data tingkat kabupaten mengenai standar data, metadata, dan interoperabilitas data;
2. bertanggung jawab dalam pelaksanaan produksi data sesuai dengan prinsip Satu Data Indonesia;
3. bertanggung jawab dalam pelaksanaan pengumpulan, pengolahan, penggunaan DG dan IG *berikut* metadatanya, serta pembaruan DG dan IG;
4. bertanggung jawab dalam penyampaian data *berikut* metadata kepada Walidata tingkat kabupaten melalui walidata pendukung tingkat kabupaten di masing-masing perangkat daerah; dan
5. berperan aktif dalam Simpul Jaringan dan Forum Satu Data Indonesia tingkat Kabupaten.

Berdasarkan *best practices* di atas, alur pengelolaan implementasi Satu Data Pemerintah Kabupaten Murung Raya dapat dilaksanakan seperti berikut ini :



Gambar 1.3.3.4. Alur Koordinasi Satu Data

Secara teknis pemerintah daerah perlu menyusun kebijakan/SOP terkait manajemen data dengan lingkup sebagai berikut :

1. Arsitektur Data yang berisi kamus data dan kewenangan wali data;
2. SOP Validasi dan verifikasi data sebelum masuk ke data *warehouse;*
3. SOP Pengumpulan data;
4. SOP Penyebarluasan data;
5. SOP Pemanfaatan data;
6. SOP Penentuan walidata dan produsen data; dan
7. SOP Pembuatan dan perubahan kamus data metadata.

1.3.4. Manajemen Aset TIK

Manajemen aset Teknologi Informasi dan Komunikasi (TIK) merupakan serangkaian proses perencanaan, pengadaan, pengelolaan, dan penghapusan perangkat keras dan perangkat lunak yang digunakan dalam SPBE. Manajemen aset TIK melibatkan pengelolaan

kebutuhan dan kebutuhan yang berubah, mengurangi biaya keseluruhan, dan memastikan ketersediaan sistem yang dibutuhkan. Manajemen aset TIK yang efektif dapat memastikan bahwa layanan teknologi informasi pemerintah berjalan dengan lancar dan berkinerja tinggi. Contoh kasus dalam mengelola pusat data perlu memastikan perangkat terpelihara, terlindungi dengan baik (tersedia *power supply* saat listrik mati, ditempatkan di ruangan ber AC agar tidak *overheat*) serta melakukan peremajaan terhadap perangkat sesuai dengan *life-time*. Mengacu pada *best practices* dalam *ISO/IEC 19770-5* tentang *IT Asset Management*, berikut aktivitas-aktivitas yang perlu dilakukan dalam manajemen Aset TIK :

Gambar 1.3.4.1. Manajemen Aset TIK

A. Mengidentifikasi kondisi aset TIK saat ini

Mencatat seluruh aset TIK *(software & hardware*) beserta kondisi dan *life-time* nya. Selain itu, *software* berbayar perlu dipastikan lisensinya sudah terbayar.

B. Mengelola aset TIK yang penting

Memastikan aset TIK selalu tersedia dan dapat diandalkan untuk dapat digunakan dalam menunjang operasional SPBE.

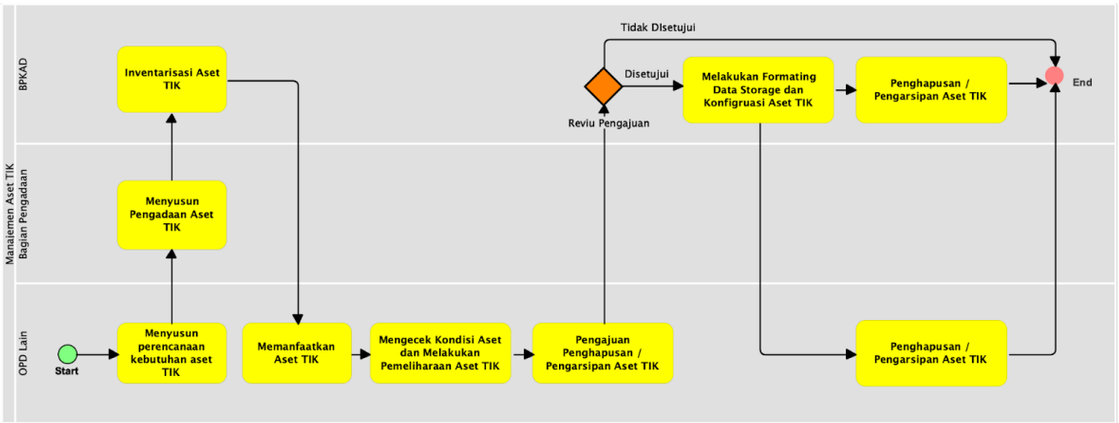
C. Mengelola siklus aset TIK

Mengelola aset mulai dari pengadaan hingga pembuangan dalam arti ketika sudah habis masa pakainya *lifetime* perlu dilakukan pembaharuan aset. Pastikan aset digunakan seefektif dan seefisien mungkin dan dapat dipertanggungjawabkan dan dilindungi secara fisik sampai akhir *lifetime*.

D. Mengoptimalisasi nilai aset TIK

Meninjau aset serta mengidentifikasi bagaimana cara mengoptimalkan aset sesuai kebutuhan proses bisnis SPBE.

Berdasarkan *best practices* di atas Pemerintah Kabupaten Murung Raya dalam alur proses pengelolaan manajemen aset TIK nya dapat merujuk pada gambar berikut ini :



Gambar 1.3.4.2. Alur Pengelolaan Manajemen Aset TIK

Secara teknis pemerintah daerah perlu menyusun kebijakan/SOP terkait manajemen Aset TIK dengan lingkup sebagai berikut:

1. SOP Pembuatan dan perubahan pengkodean Aset TIK.
2. SOP Inventarisasi & konfigurasi Aset TIK.
3. SOP Pemeliharaan dan Perbaikan Aset TIK.
4. SOP Penghapusan Aset TIK.

1.3.5. Manajemen SDM

Manajemen SDM merupakan serangkaian proses perencanaan, pengembangan, pembinaan, dan pendayagunaan SDM dalam SPBE. Manajemen SDM membantu mengelola sumber daya manusia, memberikan dukungan teknis, dan memonitor aktivitas. Selain itu, manajemen SDM membantu dalam melacak kemampuan dan kompetensi pegawai, mengatur tugas dan pekerjaan, menganalisis kinerja, mengatur jadwal, meningkatkan efisiensi operasional, memberikan informasi yang akurat tentang kesiapan SDM TIK, memungkinkan manajemen TIK untuk mengambil keputusan yang tepat dan memastikan bahwa semua aspek dari SDM TIK berfungsi dengan baik.

Manajemen SDM perlu dilakukan guna menjamin keberlangsungan peningkatan mutu layanan SPBE dan memastikan ketersediaan kompetensi SPBE. Mengacu pada Permen PANRB 38/2017 tentang standar kompetensi jabatan ASN, pemerintah daerah dituntut untuk melaksanakan beberapa aktivitas berikut ini:

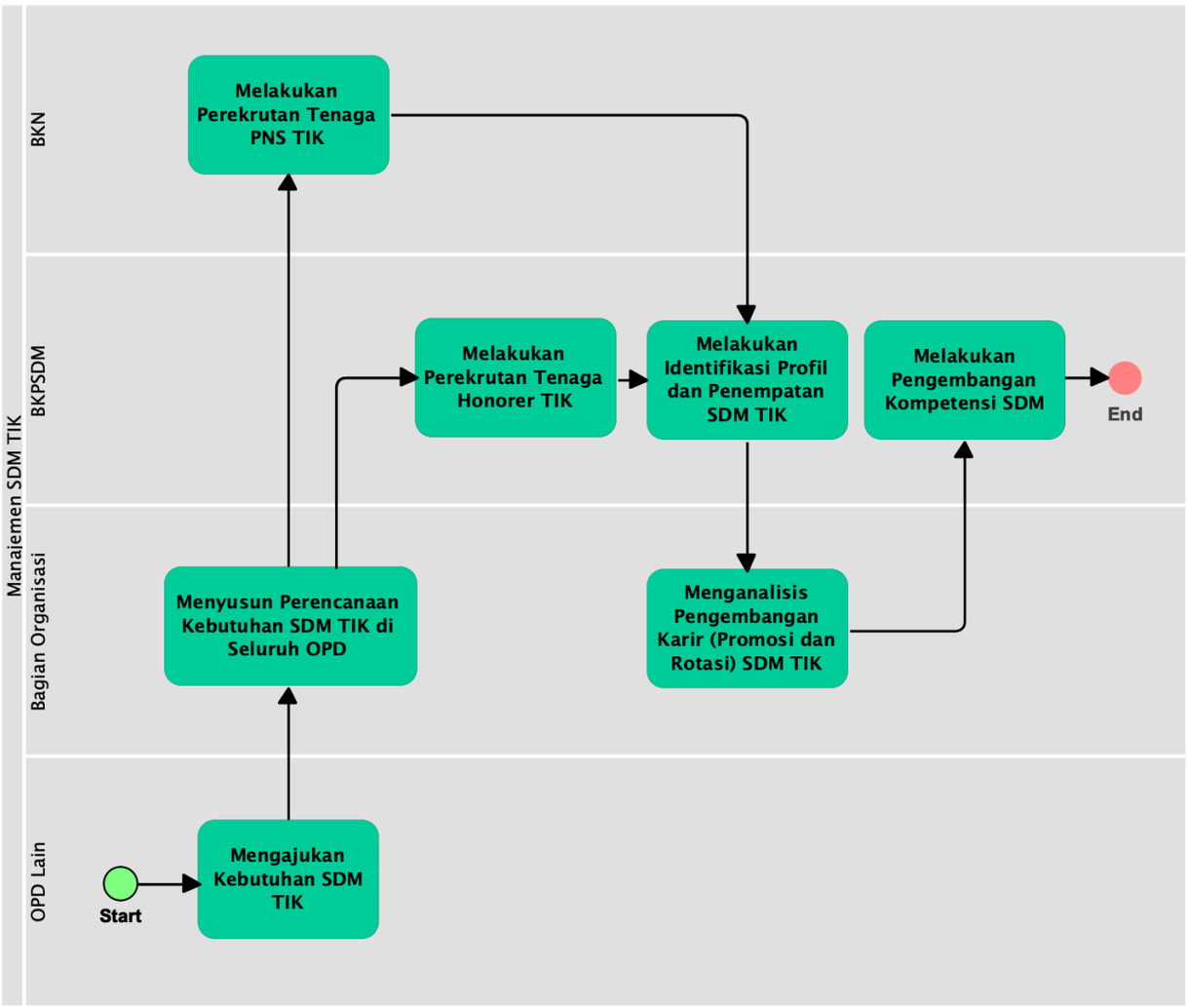
1. Perencanaan Aparatur Sipil Negara (ASN);
2. Pengadaan Aparatur Sipil Negara (ASN);
3. Pengembangan karir Aparatur Sipil Negara (ASN);
4. Pengembangan kompetensi Aparatur Sipil Negara (ASN);
5. Penempatan Aparatur Sipil Negara (ASN);
6. Promosi dan/atau mutasi Aparatur Sipil Negara (ASN);
7. Uji kompetensi Aparatur Sipil Negara (ASN);
8. Sistem informasi manajemen Aparatur Sipil Negara (ASN); dan

9. Kelompok rencana suksesi *(talent pool)* Aparatur Sipil Negara (ASN).

Pada kondisi ideal setiap perangkat daerah diharapkan memiliki SDM TIK yang dibutuhkan untuk menunjang pelaksanaan tugas dan penyelenggaraan fungsi kedinasan masing-masing pegawai. Jenis dan keahlian TIK yang dituntut sangat beragam tergantung posisi dan tugas yang diberikan. Adapun keahlian TIK yang dibutuhkan, meliputi:

1. Kebijakan SPBE: Profesional dalam bidang ini berfokus pada penyusunan kebijakan, dan regulasi terkait penggunaan dan pengembangan SPBE di pemerintahan.
2. Manajemen SPBE: Ini melibatkan perencanaan strategis, pengembangan kebijakan, pengelolaan anggaran, dan pengawasan keseluruhan aspek SPBE dalam lingkungan pemerintahan.
3. *Enterprise Architect*: Ahli transformasi digital berfokus pada merombak proses administratif dan layanan pemerintah dengan memanfaatkan teknologi terbaru untuk meningkatkan efisiensi dan kualitas layanan.
4. *Project Manager*: Spesialis pengelolaan proyek TIK bertanggung jawab untuk merencanakan, mengarahkan, dan mengelola proyek pengembangan atau peningkatan sistem TIK.
5. *System Analyst*: Profesional TIK dengan keahlian dalam menganalisis kebutuhan sistem informasi, merancang solusi berbasis teknologi, dan mengidentifikasi peluang peningkatan efisiensi.
6. *Programmer*: Ahli pengembangan perangkat lunak di pemerintahan bertanggung jawab untuk merancang, mengembangkan, dan memelihara aplikasi perangkat lunak yang mendukung berbagai tugas administratif dan layanan publik.
7. *Network Engineer*: Keahlian dalam merancang, mengelola, dan memelihara infrastruktur jaringan, server, dan sistem penyimpanan yang mendasari operasi teknologi di pemerintahan.
8. *IT Security*: Professional keamanan informasi bekerja untuk melindungi data sensitif dan infrastruktur TIK pemerintahan dari ancaman siber dan pelanggaran keamanan.
9. *Application Support*: Tim dukungan teknis menyediakan bantuan dan solusi teknis bagi pengguna dalam mengatasi masalah perangkat keras, perangkat lunak, dan jaringan.
10. *Data Scientist*: Ahli dalam pengumpulan, pengelolaan, analisis, dan visualisasi data untuk mendukung pengambilan keputusan berbasis data di pemerintahan.

Peningkatan kemampuan SDM TIK dibutuhkan dan disesuaikan dengan tugas dan kewajiban dari personil yang terlibat. Peningkatan kemampuan personel dapat dilakukan melalui pelatihan-pelatihan maupun studi tingkat lanjut. Seseorang yang mempunyai tanggung jawab terhadap sistem semakin lama akan semakin ahli pada bidangnya dan akan semakin bermanfaat jika ia tetap pada pekerjaannya. Dalam hal peningkatan SDM TIK, diperlukan bentuk penghargaan yang berbeda sehingga perlu adanya tenaga ahli TIK di masing-masing perangkat daerah yang bertugas mengelola TIK.



Gambar 1.3.5.1. Alur Prosedur Manajemen SDM

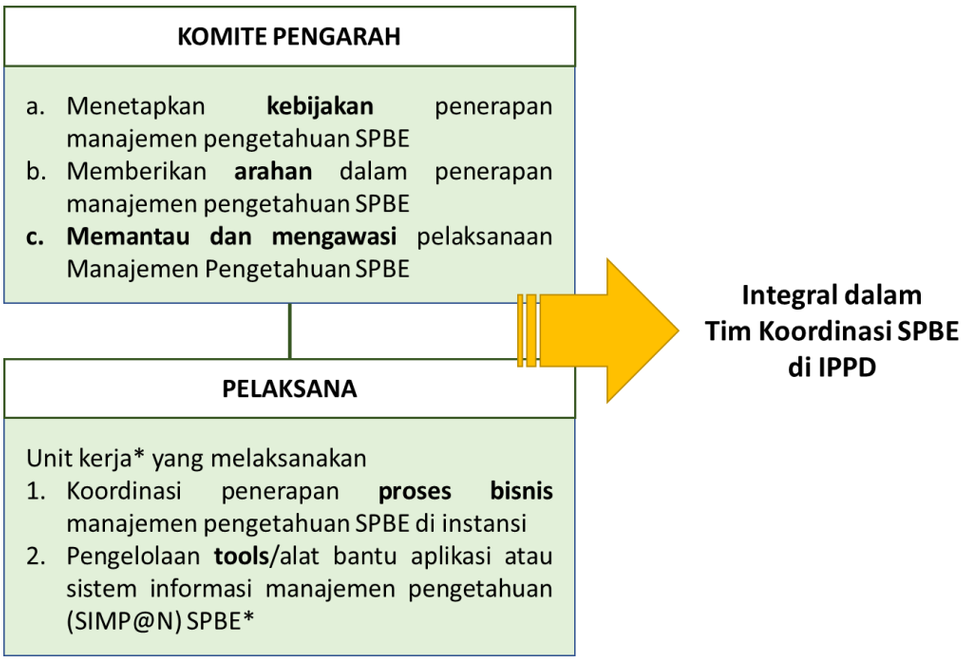
Secara teknis pemerintah daerah perlu menyusun kebijakan/SOP terkait manajemen SDM dengan lingkup sebagai berikut:

1. SOP Permintaan Kebutuhan SDM TIK perangkat daerah.
2. SOP Pengadaan & Pengelolaan SDM TIK non ASN.
3. SOP Permintaan kebutuhan training, sertifikasi & peningkatan kompetensi SDM TIK.

1.3.6. Manajemen Pengetahuan

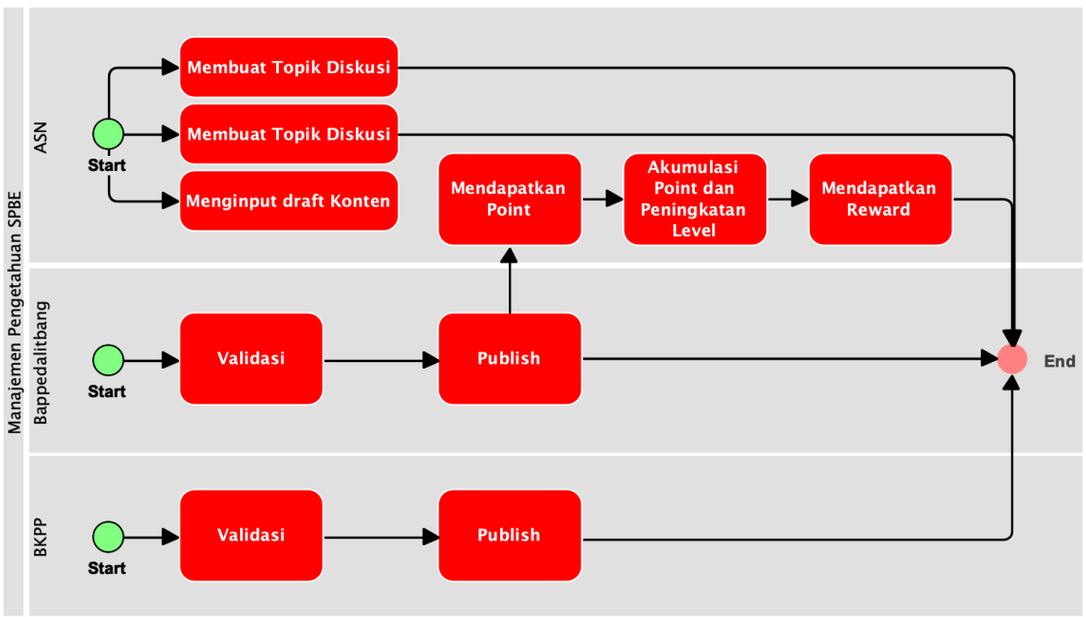
Manajemen pengetahuan adalah upaya terstruktur dan sistematis dalam mengembangkan dan menggunakan pengetahuan yang dimiliki untuk membantu proses pengambilan keputusan bagi peningkatan kinerja pemerintah daerah. Aktivitas dalam manajemen pengetahuan meliputi upaya perolehan, penyimpanan, pengolahan dan pengambilan kembali, penggunaan dan penyebaran, serta evaluasi dan penyempurnaan terhadap pengetahuan sebagai aset intelektual instansi pemerintah daerah. Manajemen pengetahuan menjadi penting karena memuat hasil pekerjaan yang berasal dari pengetahuan yang diterapkan, tumbuhnya *knowledge economies*, pengembangan SDM yang profesional, perlunya berbagi pengetahuan lintas bagian dalam organisasi, serta risiko

pergantian pegawai terhadap organisasi. Adapun struktur komite manajemen pengetahuan SPBE sebagai berikut.



Gambar 1.3.6.1. Struktur Komite Manajemen Pengetahuan

Mekanisme alur proses manajemen pengetahuan SPBE yang perlu ada di Pemerintah Kabupaten Murung Raya dijelaskan pada gambar berikut ini.



Gambar 1.3.6.2. Alur Proses Manajemen Pengetahuan

Implementasi SPBE perlu melakukan manajemen pengetahuan untuk meningkatkan layanan SPBE dan mendukung proses pengambilan keputusan. Dalam melaksanakan manajemen pengetahuan SPBE perlu mempersiapkan serangkaian proses :

1. Mensosialisasikan pentingnya manajemen pengetahuan;

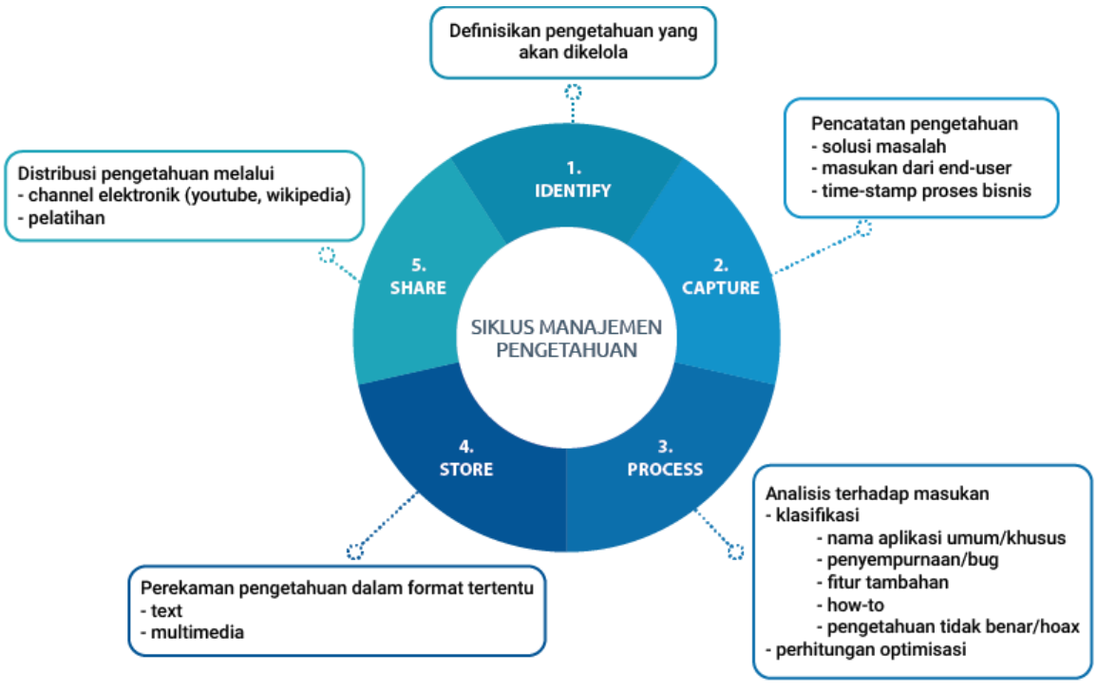
2. Membentuk kelompok kerja implementasi manajemen pengetahuan;
3. Menjabarkan visi dan misi dalam implementasi manajemen pengetahuan melalui sosialisasi secara berkala;
4. Merencanakan *Quick-Win* untuk mengatasi keraguan dan resistensi;
5. Melakukan konsolidasi manfaat yang sudah tercapai, untuk mendapatkan momentum; dan
6. Menerapkan budaya "*sharing & re-use*" sebagai cara bekerja yg efektif dan efisien.

Gambar 1.3.6.3. Manajemen Pengetahuan

Manfaat dari manajemen pengetahuan SPBE sebagai berikut :

1. Mengurangi duplikasi upaya untuk mendapatkan suatu pengetahuan atau cara kerja.
2. Mengurangi biaya dan waktu operasi layanan SPBE.
3. Meningkatkan kompetensi operator layanan SPBE.
4. Memberdayakan operator, penerima manfaat SPBE, staf TIK dan analis proses bisnis
5. Meningkatkan kualitas layanan SPBE.

Pada manajemen pengetahuan terdapat siklus hidup yang dimulai dari proses identifikasi, pencatatan, pemrosesan, penyimpanan. Adapun siklus manajemen pengetahuan digambarkan sebagai berikut.

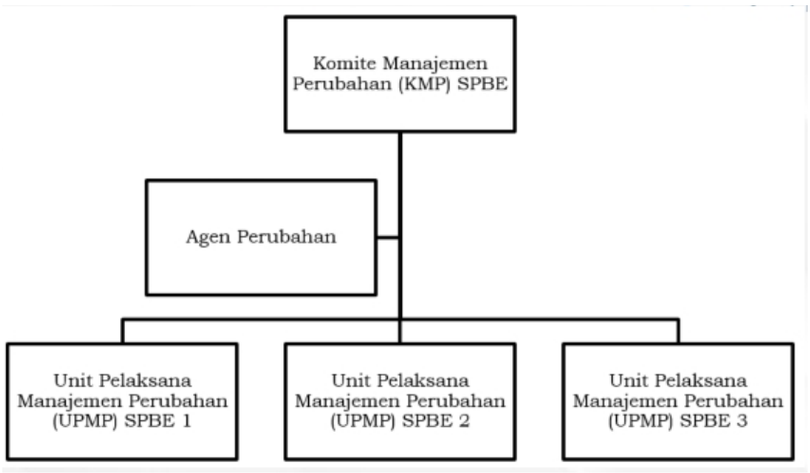


Gambar 1.3.6.4. Siklus Manajemen Pengetahuan

Secara teknis pemerintah daerah perlu menyusun kebijakan/SOP terkait manajemen pengetahuan dengan lingkup SOP Pencatatan pengalaman & *lesson learned* untuk setiap perangkat daerah.

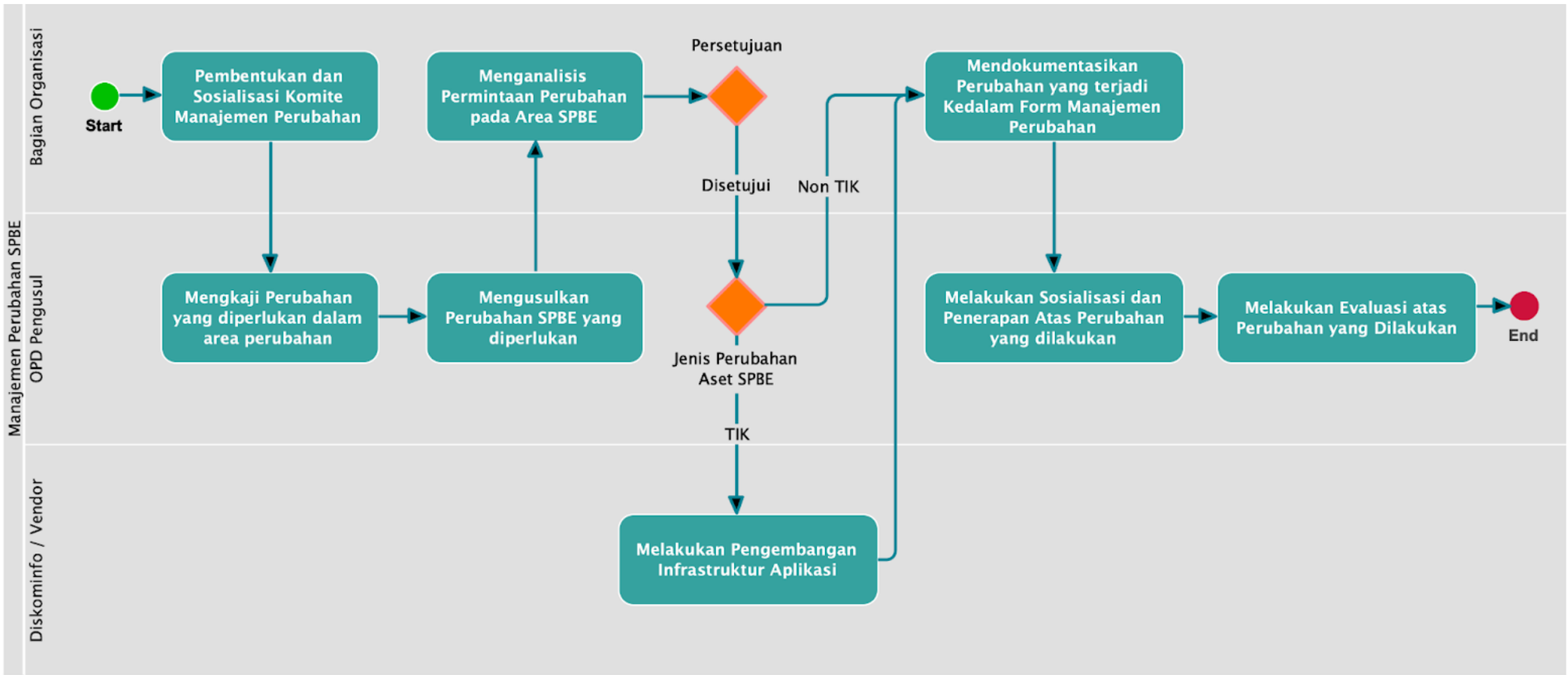
1.3.7. Manajemen Perubahan

Manajemen perubahan merupakan sebuah pendekatan siklus, dan sistematis pada transisi organisasi, program, dan kegiatan dari keadaan saat ini ke keadaan masa depan dengan target manfaat perubahan yang diharapkan. Manajemen perubahan dapat membantu pemerintah daerah dalam mengantisipasi dan merespon perubahan yang dihadapi. Selain itu, dalam manajemen perubahan digunakan untuk mengidentifikasi perubahan, mengevaluasi dampak perubahan, mengembangkan dan melaksanakan rencana perubahan, dan memonitoring dan mengevaluasi efektivitas perubahan. Oleh karena itu, dalam manajemen perubahan diperlukan sebuah komite manajemen perubahan yang bertanggung jawab untuk membuat rekomendasi, menentukan strategi, dan menciptakan kebijakan untuk memastikan bahwa perubahan berhasil diimplementasikan dengan sukses. Adapun skema komite manajemen perubahan sebagai berikut.



Gambar 1.3.7.1. Komite Manajemen Perubahan SPBE

Setiap perubahan yang terdapat pada visi dan misi/kebijakan/SOTK berimplikasi dengan perubahan pada layanan. Layanan harus mampu mengadopsi perubahan tersebut dengan melakukan manajemen perubahan pada bisnis proses, aplikasi maupun infrastrukturnya. Mekanisme alur perubahan layanan SPBE yang perlu ada di Pemerintah Kabupaten Murung Raya dijelaskan pada gambar berikut ini:



Gambar 1.3.7.2. Alur Proses Manajemen Perubahan SPBE

Secara teknis pemerintah daerah perlu menyusun kebijakan/SOP terkait manajemen perubahan dengan lingkup SOP Manajemen Perubahan.

1.3.8. Manajemen Layanan

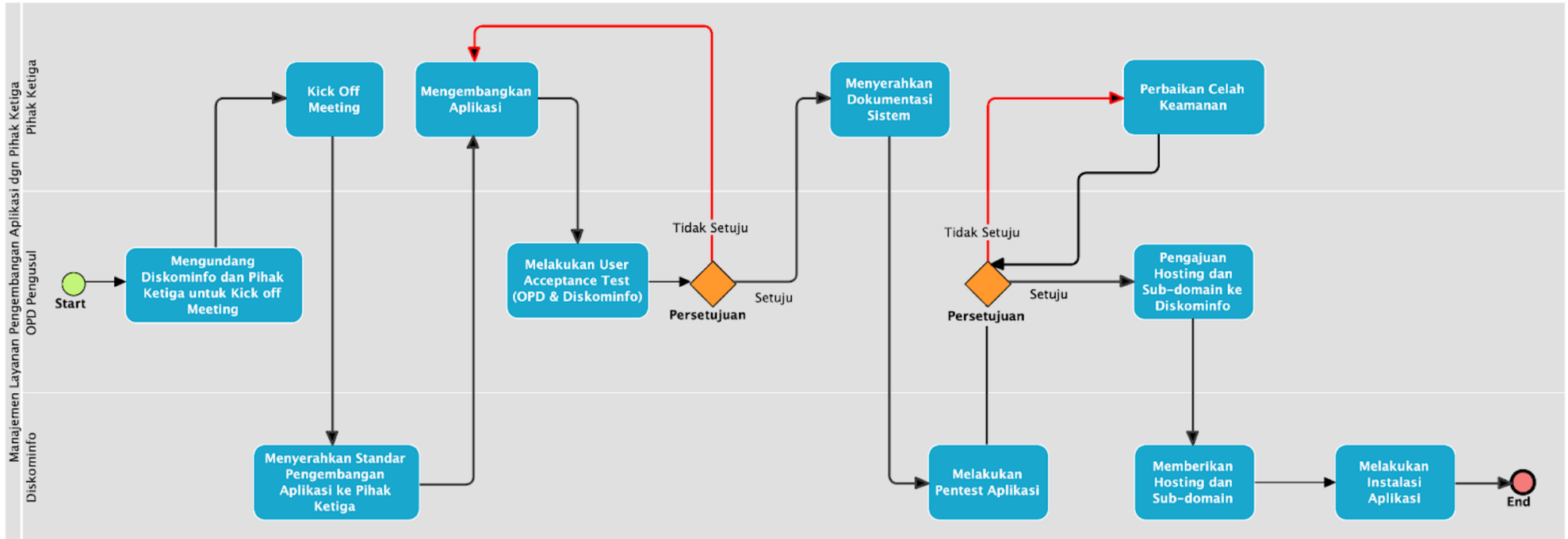
Manajemen layanan merupakan serangkaian proses pelayanan kepada pengguna, pengoperasian layanan, dan pengelolaan Aplikasi SPBE agar layanan SPBE dapat berjalan berkesinambungan dan berkualitas. Manajemen layanan SPBE membantu pemerintah dalam menyediakan layanan yang lebih cepat, tepat, dan efisien kepada masyarakat. Manajemen layanan SPBE memungkinkan pemerintah untuk melakukan pemantauan, pengujian, dan verifikasi data secara *real-time* sehingga memastikan bahwa layanan yang diberikan tepat waktu dan sesuai dengan standar kualitas yang telah ditetapkan.

Implementasi SPBE perlu memastikan portofolio layanan SPBE terpelihara dengan baik dengan berbagai cara. Mengacu pada *best practices* yang terdapat dalam pedoman ITIL v.4, terdapat beberapa aktivitas yang harus dilakukan seperti:

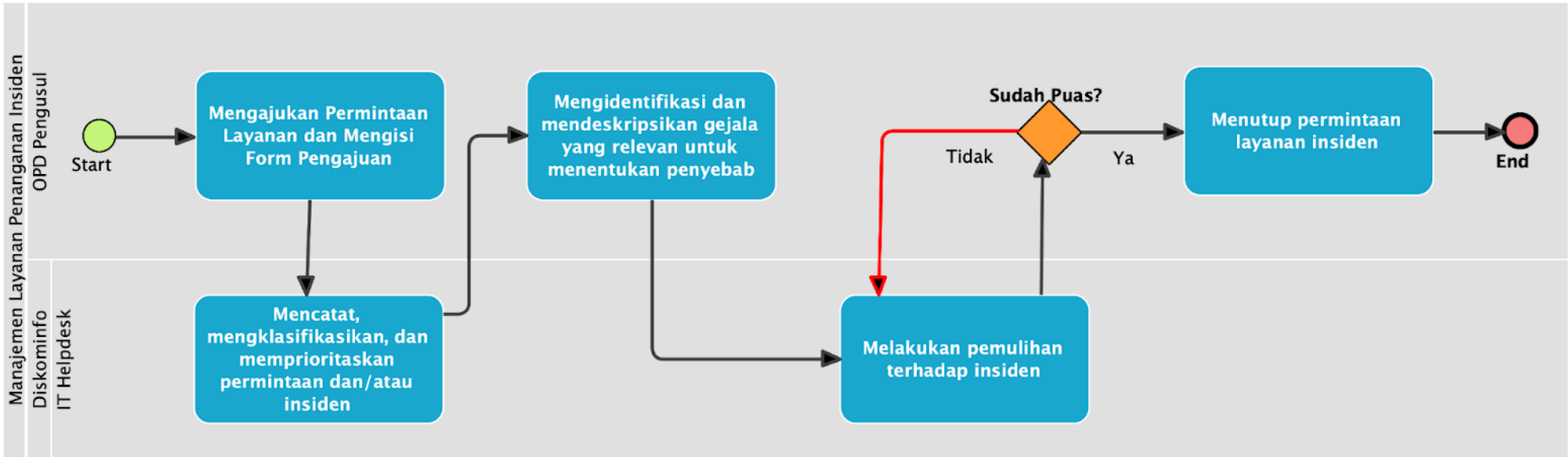
Gambar 1.3.8.1. Manajemen Layanan

1. Mengelola gangguan dengan menyediakan *platform helpdesk* TIK disertai dengan *ticketing* dan monitoring *Service Level Agreement (SLA)*.
2. Melakukan pemeliharaan aplikasi dan infrastruktur TIK secara berkala dan sesuai dengan prioritas risiko.
3. Berpedoman pada metodologi baku seperti ITIL v4 terkait standar manajemen layanan IT.

Berdasarkan *best practices* di atas Diskominfo dapat melakukan pemberian dukungan layanan TI terkait (a.) layanan pengembangan aplikasi dan (b). layanan penanganan insiden yang dijelaskan pada gambar berikut ini :



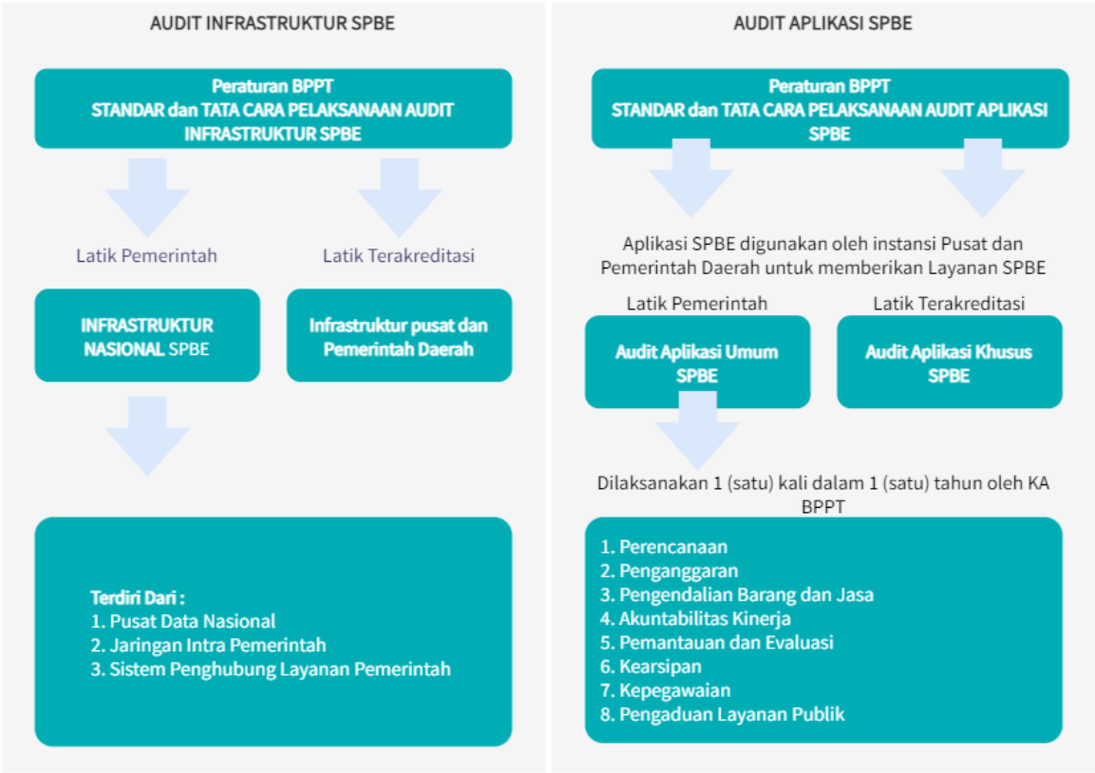
Gambar 1.3.8.2. Layanan Pengembangan Aplikasi



Gambar 1.3.8.3. Layanan Penanganan Insiden

Secara teknis pemerintah daerah perlu menyusun kebijakan/SOP terkait manajemen layanan dengan lingkup SOP Pengajuan layanan (*Helpdesk*) dan SOP Pengembangan Aplikasi dengan pihak ketiga.

1.3.9. Audit TIK



Gambar 1.3.9.1. Lingkup Audit TIK

(sumber: Paparan KemenpanRB)

Audit TIK merupakan evaluasi secara sistematis dan objektif yang dilakukan oleh auditor teknologi terhadap aset teknologi dalam rangka memberikan nilai tambah (manfaat) kepada pihak yang diaudit atau pemilik kepentingan. Audit Teknologi Informasi dan Komunikasi meliputi pemeriksaan hal pokok teknis pada:

1. Penerapan tata kelola dan manajemen teknologi informasi dan komunikasi.
2. Fungsionalitas teknologi informasi dan komunikasi.
3. Kinerja teknologi informasi dan komunikasi yang dihasilkan.
4. Aspek teknologi informasi dan komunikasi lainnya.

Audit Teknologi Informasi dan Komunikasi dilaksanakan oleh lembaga pelaksana Audit Teknologi Informasi dan Komunikasi pemerintah atau lembaga pelaksana Audit Teknologi Informasi dan Komunikasi yang terakreditasi sesuai dengan ketentuan peraturan perundang-undangan. Ada tiga hal yang harus dilakukan dalam audit teknologi informasi yaitu :

A. Audit infrastruktur SPBE, merujuk pada Perpres 95/2018 pasal 55 disebutkan:

1. Infrastruktur SPBE Nasional diaudit setiap tahun oleh Badan Riset dan Inovasi Nasional (BRIN).
2. Infrastruktur SPBE Pemerintah Daerah diaudit setiap dua tahun oleh lembaga audit TIK tersertifikasi atau terdaftar di Badan Riset dan Inovasi Nasional (BRIN).
3. Koordinasi dengan Kementerian Kominfo.

B. Audit Aplikasi SPBE dilakukan dengan mengaudit aplikasi umum setiap tahun oleh Badan Riset dan Inovasi Nasional (BRIN), sedangkan audit aplikasi khusus dilakukan setiap dua tahun oleh Lembaga Audit TIK yang berkoordinasi dengan Kementerian Kominfo.

C. Audit Keamanan Informasi pada infrastruktur SPBE Nasional dan aplikasi umum dilakukan setiap tahun oleh BSSN, sedangkan untuk audit keamanan pada infrastruktur SPBE dan aplikasi khusus di Instansi Pusat dan Instansi Daerah dilakukan setiap dua tahun oleh Lembaga Audit TIK atau perusahaan audit TIK.

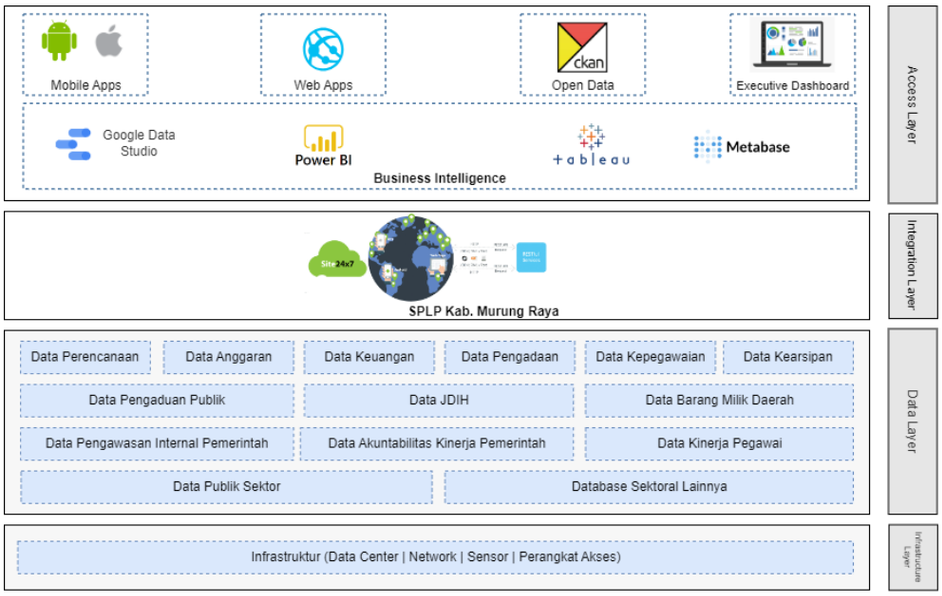
Adapun kegiatan yang dilakukan dalam Audit TIK dijabarkan sebagai berikut :

1. Menyusun Rencana Prosedur Audit Teknologi Informasi;
2. Mengalokasikan Sumber Daya Audit Teknologi Informasi;
3. Melaksanakan Prosedur Audit atas Perencanaan Teknologi Informasi;
4. Melaksanakan Prosedur Audit atas Pengembangan Teknologi Informasi;
5. Melaksanakan Prosedur Audit atas Operasional Teknologi Informasi;
6. Melaksanakan Prosedur Audit atas Pemantauan Teknologi Informasi;
7. Melaksanakan Prosedur Audit atas Aplikasi Teknologi Informasi;
8. Melaksanakan Prosedur Audit atas Infrastruktur Teknologi Informasi;
9. Mengawasi Kelayakan Pelaksanaan Prosedur Audit Teknologi Informasi;
10. Mengawasi Kelayakan Dokumentasi Hasil Pelaksanaan Prosedur Audit Teknologi Informasi;
11. Menyusun Hasil Audit Teknologi Informasi;
12. Menyusun Rekomendasi Audit Teknologi Informasi;
13. Mengidentifikasi Tindak Lanjut Audit Teknologi Informasi; dan
14. Memverifikasi Kelayakan Tindak Lanjut Audit Teknologi Informasi.

Bab II Arsitektur Target SPBE

2.1. Arsitektur Aplikasi

2.1.1. Desain Arsitektur Aplikasi



Gambar 2.1.1.1. Desain Arsitektur Aplikasi

Desain arsitektur aplikasi SPBE dijabarkan sebagai berikut:

- *Access Layer*

  Bagian ini akan terdapat aplikasi-aplikasi yang akan mendukung perangkat daerah dalam proses operasional utama di perangkat daerah. Masing-masing perangkat daerah akan memiliki aplikasi dengan alur probis (proses bisnis) yang beragam sesuai dengan tugas dan fungsi perangkat daerah tersebut. Selain itu juga perangkat daerah perlu belajar untuk memanfaatkan *tools business intelligence* dengan tujuan untuk memvisualisasikan data sebagai rangkaian dalam penerapan satu data Indonesia.

- *Integration Layer*

  Bagian ini ditujukan untuk aplikasi, *platform*, *module*, *services* yang berfungsi sebagai jembatan antara *layer* data dengan *layer* access. Proses pengaturan terhadap akses data juga dikelola oleh layanan pada *layer* ini. Pada *layer* ini akan terdapat *API gateway* yang terhubung dengan masing-masing aplikasi yang berjalan guna mengelola akses integrasi data antar aplikasi.

- *Data Layer*

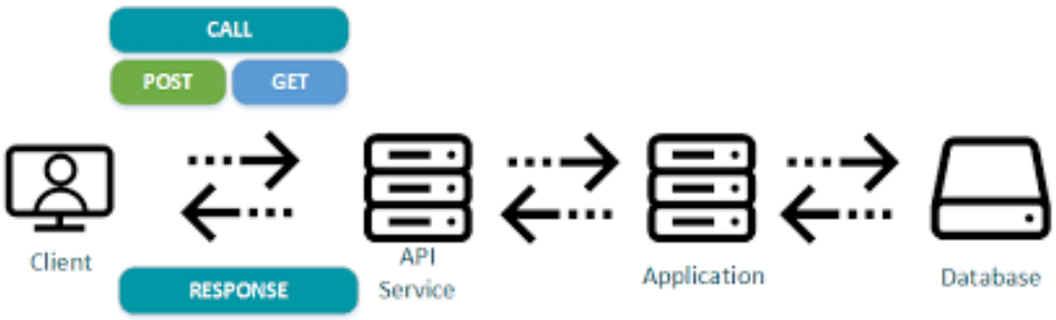
  Bagian data *layer* ini berisi *database* dari data-data pemerintahan sektoral yang berasal dari berbagai aplikasi. Secara umum *DBMS* yang digunakan di lingkungan Pemerintah Kabupaten Murung Raya yaitu *MySQL*.

- *Layer* Arsitektur

  Bagian ini terdapat perangkat jaringan, pusat data dan CCTV guna mendukung operasional aplikasi 24x7 jam.

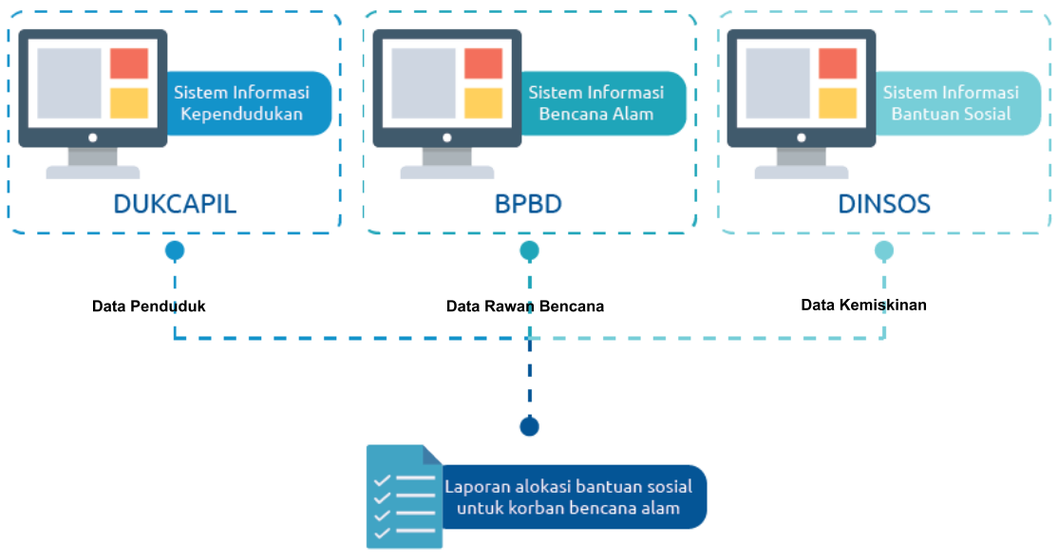
2.1.2. Integrasi Aplikasi

Permasalahan integrasi merupakan kendala yang cukup kompleks dalam implementasi SPBE. Kurang adanya integrasi antar aplikasi berdampak pada ketidak efisiennya layanan operasional pemerintahan dan rentan terjadinya duplikasi data. Aplikasi yang dikembangkan harus dapat diintegrasikan dengan menggunakan teknologi *Application Programming Interface* (API).



Gambar 2.1.2.1. Skema Alur Kerja *API*

API adalah kumpulan fungsi-fungsi untuk menggantikan bahasa yang digunakan dalam *system call* dengan bahasa yang terstruktur. *API* menyediakan fungsi untuk menghubungkan koneksi antar aplikasi. Secara umum *API* mampu menerima respon data dalam format *JSON* dan *XML*. Sebagai contoh, data kependudukan (DUKCAPIL), data bencana alam (BPBD), dan data bantuan sosial (DINSOS) saling terintegrasi sebagai dasar penyusunan laporan alokasi bantuan sosial untuk korban bencana alam.



Gambar 2.1.2.2. Ilustrasi Integrasi antar Aplikasi

2.1.3. Arsitektur Aplikasi Usulan

2.1.3.1. Katalog Aplikasi Usulan

Katalog ini mempertimbangkan inisiatif aplikasi yang diusulkan oleh masing-masing OPD Pemerintah Kabupaten Murung Raya untuk di masa mendatang. Inisiatif-inisiatif tersebut akan berkembang dan bertambah seiring dengan kebutuhan bisnis proses di masing-masing OPD. Berikut merupakan pendetailan inisiatif pengembangan aplikasi kedepannya di Pemerintah Kabupaten Murung Raya, Adapun katalog aplikasi usulan selengkapnya ditunjukkan pada link: https://bit.ly/metadataspbemurungraya.

Tabel 2.1.3.1.1 Katalog Aplikasi Usulan

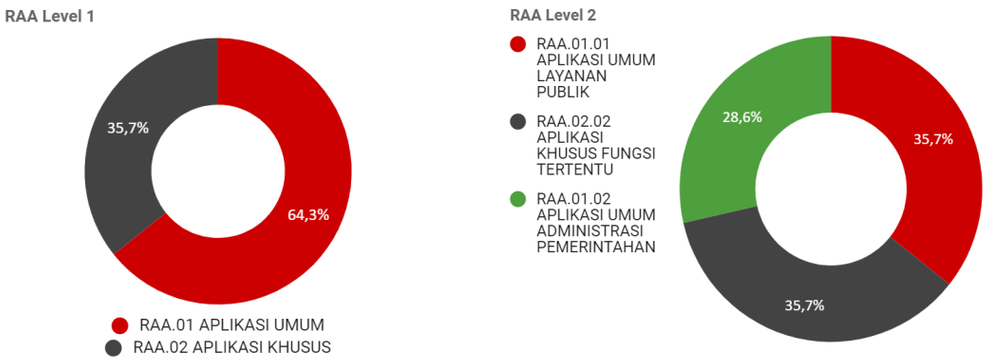
ID Aplikasi	Nama Aplikasi	Uraian Aplikasi	Basis Aplikasi	→ Layanan (Dependency)	→ Data dan Informasi (Dependency)	→ RAA Level 1 (Dependency)	→ RAA Level 2 (Dependency)	→ Unit Operasional Teknologi (Dependency)
MURA-DAA-U 01.02.01	TBIB	Sistem Tugas Belajar dan Ijin Belajar (TBIB)	Web Based	Layanan Administrasi Peningkatan Jenjang Pendidikan ASN	Data Pendidikan ASN	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Badan Kepegawaian dan Sumber Daya Manusia
MURA-DAA-U 01.02.02	e-KGB	Sistem Informasi Kenaikan Gaji Berkala	Web Based	Layanan Kenaikan Gaji Berkala	Data Kenaikan Gaji Berkala	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Badan Kepegawaian dan Sumber Daya Manusia
MURA-DAA-U 01.02.03	SIMPEGNAS	Sistem Informasi Kepegawaian Nasional	Web Based	Layanan Administrasi Kepegawaian	Data Administrasi Kepegawaian	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Badan Kepegawaian dan Sumber Daya Manusia
MURA-DAA-U 01.02.04	e-Persediaan	Sistem Informasi Pengelolaan Barang Persediaan	Web Based	Layanan Pengelolaan Barang Persediaan	Data Barang Persediaan	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Badan Pengelolaan Keuangan dan Aset Daerah
MURA-DAA-U 02.02.01	SI SAPAN (2024)	Sistem Informasi Monitoring Konstruksi Fisik	Web Based	Layanan Monitoring Konstruksi Fisik	Data Monitoring Pembangunan Fisik	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Bagian Administrasi Pembangunan
MURA-DAA-U 01.02.01	e-Regulasi (2024)	Log Aktivitas Pengusulan Produk Hukum Daerah	Web Based	Layanan Regulasi Daerah	Data Regulasi Daerah	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Bagian Hukum
MURA-DAA-U 02.02.01	e-BLUD	Sistem Informasi BLUD	Web Based	Layanan Kebijakan Pengelolaan BUMD dan BLUD	Data Bahan Penyusunan Kebijakan BUMD dan BLUD	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Bagian Perekonomian dan Sumber Daya Alam

ID Aplikasi	Nama Aplikasi	Uraian Aplikasi	Basis Aplikasi	→ Layanan (Dependency)	→ Data dan Informasi (Dependency)	→ RAA Level 1 (Dependency)	→ RAA Level 2 (Dependency)	→ Unit Operasional Teknologi (Dependency)
MURA-DAA-U 01.01.01	Satu Data Murung Raya	Sistem Informasi Satu Data Statistik Murung Raya	Web Based	Layanan Statistik Murung Raya	Data Statistik Murung Raya	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Komunikasi Informatika Statistik dan Persandian
MURA-DAA-U 01.01.02	e-Koperasi dan UMKM	Sistem Informasi Koperasi dan UMKM	Web Based	Layanan Pendataan Koperasi dan UMKM	Data Koperasi dan UMKM	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Koperasi, Usaha Kecil dan Menengah, Perindustrian dan Perdagangan
MURA-DAA-U 01.01.03	e-Sewa Prasarana	Sistem Informasi Sewa Sarana Olahraga	Web Based	Layanan Sewa Sarana Olahraga	Data Sewa Sarana Olahraga	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Pariwisata Pemuda dan Olahraga
MURA-DAA-U 01.01.04	e-Pariwisata	Sistem Informasi Potensi Destinasi Wisata	Web Based	Layanan Potensi Destinasi Wisata	Data Potensi Destinasi Wisata	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Pariwisata Pemuda dan Olahraga
MURA-DAA-U 01.01.05	e-Pelaku Ekraf	Sistem Informasi Pelaku Ekonomi Kreatif	Web Based	Layanan Ekonomi Kreatif	Data Pelaku Ekonomi Kreatif	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Pariwisata Pemuda dan Olahraga
MURA-DAA-U 02.02.01	e-Sarana Hibah	Sistem Informasi Sarana Hibah	Web Based	Layanan Sarana Hibah	Data Sarana Hibah	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Pariwisata Pemuda dan Olahraga
MURA-DAA-U 02.02.02	SiBUMDES	Sistem Informasi Badan Usaha Milik Desa	Web Based	Layanan BUMDES	Data BUMDES	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Pemberdayaan Masyarakat Desa
MURA-DAA-U 01.02.01	SP2D online	SIstem Informasi SP2D Online	Web Based	Layanan Penerbitan SP2D	Data SP2D	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Badan Pengelolaan Keuangan dan Aset Daerah
MURA-DAA-U 01.02.02	e-SAKIP	Sistem Informasi Akuntabilitas Perangkat Daerah (SIAP)	Web Based	Layanan Akuntabilitas Kinerja Organisasi	Data Akuntabilitas Kinerja Organisasi	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Bagian Organisasi
MURA-DAA-U 02.02.01	e-Ketahanan Pangan	Sistem Informasi Ketahanan Pangan	Web Based	Layanan Rekomendasi Keamanan Pangan Segar Layanan Sertifikasi Keamanan Pangan Segar Layanan Perizinan Keamanan Pangan Segar	Data Rekomendasi Keamanan Pangan Segar Data Sertifikasi Keamanan Pangan Segar Data Perizinan Keamanan Pangan Segar	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Ketahanan Pangan
MURA-DAA-U 02.02.02	e-Layanan TIK	Sistem Informasi Layanan Diskominfo Murung Raya	Web Based	Layanan Virtual Private Server	Data Permohonan Layanan TIK	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Komunikasi Informatika Statistik dan Persandian

ID Aplikasi	Nama Aplikasi	Uraian Aplikasi	Basis Aplikasi	→ Layanan (Dependency)	→ Data dan Informasi (Dependency)	→ RAA Level 1 (Dependency)	→ RAA Level 2 (Dependency)	→ Unit Operasional Teknologi (Dependency)
MURA-DAA-U 01.01.01	e-Harga Pangan	Sistem Informasi Harga Pangan	Web Based	Layanan Harga Pangan	Data Harga Pangan	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Koperasi, Usaha Kecil dan Menengah, Perindustrian dan Perdagangan
MURA-DAA-U 01.01.02	e-Pengunjung Wisata	Sistem Informasi Pengunjung Wisata	Web Based	Layanan Potensi Destinasi Wisata	Data Pengunjung Wisata	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Pariwisata Pemuda dan Olahraga
MURA-DAA-U 01.01.03	e-Potensi Investasi	Sistem Informasi Potensi Investasi	Web Based	Layanan Peta Potensi Investasi	Data Peta Potensi Investasi	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu
MURA-DAA-U 01.02.01	e-Arsip	Sistem Informasi Arsip	Web Based	Layanan Pengelolaan Arsip	Data Pengelolaan Arsip	RAA.01 APLIKASI UMUM	RAA.01.02 APLIKASI UMUM ADMINISTRASI PEMERINTAHAN	Dinas Perpustakaan dan Kearsipan
MURA-DAA-U 01.01.01	GIS	Sistem Informasi GIS Area Kumuh	Web Based	Layanan Pencatatan Kawasan Kumuh	Data Kawasan Kumuh	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Perumahan, Kawasan Permukiman dan Pertanahan
MURA-DAA-U 02.02.01	e-Pasar Kerja	Sistem Informasi Pasar Kerja	Mobile	Layanan Penerbitan Kartu Pencari Kerja (AK.1)	Data Jumlah Pencari Kerja Data Jumlah Lowongan dan Kesempatan Kerja	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Tenaga Kerja dan Transmigrasi
MURA-DAA-U 02.02.02	e-Pemuda	Sistem Informasi Organisasi Pemuda	Web Based	Layanan Organisasi Pemuda	Data Organisasi Pemuda	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Pariwisata Pemuda dan Olahraga
MURA-DAA-U 02.02.03	e-Wirausaha	Sistem Informasi Wirausaha Muda	Web Based	Layanan Wirausaha Muda	Data Wirausaha Muda	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Pariwisata Pemuda dan Olahraga
MURA-DAA-U 02.02.04	SiTeGu	Sistem Informas Tepat Guna	Web Based	Layanan Teknologi Tepat Guna	Data Teknologi Tepat Guna	RAA.02 APLIKASI KHUSUS	RAA.02.02 APLIKASI KHUSUS FUNGSI TERTENTU	Dinas Pemberdayaan Masyarakat Desa
MURA-DAA-U 01.01.01	e-Parkir	Sistem Informasi Parkir	Web Based	Layanan Permohonan Perizinan Parkir	Data Perizinan Parkir	RAA.01 APLIKASI UMUM	RAA.01.01 APLIKASI UMUM LAYANAN PUBLIK	Dinas Perhubungan

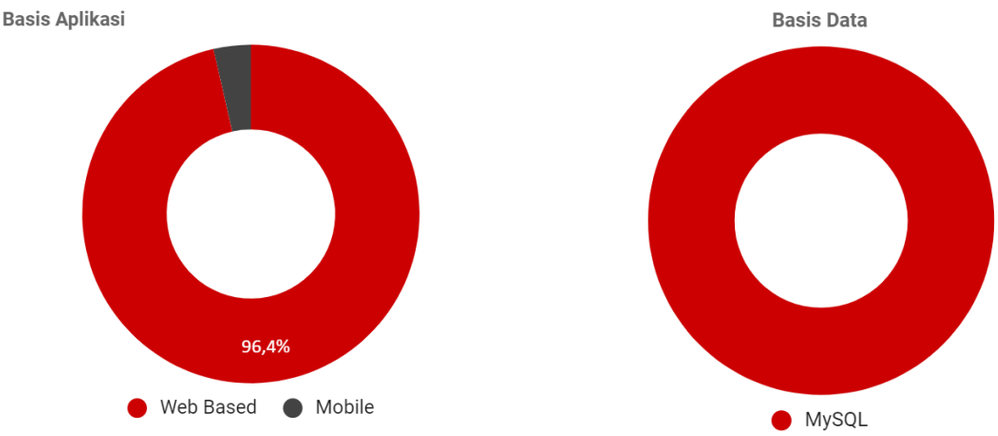
2.1.3.2. Analisis Diagram Aplikasi Usulan

Analisa terhadap kondisi aplikasi usulan dapat dijabarkan sebagai berikut:



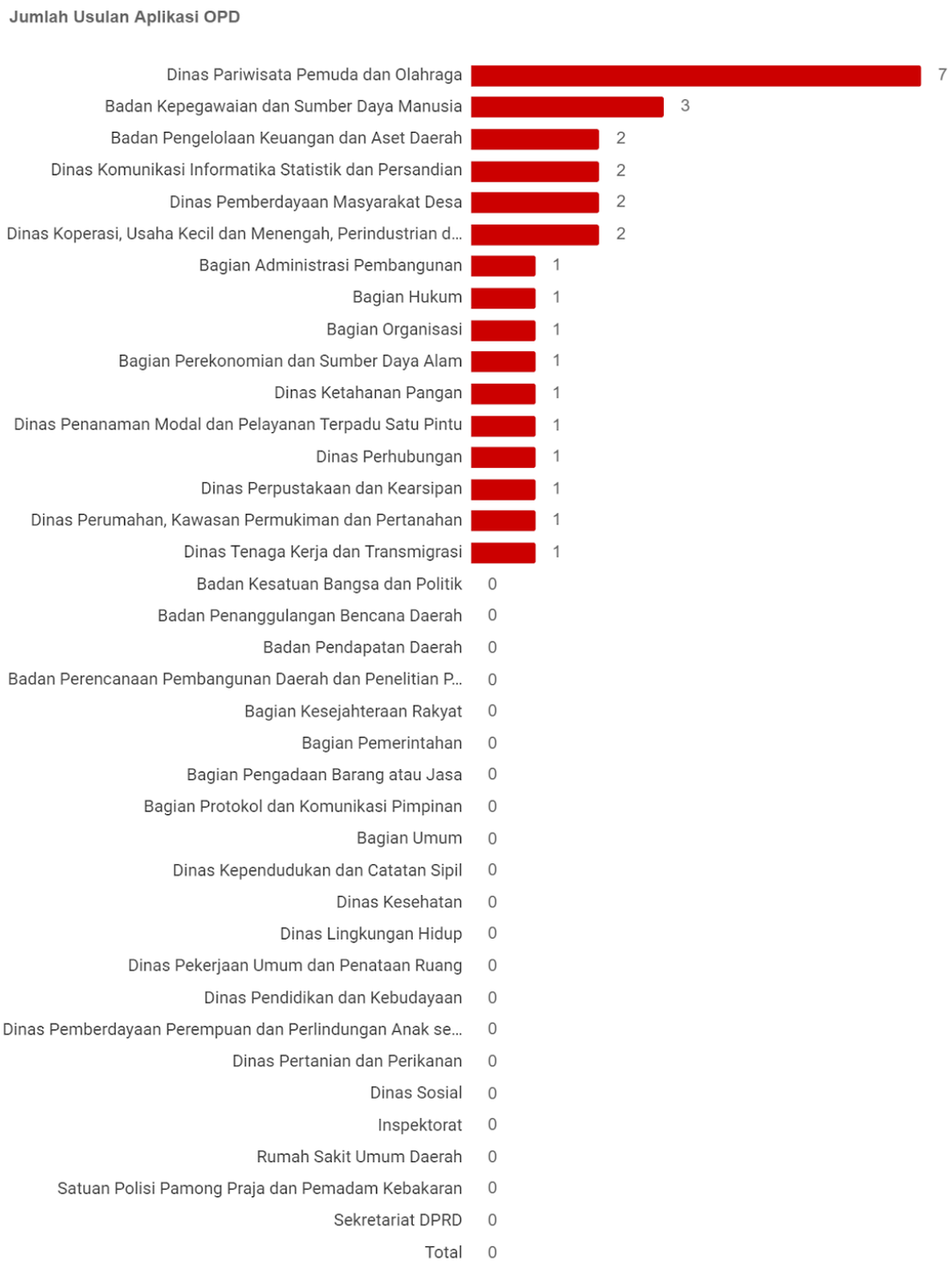
Grafik 2.1.3.2.1 Referensi Arsitektur Aplikasi Nasional

Merujuk pada Grafik 2.1.3.2.1. menunjukkan referensi arsitektur aplikasi usulan pada RAA Level 1 dan RAA Level 2. Dari grafik tersebut dapat dilihat bahwa sesuai dengan Referensi Arsitektur Nasional Level 1 terdapat 64,3% (18 Aplikasi) merupakan RAA.01 Aplikasi Umum dan 35,7% (10 Aplikasi) merupakan RAA.02 Aplikasi Khusus, selanjutnya Referensi Arsitektur Nasional Level 2 Aplikasi usulan terbagi menjadi 3 yaitu 35,7% (10 Aplikasi) merupakan RAA.01.01 Aplikasi Umum Layanan Publik, 28,6% (8 Aplikasi) merupakan RAA.01.02 Aplikasi Umum Administrasi Pemerintahan dan 35,7% (10 Aplikasi) merupakan RAA.02.02 Aplikasi Khusus Fungsi Tertentu. RAA Nasional Paling Banyak pada RAA.02 Aplikasi Umum. Sehingga dapat disimpulkan bahwa jenis aplikasi yang paling banyak diusulkan adalah aplikasi umum yang menunjang layanan umum di masyarakat maupun pemerintahan.



Grafik 2.1.3.2.2. Teknologi Platform Aplikasi Usulan

Berdasarkan Basis aplikasi yang digunakan dalam aplikasi usulan 96,4% (27 Aplikasi) merupakan Web Based dan 3,6% (1 Aplikasi) merupakan Mobile untuk Basis Datanya 100% (28 Aplikasi) merupakan MySQL. Berdasarkan kondisi aplikasi yang diusulkan oleh OPD semuanya berbasis Website, karena mudah untuk di akses di berbagai platform, selanjutnya perlu dipastikan jumlah web programmer dapat mengakomodir pengembangan aplikasi usulan tersebut.



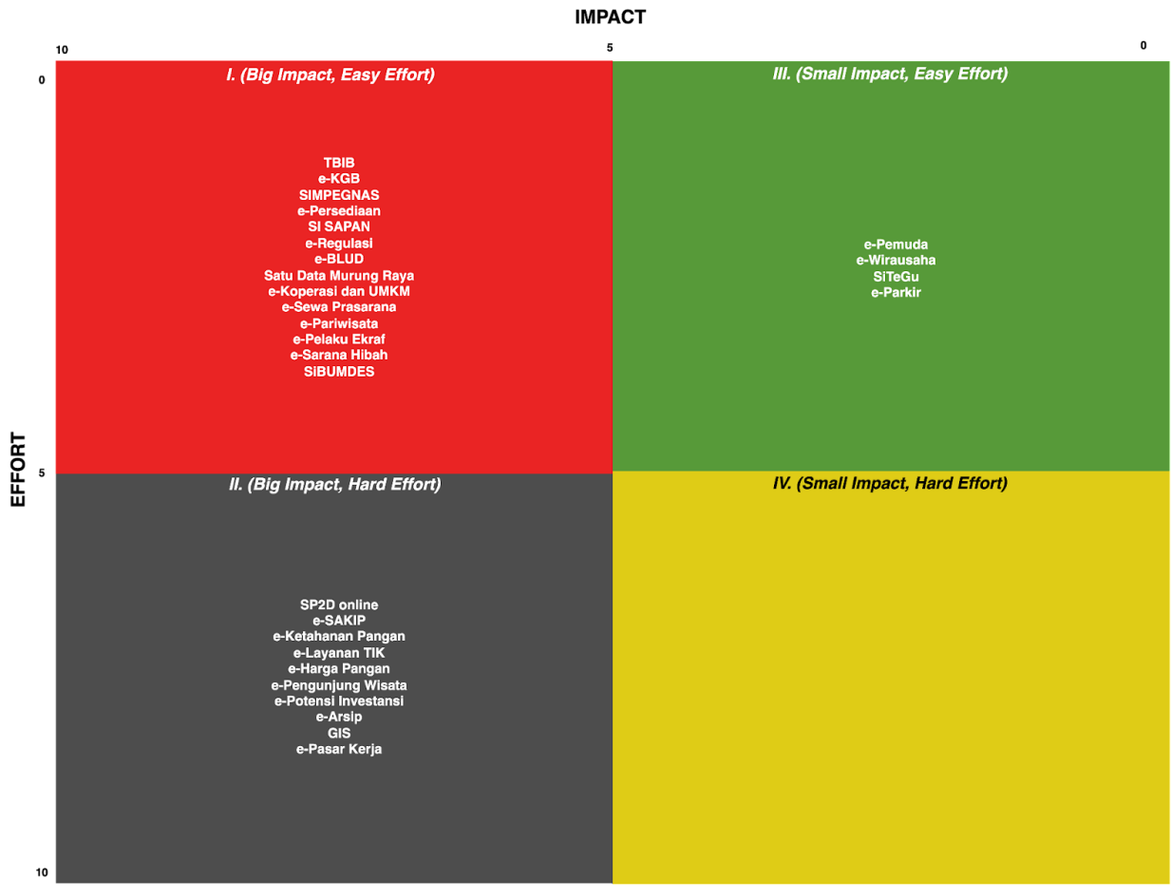
Grafik 2.1.3.2.3. OPD Pengelola Aplikasi Usulan

Merujuk pada grafik tersebut dapat dilihat OPD yang paling banyak dalam melakukan usulan yaitu Dinas Pariwisata Pemuda dan Olahraga, hal ini perlu dilakukan agar layanan di OPD tersebut bisa terdigitalisasi dan terdapat beberapa OPD yang tidak membutuhkan pengembangan aplikasi untuk 5 tahun kedepan.

2.1.3.3. Analisis *Effort Impact*

Usulan aplikasi yang direkomendasikan dapat dijadikan dasar untuk pengelolaan SPBE yang sesuai dengan kebutuhan instansi Pemerintah Kabupaten Murung Raya dan

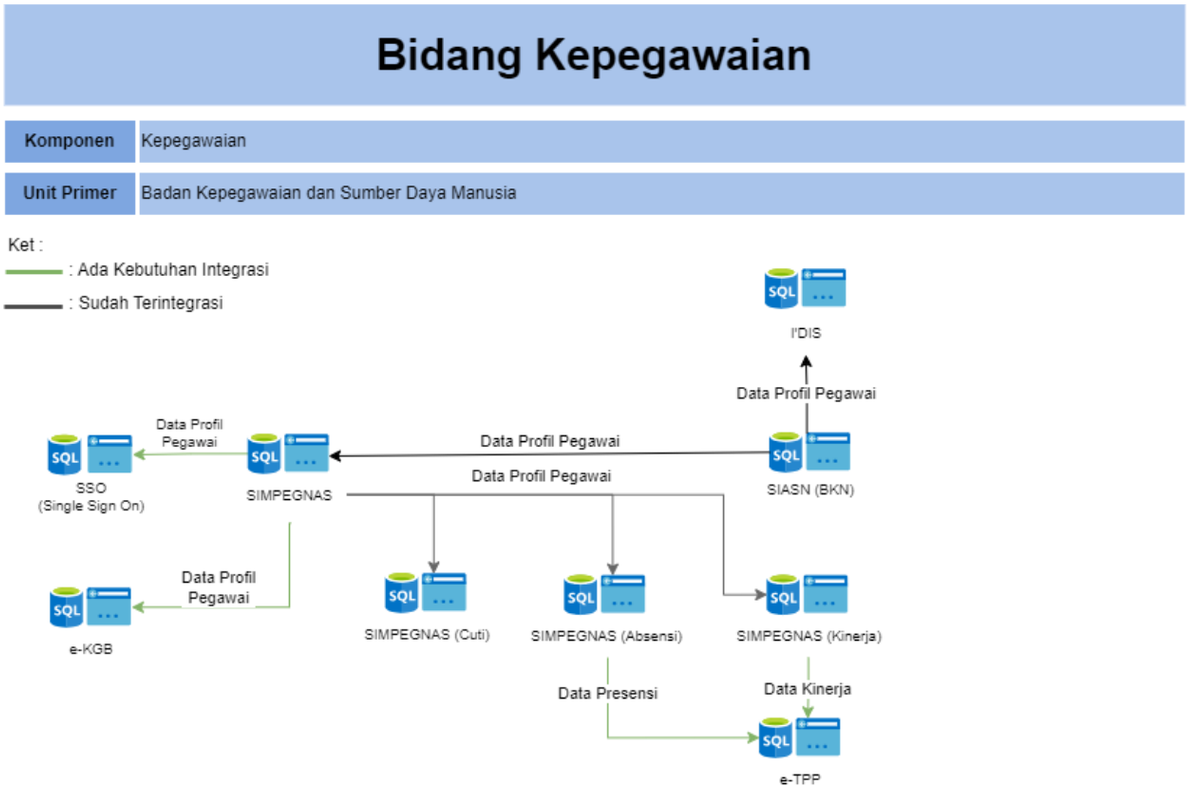
memberikan arah bagi pengembangan teknologi informasi yang mampu memberikan kontribusi positif bagi penyelesaian berbagai permasalahan Pemerintah Kabupaten Murung Raya. Berdasarkan usulan kebutuhan aplikasi yang telah dijelaskan sebelumnya. Selanjutnya perlu dilakukan analisis untuk strategi implementasinya dengan pertimbangan arahan strategis dan kapabilitas anggaran Pemerintah Kabupaten Murung Raya. Secara umum dalam implementasi perencanaan SPBE kedepan diprioritaskan ke dalam 4 kuadran utama, yaitu: Kuadran 1 (*High Impact-Low Effort*), Kuadran 2 (*High Impact-High Effort*), Kuadran 3 (*Low Impact-Low Effort*), Kuadran 4 (*Low Impact-High Effort*). Prioritas pengembangan aplikasi disusun menggunakan *matriks Effort-Impact*, seperti ditunjukkan pada gambar dibawah ini:



Gambar 2.1.2.1. *Matriks Effort-Impact*

2.1.4. Diagram Kebutuhan Integrasi Aplikasi

Integrasi aplikasi ini dimulai karena adanya kebutuhan pertukaran data/informasi antara aplikasi yang satu dengan aplikasi yang lain. Kebutuhan dari operasional pemerintahan mengharapkan data/informasi yang dipunyai oleh sebuah aplikasi dari suatu Perangkat Daerah harus dikirimkan ke aplikasi lain yang dimiliki Perangkat Daerah yang lain. Kebutuhan pertukaran data/informasi dapat berlaku dalam skala lebih luas, seperti: integrasi antara Pemerintah Kabupaten Murung Raya dengan instansi pusat untuk kepentingan pelaporan dan sebagainya. Berikut ini digambarkan aplikasi yang sudah terintegrasi di lingkungan Pemerintah Kabupaten Murung Raya.



Gambar 2.1.4.1. Usulan Integrasi Antar Aplikasi Bidang Urusan Kepegawaian Pemerintah Kabupaten Murung Raya

Gambar 2.1.4.1. menunjukkan diagram Integrasi antar aplikasi Pemerintah Kabupaten Murung Raya. Dapat dilihat terdapat beberapa aplikasi yang digunakan dalam bidang kepegawaian yaitu aplikasi SSO (Single Sign On), e-KGB, SIMPEGNAS (Cuti), SIMPEGNAS (Absensi), i'DIS, SIASN (BKN), SIMPEGNAS (Kinerja) dan e-TPP. Berikut Tabel Integrasi Aplikasi di bidang kepegawaian :

Tabel 2.1.4.1 Usulan Integrasi Antar Aplikasi Bidang Urusan Kepegawaian Pemerintah Kabupaten Murung Raya

No	Aplikasi	Data Integrasi	Status Integrasi
1	SIMPEGNAS integrasi SSO *(Single Sign On)*	Data Profil Pegawai	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
2	SIMPEGNAS integrasi e-KGB	Data Profil Pegawai	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
3	SIMPEGNAS integrasi SIMPEGNAS (Cuti)	Data Profil Pegawai	Sudah terintegrasi
4	SIMPEGNAS integrasi SIMPEGNAS (Absensi)	Data Profil Pegawai	Sudah terintegrasi
5	SIMPEGNAS integrasi SIMPEGNAS (Kinerja)	Data Profil Pegawai	Sudah terintegrasi
6	SIMPEGNAS (Absensi) integrasi e-TPP	Data Presensi	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
7	SIMPEGNAS (Kinerja)	Data Kinerja	Belum terintegrasi, direncanakan akan ada kebutuhan

No	Aplikasi	Data Integrasi	Status Integrasi
	integrasi e-TPP		integrasi
8	SIASN (BKN) integrasi SIMPEGNAS	Data Profil Pegawai	Sudah terintegrasi
9	SIASN (BKN) integrasi i'DIS	Data Profil Pegawai	Sudah terintegrasi

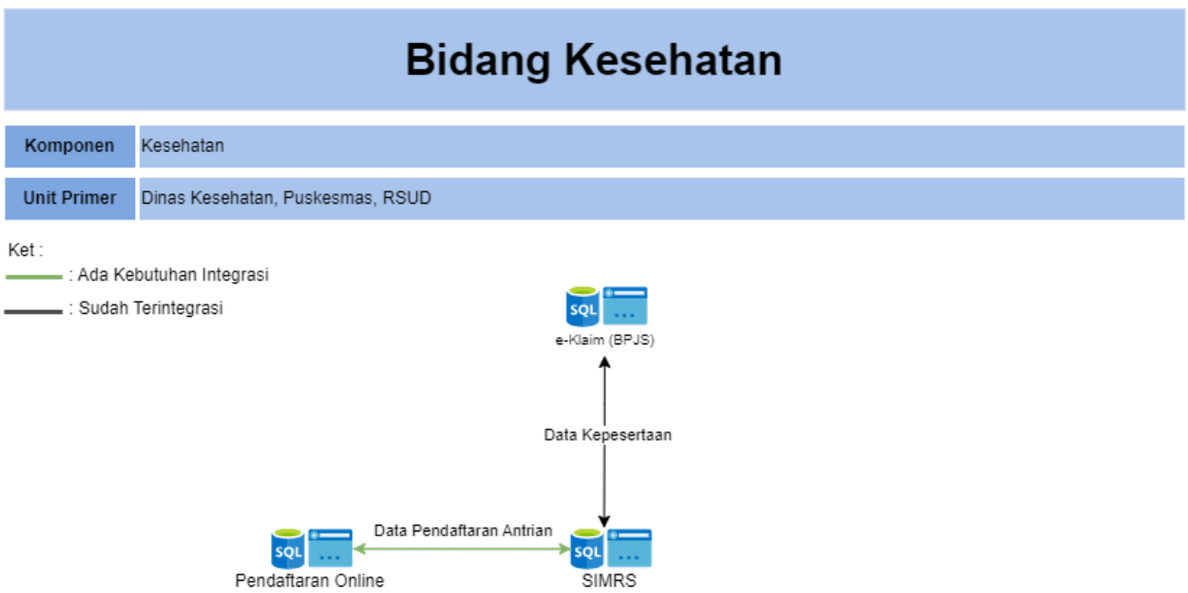
Gambar 2.1.4.2. Usulan Integrasi Antar Aplikasi Bidang Urusan Perencanaan, Penganggaran, Keuangan dan Aset Pemerintah Kabupaten Murung Raya

Gambar 2.1.4.2. menunjukkan diagram Integrasi antar aplikasi Pemerintah Kabupaten Murung Raya. Dapat dilihat terdapat beberapa aplikasi yang digunakan dalam bidang Perencanaan, Penganggaran, Keuangan dan Aset yaitu aplikasi e-Audit, SIPD RI, e-Retribusi, Bank Kalteng, SIMDA Pendapatan, e-Monev, SIMDA BMD, SIM PBB dan e-SPPT. Berikut Tabel Integrasi Aplikasi di bidang Perencanaan, Penganggaran, Keuangan dan Aset :

Tabel 2.1.4.2 Usulan Integrasi Antar Aplikasi Bidang Urusan Perencanaan, Penganggaran, Keuangan dan Aset Pemerintah Kabupaten Murung Raya

No	Aplikasi	Data Integrasi	Status Integrasi
1	SIPD RI integrasi e-Audit	Data Capaian Realisasi Anggaran	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi

No	Aplikasi	Data Integrasi	Status Integrasi
2	SIPD RI integrasi Bank Kalteng	Data Pembayaran	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
3	SIPD RI integrasi e-Monev	Data Capaian Realisasi Anggaran	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
4	SIPD RI integrasi SIMDA BMD	Data Nilai Aset	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
5	e-Retribusi integrasi SIMDA Pendapatan	Data Retribusi	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
6	SIM PBB integrasi SIMDA Pendapatan	Data Pajak	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
7	e-SPPT integrasi SIMDA Pendapatan	Data Pajak	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
8	SIMDA Pendapatan integrasi Bank Kalteng	Data Pembayaran	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
9	SIMDA Pendapatan integrasi e-Audit	Data Monitoring Pajak dan Retribusi	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi



Gambar 2.1.4.3. Usulan Integrasi Antar Aplikasi Bidang Urusan Kesehatan Pemerintah Kabupaten Murung Raya

Gambar 2.1.4.3. menunjukkan diagram Integrasi antar aplikasi Pemerintah Kabupaten Murung Raya. Dapat dilihat terdapat beberapa aplikasi yang digunakan dalam bidang kesehatan yaitu aplikasi e-Klaim (BPJS), SIMRS dan Pendaftaran Online. Berikut Tabel Integrasi Aplikasi di bidang kesehatan :

Tabel 2.1.4.3 Usulan Integrasi Antar Aplikasi Bidang Urusan Kesehatan Pemerintah Kabupaten Murung Raya

No	Aplikasi	Data Integrasi	Status Integrasi

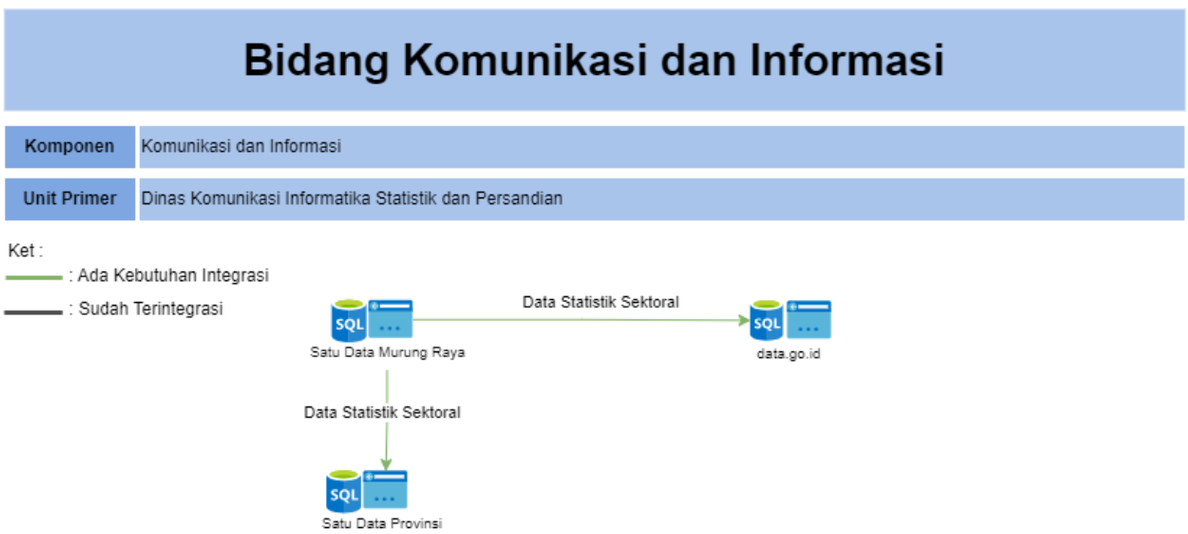
1	e-Klaim (BPJS) integrasi SIMRS	Data Kepesertaan	Sudah terintegrasi
2	Pendaftaran Online integrasi SIMRS	Data Pendaftaran Antrian	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi

Gambar 2.1.4.4. Usulan Integrasi Antar Aplikasi Bidang Urusan Perizinan Pemerintah Kabupaten Murung Raya

Gambar 2.1.4.4. menunjukkan diagram Integrasi antar aplikasi Pemerintah Kabupaten Murung Raya. Dapat dilihat terdapat beberapa aplikasi yang digunakan dalam bidang perizinan yaitu aplikasi OSS dan TTE . Berikut Tabel Integrasi Aplikasi di bidang Perizinan :

Tabel 2.1.4.4 Usulan Integrasi Antar Aplikasi Bidang Urusan Perizinan Pemerintah Kabupaten Murung Raya

No	Aplikasi	Data Integrasi	Status Integrasi
1	OSS integrasi TTE	Sertifikat Elektronik	Sudah Terintegrasi

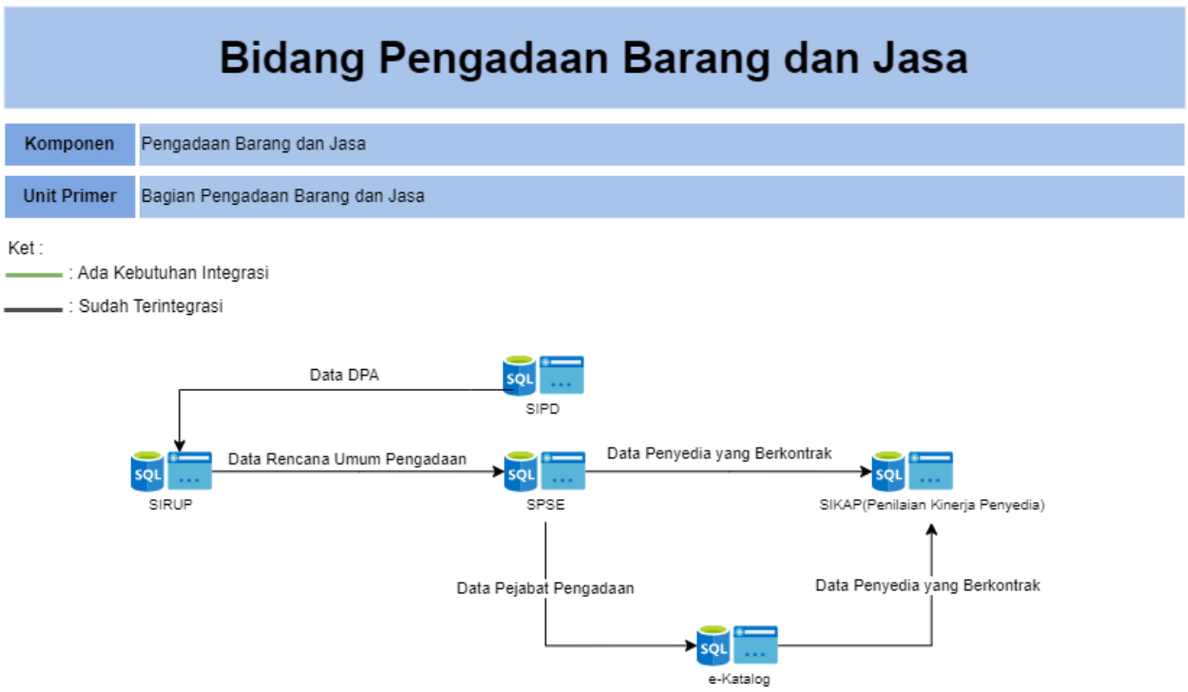


Gambar 2.1.4.5. Usulan Integrasi Antar Aplikasi Bidang Urusan Komunikasi dan Informasi Pemerintah Kabupaten Murung Raya

Gambar 2.1.4.5. menunjukkan diagram Integrasi antar aplikasi Pemerintah Kabupaten Murung Raya. Dapat dilihat terdapat beberapa aplikasi yang digunakan dalam bidang Komunikasi dan Informasi yaitu aplikasi Satu Data Murung Raya, Satu Data Provinsi dan data.go.id. Berikut Tabel Integrasi Aplikasi di bidang Komunikasi dan Informasi :

Tabel 2.1.4.5 Usulan Integrasi Antar Aplikasi Bidang Urusan Komunikasi dan Informasi Pemerintah Kabupaten Murung Raya

No	Aplikasi	Data Integrasi	Status Integrasi
1	Satu Data Murung Raya integrasi data.go.id	Data Statistik Sektoral	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi
2	Satu Data Murung Raya integrasi Satu Data Provinsi	Data Statistik Sektoral	Belum terintegrasi, direncanakan akan ada kebutuhan integrasi



Gambar 2.1.4.6. Usulan Integrasi Antar Aplikasi Bidang Urusan Pengadaan Barang dan Jasa Pemerintah Murung Raya

Gambar 2.1.4.6. menunjukkan diagram Integrasi antar aplikasi Pemerintah Kabupaten Murung Raya. Dapat dilihat terdapat beberapa aplikasi yang digunakan dalam bidang Pengadaan Barang dan Jasa yaitu aplikasi SIPD, SIRUP, SPSE, e-Katalog dan SIKAP (Penilaian Kinerja Penyedia). Berikut Tabel Integrasi Aplikasi di bidang Pengadaan Barang dan Jasa :

Tabel 2.1.4.6 Usulan Integrasi Antar Aplikasi Bidang Urusan Pengadaan Barang dan Jasa Pemerintah Kabupaten Murung Raya

No	Aplikasi	Data Integrasi	Status Integrasi
1	SIPD integrasi SIRUP	Data DPA	Sudah terintegrasi
2	SIRUP integrasi SPSE	Data Rencana Umum Pengadaan	Sudah terintegrasi
3	SPSE integrasi SIKAP (Penilaian Kinerja Penyedia)	Data Penyedia yang Berkontrak	Sudah terintegrasi
4	SPSE integrasi e-Katalog	Data Pejabat Pengadaan	Sudah terintegrasi
5	e-Katalog integrasi SIKAP (Penilaian Kinerja Penyedia)	Data Penyedia yang Berkontrak	Sudah terintegrasi

2.1.5. Portal Layanan Terpadu Pemerintah Kabupaten Murung Raya

Jenis layanan yang bervariasi di Pemerintah Kabupaten Murung Raya menjadi tantangan pengguna (ASN dan masyarakat) dalam memanfaatkan layanan SPBE. Hal ini menjadi perhatian karena pengguna harus mengingat banyaknya laman *web* dan akun login sesuai dengan layanan SPBE yang ingin digunakan. Dengan adanya portal layanan yang mengumpulkan berbagai layanan digital, memudahkan masyarakat dan juga ASN Internal untuk mengakses berbagai layanan hanya dalam satu portal saja. Gambar dibawah merupakan portal layanan Pemerintah Kabupaten Murung Raya yang dapat dibuat untuk menyatukan berbagai layanan yang sudah terintegrasi.

Gambar 2.1.5.1. Arsitektur Murung Raya Smart Services Portal Layanan Terpadu

Tabel 2.1.5.1. Daftar Layanan Murung Raya Smart Services Portal Layanan Terpadu

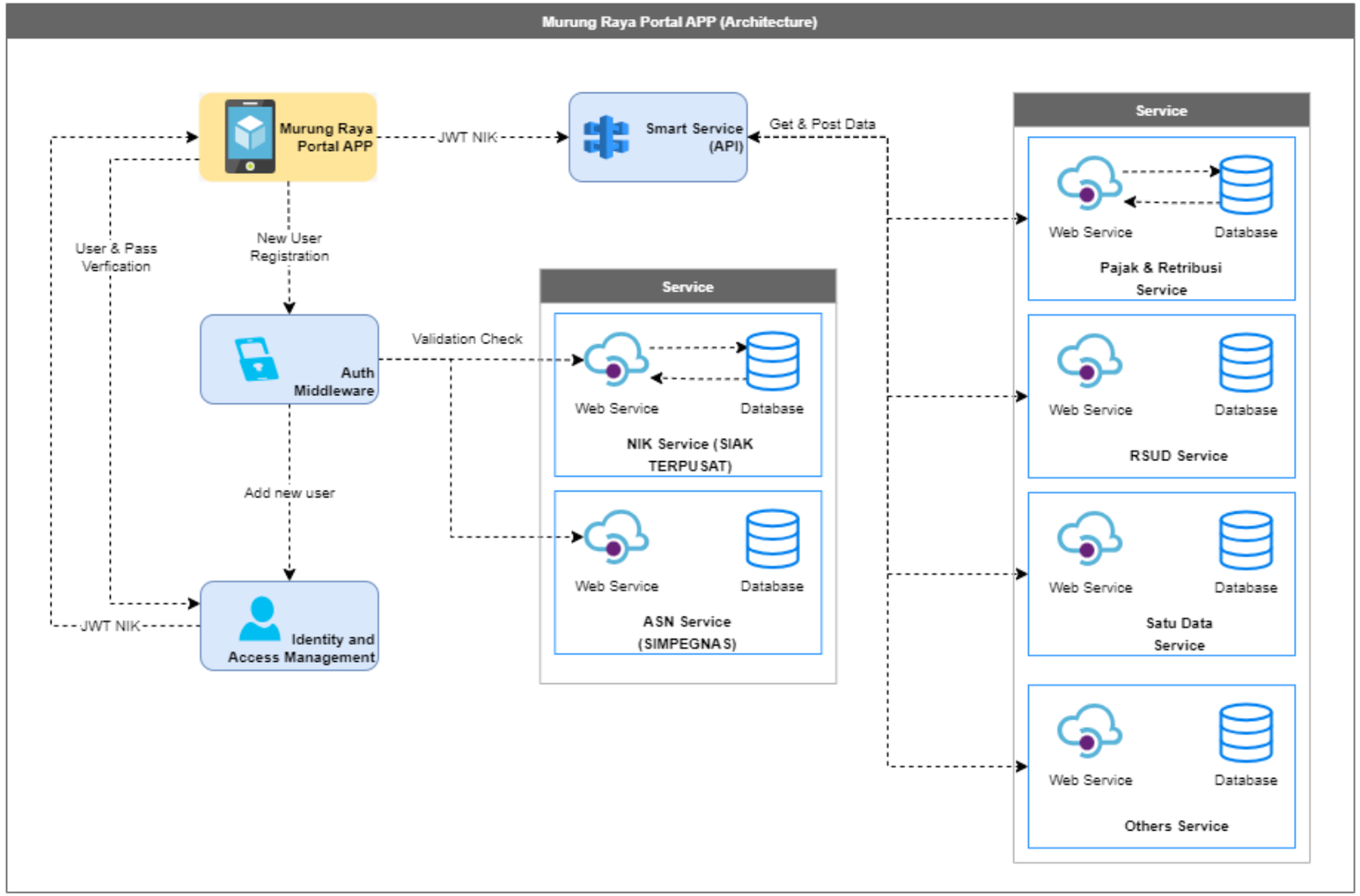
#	Layanan	Sub Layanan	Aplikasi
Layanan Publik			
1	Pengumuman		Pengumuman Daerah Murung Raya
2	Berita dan Informasi		Portal Berita Murung Raya
3	CCTV		CCTV Online Murung Raya
4	Titik Wifi publik		Wifi Publik Murung Raya

#	Layanan	Sub Layanan	Aplikasi
5	Event		Event Murung Raya
6	Iklan Layanan Masyarakat		-
7	Kependudukan	Antrian Online	-
		Layanan Kependudukan	SIAK
8	Ketenagakerjaan	Info Loker	KarirHub
		Info Pelatihan	-
9	Pendidikan	Informasi Fasilitas Pendidikan	DAPODIK
		PPDB Online	-
10	Kesehatan	Pendaftaran Online	AMANG RSUD
		Info Bed	AMANG RSUD
		Jadwal Dokter	AMANG RSUD
		Antrian Online	AMANG RSUD
		Pendaftaran Pasien Puskesmas	-
11	Hukum	Diseminasi Kebijakan	JDIH dan JDIHN
12	Penanaman Modal	Peluang Investasi	-
		Perizinan	OSS
		Perizinan Penelitian	-
13	Pajak & Retribusi	Pembayaran Pajak	My-BPHTB SAMPIAN SIMPATDA SIMPBB
		Uji Kendaraan Bermotor	SIM PKB
		Informasi Pajak	SISMIOP
		Retribusi	SIMDA Pendapatan
14	Marketplace	Data Koperasi	-
		Harga Pangan	-
		UMKM	-
15	Pariwisata	Destinasi Wisata	Rekreasi Murung Raya
16	Satu Data	Data Statistik	Satu Data Murung Raya
17	Aduan Masyarakat	Aduan Umum	SP4N Lapor SAPA
		Aduan Nomor	-
18	PPID	PPID	PPID Murung Raya Murung Raya Dalam Angka
19	Transportasi	Informasi Transportasi	API
20	Social Media	Podcast	-
		Instagram	-
21	Televisi	TV Streaming	-
22	Scan QR		-
23	Agenda Perangkat Daerah		-
24	Standar Pelayanan Masyarakat	SPM	-
25	Survei Kepuasan Masyarakat	SKM	-
Layanan Internal Pemerintahan			
26	Pengumuman ASN		
27	Persuratan	Persuratan	SRIKANDI
		TTE	TTE

#	Layanan	Sub Layanan	Aplikasi
28	Kepegawaian	Profil Kepegawaian	SIASN
		Presensi	SIMPEGNAS (Presensi)
		Cuti dan Izin	SIMPEGNAS (Cuti)
		Pengembangan Kompetensi	SIMPEGNAS (e-Kompeten)
		Kinerja Harian	SIMPEGNAS (e-Kinerja)
		Kenaikan Pangkat	SIMPEGNAS (Kenaikan Pangkat)
29	Layanan TIK	Helpdesk TIK	-
30	Dashboard Pimpinan		-
31	Knowledge Management System		-
32	Push Notification		Firebase
33	Login Page		Keycloack
34	About		
35	FAQ		

Murung Raya *Smart Services* perlu dikembangkan secara bertahap dan dapat dibagi menjadi 4 tahapan. Pengembangan Murung Raya *Smart Services* disesuaikan dengan dependensi dari berbagai aplikasi yang sudah ada. Selain itu dalam proses perancangan, desain ini harus disusun prioritas berdasarkan dari analisis kompleksitas data dan fitur di masing-masing layanan. Pengembangan tahap pertama dimulai dengan mengembangan *platform* dasar portal layanan. Tahap kedua mengintegrasikan layanan digital yang sudah didukung dengan *API*. Tahap ketiga membuat *API* dari layanan digital yang belum didukung dengan *API*. Tahap keempat terus melakukan *continous improvement* dengan melakukan penambahan layanan-layanan baru yang dibutuhkan dalam meningkatkan pelayanan di Pemerintah Kabupaten Murung Raya.

Murung Raya *Smart Services* berperan sebagai aplikasi satelit *(satellite app)/aggregator* guna memindahkan *user interface* di sisi pengguna yang ada di masing-masing aplikasi utama (*main apps*) ke dalam portal. Portal tersebut menggunakan teknologi *Single Sign On* (SSO) seperti: *Lightweight Directory Access Protocol* (LDAP)/*Keycloak* agar memudahkan pengguna yang terbagi menjadi 4 (empat) *roles*: admin, ASN Pemerintah Kabupaten Murung Raya, warga Murung Raya dan warga non Murung Raya yang dijelaskan pada gambar dibawah ini :



Gambar 2.1.5.2. Arsitektur Portal Aplikasi Murung Raya *Smart Services*

2.2. Arsitektur Infrastruktur dan Keamanan

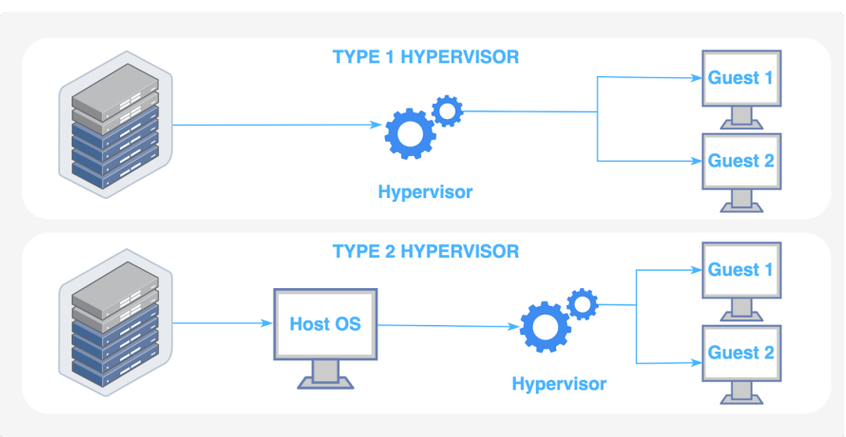
2.2.1. Tren Teknologi dan Praktek Terbaik (*Best Practice*)

2.2.1.1. Teknologi Virtualisasi

Virtualisasi merupakan pembagian pusat data fisik menjadi beberapa *virtual* pusat data yang lebih kecil dengan tujuan untuk mengoptimalkan penggunaan *resource* pusat data fisik. Dalam virtualisasi pusat data, *resource* dari pusat data fisik disembunyikan dari pengguna virtual pusat data, dan hanya admin yang bisa melihat *resource* asli dari pusat data fisik. Perbedaan arsitektur pusat data modern dengan pust data tradisional (lama) adalah virtualisasi pusat data menggunakan *hypervisor* yang digunakan untuk membagi *resource* pusat data fisik ke dalam banyak *Virtual Environment* (VE) atau yang sering disebut *Virtual Private pusat data* (VPS), *Guests, Instance, Container* atau *Emulation.*

Sebuah server fisik bisa dibuat banyak virtual pusat data, *VPS, host* dengan spesifikasi *hardware* yang bisa ditentukan (asal tidak melebihi *resource* fisik) mulai dari jumlah *core CPU, RAM, Network Interface, Storage, BIOS* dll. Dengan menggunakan teknologi virtualisasi *resource* pusat data fisik dapat dimanfaatkan secara optimal karena kita bisa meng-*install* beberapa sistem operasi yang akan dikonfigurasi menjadi pusat data sesuai kebutuhan tanpa membeli *hardware* baru.

Agar dapat mendukung implementasi virtualisasi pusat data, *CPU* dari sebuah pusat data harus mendukung teknologi virtualisasi, dan *hardware* saat ini sudah mendukung teknologi virtualisasi bahkan untuk komputer biasa pun sudah mendukung teknologi virtualisasi. Pada teknologi virtualisasi, sebuah pusat data dipecah ke dalam *virtual environment* dan setiap *virtual environment* dapat di-*install* sistem operasi yang berbeda dari sistem operasi pusat data fisik atau sistem operasi dari *virtual environment* lainnya. Ketika *virtual environment* berjalan *resource* yang digunakan tidak dapat diidentifikasi sehingga dalam teknologi virtualisasi diperlukan sebuah *Hypervisor* yang mengkoordinasi komunikasi dan instruksi antara *virtual environment* dengan *resource* fisik/*physical resource. Hypervisor* inilah yang dipegang oleh administrator dari sebuah pusat data yang mengimplementasikan teknologi virtualisasi untuk mengatur *virtual environment*.



Gambar 2.2.1.1.1 Dua Jenis *Hypervisor*

Terdapat 2 jenis h*ypervisor* dalam dunia virtualisasi saat ini:

- *Hypervisor Type 1 (Bare Metal Hypervisor)*

  Hypervisor ini mengakses langsung *hardware* fisik tanpa bantuan sistem operasi, dan biasanya untuk menggunakan *hypervisor* tipe 1 kita harus menginstall *hypervisor* sebagai sistem operasi bukan diinstall dalam sistem operasi. Contoh *Hypervisor* Type 1 diantaranya: KVM, *Red hat Enterprise Virtualisation (RHEV), XEN/Citrix* Xenpusat data, *Hyper-V,V Mware vSphere/ESXi.*

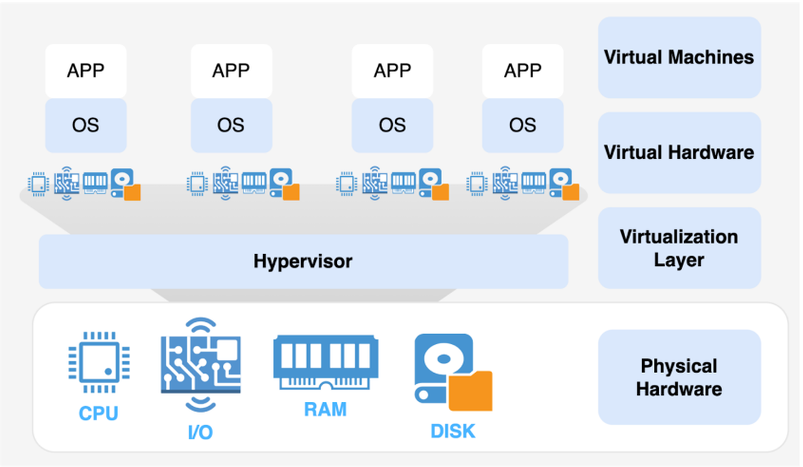
- *Hypervisor Tipe 2 (Hosted Hypervisor)*

  Jenis *hypervisor* ini memerlukan sistem operasi untuk berjalan, karena jenis *hyper visor* ini berjalan di atas sistem operasi. Contoh *Hypervisor Type 2 d*iantaranya: *Vmware Work station, VMware Player,* dan *Virtualbox.*

Perkembangan implementasi dari teknologi virtualisasi meliputi pusat data, *storage*, DC & DRC, serta perkembangan terakhir yakni *container*.

1. Virtualisasi pusat data

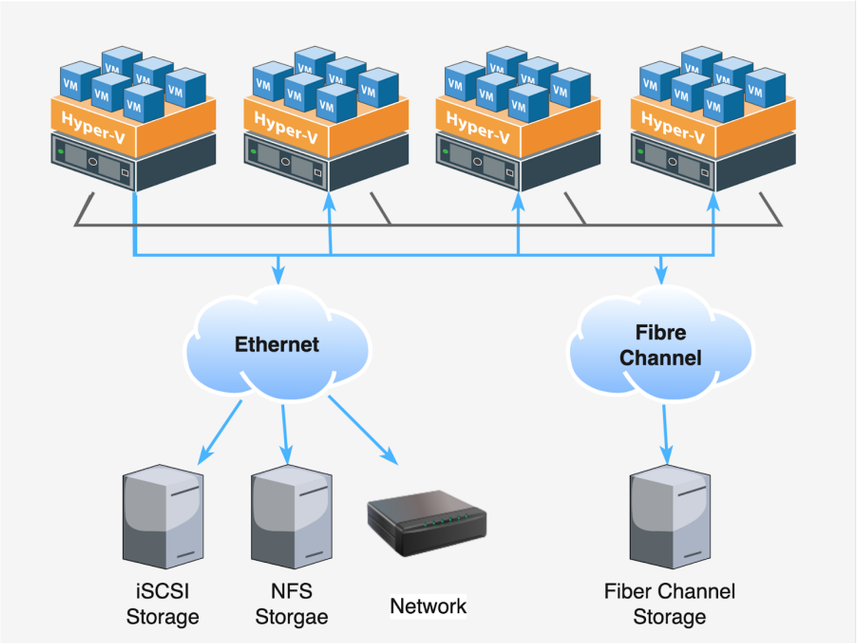
   Adalah penggunaan teknologi virtualisasi dengan tujuan untuk memecah *resource* fisik pusat data kedalam beberapa virtual pusat data yang nantinya akan diinstall berbagai macam sistem operasi sesuai kebutuhan atau bisa juga virtual pusat data ini dijual/disewakan oleh pihak *hosting*. Kita sering mendengarnya dengan istilah VPS (*Virtual Private pusat data*) *hosting*.



Gambar 2.2.1.1.2. Lapisan-lapisan Teknologi Virtualisasi pusat data

Virtualisasi pusat data adalah melakukan konsolidasi dan melakukan pengurangan jumlah pusat data dalam bentuk fisik, dengan menciptakan mesin virtual dalam jumlah banyak yang ditempatkan di beberapa *host* fisik, menggunakan *storage* dan jaringan.

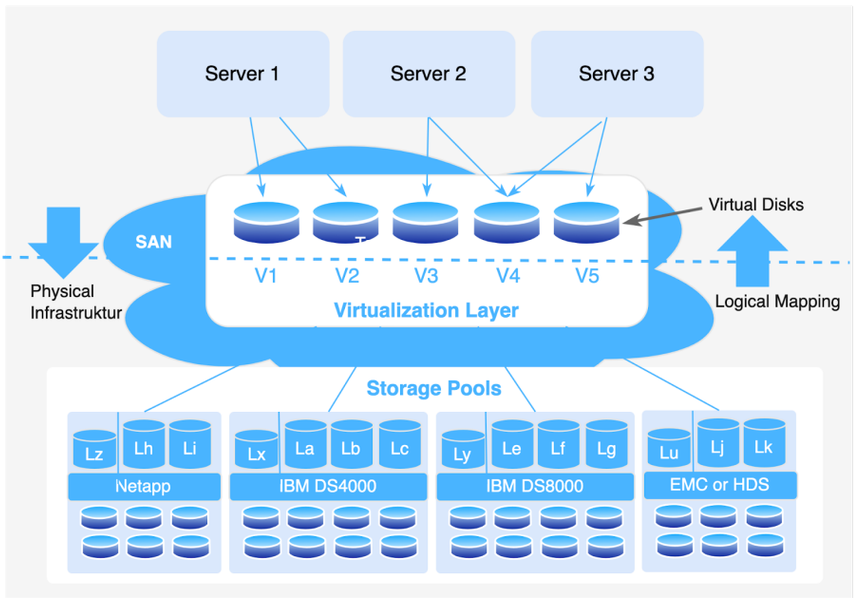
Virtualisasi memudahkan dalam perancangan pusat data dengan tingkat ketersediaan yang tinggi (*high-availability*) dengan teknik *clustering*, redudansi, dan replikasi.



Gambar 2.2.1.1.3 Topologi *Virtualisasi Pusat Data* dan *Storage* di Pusat Data

2. *Virtualisasi Storage*

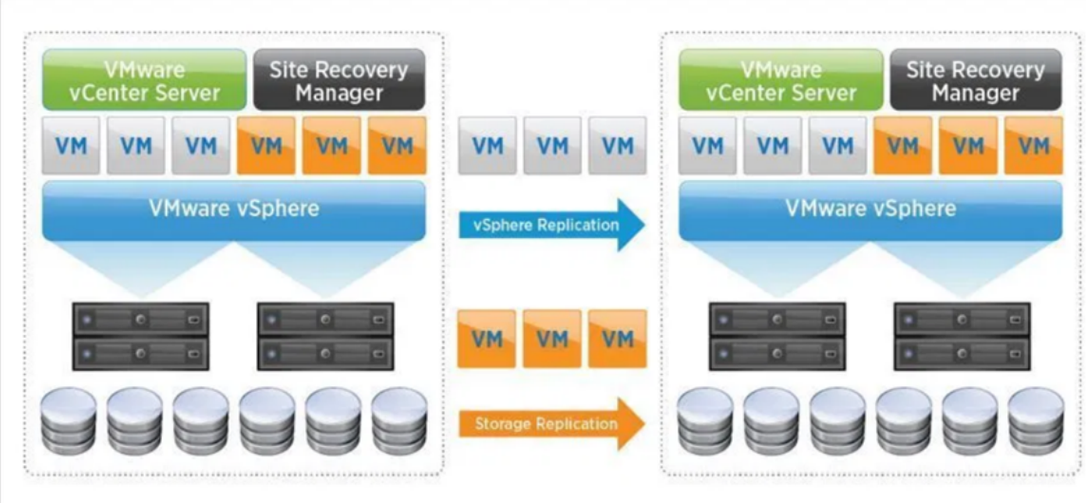
Virtualisasi storage menyediakan media penyimpan (*storage*) yang terisolasi (terpisah dari *resource* fisik), aman dan mudah dalam *failover* dan *backup*. Salah satu contoh implementasi virtualisasi *storage* yang gampang kita lihat adalah fasilitas *cloud storage*, seperti: *DropBox* dan *Google drive* yang menyediakan/menyewakan *cloud storage* bagi pelanggannya dengan menawarkan *flexibilitas* dimana pengguna bisa mengakses *storage* kapanpun dan dimanapun.



Gambar 2.2.1.1.4 *Virtualisasi Storage*

3. Virtualisasi *DC-DRC*

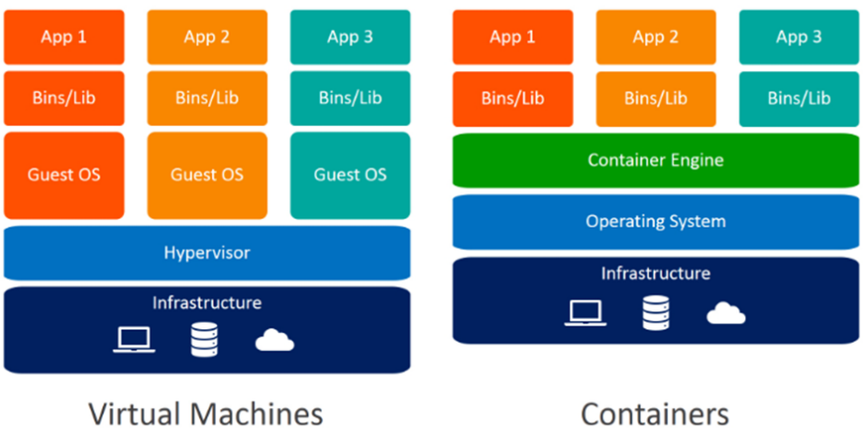
Penggunaan teknologi virtualisasi di pusat data dan *DRC* akan memudahkan dalam proses *backup*, replikasi, dan migrasi pusat data dan aplikasi. Virtualisasi juga memudahkan dalam melakukan *scale-up* atau *scale-down* pusat data sesuai dengan kebutuhan bisnis.



Gambar 2.2.1.1.5 Replikasi Pusat Data dengan Teknologi *Virtualisasi*

4. *Container*

Perkembangan dari teknologi virtualisasi yakni *container* yang menyatukan aplikasi dengan dependensinya sehingga dapat memberikan sistem yang terisolasi (*isolated environment*) pada level *OS* yang dijalankan pada satu induk *linux kernel (host).* Teknologi *container* merubah cara mengembangkan, mendistribusikan dan menyebarkan perangkat lunak.



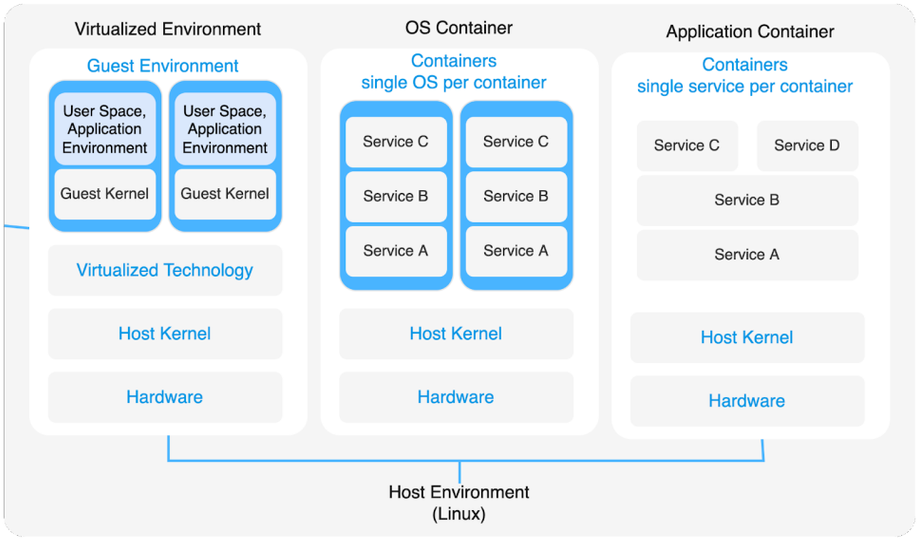
Gambar 2.2.1.1.6 Perbandingan Teknologi *Virtual Machines* dan *Containers*

Saat ini terdapat 2 jenis *container* yang umum dapat kita pergunakan, yaitu:

a. *Container* berbasis sistem operasi (*OS Container*), yakni *container* yang memberikan isolasi pada level sistem operasi dan memanfaatkan kernel yang sama dari suatu induk, contohnya adalah *LXC, OpenVZ, Linux Vpusat data, BSD Jails* and *Solaris zones.*

b. *Container* berbasis aplikasi (*Application Container*), yakni *container* yang memberikan isolasi pada level aplikasi dengan memanfaatkan beberapa

komponen yang ada pada sistem operasi induk, serta beberapa komponen pada *container-container* lain yang menjadi basis dari berjalannya sebuah aplikasi, contohnya adalah *Docker* dan *Rocket* (rkt).



Gambar 2.2.1.1.7 Perbandingan Teknologi *Virtualisasi* dan *Container*
(sumber:*https://blog.andi.dirgantara.co/teknologi-kontainer-pengantar-pengenalan-docker-706eafe03269*)

Penggunaan teknologi *container* mempunyai banyak keuntungan, antara lain:

a. Ringan

Container menyediakan virtualisasi yang berbeda konsep dengan virtualisasi perangkat keras yang tersedia di mesin virtual (*Virtual Machine*). Menggunakan *host* dan kernel yang sama *container* berbagi manajemen memori, *management* proses, I/O dll, sementara proses pada tiap *container* terisolasi dan mempunyai dependensi terpisah.

b. Kinerja Maksimal

Karena *container* dikelola pada *host* yang sama, proses pada *container* dijalankan dengan kinerja sama seperti *host*, setiap proses yang dijalankan dalam container sebenarnya adalah proses dalam *host* yang di isolasi.

c. Konsumsi Sumber Daya Lebih Rendah

Karena container tidak membutuhkan virtualisasi perangkat keras yang penuh, satu host dapat mempunyai banyak *container* dibanding VM.

d. Cepat

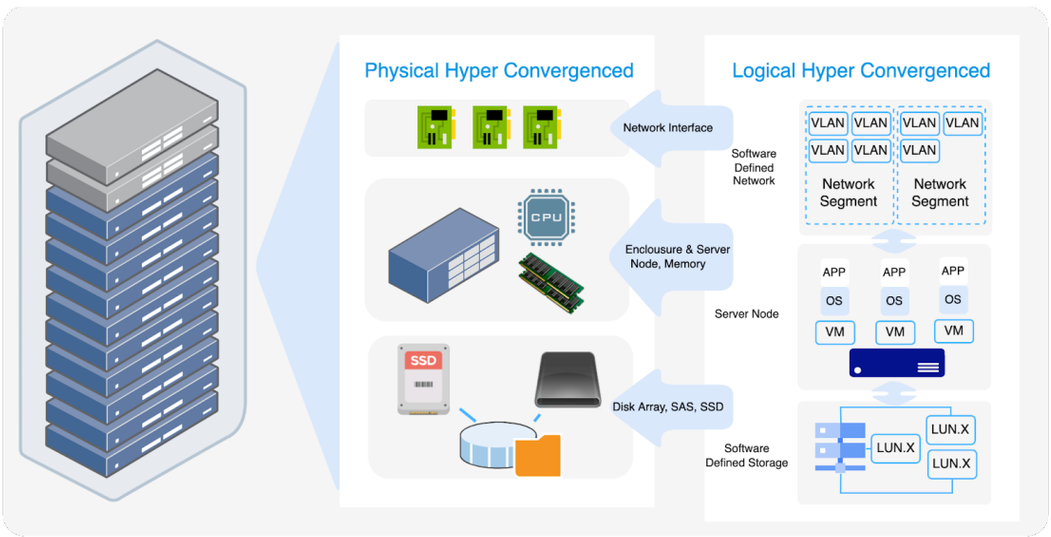
Proses perjalanan penyalaan *server* (*booting)* dalam *container* hampir sama dengan proses *booting* pada *host*, dibanding *virtual machine* yang menjalankan proses tunggal namun harus melakukan *booting* pada sistem operasi secara penuh.

2.2.1.2. Hyper *Converged Infrastructure (HCI)* Pusat Data

Teknologi *hyper-convergence* ini menggabungkan teknologi jaringan (*network*), teknologi pusat data fisik serta teknologi media penyimpanan (*storage*), sehingga ketiganya sudah tersedia menjadi satu perangkat yang dikenal dengan istilah *enclosure*. Teknologi *hyper-convergence* ini memberikan kenyamanan dalam hal pengelolaannya karena jauh lebih efektif dibandingkan dengan pengelolaan tiga perangkat terpisah.

Pengelolaan ini tergabung menjadi satu aplikasi manajemen dan dapat dikonfigurasi sesuai dengan kebutuhan rancangan di setiap organisasi. Adapun dari aspek kapasitas, teknologi ini sangat fleksibel dan mudah untuk ditingkatkan apabila ada kebutuhan tambahan kapasitas.

Pada aplikasi manajemen perangkat *HCI* dapat dilakukan konfigurasi jaringan berbasis perangkat lunak (*software defined network*), yaitu pengaturan jaringan virtual berbasis aplikasi. Pada aplikasi ini dapat dirancang jaringan yang kompleks walaupun tidak memiliki perangkat biasa. Lalu pada bagian pusat data, *enclosure* ini menyediakan *x86-based* pusat data yang dapat dikonfigurasi dengan baik sehingga dapat mencegah terjadinya kebocoran informasi. Di samping itu terdapat bagian *storage* atau media penyimpanan yang juga dapat dikonfigurasi berdasarkan kebutuhan, dengan berbasiskan aplikasi *software defined storage.* Ketiga perangkat ini tergabung menjadi satu sehingga memiliki kinerja yang sangat baik dan mudah untuk dikelola.



Gambar 2.2.1.2.1. Arsitektur *pusat data Hyper Converged Infrastructure (HCI)*

2.2.1.3. DevOps

1. Pengertian

DevOps adalah kombinasi dari budaya, praktik, dan alat untuk meningkatkan kemampuan sebuah perusahaan agar proses *delivery* aplikasi dapat dilakukan dengan kecepatan yang lebih tinggi daripada proses pengembangan aplikasi secara tradisional. Sesuai dengan namanya, istilah *DevOps* adalah gabungan dari kata *Development* dan *Operations*. Jadi secara garis besar metodologi *DevOps* akan menguraikan proses pengembangan aplikasi atau perangkat lunak yang berkualitas tinggi dengan mengotomatiskan dan mengintegrasikan aktivitas dari tim *Development* (pengembang) dan tim *IT Operations* (operasi). Di bawah model *DevOps* ini, tim pengembang dan operasi akan bekerja bersama di seluruh tahapan daur hidup pengembangan aplikasi (*software development life cycle*) untuk menghasilkan produk digital yang berkualitas secara efektif dan efisien.

2. Tujuan dan Manfaat

DevOps dirancang untuk mengatasi permasalahan yang sering terjadi yakni kecepatan dalam pemenuhan permintaan klien, dan faktor keamanan yang kadang diabaikan, dengan cara mengintegrasikan semua orang yang terkait dengan *software development* dan *deployment* baik itu *business users, developers, test engineers, security engineers, system administrators*, dan lain-lain. Tim ini akan bekerja sama untuk mencapai tujuan dan fokus utama yaitu *delivery* produk / software berkualitas tinggi yang dapat memenuhi semua user requirements namun tetap mampu menjaga integritas dan stabilitas seluruh sistem. Berikut ini beberapa manfaat yang diperoleh perusahaan yang telah mengimplementasikan *DevOps* :

A. Perusahaan dapat bergerak dengan cepat

Praktik *DevOps* memungkinkan perusahaan dapat bergerak cepat dalam berinovasi dan beradaptasi dengan perubahan pasar. Dengan demikian, praktik ini mampu mendorong bisnis agar bisa berkembang dengan cepat.

B. Delivery yang cepat

Praktik *DevOps* dapat membantu perusahaan untuk dapat merilis produk dengan waktu yang lebih cepat. Dengan cara ini, perusahaan memiliki peluang untuk bisa lebih unggul dari kompetitor.

C. Keandalan

DevOps bekerja seperti pada praktik *CI/CD* (*Continuous Integration / Continuous Delivery*) yang dapat membantu tim memastikan bahwa produk yang dikembangkan memiliki kualitas yang tinggi. Di sisi lain, tim juga dapat mengirim produk yang andal dengan kecepatan tinggi.

D. Kolaborasi tim yang lebih baik

Di bawah model *DevOps*, tim pengembang dan tim operasi akan berkolaborasi, berbagi tanggung jawab, dan menggabungkan alur kerja mereka. Cara ini dapat membantu tim untuk bekerja secara efektif dan efisien.

E. Aman

Tim dapat mengadopsi model *DevOps* tanpa perlu mengorbankan keamanan dengan menggunakan alat pengujian keamanan terintegrasi dan otomatis.

3. *DevOps Pipeline*

Pipeline DevOps adalah sekumpulan proses yang memungkinkan tim *developer* dan tim *IT operations* dapat bekerja sama untuk membangun dan menerapkan kode ke

lingkungan produksi (*production environment*). Secara garis besar fase D*evOps pipeline* meliputi:

A. Plan

Fase ini melibatkan perencanaan untuk seluruh alur kerja yang dibutuhkan sebelum tim pengembang mulai menulis kode. Dalam tahap ini, manajer produk dan manajer proyek akan memainkan peran penting. Mereka akan bekerjasama untuk mengumpulkan *requirements* dan *feedback* dari klien ataupun *stakeholders*. Informasi tersebut kemudian akan dikumpulkan untuk membangun lini masa produk untuk memandu proses pengembangan yang akan dilakukan.

B. *Code*

Setelah rencana dibuat, tim *developer* dapat mulai menulis kode yang dibutuhkan untuk mengembangkan produk. Tim *developer* biasanya akan menggunakan seperangkat *plugin* standar yang dipasang di lingkungan pengembangan mereka untuk membantu proses pengembangan, membantu menerapkan gaya kode yang konsisten, serta menghindari kelemahan keamanan umum dan anti-pattern.

C. *Build*

Setelah tim developer selesai menulis kode yang dibutuhkan, mereka akan memasukan kode tersebut ke dalam *shared code repository*. Developer akan mengirimkan *pull request*, setelah developer yang lain akan mereview perubahan yang telah dilakukan. Jika kode tidak memiliki masalah, maka developer tersebut akan menyetujui *pull request* yang telah dikirim sebelumnya.

D. *Test*

Langkah selanjutnya adalah melakukan pengujian. Jika ada masalah yang ditemukan pada fase ini, maka masalah tersebut akan dikirim kembali ke tim developer untuk diselesaikan.

E. *Release*

Fase *release* menjadi tonggak penting dalam *DevOps pipeline*. Pada tahap ini, setiap perubahan kode telah melewati serangkaian pengujian dan tim *IT operations* telah memastikan bahwa masalah yang merusak dan regresi sudah teratasi dengan baik.

F. *Deploy*

Tahap selanjutnya adalah deployment. Setelah *production environment* dibuat dan dikonfigurasi maka versi terakhir dari pengembangan yang telah dilakukan akan diterapkan.

G. Monitor

Pada tahap terakhir ini, tim *IT operations* akan terus bekerja keras untuk memantau infrastruktur, sistem, dan aplikasi. Hal ini dilakukan untuk memastikan bahwa produk atau aplikasi yang dikembangkan dapat berjalan dengan lancar. Mereka juga mengumpulkan data-data penting dari log, analitik, sistem monitoring, serta melihat *feedback* dari pengguna untuk mengetahui jika ada masalah pada kinerja aplikasi.

Gambar 2.2.1.3.1. *DevOps Pipeline* (Sumber: blog.isostech.com)

4. Praktik Terbaik untuk *DevOps* yang Efektif

Untuk menjalankan *DevOps* secara efektif terdapat beberapa praktik yang dapat diterapkan, yaitu:

1. *Continuous Integration* (CI)

   Continuous Integration adalah praktik dalam *software development* dimana tim developer akan secara rutin menggabungkan pembaruan kode ke dalam *central repository*. Tujuan utama dari *CI* adalah menemukan dan mengatasi *bug* lebih cepat, meningkatkan kualitas perangkat lunak, dan mengurangi waktu yang diperlukan untuk memvalidasi dan merilis pembaruan perangkat lunak yang baru.

2. *Continuous Delivery* (CD)

   Continuous Delivery adalah praktik dalam *software development* yang memastikan bahwa kode selalu dalam status "*deployable*". Artinya, setiap perubahan yang ada di dalam kode seperti penambahan fitur, perbaikan bug, perubahan konfigurasi, atau yang lain, akan selalu siap untuk diterapkan ke dalam *production environment* atau bahkan ke tangan *user* dengan cepat, aman, dan berkelanjutan.

3. *Microservices*

Microservice adalah gaya arsitektur yang dapat diimplementasikan dalam pengembangan aplikasi yang kompleks. Implementasi arsitektur ini memungkinkan aplikasi yang sedang dikembangkan menjadi sangat mudah dipelihara dan "*testable*".

4. *Infrastructure as Code* (IaC)

Infrastructure as Code adalah sebuah pendekatan untuk mengelola *data center server, storage*, dan infrastruktur jaringan. *IaC* digunakan untuk menyederhanakan konfigurasi dan manajemen skala besar secara signifikan.

5. *Monitoring* dan *logging*

Monitoring dapat membantu perusahaan untuk mengidentifikasi akar penyebab masalah dengan cepat sehingga dapat mencegah munculnya masalah lain yang lebih besar. Dengan cara ini, tim mampu mengukur kinerja aplikasi/ *software* dan memastikan sistem tetap bekerja secara stabil.

Selain itu, tim juga akan menganalisis *log* yang dihasilkan oleh aplikasi. Dengan demikian, tim *DevOps* dapat lebih memahami bagaimana perubahan atau pembaruan perangkat lunak yang telah dilakukan dapat memengaruhi user.

5. Peta Jalan (Road Map) *DevOps*

Implementasi *DevOps* tidak bisa dilakukan secara langsung tetapi harus melalui beberapa tahapan karena *DevOps* akan merubah pola atau budaya kerja. Peta jalan perlu disusun untuk memudahkan dalam pemantauan dan kontrol.

Gambar 2.2.1.3.2. Peta Jalan Implementasi *DevOps*

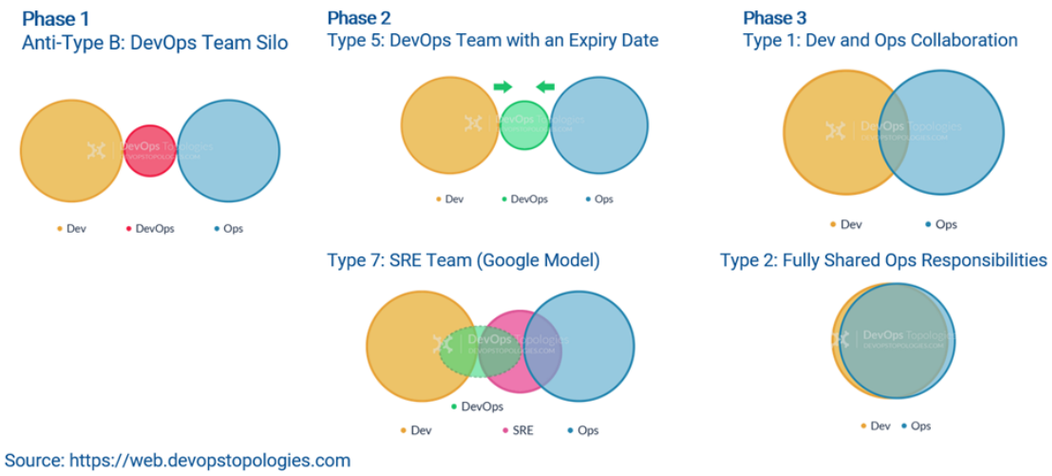
6. *Tools DevOps*

Untuk mengimplementasikan *DevOps* diperlukan aplikasi pendukung (tools) antara lain:

1. *Version Control*
   a. *Github*
   b. *Bitbucket*
   c. *GitLab*
2. *Container Management tools*
   a. *Docker*
   b. *Kubernetes*
   c. *Mesos*
3. *Application Performance Monitoring tools*
   a. *Prometheus*
   b. *Dynatrace*
   c. *AppDynamics*
4. *Deployment & Server Monitoring tools*
   a. *Datadog*
   b. *Sensu*
5. *Configuration Management tools*
   a. *Chef*
   b. *Puppet*
   c. *Ansible*
6. *CI / Deployment Automation tools*
   a. *Bamboo*
   b. *Jenkins*
   c. *IBM UrbanCode*
7. *Test Automation tools*
   a. *Test.ai*
   b. *Ranorex*
   c. *Selenium*
8. *Artifact Management tools*
   a. *JFRog Artifactory*
   b. *Sonatype NEXUS*
9. *Codeless Test Automation tools*
   a. *Testim.io*
   b. *AccelQ*

7. Transformasi Tim

Terdapat beberapa metodologi untuk topologi implementasi *DevOps* khususnya transformasi tim.



Gambar 2.2.1.3.3. Transformasi Tim DevOps

2.2.1.4. Microservices

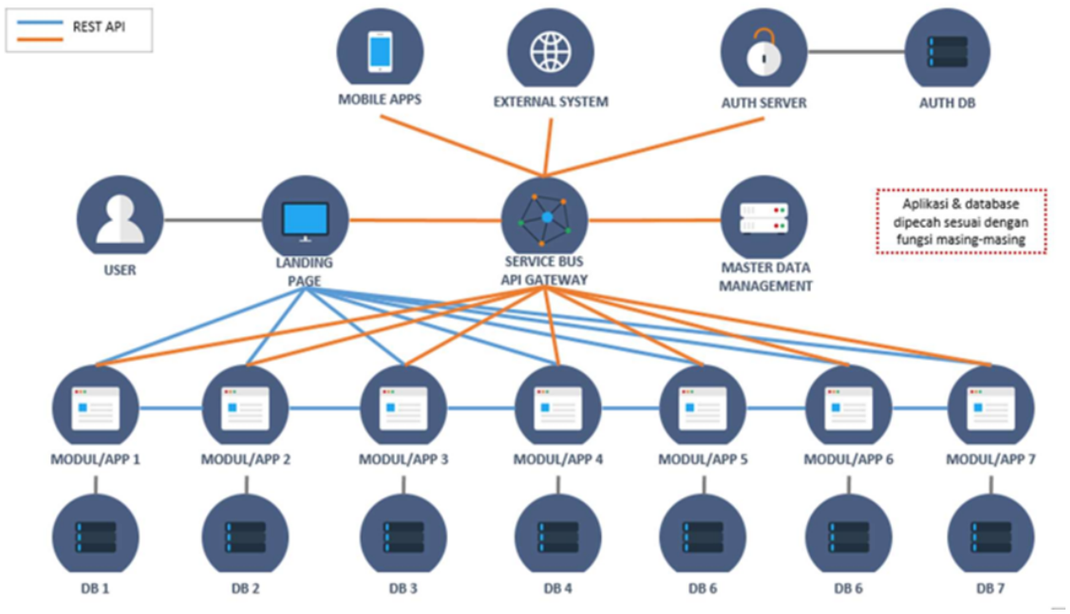
Secara sederhana, arsitektur aplikasi *microservices* menggunakan desain yang memecah aplikasi berdasarkan fungsinya secara spesifik. Aplikasi *microservices* tidak sekedar memisahkan berdasarkan *user-role* atau subdomain saja, tetapi aplikasi akan di *breakdown* lebih rinci lagi dari sisi fungsionalitasnya. Aplikasi akan dirancang agar setiap fungsi bekerja secara independen. Setiap fungsi dapat menggunakan teknologi *stack* yang sesuai dengan kebutuhan, walaupun artinya akan terdapat teknologi yang berbeda-beda dalam satu aplikasi besar. Setiap *microservices* merupakan aplikasi kecil yang memiliki arsitektur heksagonal sendiri yang terdiri dari logika beserta berbagai adapternya (bahasa pemrograman, dll).

Pola arsitektur *microservices* secara signifikan mempengaruhi hubungan antara aplikasi dan database. Berbagai skema *database* tunggal dengan *services* lainnya memiliki skema *database* tersendiri. Pendekatan ini bertentangan dengan gagasan model data *enterprise-wide* yang sering kali menghasilkan duplikasi beberapa data. Memiliki skema *database* per *service* sangat penting jika ingin mendapatkan keuntungan dari layanan *microservice*. Masing-masing *service* memiliki *database* sendiri. Selain itu, *services* dapat menggunakan jenis *database* dan bahasa pemrograman yang paling sesuai dengan kebutuhannya.

Microservices membagi *service* ke bagian yang lebih kecil dimana *service-service* tersebut saling berhubungan satu sama lain. Selain itu, dalam setiap *services* yang dibuat bisa menggunakan teknologi yang berbeda. Sedangkan untuk implementasi ke *web*, *android, iOS* dll tidak bisa secara langsung, pengembang harus membuat terlebih dahulu yang namanya *API Gateway. API Gateway* memiliki tugas seperti *load balancing, caching, access controll , API metering*, dan monitoring.

Aplikasi yang dibangun dengan menggunakan arsitektur *microservices* pada setiap modul memerlukan *engine* seperti *web server* serta basis data (*micro database*) yang akan berdampak terhadap peningkatan kinerja aplikasi yang signifikan. Di samping itu

keamanan aplikasi akan lebih terjamin dengan melakukan pengamanan melalui *REST API*, sehingga transaksi dan pertukaran data yang dilakukan akan lebih terjaga.



Gambar 2.2.1.4.1. Arsitektur *Microservices*

Arsitektur *microservices* mempunyai kelebihan sebagai berikut:

A. Komponen Terpisah

Pertama, semua layanan dapat digunakan dan diperbarui secara independen, sehingga memberikan lebih banyak fleksibilitas. Kedua, *bug* dalam satu *microservices* berdampak pada layanan tertentu dan tidak memengaruhi keseluruhan aplikasi. Selain itu, jauh lebih mudah untuk menambahkan fitur-fitur baru ke aplikasi yang dikembangkan dengan arsitektur *microservices* daripada aplikasi yang menggunakan arsitektur monolitik.

B. Pemahaman yang Lebih Mudah

Arsitektur aplikasi dengan *microservices* lebih mudah dipahami dan dikelola karena aplikasi dibagi menjadi komponen yang lebih kecil dan sederhana. Hal ini memungkinkan pengembang aplikasi untuk fokus hanya pada layanan spesifik yang terkait dengan tujuan bisnis yang telah ditentukan sebelumnya.

C. Skalabilitas yang Lebih Baik

Keuntungan lain dari pendekatan *microservices* adalah bahwa setiap elemen dapat diskalakan secara independen sehingga proses lebih efektif baik dari segi biaya dan waktu dibandingkan dengan dengan pendekatan *monolitik* dimana seluruh komponen pembentuk aplikasi harus ditingkatkan meskipun hal tersebut tidak diperlukan. Selain itu, setiap arsitektur monolitik memiliki batasan dalam hal skalabilitas komponen infrastruktur servernya, sehingga semakin kompleks elemen, maka semakin banyak masalah yang berpotensi muncul.

Selain memiliki keuntungan, arsitektur *microservices* memiliki beberapa kekurangan sebagai berikut :

A. Kompleksitas Ekstra

Arsitektur layanan *microservices* merupakan sistem terdistribusi dengan kompleksitas ekstra sehingga harus memilih dan mengatur koneksi antara semua modul dan *database*. Lebih lanjut, aplikasi tersebut termasuk layanan independen, semuanya harus dikerahkan secara independen.

B. Distribusi Sistem

Arsitektur layanan *microsoft* adalah sistem kompleks dari banyak modul dan basis data sehingga semua koneksi harus ditangani dengan hati-hati.

C. Fungsi Lintas Sektoral *(Cross-Functional)* Bertambah

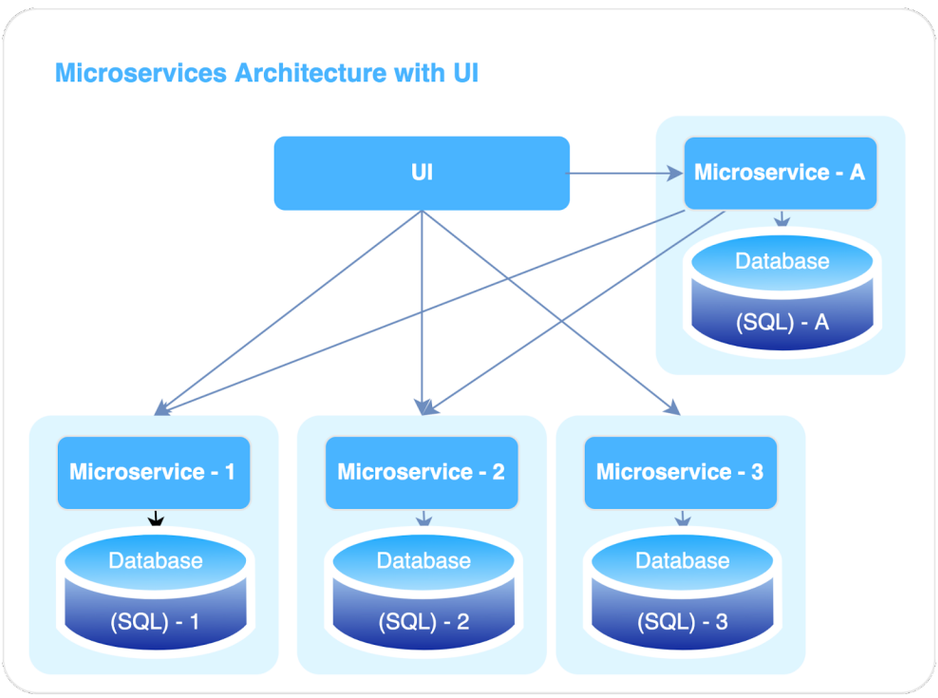
Saat membuat aplikasi *microservices*, pengembang harus berurusan dengan sejumlah masalah lintas sektoral termasuk konfigurasi eksternal, *logging*, metrik, pemeriksaan kesehatan, dan lainnya.

D. Pengujian

Sebagian besar komponen yang dapat digunakan secara terpisah membuat pengujian solusi berbasis layanan jauh lebih sulit.

Arsitektur Pangkalan Data (Database) Microservices

Arsitektur basis data yang akan diterapkan pada arsitektur aplikasi *microservices* menggunakan *two-tier architecture*, dimana dalam setiap modul aplikasi tersebut memiliki pangkalan data masing-masing sesuai dengan perannya, seperti: terlihat pada gambar berikut:

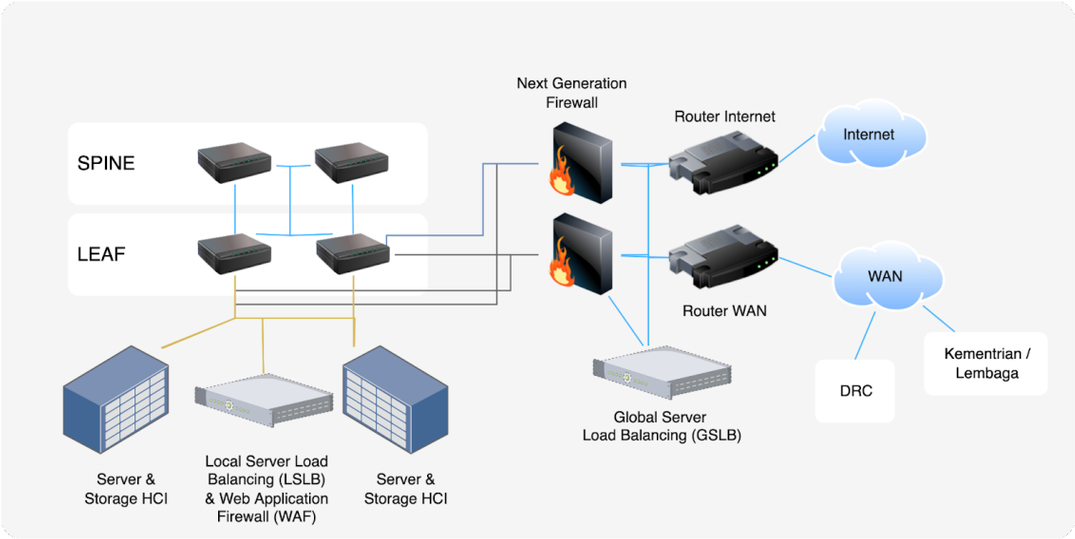


Gambar 2.2.1.4.2. Arsitektur Pangkalan Data *Microservices*

2.2.1.5. Arsitektur *Network Spine-Leaf* Pusat Data

Arsitektur *Spine-Leaf* adalah topologi jaringan pusat data yang terdiri dari dua lapisan *switching: Spine* and Leaf. *Leaf layer* terdiri dari *switch* akses yang mengumpulkan lalu lintas dari pusat data dan terhubung langsung ke *spine layer* atau jaringan inti. *Switch Spine-Leaf* menghubungkan semua *switch leaf* dalam topologi penuh ke *switch core*.

Prevalensi infrastruktur *cloud* dan *container* di pusat data modern serta lalu lintas jaringan terus meningkat. Lalu lintas pada jaringan bergerak menyamping dari satu pusat data ke pusat data lainnya. Perubahan ini terutama disebabkan oleh fakta bahwa aplikasi modern memiliki komponen yang didistribusikan di lebih banyak pusat data atau mesin virtual.



Gambar 2.2.1.6.1. Arsitektur *Network Spine-Leaf Datacenter*

2.2.1.6. OWASP 10 - 2021

OWASP TOP 10 atau yang biasa disebut *OWASP* 10 adalah sebuah daftar teratas kerentanan keamanan yang dapat mengancam keamanan suatu *website* yang dirilis oleh komunitas OWASP *(Open Web Application Security Project)*. Daftar ini terus berkembang dan berubah-ubah mengikuti perkembangan teknologi *website*/aplikasi *web* yang terus berkembang dan versi terakhir adalah 2021. OWASP Top 10 adalah sebuah panduan bagi para *developers* dan *security team* tentang kelemahan-kelemahan pada *web apps* yang mudah diserang dan harus segera disiasati. Berikut daftar *OWASP Top* 10:2021:

A. A01:2021-*Broken Access Control*

Aplikasi tidak akan bekerja dengan baik sesuai fungsinya jika penerapan otorisasi hak akses tidak berjalan efektif. Misalnya, apabila pengguna aplikasi (*user*) berhasil melewati halaman *login*, selanjutnya pengguna dapat bebas menjalankan operasi apabila mengakses tautan web tertentu dalam halaman admin, padahal mereka tidak memiliki akses.

Access control atau lebih sering disebut sebagai otorisasi, adalah suatu proses pemberian akses fungsi atau konten kepada beberapa pengguna, dan tidak kepada

pengguna lain dalam suatu aplikasi. Proses ini terjadi setelah pengguna berhasil melakukan otentikasi atau lebih umum dikenal dengan proses *login*. *Access Control* seringkali tidak didefinisikan, dibentuk dan didesain secara keseluruhan pada awal pembuatan aplikasi, melainkan berkembang seiring dengan perkembangan aplikasi itu sendiri. Pada setiap fungsi baru yang ditambahkan, aturan *access control* akan disisipkan. Hal ini menyebabkan aturan *access control* yang terkumpul akhirnya menjadi rumit dan sulit dipahami.

B. A02:2021-*Cryptographic Failures*

Implementasi enkripsi atau kriptografi yang buruk pada sebuah data sensitif, sehingga mengakibatkan permasalahan terhadap perlindungan dan kerahasiaan data, baik saat pengiriman data maupun ketika data disimpan. Permasalahan pada konsep kriptografi yang buruk sering menyebabkan maraknya data *breach*, karena data yang tidak terenkripsi kerap kali dimanfaatkan oleh *attacker* untuk mengakses data yang lebih tinggi lagi.

C. A03:2021-*Injection*

Sistem / program memproses sebuah data yang tidak valid, yang mengakibatkan peretas (*hacker*) yakni orang dengan kemampuan teknis komputer tertentu yang dapat menerobos masuk ke dalam aplikasi *web* suatu organisasi, dengan cara memecahkan kode-kode atau sandi-sandi melalui jaringan komputer atau internet. Peretas dapat menginputkan kode tertentu kepada program lalu kode tersebut akan membuat program menjalankan perintah yang salah.

D. A04:2021-*Insecure Design*

Insecure Design merujuk pada salah satu daftar kerentanan keamanan yang dirilis oleh *OWASP* (*Open Web Application Security Project*). Kerentanan ini mengacu pada kelemahan yang terkait dengan desain atau arsitektur aplikasi atau sistem yang memungkinkan serangan atau pelanggaran keamanan. Hal ini dapat terjadi karena pengembang tidak memperhatikan keamanan dalam tahap perancangan atau desain sistem. Dengan demikian pengembang perlu menerapkan prinsip keamanan salah satunya *Secure By Design* pada tahapan awal desain program atau aplikasi. *Secure By Design* dalam dunia *software engineering* adalah sebuah *software* yang seharusnya memiliki kapabilitas *design* yang cukup aman secara fundamental. Setiap *attacker* mendapatkan sebuah informasi sensitif yang terdapat pada pesan *error*, hal tersebut dapat terjadi karena pengembang tidak menggunakan *error handler* dengan baik.

Hal tersebut sering terjadi ketika pengguna salah mengisi *input* seperti tidak sesuainya tipe data yang diminta, kurang nya jumlah *character*, atau pengguna tidak sengaja mengisi null pada sebuah *input request*.

E. A05:2021-*Security Misconfiguration*

Security Misconfiguration merupakan kerentanan keamanan yang terjadi karena konfigurasi atau pengaturan sistem yang tidak tepat pada suatu aplikasi atau infrastruktur teknologi informasi. Hal ini dapat terjadi ketika pengembang tidak

melakukan konfigurasi atau pengaturan dengan benar, atau tidak memperbarui dan memperbaiki konfigurasi yang sudah ada. Akibatnya, peretas dapat dengan mudah menemukan celah keamanan dan memanfaatkannya untuk melakukan serangan ke sistem atau aplikasi yang rentan tersebut.

F. A06:2021-*Vulnerable and Outdated Components*

Kondisi dimana pengembang masih menggunakan sebuah aplikasi, *framework, library,* atau komponen versi lawas (*outdated*), dan pengembang tidak melakukan pengecekan apakah aplikasi sudah dilakukan *patching*, atau *updating*.

G. A07:2021-*Identification and Authentication Failures*

Sebuah kerentanan yang terjadi pada aktivitas pengidentifikasian serta autentikasi. Kerentanan ini disebabkan karena sistem pengidentifikasian dan autentikasi gagal mengidentifikasi pengguna, nantinya akan menyebabkan pengguna dapat terautentikasi sebagai pengguna lain, secara sengaja maupun tidak di sengaja.

H. A08:2021-*Software and Data Integrity Failures*

Gagalnya sebuah *software*/aplikasi memeriksa integritas sebuah data, yang disebabkan tidak terimplementasinya *development life cycle* dengan benar, yang mana beberapa pengembang sering melewatkan proses tes integritas sebuah data sebelum *release*, atau tidak melakukan *code review/static analysis* pada aplikasi yang akan di *deploy* dan di *release* untuk memastikan tidak ada *malicious code* yang tertanam pada *software*/aplikasi.

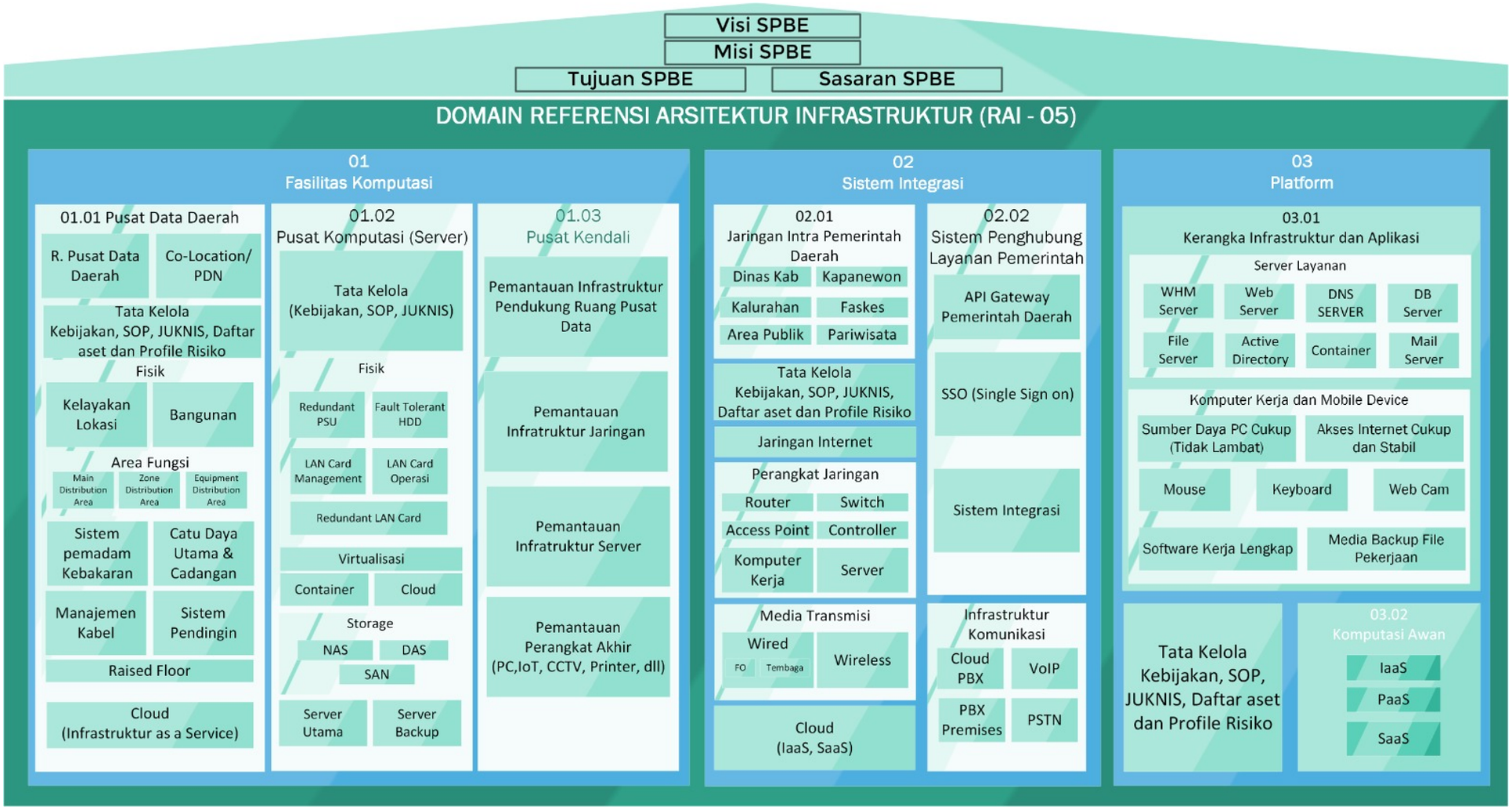
I. A09:2021-*Security Logging and Monitoring Failures*

Kondisi ketika pusat data/aplikasi tidak terpantau dengan baik, biasanya disebabkan karena manajemen rekam jejak (*log management)* yang buruk dan *log* yang tidak terformat dengan baik. Selain itu juga terdapat faktor kesalahan manusia (*human error),* yakni ketika tim *Security Operation Center* (SOC) tidak melakukan pemeriksaan lanjutan atau melakukan analisis *log* secara proaktif terhadap *alert*.

J. A10:2021-*Side Request Forgery*

Kondisi kerentanan saat sebuah aplikasi *web* meminta *remote resource* tanpa melakukan validasi URL. Hal ini menyebabkan *hacker* dapat memaksa aplikasi untuk mengirim *crafted request* ke destinasi yang tidak diharapkan, meskipun sudah dilindungi oleh *firewall*, VPN, atau tipe lain.

2.2.2. Infrastruktur SPBE



Gambar 2.2.2.1. Arsitektur Infrastruktur SPBE Pemerintah Kabupaten Murung Raya

2.2.2.1. Prinsip-prinsip Pengembangan Infrastruktur Teknologi Informasi

Infrastruktur TI merupakan tulang punggung dalam integrasi proses kerja di lingkungan Pemerintah Kabupaten Murung Raya sebagai media transfer data dari pusat data ke pengguna data atau dari sumber data ke pusat data. Untuk menjamin data terkirim dengan baik dan aman, maka pengembangan infrastruktur TI harus memiliki beberapa prinsip dasar, yaitu:

Gambar 2.2.2.1.1 Prinsip Pengembangan Infrastruktur SPBE

A. Peningkatan Kapasitas (*Scalable)*

Kemampuan infrastruktur TI Pemerintah Kabupaten Murung Raya untuk menangani pertumbuhan beban kerja dengan lancar. Data, proses, dan pengguna seiring berjalannya waktu akan semakin bertambah besar dan kompleks sehingga menuntut infrastruktur TI untuk beradaptasi dengan tuntutan bisnis tersebut.

B. Kemudahan Pengelolaan (*Manageable*)

Pengelolaan infrastruktur TI oleh Pemerintah Kabupaten Murung Raya akan mudah dilakukan melalui alat pengelolaan infrastruktur TI maupun dengan mempelajari infrastruktur yang ada di Pemerintah Kabupaten Murung Raya. Salah satu contoh kemudahan dalam pengelolaan adalah pengalokasian *IP Address* menggunakan *DHCP* (*Domain Host Control Protocol*) oleh sistem administrator, sehingga memudahkan dalam mengatur *IP Address* komputer pengguna dalam jumlah besar.

C. Tingkat Ketersediaan Tinggi (*Available*)

Infrastruktur TI Pemerintah Kabupaten Murung Raya dapat beroperasi sesuai dengan *Service Level Agreement* (SLA) yang telah disepakati atau ditarget. Pencegahan terhadap kegagalan, komponen infrastruktur TI dapat memanfaatkan *redundancy*. *Redundancy* merupakan mekanisme penduplikasian komponen kritis pada infrastruktur TI, sehingga ketika komponen utama mengalami kegagalan fungsinya dapat digantikan oleh komponen cadangan.

D. Kemudahan dalam Perbaikan (*Serviceable*)

Kemampuan infrastruktur TI Pemerintah Kabupaten Murung Raya dalam kemudahan perbaikan infrastruktur sesuai dengan persyaratan yang telah ditentukan.

SLA terkadang mencantumkan persyaratan *downtime* dari sebuah komponen infrastruktur TI, sehingga kemudahan dalam perbaikan sangat diperlukan untuk mempertahankan SLA tersebut. Kemudahan dalam perbaikan infrastruktur TI (*server, storage*, dll) jika terjadi kerusakan dapat diperoleh dengan memilih teknologi teruji di industri dan memiliki dukungan teknis dari *vendor* yang dapat diandalkan.

E. Keamanan (*Secure*)

Infrastruktur TI Pemerintah Kabupaten Murung Raya hendaknya dapat digunakan untuk menjaga kerahasiaan dan integritas data maupun sistem. Keamanan tidak hanya melibatkan pencegahan akses yang tidak sah, tetapi juga melibatkan kemampuan untuk memastikan bahwa data yang dikirim melalui infrastruktur TI terjaga keasliannya. Sebagai contoh, pengguna harus melewati proses otentikasi dan otorisasi sebelum mengakses sistem, dan digital signature dapat digunakan untuk memastikan bahwa data dikirim dengan benar dan tidak berubah selama proses transfer.

2.2.2.2. Pusat Data

Infrastruktur *server, storage*, perangkat jaringan, dan perangkat keamanan jaringan perlu ditempatkan, disimpan pada suatu lokasi yang terstandarisasi untuk sistem elektronik maupun pengolahan data yang disebut pusat data. Selain itu juga untuk menjaga keberlangsungan layanan dan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting sistem elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia maka diperlukan Pusat Pemulihan Bencana (*disaster recovery center*).

Berikut ini adalah prinsip dan kriteria dalam perancangan Pusat Data dan Pusat Pemulihan Bencana antara lain adalah:

A. Ketersediaan (*Availability*)

Pusat data dibuat untuk mampu memberikan operasi yang berkelanjutan dan terus-menerus bagi suatu perusahaan baik dalam keadaan normal maupun dalam keadaan terjadinya suatu kerusakan yang berarti atau tidak. Pusat data harus dibuat sebisa mungkin menghindari kegagalan (*zero-failure*) untuk seluruh komponennya.

B. Skalabilitas (*Scalability*)

Pusat data harus mampu beradaptasi dengan pertumbuhan kebutuhan yang cepat atau ketika ada servis baru yang harus disediakan oleh pusat data tanpa melakukan perubahan yang cukup berarti bagi pusat data secara keseluruhan. Selain itu juga kemudahan dalam implementasi tanpa perlu membeli komponen infrastruktur tambahan, dan aplikasi.

C. Keamanan (*Security*)

Pusat data menyimpan berbagai aset perusahaan yang berharga berupa aset fisik (*tangible*) seperti perangkat pusat data, jaringan, dan lain - lain maupun non fisik *(intangible)* yakni data data dan informasi. Oleh karenanya sistem pengamanan

pusat data dibuat seketat mungkin meliputi pengamanan secara fisik maupun pengamanan non-fisik.

D. Kemudahan *Backup dan Recovery*

Pusat data yang ada mudah untuk di *backup* termasuk seluruh konfigurasi sistem. Jika terjadi *crash* atau kerusakan pada *pusat data* maka mudah untuk di *recovery* tanpa perlu instalasi dan konfigurasi sehingga hemat waktu, tenaga dan sumber daya.

E. Kemudahan *Deployment*

Pusat data dapat digandakan (*cloning*) dan dapat dijalankan pada mesin lain dengan mengubah sedikit konfigurasi sehingga mempercepat proses implementasi suatu sistem.

F. Fleksibel (*Flexibility*)

Kemudahan dalam pengelolaan pusat data seperti ketika ingin memindah, merubah *resource* bahkan ketika kita ingin melakukan *live migration* atau memindahkan pusat data dalam keadaan hidup tanpa mengalami *down*. Apabila terjadi kerusakan/*error* pada *server*, *storage* yang ditempatkan di pusat data dapat dilakukan penginstalan dan pemulihan (*recovery*) kembali.

G. Redudansi

Untuk menjamin ketersediaan dan kinerja aplikasi maka diperlukan redudansi aplikasi, basis data (*database*) dengan menggunakan teknik *clustering* dan duplikasi pusat data. *Clustering pusat data* aplikasi dapat membagi beban kerja pusat data (*load sharing*) dan duplikasi pusat data dapat menjaga ketersediaan aplikasi (*fail-over*).

H. Pemulihan Bencana yang Lebih Baik

Memiliki tingkat fleksibilitas dalam rencana pemulihan bencana yang lebih mudah untuk diberlakukan dan memiliki tingkat keberhasilan yang jauh lebih tinggi. Jika terjadi bencana yang menyerang pusat data, proses pemindahan pusat data aplikasi ke tempat lain dapat dilakukan dengan mudah dan cepat.

I. Penghematan

Prinsip penghematan yang dimaksud meliputi:

1. Optimalisasi Pusat Data

   Operasionalisasi pusat data akan optimal jika infrastruktur *server*, *storage*, dan lainnya yang ditempatkan pada ruang *server* sesuai dengan perencanaan kapasitas pusat data.

2. Hemat Listrik dan *Hardware*

   Teknologi virtualisasi pusat data dapat menghemat penggunaan sumber daya listrik, dan perangkat keras pendukung pusat data, seperti: sistem pendingin ruangan, dan lainnya.

3. Hemat Ruang/Rack Pusat Data

   Semakin sedikit jumlah server fisik berarti semakin sedikit pula ruang untuk menyimpan perangkat. Jika pusat data ditempatkan pada suatu *colocation* pusat data, akan berimbas pada pengurangan biaya sewa.

4. Tidak Terikat pada Satu Vendor

   Pusat Data hendaknya tidak tergantung pada satu vendor, atau *platform* tertentu karena hal ini akan memudahkan proses pengembangan dan pemulihan jika terjadi kerusakan pada aplikasi.

5. Aplikasi Lama Masih Dapat Digunakan

   Ketika ada aplikasi lama yang sudah tidak bisa berjalan di modern *Operating System (OS)* saat ini (misalnya aplikasi *DOS*) maka aplikasi tetap dapat dijalankan dengan teknologi tertentu pada pusat data yang ada.

6. Keamanan

   Jika terjadi kasus pusat data di *hack* dan data penting dalam pusat data dihapus/dirusak maka proses mengembalikan pusat data dan data penting dapat dilakukan dengan mudah dan cepat. Selain itu untuk menghapus *backdoor* dan *malware* yang ditinggalkan *hacker* tersebut juga dapat dilakukan dengan mudah dan cepat.

Sesuai Rancangan Peraturan Menteri Komunikasi dan Informatika tahun 2018 tentang Standarisasi Infrastruktur pusat data, penyelenggara pusat data harus memperhatikan:

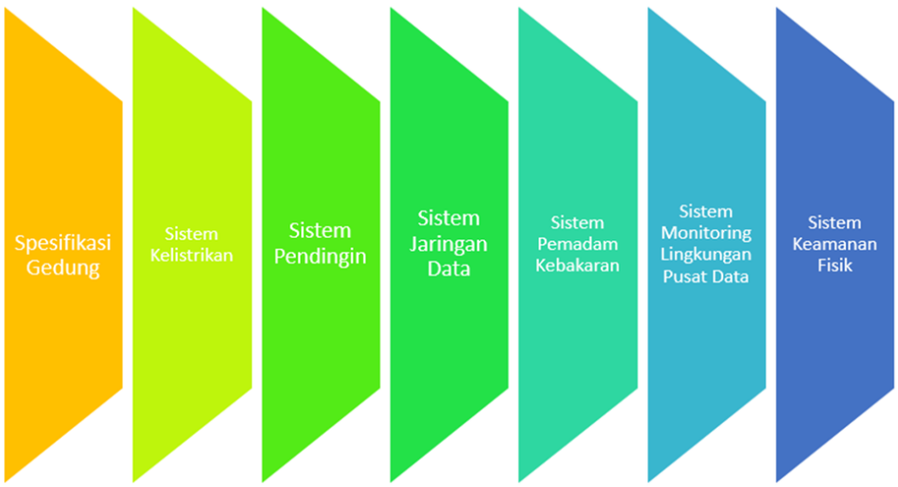
1. Lokasi pusat data hendaknya aman dari bencana, mudah diakses dan mudah melakukan pengembangan/pembangunan pusat data.
2. Rancangan dan bangunan pusat data sesuai dengan standar topologi yang dipilih sesuai kebutuhan berdasarkan kajian kebutuhan bisnis dan analisis dampak bisnis (*business impact analysis*).
3. Kapasitas *bandwidth* untuk keperluan komunikasi yang diperlukan dan memiliki jalur komunikasi data alternatif guna menghindari kepadatan lintas data serta mencegah kegagalan satu jalur *(single point of failure)*.
4. Jalur *supply utility* dan logistik untuk keberlangsungan layanan Pusat Data. menyediakan *bandwidth* untuk keperluan komunikasi yang diperlukan dan memiliki jalur komunikasi data alternatif guna menghindari kepadatan lintas data serta mencegah kegagalan satu jalur (*single point of failure*).
5. Sistem pemantauan lingkungan pusat data (*environment monitoring system*) yang meliputi antara lain monitoring temperatur, kelembaban, asap, kebakaran, kebocoran air, dan tegangan listrik.
6. Standar operasional prosedur untuk operasi dan perawatan.
7. Rencana keberlangsungan usaha (*business continuity plan*) dan rencana pemulihan bencana (*disaster recovery plan*) yang komprehensif serta proses pemulihan bencana yang cepat dan adaptif

8. SNI Pusat Data

Standar Nasional Indonesia (SNI) tentang pusat data terdiri dari:

1. SNI No 8799-1:2019 tentang Panduan Spesifikasi Teknis Pusat Data

   Bagian seri standar pusat data ini bertujuan untuk memberi panduan spesifikasi teknis pusat data yang diberlakukan di wilayah Indonesia bagi penyedia layanan berbasis elektronik, baik penyedia layanan berbasis elektronik untuk publik maupun yang dipergunakan untuk keperluan sendiri.



Gambar **2.2.2.2.1** SNI No 8799-1:2019 - Panduan Spesifikasi Teknis Pusat Data

Standar Panduan Spesifikasi Teknis Pusat Data merinci persyaratan spesifikasi teknis pusat data sebagai berikut:

a. Spesifikasi gedung

- Lokasi Gedung Pusat Data

  Ketentuan lokasi gedung pusat data antara lain tidak berada pada area rentan bencana seperti yang dipetakan pada peta BMKG, tidak berada pada lokasi rawan huru hara, perkampungan padat atau kumuh, jarak dengan arteri lalu lintas (jalan raya utama dan jalur kereta api) minimal 91 m.
- Ketahanan gempa

  Bangunan pusat data memiliki ketahanan terhadap gempa sesuai dengan SNI 1726:2012 sekurang-kurangnya kategori resiko II.
- Ketahanan beban gedung

  Bangunan pusat data dapat menahan beban terpusat sekurang-kurangnya hingga 1.000 kg per meter persegi. Beban dimaksud adalah beban merata bukan hanya pada tulang lantai.
- Pembagian ruangan

  Pembagian ruangan meliputi area perkantoran (area publik, pribadi, ruang fasilitas penunjang), area telekomunikasi, dan area pusat data.
- Ketahanan material gedung

Persyaratan ketahanan material gedung meliputi persyaratan ketahanan api dan ketahanan penggembungan.

- Sistem monitoring gedung

  Sistem monitoring gedung pusat data memiliki fitur sekurang - kurangnya antara lain pengelolaan manajemen risiko, pengelolaan operasional gedung, pelayanan penghuni atau tamu, pengelolaan pengamanan dan pengelolaan energi.

b. Spesifikasi sistem kelistrikan

- Catu daya listrik

  Pusat data memiliki distribusi jaringan sistem kelistrikan dari catu daya listrik primer atau catu daya listrik sekunder.

- Sistem kelistrikan berkesinambungan

  Pusat data memiliki distribusi jaringan sistem kelistrikan berkesinambungan dengan catu daya cadangan seperti genset dan *Uninterruptible Power Supply* (UPS) dengan pemisahan panel-panel distribusi listrik untuk area pusat data hingga perangkat yang berada didalam gedung pusat data.

- Persediaan bahan bakar

  Pusat data memiliki tangki bahan bakar penyuplai genset dengan jumlah dan kapasitas minimum tertentu untuk melayani operasi pusat data.

- *Uninterruptible Power Supply (UPS)*

  Pusat data memiliki UPS untuk menjaga ketersedian kelistrikan tidak terputus. Kapasitas Perhitungan kapasitas UPS minimum yakni beban puncak pusat data sebelum arus kelistrikan digantikan oleh arus listrik dari genset. Pusat data memiliki sekurang-kurangnya 120% kapasitas listrik untuk dapat memenuhi kebutuhan pusat data dengan prioritas utama, beserta ruang-ruang lain yang yang diperlukan dalam operasi pusat data. Tersedia sambungan langsung otomatis atau manual untuk sistem kelistrikan yang diperlukan dalam perawatan jaringan kelistrikan.

- Analisis sistem listrik

  Pusat data memiliki analisis sistem listrik untuk mendapatkan kapasitas ukuran dari pemutus arus sesuai dengan beban yang ada sehingga jika terjadi hubungan singkat pada perangkat teknologi informasi tidak menyebabkan pemutus arus utama terputus.

- Konstruksi panel listrik

  Setiap panel listrik memiliki persyaratan konstruksi khususnya untuk panel induk pada masing-masing kategori strata pusat data.

- Jalur kabel listrik

  Pusat data memiliki pemisahan jalur kabel bermuatan listrik untuk menghindari radiasi dan interferensi elektromagnetik. Setiap kabel memiliki label jalur dan tercatat dalam dokumentasi dan diagram.

- Pembumian

  Pusat data memiliki pembumian bagi perangkat teknologi informasi, panel elektrikal, perangkat dari bahan metal dan pembumian penangkal petir sesuai ketentuan SNI 0225:2011. Pusat data memiliki sistem perlindungan terhadap bahaya petir dan pembumian dengan ketahanan sekurang-kurangnya 3 (tiga) ohm.
- Efisiensi pemakaian listrik pada pusat data *(Power Usage Effectiveness)*

  Memiliki perhitungan efisiensi pemakaian listrik pada pusat data (*Power Usage Effectiveness*) terhadap keseluruhan beban daya maksimum pusat data.

c. Spesifikasi sistem pendinginan

Pusat data memiliki dokumen spesifikasi teknis sistem pendingin, skema diagram sistem pendinginan, jaminan layanan purna jual, nomor kontak layanan, dan kontrak perawatan. Pengoperasian peralatan teknologi informasi di dalam area pusat data dan area telekomunikasi harus memenuhi pengukuran:

- Temperatur ruangan : 18oC – 27oC;
- Tingkat perubahan temperatur ruangan per-jam maksimum : 5oC;
- Kelembaban ruangan : RH (*Relative Humidity*) ≤ 60%, titik embun : 5.5oC – 15oC; dan
- Tingkat perubahan kelembaban ruangan maksimum per-jam : 5% RH.

Penyusunan posisi rak pusat data harus mampu memisahkan jalur panas dan dingin. Jalur panas adalah bagian belakang dari rak pusat data. Jalur dingin adalah bagian depan dari rak pusat data sebagai jalur masuk udara dingin dari sistem pendingin.

Bagian pada rak pusat data yang kosong harus ditutup untuk menjaga pendinginan maksimal. Insulasi diperlukan untuk mencegah terjadinya pengembunan yang disebabkan oleh perbedaan temperatur antara ruang pusat data dengan ruang sekitarnya. Insulasi dapat berupa material pelindung berbahan *alumunium foil* berserat dan karet berbahan NBR sesuai ISO 6944-1.

d. Spesifikasi sistem jaringan data

Pusat data memiliki topologi jaringan data terperinci pada area ruang pusat data dan ruang interkoneksi telekomunikasi. Pusat data memiliki topologi distribusi jaringan utama dari ruang pusat data kepada pengguna jasa pusat data. Distribusi jaringan dapat menggunakan berbagai moda kabel dan berbagai perangkat komunikasi serta memiliki label kabel. Pusat data memiliki sistem monitoring jaringan dengan *fitur* peringatan dini dan alur alternatif sesuai dengan kategori strata pusat data.

e. Spesifikasi sistem kebakaran

Spesifikasi sistem kebakaran ditinjau dari berbagai aspek, seperti pemilihan dan pemasangan peralatan pemadam kebakaran (seperti *sprinkler,* alat pemadam api, dan detektor asap), sistem alarm, konfigurasi jaringan, dan prosedur pengujian dan pemeliharaan. Tujuan dari tinjuan spesifikasi ini adalah untuk memastikan bahwa sistem kebakaran dapat bekerja secara efektif dan efisien dalam mencegah, mendeteksi, dan memadamkan kebakaran terjadi, sehingga dapat melindungi keamanan dan keselamatan manusia serta properti yang berharga. Sistem pemadam kebakaran yang ada di pusat data perlu dipantau dan dievaluasi secara periodik. Pusat data hendaknya memiliki sistem monitoring dan deteksi dini bahaya kebakaran yang meliputi deteksi asap dan deteksi panas dengan moda sinar ultra.

f. Spesifikasi sistem *monitoring* lingkungan

Pusat data memiliki sistem *monitoring* lingkungan yang terdiri dari:

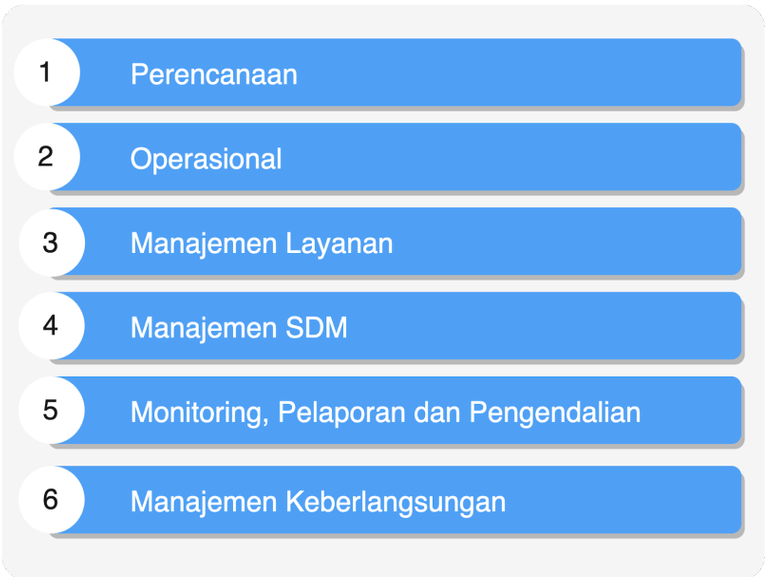
- stabilitas tegangan arus listrik dan penggunaan daya listrik yang dapat memberikan peringatan sebelum terjadi kelebihan beban;
- suhu perangkat serta kelembaban relatif ruangan di dalam area pusat data dan area telekomunikasi; dan
- sistem pemipaan dengan *fitur monitoring* kebocoran pipa air atau genangan di bawah *raised floor*.

g. Spesifikasi sistem keamanan fisik

Spesifikasi sistem keamanan fisik mencakup berbagai aspek seperti pemilihan dan pemasangan perangkat keamanan fisik (seperti kamera, sensor gerak, dan alarm), konfigurasi jaringan, sistem kontrol akses, dan prosedur pengujian dan pemeliharaan. Spesifikasi ini bertujuan untuk memastikan bahwa sistem keamanan fisik dapat bekerja sesuai dengan tujuan dan kebutuhan pengguna, serta dapat melindungi aset dan sumber daya dari ancaman keamanan. Moda memasuki pusat data bisa dengan mempergunakan kartu akses elektronik, biometrik atau pemindai jari. Penyambungan interkoneksi telekomunikasi memerlukan persetujuan pihak penyedia jasa telekomunikasi dan pengawas penyedia jasa layanan pusat data untuk keamanan pusat data ditetapkan perimeter tertentu sesuai dengan kategori strata pusat data.

2. SNI No 8799-2:2019 tentang Panduan Manajemen Pusat Data

Standar ini bertujuan untuk menyediakan panduan tentang desain dan penetapan pengaturan manajemen pusat data, mengklarifikasi peran dan tanggung jawab pemangku kepentingan utama di dalam penyelenggara pusat data, serta menyediakan contoh-contoh untuk dipertimbangkan dalam manajemen pusat data. Manajemen pusat data perlu diterapkan secara sistematis dan konsisten agar penyediaan layanan pusat data yang berkualitas dapat dilakukan secara efektif dan efisien. Standar Panduan Manajemen Pusat Data dapat digunakan oleh penyelenggara yang bertanggung jawab atas manajemen atau pengelolaan Pusat Data, meliputi: perencanaan, operasional, manajemen layanan, manajemen SDM, monitoring, pelaporan dan pengendalian, serta manajemen keberlangsungan.



Gambar 2.2.2.2.2 SNI: No 8799-2:2019-Panduan Manajemen Pusat Data

Panduan Manajemen Pusat Data sebagai berikut :

a. Perencanaan

Meliputi analisis kebutuhan, serta manajemen risiko dan kesesuaian.

b. Operasional

Meliputi organisasi penyelenggara pusat data, sistem manajemen layanan operasional pusat data, infrastruktur (lokasi pusat data, manajemen fasilitas pusat data, manajemen aset, manajemen konfigurasi).

c. Manajemen layanan

Meliputi manajemen layanan pusat data (sistem manajemen tingkat layanan, manajemen keselamatan, manajemen keamanan, dan manajemen proyek.

d. Manajemen SDM

Meliputi pengelolaan kompetensi, pelatihan, dan manajemen kinerja.

e. Monitoring, pelaporan dan pengendalian

Lingkup monitoring meliputi aktivitas pada gedung pusat data, aktivitas yang sedang berlangsung. Pelaporan kejadian tercatat dengan rincian waktu kejadian, waktu pelaporan, dan resolusi akhir kejadian. Perubahan kendali tercatat dalam dokumen pengendalian.

f. Manajemen keberlangsungan

Meliputi manajemen keberlangsungan kegiatan, dan manajemen keberlangsungan lingkungan.

g. Pengembangan Pusat Data

1. Topologi Pusat Data

Terdiri dari sistem-sistem pendukung, infrastruktur utama, dan infrastruktur pendukung pusat data. Rincian topologi pusat data *sebagai berikut :*

a. Sistem–sistem pendukung pusat data meliputi:
   - Sistem kelistrikan;
   - Sistem pendingin dan kelembaban;
   - Sistem pemadam kebakaran;
   - Sistem pengkabelan;
   - Desain ruang komputer, meliputi: *raised floor, cable tray, dan lokasi rack pusat data*;
   - Sistem keamanan;
   - Sistem pencahayaan; dan
   - Sistem pemantau lingkungan.

b. Infrastruktur Utama pusat data meliputi :
   - Infrastruktur jaringan;
   - Infrastruktur pusat data & *storage;*
   - Model pusat data; dan
   - Aplikasi pendukung (*Software*).

c. Infrastruktur Pendukung pusat data meliputi :
   - *Local Area Network;*
   - *Wireless LAN;*
   - WAN;
   - *Remote Access* dan VPN;
   - Internet; dan
   - Telekomunikasi.

2. Ruang Pendukung

Ruang pendukung pusat data adalah ruangan–ruangan untuk menempatkan perangkat–perangkat pendukung operasional pusat data seperti ruang perangkat sistem pendingin dan kelembaban, ruang perangkat *fire suppression* dll. Ruang operasional dan pemantauan pusat data juga termasuk ruang pendukung pusat

data. Rincian ruang pendukung pusat data yang direkomendasikan antara lain:

a. *Lobby*

   Lokasi ruang tunggu tamu, rekanan, penukaran kartu identitas dengan kartu akses.

b. *Security*

   Lokasi ruang operasi keamanan meliputi pemantauan *CCTV*, kontrol akses ke ruangan.

c. *Office*

   Ruang kerja administrasi pusat data termasuk ruang kepala pusat data.

d. *Facility Control*

   Ruang kontrol fasilitas pusat data seperti kontrol suhu & kelembaban, power, listrik dan lain – lain.

e. *Hall*

   Ruang serba guna yang bisa digunakan untuk kegiatan meeting dalam jumlah besar atau lainnya.

f. *Operations Command Center*

   Petugas memonitor pusat data melalui *dashboard* yang ditayangkan dalam layar lebar.

g. *Network Room*

   Lokasi rak perangkat jaringan dan keamanan jaringan. Semua struktur kabel data baik UTP maupun *Fiber optic* berakhir di ruang jaringan.

h. *Meet Me Room*

   Ruang terminasi (akhir) kabel jaringan dari *provider internet* (ISP), dan telekomunikasi.

i. *Network Operating Center*

   Ruang pemantauan kinerja jaringan pusat data yang ditayangkan melalui dashboard.

j. *Meeting Room*

   Ruang pertemuan untuk rapat atau diskusi pengelola pusat data.

k. *Fire Suppression System*

   Ruang untuk menempatkan perangkat – perangkat pendukung sistem pemadam kebakaran (*fire suppression*).

l. UPS

   Ruang untuk perangkat UPS pendukung catu daya cadangan ruang pusat data, lampu, cctv, *access control* dll.

m. *UPS Battery*

   Ruang *battery* UPS yang terpisah dari UPS sehingga mudah untuk perawatan dan penggantian *battery*.

n. *Loading Dock*

Tempat untuk menerima peralatan yang baru datang untuk pusat data.

o. *Build Room/Staging Area*

Tempat untuk membangun dan mengkonfigurasi peralatan yang akan digunakan bagi pusat data.

p. *Chiller*

Ruang untuk perangkat *chiller* pendingin suhu.

q. *Warehouse*

Ruang untuk perangkat listrik.

r. *Genset Room*

Ruang untuk meletakkan perangkat generator pembangkit listrik cadangan (genset).

s. *Trafo*

Ruang untuk meletakkan trafo listrik dari PLN.

t. *Solar Tank*

Ruang untuk menyimpan solar sebagai bahan bakar genset.

u. Ruang Mekanik

Ruang kerja *Mechanical Engineering* (ME).

v. Ruang *Sparepart*

Ruang gudang penyimpanan suku cadang *(sparepart)* perangkat *mechanical* dan listrik pusat data.

3. Sistem Kelistrikan

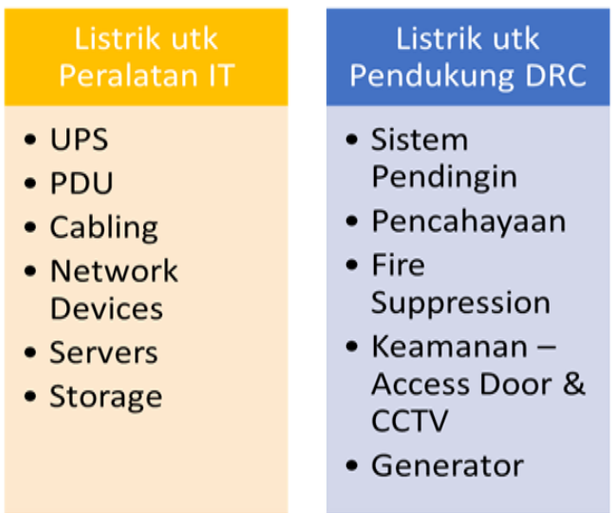
Sistem kelistrikan meliputi catu daya utama dan catu daya cadangan. Catu daya utama berasal dari listrik PLN sedangkan catu daya cadangan berasal dari generator, dan UPS. Ketentuan tentang sistem kelistrikan di pusat data sebagai berikut :

a. Kabel daya masuk ke dalam bangunan pusat data determinasi di ruang kendali penyambungan listrik yang handal;
b. Daya listrik utama paling sedikit 20% lebih besar dari proyeksi beban puncak di mana pusat data berada;
c. Tersedianya catu daya listrik alternatif seperti *generator standby* dengan kapasitas yang memadai untuk operasional minimal 3 jam selama kejadian gangguan listrik utama;
d. Perangkat *pusat data, storage, jaringan, keamanan pusat data & jaringan, CCTV, access control,* penerangan harus diproteksi dengan *Uninterruptible Power Supply* (UPS) atau catu daya cadangan lainnya;
e. UPS atau catu daya cadangan lainnya harus memiliki kapasitas memadai untuk memasok beban pusat data sampai catu daya

alternatif mampu memikul beban perangkat pusat data *(steady-state)*;

f. Kapasitas UPS harus lebih besar dari proyeksi beban puncak perangkat pusat data. Kapasitas beban rata-rata tidak lebih besar dari 80% kapasitas UPS;
g. UPS memiliki sistem pelaporan, pemantauan kinerja, dan sistem peringatan;
h. UPS yang digunakan telah memiliki jaminan dari pabrikan untuk dapat berfungsi sesuai spesifikasinya;
i. Bangunan harus dilengkapi dengan sistem proteksi petir;
j. Kabel komunikasi tembaga dari luar gedung diproteksi dengan peredam tegangan lebih (*surge suppressor*) sebelum ke ruang pusat data;
k. Ruang pusat data memiliki terminal pembumian (*grounding*) tembaga yang menjadi titik acuan pembumian ruangan tersebut;
l. Sistem grounding untuk peralatan pusat data harus dibedakan dengan peralatan lainnya seperti sistem penangkal petir pada bangunan pusat data; dan
m. Semua benda logam harus terikat ke tanah termasuk lemari, rak, *PDU, CRAC (AC* Ruangan pusat data), jalur kabel, dan setiap *raised floor* dengan *resistansi grounding* kurang dari 1 Ohm.

Kebutuhan listrik di pusat data untuk mendukung dua komponen yakni peralatan TI dan peralatan pendukung seperti tabel di bawah ini :



Gambar 2.2.2.2.3. Kebutuhan Listrik Pusat Data

4. Distribusi Listrik Ruang Pusat Data

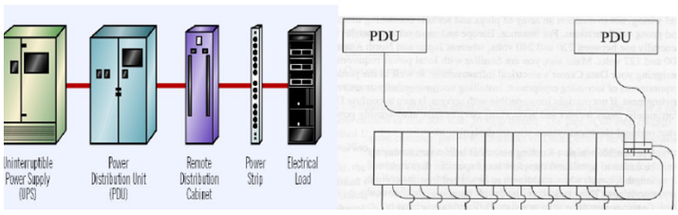
Sistem kelistrikan di pusat data akan didistribusikan ke perangkat utama di dalam ruang komputer pusat data dengan dua teknik yakni:

a. Distribusi secara langsung dari PDU (*Power Distribution Units*)

Dari PDU listrik akan didistribusikan ke setiap lokasi kabinet tanpa melalui perantara apapun. Namun untuk pusat data yang berkapasitas besar hal ini tidak mungkin dilakukan karena tidak efisien dari segi pengkabelan.

b. Distribusi melalui *panel circuit*

PDU akan menuju ke *panel circuit* dan dari tempat tersebut akan didistribusikan ke masing-masing lokasi kabinet. Hal ini, jauh lebih efisien dari segi pengkabelan karena dapat meminimalkan jarak yang jauh antara lokasi kabinet pusat data dengan PDU.



Gambar 2.2.2.2.4 Distribusi Listrik dari PDU melalui *Panel Circuit.*

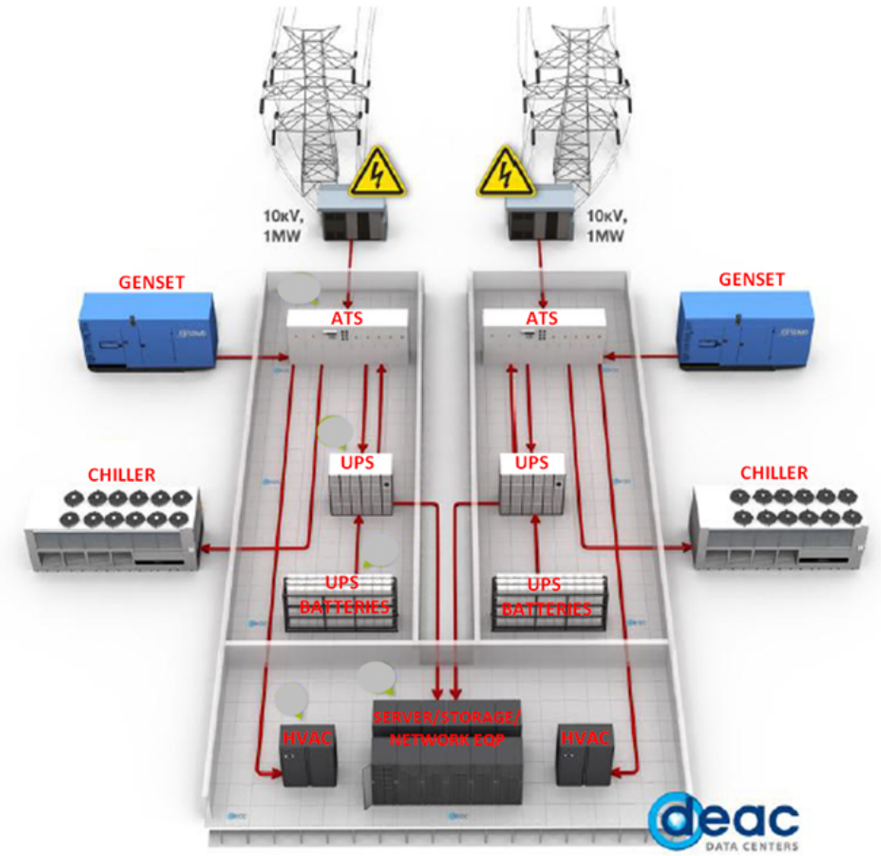
Gambar di atas adalah distribusi listrik dengan menggunakan *panel circuit* yang tersebar di perangkat *remote distribution cabinet* untuk mendistribusikan listrik dari perangkat UPS ke beberapa panel sirkuit melalui *PDU. Distribution cabinet power* dari perangkat UPS akan diteruskan ke *PDU* untuk selanjutnya didistribusikan ke beberapa panel circuit *(remote distribution cabinet)*. Untuk selanjutnya *power* akan didistribusikan ke *power strip* yang ada di tiap rak *cabinet*. Di setiap *power strip* terdapat perangkat untuk pemantauan beban listrik (*electrical load*).

5. Redudansi Sumber Listrik

Untuk mencapai tingkat reliabilitas yang tinggi maka diperlukan redudansi pada perangkat utama maupun cadangan dan jalur masuk ke pusat data. Saluran listrik ke lokasi pusat data berasal dari sumber gardu listrik yang berbeda. Selain itu, jalur masuk ke pusat data dari arah yang berbeda juga.

Redudansi sumber listrik utama (PLN) dan sumber listrik cadangan diperlukan untuk menjamin keberlangsungan dan kehandalan dari pusat data. Redudansi meliputi sumber listrik PLN dari gardu listrik

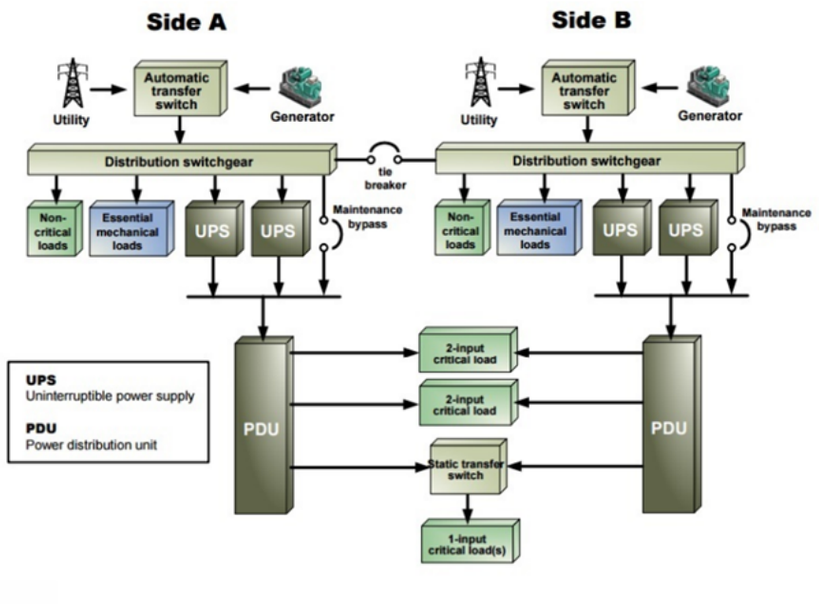
yang berbeda, jalur (lintasan) aliran listrik dari gardu menuju kawasan pusat data. Selain itu juga redudansi dari perangkat sumber listrik cadangan seperti generator, UPS, dan *automatic transfer switch (ATS).*



Gambar 2.2.2.2.5. Instalasi Jaringan Listrik dan Pendukung DC

Gambar di atas adalah gambar fisik instalasi sistem kelistrikan yang redundan. Listrik utama *DC* berasal dari dua sumber yang berbeda dengan jalur masuknya pun berbeda. Perangkat pendukung sistem kelistrikan, sistem pendingin diletakkan pada posisi yang berbeda yang memiliki jalur distribusi sendiri. Desain ini untuk menghindari adanya kegagalan pada sistem listrik atau pendingin karena adanya kerusakan pada salah satu jalur. Rak pusat data akan memiliki dua *power strip* dan akan ada *receptacle* yang berbeda juga disetiap pusat data.

Gambar di bawah ini adalah topologi infrastruktur jaringan kelistrikan secara logik. Setiap PDU terhubung ke sumber listrik cadangan (*UPS*) yang berbeda dengan sumber listrik utama dari dua sumber juga.



Gambar 2.2.2.2.6. Instalasi Logik dari Sistem Kelistrikan

6. Listrik Cadangan *(Standby Power)*

Sistem listrik yang berperan sebagai *standby power* pada pusat data merupakan sumber tenaga *back-up*-an ketika sistem listrik utama mengalami kegagalan. *Standby power* yang dibuat mempertimbangkan 3 (tiga) aspek yaitu redudansi, kesederhanaan, dan biaya. Berbagai perangkat terkait dengan *standby power* pada pusat data antara lain generator, *UPS*, dan baterai.

Berdasarkan fungsinya, *UPS* merupakan sebuah perangkat elektronik yang mampu menggantikan sementara, bahkan memperbaiki pasokan listrik yang diterima oleh satu atau beberapa perangkat yang dikoneksikan ke jalur keluaran *UPS*. Topologi *UPS* ada tiga, yaitu *offline UPS*, *online* UPS atau yang dikenal dengan *line-interactive* UPS, serta *true-online double conversion UPS*. Ketiganya memiliki perbedaan sangat mendasar, terutama pada besaran waktu perpindahan dari sumber listrik utama atau PLN ke sumber listrik *UPS,* yaitu baterai. Jika terjadi putus aliran listrik dari PLN, jika beban yang akan di-*back-up* oleh UPS adalah beban yang kritikal, maka sebaiknya menggunakan *True-online Double Conversion UPS* karena waktu perpindahannya adalah nol detik.

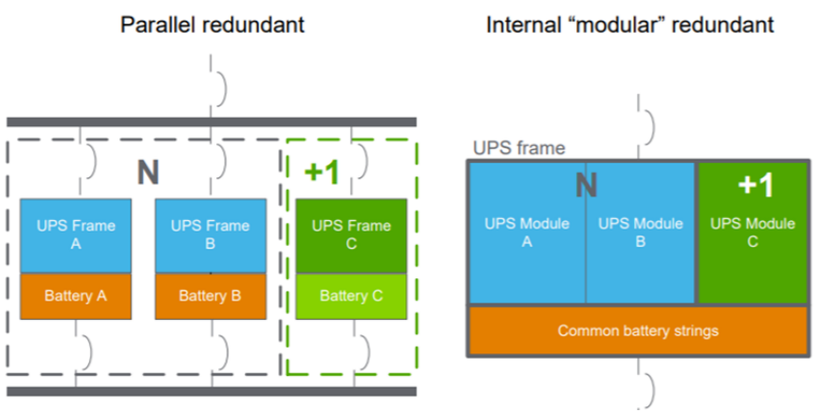
Selain lamanya waktu perpindahan, yang perlu dicatat adalah kehandalan dari masing-masing tipe terhadap kemampuan menangani permasalahan yang timbul dari jaringan listrik PLN, yaitu antara lain adalah kemampuan menangani tegangan naik atau turun, harmonik, *sag* (mati sesaat atau berkedip), *swell* (lonjakan tegangan), pergeseran fase, dan kemampuan untuk menerima daya dari genset sebagai pengganti listrik PLN untuk

beberapa jam per-hari. *UPS* untuk *DC* sebaiknya memiliki kriteria antara lain:

- *UPS* memiliki *power factor* 0.9% agar efisien dan dapat diandalkan;
- *Runtime UPS* atau kemampuan *UPS* hidup selama sumber utama mati yakni UPS dapat bertahan 30 menit sampai 60 menit; dan
- Perhitungan kapasitas *UPS* adalah lebihkan 25% dari beban puncak.

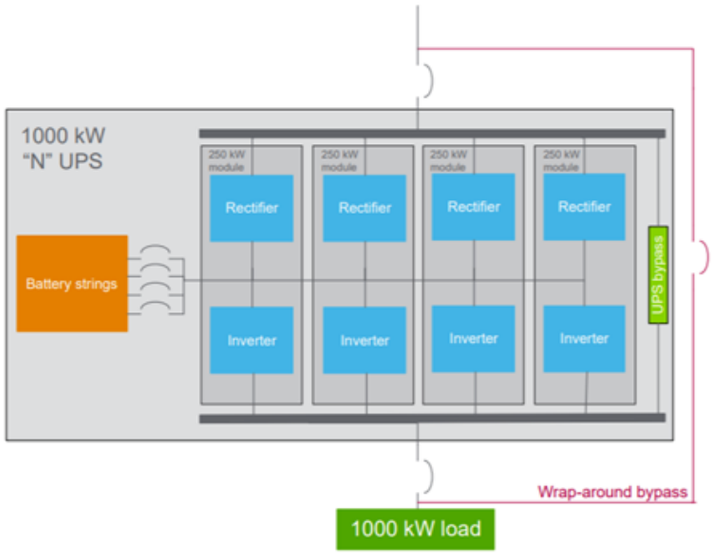
a. Redudansi UPS

Redudansi UPS terdiri dari dua model yakni *parallel redundant* atau *internal modular redundant*. *Parallel redundant* merupakan perangkat *UPS* yang terdiri dari *UPS Module* dengan baterai redundan N+1, dimana N adalah jumlah *UPS* pada beban puncak. Selain itu, *internal modular redundant* merupakan jumlah modul *redundant* tanpa baterai. Secara umum, gambar di bawah memberikan informasi topologi perangkat *UPS* dengan dua model, yakni: *parallel redundant* dan *internal modular redundant*.



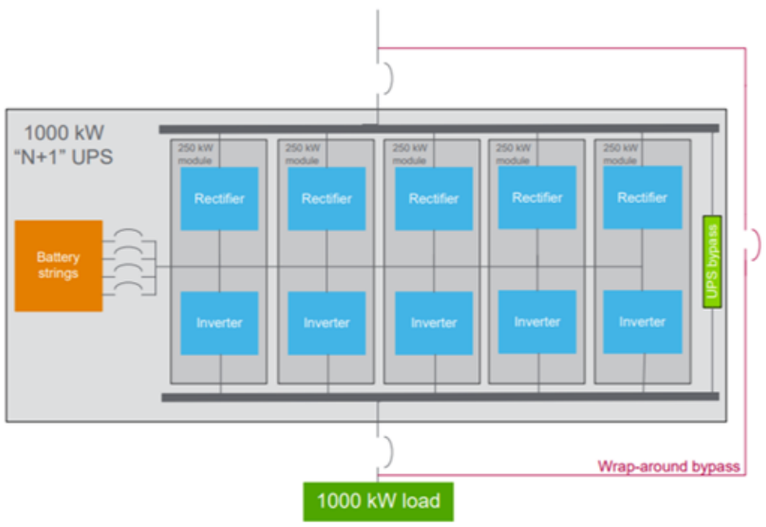
Gambar 2.2.2.2.7. Perbandingan Dua Model UPS DC

Gambar berikut menunjukkan contoh topologi perangkat UPS dengan kapasitas 1000kW yang terdiri dari 4 modul masing-masing 250kW, dimana *baseline* 1N *configuration* adalah satu UPS dengan empat modul tanpa *redundant*.



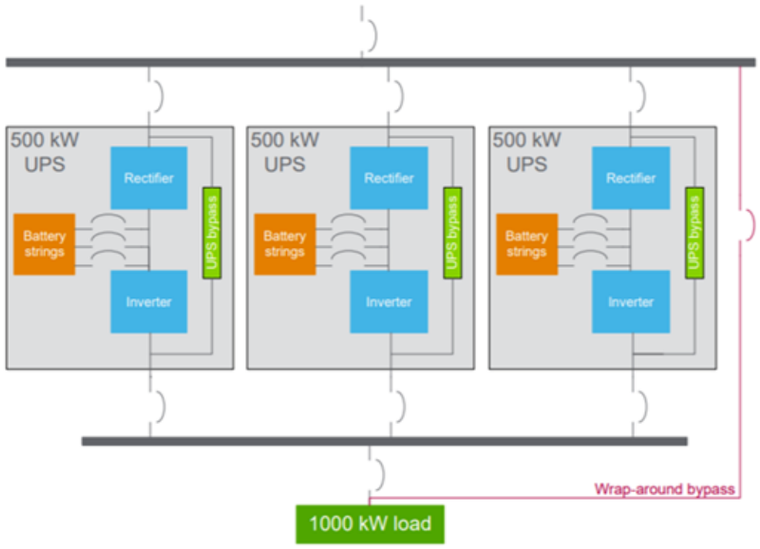
Gambar 2.2.2.2.8. UPS dengan Empat Modul Tanpa Redudansi

Gambar berikut menunjukkan topologi *UPS* dengan konfigurasi N+1 yang redundan secara internal dengan model modular. Terdapat lima modul *UPS,* yaitu empat modul utama dan satu cadangan.



Gambar 2.2.2.2.9. UPS dengan *Internally Modular Redundancy*

Gambar berikut menunjukkan topologi UPS dengan konfigurasi N+1 yang redundan secara paralel. UPS utama terdiri dari dua modul dengan masing-masing daya 500 kW, serta satu modul cadangan dengan daya 500 kW.



Gambar 2.2.2.2.10. UPS dengan *Parallel Redundant N+1*

b. *Fault Tolerance* UPS

Fault Tolerance adalah kegiatan yang memungkinkan suatu sistem untuk terus beroperasi (dalam hal ini, mendukung beban TI) jika terjadi kegagalan beberapa komponen. Beberapa *UPS* dirancang dengan tingkat toleransi kesalahan yang lebih tinggi daripada yang lain. Oleh karena itu, dalam pemilihan *UPS* penting untuk mempertimbangkan atribut desain toleransi kesalahan provinsi terutama jika arsitektur yang dipilih terdiri dari satu bingkai *UPS* (seperti pada konfigurasi 1 dan 2). Di bawah ini contoh atribut desain toleransi kesalahan:

- Redudansi modul daya (*inverter*/penyearah);
- Redudansi penggemar;
- Redudansi catu daya pada pengontrol;
- Redudansi *string* baterai;
- Redudansi bus komunikasi;
- Redundansi dalam sistem kontrol; dan
- Saklar statis berukuran lebih besar dari beban maksimum yang diharapkan untuk mengakomodasi muatan *in-rush*/step peralatan IT.

7. Sistem Pendingin & Kelembaban

Sistem pendingin berfungsi untuk menjaga suhu dan kelembaban di ruang pusat data tetap terjaga sesuai dengan standar yang telah ditetapkan. Jika suhu terlalu panas atau terlalu dingin dapat menyebabkan kerusakan pada perangkat di dalam ruang pusat data.

Kriteria umum untuk sistem pendingin dan kelembaban adalah :

- Temperatur dan kelembaban ruangan dijaga dan dikendalikan sesuai dengan kebutuhan operasional normal perangkat di ruang pusat data yang paling peka;
- Peralatan pengatur temperatur dan kelembaban harus dihubungkan ke catu daya utama (didukung oleh catu daya alternatif);
- Memiliki skalabilitas dan adaptabilitas yang sangat baik; dan
- Sudah terstandarisasi.

Keadaan temperatur dan kelembaban yang harus dijaga di dalam pusat data:

- Temperatur kering: 200C–250C (680F-770F), dengan rata-rata keadaan temperatur normal di set menjadi 220C±100C;
- Kelembaban relatif (*Relative Humidity*) adalah jumlah air di udara pada suhu lingkungan : 40%-50%, dengan titik normal berada pada 45%±5%;
- Titik embun pada rentang 41,90F sampai 590F maksimum: 210C (69.80F); dan
- Perubahan maksimum yang boleh terjadi dari batas suhu sekarang adalah sebesar 50 C (90F) per jam.

Berikut ini adalah penjelasan dari perangkat sistem pendingin, tekanan udara, kelembaban, konsumsi listrik sistem pendingin, dan teknik pendinginan ruangan/pusat data :

Perangkat Sistem Pendingin

HVAC (*Heating, Ventilation, Air Conditioning*) bertujuan untuk menjaga agar temperatur tetap dalam keadaan rendah dan konstan serta menyebarkan titik-titik panas yang terletak di pusat data. Temperatur yang rendah sangat diperlukan untuk efisiensi operasi pusat data dan perangkat jaringan. Sistem pendingin pada pusat data pada prinsipnya adalah sistem aliran udara dingin, yang terbagi menjadi tiga perangkat utama, yaitu: *air handler, chiller, dan cooling towers*. Sistem pendingin dapat melakukan redudansi dengan memasang lebih dari satu air *handler* dan menara pendingin tambahan untuk setiap *chiller*. Selain itu, suplai air yang dibutuhkan untuk menciptakan udara dingin juga perlu dijamin keberadaannya dengan cara seperti membangun *container* penyimpan air yang dapat diandalkan.

Tekanan Udara

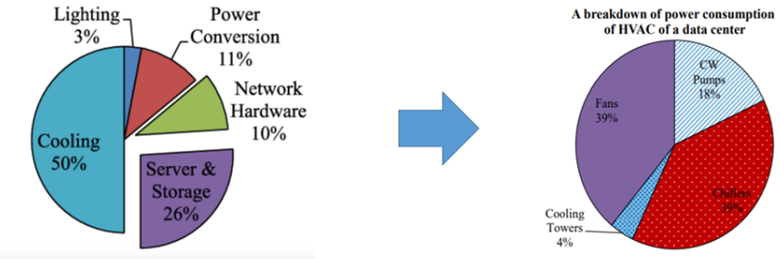
Tekanan udara pada pusat data harus dijaga pada level tertentu yang disebut sebagai tekanan statis. Pusat data didesain memiliki tekanan antara 0.2-0.5 *in. wc* guna menjaga agar tekanan udara tetap stabil maka periksa seluruh ruangan apakah telah tertutup dengan baik dan yakin bahwa tidak ada lubang sedikit pun. Mayoritas *handler* membutuhkan *buffer* sekitar 36-42 in (91.4-106.7 cm) sehingga perlu diletakan jauh dari *DC* air *handler*.

Kelembaban

Kelembaban merupakan konsentrasi uap air di udara. Kelembaban relatif menjadi salah satu aspek yang perlu dijaga dalam ruangan pusat data. Kelembaban relatif adalah persentase perbandingan dari jumlah uap air yang ada di udara dengan jumlah uap air di udara kering. Perangkat pusat data dan jaringan dapat berfungsi pada rentang level kelembaban yang cukup panjang yaitu sekitar 20%-80%. Menjaga kelembaban relatif dalam keadaan normal berfungsi untuk mencegah terjadinya korosi pada beberapa perangkat di pusat data karena penguapan (kelembaban tinggi) atau mencegah munculnya elektrostatis pada beberapa perangkat metal (kelembaban yang rendah). Cara yang dilakukan adalah melengkapi *Air Handling Unit (AH)* dengan kemampuan humidification atau melalui penggunaan unit-unit *humidification* yang terpisah dari *Air Handling Unit (AH).* Kelembaban relatif yang memungkinkan untuk suatu ruangan pusat data adalah sekitar 45%-55%, yaitu level kelembaban relatif normal sebesar 50% dengan tingkat sensitivitas sekitar 10%, yang memungkinkan variasi pada level kelembaban sehingga komponen infrastruktur tidak konstan berada level tersebut.

Konsumsi Listrik Sistem Pendingin

Konsumsi listrik pusat data terbesar adalah pada sistem pendingin & kelembaban (50%), pusat data & *storage* (26%), perangkat jaringan (10%), *power conversion* (11%), dan *lighting* (3%). Untuk sistem pendingin & kelembaban, komponen *chiller* mengkonsumsi daya listrik terbesar (39%), kipas (*fans)* (39%), *CW Pomps* (18%) dan paling kecil adalah *cooling towers* (4%).

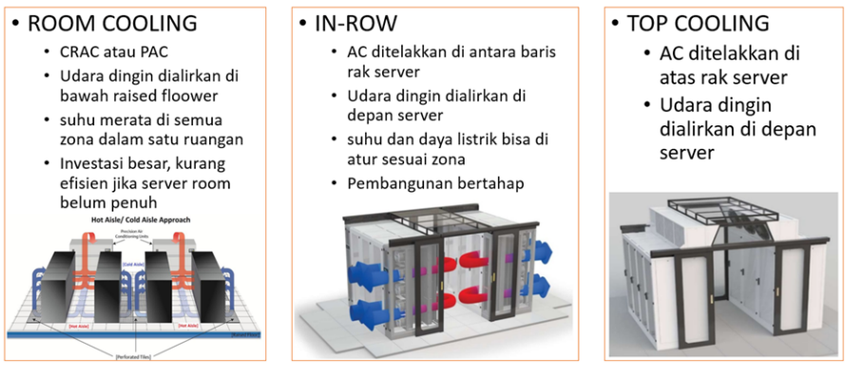


Gambar 2.2.2.2.11. Grafik Konsumsi Listrik di Pusat Data

Dari informasi di atas, diperlukan sistem pendingin & kelembaban yang efisien dan efektif serta dukungan dari perangkat yang ada. Sistem pendingin & kelembaban berfungsi untuk mendinginkan perangkat pusat data, storage, dan perangkat jaringan. Jika kapasitas ruang pusat data belum maksimal, maka diperlukan strategi agar tidak terjadi pemborosan karena prinsipnya adalah mendinginkan pusat data bukan ruang pusat data.

8. Teknik Pendinginan Ruangan/Pusat Data

Terdapat tiga teknik pendinginan ruangan pusat data atau rak pusat data yakni R*oom Cooling atau Cooling Room Air Conditioner (CRAC), IN-ROW,* dan *TOP Cooling.*



Gambar 2.2.2.2.12. Perbandingan Keuntungan dari Tiga Model Sistem Pendinginan Pusat Data

a) ROOM-COOLING

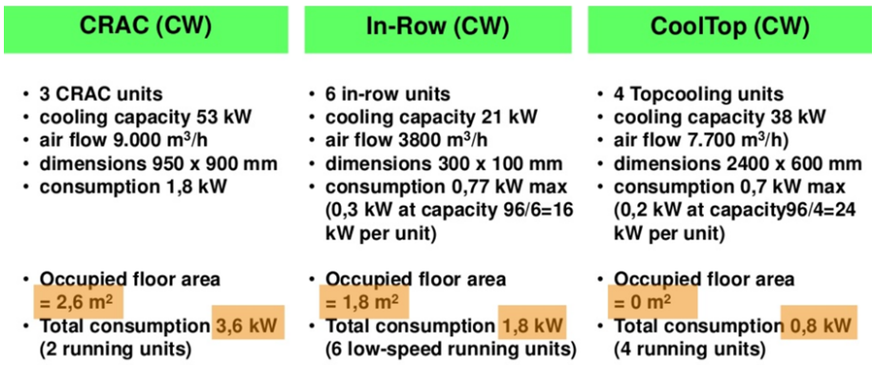
- Fungsi mendinginkan seluruh ruangan pusat data secara merata;
- *CRAC/PAC* disebar di sisi-sisi ruang pusat data;
- Jalur udara dingin (*cold aisle*) mengalir dari bawah *raised floor* naik ke atas melalui lubang – lubang kecil di papan *raised floor* arah depan *rack* pusat data;
- Jalur udara panas (*hot aisle*) yang berasal dari belakang *rack* pusat data akan mengalir ke perangkat *CRAC; dan*
- Kurang efisien jika ruang *pusat data* belum terisi penuh.

b) IN-ROW

- *CRAC/PAC* tidak lagi disebar di sisi-sisi ruang pusat data tapi sudah disebar di barisan *rack* pusat datanya;
- *CRAC/PAC* sudah disebar di barisan *rack pusat data*nya, di dalam barisan *rack-rack pusat data* ini di sisipkan *cooling system* yang mendinginkan udara panas di belakang pusat data dan menghembuskan ke sisi depan pusat data;
- Menutup jalur udara panas (*hot containment aisle*) agar tidak bercampur dengan jalur udara dingin, semua udara panas di dalam *hot containment* ini akan didinginkan oleh *CRAC* yang ada di samping *rack* pusat data; dan
- Tingkat efisiensi tinggi karena pembangunan bisa secara bertahap tergantung kebutuhan *rack* pusat data.

c) TOP-COOLING

- *CRAC/PAC* tidak lagi disebar di sisi-sisi ruang *pusat data* tapi diletakkan di atas *rack* pusat data;
- Di atas *rack-rack pusat data* ini disisipkan *cooling system* yang menghembuskan udara dingin ke sisi depan *pusat data* dan mendinginkan udara panas di belakang pusat data; dan
- Tingkat efisiensi tinggi paling tinggi karena tempat yang dibutuhkan paling kecil, konsumsi daya listrik paling kecil juga di bandingkan dua teknik lainnya.



Gambar 2.2.2.2.12. Perbandingan Tiga Model Sistem Pendingin Pusat Data

Berdasarkan gambar diatas diperoleh informasi perbandingan teknik pendinginan ruang pusat data, teknik *CoolTop* mengkonsumsi daya listrik paling kecil dibanding dua teknik lainnya sebesar 0,8kW. Selain itu luasan yang digunakan untuk perangkat pendingin juga paling kecil dibandingkan dua lainnya (0 m2) karena perangkat di pasang di atas *rack* pusat data tidak menambah ruang di bawah. Kesimpulannya teknik *CoolTop* memiliki tingkat efisiensi paling tinggi untuk mendinginkan *rack*

pusat data. Pada kondisi ruang *pusat data* yang belum terisi penuh, teknik ini juga sebagai solusi menekan biaya listrik.

9. Fire *Suppression System*

Perlindungan pusat data dari api mempunyai tiga tujuan utama yakni: identifikasi adanya api (*detection*), pemberitahuan adanya api ke seluruh penghuni Pusat Data dan orang-orang yang berkepentingan (*alarm*), dan memadamkan api (*suppression*). Acuan Standar dalam pembangunan *fire suppression system* menggunakan standar dari *NFPA* (*National Fire Protection Association*). Tipe *Suppression System* yang ada antara lain:

a. Gas System

Sistem gas tidak merusak perangkat pusat data dan perangkat lain efektif tetapi waktu singkat.

- Inert Gas Suppression System = mengurangi kadar oksigen sampai 15% untuk memadamkan api sehingga ruangan masih bisa digunakan untuk bekerja; dan
- *Synthetic Gas Suppression = cooling mechanism* untuk memadamkan api dengan menggunakan beberapa tipe gas seperti FM-200, Halon 1301, CO2.

b. Water sprinklers

Sistem air dapat merusak perangkat pusat data dll, dapat digunakan untuk melindungi bangunan dan memadamkan api. Kriteria *Fire Suppression System* untuk pusat data adalah sebagai berikut :

- *QUICK*

  Sistem dapat memberikan respon cepat jika terjadi kebakaran untuk meminimalkan terjadinya kerusakan pada perangkat pusat data dll.
- *CLEAN*

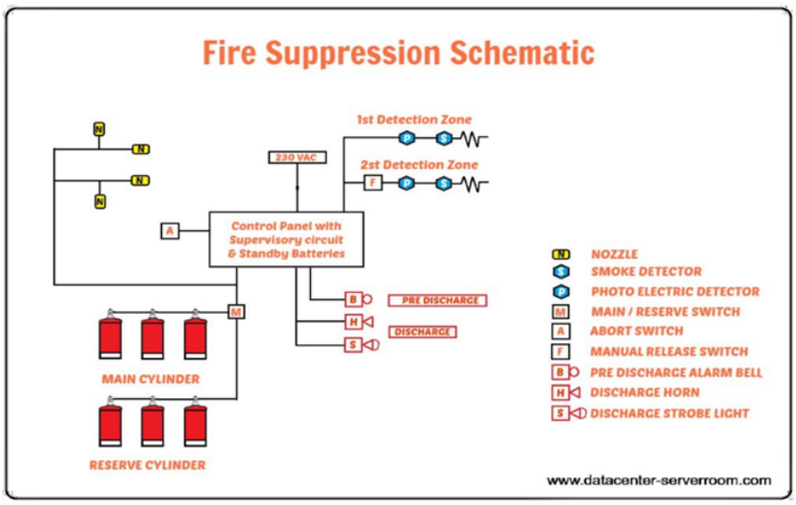
  Jika terjadi insiden adanya titik api dan setelah gas dilepas serta proses pemadaman, tidak ada sampah atau sisa gas yang tertinggal.
- *ODORLESS*

  Gas yang dikeluarkan tidak menimbulkan bau yang menyengat.
- *NON-TOXIC*

  Gas yang dikeluarkan tergolong aman untuk manusia (tidak beracun).
- *NON-CONDUCTIVE*

  Gas yang dikeluarkan bukan penghantar panas atau elektrik karena dapat menyebabkan kerusakan.
- *LOW STORAGE SPACE*

Perangkat utama dan pendukung hanya membutuhkan tempat yang kecil.



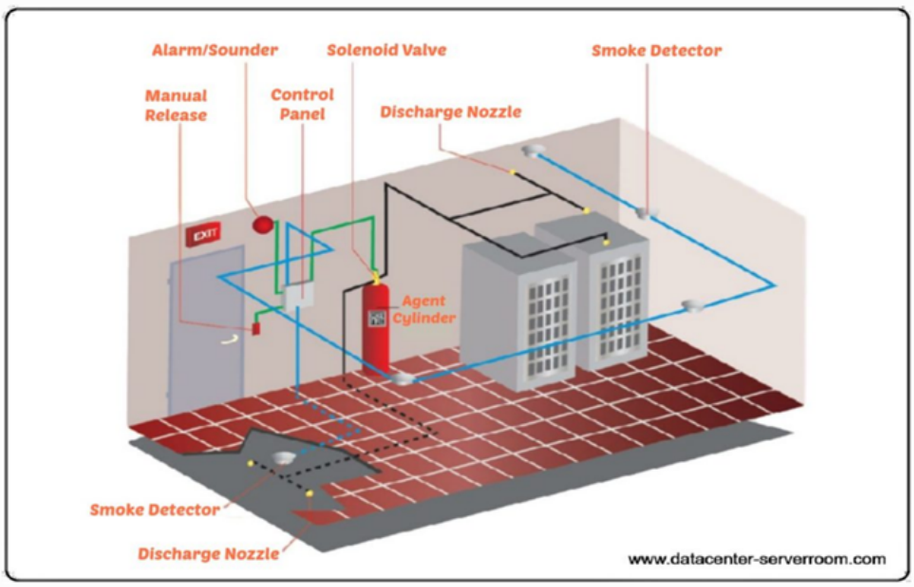
Gambar 2.2.2.2.13. *Skema Fire Suppression System* DC

Secara umum, sistem *fire suppression* terdiri atas elemen-elemen sebagai berikut:

1. Deteksi panas yang linier (kabel sensor panas), ditempatkan sepanjang *tray wire* dan jalur elektrik baik diatas maupun dibawah *raised-floor*. Alarm pada sensor dibunyikan pada sistem kontrol bukan untuk memicu bekerjanya sistem *fire suppression;*
2. Deteksi tipe *spot* secara *intelligent* (*photoelectric detector*);
3. Deteksi asap (*smoke detector*);
4. *Portable fire extinguisher;*
5. Agen pembersih sistem *fire suppression;* dan
6. *Pull station*, perangkat sinyal, dan sistem kontrol.

Sistem peringatan proteksi dini sangat penting untuk menghindari kerusakan dan kehilangan yang dapat terjadi selama status kebakaran belum benar-benar terjadi (atau awal terjadinya kebakaran), karena kerusakan peralatan yang signifikan dapat semata-mata terjadi karena asap atau pembakaran produk-produk lain terhadap peralatan elektronik. Contoh sebuah sistem peringatan proteksi dini adalah air sampling *smoke detection systems* yang menyediakan proteksi level lain untuk ruang komputer dan fasilitas-fasilitas pintu masuk terkait, ruang mekanik, dan ruang listrik. Sistem peringatan proteksi dini juga disediakan sebagai pengganti *smoke detectors* biasa, karena sensitivitas dan kapabilitas deteksinya jauh melampaui detektor konvensional.

Gambar berikut adalah topologi *fire suppression system* yang terdiri dari perangkat utama dan pendukung serta topologi instalasinya. Silinder tabung gas terdiri dari silinder utama dan silinder cadangan untuk redudansi. Gambar di bawah adalah instalasi *fire suppression system* di ruang pusat data. *Smoke detector* di pasang di atas rack pusat data dan di bawah *raised floor.*



Gambar 2.2.2.2.14. *Instalasi Fire Suppression System* Pusat Data

Ketentuan dalam pembangunan *fire suppression system* pusat data sebagai berikut :

a. Jumlah dan lokasi pintu darurat kebakaran sesuai dengan peraturan perundang-undangan;
b. Pintu darurat kebakaran dapat dibuka ke arah luar;
c. Lampu darurat dan tanda keluar diletakkan pada lokasi sesuai dengan peraturan perundang-undangan;
d. Titik panggil manual harus dipasang sesuai dengan peraturan perundang-undangan;
e. Dinding dan pintu ke ruang pusat data, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan ruangan penting lainnya memiliki tingkat terbakar (*fire-rating*) sesuai dengan peraturan perundang-undangan;
f. Ruang komputer harus diproteksi dengan sistem pendeteksi asap. Seluruh sistem deteksi asap bangunan harus diintegrasikan ke dalam satu alarm bersama;
g. Catatan pemeliharaan yang mencakup seluruh aspek yang berkaitan dengan deteksi api dan pemadaman harus tersedia untuk keperluan pemeriksaan;

h. Bukti pelatihan staf pada simulasi pengendalian kebakaran harus tersedia;
i. Ruang pusat data harus dilindungi dengan sistem pemadam kebakaran. Sistem pemadam kebakaran otomatis harus dapat diaktifkan secara manual;
j. Alat pemadam kebakaran harus ditempatkan sesuai ketentuan peraturan perundangan-undangan;
k. Semua tanda peringatan kebakaran harus ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan;
l. Seluruh sistem pendeteksi dan pemadam kebakaran harus didesain dan dipasang oleh tenaga ahli yang telah memenuhi persyaratan dan memiliki kompetensi di bidang desain dan pemasangan sistem pendeteksi dan pemadam kebakaran sesuai standar internasional/nasional atau regulasi nasional;
m. Jika ruang pusat data, ruang telekomunikasi, ruang mekanikal dan kelistrikan memiliki sistem pemadam api otomatis (*sprinkler*), maka sistem tersebut harus tipe *preaction*; dan
n. Jika ruang atau bangunan yang berdekatan dengan lokasi pusat data tidak memiliki sistem pemadam api otomatis (*sprinkler)*, maka risiko kebakaran harus dikaji.

10. Sistem Pengkabelan

Sistem pengkabelan mengambil peran dalam komunikasi antar item di dalam pusat data atau ke dunia luar. Sistem pengkabelan infrastruktur jaringan data di pusat data menjadi salah satu hal yang paling rumit untuk merancangnya. Beberapa kriteria sistem pengkabelan yang baik antara lain adalah:

a. Mampu menyediakan konektivitas yang luas *(wide channel-capacity)* dan terstruktur dengan baik (sesuai dengan ketentuan).
b. Sederhana, yang berarti struktur pengkabelan yang dibuat tidak rumit sehingga memudahkan relokasi atau *maintenance*.
c. *Scalable* dan fleksibel, dapat mengakomodasi kebutuhan mendatang dan perubahan yang terjadi, serta keragaman dari aplikasi *user* (servis yang dimiliki pusat data).

Pertimbangan desain sistem pengkabelan yang akan digunakan yaitu:

a. Kabel menyumbang kurang dari 10 persen dari total biaya infrastruktur jaringan.

b. Rentang hidup dari sistem kabel yang khas adalah 16 tahun ke atas, sehingga kabel adalah komponen yang terpenting dalam sistem pengkabelan terstruktur.
c. Hampir 70 persen dari semua jaringan yang bermasalah berasal dari pemasangan kabel yang tak memenuhi standar dan komponen kabel itu sendiri.

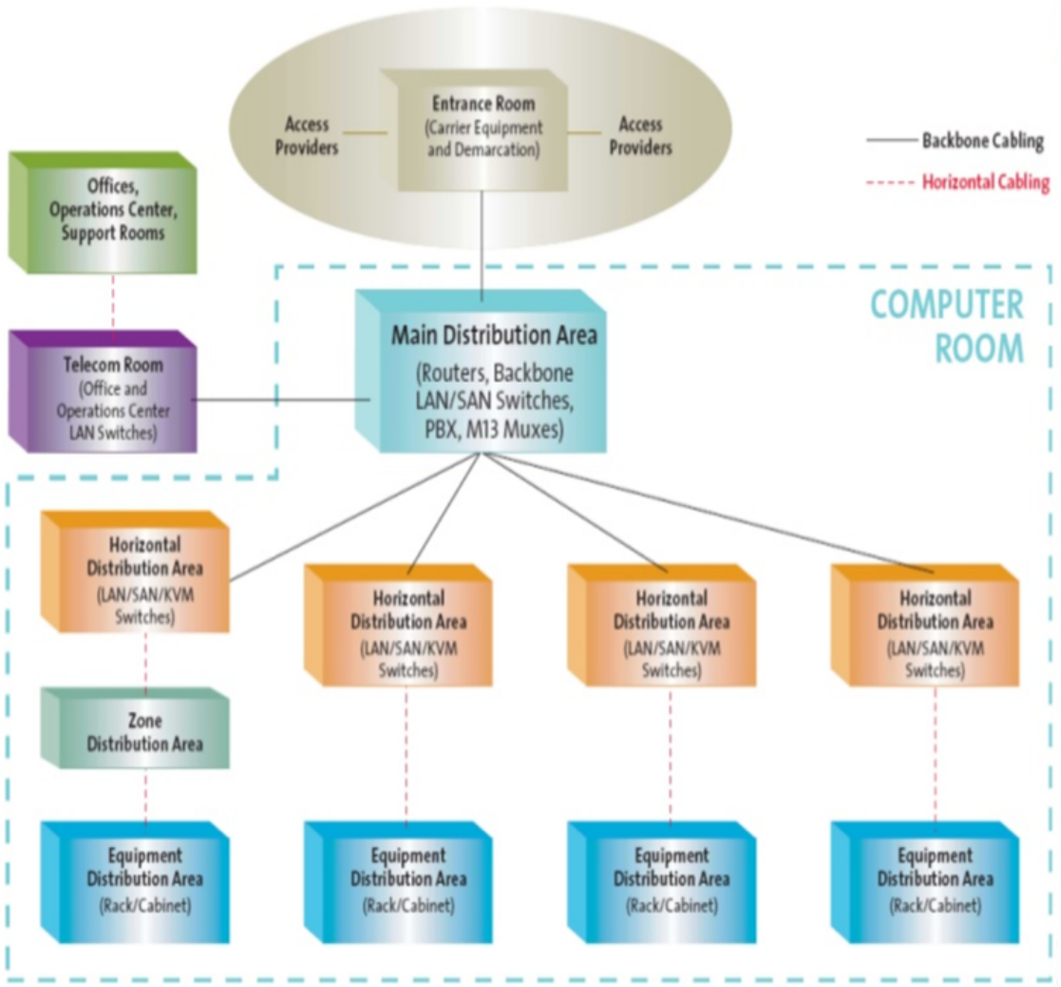
Beberapa ketentuan umum sistem pengkabelan listrik dan data di *DC* antara lain:

a. Kabel kelistrikan dan kabel data harus dipisah, beberapa kabel harus diisolasi untuk menghindari gangguan.
b. Sistem kabel di atas dan dibawah yang terstruktur serta terlindungi, mendukung kemudahan dalam instalasi dan keamanan dari hubungan arus pendek.
c. Jalur kabel data harus memiliki jarak dari jalur listrik dan jalur *grounding* anti petir sesuai standard ANSI/TIA-469-B.
d. Infrastruktur kabel sesuai standar TIA-942 :
    - Standar fiber optik jenis s*ingle mode;*
    - Jaringan backbone menggunakan *fiber optic multimode* dengan ukuran 50 *micron* kategori *lazer-optimized;*
    - UTP CAT6;
    - *Backbone fiber optic* maksimal 300 meter; dan
    - Horizontal kabel maksimal 100 meter.

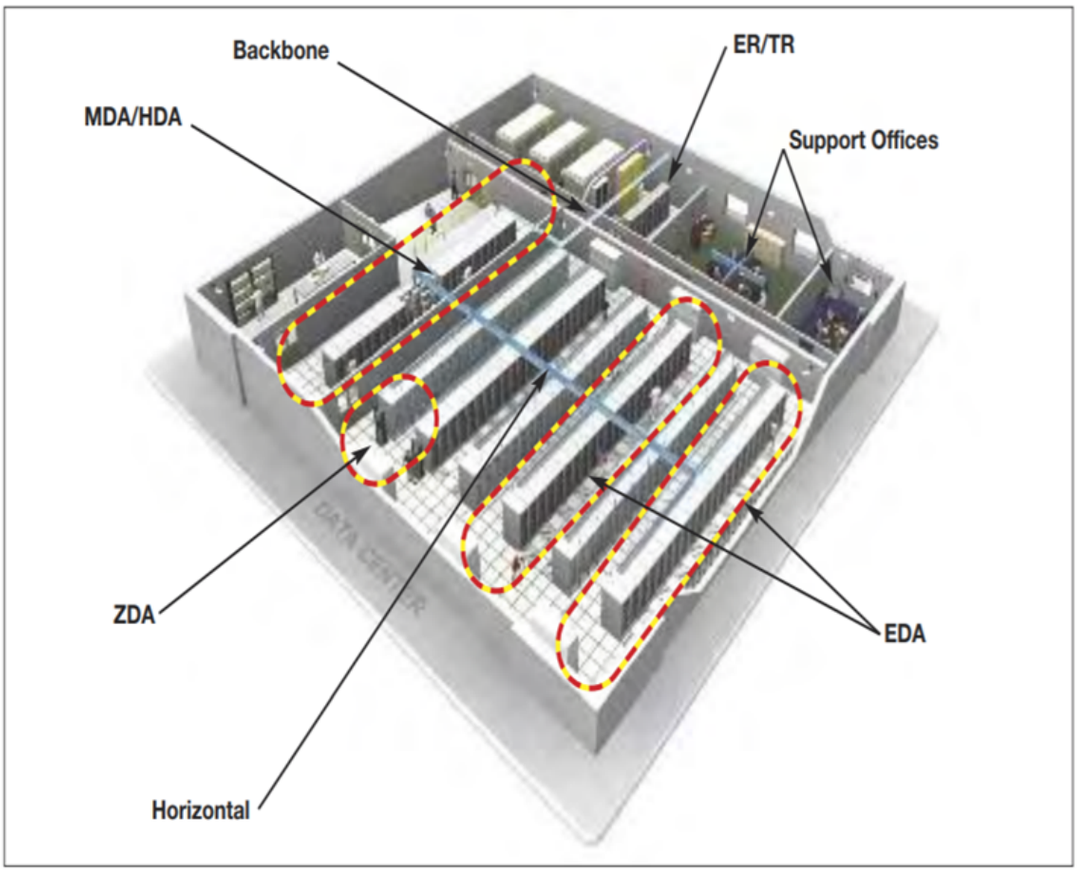
Standar ANSI/TIA/EIA-568-B berisi elemen dasar dari struktur sistem pengkabelan pada pusat data adalah sebagai berikut:

1. Sistem pengkabelan horizontal (*horizontal cabling*);
2. Sistem pengkabelan *backbone* (*backbone cabling*);
3. *Cross-connect* pada pintu masuk (*entrance room*) atau area kerja (*main distribution area*);
4. *Main cross-connect* (MC) pada area distribusi utama(*main distribution area*);
5. *Horizontal cross-connect* (MC) pada ruang telekomunikasi, *HDA* atau *MDA*;
6. *Zone outlet* atau konsolidasi titik pada zone distribution area; dan
7. *Outlet* pada area distribusi perangkat (*equipment distribution area*).

Gambar di bawah ini adalah elemen fungsional yang saling terhubung satu sama lain pada sistem pengkabelan pusat data.



Gambar 2.2.2.2.15. Topologi Sistem Pengkabelan Pusat Data



Gambar 2.2.2.2.16. Arsitektur Instalasi Sistem Pengkabelan Pusat Data

1. *Horizontal Cabling* (Pengkabelan Horizontal)

   Pengkabelan horisontal, sebagaimana ditentukan oleh ANSI/TIA/EIA-568-B, adalah kabel yang membentang dari ruang telekomunikasi ke area kerja dan berakhir di *outlet* telekomunikasi (informasi *outlet* atau dinding). *Wiring horizontal* dijalankan dari setiap *workstation* di suatu lantai yang sama ke ruang telekomunikasi, kemudian berakhir pada pemutusan *punchdown*, atau langsung ke *patch panel*. Di ruang telekomunikasi, peralatan jaringan seperti hub atau *switch* terhubung ke setiap stasiun kabel. Hub atau *switch* kemudian melewati sinyal komputer ke *workstation* lain atau ke pusat data, atau bahkan ruang telekomunikasi lainnya untuk konektivitas utama dengan seluruh jaringan. Pengkabelan horizontal meliputi :

   a. Kabel dari *patch panel* ke area kerja;
   b. Outlet telekomunikasi;
   c. Kabel penghentian;
   d. *Cross-connections* (jika diizinkan);
   e. Pembatasan maksimal pada satu titik transisi;
   f. Komponen jaringan yang spesifik *(switch router)* tidak harus dipasang sebagai bagian dari kabel dengan sistem horizontal (dalam dinding). Perangkat *switch* atau *router* harus dipasang di ruang telekomunikasi atau area kerja; dan
   g. Titik transisi ANSI/TIA/EIA-568-B memungkinkan untuk satu titik transisi di kabel horisontal. Titik transisi adalah di mana salah satu jenis kabel terhubung ke yang lain, seperti di mana kabel bulat terhubung ke bawah karpet kabel. Sebuah titik transisi juga bisa menjadi titik dimana kabel didistribusikan ke *furniture modular*.

2. *Backbone Cabling* (Pengkabelan *Backbone*)

   Kabel *backbone* diperlukan untuk menghubungkan fasilitas pintu masuk, ruang peralatan dan telekomunikasi, pengkabelan *backbone* juga bisa diaplikasikan antara lain untuk pemasangan kabel antara ruang inventaris dengan pintu masuk fasilitas pada bangunan dan koneksi vertikal antar lantai.

3. *Office, Operation Center* (Area Kerja)

   Ruang bangunan di mana pengguna menggunakan peralatan telekomunikasi, mencakup semua komponen kabel antara outlet komunikasi (soket dinding) dan peralatan telekomunikasi pengguna akhir, seperti telepon, *workstation*

dan printer, termasuk *outlet* komunikasi itu sendiri. Area kerja kabel sistem dirancang agar fleksibel, tapi masih memerlukan manajemen hati-hati. Agar terhindar dari masalah seperti pasangan kabel yang tidak cocok, kita perlu memasang *outlet* area kerja dengan prosedur standar dan menggunakan standar yang sama (T568A atau T568B) di seluruh sistem saat menyelesaikan kabelnya. Standar T568B lebih umum digunakan dalam aplikasi data. Standar ini memerlukan dua lubang *outlet* pada setiap dinding, satu untuk suara, dan satu lagi untuk *data.568B* standar yang lebih umum digunakan dalam aplikasi data.

4. *Telecom Room* (Telekomunikasi)

   Daerah tertutup seperti ruang atau lemari, peralatan telekomunikasi perumahan, frame distribusi, terminasi kabel dan lintas menghubungkan kabel jaringan yang masuk dan keluar dari ruangan tersebut. Dengan kata lain, semua perangkat keras yang diperlukan untuk menghubungkan kabel horizontal untuk kabel vertikal. Daerah ini sering juga rumah peralatan bantu, termasuk berkas pusat data jaringan. Setiap bangunan harus memiliki minimal satu kabel lemari, dan standar merekomendasikan satu per lantai. Ukuran lemari khusus juga dianjurkan, tergantung pada ukuran area layanan. Harus ada ruang yang cukup untuk tenaga pelayanan untuk melakukan pemeliharaan dan melaksanakan tugas-tugas lain, serta untuk semua *hardware* yang dibutuhkan. Pencahayaan, pasokan listrik dan kondisi lingkungan juga harus memenuhi persyaratan yang ditentukan oleh standar.

5. *Equipment Room* (Peralatan Kamar)

   Setiap rumah tentu perlu membangun sebuah sistem telekomunikasi, seperti: *PBX*s, pusat data, *switch* dll, dan penghentian mekanik dari sistem kabel telekomunikasi. Hal ini dianggap berbeda dari lemari telekomunikasi karena kompleksitas komponen. Ruang peralatan mengambil tempat dari lemari telekomunikasi atau menjadi fasilitas terpisah. Secara umum, fungsi ruang peralatan dapat dimasukkan dalam lemari kabel. Ruang peralatan menyediakan titik terminasi untuk vertikal (*backbone*) kabel yang terhubung ke satu atau lebih lemari telekomunikasi. Hal ini juga dapat menjadi titik *cross*-koneksi utama untuk seluruh fasilitas. Sebagai contoh, di lingkungan kampus, setiap bangunan dapat memiliki ruang dan peralatan sendiri dimana peralatan

lemari telekomunikasi saling terhubung. Peralatan di ruangan juga dapat terhubung ke fasilitas kampus yang terhubung ke seluruh kampus.

6. *Entrance Room* (Fasilitas Pintu Masuk)

   Berisi pintu masuk layanan telekomunikasi ke gedung, dan mungkin juga mengandung koneksi *backbone*. Hal ini juga berisi titik demarkasi jaringan, yang merupakan interkoneksi untuk fasilitas telekomunikasi pertukaran operator lokal. Titik demarkasi biasanya 12 inci dari fasilitas pengangkut memasuki gedung, tapi *carrier* dapat menunjuk sebaliknya.

7. Administrasi Kabel

   Administrasi kabel adalah kegiatan yang mencakup seluruh aspek pengaturan kabel dalam suatu bangunan, seperti: mencatat, mengelola, dan menguji sistem kabel, membuat serta menjaga rencana sistem yang telah dirancang.

   A. Kabel Data *Ethernet*

      Kabel data yang digunakan menggunakan tipe *UTP Category* 6 (UTP Cat6) yang mampu meneruskan paket data sampai dengan 10 *Gbps* pada jarak 55 meter atau 1 *Gbps* pada jarak 100 meter. Di bawah ini adalah tabel kategori *UTP* dari yang awal *cat1* sampai dengan terbaru *Cat7*.

UTP Categories - Copper Cable				
UTP Category	**Data Rate**	**Max. Length**	**Cable Type**	**Application**
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Gambar 2.2.2.2.17. Kategori Kabel *UTP–Ethernet*

B. *Fiber Optic*

   Standar ANSI/TIA/EIA-568-B memungkinkan penggunaan kabel serat optik baik yang menggunakan *mode single-mode* maupun *multimode*. Dengan kata lain, standar tersebut mengizinkan kabel serat optik yang memiliki karakteristik dan jenis mode yang berbeda untuk digunakan pada jaringan. Sistem pengkabelan horisontal ditetapkan dengan menggunakan kabel 62.5/125-*micron multimode*, sedangkan

pengkabelan *backbone* dapat menggunakan baik kabel optik-serat *multimode* atau *single-mode*. Terdapat dua konektor yang sebelumnya banyak digunakan untuk pemasangan kabel dengan sistem serat optik, yaitu *ST* dan konektor *SC*. Banyak instalasi telah menggunakan jenis konektor *ST*, tetapi standar sekarang mengakui hanya konektor 568SC-jenis. Hal ini pun berubah sehingga serat-optik spesifikasi ANSI/TIA/EIA-568-B dapat menyetujui dengan Standar IEC 11801 yang digunakan di Eropa. Standar ANSI/TIA/EIA-568-B menggunakan *small-form factor* konektor seperti konektor MT-RJ.

Merujuk pada Gambar 2.2.2.2.18., menunjukkan gambaran singkat mengenai standar kabel serat optik yang digunakan pada pengkabelan premis. Terdapat empat tipe serat optik yang terdiri dari tiga jenis serat *multimode* (OM1, OM2, OM3) dan satu jenis serat *singlemode* (OS1).

Tipe Serat Optik	Panjang Gelombang	Atenuasi dB/Km (maks)	OFL Bandwidth MHz Km (Min)	EFL Bandwidth MHz Km (Min)
OM1	850 nm	3,5	200	Tidak ditentukan
(50/125úm atau 62,5/125 úm)	1300 nm	1,5	500	Tidak ditentukan
OM2	850 nm	3,5	500	Tidak ditentukan
(50/125úm atau 62,5/125 úm)	1300 nm	1,5	500	Tidak ditentukan
OM3	850 nm	3,5	1500 500	Tidak ditentukan
(50/125úm)	1300 nm	1,5		Tidak ditentukan
OS1	1310 nm	1,0	Tidak ditentukan	Tidak ditentukan
(ITU-T G.652)	1550 nm	1,0	Tidak ditentukan	Tidak ditentukan

Gambar 2.2.2.2.18. Kategori Tipe Kabel Serat Optik

11. Desain Ruang Pusat Data

a. Desain *Raised Floor*

Disebut juga *access floor* atau *raised access floor*

FUNGSI

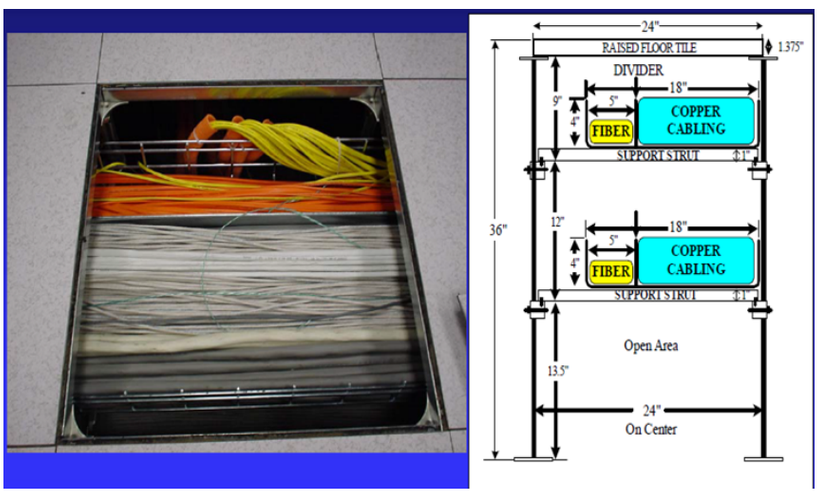
- Sistem distribusi udara dingin untuk mendinginkan peralatan IT;
- Jalur kabel data;
- Jalur kabel listrik;
- Jaringan kabel tembaga untuk *grounding* peralatan; dan
- Lokasi untuk mengalirkan air dingin (*chilled water*) atau pipa utilitas lainnya

Ukuran

- *Panel* : 60x60cm;
- Tebal : 28-42 mm; dan
- Tinggi penyangga : 35cm.

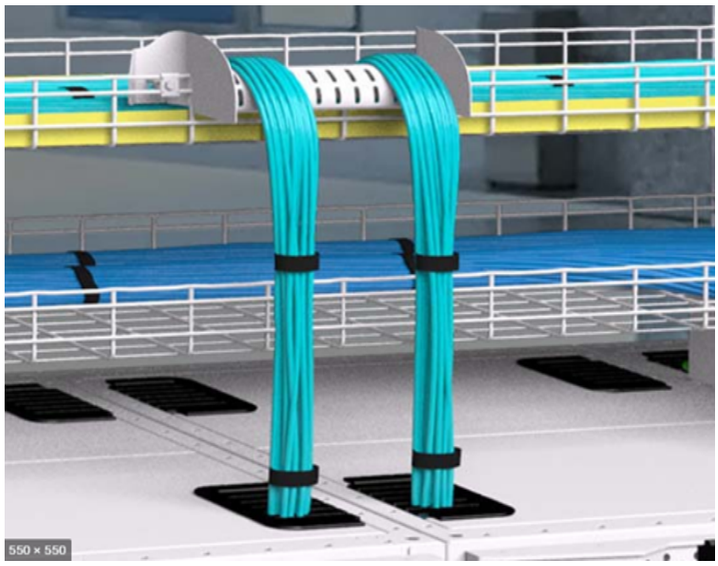
Gambar 2.2.2.2.19. Komponen Pendukung *Raised Floor*

1. *Cable Tray*
   a. Bawah *Raised Floor*
      - 2 *cable tray* untuk listrik & data
      - Standar TIA-569-B : kabel data dan listrik terpisah minimal 61 cm

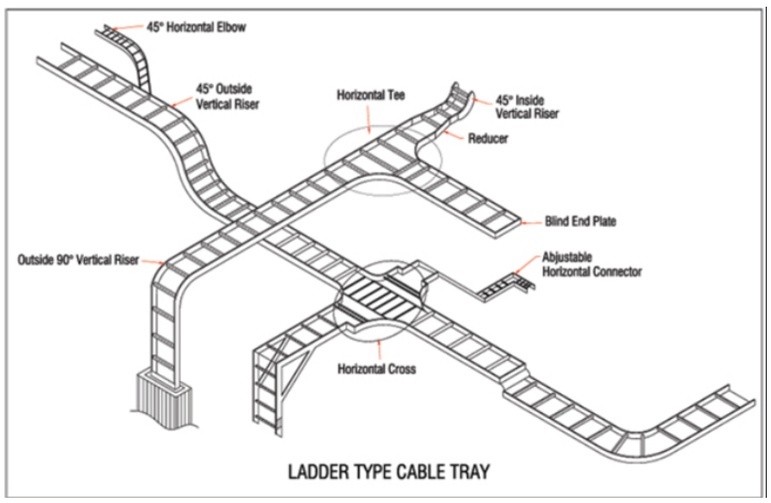


Gambar 2.2.2.2.20. Instalasi Kabel Data & *Power* di Bawah *Raised Floor*

   b. Atas *Rack* Pusat Data



Gambar 2.2.2.2.21. Instalasi Kabel Data di Atas *Rack* pusat data dengan *Cable Tray*



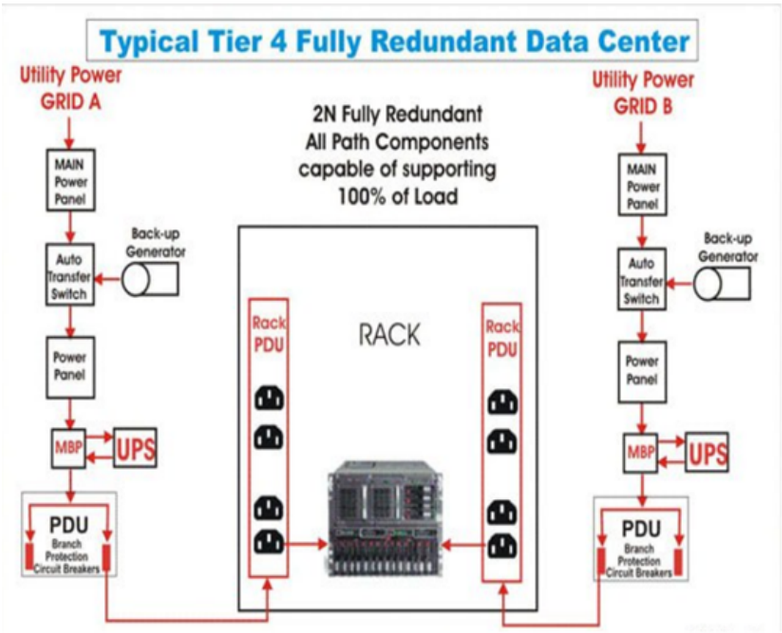
Gambar 2.2.2.2.22. Type Kabel *Tray* Untuk Instalasi Sistem Pengkabelan

c. *Rack Location Unit*

- Rack pusat data memenuhi persyaratan *EIA-310 (Electrical Industry Alliance Standards)* pada perangkat *rack 19"*.
- Memiliki jalur akses listrik dan jalur kabel data di bagian atas dan bawah, selain dari bagian depan dan belakang.
- Tata letak kabinet diatur sedemikian rupa untuk dapat mudah diakses oleh para teknisi dan diberikan ruang kosong agar suhu pada *rack* pusat data dapat lebih terkendali.

- Seluruh perangkat pusat data dan peralatan lainnya yang besar diletakan dibagian paling bawah *rack* pusat data.
- Setiap *rack* pusat data memiliki dua *strip power* dengan sumber listrik dari sumber yang berbeda.

Gambar dibawah ini adalah topologi redudansi sistem kelistrikan untuk tipe Tier 4 dengan *mode* aktif-aktif. Dua buah *power strip* yang ada di *rack* pusat data di-*supply* oleh sumber listrik yang berbeda.



Gambar 2.2.2.2.23 Instalasi Sistem Kelistrikan *Tier-4-Fully Redundant*

12. Sistem Keamanan Fisik

Terdiri dari sistem pengamanan fisik dan non-fisik pada pusat data. *Fitur* sistem pengamanan fisik meliputi akses user ke pusat data berupa kunci akses memasuki ruangan (kartu akses atau biometrik) dan seluruh petugas keamanan yang mengawasi keadaan pusat data (baik di dalam maupun di luar). Pengamanan fisik juga dapat diterapkan pada seperangkat infrastruktur dengan melakukan penguncian dengan kunci gembok tertentu. Di dalam tabel sistem keamanan fisik pusat data terdiri dari keamanan gedung, keamanan ruang komputer, dan kebijakan serta prosedur keamanan.

Building	Computer Room	Policy & Procedure
•Alarms •Security Operation Center •Kamera keamanan •Informasi kegempaan	•Two-factor access control dengan biometric dan kartu akses •Kamera •Catu daya cadangan	•SOP •Rekaman video dan log akses disimpan minimal 30 hari •Audit secara teratur

Gambar 2.2.2.2.24 Keamanan Pusat Data

Gambar di bawah ini adalah contoh perangkat pendukung sistem keamanan di pusat data untuk keamanan rak pusat data, dan pintu masuk ruang pusat data.

Gambar 2.2.2.2.25 Perangkat Pendukung Keamanan Fisik Pusat Data

13. Sistem Pencahayaan

Sistem pencahayaan pusat data diperlukan untuk menerangi ruang pusat data utama dan ruang–ruang lainnya termasuk jalur masuk atau lorong. Standar sistem pencahayaan menggunakan TIA-942-A. Lokasi penempatan lampu–lampu antara lain di atas lorong dan di atas antara rak cabinet. Selain lampu utama terdapat juga Lampu dan petunjuk darurat (*emergency lighting & signs*), jalur darurat. Penempatan dan intensitas cahaya lampu pusat data dibagi menjadi tiga lapisan yakni :

- Level 1: untuk lokasi yang tidak dihuni. Pencahayaan tidak perlu untuk mendukung kejelasan penglihatan manusia tetapi peralatan pengawas video harus tetap dapat bekerja dengan baik.
- Level 2: untuk lokasi menuju ruang pusat *Farm* berupa gang-gang dan lorong-lorong yang cukup diterangi untuk

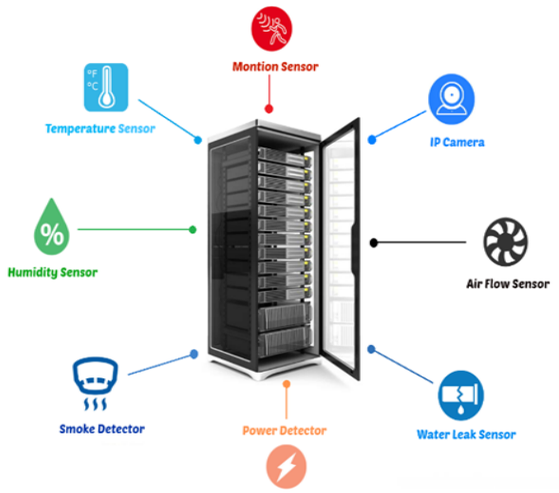
pergerakan yang aman dan kamera keamanan dapat bekerja dengan baik.

- Level 3: lokasi utama pusat data *Farm* dll dan ditempati di mana karyawan akan bekerja. Tingkat cahaya bidang horizontal: 500 *lux* dan bidang vertikal: 200 *lux.*

14. Sistem Pemantau Lingkungan

Fungsi utama dari *EMS* (*Environment Monitoring System*) adalah memonitor operasional pusat data dari ancaman lingkungan yang ada disekitarnya. Oleh karena operasional pusat data yang *non-stop* maka perlindungan dan monitoring pada fasilitas ini harus diutamakan. Pada umumnya gangguan yang dimonitor oleh *EMS* ini adalah suhu & kelembaban pada pusat data *room*, kebocoran air di bawah *raised floor* (*Water Leak*) yang diakibatkan kondensasi *AC*, getaran, dan tegangan listrik akibat pemadaman yang tiba-tiba. Untuk memonitoring perangkat *EMS* ini didukung oleh beberapa sensor cerdas yang berupa *modular sensor*. Sensor ini bervariasi, diantaranya *sensor status on/off AC, sensor water leak, door contact, temperature, humidity, vibration, air flow, voltage, smoke detector*, dll. Sensor ini mendeteksi adanya kelainan pada lingkungan pusat data, yang kemudian informasi tersebut dikirimkan ke perangkat *EMS*. Perangkat ini kemudian akan mengirimkan sinyal peringatan berupa *alarm, buzzers, e-mail, sms,* dan telepon ke *system administrator* atau *network administrator* yang selalu siaga di *NOC*, sehingga masalah tersebut dapat ditangani secepat mungkin. *EMS* akan melakukan pemantauan komponen berikut ini :

- tegangan;
- akses masuk keluar ruangan;
- suhu/*temperatur;*
- kelembaban;
- adanya air di ruangan;
- adanya asap/*smoke* di ruangan;
- memonitor sisa solar di tangki genset;
- mengaktifkan *AC* tambahan; dan
- mendapatkan *alert* melalui *email/SMS* terintegrasi dengan *NMS* yang ada.



Gambar 2.2.2.2.26. Komponen Lingkungan yang akan di Pantau di Pusat Data

Gambar 2.2.2.2.27. Metode Notifikasi Sistem Pemantauan Lingkungan Pusat Data

15. **Pusat Pemulihan Bencana (*Disaster Recovery Center*)**

    Data dan informasi merupakan "aset" paling berharga bagi organisasi pemerintahan maupun perusahaan. Oleh karena itu, perlu ada perlindungan dan pencadangan terhadap data dan informasi, sehingga data tetap aman apabila terjadi bencana. Dengan begitu aktivitas bisnis tetap berlanjut. Oleh karenanya dibutuhkan Pusat Pemulihan Bencana atau *Disaster Recovery Center* (*DRC*) untuk membuat data, informasi, dan aplikasi tetap aman dan dapat diakses. *DRC* adalah sebuah tempat yang ditujukan untuk menempatkan perangkat IT, sistem, aplikasi dan data cadangan untuk persiapan menghadapi bencana yang diperlukan oleh perusahaan besar dan organisasi pemerintahan.

DRC diperlukan oleh organisasi pemerintahan maupun perusahaan dengan beberapa pertimbangan antara lain:

1. Kegagalan mesin dan perangkat keras (*hardware*)

   Meskipun perusahaan telah berinvestasi dengan membeli mesin dan perangkat keras (*hardware*) kelas tinggi, bukan berarti tidak perlu membangun *DRC*. Mesin canggih dengan *hardware* tinggi dan *DRC*, akan membuat perusahaan tidak menemukan kegagalan layanan dikarenakan fungsi *hardware*.

2. Faktor kesalahan manusia

   Pencegahan terhadap kesalahan manusia (*human error*) seperti penghapusan data atau kesalah konfigurasi yang tidak disengaja. Organisasi bisa mencadangkan data dan mengembalikannya lagi seperti sebelum dilakukan kesalahan.

3. Faktor alam yang tak bisa diprediksi

   Bencana tidak bisa dihindari dan diprediksi, untuk itu, memiliki *DRC* yang berada di beberapa tempat yang secara teori aman terhadap bencana besar.

4. Optimalisasi layanan

   Kepemilikan *DRC* berarti memberikan layanan kepada masyarakat yang baik. Saat ini masyarakat ingin mendapatkan layanan cepat, dan itu bisa terjadi jika infrastruktur bisa diakses kapan saja. Keandalan dan kelancaran suatu layanan *DRC* bergantung pada terpenuhinya beberapa syarat bangunan dan arsitektur sebagai berikut:

- Jarak fisik antara Pusat Data utama (*DC*) dan Pusat Pemulihan Bencana (*DRC*) minimal lebih dari 40 km.
- Berada di luar radius mitigasi bencana seperti gunung berapi, tsunami, banjir, dan lain – lain.
- Tidak berada pada jalur patahan geologi.
- Indeks rawan bencana rendah di Indonesia (Sumber: Indeks Rawan Bencana Indonesia BNPB, 2011).
- Akses jaringan internet memadai, mudah dijangkau.
- Bangunan harus memiliki area bongkar muat yang memadai untuk menangani keluar - masuk barang/peralatan.

Terdapat 3 (tiga) jenis Pusat Pemulihan Bencana (*DRC*) yakni:

1. *Cold DRC*

   Cold DRC adalah jenis yang paling sederhana terdiri dari elemen daya dan kemampuan jaringan serta pendinginan tetapi tidak termasuk elemen perangkat keras lain seperti pusat data dan penyimpanan. Sebelum dapat digunakan,

data cadangan bersama dengan beberapa perangkat keras tambahan harus dikirim ke lokasi *DRC* dan diinstal.

2. *Warm DRC*

   Warm DRC adalah tipe DRC yang standar terdiri dari komputer dengan segala komponennya seperti aplikasi, jalur komunikasi data, serta *backup* data yang paling terbaru, dimana sistem tidak secara otomatis berpindah, tetapi masih terdapat proses manual meskipun dilakukan seminimal mungkin.

   Ketika *DC* utama mengalami masalah atau bencana, semua akan dialihkan ke *DC* kedua yaitu *DRC* dan sementara itu *DRC* beroperasi, personel juga mulai memulihkan data yang ada pada *DC* utama agar *DC* utama bisa beroperasi kembali.

3. *Hot DRC*

   Hot DRC merupakan tipe *DRC* yang paling cepat dengan mengatur secepat mungkin operasional bisnis, sistem aplikasi, jaringan komunikasi data yang sama sudah dipasang dan sudah tersedia di lokasi *DRC*. Data secara terus menerus (*realtime*) di *backup* menggunakan koneksi antara *DC* dan lokasi *DRC*, dan operasional bisnis akan berjalan pada saat itu juga,tanpa harus mematikan sistem di pusat data lama.

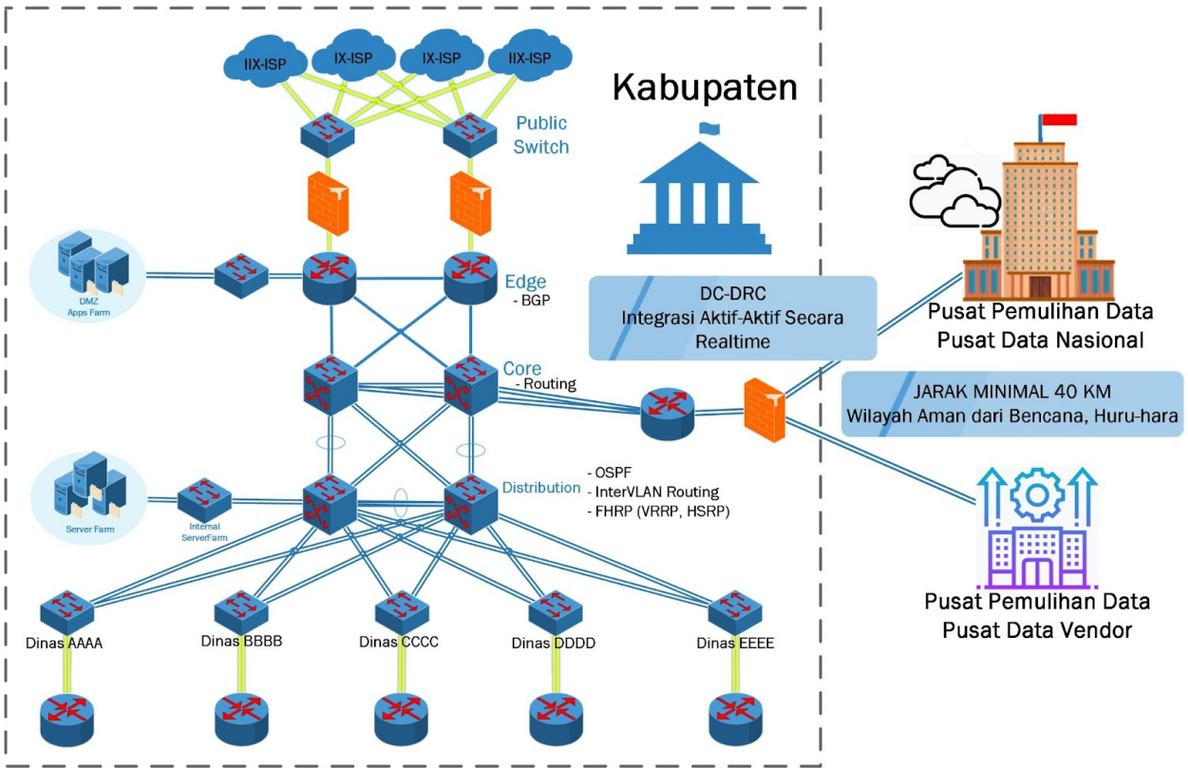
A. Kondisi Eksisting Pusat Data

Kondisi saat ini server aplikasi Pemerintah Kabupaten Murung Raya ditempatkan di Pusat Data Diskominfo Pemkab Murung Raya. Secara bertahap server aplikasi mulai dimigrasikan ke layanan *Virtual Private Server* (VPS) Pusat Data Nasional.

Source aplikasi dicadangkan (*backup*) di *repository server*, sedangkan untuk berkas (file) dan *database* masih dicadangkan di server yang berbeda di Pusat Data Diskominfo.

B. Usulan Topologi Pusat Data dan Pusat Pemulihan Bencana (DRC)

Kondisi saat ini Pemerintah Kabupaten Murung Raya belum memiliki Pusat Pemulihan Bencana atau DRC. Sesuai dengan arahan dari Kebijakan Pemerintah untuk memanfaatkan Pusat Data Nasional. Diskominfo dapat memanfaatkan layanan Pusat Data Nasional sebagai lokasi DRC.



Gambar 2.2.2.2.29 Usulan Topologi DC-DRC

2.2.2.3. Jaringan Intra Pemerintah

Prinsip utama dalam penyediaan jaringan data meliputi aspek ketersediaan, keamanan, dan pengendalian. Untuk memenuhi ketiga prinsip tersebut maka pengembangan arsitektur jaringan intra pemerintah di Pemerintah Kabupaten Murung Raya dapat bertumpu pada empat karakteristik yakni berjenjang atau hirarki (*hierarchy*), zonasi (*zoning*), redudansi (*redudancy*), dan keamanan (*security*). Hierarki dan zonasi memungkinkan pengembangan jaringan yang terdiri dari banyak komponen yang saling terkait secara berlapis dan terstruktur. Model hierarkis dapat membantu untuk memaksimalkan kinerja jaringan, mengurangi waktu untuk mengimplementasikan dan memecahkan masalah desain, dan meminimalkan biaya.

Desain jaringan redudansi untuk memenuhi persyaratan untuk ketersediaan jaringan dengan menduplikasi komponen jaringan, jalur koneksi jaringan, dan rute jaringan (*routing*). Redudansi dapat menghilangkan satu titik kegagalan pada jaringan. Redudansi juga memfasilitasi pembagian beban, yang meningkatkan kinerja jaringan. Redudansi akan menambah kompleksitas dan biaya pada jaringan, dan harus dirancang dengan hati-hati. Desain keamanan jaringan ditujukan untuk peningkatkan keamanan jaringan Pemerintah Kabupaten Murung Raya dari serangan yang dilakukan oleh pihak luar. Perangkat f*irewall* berfungsi untuk memantau lalu lintas jaringan dan membatasi akses ke dalam jaringan internal, sehingga dapat membantu melindungi jaringan dari serangan yang tidak diinginkan dan memperkuat sistem keamanan jaringan secara keseluruhan.

A. Topologi Jaringan

Jaringan *LAN* harus dibangun secara terstruktur, baik dari sisi topologi jaringan, segmentasi jaringan, pengalamatan (*addressing*) maupun penggunaan perangkatnya. Dengan memiliki struktur jaringan yang baik maka akan dapat dilakukan pengaturan, pengawasan serta pemanfaatan yang lebih maksimal. Perangkat aktif jaringan sebagai komponen utama di jaringan tentunya harus memiliki kemampuan untuk mengelola sumber daya jaringan, seperti kapasitas *bandwidth*, menyaring paket data yang lewat (*traffic filtering*), segmentasi jaringan (*VLAN)*, mengatur prioritas lalu lintas paket data (*traffic priority*), dan ketahanan jaringan (*network reliability*) yang baik, serta berbagai fungsi pengontrolan lainnya, sehingga pemanfaatan TI dalam proses bisnis organisasi dapat berjalan dengan baik dan lancar serta memberikan hasil yang maksimal.

B. Berjenjang atau hirarki (*3-Tier Hierarchy*)

Model desain jaringan berjenjang atau hirarki untuk membantu dalam mengembangkan topologi di lapisan *diskrit*. Setiap lapisan atau *tier*, dalam hierarki menyediakan fungsi tertentu yang mendefinisikan perannya dalam jaringan secara keseluruhan. Setiap lapisan dapat difokuskan pada fungsi tertentu, memungkinkan untuk memilih sistem dan fitur yang tepat untuk setiap lapisan.

Setiap lapisan model hirarkis memiliki peran spesifik :

1. Lapisan inti (*Core Layer*)

   Menyediakan transportasi optimal antar lokasi. Lapisan inti dari topologi hierarkis tiga lapis adalah tulang punggung berkecepatan tinggi *internetwork*. Karena lapisan inti sangat penting untuk interkonektivitas, maka komponen pendukung harus redudansi. Lapisan inti harus sangat andal dan harus beradaptasi dengan perubahan dengan cepat.

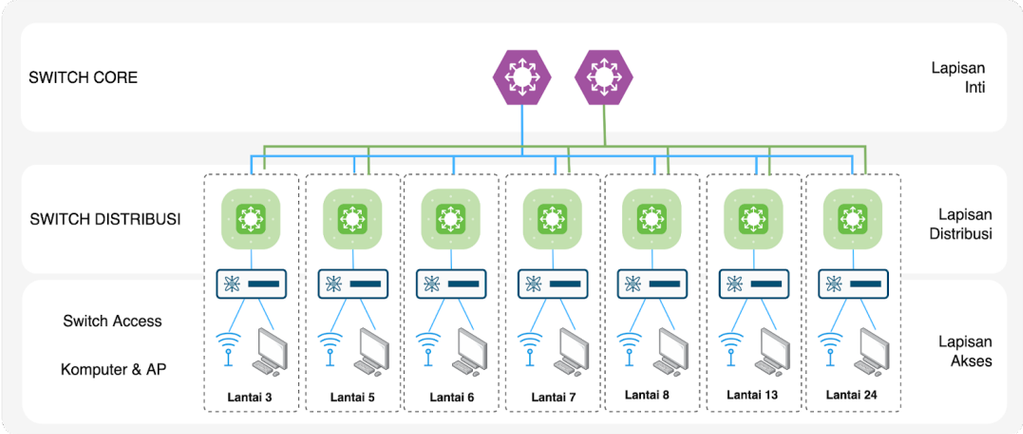
2. Lapisan distribusi (*Distribution Layer*)

   Lapisan distribusi dapat berfungsi sebagai penghubung antara layanan jaringan pada lapisan akses dengan lapisan inti, penerapan kebijakan keamanan, lalu lintas paket data, dan perutean *(routing)*.

   Pada lapisan distribusi dapat dikonfigurasi agar dapat merutekan atau menghubungkan antara satu *VLAN* dengan *VLAN* yang lain. Hal ini memungkinkan untuk terciptanya hubungan antar *VLAN* dalam satu jaringan yang sama, sehingga dapat meningkatkan efisiensi dan pengelolaan jaringan secara keseluruhan.

3. Lapisan Akses

   Lapisan akses adalah lapisan yang langsung berinteraksi dengan perangkat pengguna seperti komputer desktop, laptop, printer, *CCTV,* dan lain – lain. Perangkat jaringan yang digunakan pada lapisan akses meliputi *switch access* dan *Access Point* (AP) pada jaringan nirkabel.



Gambar 2.2.2.3.1 Topologi Jaringan *3-Tier Hierarchy*

Penggunaan model hirarki dapat membantu untuk meminimalkan biaya. Pembelian perangkat yang sesuai untuk setiap lapisan hierarki, dapat menghindari pengeluaran uang pada *fitur* yang tidak perlu. Pendekatan modular dari desain hierarkis memungkinkan perencanaan kapasitas yang akurat dalam setiap lapisan hierarki, sehingga mengurangi *bandwidth* yang terbuang.

Desain jaringan dengan pendekatan zonasi memungkinkan untuk menjaga setiap elemen desain sederhana dan mudah dipahami. Kesederhanaan meminimalkan kebutuhan untuk pelatihan ekstensif untuk personel operasi jaringan dan mempercepat implementasi suatu desain. Menguji desain jaringan menjadi mudah karena ada fungsionalitas yang jelas di setiap lapisan. Isolasi kesalahan ditingkatkan karena jaringan teknisi dapat dengan mudah mengenali titik transisi dalam jaringan untuk membantu mereka mengisolasi kemungkinan titik kegagalan.

Tabel 2.2.2.3.1 Penerapan 3 (Tiga) Lapisan Jaringan Berjenjang (*3-Tier Hierarchy*)

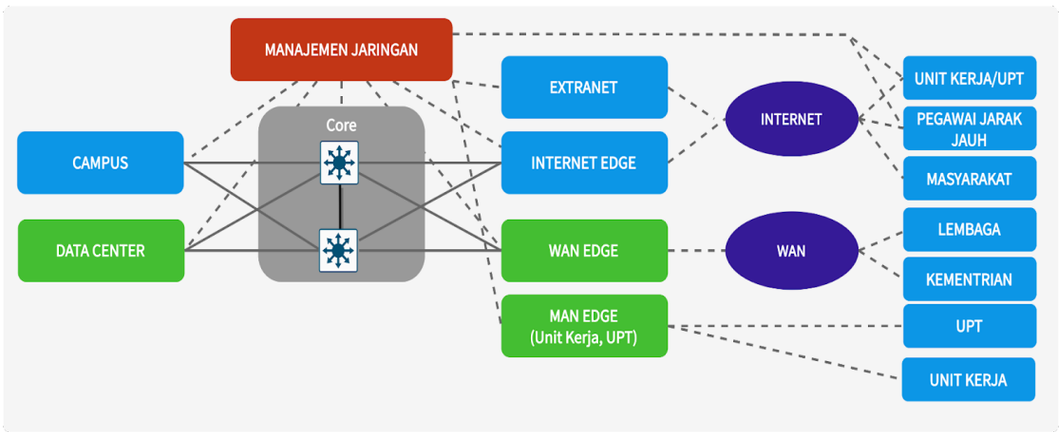
Penerapan 3 (Tiga) Lapisan Jaringan Berjenjang (*3-Tier Hierarchy*)
Lapisan Inti (*Core Layer*)
Jaringan pada *core layer* dirancang dengan mempertimbangkan: • Sebagai tulang punggung (*backbone*) jaringan yang menghubungkan zona-zona jaringan • Memiliki performansi dan stabilitas yang tinggi • Memiliki tingkat kompleksitas yang rendah • Sebagai titik agregasi layer distribusi • Memiliki skalabilitas yang tinggi untuk pengembangan ke depan • Memiliki rancangan yang independen dari sisi teknologi (menerapkan *open standard*)
Lapisan Distribusi (*Distribution Layer*)

Penerapan 3 (Tiga) Lapisan Jaringan Berjenjang (*3-Tier Hierarchy*)
Jaringan pada layer distribusi dirancang dengan mempertimbangkan: ● *Availability, load balancing, QoS* dan *provisioning* ● Agregasi layer akses dan keterhubungan ke jaringan inti (*uplink*) ● Mengamankan jaringan inti dari permasalahan di jaringan akses ● Penerapan penyederhanaan *routing*, kecepatan konvergensi, jalur *redundant* dan *load sharing* ● redundansi perangkat (HSRP, GLB)
Lapisan Akses (*Access Layer*)
Penerapan teknologi jaringan pada akses layer yang meliputi: ● Jaringan *layer* 2/*layer* 3, mendukung konvergensi standar jaringan dan *storage*, HA, *security*, QoS, IP *multicast*. ● Memiliki kemampuan *Intelligent Network Services*: QoS, *boardcast suppression*, VLAN dan VTP, internal *routing protocol, port aggregation*. ● Mendukung fitur *security* yang terintegrasi 802. 1x, CISF, *port security*, *DHCP snooping*. ● Memiliki kompatibilitas interkoneksi dengan perangkat layanan: *Phone Discovery*, *PoE, auxiliary* VLAN. ● Jaringan dikelompokkan menjadi tiga kategori yang disesuaikan dengan karakteristik kebutuhan implementasi dan layanannya sebagai berikut:
a. Jaringan internal
Local Area Network (LAN), memberikan akses jaringan di semua gedung dengan menggunakan kabel *fiber optic* (FO). Kabel FO dipilih karena kabel FO memiliki kekebalan terhadap imbas petir dan gangguan elektromagnetik. Sehingga dalam rancangan ini ditetapkan bila jaringan melintas keluar bangunan maka harus memakai kabel FO.
Metropolitan Area Network (MAN) dan *Wide Area Network* (WAN), memberikan akses jaringan pada *remote site internal* dengan menggunakan interkoneksi yang disediakan oleh penyedia jaringan akses. Titik masuk jaringan WAN diharuskan melalui fasilitas ruang telekomunikasi (*Telecommunication Room Facility*) yang ada di pusat data, yang berfungsi sebagai area demarkasi kepemilikan infrastruktur dan pengamanan masalah fisik.
Redundancy Link, penerapan jalur berganda pada jaringan LAN dan WAN untuk mendukung ketersediaan layanan yang tinggi pada jaringan data.
Penggunaan protokol *routing* internal seperti OSPF digunakan dengan pertimbangan kebutuhan konvergensi yang cepat untuk melayani jaringan internal.
b. Jaringan Pusat Data
Jaringan pusat data memberikan akses jaringan untuk semua pusat data yang ada pada pusat data. Jaringan memiliki fleksibilitas dalam mendukung konektivitas yang dinamis berbasis modul atau zone, memiliki densitas *port interface* perangkat yang tinggi dan kemampuan melayani lalu-lintas jaringan dengan *bandwidth* yang tinggi.

Penerapan 3 (Tiga) Lapisan Jaringan Berjenjang (*3-Tier Hierarchy*)	
	Memiliki fleksibilitas untuk mendukung standar sistem storage berbasis jaringan seperti *Network Area Storage* (NAS) maupun standar *Storage Area Network* (SAN) seperti iSCSI dan FcoE.

C. Zonasi (*Zoning*)

Proyek desain jaringan besar dan implementasi jaringan besar pada umumnya terdiri dari area yang berbeda atau zona. Setiap zona harus dirancang menggunakan pendekatan sistematis, *top-down*, penerapan hierarki dan redudansi.



Gambar 2.2.2.3.2. Arsitektur Jaringan Berbasis Zonasi (*Zoning*)

Arsitektur Jaringan Berbasis Zonasi (*Zoning*) terdiri dari beberapa zona sebagai berikut:

1. Zona Inti (*Core*)

   Zona inti menghubungkan semua zona lainnya dan merupakan infrastruktur berkecepatan tinggi yang menyediakan transportasi *Layer 2* dan *Layer 3* yang andal dan dapat diukur. *Core* biasanya diimplementasikan dengan penggunaan dua unit *switch* (redundant) untuk menghubungkan ke zona kampus, pusat data, *WAN edge*, dan Internet *edge*.

2. Pusat Data

   Pusat data menampung server, aplikasi, dan perangkat penyimpanan untuk digunakan oleh pengguna internal. Pusat data juga menghubungkan infrastruktur jaringan. Pusat data tidak bisa diakses langsung oleh masyarakat umum melalui jaringan internet.

3. Kampus (*Campus*)

   Jaringan kampus menyediakan akses jaringan ke pengguna dan perangkat akhir (*endpoint*) yang terletak di satu lokasi. Kampus dapat menjangkau beberapa lantai dalam satu bangunan atau beberapa bangunan untuk perusahaan besar. Kampus ini menyelenggarakan layanan data. Desain kampus harus memungkinkan pengguna kampus aman mengakses pusat data dan sumber daya Internet dari infrastruktur kampus.

4. Manajemen

Jaringan manajemen menyediakan pemantauan, analisis, otentikasi, dan layanan rekam jejak (*logging*). pusat data manajemen mendukung *RADIUS, Kerberos, Protokol Waktu Jaringan (Network Time Protocol), Protokol Manajemen Jaringan Sederhana (Simple Network Management Protocol)*, dan lalu lintas *syslog*.

Tabel 2.2.2.3.2 Aplikasi pusat data Manajemen Jaringan

No	Aplikasi pusat data	Fungsi
1	*Dynamic Host Configuration Protocol* (DHCP)	pusat data yang memudahkan penyebaran *IP Address* ke sebuah jaringan secara merata tanpa perlu dilakukan dengan manual dengan memasukkan *IP Address* satu persatu ke perangkat.
2	*Domain Name pusat data* (DNS) Lokal	Sistem yang menghubungkan *Uniform Resource Locator* (URL) dengan *IP Address*. pusat data DNS berisi *database* alamat IP privat dan nama *host* terkait. pusat data DNS ini untuk melayani permintaan akses nama domain aplikasi intranet. Dengan adanya DNS Lokal, pengguna tidak perlu menghafal alamat IP dari aplikasi, cukup memasukkan nama domain.
3	*Directory Service*	pusat data yang memberikan layanan untuk mengelola aturan, hak akses, dan *security* pada pengguna atau jaringan komputer di perusahaan. Directory Service menyimpan konfigurasi jaringan baik *user, group*, komputer, *hardware*, serta berbagai *policy* keamanan dalam satu *database* terpusat. Contoh directory service pusat data yakni *Active Directory Domain Service* (ADDS) pada Windows pusat data, *Lightweight Directory Access Protocol* (LDAP) pada distro Linux.
4	*Network Time Protocol* (NTP)	pusat data untuk melakukan sinkronisasi terhadap penunjuk waktu dalam sebuah sistem komputer dan jaringan. Proses sinkronisasi ini dilakukan di dalam jalur komunikasi data yang biasanya menggunakan protokol komunikasi TCP/IP.
5	*Remote Authentication Dial In User Service* (RADIUS)	pusat data yang digunakan untuk melayani service *Authentication, Authorization,* dan *Accounting* (AAA) di dalam sebuah jaringan. Singkatnya RADIUS pusat data ini menyimpan kumpulan *user* dimana *user-user* tersebut dapat digunakan oleh *client* atau *user* yang berada dalam satu jaringan dengan RADIUS pusat data tersebut.
6	*Network Monitoring System*(NMS)	Suatu pusat data yang diperuntukan oleh administrator jaringan untuk memantau performansi jaringannya, seperti *Memory usage, CPU load, disk usage, service states, running process*, dan lain sebagainya. NMS menggunakan protokol SNMP (*Simple Network Management Protocol*) yang merupakan standar manajemen jaringan pada TCP/IP.
7	*System Logging Protocol* (Syslog)	Protokol standar yang digunakan untuk mengirim log sistem atau pesan peristiwa ke pusat data tertentu, yang disebut pusat data syslog. Ini terutama digunakan untuk mengumpulkan berbagai log perangkat dari beberapa mesin berbeda di lokasi pusat untuk pemantauan dan peninjauan.

5. Jaringan Skala Luas (*Wide Area Network*)

   WAN adalah bagian dari jaringan yang menghubungkan Pusat Data dengan kantor Kementerian/Lembaga, dan lokasi Pusat Pemulihan Bencana (*DRC*).

6. Jaringan Dalam Kota (*Metropolitan Area Network*)

MAN (*Metropolitan Area Network*) adalah bagian dari jaringan komputer yang menghubungkan beberapa kantor perangkat daerah, dan UPT (Unit Pelaksana Teknis) yang berada di area kabupaten/kota yang sama dengan pusat data.

7. Internet

   Internet adalah infrastruktur yang menyediakan konektivitas Internet dan yang bertindak sebagai pintu gerbang (*gateway*) ke seluruh dunia. Layanan Internet termasuk akses *De-Militerized Zone (DMZ)*, internet pengguna dilingkungan Pemerintah Kabupaten Murung Raya, dan akses jarak jauh *Virtual Private Network* (VPN).

D. Redudansi (*Redundancy*)

Desain jaringan redudansi untuk memenuhi persyaratan ketersediaan jaringan. Redudansi akan menghilangkan titik tunggal dari kegagalan (*single point of failure*) pada jaringan. Tujuannya adalah untuk menduplikasi komponen yang penting (utama) untuk menghindari aplikasi penting tidak dapat diakses. Komponen tersebut bisa berupa *router* into, *switch*, tautan antara dua *switch*, catu daya, *WAN Router*, konektivitas internet, dan sebagainya. Redudansi meliputi:

1. Duplikasi Komponen Kritis (*Duplicating High Critical Component)*

   Untuk menjaga ketersediaan layanan dan akses ke aplikasi utama maka komponen jaringan yang kritis seperti *switch core, firewall, router* internet harus diduplikasi dengan konfigurasi *High Availability (HA)* sehingga jika salah satu perangkat mengalami gangguan maka masih ada perangkat cadangan yang akan menggantikan secara otomatis.

2. Koneksi dan Jalur Cadangan (*Backup Path)*

   Untuk menjaga interkonektivitas ketika satu atau lebih jalur utama sedang terputus, maka lalu lintas paket data akan melalui jalur cadangan secara otomatis. Untuk melakukan proses otomatisasi perpindahan jalur utama ke cadangan maka diimplementasikan protokol rute *(routing protocol)* tertentu.

3. Pembagian Beban (*Load Sharing*)

   Tujuan utama redudansi adalah untuk memenuhi persyaratan ketersediaan. Tujuan lainnya adalah untuk meningkatkan kinerja dengan mendukung pembagian beban lintas tautan paralel. *Load Sharing*, terkadang disebut *load balancing*, memungkinkan dua atau lebih antarmuka atau jalur untuk dibagikan beban lalu lintas.

E. Keamanan (*Security*)

Keamanan adalah tujuan teknis utama, dan desain keamanan adalah salah satu aspek terpenting desain jaringan organisasi. Meningkatnya ancaman baik dari dalam maupun dari luar jaringan organisasi memerlukan aturan dan teknologi keamanan paling mutakhir. Secara keseluruhan tujuan yang dimiliki sebagian besar organisasi adalah bahwa masalah keamanan seharusnya tidak mengganggu operasional organisasi.

Kegiatan perancangan desain keamanan jaringan secara efektif meliputi:

1. Mengidentifikasi Aset Jaringan *(Identifying Network Assets)*

   Mengidentifikasi aset yang harus dilindungi, nilainya aset, dan biaya yang diharapkan terkait dengan kehilangan aset ini jika keamanan pelanggaran terjadi. Aset jaringan meliputi perangkat keras, perangkat lunak, aplikasi, dan data. Aktiva juga termasuk kekayaan intelektual, rahasia dagang, dan reputasi perusahaan.

   Data yang digunakan perusahaan untuk mencapai misinya adalah aset yang sering diabaikan. Data dapat mencakup *blueprint*, dokumen perencanaan keuangan, hubungan pelanggan informasi, dokumen analisis persaingan, informasi konfigurasi untuk perangkat keras dan perangkat lunak, nomor Jaminan Sosial karyawan, informasi lencana karyawan, dan sebagainya.

   Integritas dan kerahasiaan data harus dilindungi dari kerusakan yang disengaja atau tidak disengaja. Beberapa aset penting dalam jaringan adalah perangkat jaringan seperti *switch, router, firewall,* dan sistem deteksi intrusi (IDS) yang memberikan layanan keamanan untuk pengguna jaringan. Oleh karena perangkat-perangkat ini menjadi target bagi peretas, maka perlu diperkuat agar tidak mudah diintervensi terhadap intrusi.

2. Menganalisis Risiko Keamanan *(Analyzing Security Risk)*

   Menganalisa ancaman potensial dan mendapatkan pemahaman tentang kemungkinan dampak bisnis mereka. Penyusunan kebijakan keamanan dan desain jaringan yang aman memerlukan proses analisis risiko dan konsekuensinya yang berkelanjutan karena risiko dapat berubah dalam tingkat keparahan dan probabilitasnya.

3. Membangun Kebutuhan Keamanan (*Developing Security Requirements*)

   Masalah keamanan seharusnya tidak mengganggu kemampuan organisasi untuk melakukan bisnis. Persyaratan keamanan paling mendasar yang dimiliki setiap organisasi. Keamanan sekunder persyaratannya adalah untuk melindungi aset agar tidak lumpuh, dicuri, diubah, atau dirugikan.

4. Menetapkan kebijakan keamanan (*Developing a Security Policy*)

   Kebijakan keamanan memberitahu pengguna dan pimpinan tentang kewajiban mereka untuk melindungi aset teknologi dan informasi. Secara umum, suatu kebijakan setidaknya harus mencakup item-item berikut:

   a. Kebijakan akses yang menetapkan hak dan hak akses. Kebijakan akses harus memberikan pedoman untuk menghubungkan jaringan eksternal, menghubungkan perangkat ke jaringan, dan menambahkan perangkat lunak baru ke sistem. Kebijakan akses mungkin juga membahas caranya data dikategorikan (misalnya, rahasia, internal, dan sangat rahasia).

   b. Kebijakan akuntabilitas yang mendefinisikan tanggung jawab pengguna, staf operasi, dan manajemen. Kebijakan akuntabilitas harus menetapkan kemampuan audit dan memberikan pedoman penanganan insiden yang menentukan apa yang harus dilakukan dan siapa yang harus dihubungi jika kemungkinan intrusi terdeteksi.

c. Kebijakan otentikasi yang membangun kepercayaan melalui kebijakan kata sandi yang efektif dan mengatur pedoman untuk otentikasi lokasi jauh.
d. Kebijakan privasi yang menetapkan ekspektasi privasi yang wajar mengenai pemantauan surat elektronik, pencatatan penekanan tombol, dan akses ke file pengguna.
e. Pedoman pembelian teknologi komputer yang menentukan persyaratan untuk memperoleh, mengkonfigurasi, dan mengaudit sistem dan jaringan komputer untuk kepatuhan dengan kebijakan tersebut.

5. Mengembangkan prosedur untuk menerapkan kebijakan keamanan (*Develop procedures for applying security policies*)

   Prosedur keamanan merupakan penerapan dari kebijakan keamanan. Prosedur tersebut meliputi konfigurasi, login, proses audit, dan pemeliharaan. Prosedur keamanan harus ditulis untuk pengguna, administrator jaringan, dan administrator keamanan. Prosedur keamanan juga memuat penanganan insiden yaitu, apa yang harus dilakukan dan siapa yang harus dihubungi jika intrusi terdeteksi.

6. Menguji keamanan secara periodik

   Pengujian keamanan jaringan dilakukan secara periodik misal satu tahun sekali untuk memastikan konfigurasi dan perangkat lunak perangkat keamanan jaringan sudah optimal, dan jika ditemukan adanya celah keamanan dapat segera dilakukan perbaikan.

7. Memelihara keamanan (*Maintain security*)

   Keamanan harus dijaga dengan menjadwalkan audit independen berkala, membaca audit log, menanggapi insiden, membaca literatur saat ini dan peringatan agen, melakukan pengujian keamanan, pelatihan administrator keamanan, dan memperbarui rencana dan kebijakan keamanan.

   Keamanan jaringan harus menjadi proses abadi. Risiko berubah seiring waktu, dan sebagainya harus keamanan. Penerapan, pemantauan, pengujian, dan peningkatan keamanan adalah proses yang tidak pernah berakhir.

F. Kondisi *Eksisting* Jaringan Intra Pemerintah

Kondisi *eksisting* Jaringan Intra Pemerintah Kabupaten Murung Raya dapat dibagi menjadi 3 (tiga) zona yakni :

1. Zona internet

   Terdiri dari 1 (satu) koneksi ke penyedia jasa layanan internet (*Internet Service Provider* - ISP) dengan kapasitas yakni *bandwidth* sebesar 1300 Mbps.

   Layanan internet yang digunakan yakni IP Transit karena Diskominfo Murung Raya telah memiliki *Autonomous System* (AS) *Number* yakni AS139441 atas nama Dinas Komunikasi, Informatika, Statistik dan Persandian Kab. Murung Raya. Dengan memiliki AS Number sendiri maka Diskominfo memperoleh IP Publik yang dapat digunakan sebanyak 256 dengan alamat 103.145.27.0/24.

2. Zona Jaringan Area Kabupaten (MAN)

Jaringan area metropolitan atau Metropolitan Area Network merupakan jaringan untuk menghubungkan lokasi Organisasi Perangkat Daerah (OPD), dan Unit Pelaksana Teknis (UPT) ke Pusat Data atau Pusat Operasi Jaringan (Network Operation Center - NOC). Kondisi saat ini sebagian besar lokasi OPD, kecamatan, dan UPT sudah terhubung ke Jaringan Intra Pemerintah Kabupaten Murung Raya yang dikelola oleh Diskominfo dengan menggunakan media koneksi kabel f*iber optic* (FO). Tersisa satu lokasi yang 1 (satu) lokasi OPD yang belum terhubung ke JIP. Infrastruktur fisik jaringan MAN yakni kabel FO dikelola sendiri oleh Diskominfo.

3. Zona DeMilitarized Zone (DMZ)

   Zona DMZ untuk penempatan server - server aplikasi. *Switch server* langsung terhubung dengan *Router Firewall*. Akses dari internal maupun eksternal akan disaring (filter) oleh *Router Firewall*.

G. Usulan Infrastruktur Jaringan Data

Infrastruktur jaringan data yang ada saat ini kurang adaptif terhadap semakin besarnya lalu lintas data, proses, dan pengguna serta keamanan jaringan. Oleh karena itu, arsitektur infrastruktur jaringan perlu didesain dengan menggunakan pendekatan zonasi. Zonasi infrastruktur jaringan akan memudahkan dalam pengembangan skalabilitas (*scalable*) sesuai dengan fungsi atau layanan dari zona tersebut. Zonasi yang diusulkan terdiri dari:

a. Zona Jaringan Inti (*Core Network*)

   Merupakan zona interkoneksi antar zona. Perangkat pendukung zona jaringan inti adalah *Switch Layer 3* dengan kapasitas besar untuk menangani lalu lintas data antar zona. Perangkat *switch Core* ini sebaiknya tidak digunakan untuk fungsi lainnya seperti *DHPC pusat data,* dan lainnya.

b. Zona Jaringan Antar Gedung (*Campuss Network*)

   Jaringan lokal yang ada di setiap gedung–gedung di komplek perkantoran Pemerintah Kabupaten Murung Raya yang berdekatan dengan kantor Diskominfo dapat dikelola dalam satu jaringan lokal yakni jaringan antar gedung (*Campuss Network*).

c. Zona pusat data (*pusat data Farm*)

   pusat data database, file pusat data, storage yang tidak langsung diakses oleh pengguna ditempatkan di zona *pusat data Farm.*

d. Zona Internet (*Internet Edge*)

   Zona internet adalah zona yang melayani akses internet pengguna atau akses ke aplikasi *web* internet Pemerintah Kabupaten Murung Raya.

   Selain itu, terdapat *De-Militerized Zone* (DMZ) untuk lokasi pusat data – pusat data yang diakses oleh publik melalui internet seperti *web pusat data, mail pusat data,* dan *cloud file pusat data.* Interkoneksi dari *web* pusat data ke *database pusat data* atau *file storage* harus difilter terlebih dahulu oleh *firewall*.

e. Zona Jaringan Antar perangkat daerah (MAN)

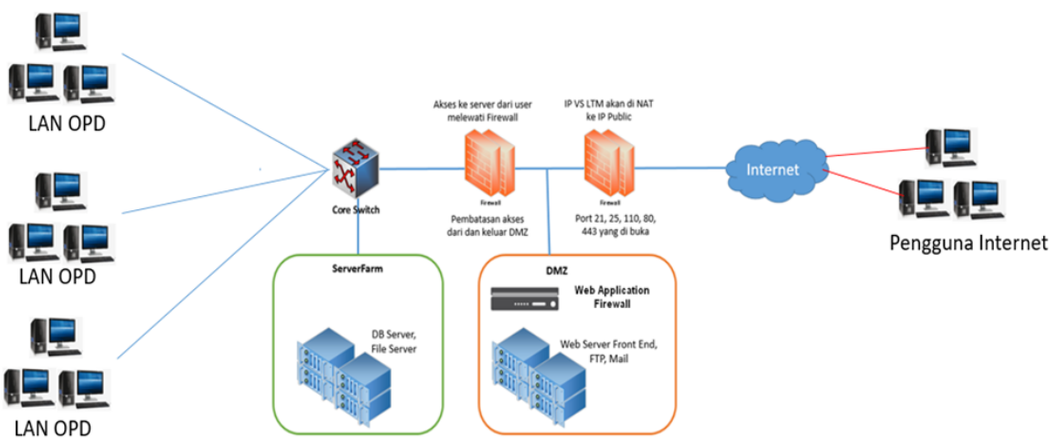
Interkoneksi antara pusat data dengan Perangkat Daerah/Unit Pelaksana Teknis ada di zona *Metropolitan Area Network (MAN)* dengan koneksi menggunakan kabel jaringan *fiber optic* atau radio link. Setiap perangkat daerah atau UPT memiliki jaringan lokal komputer *(LAN)* sendiri. Sehingga akses ke *pusat data* atau internet dari Perangkat Daerah/Unit Pelaksana Teknis menggunakan protokol *routing* seperti *static route*.

f. Zona Jaringan Antar Kementerian/Lembaga (*WAN*)

Interkoneksi antara pusat data dengan kementerian atau lembaga lainnya berada di zona *Wide Area Network (WAN)*. Interkoneksi ini menggunakan jaringan *Metro-E* atau *VPN-IP* dari penyedia layanan *WAN (provider)*. Pembatasan akses ke pusat data – pusat data di Pusat Data seperti alamat *IP, port*, dan lainnya akan dikonfigurasi di *router WAN*.

Server Farm dan DMZ

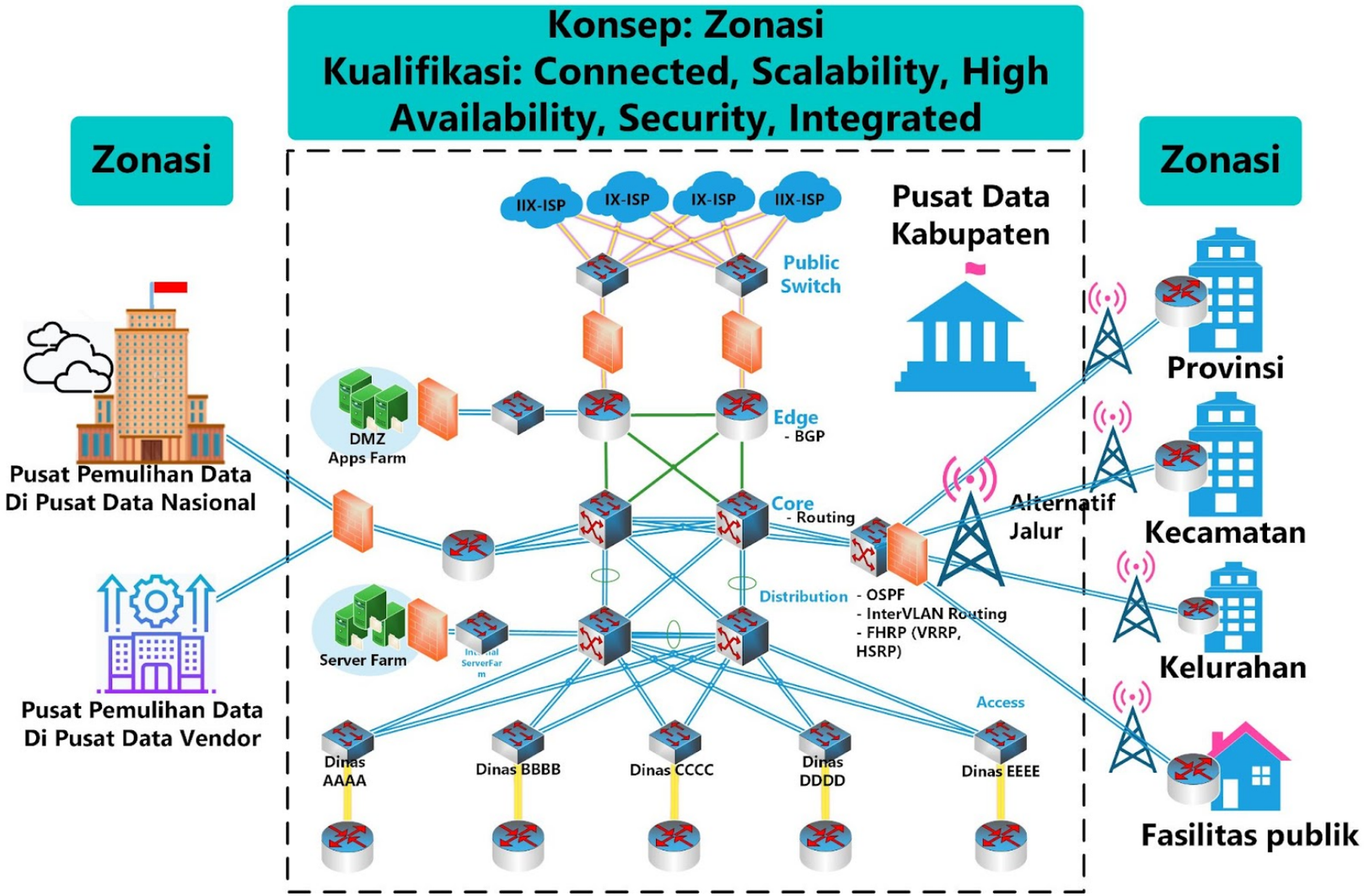
Topologi *Server Farm* dengan DMZ dapat digambarkan secara sederhana seperti di bawah ini :



Gambar 2.2.2.3.3 Pemisahan Logik Server *Farm* dengan *DMZ*

Berdasarkan gambar di atas terlihat bahwa antara pusat data *Farm* dan *DMZ* dipisahkan oleh perangkat *firewall* dan *Core Switch*. Pengguna – pengguna di perangkat daerah atau UPT akan dibatasi akses ke *server farm* melalui konfigurasi di *router* MAN. Akses aplikasi *web* dari pengguna di perangkat daerah/UPT menggunakan jaringan lokal (intranet). Akses aplikasi *web* melalui internet akan melewati *firewall* yang telah dikonfigurasi hanya *port* tertentu misal *port* 80 (*http*) atau *port* 443 (*https*) yang dibuka (*open*). *Firewall* secara logik akan dikonfigurasi untuk menyaring akses dari paket data dari *pusat data Farm* ke *DMZ* dan sebaliknya. Di dalam *DMZ* juga terdapat perangkat *Web Application Firewall* untuk perlindungan aplikasi *web* dari serangan seperti *SQL Injection, Site Cross Scripting (XSS),* dan lain-lain. Berikut ini adalah gambar usulan arsitektur jaringan data Diskominfo Pemerintah Kabupaten Murung Raya berbasis Zonasi.

Berikut ini adalah usulan topologi Jaringan Intra Pemerintah Kabupaten Murung Raya.



Gambar 2.2.2.3.4. Usulan Topologi Jaringan Intra Pemerintah

Berdasarkan gambar topologi di atas sebagai berikut :

1. koneksi internet dibagi menjadi 2 (dua) layanan yakni :
   a. IP Transit yang digunakan untuk akses internet pusat data.
   b. *Broadband* yang digunakan untuk akses internet komputer pengguna, perangkat bergerak (laptop), maupun telepon cerdas (*smartphone*).
2. koneksi internet *IP Transit* maupun *Broadband* menggunakan 2 (dua) penyedia layanan internet (ISP).
3. semua perangkat inti dan kritis sudah *redundant* seperti :
   a. *router internet IP Transit* maupun *router internet Broadband;*
   b. Next-Generation Firewall (NG-Firewall);
   c. *Core Switch*; dan
   d. *Switch* pusat data.
4. *DMZ* digunakan untuk penempatan pusat data - pusat data yang diakses oleh publik/masyarakat melalui internet seperti *web* pusat data aplikasi, email pusat data, dan *cloud storage*. *Switch* pusat data DMZ langsung terkoneksi ke *NG-Firewall.*
5. *Pusat data Farm* digunakan untuk penempatan pusat data - pusat data yang hanya dapat diakses dari dalam jaringan Diskominfo antara lain pusat data Database, File pusat data, DNS pusat data, NTP pusat data, DHCP, dan lain - lain. *Switch pusat data Farm* langsung terkoneksi ke *Switch Core*.
6. Jaringan Lokal (LAN) Gedung A, dan B merupakan koneksi komputer, printer, dan lainnya yang berada satu gedung (Diskominfo) dengan perangkat jaringan utama. Jaringan LAN terdiri dari jaringan kabel (*wired*) dan non-kabel *(wireless).* Pengaturan perangkat *Access Point* pada jaringan *wireless* menggunakan *Wireless Controller* yang terkoneksi dengan *Switch Core*.
7. Jaringan Dalam Kota (*MAN*) merupakan koneksi antar *LAN* di setiap kantor perangkat daerah yang tersebar di beberapa lokasi. Interkoneksi menggunakan media *fiber optic* atau radio *link (wireless)*.
8. Jaringan Skala Luas (*WAN*) merupakan koneksi antara jaringan Diskominfo dengan Kementerian/Lembaga lain. Interkoneksi menggunakan layanan *VPN-IP* atau *Metro-E.*

2.2.2.4. Sistem Penghubung Layanan Pemerintah

Seiring dengan adanya perkembangan proses bisnis serta kebutuhan pengguna informasi seperti pertukaran data/informasi antar organisasi di lingkungan pemerintahan, dan teknologi aplikasi yang heterogen maka diperlukan suatu sistem yang memudahkan dalam proses pertukaran data antar organisasi. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik paragraf 7 Sistem Penghubung Layanan Pemerintah pasal 33:

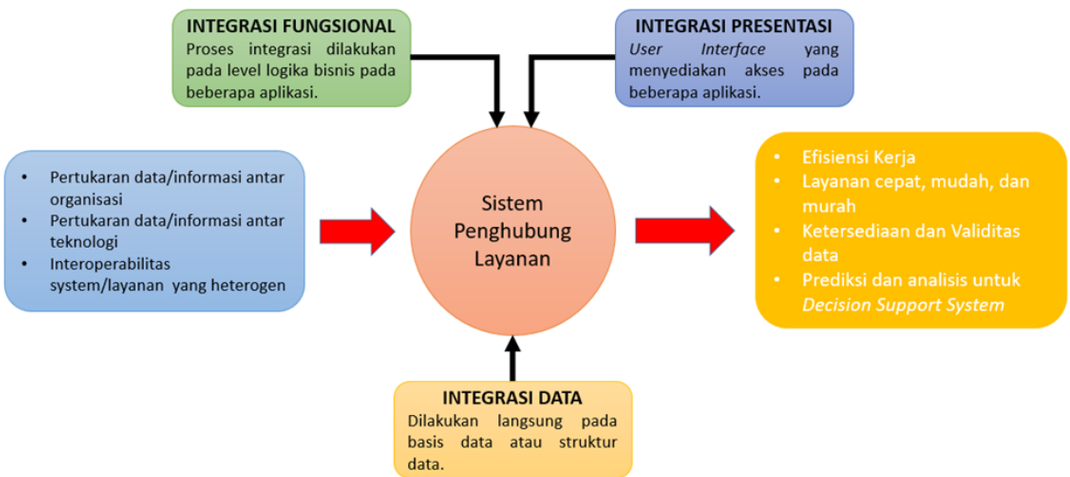
1. Penggunaan Sistem Penghubung Layanan pemerintah bertujuan untuk memudahkan dalam melakukan integrasi antar Layanan SPBE.

2. Setiap Instansi Pusat dan Pemerintah Daerah harus menggunakan Sistem Penghubung Layanan Pemerintah.

Sistem Penghubung Layanan Pemerintah adalah sistem yang digunakan untuk menghubungkan berbagai layanan yang ditawarkan oleh pemerintah melalui satu *platform* atau portal tunggal. Ini memungkinkan masyarakat untuk dengan mudah menemukan dan mengakses berbagai layanan pemerintah yang dibutuhkan tanpa harus mengunjungi berbagai situs *web* atau kantor pemerintah yang berbeda. Sistem ini biasanya mencakup *fitur* seperti pengajuan permohonan *online*, informasi status permohonan, dan pembayaran *online* untuk layanan yang ditawarkan.

Sistem penghubung layanan pemerintah adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE dengan tujuan antara lain:

a. efisiensi kerja;
b. mewujudkan layanan yang cepat, mudah, dan murah;
c. meningkatkan tingkat ketersediaan, dan validitas data; dan
d. dapat melakukan prediksi dan analisis untuk sistem pengambil keputusan (*Decision Support System*).



Gambar 2.2.2.4.1. Sistem Penghubung Layanan Pemerintah

Secara umum, Sistem Penghubung Layanan Pemerintah terdiri dari: Integrasi Data (Proses integrasi dilakukan langsung pada basis data atau struktur data dari aplikasi), Integrasi Presentasi (Proses integrasi dengan membuat antarmuka pengguna yang menyediakan akses pada beberapa aplikasi) dan Integrasi Fungsional (Proses integrasi dilakukan pada level logika bisnis pada beberapa aplikasi). Adapun secara detail Sistem Penghubung Layanan Pemerintah dijabarkan sebagai berikut :

A. Integrasi Data

Integrasi data fokus pada perpindahan data antara aplikasi dengan tujuan membagi data yang sama ke beberapa aplikasi yang berbeda. Dari sudut pandang teknis, integrasi level data ini secara relatif lebih sederhana yang sudah sangat dikenal

oleh kebanyakan pengembang. Mengakses basis data lebih mudah dan ada beberapa *tools* yang memudahkan *sharing* data dan mempercepat. Selain itu, integrasi level data tidak memerlukan perubahan aplikasi. Integrasi data merupakan proses mengkombinasikan dua atau lebih set data agar mempermudah dalam berbagi data rangka mendukung manajemen informasi di dalam sebuah lingkungan kerja. Integrasi data menggabungkan data dari berbagai sumber database yang berbeda ke dalam sebuah penyimpanan seperti gudang data (*data warehouse*). Integrasi data diperlukan karena adanya berbagai kebutuhan, seperti :

a. Data yang sama (misalnya: data penduduk) dapat dipakai bersama antar bagian organisasi (antar instansi); dan
b. Data suatu instansi dapat dipakai bersama oleh instansi-instansi lain yang memerlukan (tidak perlu ada duplikasi data dalam suatu lingkungan organisasi).

Beberapa hal yang harus diperhatikan dalam proses integrasi data antara lain :

a. Integrasi data perlu dilakukan secara cermat karena kesalahan pada integrasi data dapat menghasilkan *output*/keluaran yang tidak sesuai dan berdampak pada pengambilan keputusan.
b. Syarat integrasi harus dipenuhi dan dapat dilakukan dengan berbagai cara, seperti: konsisten dalam penamaan variabel, konsisten dalam ukuran variabel, konsisten dalam struktur pengkodean dan konsisten dalam atribut fisik dari data. Adapun masalah-masalah yang mungkin ada pada integrasi data yaitu adanya heterogenitas data, otonomi sumber data, kebenaran dan kinerja *query*/permintaan.

Penerapan interoperabilitas data diperlukan kaidah sebagai berikut :

1. Konsisten dalam sintak/ bentuk, struktur/skema/ komposisi penyajian, dan semantik/artikulasi keterbacaan.
2. Disimpan dalam format terbuka yang dapat dibaca sistem elektronik.

Fokus Pengembangan SPL

SPL dapat dikembangkan dengan berdasarkan pemangku kepentingan yang terlibat seperti pemerintah, swasta baik lokal maupun internasional :

1. G2G: Interaksi sistem antar lembaga atau badan pemerintahan;
2. G2B: Interaksi sistem antara badan pemerintahan dan bisnis/industri;
3. G2C: Interaksi sistem antara badan pemerintahan dengan masyarakat;
4. G2Org: Interaksi sistem antara badan pemerintahan dengan organisasi non pemerintah; dan
5. G2OG: Interaksi sistem badan pemerintahan antar negara.

***Application Programming Interface* (API)**

Aplikasi Perantara Akses Data Elektronik yang berbasis Layanan *Web* umumnya dinamakan Antarmuka Program Aplikasi (*Application Programming Interface*/API) atau disingkat *Web-API*. *API* adalah sekumpulan kode pemrograman yang membantu

pengembang (*developer*) aplikasi melakukan integrasi data antara dua aplikasi berbeda secara bersamaan. *API* memungkinkan *developer* untuk membuat aplikasi dengan berbagai elemen seperti *function, protocols* dan *tools* lain. API bisa digunakan untuk berkomunikasi dengan berbagai bahasa pemrograman.

Keuntungan memprogram dengan menggunakan API adalah:

1. Portabilitas

   Programmer yang menggunakan *API* dapat menjalankan programnya dalam sistem operasi mana saja asalkan sudah terinstall *API* tersebut. Sedangkan *system call* berbeda antar sistem operasi, dengan catatan dalam implementasinya mungkin saja berbeda.
2. Lebih mudah dimengerti.

   API menggunakan bahasa yang lebih terstruktur dan mudah dimengerti daripada bahasa *system call*. Hal ini sangat penting dalam hal editing dan pengembangan.
3. Daur ulang (*Reusable*)

   Web-API bersifat *reusable* (dapat didaur ulang) tanpa merubah akses layanan yakni alamat dan atribut *end point*.

   Web-API digunakan sebagai akses terhadap suatu fungsi/prosedur pengolahan data dalam program aplikasi yang dikomunikasikan dari aplikasi lain yang berbeda *platform* dan lokasi bahkan dengan jarak yang berjauhan melalui jaringan internet umumnya dinamakan *Remote Procedure Call* (RPC) atau dengan kata lain *Web-API* dapat mengakses sumberdaya layanan, program, informasi atau data dari tempat yang berbeda.

   Web-API berfungsi menterjemahkan bentuk, struktur, dan semantik suatu sumber data ke dalam format data standar yang dapat dibaca oleh semua Aplikasi berupa format data *XML, JSON, PHP-ARRAY, PHP-SERIALIZE*.

   Komunikasi data melalui *Web-API* dapat dilakukan melalui beberapa model interkoneksi, diantaranya:

   a. *SOAP (Simple Object Access Protocol)*

Gambar 2.2.2.4.2 Arsitektur *SOAP*

Komunikasi data model *SOAP* dilakukan antara Aplikasi C*lient/Request (SOAP-Client)* dengan *Web-API/Provider (SOAP-pusat data)* melalui alamat *Web-API* dengan protokol *HTTPs (Hypertext Transfer Protocol/Secure)*. Informasi Metadata yang disediakan *SOAP-pusat data* dapat disajikan melalui aplikasi Web-Browser dalam bentuk dokumen format *XML* dengan nama *Web Services*

Description Language (WSDL), sementara data permintaan *(SOAP-Request)* dan tanggapan (SOAP-Response) dilewatkan diantara *SOAP-Client* dan *SOAP-pusat data* dalam format dokumen *XML SOAP-Envelope* yang dibentuk oleh fungsi *SOAP-pusat data* pada *Web-API.*

b. *REST (Representational State Transfer)*

Gambar 2.2.2.4.3. Arsitektur *REST*

Komunikasi model *REST* dilakukan antara Aplikasi *Client/Requester* dengan *Web-API/Provider* melalui Alamat Web-API dengan protokol *HTTPs (Hypertext Transfer Protocol/Secure)*. Informasi Metadata yang disediakan *Web-API* dapat disajikan melalui aplikasi *Web-Browser* dalam bentuk dokumen format *XML/HTML/JSON/CSV* dengan nama *Web Application Description Language (WADL)*, sementara data permintaan *(Adapter-Request)* dan tanggapan *(API-Response)* dilewatkan di antara Aplikasi dan *Web-API* dalam format dokumen standar *XML, JSON, RSS* yang dibentuk oleh *Web-API.*

B. Integrasi Presentasi

Integrasi interaksi pengguna dapat dicapai melalui pembuatan pengguna dengan sistem data yang berbeda. Misalnya menggunakan pintu untuk berinteraksi dengan data dan sistem intelegensi bisnis yang berbeda. Dengan demikian aplikasi dapat terintegrasi sehingga pengguna dapat melakukan operasi dengan *Single Sign On (SSO).*

Sistem *SSO* merupakan salah satu teknologi yang dapat mengizinkan para penggunanya untuk dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Sistem *SSO* merupakan salah satu solusi untuk *identity management* dan *access control* yang ada di dalamnya. Penerapan sistem *SSO* memberikan kemudahan kepada pengguna dengan cukup melakukan otentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat di dalam suatu jaringan atau aplikasi.

C. Integrasi Fungsional (Proses Bisnis)

Integrasi proses bisnis dilakukan dengan cara mengkoordinasikan setiap aktivitas melalui proses bisnis, seperti penjualan dan penagihan. Adapun tahapan dalam integrasi proses bisnis yaitu perencanaan dalam menentukan arah perusahaan, menerjemahkan strategi yang dibentuk dalam proses bisnis perusahaan, dan menerapkan serta memastikan bahwa proses bisnis yang direncanakan dijalankan

sesuai dengan strategi perusahaan. Latar belakang diperlukannya integrasi proses bisnis antara lain:

a. Efisiensi

   Beberapa proses bisnis digabungkan menjadi satu proses yang terintegrasi.

b. Persaingan bisnis

   Persaingan instansi lain dengan konsep proses bisnis yang terintegrasi, sehingga integrasi harus dilakukan untuk bersaing

c. Perkembangan Teknologi Informasi

   Semakin berkembangnya teknologi informasi sehingga integrasi proses bisnis semakin lebih mudah dilakukan.

D. Kondisi Eksisting Sistem Penghubung Layanan

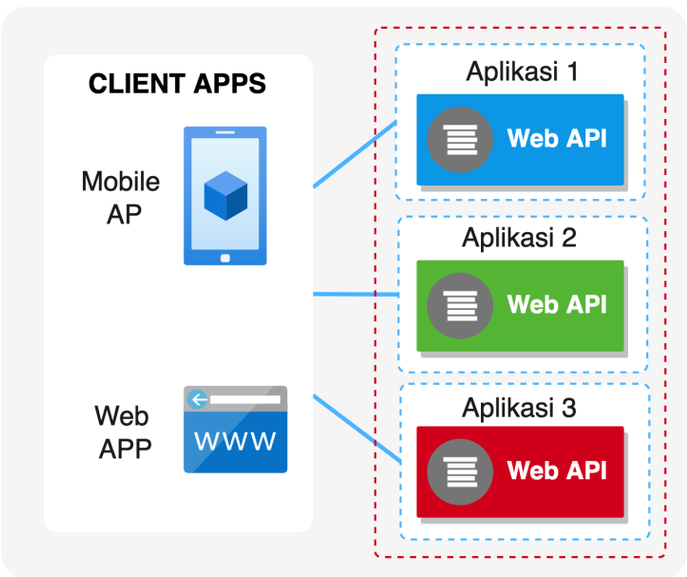
Kondisi saat ini, Pemerintah Kabupaten Murung Raya sudah mengimplementasikan teknologi *Application Programming Interface* (API) sebagai antarmuka yang dapat menghubungkan satu aplikasi dengan aplikasi lainnya untuk berbagi data. Koneksi API masih *point-to-point* antar aplikasi, dan belum dikelola dalam satu manajemen (API *Gateway*).

E. Usulan Pengembangan Sistem Penghubung Layanan

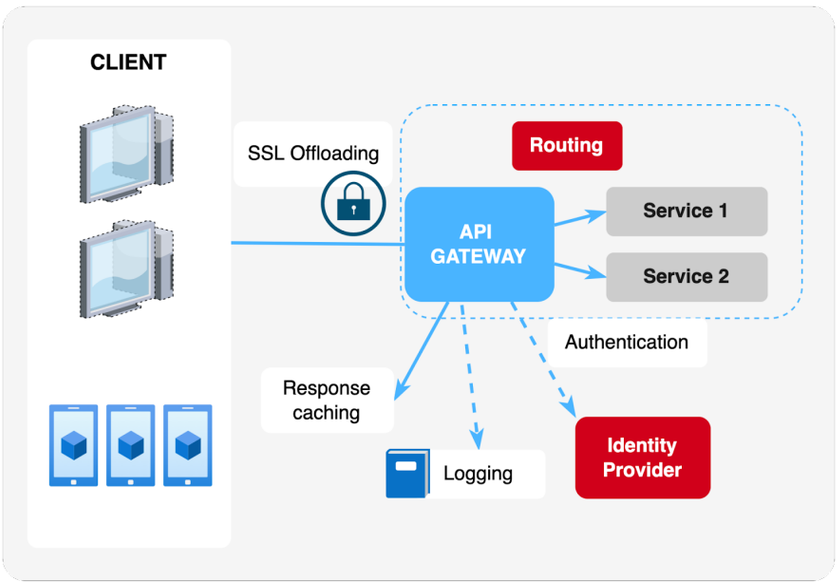
Terdapat beberapa cara suatu aplikasi mengakses *service* pada aplikasi lainnya. Salah satunya dengan pengaksesan langsung atau *direct access* pada *service* yang dimiliki oleh suatu aplikasi.

Akses langsung pada *Web* API Aplikasi

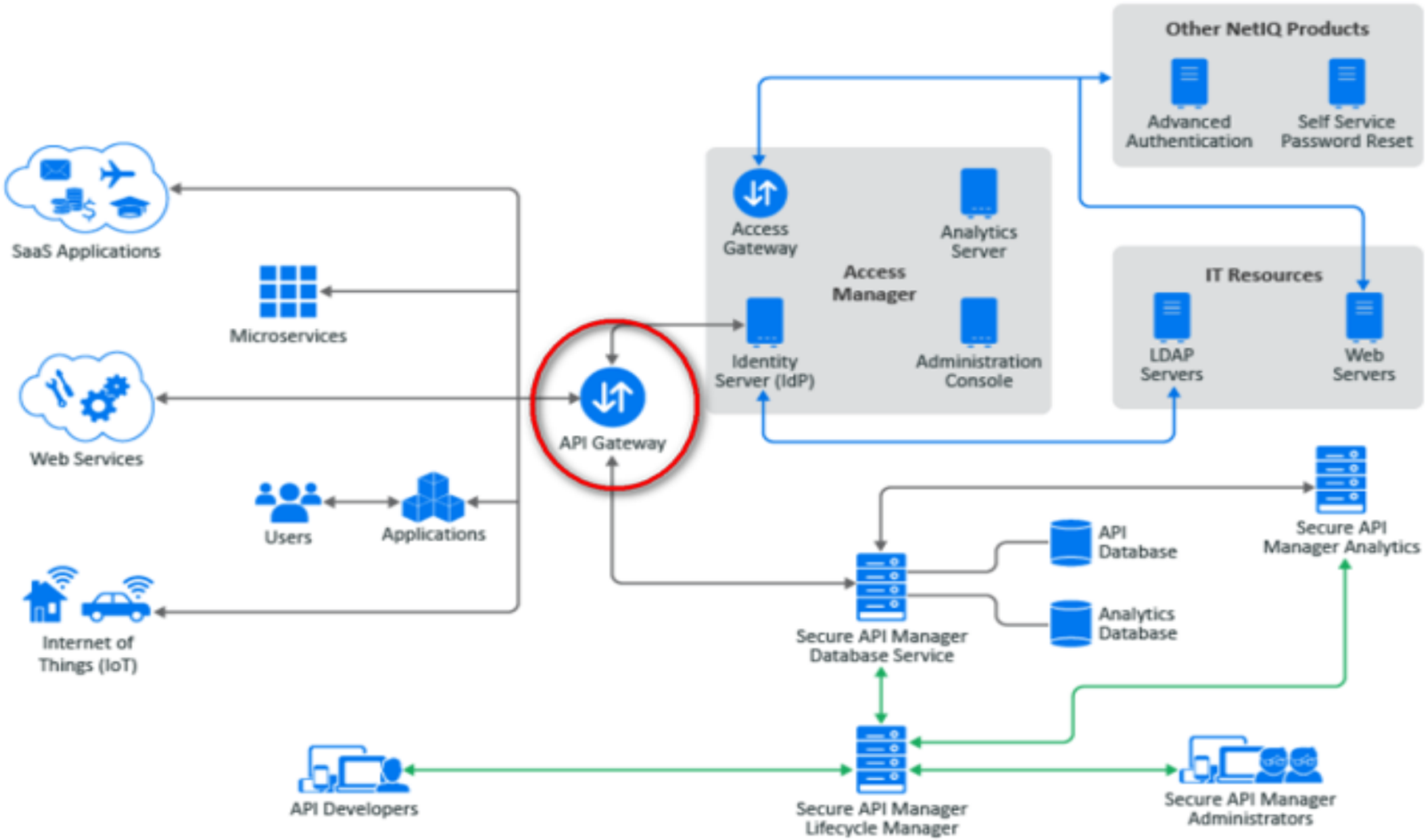
Cara pertama yang sering banyak digunakan, walaupun bukan pendekatan yang terbaik adalah dengan cara mengakses langsung pada setiap *service.* Biasanya setiap *service* memiliki suatu *IP public* yang dapat diakses dari jaringan internet. Terkadang juga dengan satu *IP public* tetapi dibedakan *port* untuk melayani setiap *service*-nya.



Gambar 2.2.2.4.4 Akses Langsung Antar API



Gambar 2.2.2.4.5. Fungsi API *Gateway*



Gambar 2.2.2.4.6. Arsitektur *API Gateway*

Berdasarkan diagram di atas maka semua *request* yang datang dari berbagai *platform* akan di *handle* atau melalui *API Gateway*.

Fitur Utama dari API *Gateway*

Berikut adalah *fitur* utama yang harus ada pada sebuah API *Gateway*.

- *Authentication dan authorization;*
- *Service discovery integration;*
- *Response caching;*
- *Retry policies, circuit breaker, dan QoS;*
- *Rate limiting dan throttling;*
- *Load balancing;*
- *Logging, tracing, dan correlation;*
- *Headers, query strings, dan claims transformation;*
- *IP whitelisting;*
- *Aggregator Request; dan*
- *Reverse proxy.*

API *Management*

API *management* adalah proses merancang, menerbitkan, mendokumentasikan, dan menganalisis API *(Application Programming Interface)* dalam lingkungan yang aman. Kebutuhan API *management* mungkin berbeda pada setiap pemangku kepentingan, namun fungsi dasarnya adalah untuk menjamin keamanan dan kelancaran proses *monitoring*. Dengan memanfaatkan API *management*, perusahaan dapat menjamin bahwa *public* atau internal API yang mereka buat aman untuk digunakan.

Fitur Utama *API Management*

Solusi API management biasanya menawarkan beberapa fitur utama yang bisa digunakan oleh *user*, diantaranya adalah:

- *API design*

  API design memberi *user* dari *developer* hingga *partner* kemampuan untuk merancang, menerbitkan, menerapkan API serta merekam dokumentasi, kebijakan keamanan, batas penggunaan, dan informasi relevan lainnya.
- *API gateway*

  Solusi API management pada umumnya juga berfungsi sebagai *API gateway*, yang bertindak sebagai *gatekeeper* untuk semua API dengan menegakkan kebijakan dan permintaan keamanan API yang relevan, serta menjamin keamanan.
- *API store*

  API Store memungkinkan *user* untuk menyimpan API di lokasi dimana mereka dapat memperlihatkannya kepada pihak internal atau eksternal. API *store* ini berfungsi sebagai tempat untuk API, dimana *user* dapat berlangganan API, mendapatkan dukungan dari *user* lain dan masih banyak lagi.

- *API analytics*

  Fungsi *API analytics* memungkinkan *user* untuk memonitor penggunaan *API, load, transaction logs*, data historis, dan metrik lain yang menginformasikan status serta keberhasilan API yang tersedia.

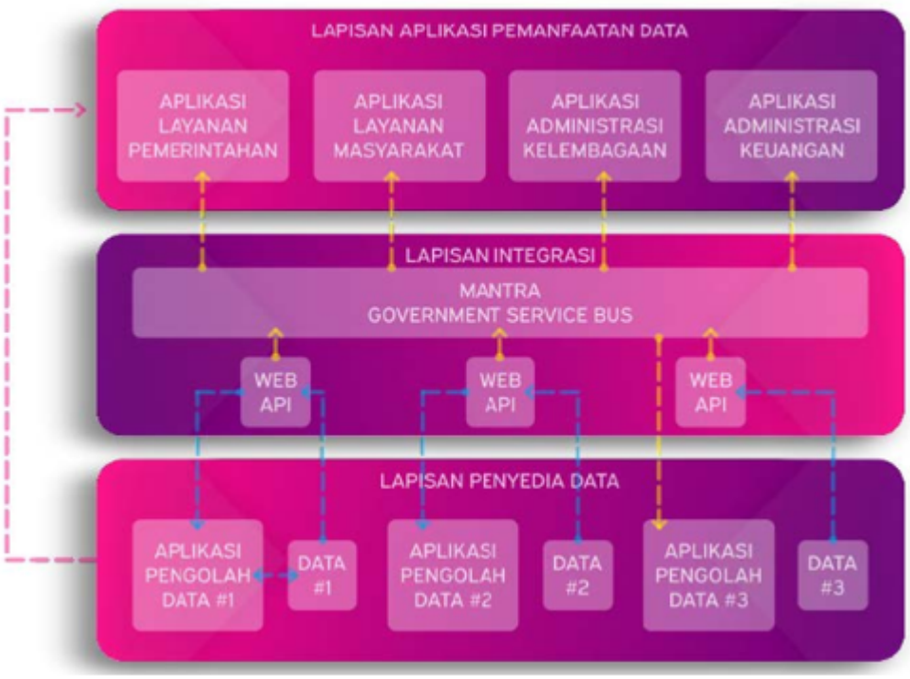
Platform* API *Management

Saat ini telah tersedia *platform* API *Gateway* yang sudah siap digunakan :

1. Zuul (*https://github.com/Netflix/zuul*);
2. Kong *(https://konghq.com/kong/);*
3. Krakend (*https://www.krakend.io/);*
4. Tyk (*https://tyk.io/);*
5. *Spring Cloud Gateway* (*https://spring.io/projects/spring-cloud-gateway*); dan
6. MANTRA-WSO2(Manajemen Integrasi Informasi dan Pertukaran Data)-Kominfo.

Sejak 2011, Kementerian Komunikasi dan Informatika telah mengembangkan aplikasi MANTRA yang berfungsi sebagai manajemen dan kanal pertukaran data antar instansi pemerintah, atau dikenal dengan *Government Service Bus* (*GSB*). *MANTRA* menerapkan prinsip arsitektur berbasis sumber daya *(Resource Oriented Architecture/ROA)* yang memanfaatkan teknologi Web-API (*Web Application Programming Interface*) untuk memfasilitasi pertukaran data.

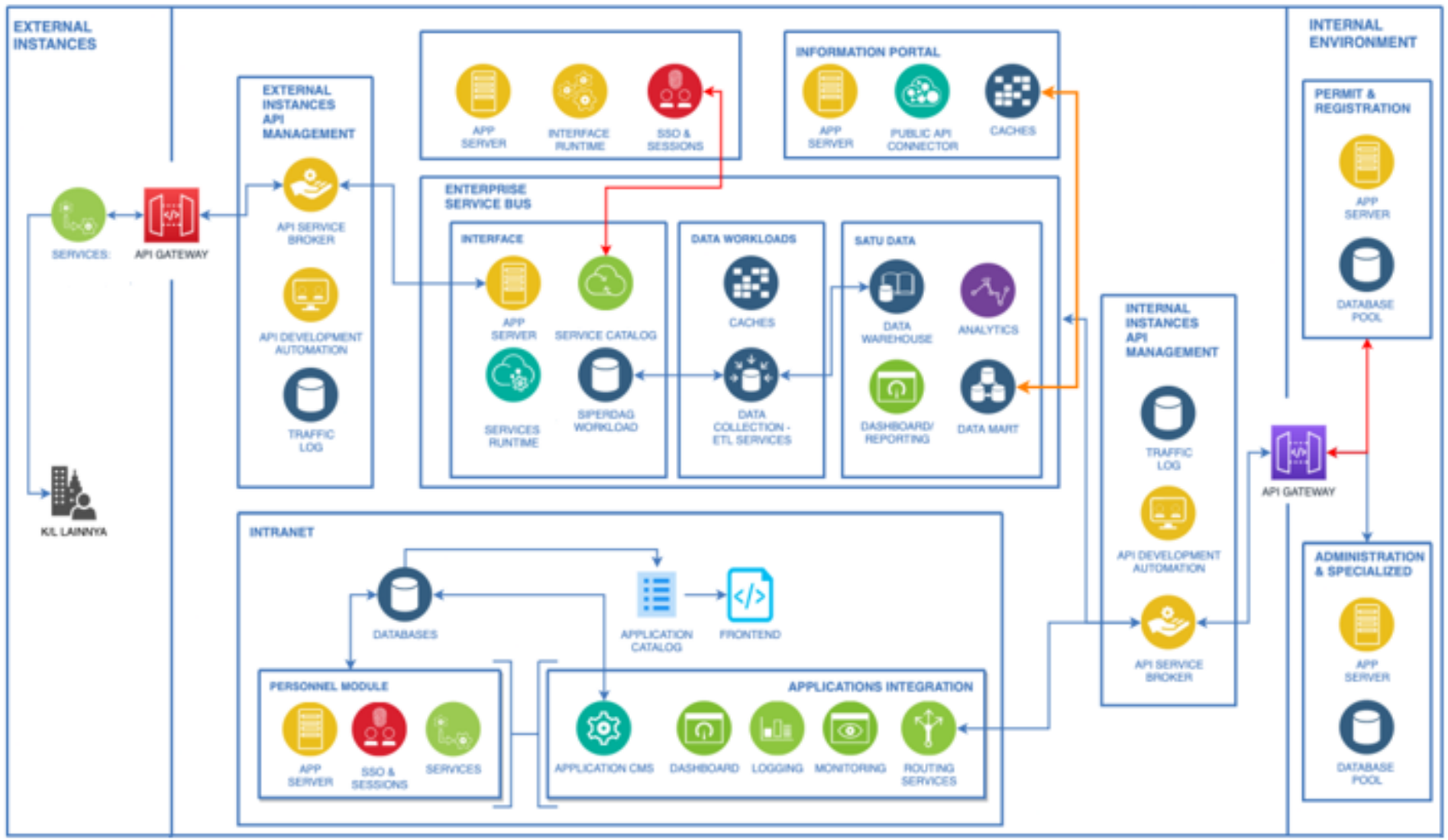
Aplikasi MANTRA dikembangkan dengan menerapkan teknologi dan pemrograman berbasis standar terbuka (*open standard*), antara lain PHP, SOAP (*Simple Object Access Protocol*), REST (*Representational State Transfer*), HTTP (*Hypertext Transfer Protocol*), dan menggunakan format data XML (*Extensible Markup Language*) dan JSON (*JavaScript Object Notation*).



Gambar 2.2.2.4.7. Arsitektur API Gateway MANTRA

Usulan Sistem Penghubung Layanan

Untuk menjaga keamanan pertukaran data, dan tingkat ketersediaan *API Manager* maka pengembangan *API Gateway* dapat menyesuaikan dengan proses bisnis dan kebutuhan serta keamanan. *API Gateway* internal dapat digunakan untuk pertukaran data yang terjadi di lingkungan internal pusat data (intranet). Sedangkan *API Gateway* eksternal digunakan untuk pertukaran data dengan pihak lain seperti Kementerian/Instansi Pemerintah Daerah lain melalui melalui jalur internet.



Gambar 2.2.2.4.8. Arsitektur API *Gateway* Internal dan Eksternal

Gambar di atas, memperlihatkan bahwa terdapat dua API *Gateway* yakni API *Gateway* Eksternal (kotak warna merah sebelah kiri) untuk melayani akses ke Kementerian/Lembaga dan API *Gateway* Internal untuk melayani akses *service* internal/intranet.

2.2.3. Keamanan Informasi SPBE

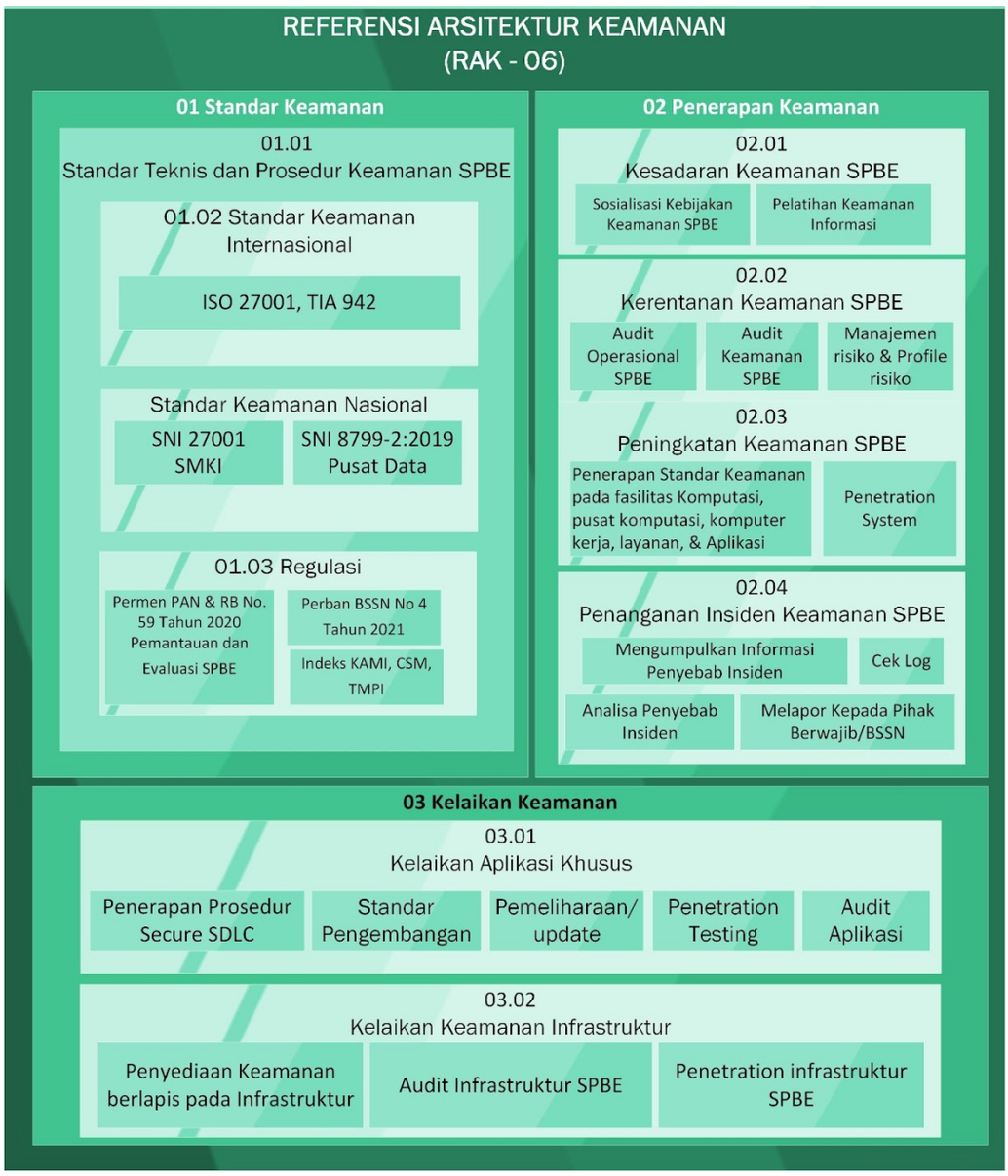
2.2.3.1. Kondisi Eksisting Keamanan SPBE

Kondisi saat ini Pemerintah Kabupaten Murung Raya belum memiliki kebijakan, standar, maupun prosedur keamanan informasi. Selain itu kegiatan seperti sosialisasi, peningkatan keamanan, dan penilaian mandiri keamanan informasi belum dapat dilaksanakan.

2.2.3.2. Arsitektur Keamanan SPBE

Arsitektur keamanan merupakan aspek vital dalam usaha organisasi untuk melindungi aset-aset penting yang dimiliki. Arsitektur keamanan menjelaskan bagaimana struktur, komponen-komponen, hubungan antar komponen dan tata letak kontrol-kontrol keamanan yang diterapkan pada infrastruktur TI organisasi. Arsitektur keamanan bisa berbeda-beda antara satu organisasi dengan organisasi lainnya, bergantung pada subsistem, produk dan aplikasi-aplikasi yang dikelola/digunakannya. Perbedaan kondisi tersebut pada gilirannya akan menyebabkan perbedaan pendekatan dalam menerapkan pertahanan mendalam (*defense in depth*).

Arsitektur keamanan mengilustrasikan bagaimana sebuah organisasi menerapkan pertahanan mendalam, serta bagaimana lapisan-lapisan kontrolnya berhubungan satu dengan lainnya. Desain dan implementasi kontrol-kontrol keamanan yang berlapis ini sangat penting terutama untuk lingkungan yang cukup kompleks. Setiap komponen pada arsitektur keamanan juga mengandung risiko keamanan. Mengingat kondisi yang berbeda-beda antara satu organisasi dengan organisasi lainnya, maka analisis dan desain arsitekturnya harus mempertimbangkan variabel dan risiko spesifik yang mungkin terjadi pada masing-masing organisasi.



Gambar 2.2.3.1.1. Arsitektur Keamanan SPBE

2.2.3.3. Manajemen Keamanan Informasi SPBE

Adapun dasar hukum dari manajemen keamanan informasi SPBE yakni:

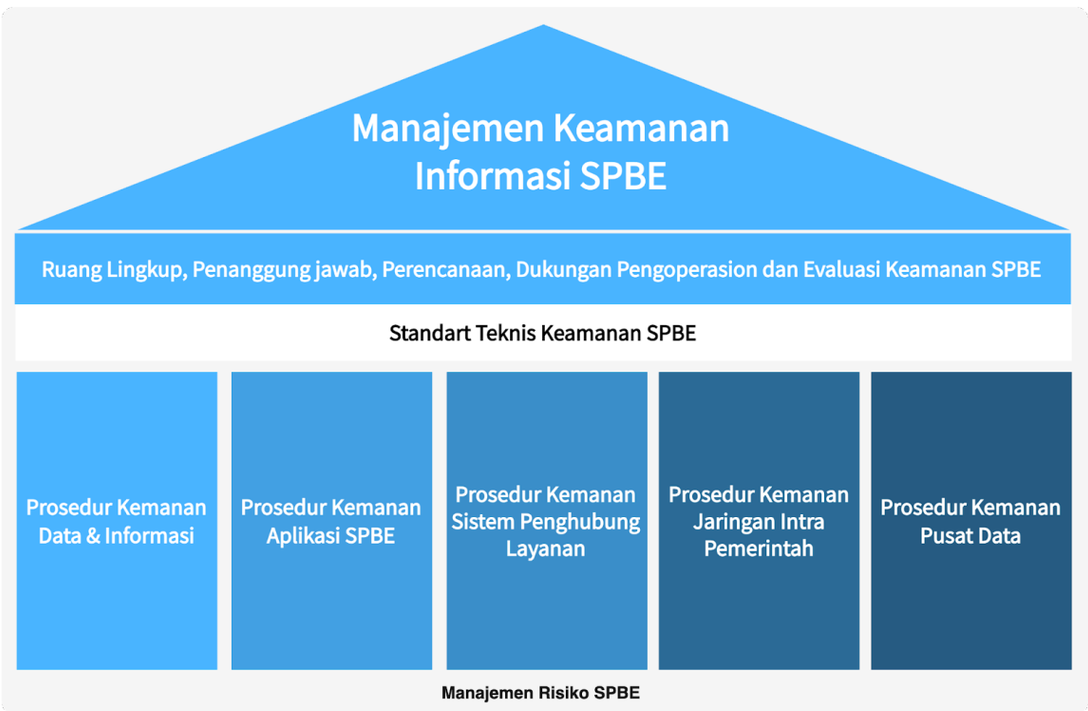
a. Perpres Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
b. Permenpan-RB Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
c. Permendagri Nomor 18 Tahun 2020 tentang Peraturan Pelaksanaan Peraturan Pemerintah Nomor 13 Tahun 2019 tentang Laporan dan Evaluasi Penyelenggaraan Pemerintah Daerah; dan
d. Peraturan BSSN Nomor 04 Tahun 2021 tentang Pedoman Manajemen Keamanan SPBE dan Standar Teknis & Prosedur Keamanan SPBE.

Perpres 95 menyebutkan bahwa Manajemen Keamanan Informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan

informasi. Selanjutnya, dalam Peraturan BSSN Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik Pasal 3 disebutkan bahwa pedoman manajemen keamanan informasi merupakan acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasioan, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi SPBE.

A. Pilar Manajemen dan Standar Teknis Keamanan SPBE

Standar teknis dan prosedur keamanan digunakan sebagai panduan untuk memastikan bahwa persyaratan keamanan minimal terpenuhi. Standar tersebut mencakup standar nasional dan internasional, serta peraturan regulasi yang berkaitan dengan keamanan SPBE. Penyusunan pedoman manajemen dan keamanan informasi berbasis risiko yang artinya melibatkan proses asesmen, identifikasi, dan manajemen risiko penggunaan teknologi informasi di SPBE yang dapat digambarkan sebagai pilar seperti di bawah ini.



Gambar 2.2.3.2.1. Pilar Manajemen dan Standar Teknis Keamanan SPBE

Proses penyusunan manajemen keamanan SPBE dapat mengacu pada gambar di bawah ini :

Gambar 2.2.3.2.2. Proses Manajemen Keamanan Informasi SPBE

B. SNI ISO 27001:2022 – Sistem Manajemen Keamanan Informasi

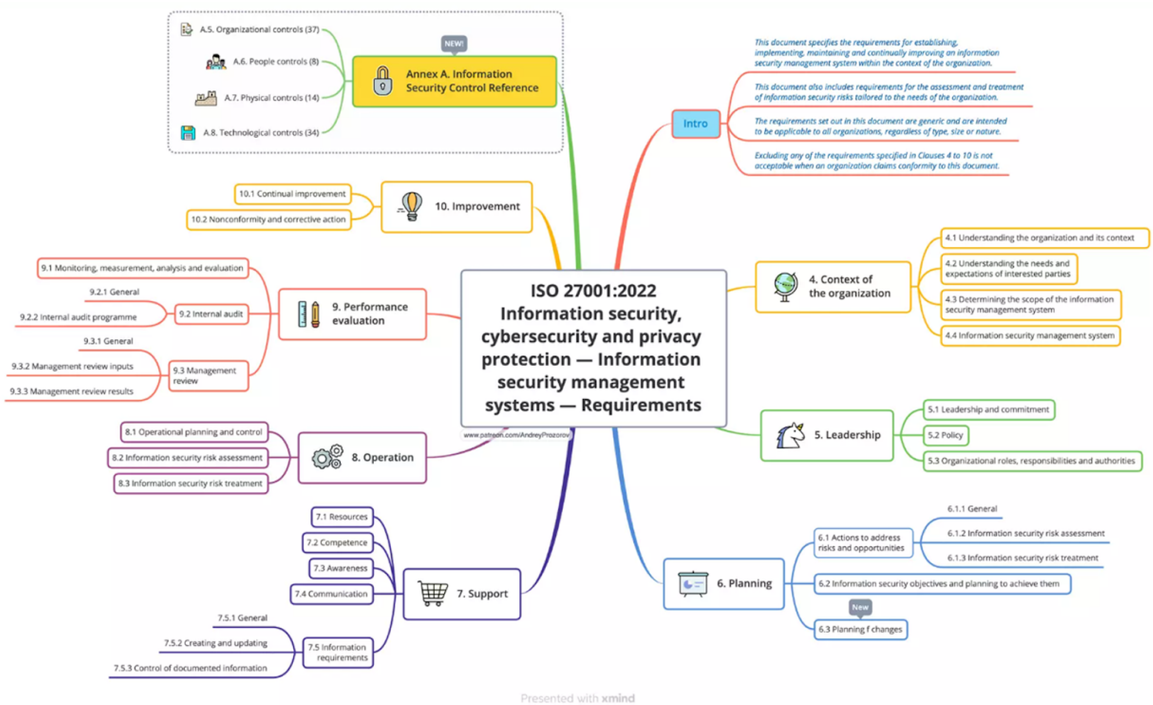
Sistem Manajemen Keamanan Informasi (SMKI) adalah cara untuk melindungi dan mengelola informasi berdasarkan pendekatan risiko bisnis yang sistematis untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi. Proses dalam SMKI disusun berdasarkan risiko pendekatan bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitor dan meninjau ulang (*Check*) serta memelihara dan meningkatkan atau mengembangkan (*Act*).

Tabel 2.2.3.2.1. Peta PDCA dalam Proses SMKI

Plan **(Penetapan SMKI)**	Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
Do **(Penerapan dan Pengoperasian SMKI)**	Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
Check **(Pemantauan dan Pengkajian SMKI)**	Mengakses dan apabila berlaku mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
Act **(Peningkatan dan Pemeliharaan SMKI)**	Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI.

Lingkup dan tujuan sistem manajemen keamanan aplikasi dari SNI ISO 27001:2022 meliputi :

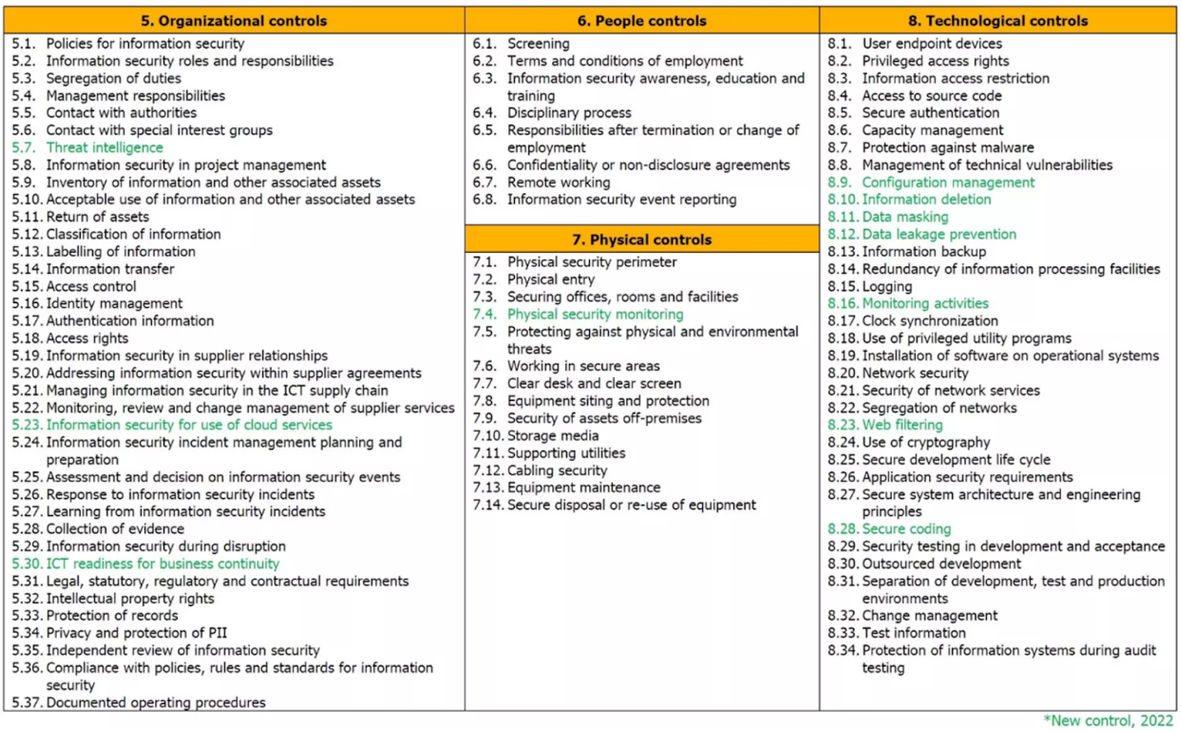
a. Mendefinisikan persyaratan untuk menetapkan, menerapkan, memelihara, meningkatkan secara berkesinambungan terhadap sistem manajemen keamanan informasi;
b. Persyaratan dalam standar ini bersifat umum dimaksudkan agar dapat diterapkan oleh organisasi tanpa membatasi jenis, ukuran, serta sifat organisasi;
c. Merupakan standar dengan pendekatan berbasis risiko, artinya melibatkan asesmen serta manajemen risiko terkait keamanan informasi; dan
d. Merupakan standar internasional dengan sasaran melindungi informasi dalam kontak CIA (*Confidentiality, Integrity*, dan *Availability*).



Gambar 2.2.3.2.3 Struktur SNI ISO 27001:2022

Berbeda dengan ISO/IEC 27001:2013, judul lengkap versi 2022 ini adalah ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection. Bagian yang mengalami perubahan paling signifikan adalah Annex A ISO/IEC 27001 yang selaras dengan pembaruan ISO/IEC 27002:2022. Annex A dari ISO/IEC 27001:2022 berisi perubahan pada keduanya, jumlah kontrol, dan daftarnya dalam grup. Judul Lampiran juga telah berubah dari "tujuan dan kontrol-kontrol referensi" menjadi "referensi kontrol keamanan informasi". Oleh karena itu, tujuan referensi dari setiap kelompok-kontrol yang ada di versi standar sebelumnya, sekarang telah dihapus.

Jumlah kontrol Annex A telah berkurang dari 114 menjadi 93. Penurunan jumlah kontrol sebagian besar berasal dari penggabungan banyak kontrol. 35 kontrol tetap sama, 23 kontrol diganti namanya, 57 kontrol digabungkan menjadi 24 kontrol, dan 1 kontrol telah dibagi menjadi 2 kontrol. 93 kontrol telah direstrukturisasi menjadi empat grup kontrol.



5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets	**7. Physical controls**	8.9. Configuration management
5.10. Acceptable use of information and other associated assets	7.1. Physical security perimeter	8.10. Information deletion
5.11. Return of assets	7.2. Physical entry	8.11. Data masking
5.12. Classification of information	7.3. Securing offices, rooms and facilities	8.12. Data leakage prevention
5.13. Labelling of information	7.4. Physical security monitoring	8.13. Information backup
5.14. Information transfer	7.5. Protecting against physical and environmental threats	8.14. Redundancy of information processing facilities
5.15. Access control	7.6. Working in secure areas	8.15. Logging
5.16. Identity management	7.7. Clear desk and clear screen	8.16. Monitoring activities
5.17. Authentication information	7.8. Equipment siting and protection	8.17. Clock synchronization
5.18. Access rights	7.9. Security of assets off-premises	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.10. Storage media	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.11. Supporting utilities	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.12. Cabling security	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.13. Equipment maintenance	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.14. Secure disposal or re-use of equipment	8.23. Web filtering
5.24. Information security incident management planning and preparation		8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

Gambar 2.2.3.2.4 Struktur SNI ISO 27001:2022

A.5 Kontrol organisasi (*organizational*) - berisi 37 kontrol

A.6 Kontrol orang (*people*) - berisi 8 kontrol

A.7 Kontrol fisik (*physical*) - berisi 14 kontrol

A.8 Kontrol teknologi (*technology*) - berisi 34 kontrol

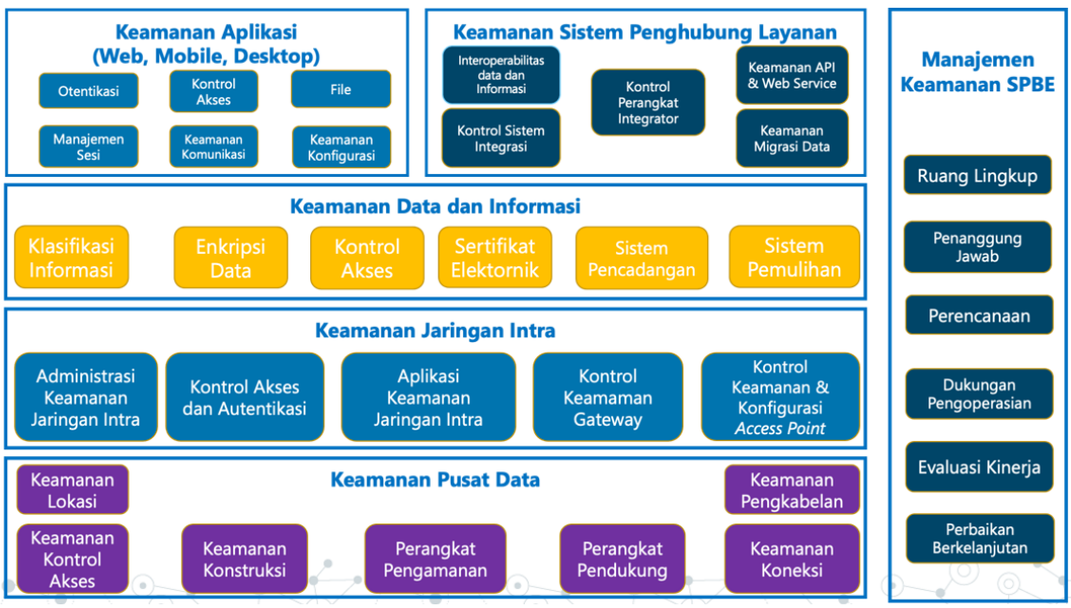
ISO/IEC 27001:2022 juga telah menambahkan 11 kontrol baru yang disebutkan di bawah ke Annex A:

1. *Threat Intelligence (A.5.7)*
2. *ICT readiness for business continuity (A.5.30)*
3. *Information security for cloud services (A.5.23)*
4. *Physical security monitoring (A.7.4)*
5. *Configuration management (A.8.9)*
6. *Information deletion (A.8.10)*
7. *Data masking (A.8.11)*
8. *Data leakage prevention (A.8.12)*
9. *Monitoring activities (A.8.16)*
10. *Web filtering (A.8.23)*
11. *Secure coding (A.8.28)*

Perusahaan yang sudah tersertifikasi ISO 27001:2013 harus menyelesaikan transisi ke ISO 27001:2022 sebelum 31 Oktober 2025. Sedangkan bagi Badan sertifikasi harus mulai mensertifikasi perusahaan dengan standar ISO 27001:2022 paling lambat 31 Oktober 2023.

2.2.3.4. Standar Teknis dan Prosedur

Standar keamanan merupakan acuan persyaratan minimal keamanan dalam bentuk standar nasional, internasional serta regulasi peraturan terkait keamanan SPBE yang telah diterapkan oleh IPPD masing-masing. Standar keamanan memastikan penerapan fungsi keamanan pada data dan informasi, infrastruktur SPBE dan aplikasi SPBE sesuai dengan persyaratan keamanan yang telah ditetapkan secara nasional ataupun internasional. Saat ini telah terbit Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.



Gambar 2.2.3.3.1. Fungsi - Fungsi pada Standar Teknis Keamanan SPBE

A. Keamanan Data dan Informasi

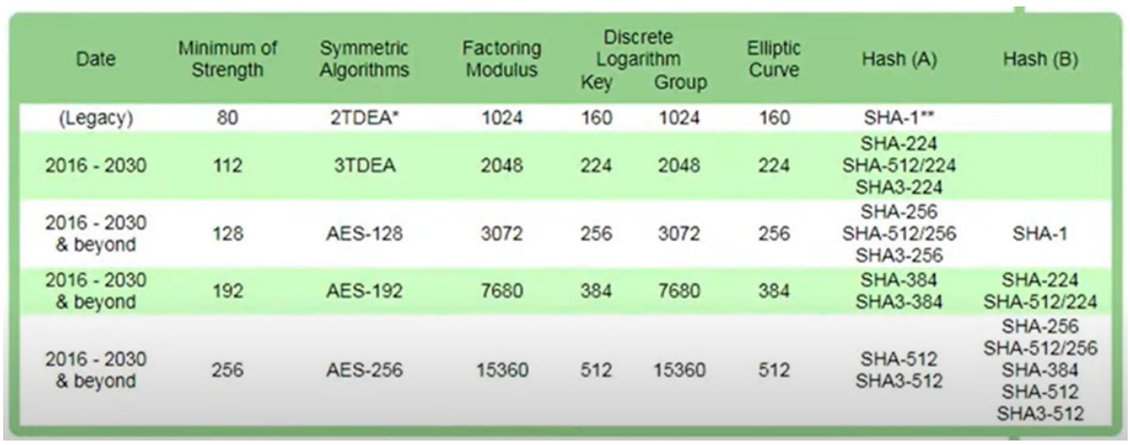
Fungsi - fungsi yang ada di dalam standar teknis keamanan data dan informasi meliputi aspek: (a) Kerahasiaan (*Confidentiality*), (b) Keaslian (*Authentication*), (c) Keutuhan (*Integrity*), (d) Kenirsangkalan (*Non-Repudiation*), dan (e) Ketersediaan (*Availability*). Berikut ini adalah rincian beberapa prosedur untuk memenuhi fungsi standar teknis.

a. Kerahasiaan dengan menerapkan:
   - Klasifikasi informasi;
   - Enkripsi dengan sistem kriptografi; dan
   - Kontrol akses atau pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.

Penerapan klasifikasi informasi dapat mengacu pada Perka ANRI Nomor 17 Tahun 2011 tentang Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis.

Tabel 2.2.3.3.1 Klasifikasi Informasi

Klasifikasi Informasi	Penjelasan
SANGAT RAHASIA	Jika diketahui oleh pihak yang tidak berhak dapat membahayakan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan bangsa
RAHASIA	Jika diketahui oleh tidak berhak dapat mengakibatkan terganggunya fungsi penyelenggaraan negara, sumber daya nasional, ketertiban umum, termasuk dampak ekonomi makro.
TERBATAS	Jika diketahui oleh pihak yang tidak berhak dapat mengakibatkan terganggunya pelaksanaan fungsi dan tugas lembaga pemerintahan, seperti kerugian finansial yang signifikan.
PUBLIK	Jika dibuka untuk umum tidak membawa dampak apapun terhadap keamanan negara.



Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

Gambar 2.2.3.3.2 Standar Kriptografi untuk Enkripsi

b. Keaslian
   - Mekanisme verifikasi;
   - Mekanisme validasi; dan
   - Menerapkan sistem *hash function*.

c. Keutuhan
   - Penerapan pendeteksian modifikasi; dan
   - Penerapan tanda tangan elektronik tersertifikasi.

d. Kenirsangkalan
   - Penerapan tanda tangan elektronik tersertifikasi; dan
   - Penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

e. Ketersediaan
   - Penerapan sistem pencadangan secara berkala;
   - Pembuatan perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan

- Penerapan sistem pemulihan.

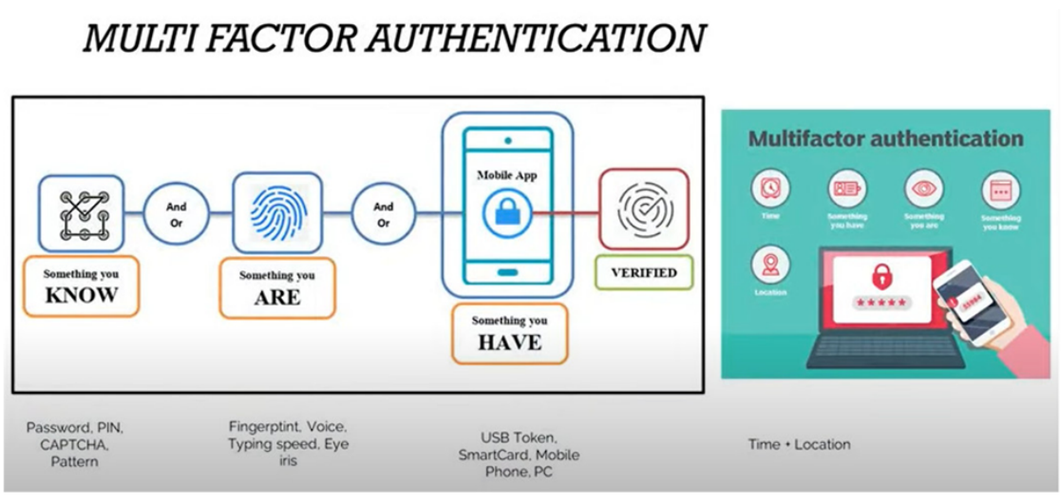
B. Keamanan Aplikasi SPBE

Keamanan aplikasi SPBE meliputi aplikasi berbasis *web* dan aplikasi berbasis *mobile*. Fungsi yang ada di dalam standar teknis keamanan aplikasi berbasis *web* meliputi aspek :

1. Autentikasi;
2. Manajemen sesi;
3. Persyaratan kontrol akses;
4. Validasi *input*;
5. Kriptografi pada verifikasi statis;
6. Penanganan *error* dan pencatatan *log*;
7. Proteksi data;
8. Keamanan komunikasi;
9. Pengendalian kode berbahaya;
10. Logika bisnis;
11. *File*;
12. Keamanan *API* dan *web service*; dan
13. Keamanan konfigurasi.

Pemenuhan beberapa aspek standar keamanan aplikasi berbasis *web* diperlukan prosedur – prosedur seperti berikut ini :

1. Autentikasi
   - menggunakan manajemen kata sandi untuk proses autentikasi;
   - menerapkan verifikasi kata sandi pada sisi pusat data;
   - mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
   - mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
   - mengatur mekanisme pemulihan kata sandi;
   - menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
   - menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.



Gambar 2.2.3.3.3. *Multi Factor Authentication*

2. Manajemen sesi
    - menggunakan pengendali sesi untuk proses manajemen sesi;
    - menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
    - mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
    - mengatur kondisi dan jangka waktu habis sesi;
    - validasi dan pencantuman *session id*;
    - perlindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
    - perlindungan terhadap duplikasi dan mekanisme persetujuan pengguna.
3. Persyaratan kontrol akses
    - menetapkan otorisasi pengguna untuk membatasi kontrol akses;
    - mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
    - mengatur antarmuka pada sisi administrator; dan
    - mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.
4. Validasi input
    - menerapkan fungsi validasi *input* pada sisi pusat data;
    - menerapkan mekanisme penolakan *input* jika terjadi kesalahan validasi;
    - memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi *input*;
    - melakukan validasi positif pada seluruh *input*;
    - melakukan *filter* terhadap data yang tidak dipercaya;
    - menggunakan *fitur* kode dinamis;
    - melakukan perlindungan terhadap akses yang mengandung konten skrip; dan
    - melakukan perlindungan dari serangan injeksi basis data.
5. Kriptografi pada verifikasi statis
    - menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
    - melakukan autentikasi data yang dienkripsi;
    - menerapkan manajemen kunci kriptografi; dan
    - membuat angka acak yang menggunakan generator angka acak kriptografi.
6. Penanganan *error* dan pencatatan *log*
    - mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
    - menggunakan metode penanganan *error* untuk mencegah kesalahan terprediksi dan tidak terduga;
    - menangani seluruh pengecualian yang tidak ditangani;
    - tidak mencantumkan informasi yang dikecualikan dalam pencatatan *log*;
    - mengatur cakupan *log* yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;

- mengatur perlindungan *log* aplikasi dari akses dan modifikasi yang tidak sah;
- melakukan enkripsi pada data yang disimpan untuk mencegah injeksi *log*; dan
- melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

7. Proteksi data
   - melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
   - melakukan perlindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
   - melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
   - melakukan penentuan jumlah parameter;
   - memastikan data disimpan dengan aman;
   - menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
   - membersihkan memori setelah tidak diperlukan.
8. Keamanan komunikasi
   - menggunakan komunikasi terenkripsi;
   - mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
   - mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
   - mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.
9. Pengendalian kode berbahaya
   - menggunakan analisis kode dalam kontrol kode berbahaya;
   - memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
   - mengatur izin terkait *fitur* atau sensor terkait privasi;
   - mengatur perlindungan integritas; dan
   - mengatur mekanisme *fitur* pembaruan.
10. Logika bisnis
    - memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
    - memastikan logika bisnis memiliki batasan dan validasi;
    - memonitor aktivitas yang tidak biasa;
    - membantu dalam kontrol anti otomatisasi; dan
    - memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.
11. File
    - mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran *file* yang diunggah;
    - melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
    - melakukan perlindungan terhadap metadata *input* dan metadata *file*;
    - melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan

- melakukan konfigurasi pusat data untuk mengunduh *file* sesuai ekstensi yang ditentukan.

12. Keamanan API dan *web service*
    - melakukan konfigurasi layanan *web*;
    - memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
    - membuat keputusan otorisasi;
    - menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;
    - menggunakan validasi skema dan verifikasi sebelum menerima input;
    - menggunakan metode perlindungan layanan berbasis *web*; dan
    - menerapkan kontrol anti otomatisasi.
13. Keamanan konfigurasi
    - mengkonfigurasi pusat data sesuai rekomendasi pusat data aplikasi dan kerangka kerja aplikasi yang digunakan;
    - mendokumentasi, menyalin konfigurasi, dan semua dependensi;
    - menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
    - memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
    - menggunakan respons aplikasi dan konten yang aman.

Standar teknis keamanan aplikasi berbasis mobile terdiri dari:

a. penyimpanan data dan persyaratan privasi;
b. kriptografi;
c. autentikasi dan manajemen sesi;
d. komunikasi jaringan;
e. interaksi *platform*;
f. kualitas kode dan pengaturan *build*; dan
g. ketahanan.

Prosedur–prosedur yang dapat diterapkan untuk memenuhi standar teknis keamanan aplikasi berbasis mobile meliputi:

a. penyimpanan data dan persyaratan privasi
    - menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
    - membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*;
    - menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan;
    - melindungi informasi yang dikecualikan saat terjadi *inter process communication*; dan
    - melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.

b. Kriptografi
   - menghindari penggunaan kriptografi simetrik dengan *hardcoded key*;
   - mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
   - menghindari penggunaan protokol kriptografi atau algoritma kriptografi yang obsolet;
   - menghindari penggunaan kunci kriptografi yang sama; dan
   - menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

c. Autentikasi dan manajemen sesi
   - menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
   - menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi;
   - memastikan pusat data menyediakan token yang telah ditandatangani menggunakan algoritma yang aman apabila menggunakan autentikasi *stateless* berbasis token;
   - memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out*;
   - menerapkan pengaturan sandi pada *remote endpoint*;
   - membatasi jumlah percobaan *log in* pada *remote endpoint*;
   - menentukan masa berlaku sesi dan masa kadaluarsa token pada *remote endpoint*; dan
   - melakukan otorisasi pada *remote endpoint*.

d. Komunikasi jaringan
   - menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
   - memverifikasi sertifikat *remote endpoint*.

e. Interaksi *platform*
   - memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
   - melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
   - menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication;*
   - menghindari penggunaan *JavaScript* dalam *WebView*;
   - menggunakan protokol *hypertext transfer protocol secure* pada *WebView;* dan
   - mengimplementasikan penggunaan serialisasi API yang aman.

f. Kualitas kode dan pengaturan *build*
   - menandatangani aplikasi dengan sertifikat yang valid;
   - memastikan aplikasi dalam *mode rilis*;
   - menghapus simbol *debugging* dari *native binary*;
   - menghapus kode *debugging* dan kode bantuan pengembang;
   - mengidentifikasi kelemahan seluruh komponen *third party*;
   - menentukan mekanisme penanganan *error*;
   - mengelola memori secara aman; dan

- mengaktifkan fitur keamanan yang tersedia.

g. Ketahanan
   - mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
   - mendeteksi dan merespons *debugger*;
   - mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
   - mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
   - mencegah aplikasi berjalan dalam *emulator*;
   - mendeteksi perubahan kode dan data di ruang memori;
   - menerapkan fungsi *device binding* dengan menggunakan *properti* unik pada perangkat;
   - melindungi seluruh *file* dan *library* pada aplikasi; dan
   - menerapkan metode *obfuscation*.

C. Keamanan Sistem Penghubung Layanan

Standar keamanan pada Sistem Penghubung Layanan untuk memastikan penerapan kontrol sistem yang menghubungkan antara Aplikasi SPBE dengan aplikasi SPBE lainnya, atau antara Aplikasi SPBE dengan web pusat data, meliputi:

a. Keamanan interoperabilitas data dan informasi
   - menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
   - menerapkan sistem enkripsi data;
   - memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan
   - menerapkan sistem *hash function* pada file.

b. Penerapan kontrol sistem integrasi
   - menerapkan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi;
   - menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/internet protocol*;
   - menerapkan sistem anti *distributed denial of service*;
   - menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung;
   - menerapkan manajemen keamanan sesi;
   - menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
   - menerapkan validasi input;
   - menerapkan kriptografi pada verifikasi statis;
   - menerapkan sertifikat elektronik pada *web authentication*;
   - menerapkan penanganan *error* dan pencatatan *log*;
   - menerapkan proteksi data dan jalur komunikasi;
   - menerapkan pendeteksi virus untuk memeriksa beberapa konten file;

- menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus); dan
- memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

c. Penerapan kontrol perangkat integrator
- menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
- menggunakan anti virus dan *anti-spyware* terkini;
- mengaktifkan fitur keamanan pada peramban *web*;
- menerapkan *firewall* dan *host-based intrusion detection systems*;
- mencegah instalasi perangkat lunak yang belum terverifikasi;
- mencegah akses terhadap situs yang tidak sah; dan
- mengaktifkan *sistem recovery* dan *restore* pada perangkat integrator.

d. Keamanan *API* dan *web service*
- menerapkan protokol *secure socket layer* atau protokol *transport layer security* di antara pengirim dan penerima *API*;
- menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner*, *resource pusat data* dan/atau *third party*;
- menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;
- melindungi layanan *web* RESTful yang menggunakan *cookie* dari *cross-site request forgery*; dan
- memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

e. Keamanan migrasi data
- memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
- memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
- mendokumentasikan format sistem basis data lama secara rinci;
- melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;
- menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan
- melakukan validasi data ketika proses migrasi data selesai.

D. Keamanan Jaringan Intra Pemerintah

Standar teknis keamanan jaringan intra diterapkan pada Jaringan Intra Pemerintah (JIP), dan Jaringan Intra Instansi Pusat dan Pemerintah Daerah (JIPPD).

Standar teknis keamanan jaringan intra meliputi :

1. aspek administrasi keamanan jaringan intra;

2. kontrol akses dan autentikasi;
3. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
4. kontrol keamanan *gateway*;
5. kontrol keamanan *access point* pada jaringan nirkabel; dan
6. kontrol konfigurasi *access point* pada jaringan nirkabel.

Beberapa aspek pemenuhan standar teknis keamanan jaringan intra diperlukan prosedur–prosedur seperti berikut ini:

1. **Aspek administrasi keamanan jaringan intra**
   - menyusun dan mengevaluasi dokumen arsitektur jaringan intra;
   - mengidentifikasi seluruh aset infrastruktur jaringan;
   - menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan jaringan intra; dan
   - membuat laporan pengawasan keamanan jaringan secara periodik.
2. **Kontrol akses dan autentikasi**
   - menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
   - menggunakan autentikasi untuk mengakses jaringan intra;
   - menerapkan pembatasan akses dalam jaringan intra;
   - mematikan atau membatasi *protocol*, *port*, dan layanan yang tidak digunakan;
   - menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
   - menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
   - menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
   - memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam jaringan intra;
   - menerapkan *secure endpoint*;
   - memblokir layanan yang tidak dikenal;
   - menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses jaringan Intra; dan
   - menerapkan pusat data perantara saat *client* mengakses pusat data *database* dalam rangka pemeliharaan.
3. **Persyaratan perangkat dan aplikasi keamanan Jaringan Intra**
   - menggunakan perangkat *security information and event management* untuk *network logging* dan *monitoring*;
   - menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
   - menggunakan perangkat *firewall*;
   - menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*;
   - menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;

- menerapkan kontrol *update patching* pada infrastruktur jaringan intra dan sistem komputer;
- menggunakan perangkat *web application firewall*;
- menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
- memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
- mengunduh perangkat lunak melalui *enterprise software distribution system*; dan
- menerapkan sertifikat elektronik.

4. Kontrol keamanan *gateway*

- menerapkan *content filtering*;
- menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada Jaringan Intra;
- menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;
- memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;
- melaksanakan manajemen *traffic gateway*; dan
- memastikan *port* tidak dibuka secara *default*.

5. Kontrol keamanan access point pada jaringan nirkabel

- menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
- menerapkan *media access control* pada *address filtering;*
- menerapkan *dedicated service set identifier*;
- menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
- menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
- menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan
- melakukan *patching firmware* secara rutin.

6. Kontrol konfigurasi *access point* pada jaringan nirkabel

- menggunakan kata sandi yang kuat;
- menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi administrator *access point*;
- memastikan *fitur* akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;
- mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
- menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

E. Keamanan Pusat Data

Standar teknis keamanan Pusat Data yakni persyaratan keamanan fisik dan persyaratan koneksi ke perangkat pusat data. Persyaratan keamanan fisik pusat data mengacu pada Standar Nasional Indonesia (SNI) yakni SNI No 8799-1:2019 tentang Panduan Spesifikasi Teknis Pusat Data:

a. Lokasi
   - Tidak berada pada area rentan bencana seperti yang dipetakan pada peta BMKG;
   - Tidak berada pada lokasi rawan hurahara seperti perkampungan padat atau kumuh;
   - Jarak dengan arteri lalu linta, jalan raya utama dan jalur kereta api umata minimal lebih dari 91 meter; dan
   - Jarak ke bandara utama dan/atau pelabuhan minimal lebih dari 1,6 km.

b. Kontrol Akses
   - Pusat data merupakan area kunjungan terbatas dan diperuntukan bagi yang telah mendapat izin memasuki area pusat data;
   - Moda memasuki pusat data bisa dengan mempergunakan kartu akses elektronik, biometrik atau pemindai jari;
   - Penyambungan interkoneksi telekomunikasi memerlukan persetujuan para pihak penyedia jasa telekomunikasi dan pengawas penyedia jasa layanan pusat data; dan
   - Untuk keamanan pusat data ditetapkan perimeter tertentu sesuai dengan kategori strata pusat data.

c. Konstruksi
   - Bangunan pusat data memiliki ketahanan terhadap gempa sesuai dengan SNI 1726:2012 sekurang – kurangnya kategori risiko II;
   - Bangunan pusat data dapat menahan beban terpusat sekurang-kurangnya hingga 1.000 kg per meter persegi. Beban dimaksud adalah beban merata bukan hanya pada tulang lantai; dan
   - Memenuhi persyaratan ketahanan material gedung meliputi ketahanan api, dan pengembunan.

d. Perangkat Pengamanan dan Pendukung
   - CCTV;
   - Access door;
   - Sistem pemadam kebakaran;
   - Sistem pendinginan;dan
   - Sistem monitoring lingkungan (suhu, kelembaban relatif ruangan, genangan air).

e. Pengkabelan
   - Pusat data memiliki pemisahan jalur kabel bermuatan listrik untuk menghindari radiasi dan interferensi elektromagnetik;

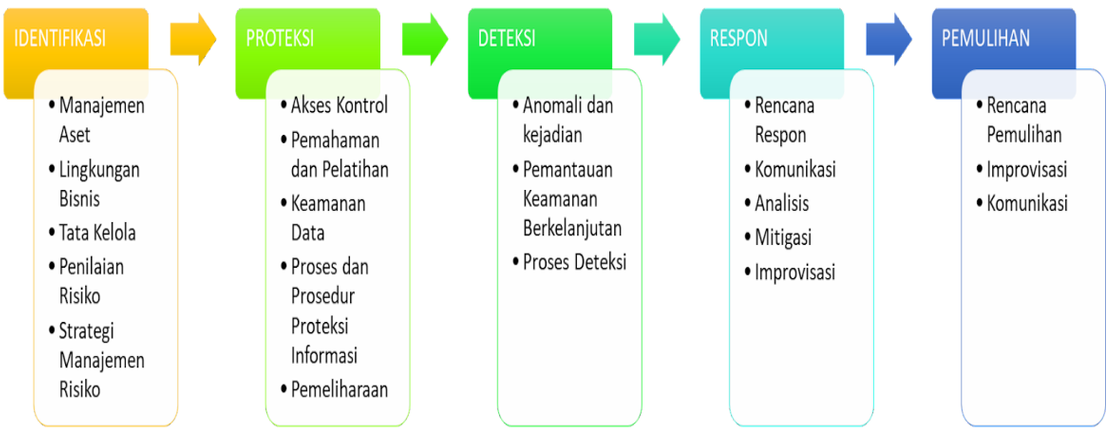
- Setiap kabel memiliki label jalur dan tercatat dalam dokumentasi dan diagram; dan
- Pusat data memiliki topologi distribusi jaringan utama dari ruang pusat data kepada pengguna jasa pusat data. Distribusi jaringan dapat mempergunakan berbagai moda kabel dan berbagai perangkat komunikasi serta memiliki label kabel.

Persyaratan keamanan koneksi ke pusat data meliputi:

1. Memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data Nasional.
2. Memutus akses fisik atau logik dari perangkat yang tidak terotorisasi.
3. Memastikan akses tingkat *administrator* ke pusat data dan perangkat jaringan utama tidak boleh dilakukan secara *remote*.

2.2.3.5. Aktivitas Keamanan Informasi

Guna menjalankan keamanan SPBE, Pemerintah Kabupaten Murung Raya dapat menerapkan keamanan SPBE yang mengacu pada Kerangka Kerja Keamanan Siber (*Cyber Security Framework*) yang dipublikasikan oleh lembaga *US National Institute of Standards and Technology* (NIST). Pada kerangka kerja tersebut terdapat 5 (lima) aktivitas yang perlu dilakukan oleh setiap organisasi dalam menghadapi serangan siber yakni identifikasi (*identity*), proteksi (*protect*), deteksi (*detect*), respon (*respond*), dan pemulihan (*recover*). Masing-masing aktivitas tersebut memiliki tujuan dan manfaat serta kegiatan atau inisiatif yang berbeda-beda, sesuai dengan fungsinya.



Gambar 2.2.3.3.4. Fungsi dan Kategori Aktivitas Keamanan Informasi

A. Identifikasi (*Identify*)

Pada tahap ini Diskominfo perlu mengidentifikasi sistem, data, aset informasi, dan kemampuan yang harus dilindungi sesuai dengan tingkat kritikalitas dan prioritas yang ditentukan. Kegiatan dalam tahap identifikasi antara lain:

1. Manajemen aset;
2. Lingkungan bisnis;
3. Tata kelola;

4. Penilaian risiko; dan
5. Strategi manajemen risiko.

B. Proteksi (*Protect*)

Pada tahap ini Diskominfo perlu melakukan tindakan mengembangkan dan menerapkan perlindungan terhadap seluruh aset informasi sesuai dengan kategori keamanan data yang telah ditentukan. Kegiatan dalam tahap proteksi antara lain:

1. Akses kontrol;
2. Pemahaman dan pelatihan;
3. Keamanan data;
4. Proses dan prosedur proteksi informasi; dan
5. Pemeliharaan.

C. Deteksi (*Detect*)

Pada tahap ini bertujuan untuk dapat mengidentifikasi terjadinya serangan siber. Kegiatan dalam tahap deteksi antara lain:

1. Anomali dan kejadian;
2. Pemantauan Keamanan berkelanjutan; dan
3. Proses deteksi.

D. Respon (*Respond*)

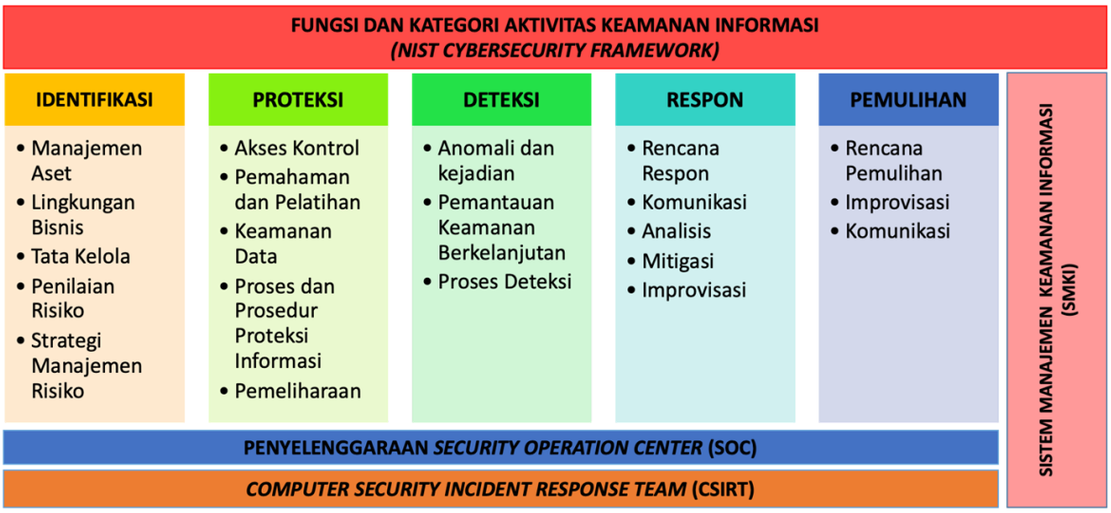
Pada tahap ini Diskominfo diharapkan dapat melakukan tindak lanjut terhadap insiden keamanan yang terdeteksi atau terjadi. Kegiatan dalam tahap respon antara lain:

1. Rencana Respon;
2. Komunikasi;
3. Analisis;
4. Mitigasi; dan
5. Improvisasi.

E. Pemulihan (*Recover*)

Pada tahap ini Diskominfo diharapkan dapat memperbaiki atau memulihkan kemampuan, layanan, dan kondisi bisnis kembali seperti sedia kala yang mengalami gangguan keamanan/siber. Kegiatan dalam tahap pemulihan antara lain:

1. Rencana Pemulihan;
2. Improvisasi; dan
3. Komunikasi.



Gambar 2.2.3.3.5. Aktivitas Keamanan Informasi

Aktivitas dan kegiatan dari identifikasi sampai dengan pemulihan dapat dilaksanakan oleh *Security Operation Center* (SOC). Dalam melaksanakan kegiatan pengamanan informasi, SOC berpedoman pada Sistem Manajemen Keamanan Informasi (SMKI). Untuk selanjutnya SOC bisa bekerja sama dengan *Computer Security Incident Response Team* (CSIRT) yang dibentuk bekerja sama dengan Badan Siber dan Sandi Negara (BSSN). CSIRT adalah tim yang menyediakan pelayanan dalam mencegah, menanggulangi dan menanggapi insiden keamanan siber, pada suatu wilayah (*constituency*) yang bertanggung jawab atas penerimaan, pemantauan dan penanganan laporan dan aktivitas insiden keamanan siber. Tim CSIRT akan bertanggung jawab penuh untuk memonitor dan mengelola berbagai isu-isu terkait dengan keamanan internet untuk menjaga aset informasi dan komunikasi dari seluruh unit-unit aktivitas organisasi.Laporan Arsitektur Kondisi Target SPBE (Sistem Pemerintahan Berbasis Elektronik) ini disusun guna memberikan gambaran kondisi kedepan yang perlu diimplementasikan di lingkungan Pemerintah Kabupaten Murung Raya. Kondisi target yang disampaikan dalam laporan ini diperoleh dari proses tabulasi dan analisa kesenjangan dari kondisi eksisting dan kondisi yang ingin dicapai.

2.2.3.6. *Security Operation Center* (SOC)

Meningkatnya serangan dan insiden siber mendorong Pemerintah Kabupaten Murung Raya untuk mengimplementasikan berbagai solusi keamanan TI yang mencakup banyak bidang area. Pemerintah Kabupaten Murung Raya merupakan salah satu lembaga yang menjadi target untuk banyak jenis serangan, sehingga perlu mengetahui kondisi keseluruhan postur keamanan saat ini dan melindunginya. Unit *Security Operation Center* (SOC) dibentuk untuk melakukan pemantauan dan perlindungan terhadap aset Pemerintah Kabupaten Murung Raya dari serangan siber. SOC menyediakan fungsi penting dalam memantau dan mendeteksi setiap kejadian yang dapat mengancam, dimana hal ini sangat penting bagi keamanan Pemerintah Kabupaten Murung Raya. Fungsi – fungsi umum yang dilakukan oleh SOC meliputi :

1. Pengelolaan Log
2. Pemantauan Proaktif berkelanjutan
3. Peringkat dan manajemen peringatan
4. Investigasi penyebab insiden
5. Respon ancaman
6. Penyempurnaan dan peningkatan keamanan
7. Pemulihan dan remediasi
8. Manajemen kepatuhan

A. Triad SOC

Triad CSOC yang mencakup yakni:

- *People* untuk berkolaborasi dan berkomunikasi dengan berbagai fungsi;
- *Technology* berupa produk keamanan yang berbeda; dan
- *Process* terdiri dari berbagai proses dan prosedur.

Gambar 2.2.3.6.1. Triad SOC

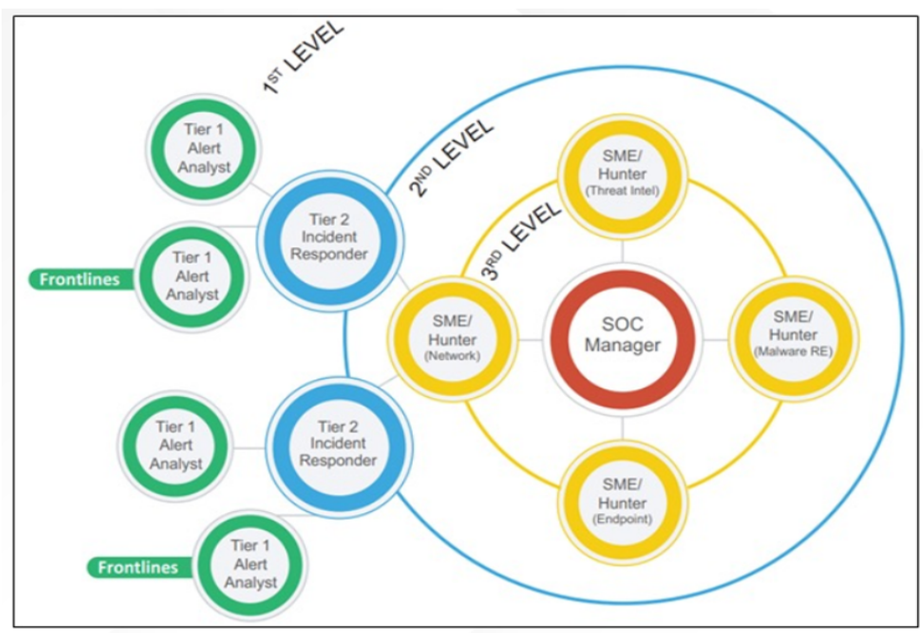
Perangkat keamanan TI yang telah dimiliki dan dikelola oleh Pemerintah Kabupaten Murung Raya seperti firewall, *Intrusion Prevention System* (IPS), *Web Application Firewall* (WAF), *Antivirus* dan lain – lain memiliki fungsi utama untuk melindungi aset Pemerintah Kabupaten Murung Raya dari jenis serangan siber tertentu. Karena dengan banyaknya solusi keamanan TI yang tersedia dan diimplementasikan, ada kebutuhan untuk

mengkonsolidasikan dan mengatur semua solusi tersebut untuk manajemen keamanan yang lebih baik. Solusi *Security Information and Events Management* (SIEM) untuk mendapatkan informasi tentang kondisi keamanan TI secara keseluruhan, sehingga Pemerintah Kabupaten Murung Raya dapat mendeteksi dan bereaksi lebih baik dan lebih cepat terhadap serangan
siber.

B. SOC – People

Operasional SOC dapat dibagi menjadi 4 (empat) tingkat atau level yakni:

- *Tier 1* (*Frontliner*)
  Monitoring dan menganalisa alert, monitoring sensor keamanan dan endpoint, mengumpulkan data penting untuk di eskalasikan ke Tier 2.
- *Tier 2* (*Incident Responder*)
  Melakukan analisa insiden secara mendalam dengan menghubungkan data dari berbagai sumber, menentukan jika ada sistem atau data yang terkena impact, memberi saran terkait remediasi, menyediakan metode analisa untuk mendeteksi ancaman.
- *Tier 3* (*SME/Hunter*)
  Memiliki pemahaman yang mendalam mengenai jaringan, endpoint, threat intelligence, forensik, dan malware reverse engineering, melakukan threat hunting, melakukan tuning dan implementasi threat detection analytics.
- *Tier 4* (*SOC Manager*)
  Mengelola sumber daya termasuk personil, anggaran, penjadwalan shift, dan strategi teknologi untuk memenuhi SLA.



Gambar 2.2.3.6.2. Hirarki Tugas dan Tanggung Jawab SOC

Untuk pemenuhan SDM untuk operasional SOC diperlukan pengetahuan dan kompetensi seperti tabel di bawah ini.

Tabel 2.2.3.6.1. Pengetahuan dan Kompetensi SDM untuk SOC

Knowledge & Skill Level	Tier-1	Tier-2	Tier-3
Basic	• CompTIA Security+ • MITRE ATTACK Framework (fundamental)	• CompTIA Security + • MITRE ATTACK Framework (fundamental)	• CompTIA Security+ • MITRE ATTACK Framework (fundamental)
Intermediate		• CompTIA CySA+ • CompTIA PenTest+ • MITRE ATTACK Framework (Intermediate)	• CompTIA CySA+ • CompTIA PenTest+ • MITRE ATTACK Framework (Intermediate)
Advance		• Cyber Intrusion Detection and Analysis • Incident Response	• CompTIA CASP+ • Incident Response

C. SOC – Process

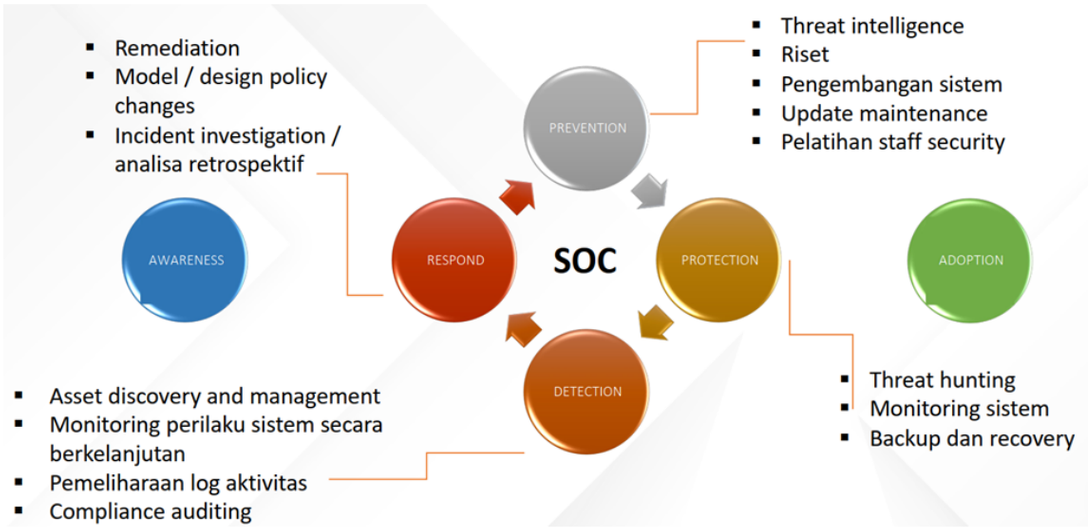
Tahapan kegiatan yang ada di SOC terdiri dari:

A. Deteksi (*Detection*), meliputi aktivitas:
- Pengumpulan dan Manajemen aset;
- Pemantauan perilaku sistem secara berkelanjutan (anomali dan kejadian);
- ·Pemeliharaan log aktivitas;
- Proses deteksi;

B. Proteksi (*Protection*), meliputi aktivitas:
- Akses kontrol
- Pemantauan sistem
- Rekam cadang (backup) dan pemulihan (recovery)
- *Threat hunting*
- Keamanan data

C. Respon (*Respond*), meliputi aktivitas:
- Rencana respon
- Komunikasi
- Remediasi
- Investigasi/analisa retrospektif

D. Pencegahan (*Prevention*), meliputi aktivitas:
- Riset
- Pengembangan sistem
- Pemeliharaan pembaruan sistem
- Pelatihan staf SOC
- *Threat intelligence*



Gambar 2.2.3.6.3. Tahapan Kegiatan di SOC

D. SOC – Technology

SOC mengumpulkan data – data dari perangkat jaringan, server, dan lainnya seperti :

- *Network Device* (*Firewall, router*)
- *Security tools*
- SaaS (Microsoft 365, Gsuite)
- *User device* (*laptop, PC*)
- *Server / virtual machine*
- *Workstation*
- *Active Directory, LDAP, DHCP*
- *Web application*
- *Digital asset* (*Domain, company name, Brand name, VIP email*, etc)

Pilihan teknologi yang dapat diimplementasikan di SOC antara lain :

- SIEM (*Security Information & Event Management*)
- IDPS
- *Security Monitoring* dan *Analytic*
- *Security Incident Management*
- SOAR (*Security Orchestration, Automation, Response*)
- *Threat Intelligence*
- *Threat Hunting*
- *Vulnerability management*
- *Log data management*

E. SIEM

SIEM (*Security Information and Event Management*) pada dasarnya menyediakan analisis real-time dari *security alert* yang dihasilkan oleh aplikasi, *server*, perangkat security

dan network. Dengan memiliki data (berbentuk *logs* dan *events*) dari berbagai perangkat IT, SIEM dapat digunakan untuk deteksi dini terhadap *targeted attack* dan pencurian data, serta untuk mengumpulkan, menyimpan, menganalisis, menyelidiki dan melaporkan data kejadian untuk respons insiden, forensik dan kepatuhan terhadap peraturan (*regulatory compliance*). Cara SIEM melakukan fungsi di atas adalah dengan menggabungkan data yang relevan dari berbagai sumber, mengidentifikasi penyimpangan dari data normal dan mengambil tindakan yang tepat (peringatan dan pelaporan). Untuk mencapai tujuan utamanya, SIEM perlu melakukan beberapa tugas dan fungsi yang menjadi kemampuan utamanya, yaitu :

A. *Log Management*

Manajemen log dari semua data yang dikumpulkan dari berbagai perangkat, seperti *server*, *database*, aplikasi dan perangkat *security*.

B. *Data aggregation*

Log Management mengumpulkan data dari berbagai sumber, termasuk *network, security, database* dan aplikasi, menyediakan kemampuan untuk mengkonsolidasi data yang dimonitor, sehingga membantu untuk mencegah hilangnya data/*event* yang penting.

C. *Correlation*

Mencari atribut yang bersifat umum, dan menghubungkan peristiwa bersama menjadi informasi yang bermakna. Teknologi ini menyediakan kemampuan untuk melakukan berbagai teknik korelasi untuk mengintegrasikan berbagai sumber, untuk mengubah data menjadi informasi yang berguna. Korelasi biasanya merupakan fungsi dari bagian Manajemen Event Keamanan dari solusi SIEM penuh.

D. *Alerting*

Analisis otomatis dari sebuah kejadian yang terkait dan membuat peringatan, untuk memberi tahu kepada pihak yang terkait dengan segera. *Alert* dapat ditampilkan ke *dashboard*, atau dikirim melalui saluran pihak ketiga seperti
email, *telegram*.

E. *Dashboards*

Perangkat SIEM dapat mengambil data peristiwa dan mengubahnya menjadi informasi berbentuk grafik untuk membantu dalam melihat pola, atau mengidentifikasi aktivitas diluar pola standar.

F. *Compliance*

Perangkat SIEM dapat digunakan untuk mengotomatisasi pengumpulan data terkait kepatuhan (*compliance*), menghasilkan laporan yang beradaptasi dengan proses keamanan, tata kelola dan audit yang ada.

G. *Searching*

Mencari ke semua log berdasarkan bermacam kriteria untuk tujuan analisa forensik dan melihat data lampau.

H. *Retention*

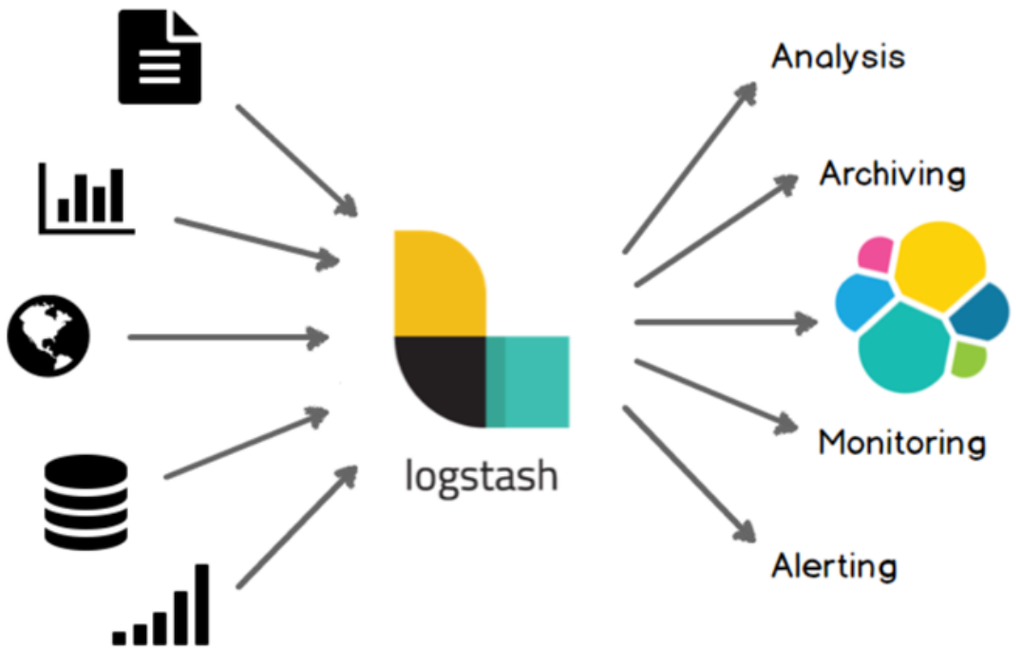
Menyediakan penyimpanan data historis jangka panjang untuk memfasilitasi korelasi data dari waktu ke waktu, dan untuk menyediakan retensi yang diperlukan untuk persyaratan kepatuhan. Retensi data log jangka panjang sangat penting dalam penyelidikan forensik karena amat jarang untuk menemukan pelanggaran jaringan akan terjadi pada saat pelanggaran terjadi.

I. *Security & Forensic analysis*: Kemampuan untuk mencari di log pada berbagai *node* dan periode waktu berdasarkan kriteria tertentu. Ini mengurangi beban, dimana harus mencari melalui ribuan bahkan jutaan log.
J. Berdasarkan uraian di atas SIEM memegang peran penting dalam implementasi dan operasi dari *Security Operation Center* (CSOC). Bersama dengan alat pemantauan, forensik dan analisis lain seperti *network forensic* dan End Point Detection and Response (EDR), analis keamanan di SOC akan melakukan pemantauan dan analisis postur keamanan organisasi, untuk menemukan ancaman apa pun yang mungkin membahayakan dan melakukan mitigasi yang diperlukan.
K. Terdapat beberapa solusi *proprietary platform* SIEM seperti LogRhytm, Splunk, dan ArcSight. Solusi ini cukup mahal, khususnya untuk pemakaian jangka panjang dan organisasi yang besar. Selain itu juga tersedia solusi open source platform antara lain AlienVault OSSIM, ELK Stack, OSSEC, Wazuh, SIEMOnster, dan lain – lain.

F. ELK

ELK terdiri dari 3 jenis perangkat lunak: *Elasticsearch, Logstash* dan *Kibana*. Semua perangkat lunak itu akan berkolaborasi satu sama lain secara *native*, mulai dari menerima log dan informasi dari berbagai sumber, sampai melaporkan, memberikan *alert* serta memvisualisasikan hasilnya. Komponen pertama yang menerima informasi adalah Logstash. Logstash adalah seperti pipa pengolahan data (server-dise) yang menerima data dari banyak sumber secara bersamaan, mengubahnya sesuai keinginan, dan kemudian mengirimkannya ke "penyimpanan" favorit. Logstash mendukung berbagai *input* yang mengambil *event* dari banyak sumber yang umum, semua secara *realtime*. Logstash juga dapat dengan mudah menerima data berbentuk log, metrik, aplikasi web, *data stores*, secara terus menerus, secara streaming. Ketika data berpindah dari sebuah sumber ke tempat lain,Logstash memfilter dan mengurai setiap peristiwa, mengidentifikasi *named*

fields untuk membuat *structure*, dan mengubahnya menjadi kumpulan format yang umum untuk tujuan analisis, dan mendapatkan nilai bisnis yang lebih mudah dan lebih cepat.



Gambar 2.2.3.6.4. Logstash

Setelah menerima, mengurai, dan mengubah data, Logstash akan mengirim data ke tujuan dan format apa pun. Logstash memiliki berbagai output yang memungkinkan mengirimkan data kemana saja, memberikan fleksibilitas untuk banyak *use-case*.Setelah log diterima, diubah dan diformat ulang oleh Logstash, akan mengirim *output* ke Elasticsearch. Elasticsearch adalah mesin pencarian dan analisis terdetail, berbasis RESTful, yang mampu memecahkan semakin banyak *use-case*. Sebagai inti dari *Elastic Stack*, Elasticsearch menyimpan data secara tersentralisasi, sehingga dapat menemukan data yang diinginkan dan mengungkap data tak terduga. Elasticsearch dapat digunakan untuk mencari semua jenis dokumen. Elasticsearch dapat melakukan dan menggabungkan banyak jenis pencarian - terstruktur, tidak terstruktur, geometrik, dan lain sebagainya.

Stack ELK terakhir sebagai SIEM dan alat *Log Management* adalah Kibana. Kibana adalah platform *analytics* dan *visualization* berbasis OSS yang dirancang untuk bekerja dengan Elasticsearch. Dengan Kibara dapat memvisualisasikan data Elasticsearch dan menavigasi *Elastic Stack*. Kibana untuk mencari, melihat, dan berinteraksi dengan data yang disimpan dalam indeks Elasticsearch.

Gambar 2.2.3.6.5. Hubungan antar Stack pada ELK

Bab III Penutup

Dokumen kondisi target ini akan dijadikan sebagai landasan dalam implementasi layanan Sistem Pemerintahan Berbasis Elektronik yang sesuai bagi Pemerintah Kabupaten Murung Raya selama 5 (lima) tahun mendatang yang dituangkan dalam dokumen Arsitektur *Eksisting* SPBE Pemerintah Kabupaten Murung Raya.

Pemerintah Kabupaten Murung Raya