BUKU II

KONDISI TARGET ARSITEKTUR SPBE

Pemerintah Kabupaten Tapin

2022

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, *trend* teknologi informasi saat ini dan yang akan datang. Sesuai dengan Perpres 95/2018 tentang Sistem Pemerintahan Berbasis Elektronik dalam paragraf Tujuan Pengembangan SPBE yang diarahkan untuk mencapai tiga tujuan utama, 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.

Dalam kerangka ini 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.

Teknologi Informasi dan Komunikasi perlu menganut prinsip-prinsip dasar untuk pemicu kesuksesan implementasi SPBE. Tinjauan dari unsur-unsur penyusun SPBE guna mencapai tujuan di atas adalah sebagai berikut:

A. Kondisi Ideal Kelembagaan

Model kelembagaan yang ideal dalam pengelolaan sumber daya SPBE di lingkungan Pemerintah Kabupaten Tapin adalah perpaduan model sentralisasi. Sentralisasi kewenangan diperlukan guna mengontrol penerapan SPBE di masing-masing SKPD. Dalam penerapan SPBE perlu dibentuk Tim Koordinasi SPBE. Tim Koordinasi terdiri dari Tim Pengarah dan Tim Pelaksana Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Tapin.

Tim Pengarah dalam Tim Koordinasi Sistem Pemerintahan Berbasis Elektronik Kabupaten Tapin mempunyai tugas:

1. Memberikan arahan dan persetujuan terhadap seluruh inisiatif program dan kegiatan SPBE di lingkungan Pemerintah Kabupaten Tapin, khususnya yang bersifat kebijakan dan anggaran/investasi.
2. Memfasilitasi proses koordinasi, kerjasama, atau integrasi penerapan SPBE dengan Instansi Pusat/Pemerintah Daerah lain.
3. Memfasilitasi penerapan tata kelola dan manajemen SPBE.
4. Melakukan pemantauan dan evaluasi berkala atas penerapan SPBE.

5. Melakukan perbaikan dan pengembangan atas hasil rekomendasi pemantauan dan evaluasi penerapan SPBE.

Tim Pelaksana dalam Tim Koordinasi Sistem Pemerintahan Berbasis Elektronik Kabupaten Tapin terdiri dari Kepala Perangkat Daerah yang mempunyai tanggung jawab terhadap aplikasi maupun sistem informasi manajemen, infrastruktur maupun keamanan informasi yang ada di lingkungan kerja masing-masing yang mempunyai tugas:

1. Mengkoordinasikan perencanaan, realisasi, operasional, dan evaluasi SPBE khususnya terkait dengan inisiatif SPBE prioritas Pemerintah Kabupaten Tapin, bekerja sama dengan perangkat daerah pengelola SPBE dan perangkat daerah pemilik proses bisnis maupun pengguna TIK lainnya;
2. Mengkoordinasikan Tim SPBE perangkat daerah;
3. Memfasilitasi perencanaan dan implementasi inisiatif SPBE lintas perangkat daerah di tingkat Pemerintah Daerah, khususnya inisiatif SPBE prioritas Pemerintah Kabupaten Tapin;
4. Memfasilitasi tata kelola SPBE yang baik di Pemerintah Kabupaten Tapin melalui penerbitan kebijakan, standar, prosedur, atau panduan yang relevan;
5. Mengkoordinasikan perencanaan dan pelaksanaan inisiatif dan portofolio SPBE Pemerintah Kabupaten Tapin;
6. Melakukan *review* berkala atas pelaksanaan implementasi SPBE di Pemerintah Kabupaten Tapin.

Tim Pelaksana Sistem Pemerintahan Berbasis Elektronik Kabupaten Tapin terdiri dari seluruh Kepala Bidang yang ada di lingkungan Dinas Komunikasi dan Informatika Kabupaten Tapin sebagai *Leading Sector* yang memiliki tugas:

1. Perumusan konsep, pelaksanaan kebijakan pengkoordinasian dan pemantauan informasi publik;
2. Perumusan dan pengkoordinasian dalam pengelolaan domain dan subdomain bagi lembaga pelayanan publik;
3. Perumusan regulasi tata kelola teknologi dan informasi menuju SPBE;
4. Perumusan konsep, pelaksanaan kebijakan, pemantauan dan evaluasi pusat data, jaringan teknologi informasi serta pengembangan sistem informasi dan keamanan informasi;
5. Pengelolaan manajemen data informasi *e-government* yang terintegrasi dengan layanan publik dan pemerintahan.

Dalam menjalankan tugasnya Tim Pengarah dan Tim Pelaksana dibantu oleh seluruh pelaksana baik dalam jabatan fungsional pranata komputer maupun jabatan fungsional teknis yang ada di Dinas Komunikasi dan Informatika Kabupaten Tapin yang dalam melaksanakan tugasnya wajib berkoordinasi maupun bekerja sama sesuai kebutuhan dan mekanisme yang berlaku.

Dalam melaksanakan evaluasi berkala terhadap implementasi Sistem Pemerintahan Berbasis Elektronik dilakukan oleh Tim Koordinasi SPBE.

Penyelenggaraan SPBE Kab. Tapin harus berdasarkan pada asas:

1. Kepastian hukum

Asas kepastian hukum merupakan landasan bahwa hukum dan ketentuan perundang-undangan harus diletakkan sebagai dasar dalam setiap kebijakan dan tindakan dalam penyelenggaraan SPBE.

2. Kemanfaatan

   Asas kemanfaatan sebagai landasan bahwa penyelenggaraan SPBE di Daerah harus dapat memberikan manfaat dan nilai tambah bagi seluruh masyarakat di Daerah, serta berbagai pihak dan komponen yang terlibat dalam penyelenggaraan SPBE di Daerah.

3. Kemudahan dan Keterjangkauan;

   Asas kemudahan dan keterjangkauan sebagai landasan bahwa penyelenggaraan SPBE di Daerah ditujukan untuk mempermudah akses Pengguna SPBE terhadap layanan SPBE, serta menyediakan layanan SPBE yang dapat dijangkau oleh seluruh kalangan masyarakat di Daerah.

4. Keterpaduan;

   Asas keterpaduan sebagai landasan bahwa penyelenggaraan SPBE harus mengedepankan adanya keterpaduan dan integrasi dari berbagai komponen dan sumber daya SPBE di Daerah.

5. Keterbukaan

   Asas keterbukaan sebagai landasan bahwa penyelenggaraan SPBE harus mengedepankan keterbukaan terhadap hak masyarakat untuk memperoleh informasi yang benar, jujur dan tidak diskriminatif mengenai penyelenggaraan SPBE, dengan tetap memperhatikan perlindungan hak asasi pribadi.

6. Akuntabilitas

   Asas akuntabilitas sebagai landasan bahwa penyelenggaraan SPBE harus dapat dipertanggungjawabkan kepada masyarakat sesuai dengan ketentuan peraturan perundang-undangan.

7. Keamanan dan keandalan

   Asas keamanan dan keandalan sebagai landasan bahwa penyelenggaraan SPBE harus dapat menjamin kerahasiaan, keandalan, keutuhan, dan ketersediaan data dan informasi yang berdasarkan peraturan perundang-undangan harus diperlakukan secara khusus, serta memastikan seluruh sumber daya pendukung SPBE dapat berjalan optimal dan sesuai dengan kebutuhan.

8. Partisipatif dan akomodatif

   Asas partisipatif dan akomodatif sebagai landasan bahwa penyelenggaraan SPBE harus dapat mendorong partisipasi aktif dari seluruh Pengguna SPBE dan dapat mengakomodasi berbagai kebutuhan dan kepentingan berbagai Pengguna SPBE.

9. Non-diskriminatif

   Asas non-diskriminatif sebagai landasan bahwa dalam penyelenggaraan SPBE, khususnya dalam pemberian Layanan SPBE, tidak membedakan suku, agama, ras, golongan, gender, dan status ekonomi.

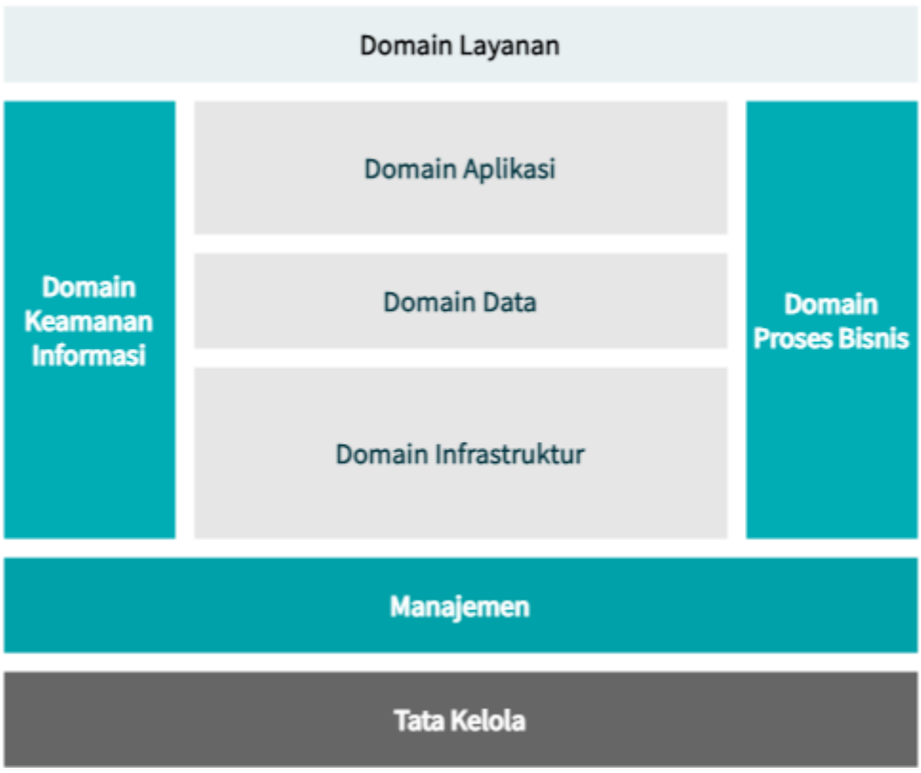
1. Kebijakan SPBE

Penyusunan kebijakan dan SOP perlu dilakukan untuk mendukung pengembangan, penggunaan, maupun pemeliharaan sumber daya TIK. Berikut ini daftar kebijakan yang diundangkan melalui peraturan yang perlu disusun.

a. Kebijakan internal arsitektur SPBE Pemerintah Daerah
b. Kebijakan internal peta rencana SPBE Pemerintah Daerah
c. Kebijakan internal layanan jaringan intra Pemerintah Daerah
d. Kebijakan internal audit teknologi informasi dan komunikasi
e. Kebijakan internal tim koordinasi SPBE Pemerintah Daerah

B. Tata Kelola Arsitektur SPBE

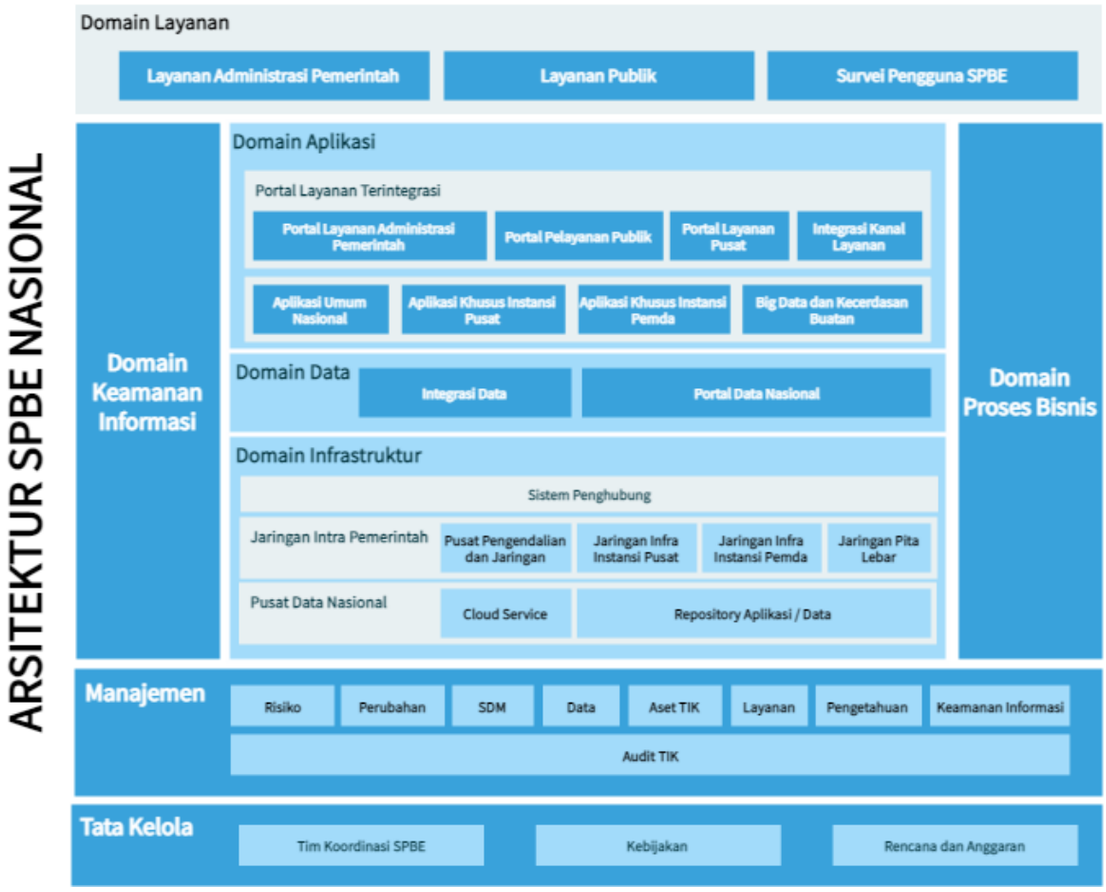
Arsitektur dan Peta Jalan SPBE merupakan panduan dalam pelaksanaan integrasi Proses Bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terpadu. Arsitektur memuat beberapa domain yang dijelaskan sebagai berikut:



Gambar 1.1.1. Domain Arsitektur SPBE

Dari gambar diatas 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 dan terarah.

Setiap domain yang disebutkan dalam kerangka SPBE memiliki detail masing-masing yang kemudian saling terkait dan dapat mendorong keberhasilan domain-domain lainnya. Detail dari masing-masing domain dijelaskan dalam Gambar 1.13



Gambar 1.1.2. Domain Arsitektur SPBE (ii)

Dalam proses penyusunan dokumen arsitektur SPBE, langkah awal yang perlu disusun terlebih dahulu adalah bidang Tata Kelola. Tata Kelola adalah rangkaian proses, kebiasaan, kebijakan, aturan, dan institusi yang mempengaruhi pengarahan, pengelolaan, serta pengontrolan kegiatan dalam institusi. 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 dan Anggaran.

Langkah kedua dalam membangun arsitektur SPBE adalah dengan menentukan bentuk-bentuk Manajemen yang akan dilakukan dalam proses pengembangan SPBE di Institusi. 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. Hal-hal yang harus ditentukan dalam proses penentuan manajemen adalah :

- Manajemen Resiko,
- Manajemen Perubahan,
- Manajemen Data,

- Manajemen SDM,
- Manajemen Aset TIK,
- Manajemen Layanan,
- Manajemen Pengetahuan, dan
- Manajemen Keamanan Informasi.

Selanjutnya manajemen yang dilakukan mencakup hal-hal dalam mendukung pengembangan domain lainnya. Domain yang akan dikelola pertama adalah Domain Proses Bisnis, disini proses bisnis dikelola sedemikian rupa sehingga dapat memberikan alur organisasi internal dan pelayanan paling efektif dan efisien. Dari 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 berbagai aplikasi lain. Adapun beberapa portal layanan yang dapat dibangun antara lain:

- Portal layanan administrasi internal pemerintah
- Portal layanan publik

Aplikasi juga dapat dibagi berdasarkan penggunaannya, yaitu aplikasi yang bersifat khusus dan bersifat umum. Adapun berdasarkan penggunaannya dapat diklasifikasikan sebagai berikut :

- Aplikasi umum nasional
- Aplikasi khusus instansi pusat
- Aplikasi khusus instansi pemda
- *Big data* dan kecerdasan buatan

Pembangunan aplikasi tentunya mengacu pada data yang dikelola oleh instansi, dalam domain data memungkinkan adanya integrasi data dan portal data nasional. Domain lain yang dikembangkan dalam proses pembangunan SPBE adalah domain infrastruktur, domain ini dikembangkan sebagai bentuk penanganan alat yang digunakan dalam pelayanan yang ada. Dalam domain infrastruktur dibagi menjadi 2 jenis yaitu infrastruktur Jaringan dan infrastruktur pusat data. Infrastruktur jaringan adalah hal-hal mengenai pengelolaan koneksi yang ada pada instansi. Termasuk didalamnya ada diantaranya pusat pengendalian dan jaringan, jaringan intra instansi pusat, jaringan intra instansi pemda, dan jaringan pita lebar. Selanjutnya untuk pusat data nasional didalamnya ada *cloud services* dan repositori aplikasi / data.

Domain terakhir yang digunakan dalam peningkatan layanan instansi adalah domain keamanan informasi, dimana aspek keamanan informasi adalah aspek-aspek yang dilingkupi dan melingkupi keamanan informasi dalam sebuah sistem informasi. Aspek-aspek ini adalah: privasi/kerahasiaan, menjaga kerahasiaan informasi dari semua pihak, kecuali yang memiliki kewenangan.

Arsitektur SPBE Kab Tapin disusun dengan berpedoman pada Arsitektur SPBE Nasional. Penyusunan Arsitektur SPBE lakukan oleh Tim Koordinasi SPBE. Untuk menyelaraskan Arsitektur SPBE Kab Tapin dengan Arsitektur SPBE Nasional, Tim Pelaksana berkoordinasi dan melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur

negara.Arsitektur SPBE dan Peta Jalan ini perlu ditinjau secara berkala minimal satu tahun sekali, dan perlu dilakukan perubahan ketika terjadi:

1. Perubahan Arsitektur SPBE Nasional;
2. Hasil pemantauan dan evaluasi pelaksanaan SPBE di Kab Tapin;
3. Perubahan substansi kondisi Arsitektur SPBE.

Peninjauan Arsitektur SPBE dan Peta Jalan dilakukan oleh Tim Koordinator SPBE. Hasil peninjauan dijadikan sebagai dasar dalam mengubah Arsitektur SPBE dan Peta Jalan.

C. Penganggaran SPBE

Anggaran dan belanja SPBE disusun dengan berpedoman pada Arsitektur SPBE Pemerintah Kab. Tapin yang kemudian dituangkan dalam Peta Rencana SPBE. Anggaran dan belanja SPBE disusun dalam bentuk inventarisasi kebutuhan anggaran dan belanja SKPD. 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 SKPD.

Sekretariat Daerah dan Diskominfo, bertugas untuk memastikan kesesuaian rencana anggaran dan belanja SPBE dengan perencanaan yang tertuang dalam rencana kerja Pemerintah Kab. Tapin.

Anggaran dan belanja SPBE harus mendapatkan persetujuan oleh Tim Pengarah lalu Tim Pengarah melakukan peninjauan terhadap realisasi penggunaan anggaran dan belanja SPBE secara berkala. Hasil peninjauan digunakan sebagai pertimbangan dalam penyusunan rencana anggaran dan belanja SPBE periode selanjutnya.

D. Tata Kelola Kebijakan SPBE

Penyusunan kebijakan perlu dilakukan untuk mendukung pengembangan dan operasional SPBE. adapun 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. Rekomendasi kebijakan terkait tata kelola dan manajemen SPBE di Pemerintah Kabupaten Tapin adalah sebagai berikut:

1) Kebijakan internal arsitektur SPBE

- 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, dan Layanan SPBE)
- Menjadwalkan dan melakukan reviu secara periodik kebijakan internal Arsitektur SPBE

2) Kebijakan internal peta rencana SPBE

- 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)

- Membuat jadwal reviu dan melakukan evaluasi secara periodik pada kebijakan internal Peta Rencana SPBE.

3) **Kebijakan internal manajemen data**
   - Menetapkan kebijakan manajemen data yang mengatur seluruh rangkaian proses pengelolaan arsitektur data, data induk, data referensi, basis data, kualitas data, dan interoperabilitas data.
   - Menjadwalkan dan melakukan reviu secara periodik kebijakan internal manajemen data
4) **Kebijakan internal pembangunan aplikasi SPBE**
   - Menetapkan kebijakan internal pembangunan aplikasi SPBE yang mengatur siklus Pembangunan Aplikasi SPBE dengan unit kerja/perangkat daerah yang menjalankan fungsi pengelolaan TIK.
   - Menjadwalkan dan melakukan reviu secara periodik kebijakan internal pembangunan aplikasi SPBE
5) **Kebijakan internal layanan Pusat Data**
   - 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.
   - Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan Pusat Data.
6) **Kebijakan internal layanan jaringan intra Pemerintah**
   - Menetapkan konsep kebijakan internal terkait Layanan Jaringan Intra yang mengatur interkoneksi Layanan Jaringan Intra Pemerintah.
   - Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan jaringan intra Pemerintah.
7) **Kebijakan internal penggunaan sistem penghubung layanan Pemerintah**
   - Menetapkan konsep kebijakan internal terkait Sistem Penghubung Layanan yang mengatur penggunaan Sistem Penghubung Layanan untuk seluruh SKPD & keterhubungan dengan Sistem Penghubung Layanan Pemerintah.
   - Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan sistem penghubung layanan Pemerintah.
8) **Kebijakan internal manajemen keamanan informasi**
   - Menetapkan kebijakan internal terkait Manajemen Keamanan Informasi telah mengatur penerapan untuk seluruh SKPD.
   - Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan manajemen keamanan informasi.
9) **Kebijakan internal audit teknologi informasi dan komunikasi**
   - Menetapkan kebijakan internal terkait Audit TIK yang telah mengatur pelaksanaan seluruh Audit TIK (Audit Infrastruktur SPBE Audit Aplikasi SPBE, dan Audit Keamanan SPBE).
   - Menjadwalkan dan melakukan reviu secara periodik kebijakan internal layanan audit teknologi informasi dan komunikasi.
10) **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 SKPD.
2. Menjadwalkan dan melakukan reviu secara periodik kebijakan internal tim koordinasi SPBE.

E. Tata Kelola Proses Bisnis

Beberapa tahun terakhir telah banyak pemerintahan yang memanfaatkan solusi dengan teknologi informasi (TI) untuk mengoptimasi proses bisnis yang dimilikinya, tapi kadang solusi yang dikembangkan masih setengah-setengah. Umumnya pemerintah membangun solusi TI tersebut dalam beberapa sistem yang terpisah, bukan dalam satu kesatuan. Sistem yang dibangun biasanya terbagi berdasarkan unit kerja, atau berdasarkan proses bisnis yang ada. Hal ini tentunya dapat menimbulkan beberapa masalah ketika suatu saat terdapat proses bisnis yang membutuhkan adanya kolaborasi ataupun pertukaran informasi antar unit kerja atau antar proses bisnis untuk menyelesaikan rangkaian prosesnya tersebut, yang tentunya hal ini tidak akan dapat ditangani dengan solusi TI model seperti ini. Solusi TI seperti ini sebenarnya sudah tidak relevan lagi untuk digunakan pada dunia bisnis yang sangat dinamis seperti saat ini.

F. Tata Kelola Data

Menurut Peraturan Presiden Republik Indonesia No 39 Tahun 2019 tentang Satu Data Indonesia bahwa Satu Data Indonesia adalah kebijakan tata kelola Data pemerintah untuk menghasilkan Data yang akurat, mutakhir, terpadu, dan 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.

Kemudian 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 untuk Data selain Data Statistik dan Data Geospasial ditetapkan oleh Pembina Data, yang merupakan salah satu Instansi Daerah yang diberi kewenangan melakukan pembinaan terkait Data sebagaimana diatur dalam Peraturan Presiden No. 39 Tahun 2019 tentang Satu Data Indonesia, selain badan yang melaksanakan tugas pemerintahan di bidang kegiatan statistik atau badan yang melaksanakan tugas pemerintahan di bidang informasi geospasial.
Pemerintah Kabupaten Tapin menetapkan Standar Data untuk Data yang pemanfaatannya ditujukan untuk memenuhi kebutuhan instansi sesuai dengan tugas dan fungsinya, sepanjang ditetapkan berdasarkan Standar Data yang telah ditetapkan oleh Pembina Data.

Data yang dihasilkan oleh Produsen Data harus dilengkapi dengan Metadata, yang informasinya mengikuti struktur yang baku dan format yang baku merujuk pada bagian informasi tentang Data yang harus dicakup dalam Metadata, dan merujuk pada spesifikasi atau standar teknis dari Metadata. Struktur yang baku dan format yang baku untuk Data yang berlaku lintas Instansi Pusat dan/atau Instansi Daerah, menurut Perpres ini, ditetapkan oleh Pembina Data. Standar Metadata Kabupaten Tapin:

Elemen	Keterangan
Sumber	Nama instansi pemilik data
Author	Bidang di SKPD 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 Tapin dapat menetapkan struktur yang baku dan format yang baku untuk Data yang pemanfaatannya ditujukan untuk memenuhi kebutuhan instansi sesuai dengan tugas dan fungsinya, sepanjang ditetapkan berdasarkan struktur yang baku dan format yang baku yang telah ditetapkan oleh Pembina Data.

Data dari Produsen Data harus memenuhi kaidah Interoperabilitas Data. Oleh karenanya Data harus:

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

Untuk mengatasi permasalahan data, maka pemerintah memiliki panduan dasar yang merujuk pada Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia yang dapat diikuti untuk pemerintah Kabupaten Tapin sebagai berikut.

1. **Forum Satu Data Indonesia**
   Mengacu pada Perpres 39 Tahun 2019 tentang Satu Data Indonesia Pasal 10 Ayat (3) huruf a. Yaitu Forum Satu Data Indonesia akan menyepakati:
   - Kode Referensi dan/atau Data Induk; dan

- Instansi Daerah yang unit kerjanya menjadi Produsen Data atas Kode Referensi dan/atau Data Induk tersebut.

2. **Penyelenggara Satu Data Indonesia**

   Penyelenggara Satu Data Indonesia dilaksanakan oleh:
   - Dewan Pengarah;
   - Pembina Data;
   - Produsen Data

3. **Dewan Pengarah Satu Data Indonesia**

   Tugas Dewan Pengarah Satu Data Indonesia:
   - Mengkoordinasikan dan menetapkan kebijakan terkait Satu Data Indonesia;
   - Mengkoordinasikan pelaksanaan Satu Data Indonesia;
   - Melakukan pemantauan dan evaluasi pelaksanaan Satu Data Indonesia;
   - Mengkoordinasikan penyelesaian permasalahan dan hambatan pelaksanaan Satu Data Indonesia.

4. **Komposisi Dewan Pengarah Satu Data Indonesia**

   Dewan Pengarah Satu Data Indonesia terdiri dari:
   - Ketua merangkap anggota, yaitu Sekda;
   - Anggota, terdiri atas Kepala Dinas dari masing-masing SKPD.

5. **Pembina Data Tingkat Daerah**

   Tugas Pembina Data Tingkat Daerah:
   - Menetapkan Standar Data yang berlaku lintas Instansi Daerah;
   - Menetapkan struktur yang baku dan format yang baku dari Metadata yang berlaku lintas Instansi Daerah;
   - Memberikan rekomendasi dalam proses perencanaan pengumpulan Data;
   - Melakukan pemeriksaan ulang terhadap Data Prioritas; dan
   - Melakukan pembinaan penyelenggaraan Satu Data Indonesia sesuai dengan ketentuan peraturan perundang-undangan.

6. **Produsen Data**

   Tugas produsen data tingkat Daerah:
   - Mengumpulkan, memeriksa kesesuaian Data, dan mengelola Data yang disampaikan oleh Produsen Data sesuai dengan prinsip Satu Data Indonesia;
   - Menyebarluaskan Data, Metadata, Kode Referensi, dan Data Induk di Portal Satu Data Indonesia; dan
   - Membantu Pembina Data dalam membina Produsen Data.
   - Memberikan masukan kepada Pembina Data dan Kepala Dinas mengenai Standar Data, Metadata, dan Interoperabilitas Data;
   - Menghasilkan Data sesuai dengan prinsip Satu Data Indonesia; dan
   - Menyampaikan Data dan Metadata kepada produsen data.

Produsen Data melakukan pengumpulan Data sesuai dengan:

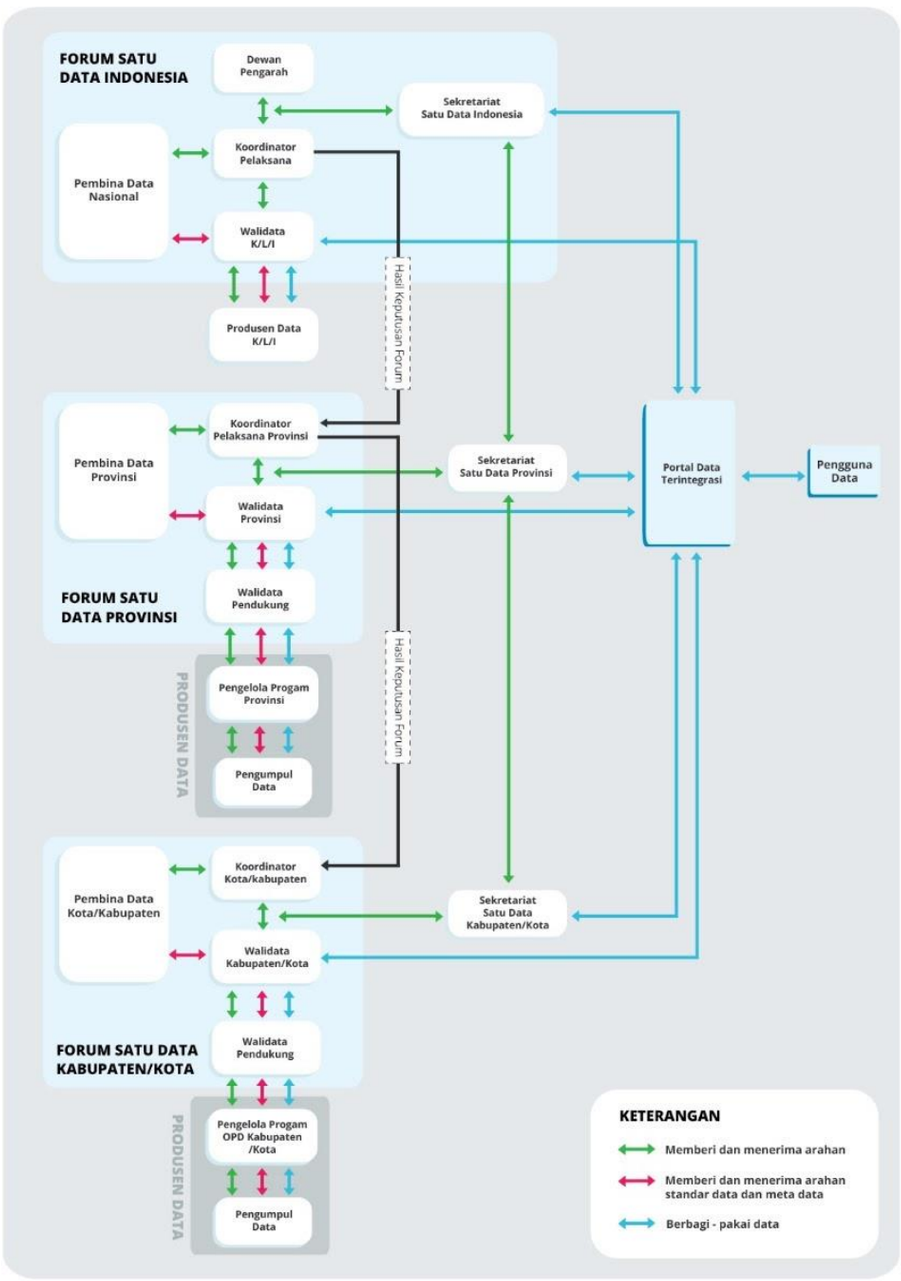
- Standar Data;
- Daftar data yang telah ditentukan dalam Forum Satu Data Indonesia; dan
- Jadwal pemutakhiran Data atau rilis Data, dan selanjutnya disampaikan kepada produsen data.

7. Pelaksana Penyelenggaraan Satu Data Indonesia

Pelaksana Penyelenggaraan Satu Data Indonesia dilakukan oleh:

- Pembina Data tingkat daerah;
- Produsen Data tingkat daerah;
- Produsen Data pendukung; dan
- 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 1.1.3. Alur Koordinasi Aktor Forum Satu Data

G. Tata Kelola Layanan

Dalam SPBE terdapat Layanan yang perlu ditransformasi digitalkan untuk mendukung visi misi dan tujuan SPBE. Layanan SPBE terbagi menjadi 2 kategori yaitu Layanan Administrasi Pemerintahan dan Layanan Publik. Berikut ini merupakan gambaran mengenai 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 1.1.4. Layanan SPBE

Berdasarkan hasil assessment mengenai kondisi Eksisting layanan SPBE di Kab. Tapin, seluruh layanan SPBE yang ada telah didukung oleh pemanfaatan sistem informasi, hanya saja kedepan perlu adanya integrasi antar sistem di Kab. Tapin, baik integrasi dengan sistem internal daerah maupun dengan sistem kementerian pusat.

H. Tata Kelola Aplikasi

Dengan cukup banyaknya sistem yang akan dibangun, diperlukan sebuah metode untuk menentukan prioritas sistem yang akan diakomodasi terlebih dahulu.

Pemilihan prioritas menggunakan *matrix impact-implementation*. Cara membaca tabel prioritas yaitu dimulai dari kanan atas (sistem yang mudah diimplementasikan, dan memiliki *impact* tinggi) ke bawah, dilanjutkan dengan sistem dengan implementasi dan *impact* sedang menuju ke bagian *impact* tinggi. Aplikasi-aplikasi yang akan dibangun, baik usulan dari unit kerja, maupun inisiatif dari Diskominfo dipetakan dalam matriks sebagai berikut:

Gambar 1.1.5. *Matrix Easy Implementation*

Pengembangan sistem informasi (aplikasi) dikategorikan mudah (*easy*) jika:

- Aplikasi telah ada/pernah digunakan di SKPD lain sebelumnya,
- Biaya pengembangan aplikasi sama dengan atau lebih kecil dari rata-rata biaya pengembangan aplikasi,
- *Platform* aplikasi relevan dengan kualifikasi SDM TIK di Dinas Kominfo/SKPD,
- Proses kerja aplikasi tidak terlalu kompleks.

Sistem informasi (aplikasi) dikategorikan memiliki *impact* yang besar (*high impact*) jika:

- Aplikasi yang langsung dapat dirasakan manfaatnya bagi masyarakat (G2C),
- Aplikasi diusulkan oleh lebih dari satu SKPD,
- Aplikasi dapat digunakan oleh lebih dari satu SKPD,
- Aplikasi pesanan langsung dari pimpinan (*strategic decision maker*).

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

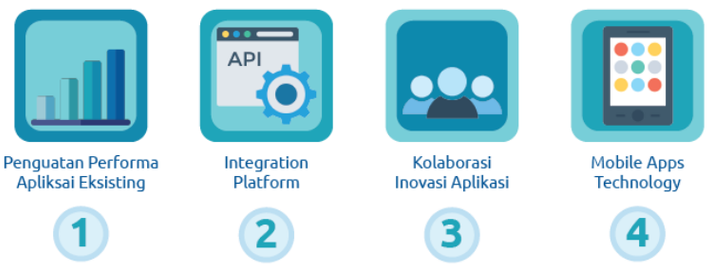
Gambar 1.1.6. Bagan Strategi Prioritasisasi Pengembangan Aplikasi

Aplikasi yang sifatnya mendukung pelayanan publik dan yang menyentuh jajaran eksekutif/pimpinan akan didahulukan. Hal ini dimaksudkan agar masyarakat dan pimpinan sebagai pemangku kepentingan utama pemerintahan dapat memberikan dukungan penuh terhadap pengembangan aplikasi secara keseluruhan. Kemudian dilanjutkan dengan aplikasi-aplikasi yang ditujukan untuk mengefisiensikan kolaborasi antar unit kerja. Hal ini dimaksudkan

agar proses secara internal dapat dioptimalkan sehingga proses layanan kepada masyarakat dan pelaporan kepada eksekutif dapat menjadi lebih efisien.

Terakhir aplikasi-aplikasi yang sifatnya untuk kalangan bisnis dan investor dibangun manakala secara internal institusi sudah siap, dan dukungan dari masyarakat dan pimpinan Pemda telah memberikan dukungan secara penuh terhadap pengembangan Layanan SPBE.

Pengembangan SI dapat diinisiasi melalui penyusunan panduan integrasi lintas satuan kerja; pengembangan dan pemeliharaan *platform* integrasi aplikasi (*web services*); pengembangan dan pemeliharaan *data warehouse* dan sistem *dashboard*; pengembangan dan pemeliharaan aplikasi (18 aplikasi); *upgrade* eksisting aplikasi (audit dan *tuning* performa) dengan fokus utama pengembangan aplikasi fungsi yudisial (manajemen perkara dan manajemen pengadilan), selanjutnya pengembangan aplikasi fungsi non yudisial (khususnya yang sudah dikembangkan dari inisiatif satuan kerja daerah); dan pengembangan dan pemeliharaan sistem informasi (aplikasi) berdasarkan kesiapan bisnis proses.



Gambar 1.1.7. Inisiatif Pengembangan Aplikasi

Sebagai langkah untuk mengembangkan dan mengintegrasikan aplikasi, maka 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 satuan kerja memiliki rujukan untuk interoperabilitas sistem maupun data.
3. Kolaborasi bersama dengan inisiatif pengembangan aplikasi di satuan kerja agar bisa dimanfaatkan secara level nasional.
4. Pengembangan *mobile applications* untuk menyajikan layanan peradilan yang transparan dan akuntabel bagi masyarakat.

a. Prinsip Pengembangan Sistem Informasi

Prinsip-prinsip pengembangan sistem informasi di Pemerintah Kabupaten Tapin harus meliputi aspek: *Sustainable, Mobile, Agile, Reliability, Transparency* (SMART).

1. *Sustainability*

   Sistem informasi yang dikembangkan dapat ditingkatkan secara terus menerus (*continuous improvement*) dan berkembang menyesuaikan kebutuhan. Dalam hal pengembangan sistem konsep ini dikenal dengan istilah *System Development Life Cycle* (SDLC).
2. *Mobile*

Sistem informasi yang dikembangkan di Pemerintah Kabupaten Tapin harus dapat meningkatkan fleksibilitas pemanfaatan teknologi dan kemudahan bagi masyarakat.

3. *Agile*

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

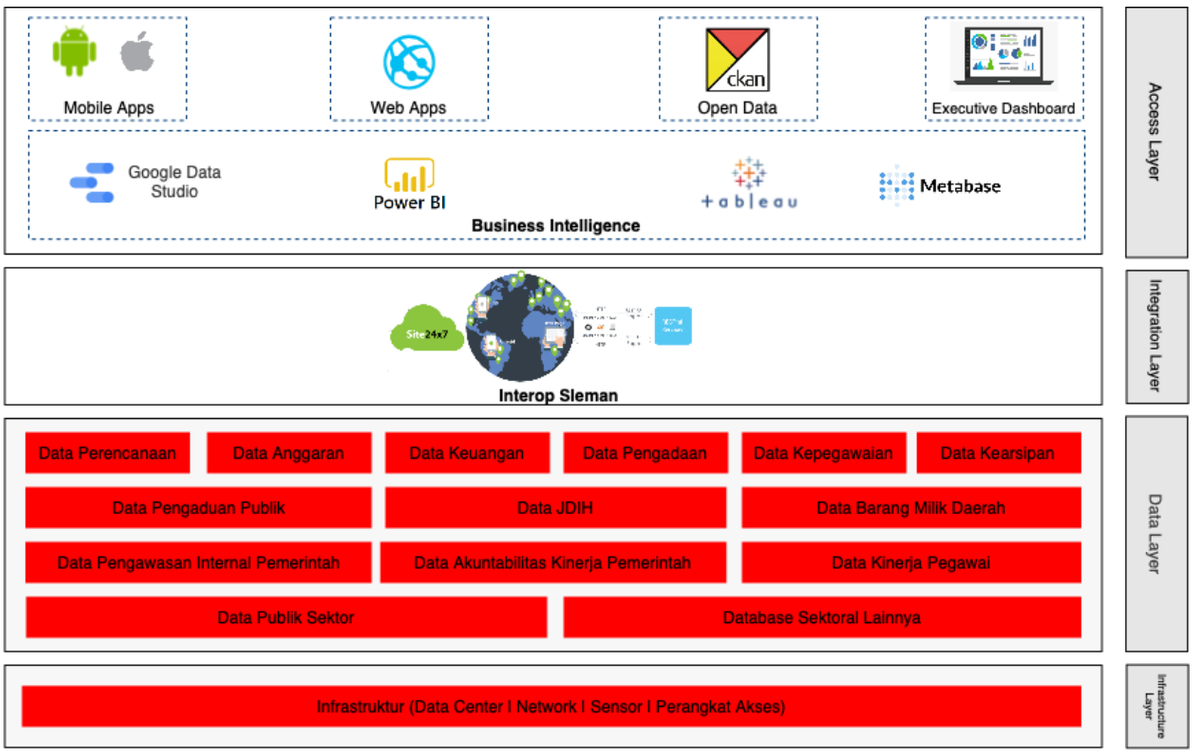
4. *Reliability*

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

5. *Transparency*

   Sistem informasi yang dikembangkan harus dapat mendukung budaya transparansi di Pemerintah Kabupaten Tapin agar tercipta pelayanan prima kepada masyarakat.

b. Desain Arsitektur Sistem Informasi



Gambar 1.1.8. Desain Arsitektur Sistem Informasi

Arsitektur Sistem Informasi dijabarkan sebagai berikut:

- *Access Layer*

  Pada bagian ini akan terdapat aplikasi-aplikasi yang akan mendukung perangkat daerah dalam proses operasional utama di unit kerjanya. Masing-masing SKPD akan memiliki aplikasi dengan alur proses (proses bisnis) yang beragam sesuai dengan tugas dan fungsi SKPD tersebut. Selain itu juga SKPD 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*
  Pada 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 Tapin yaitu MySQL.
- *Layer* *Arsitektur*
  Pada bagian ini terdapat perangkat jaringan, *server dan* CCTV guna mendukung operasional aplikasi 24x7 jam..

c. Integrasi Sistem

Permasalahan integrasi merupakan kendala yang cukup kompleks dalam implementasi SPBE. Kurang adanya integrasi antar sistem menyebabkan kurang efisiennya operasional pemerintahan. Untuk itu integrasi sistem informasi yang ada perlu disesuaikan dengan Blok/Sub Blok fungsi yang telah didefinisikan sesuai dengan kebutuhan pengembangan sistem informasi. Berikut ini modul integrasi sistem berdasarkan modul-modul Blok/Sub Blok Fungsi yang telah didefinisikan sesuai dengan kebutuhan pengembangan layanan SPBE:

Gambar 1.1.9. Data Urusan Pemerintahan

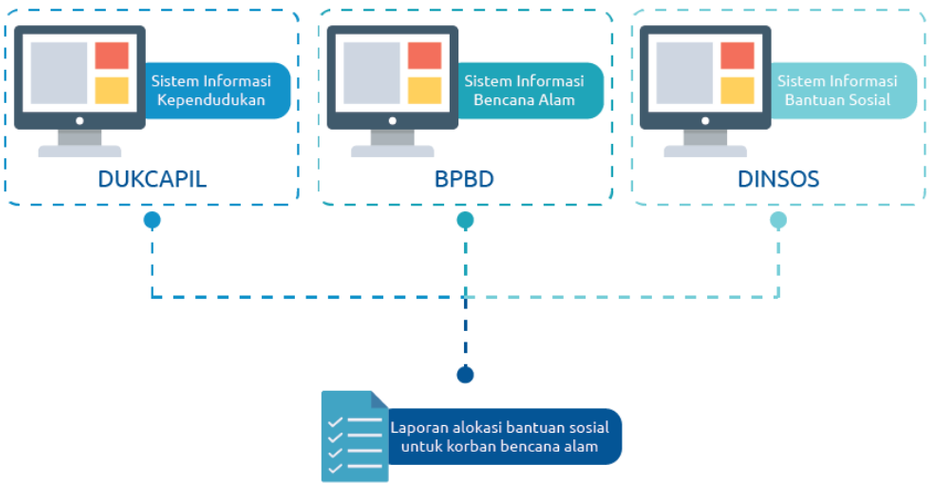
Sistem informasi yang dikembangkan dapat diintegrasikan dengan menggunakan *Application Programming Interface* (API), API adalah kumpulan fungsi-fungsi untuk menggantikan bahasa yang digunakan dalam *system call* dengan bahasa yang terstruktur. API menyediakan fungsi untuk menghubungkan koneksi antar sistem. Secara umum API mampu menerima respon data dalam format JSON dan XML.

d. Integrasi Data

Kebijakan publik, pelayanan publik, penegakan hukum, pengawasan kinerja pemerintah, hingga peluang bisnis, semuanya membutuhkan data yang kredibel. Faktanya di pemerintahan, data masih sering tidak dikelola secara serius. Masih banyak ditemukan kasus di mana terdapat data yang tidak hanya memiliki beragam format, namun sering juga saling kontradiktif di antara satu dengan yang lainnya sehingga memperlambat proses pelaporan dan pengambilan keputusan.

Gambar 1.1.10. Fakta Kondisi Data Pemerintahan Saat ini

Berdasarkan hal ini data yang ada pada Pemerintah Daerah perlu diinventarisir, dipetakan dan diintegrasikan. Inisiatif Satu Data, atau yang biasa disebut Satu Data Indonesia, merupakan salah satu inisiatif pemerintah Indonesia yang mencoba untuk membenahi permasalahan dalam penyelenggaraan dan pengelolaan data pemerintah tersebut. Pengembangan inisiatif ini juga diinstruksikan melalui Perpres 39 Tahun 2019. Harapannya dengan mengimplementasikan inisiatif ini data dapat terkumpul dengan baik dan laporan ke eksekutif bisa dilakukan secara cepat dan representatif dalam bentuk *dashboard*. Berikut ini ilustrasi dari implementasi integrasi sistem:



Gambar 1.1.11. Ilustrasi Model Integrasi Sistem

e. Pilihan Teknologi

1) *Scripting Language* (PHP, HTML-5, CSS, Javascript, Python, Java, Kotlin, Flutter)

Di masa yang akan datang, teknologi *web* tentu akan semakin memberikan kemudahan bagi para pengguna sistem informasi karena ini adalah salah satu model yang sudah menghilangkan kendala lokasi dan posisi seseorang dalam mengakses sebuah informasi.

Sistem informasi di lingkungan Pemerintah daerah, tentunya akan terus diarahkan dan diproyeksikan menjadi sebuah sistem yang mampu mendukung bisnis proses dasar dan pendukung yang ada. Pegawai pemerintahan tidak lagi terkendala dengan lokasi mereka, dan jarak yang berjauhan.

Teknologi *scripting* PHP, HTML5, CSS dan Javascript akan mampu menjawab tantangan kompleksitas bisnis proses dan penyajian informasi yang dituntut untuk semakin tinggi oleh para pengguna. Jadi sebuah aplikasi yang sangat men-*support* dan mendukung layanan operasional di *frontend* maupun *backend* akan sangat mutlak dibutuhkan. Cepat, akurat, dan menghasilkan *output* yang sesuai adalah harapan dari semua pengguna yang dilayani oleh sistem informasi.

Teknologi *scripting* PHP yang dikombinasikan dengan HTML-5, serta Javascript akan menghasilkan sebuah aplikasi berbasis *web* yang mampu dibuka dan disajikan dalam berbagai ukuran layar, hal inilah kemudian yang sering disebut dengan *web* responsif. Pengguna aplikasi tidak lagi terkendala dengan penyajian aplikasi yang "berantakan" ketika diakses melalui ponselnya, tetapi akan otomatis menyesuaikan dan nyaman (*eye-catching*).

Gambar 1.1.12. *Scripting Language*

Python adalah bahasa pemrograman interpretatif multiguna. Python lebih menekankan pada keterbacaan kode agar lebih mudah untuk memahami sintaks. Bahasa Python mendukung hampir semua sistem operasi, termasuk sistem operasi Linux. Bahasa pemrograman direkomendasikan untuk melakukan analisis data (*data mining*) karena menyediakan fungsi-fungsi untuk melakukan manipulasi data.

Java adalah bahasa pemrograman *multi platform* dan *multi device* yang berbasis kelas, berorientasi objek, dan dirancang untuk memiliki dependensi implementasi sesedikit mungkin. Bahasa pemrograman ini direkomendasikan untuk membangun sistem yang kompleks berbasis *desktop* dan *mobile*.

Kotlin merupakan Bahasa Pemrograman modern yang bersifat *statically-typed* yang dapat dijalankan di atas *platform Java Virtual Machine* (JVM). Kotlin juga dapat di kompilasi (*compile*) ke dalam bentuk JavaScript. Tools yang mendukung bahasa pemrograman ini yaitu Android Studio. Bahasa pemrograman ini direkomendasikan untuk mengembangkan aplikasi berbasis Android *mobile*.

Flutter adalah sebuah *framework* aplikasi mobil sumber terbuka yang diciptakan oleh Google. Flutter digunakan dalam pengembangan aplikasi untuk sistem operasi Android dan iOS. Saat ini Flutter masih dalam tahap pengembangan sehingga untuk di beberapa perangkat *smartphone* masih perlu tambahan *plugin* agar aplikasi bisa berjalan dengan baik.

2) *Library output dokumen (PDF, CSV, XLS, RTF)*

Variasi *output* dari sistem informasi dalam bentuk file PDF, XLS, CSV, ataupun RTF sangat mutlak dibutuhkan. Hal ini untuk mengantisipasi berbagai kebutuhan *formatting* oleh pihak eksternal.

Cukup banyak di internet berbagai *library* yang semakin memanjakan pengguna dalam menghasilkan sebuah *output* yang bervariasi. Semua sistem informasi yang dikembangkan di lingkungan Pemerintah Daerah mutlak dituntut untuk bisa menghasilkan keluaran yang bervariasi, tidak terbatas pada PDF, XLS, CSV dan RTF.

3) *Database Engine (Mysql, Oracle, PostgreSQL, Maria db)*

Database Engine dapat merupakan komponen penting dalam sebuah sistem. Di sinilah seluruh data dari aplikasi akan disimpan. Dewasa ini telah banyak jenis *Relational Database Management System* (RDBMS) yang dapat dipilih untuk pembuatan aplikasi, dua yang cukup populer digunakan adalah MySQL dan Oracle. Setiap *database engine* tersebut memiliki kelebihan dan kekurangan. Harus pandai menempatkan posisi *database engine* dalam mendukung pengembangan aplikasi di lingkungan Pemerintah Daerah.

Sangat disarankan segala pengembangan aplikasi operasional tetap menggunakan RDBMS yang *open source*, dengan pertimbangan ringan, dan mudah dalam proses instalasi serta implementasinya sehingga dapat berhemat dalam pengembangan (karena tidak perlu membayar lisensi) sehingga MySQL adalah jawabannya. *Engine* ini sudah sangat umum digunakan untuk frekuensi trafik data yang sampai level menengah (ribuan data per hari). Namun demikian jika trafik data sudah cukup tinggi penggunaan *database open source* sudah mulai kurang tepat. Penggunaan Oracle kemudian menjadi jawaban untuk pengembangan *data warehouse* dan pengelolaan data yang sangat besar sehingga kemampuan *engine* ini bisa maksimal penggunaannya, tidak hanya sebatas digunakan sebagai *storage*. Keunggulan dari Oracle adalah *database* berkelas *enterprise* dan komputasi *query* yang cepat sehingga dapat melakukan *processing* data yang kompleks (*Big Data*), *database* dapat dikembalikan ke kondisi *checkpoint*

(*rollback*) sehingga proses penanganan insiden (*incident handling*) menjadi lebih mudah. Untuk memanfaatkan Oracle harus berlangganan lisensi dengan biaya yang relatif mahal.

Gambar 1.1.13. *Database Engine*

PostgreSQL adalah sebuah sistem basis data yang disebarluaskan secara bebas menurut perjanjian lisensi BSD, sehingga tidak perlu mengeluarkan biaya. Peranti lunak ini merupakan salah satu basis data yang paling banyak digunakan saat ini, selain MySQL dan Oracle. PostgreSQL menyediakan fitur yang berguna untuk replikasi basis data. Keunggulan dari PostgreSQL adalah *database* berkelas *enterprise* dan database dapat dikembalikan ke kondisi *checkpoint* (*rollback*) sehingga proses penanganan insiden (*incident handling*) menjadi lebih mudah. PostgreSQL mampu menyimpan data sebesar 16 terabyte.

MariaDB adalah sistem manajemen *database* relasional yang dikembangkan dari MySQL. MariaDB dikembangkan oleh komunitas pengembang yang sebelumnya berkontribusi untuk *database* MySQL. Keunggulan dari MariaDB adalah sistem manajemen *database* yang *open source*, memiliki pengaturan yang mudah, dan gratis, meskipun begitu MariaDB memiliki performa yang bagus dan dapat meng-*import* data dari MySQL.

4) *SSO: Single Sign On (LDAP = Lightweight Directory Access Protocol)*

Guna mempermudah pengguna dalam mengakses banyak aplikasi yang tergabung dalam sebuah solusi sistem terintegrasi, diperlukan implementasi dari konsep *single sign on*. Konsep ini memungkinkan pengguna untuk *login* hanya pada satu aplikasi tertentu dan selanjutnya secara otomatis ter-*login* pada aplikasi lain, tentu dengan syarat, pengguna tersebut memang memiliki hak akses terhadap aplikasinya.

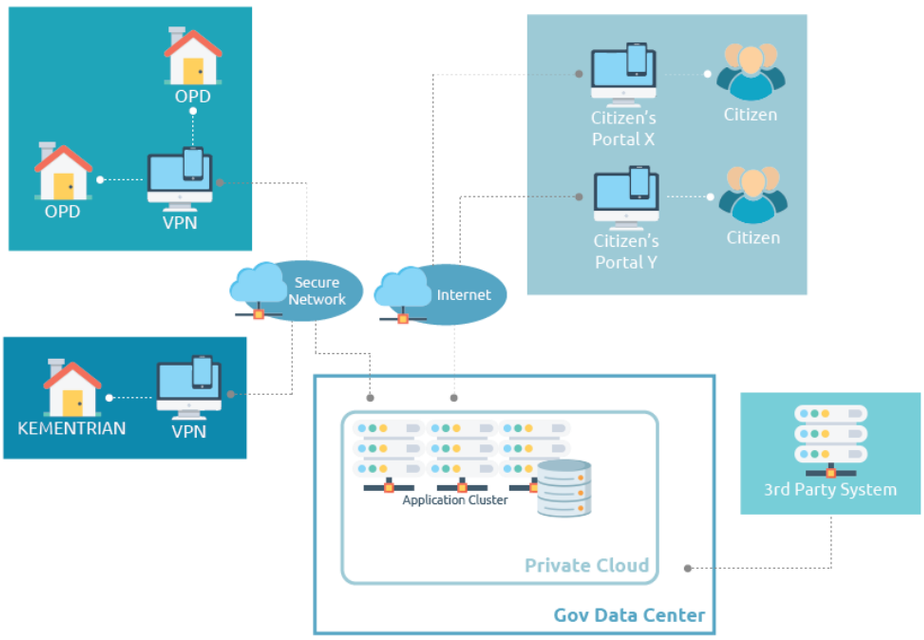
Dalam penerapan konsep *single sign on* diperlukan sebuah *protokol* untuk menyimpan *account* pengguna beserta hak aksesnya yang lintas aplikasi. Nantinya setiap aplikasi yang terhubung pada *server* tersebut akan selalu merujuk pada *account* pengguna yang tunggal. Protocol tersebut dinamai *Lightweight Directory Access Protocol (LDAP)*.

Institusi Pemerintahan dengan jumlah solusi sistem informasi yang banyak sudah selayaknya menggunakan teknologi ini di masa yang akan datang.

5) *Integrasi Data dengan Platform Interoperabilitas*

- *WSO2*

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 1.1.14 Arsitektur Bisnis dari Sebuah Sistem Layanan Publik

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

I. 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. Di dalam Pusat Data terdapat beberapa komponen antara lain *server*, *storage*, perangkat pendukung pusat data, dan teknologi yang digunakan untuk pengembangan aplikasi.

Penggunaan Jaringan Intra pemerintah bertujuan untuk menjaga keamanan dalam melakukan pengiriman data dan informasi antar Instansi Pusat dan/atau Pemerintah Daerah.

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

A. Pusat Data

Gambar 1.1.15. SNI No 8799-1:2019 tentang Panduan Spesifikasi Teknis Pusat Data

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

a. Spesifikasi gedung

Lokasi gedung pusat data. Informasi lokasi rawan bencana dapat mengacu pada Katalog 'Gempabumi Signifikan dan Merusak 1821 – 2018' dari BMKG dengan alamat https://cdn.bmkg.go.id/Web/Katalog-Gempabumi-Signifikan-dan-Merusak-1821-2018.pdf dan dokumen Risiko Bencana Indonesia (RBI) dari BNPB dengan alamat https://bnpb.go.id/uploads/24/buku-rbi-1.pdf .

i. Ketahanan gempa
ii. Ketahanan beban gempa
iii. Pembagian ruangan
iv. Ketahanan material gedung
v. Sistem monitoring gedung

b. Spesifikasi sistem kelistrikan

i. Catu daya listrik
ii. Sistem kelistrikan berkesinambungan
iii. Persediaan bahan bakar
iv. Uninterruptible Power Supply (UPS)
v. Analisis sistem listrik
vi. Konstruksi panel listrik
vii. Jalur kabel listrik
viii. Pembumian
ix. Efisiensi pemakaian listrik pada pusat data (power usage effectiveness)

c. Spesifikasi sistem pendinginan
d. Spesifikasi sistem jaringan data
e. Spesifikasi sistem pemadam kebakaran
f. Spesifikasi sistem monitoring lingkungan pusat data
g. Spesifikasi sistem keamanan akses fisik

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

Gambar 1.1.16 SNI No 8799-1:2019 tentang Panduan Manajemen Pusat Data

a. Perencanaan
   - Analisis kebutuhan
   - Manajemen risiko dan kesesuaian

b. Operasional
   - Organisasi penyelenggara pusat data
   - Sistem manajemen layanan operasional pusat data
   - Infrastruktur

c. Manajemen layanan
   - Sistem manajemen layanan tingkat lanjut (STML)
   - Manajemen keselamatan
   - Manajemen keamanan
   - Manajemen proyek

d. Manajemen SDM
   - Pengelolaan kompetensi
   - Pelatihan
   - Manajemen kinerja

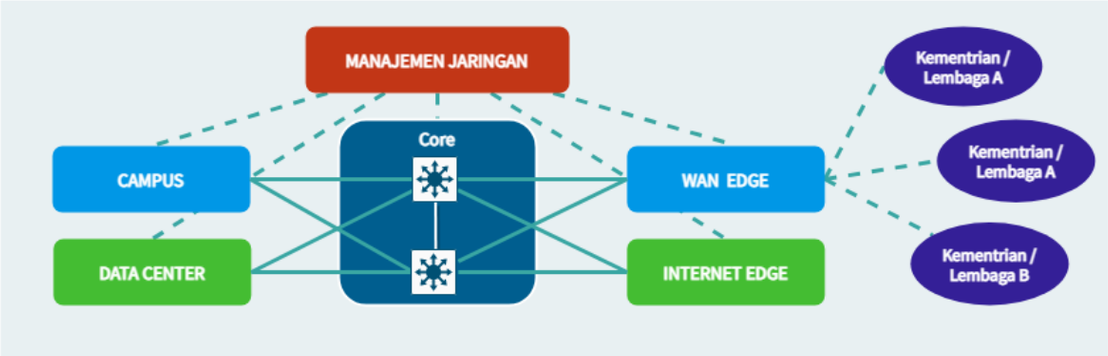
e. *Monitoring*, pelaporan dan pengendalian

f. Manajemen keberlangsungan
   - Manajemen keberlangsungan kegiatan
   - Manajemen keberlangsungan lingkungan

3. SNI No 8799-3:2019 beserta amandemennya tentang Panduan Audit Pusat Data
   a. Program audit
   b. Kegiatan audit
   c. Penyiapan, pengesahan dan penyampaian laporan audit
   d. Kompetensi auditor

B. Jaringan Intra Pemerintah

Jaringan intra pemerintah menghubungkan jaringan Diskominfo Kabupaten Tapin dengan kementerian atau lembaga lainnya.

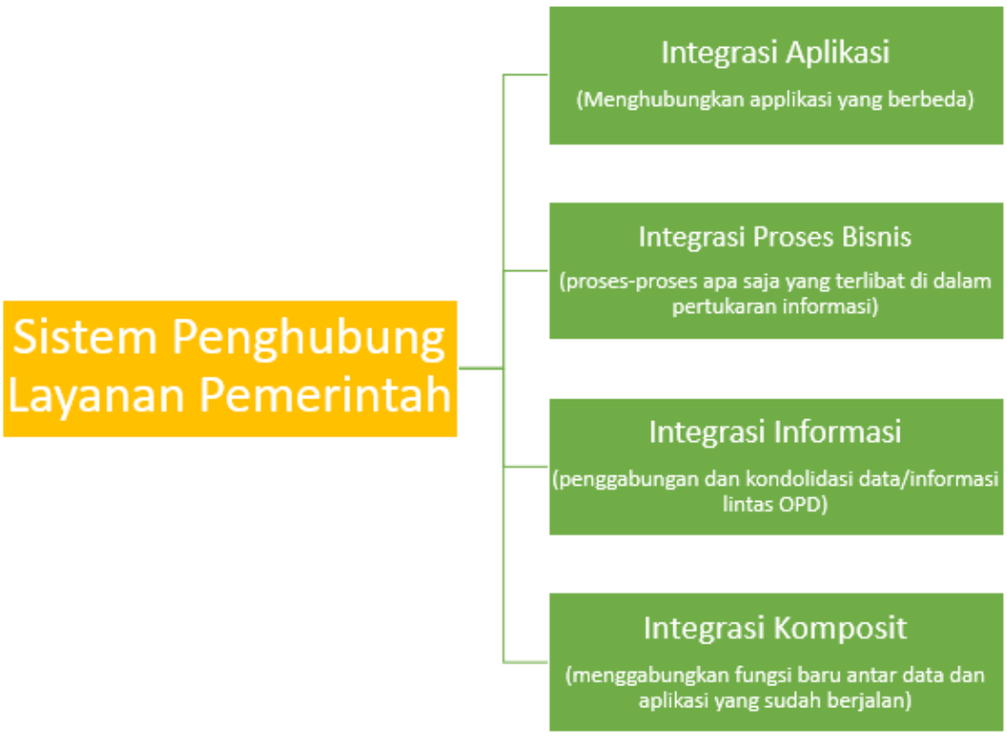


Gambar 1.1.17. Arsitektur Jaringan Intra Diskominfo Kabupaten Tapin

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

C. Sistem Penghubung Layanan Pemerintah

Sistem penghubung layanan pemerintah adalah integrasi kolaborasi.

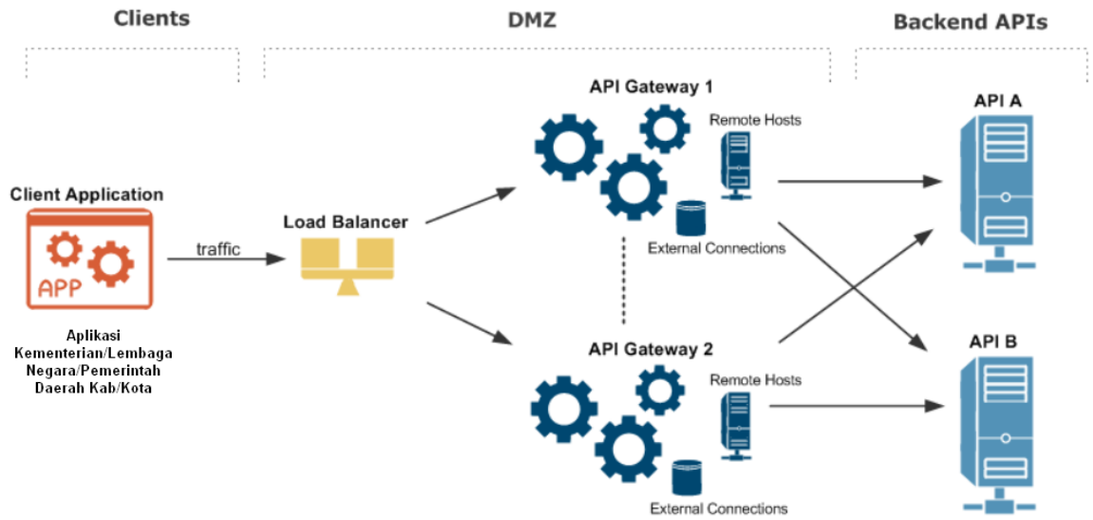


Gambar Gambar 1.1.18. Sistem Penghubung Layanan Pemerintah

1) *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 bisa digunakan untuk berkomunikasi dengan berbagai bahasa pemrograman.



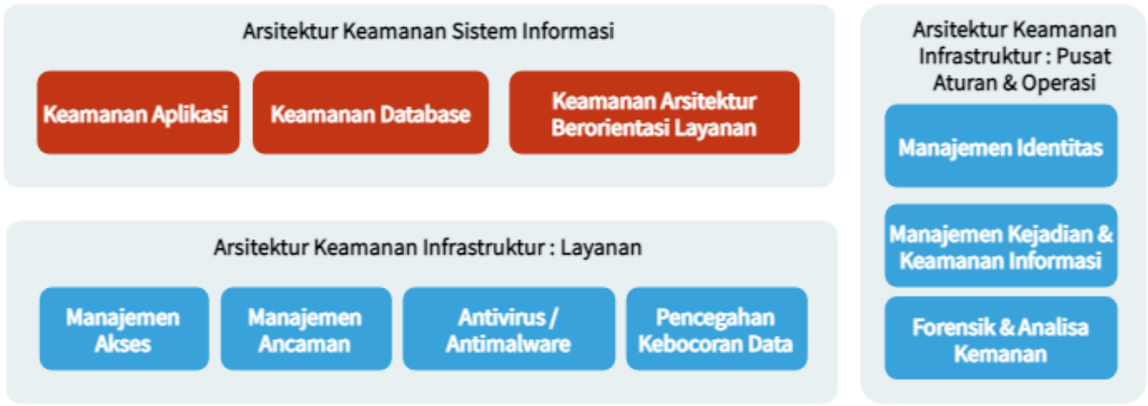
Gambar 1.1.19. Arsitektur API Gateway dengan konfigurasi *High Availability*

Berikut ini adalah penjelasan dari gambar Arsitektur API Gateway dengan konfigurasi High Availability (HA):

- Aplikasi klien eksternal membuat panggilan masuk yang mengirimkan lalu lintas bisnis melalui protokol pengangkutan pesan tertentu (misalnya, HTTP, JMS, atau FTP) ke penyeimbang beban.
- Penyeimbang beban pihak ketiga standar melakukan pemeriksaan kesehatan pada setiap instance API Gateway, dan mendistribusikan beban pesan ke port mendengarkan di setiap instance API Gateway (default-nya adalah 8080).
- Setiap instance API Gateway memiliki Koneksi Eksternal ke sistem pihak ketiga. Misalnya, ini termasuk database seperti Oracle dan MySQL, dan *Authentication Repositories seperti CA SiteMinder, Oracle Access Manager, server Local Directory Access Protocol (LDAP)*, dan sebagainya.
- *Caching* direplikasi antara setiap instance API Gateway menggunakan sistem *caching* terdistribusi berdasarkan Ehcache.
- Setiap instance API Gateway memiliki antarmuka Host Jarak Jauh yang menentukan koneksi keluar ke sistem API *backend*, dan yang dapat menyeimbangkan beban pesan berdasarkan prioritas yang ditentukan untuk Host Jarak Jauh.
- Setiap instans API Gateway berisi database Apache Cassandra yang disematkan yang digunakan oleh fitur-fitur tertentu untuk penyimpanan data persisten, dan yang memiliki kemampuan HA-nya sendiri.
- Setiap instans API Gateway berisi sistem pesan Apache ActiveMQ tertanam, yang dapat dikonfigurasi untuk HA dalam sistem file bersama.
- Setiap API backend juga direplikasi untuk memastikan tidak ada satu titik kegagalan di tingkat server.

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

J. Tata Kelola Keamanan



Gambar 1.1.20. Keamanan SPBE

Keamanan SPBE terdiri atas:

a. 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. Dalam rangka memastikan 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.

b. 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.

c. Arsitektur Keamanan Infrastruktur: Pusat Aturan dan Operasi

   Terdiri dari manajemen identitas, manajemen kejadian & keamanan informasi, dan forensik & analisa keamanan.

Pelaksanaan terhadap Keamanan SPBE mencakup:

- Penjaminan kerahasiaan;
- Penjaminan keutuhan;
- Penjaminan ketersediaan;

- 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.

1.2. Manajemen SPBE

Dalam implementasi SPBE perlu adanya manajemen yang mengakomodir proses operasional SPBE. Mengacu dari Perpres 95/2018 dimana menyebutkan manajemen SPBE memiliki beberapa lingkup yang diuraikan sebagai berikut:

Tabel 1.2.1. Lingkup Manajemen SPBE

#	Lingkup	Referensi	Kegiatan	Pelaksana
a.	Manajemen Risiko	PermenpanRB 05/2020, ISO 31000, 27005	1. Komunikasi dan konsultasi 2. Penetapan konteks risiko SPBE 3. Penilaian risiko SPBE 4. Penanganan risiko SPBE 5. Pemantauan dan evaluasi	Inspektorat (Koordinator) & Seluruh SKPD (Anggota) dalam Forum Manajemen Risiko
b.	Manajemen Keamanan Informasi	ISO 27001, Indeks KAMI	1. Penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan terhadap data dan informasi. 2. Penjaminan ketersediaan infrastruktur 3. Penjaminan keutuhan, ketersediaan dan keaslian aplikasi.	Diskominfo (Koordinator) & Seluruh SKPD (Anggota)
c.	Manajemen Data	Perpres 39/2019, Permen PPN 16/2020, SNI 8799:2019, ISO 11179	1. Menentukan peran dalam manajemen data daerah 2. Membangun aplikasi/sistem/layanan 3. Membuat dan menjalankan Kebijakan dan SOP manajemen data 4. Memiliki dokumen arsitektur data dan informasi	Bappeda (Koordinator) & Seluruh SKPD (Anggota) dalam Forum Satu Data
d.	Manajemen Aset TIK	ISO 55001	1. Manajemen dan perencanaan 2. Identifikasi konfigurasi 3. Kontrol konfigurasi 4. Akuntansi dan pelaporan status aset 5. Verifikasi dan audit	BKAD (Koordinator) & Seluruh SKPD (Anggota)
e.	Manajemen SDM	PermenPANRB 38/2017, SFIA Framework, ISO 30400	1. Menentukan arah kebijakan dan strategi SDM SPBE 2. Penentuan peta rencana strategis SPBE	BKPSDM (Koordinator) & Seluruh SKPD (Anggota)

f.	Manajemen Pengetahuan	ISO 30401	1. Merencanakan Implementasi Manajemen Pengetahuan 2. Mengimplementasikan manajemen pengetahuan 3. Evaluasi dan penyempurnaan	BKPSDM (Koordinator) & Seluruh SKPD (Anggota)
g.	Manajemen Perubahan	Change Management (ITIL) COBIT 2019	1. Merumuskan rencana perubahan 2. Mengelola / melaksanakan perubahan 3. Memperkuat hasil perubahan	Diskominfo (Koordinator) & Seluruh SKPD (Anggota)
h.	Manajemen Layanan	ITIL	1. Pelayanan pengguna SPBE, meliputi pengelolaan keluhan, gangguan, masalah, permintaan, dan perubahan Layanan SPBE dari penggu 2. Pengoperasian layanan, meliputi pendayagunaan dan pemeliharaan infrastruktur SPBE dan aplikasi SPBE 3. Pengelolaan aplikasi SPBE, meliputi pembangunan dan pengembangan aplikasi yang berpedoman pada metodologi pembangunan dan pengembangan aplikasi	Diskominfo (Koordinator) & Seluruh SKPD (Anggota)

A. Manajemen Risiko SPBE

Gambar 1.2.1. Manajemen Risiko SPBE (sumber: paparan KemenpanRB)

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.
3. keputusan melalui penyajian informasi Risiko SPBE yang memadai di Pemerintah Daerah dalam penerapan SPBE.
4. Meningkatkan optimalisasi pemanfaatan sumber daya SPBE di Instansi Pemerintah Daerah dalam penerapan SPBE.
5. Meningkatkan kepatuhan kepada peraturan dalam penerapan SPBE.
6. Menciptakan budaya sadar Risiko SPBE bagi pegawai ASN di lingkungan Pemerintah Daerah dalam penerapan SPBE.

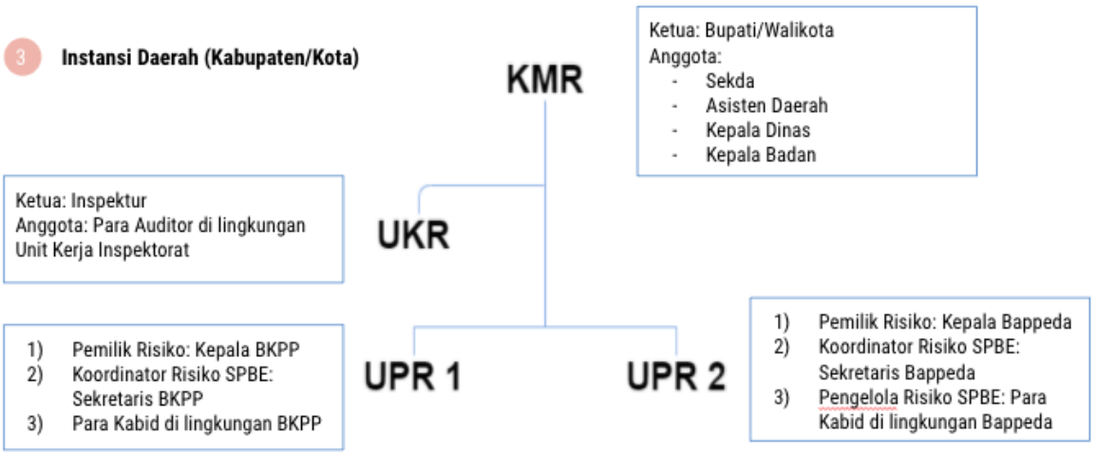
Manfaat dari penerapan Manajemen Risiko SPBE dalam penerapan SPBE adalah:

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, Pemkab. Tapin perlu menyusun struktur manajemen risiko SPBE sebagaimana yang telah tertuang dalam PermenpanRB No. 05/2020 dan dijelaskan sebagai berikut:

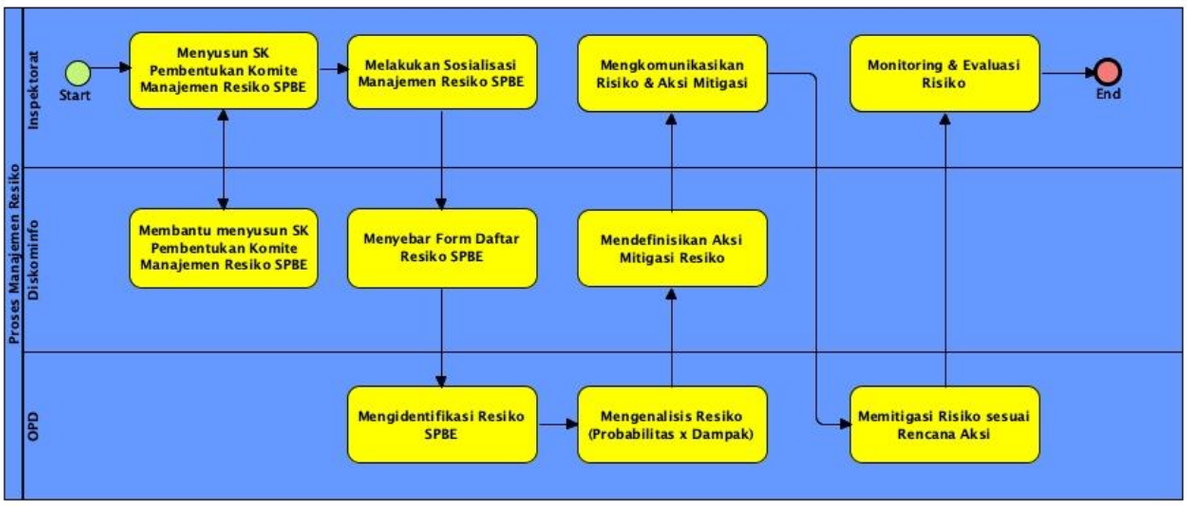
Gambar 1.2.2. Pedoman Struktur Manajemen Risiko SPBE Daerah (sumber: paparan KemenpanRB)

Mengacu pada gambar diatas maka susunan untuk struktur manajemen risiko spbe di Kab. Tapin dijelaskan sebagai berikut:



Gambar 1.2.3. Struktur Manajemen Risiko SPBE Kab. Tapin

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 1.2.4 Beberapa aktivitas yang dapat dilakukan oleh pemerintah daerah dalam upaya menajemen SPBE

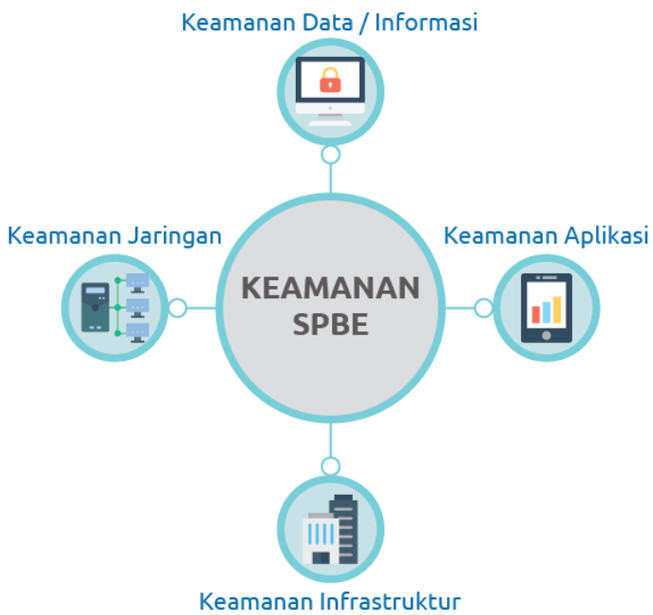
Secara teknis pemerintah daerah perlu menyusun Kajian dan SOP terkait manajemen risiko dengan lingkup sebagai berikut:

1. SOP Manajemen Risiko SPBE oleh setiap SKPD
2. Kajian Manajemen Risiko

B. Manajemen Keamanan Informasi

Gambar 1.2.5. Manajemen Keamanan Informasi

Dalam SPBE perlu menetapkan dan memelihara sistem manajemen keamanan informasi *(Information Security Management System / ISMS)* yang menyediakan pendekatan standar, formal dan berkelanjutan untuk manajemen keamanan informasi, memungkinkan teknologi yang aman dan proses bisnis yang selaras dengan persyaratan tugas pekerjaan.



Gambar 1.2.6. Keamanan Informasi SPBE

Secara umum terdapat empat fokus dalam keamanan SPBE yaitu:

1. Keamanan Data / Informasi
2. Keamanan Aplikasi
3. Keamanan Jaringan
4. Keamanan Infrastruktur

Mengacu pada *best practices* dalam COBIT 2019, Berikut aktivitas-aktivitas yang perlu dilakukan dalam manajemen keamanan informasi yaitu:

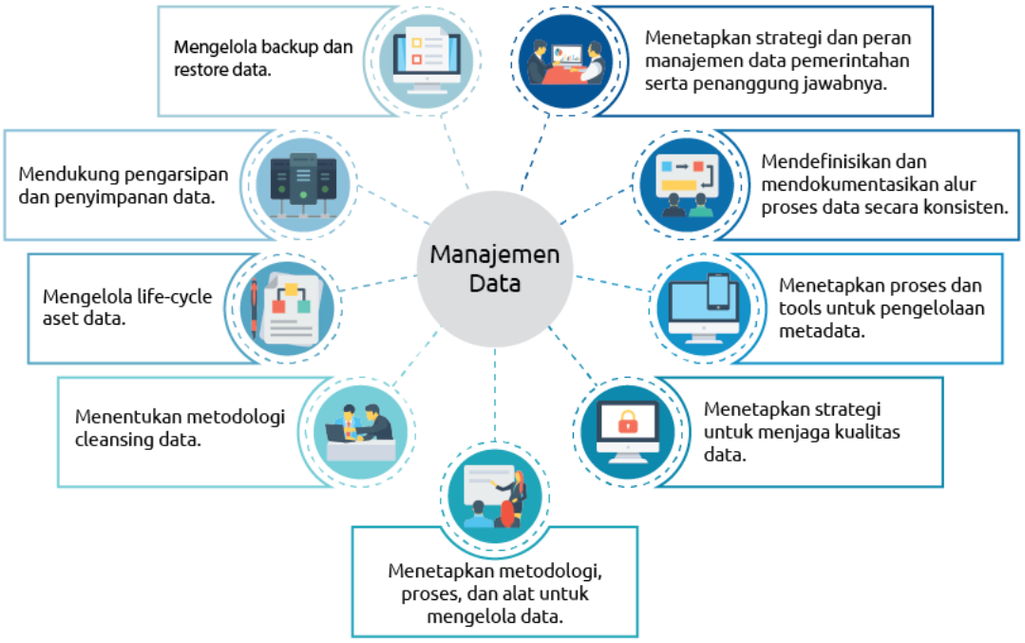
1. Menentukan ruang lingkup dan batas-batas manajemen keamanan informasi dalam hal karakteristik organisasi, lokasi, aset dan teknologi.
2. Menetapkan manajemen keamanan informasi sesuai dengan kebijakan instansi dan konteks dimana instansi beroperasi.
3. Menyelaraskan manajemen keamanan informasi dengan pendekatan organisasional secara keseluruhan pada manajemen keamanan.
4. Mendapatkan otorisasi dari pejabat struktural untuk menerapkan dan mengoperasikan atau mengubah manajemen keamanan informasi.
5. Mempersiapkan dan memelihara pernyataan penerapan yang menggambarkan ruang lingkup manajemen keamanan informasi.
6. Menetapkan serta mengkomunikasikan peran dan tanggung jawab pengelola keamanan informasi.
7. Mengkomunikasikan pendekatan manajemen keamanan informasi.

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

1. SOP Akses Ruang Server
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 Server
8. SOP Evaluasi Keamanan SPBE

C. Manajemen Data

Data menjadi kebutuhan penting dalam pemerintahan, data dihasilkan dari proses bisnis yang dijalankan oleh pemerintah. Dalam implementasi SPBE perlu melakukan manajemen aset data pemerintahan yang efektif di seluruh *life-cycle* data mulai dari: produksi, pengiriman, pemeliharaan dan pengarsipan. Hal ini bertujuan untuk memastikan pemanfaatan aset data pemerintahan berfungsi efektif untuk mencapai tujuan dan sasaran pemerintahan. Mengacu pada *best practices* dalam COBIT 2019, Berikut aktivitas-aktivitas yang perlu dilakukan dalam manajemen data yaitu:



Gambar 1.2.7. Manajemen Data

1. **Menetapkan strategi dan peran manajemen data pemerintahan serta penanggung jawabnya.**
   Membentuk pertemuan Forum Satu Data guna menetapkan cara mengelola dan meningkatkan aset berupa data-data pemerintahan yang sejalan dengan arah pemerintahan. Mengkomunikasikan strategi pengelolaan data di seluruh SKPD. Menetapkan peran dan tanggung jawab masing-masing SKPD terhadap pengelolaan data untuk memastikan bahwa data pemerintahan dikelola dengan baik. Strategi manajemen data ini perlu diterapkan secara efektif dan berkelanjutan.

2. **Mendefinisikan dan mendokumentasikan alur proses data secara konsisten.**
   Membuat alur diagram untuk pemrosesan data mulai dari produksi data, *cleansing* data, persyaratan pemanfaatan data, dan pengarsipan data. Selanjutnya menyetujui dan melaksanakan alur pemanfaatan data tersebut di seluruh SKPD.

3. **Menetapkan proses dan tools untuk pengelolaan metadata.**
   Menetapkan proses dan tools untuk menentukan metadata tentang data data pemerintahan, membina dan mendukung *sharing* data, memastikan penggunaan data yang sesuai dan valid, meningkatkan adaptasi untuk perubahan bisnis proses.

4. **Menetapkan strategi untuk menjaga kualitas data.**
   Menetapkan strategi yang terpadu untuk SKPD guna mempertahankan kualitas data pemerintahan dari sisi (kompleksitas, integritas, akurasi, kelengkapan, validitas dan ketepatan waktu).

5. **Menetapkan metodologi, proses, dan alat untuk mengelola data.**
   Menerapkan metodologi, proses, dan alat untuk standarisasi atribut data melalui template yang dapat diterapkan di beberapa tempat penyimpanan data (*database*).

6. **Menentukan metodologi *cleansing data.***

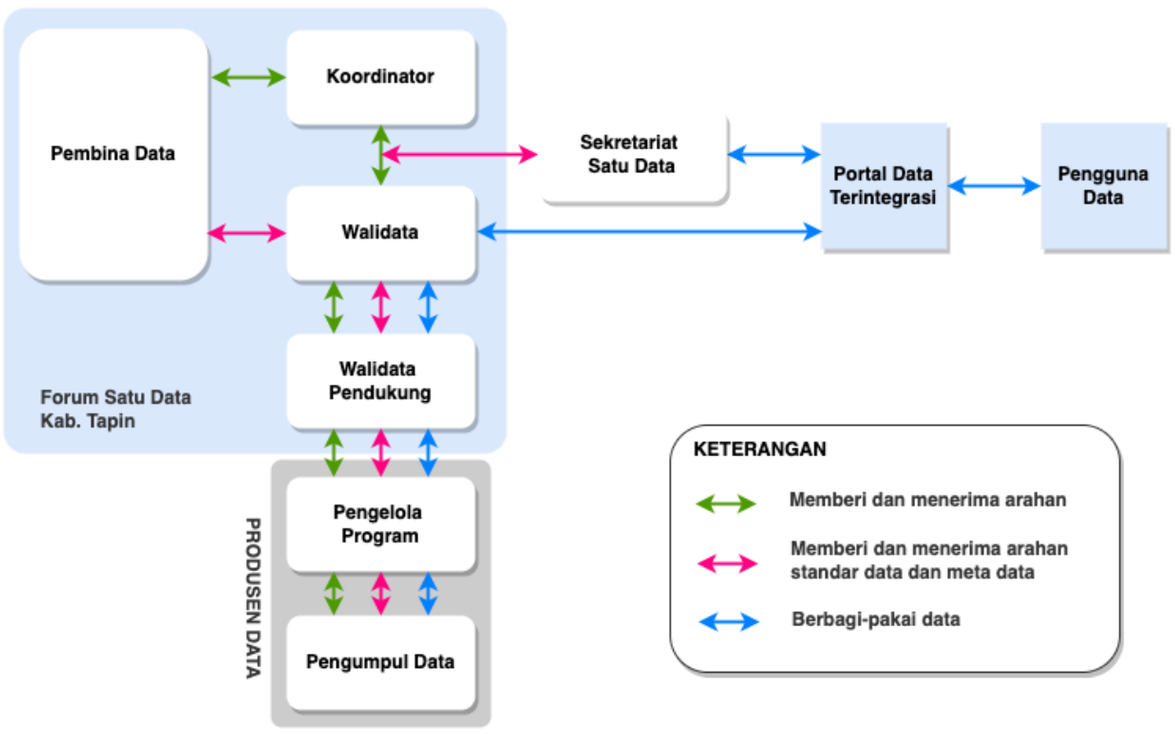
Menetapkan mekanisme proses dan metode untuk memvalidasi dan memperbaiki kualitas data yang sesuai dengan bisnis prosesnya.

7. **Mengelola *life-cycle* aset data.**
   Memastikan bahwa SKPD memahami, memetakan, menginventarisir, dan mengontrol aliran datanya melalui siklus proses bisnis mulai dari produksi data, akuisisi data hingga penyimpanan dan pengarsipan.

8. **Mendukung pengarsipan dan penyimpanan data.**
   Pastikan bahwa data-data pemerintahan disimpan dengan baik dan wali data perlu menetapkan retensi atas data tersebut untuk menjamin ketersediaan data historis.

9. **Mengelola *backup* dan *restore* data.**
   Melakukan backup secara berkala terhadap data digital dan melakukan restore ketika terjadi kerusakan data.

Mengacu pada Perpres 39/2019 tentang Satu Data Indonesia, dalam Penerapan Manajemen Data Kab. Tapin perlu menyusun struktur forum satu data seperti berikut:



Gambar 1.2.8. Forum Satu Data Kab. Tapin

Penugasan:

Koordinator	Sekda
Pembina Data	Bappeda & BPS
Walidata	Diskominfo
Walidata Pendukung	Masing-masing SKPD (Bag. Program)

Produsen Data	Masing-masing SKPD (Seluruh Bidang)

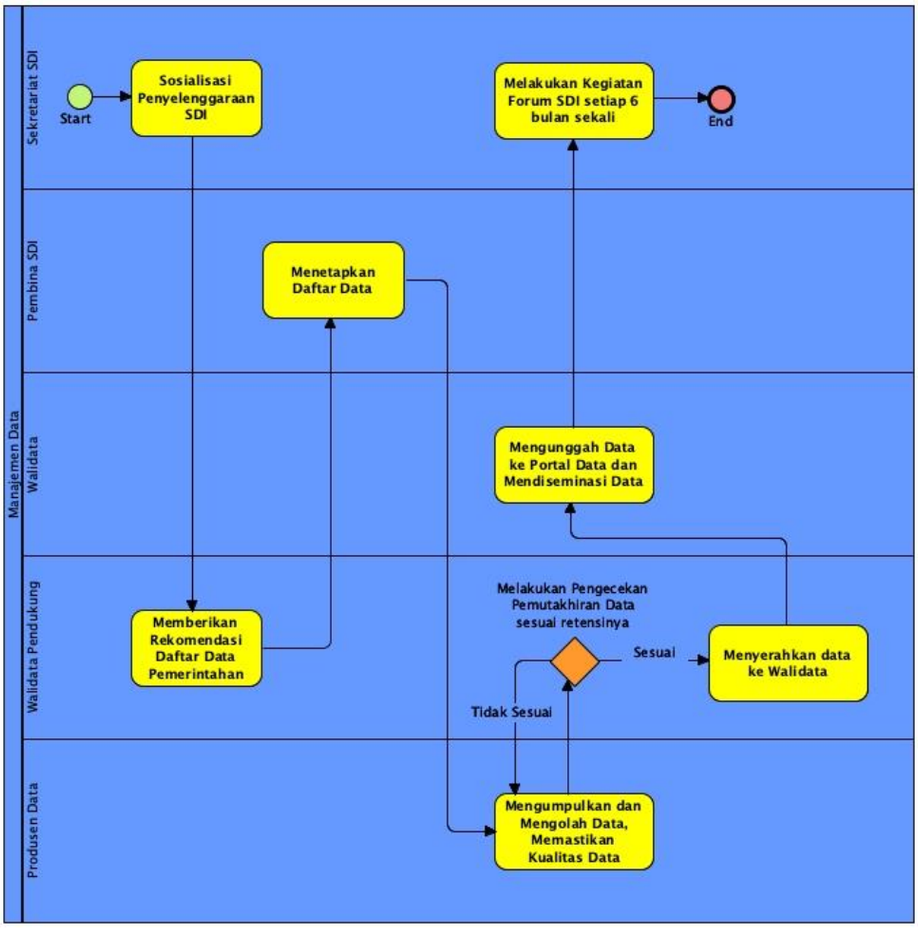
Tugas Pembina Data Tingkat Daerah:

- Menetapkan Standar Data yang berlaku lintas Instansi Daerah;
- Menetapkan struktur yang baku dan format yang baku dari Metadata yang berlaku lintas Instansi Pusat dan/atau Instansi Daerah;
- Memberikan rekomendasi dalam proses perencanaan pengumpulan Data;
- Melakukan pemeriksaan ulang terhadap Data Prioritas; dan
- Melakukan pembinaan penyelenggaraan Satu Data Indonesia sesuai dengan ketentuan peraturan perundang-undangan.

Tugas Produsen Data Tingkat Daerah:

- Mengumpulkan, memeriksa kesesuaian Data, dan mengelola Data yang disampaikan oleh Produsen Data sesuai dengan prinsip Satu Data Indonesia;
- Menyebarluaskan Data, Metadata, Kode Referensi, dan Data Induk di Portal Satu Data Indonesia; dan
- Membantu Pembina Data dalam membina Produsen Data.
- Memberikan masukan kepada Pembina Data dan Kepala Dinas mengenai Standar Data, Metadata, dan Interoperabilitas Data;
- Menghasilkan Data sesuai dengan prinsip Satu Data Indonesia; dan
- Menyampaikan Data dan Metadata kepada produsen data.

Berdasarkan *best practices* di atas pemerintah kabupaten Tapin dalam alur pengelolaan satu datanya perlu melakukan hal seperti berikut ini.



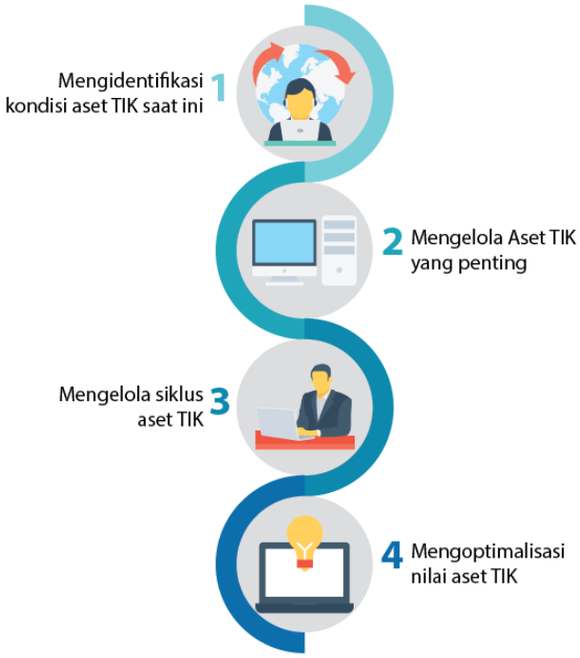
Gambar 1.2.9. Alur Koordinasi Satu Data

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
7. SOP Pembuatan dan perubahan kamus data metadata

D. Manajemen Aset TIK

Dalam implementasi SPBE perlu melakukan manajemen aset TIK untuk memastikan penggunaan aset berfungsi dengan baik untuk mendukung kemampuan layanan pemerintahan dan pemeliharaannya harus optimal agar aset TIK selalu tersedia dan dapat diandalkan. Contoh kasus misalkan dalam mengelola server / data center 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*) nya. Mengacu pada *best practices* dalam ITIL, Berikut aktivitas-aktivitas yang perlu dilakukan dalam manajemen Aset TIK yaitu:



Gambar 1.2.10. Manajemen Aset TIK

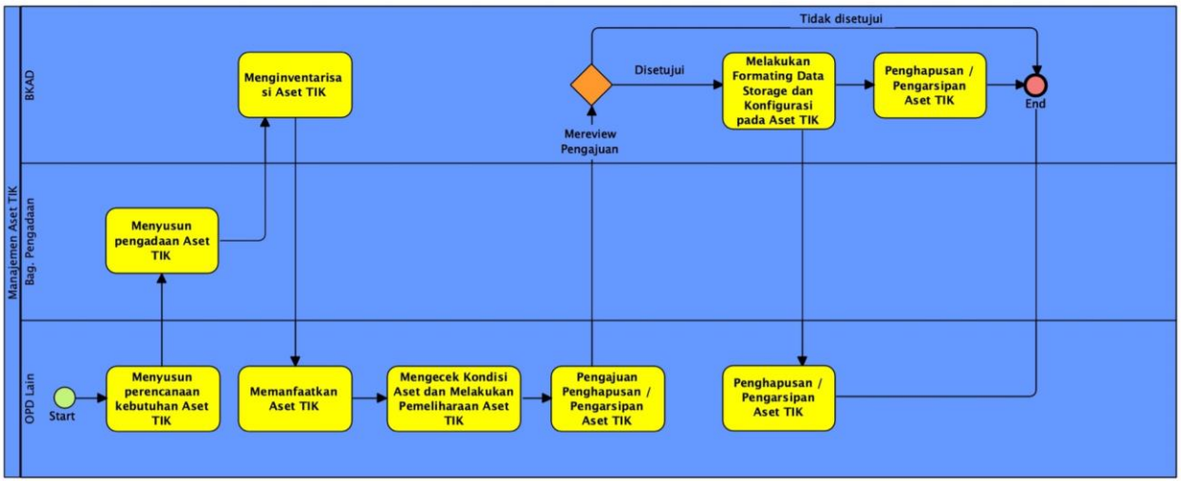
1. **Mengidentifikasi kondisi aset TIK saat ini**
   Mencatat seluruh aset TIK (software & hardware) beserta kondisi dan *life-time* nya, untuk software berbayar pastikan lisensinya terbayar.

2. **Mengelola Aset TIK yang penting**
   Memastikan aset TIK selalu tersedia dan dapat diandalkan untuk dapat digunakan dalam menunjang operasional SPBE.

3. **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* nya.

4. **Mengoptimalisasi nilai aset TIK**
   Secara berkala meninjau aset secara menyeluruh untuk mengidentifikasi bagaimana cara untuk mengoptimalkan aset sejalan dengan kebutuhan bisnis SPBE.

Berdasarkan *best practices* di atas pemerintah kabupaten Tapin dalam alur proses pengelolaan manajemen aset TIK nya dapat merujuk pada gambar berikut ini.



Gambar 1.2.11. 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 Penghentian dan Pembuangan Aset TIK.

E. Manajemen SDM

Manajemen SDM perlu dilakukan guna menjamin keberlangsungan dan 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
2. Pengadaan aparatur sipil negara
3. Pengembangan karir aparatur sipil negara
4. Pengembangan kompetensi aparatur sipil negara
5. Penempatan aparatur sipil negara
6. Promosi dan/atau mutasi aparatur sipil negara
7. Uji kompetensi aparatur sipil negara
8. Sistem informasi manajemen aparatur sipil negara
9. Kelompok rencana suksesi *(talent pool)* aparatur sipil negara.

Dalam kondisi ideal setiap SKPD 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. Teknisi Komputer/Jaringan/Telekomunikasi
   Personil yang bertugas untuk merawat atau memperbaiki perangkat keras, berupa komputer dan jaringan, ataupun peralatan telekomunikasi lainnya.

2. *Programmer*

   Personil yang bertugas untuk menyusun program komputer (aplikasi) berdasarkan petunjuk rancangan Sistem Analis, dan mendeteksi serta memperbaiki kesalahan pemrograman pada aplikasi.

3. *Web Administrator*

   Personil yang bertugas untuk mengelola *web server* pemerintah daerah, dan bertanggung jawab secara teknis untuk mengkoordinir penyediaan data yang akan ditampilkan di *website* resmi pemerintahan daerah.

4. Sistem Analis

   Personil yang bertugas untuk merancang pembangunan (pengembangan) sistem informasi (aplikasi) yang dibutuhkan sesuai kaidah standar dalam pengembangan sistem informasi, dan mendokumentasikan hasil analisa dan perancangan sistem informasi dengan baik, sehingga memudahkan dalam perawatan ataupun kelanjutan pembangunan sistem informasi.

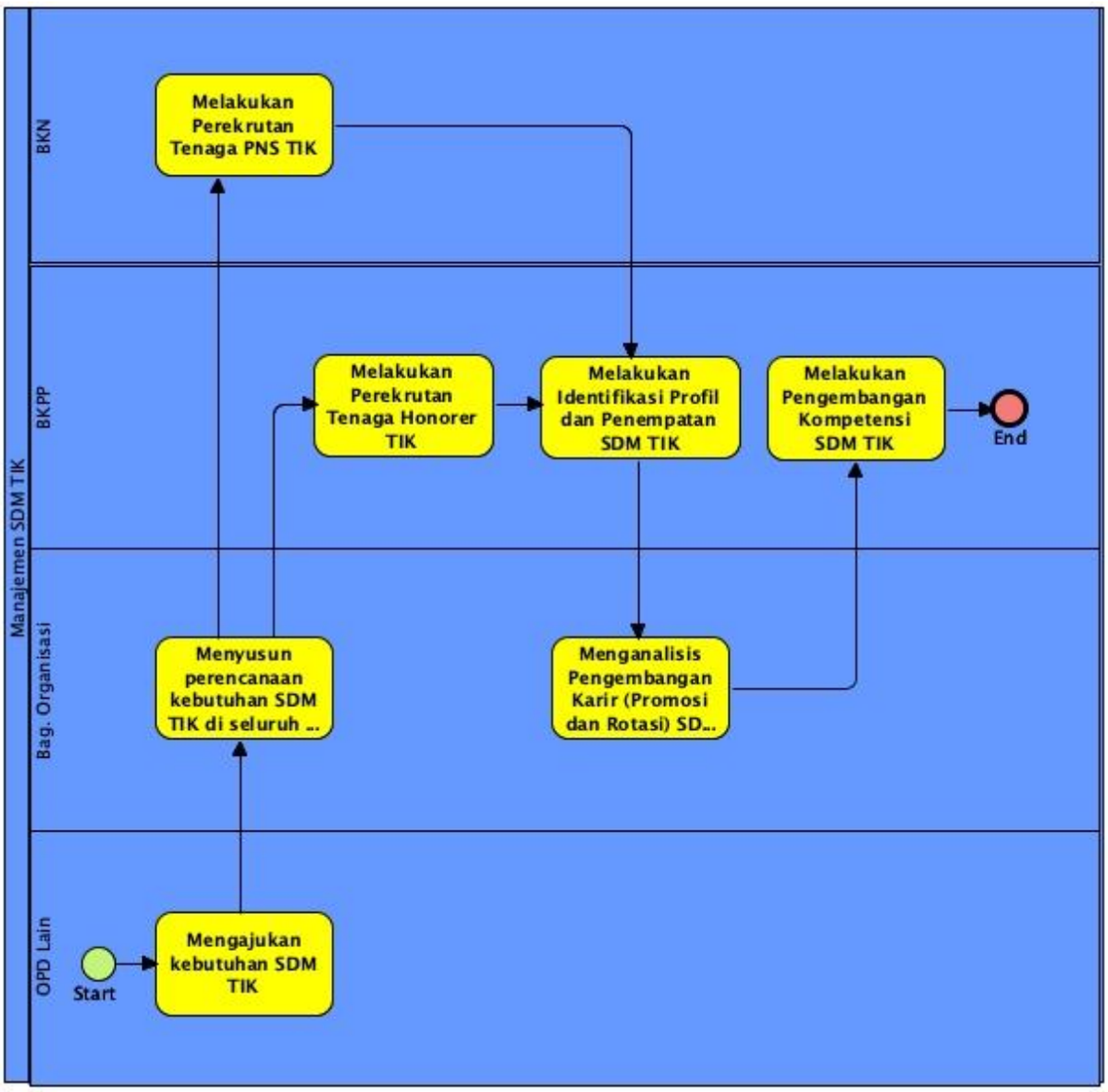
5. Administrator Sistem

   Personil yang bertugas untuk mengelola sistem informasi (aplikasi) yang tersedia di masing-masing SKPD pemerintah daerah, mengatur pendaftaran pengguna, dan memberikan hak akses dan kewenangan setiap pengguna.

6. Administrator Jaringan

   Personil yang bertugas untuk mengelola jaringan komputer, termasuk ketersediaan jaringan (*network availability*), keamanan jaringan (*network security*), kehandalan jaringan (*network reliability*), dan pengendalian hak akses (*access control*).

Peningkatan kemampuan SDM TIK dibutuhkan dan disesuaikan dengan tugas dan kewajiban dari personil yang bersangkutan. Peningkatan kemampuan personel dapat dilakukan melalui pelatihan-pelatihan maupun studi tingkat lanjut. Seseorang yang mempunyai tanggung jawab terhadap sistem ini semakin lama akan semakin ahli pada bidangnya dan akan semakin bermanfaat jika ia tetap pada pekerjaannya. Dengan demikian diperlukan mekanisme apresiasi yang berbeda bagi mereka. Sehingga perlu adanya SDM fungsional pranata komputer yang tugasnya adalah melakukan pengelolaan TIK di masing-masing SKPD.



Gambar 1.2.12. Manajemen SDM

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

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

F. Manajemen Pengetahuan

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

1. Sosialisasikan pentingnya manajemen pengetahuan
2. Pembentukan Pokja beberapa unit-kerja untuk koordinasi implementasi manajemen dipimpin oleh pimpinan pemerintah daerah.
3. Definisikan visi dan misi dalam implementasi manajemen manajemen pengetahuan. Sosialisasikan secara terus-menerus.
4. Rencanakan *Quick-Win* untuk mengatasi keragu-raguan dan resistensi.

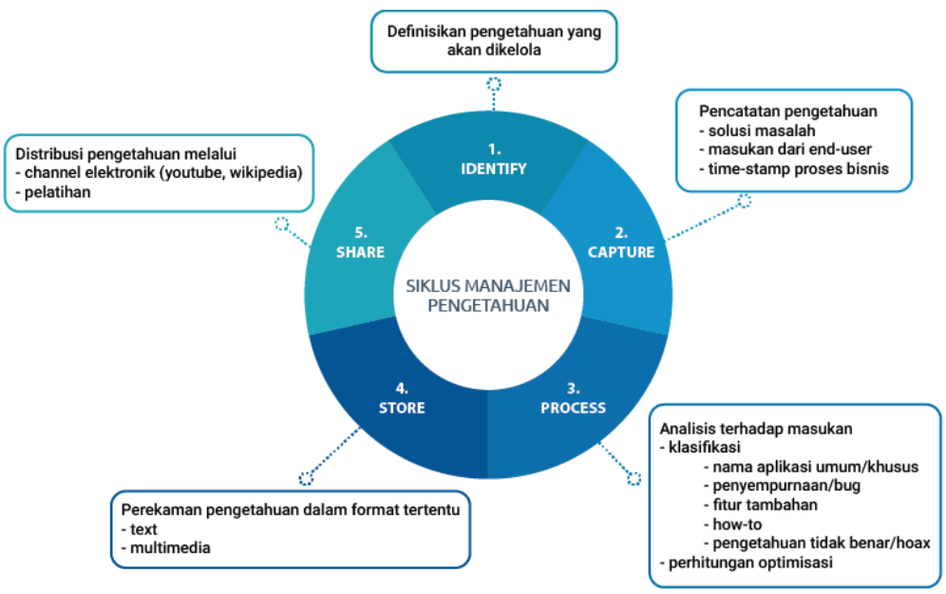
5. Konsolidasikan semua manfaat yang sudah tercapai, untuk mendapatkan momentum.
6. Budayakan "*sharing & re-use*" sebagai cara bekerja yg efektif dan efisien.

Gambar 1.2.13. Manajemen Pengetahuan

Adapun manfaat dari manajemen pengetahuan SPBE yakni:

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

Dalam manajemen pengetahuan terdapat siklus hidup yang dimulai dari proses identifikasi, pencatatan, pemrosesan, penyimpanan, dan berbagi dan digambarkan sebagai berikut ini:



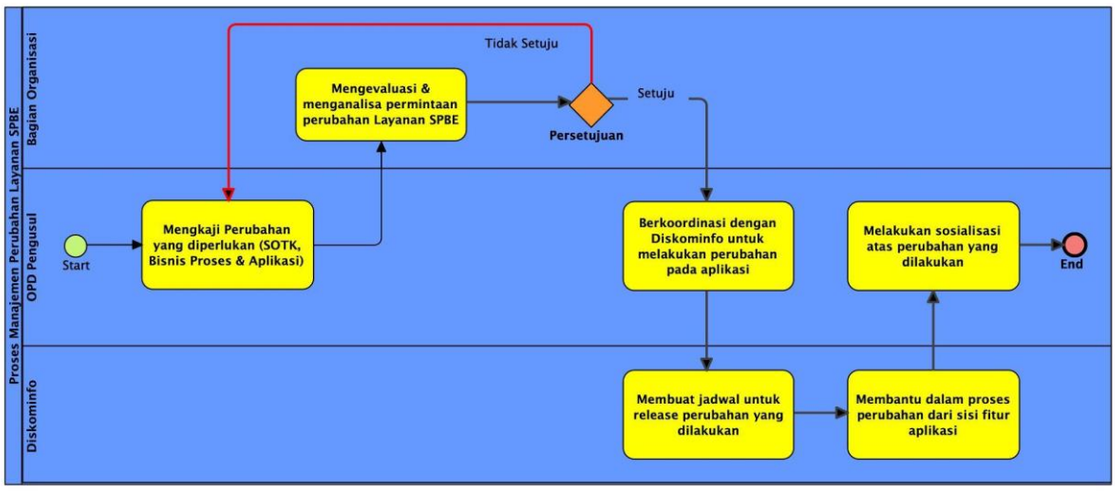
Gambar 1.2.14. Siklus Manajemen Pengetahuan

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

1. SOP Pencatatan pengalaman & lesson learned untuk setiap SKPD

G. Manajemen Perubahan

Ketika terjadi perubahan pada visi & misi / kebijakan / SOTK maka layanan harus mampu mengadopsi perubahan tersebut dengan melakukan manajemen perubahan pada bisnis proses, aplikasi maupun infrastrukturnya. Adapun mekanisme alur perubahan layanan SPBE yang perlu ada di pemerintah kabupaten Tapin dijelaskan pada gambar berikut ini.



Gambar 1.2.15. Manajemen Perubahan

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

1. SOP Manajemen Perubahan.

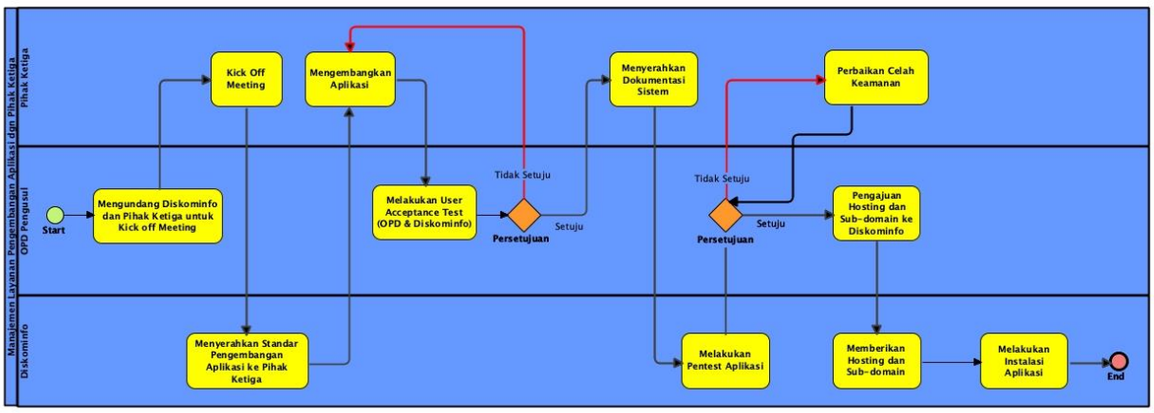
H. Manajemen Layanan

Dalam 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 1.2.16. Manajemen Layanan

1. Mengelola Gangguan dengan menyediakan platform helpdesk TIK disertai dengan ticketing dan monitoring 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* diatas Diskominfo dapat melakukan pemberian dukungan layanan TI terkait (a.) layanan pengembangan aplikasi dan (b). layanan penanganan insiden yang dijelaskan pada gambar berikut ini.



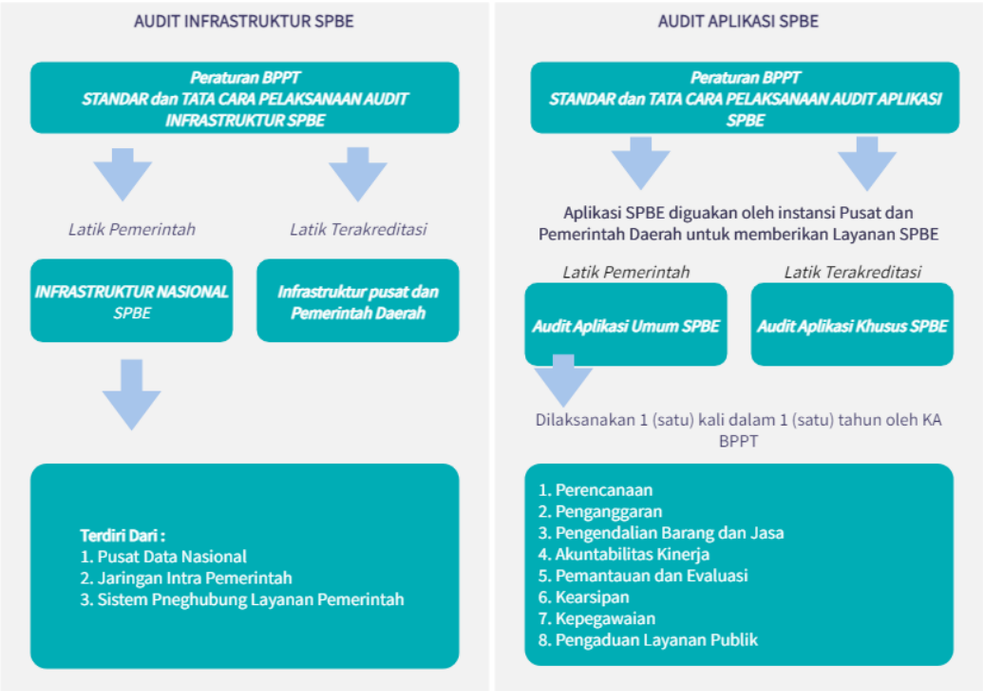
Gambar 1.2.17. Layanan Pengembangan Aplikasi

Gambar 1.2.18. Layanan Penanganan Insiden

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

A. SOP Pengajuan layanan (Helpdesk)

I. Audit TIK



Gambar 1.2.19. 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:

a. Penerapan tata kelola dan manajemen teknologi informasi dan komunikasi;
b. Fungsionalitas teknologi informasi dan komunikasi;
c. Kinerja teknologi informasi dan komunikasi yang dihasilkan; dan
d. 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 :

1. Audit infrastruktur SPBE, merujuk pada Perpres 95/2018 pasal 55 disebutkan:
   - Infrastruktur SPBE Nasional diaudit setiap tahun oleh BPPT;
   - Infrastruktur SPBE Pemerintah Daerah diaudit setiap dua tahun oleh lembaga audit TIK atau perusahaan audit TIK;
   - Koordinasi dengan Kementerian Kominfo.
2. Audit Aplikasi SPBE dimana Aplikasi umum diaudit setiap tahun oleh BPPT; Aplikasi khusus diaudit setiap dua tahun oleh Lembaga Audit TIK; Koordinasi dengan Kementerian Kominfo.
3. Audit Keamanan Informasi dimana Audit keamanan pada infrastruktur SPBE Nasional dan Aplikasi Umum dilakukan setiap tahun oleh BSSN; Audit keamanan pada infrastruktur SPBE

Instansi Pusat dan Instansi Daerah serta Aplikasi Khusus dilakukan setiap dua tahun oleh Lembaga Audit TIK atau perusahaan audit TIK;.

Adapun kegiatan yang dilakukan dalam Audit TIK dijabarkan sebagai berikut ini:

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.
14. Memverifikasi Kelayakan Tindak Lanjut Audit Teknologi Informasi.

Bab II

Arsitektur Target SPBE

2.1. Arsitektur Data

A. Katalog Entitas Data

Data yang dikelola pada SPBE merupakan suatu kumpulan yang terdiri dari obyek-obyek kerja untuk memberikan gambaran yang lebih luas terkait dengan suatu pelayanan maupun pengelolaan pemerintahan. Setiap data yang dikelola memungkinkan berupa data yang bersifat publik dan memungkinkan bersifat privat. Berdasarkan dari hasil survei yang dilaksanakan terhadap seluruh SKPD di Kabupaten Tapin, berikut ini disajikan daftar data yang dikelola secara mendetail oleh SKPD di Kabupaten Tapin.

Tabel 2.1.1 Daftar Data yang dikelola oleh SKPD di Kabupaten Tapin

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-001	Data Kepegawaian	Data Kepegawaian	Terbatas	Text	Realtime	Badan Kepegawaian dan Pengembangan Sumber Daya Manusia	TPN-08.02. Pengelolaan Kepegawaian	Layanan Profil Kepegawaian	RAD 09. Informasi Pemerintahan Umum	RAD 09.06. Data Aparatur Sipil Negara
Data-002	Data Gaji	Data Gaji Pegawai	Terbatas	Text	Realtime	Badan Kepegawaian dan Pengembangan Sumber Daya Manusia	TPN-08.02. Pengelolaan Kepegawaian	Layanan Gaji Berkala	RAD 09. Informasi Pemerintahan Umum	RAD 09.06. Data Aparatur Sipil Negara
Data-003	Data TPP	Data TPP	Terbatas	Text	Realtime	Badan Kepegawaian dan Pengembangan Sumber Daya Manusia	TPN-08.02. Pengelolaan Kepegawaian	Layanan TPP	RAD 09. Informasi Pemerintahan Umum	RAD 09.06. Data Aparatur Sipil Negara
Data-004	Data Pelatihan	Data Pelatihan	Terbuka	Text	Harian	Badan Kepegawaian dan Pengembangan Sumber Daya Manusia	TPN-08.02. Pengelolaan Kepegawaian	Layanan Pelatihan ASN	RAD 09. Informasi Pemerintahan Umum	RAD 09.06. Data Aparatur Sipil Negara

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-005	Data Parpol	Data Parpol	Terbuka	Text	Bulanan	Badan Kesatuan Bangsa dan Politik	TPN-09.03. Pembinaan Ideologi, Wawasan Kebangsaan, Dan Politik	Layanan Pendataan dan Permohonan SKT	RAD 05. Informasi Ketertiban Umum dan Keselamatan	RAD 05.02. Data Keamanan
Data-006	Data Ormas	Data Ormas	Terbuka	Text	Bulanan	Badan Kesatuan Bangsa dan Politik	TPN-09.03. Pembinaan Ideologi, Wawasan Kebangsaan, Dan Politik	Layanan Pendataan dan Permohonan SKT	RAD 05. Informasi Ketertiban Umum dan Keselamatan	RAD 05.02. Data Keamanan
Data-007	Data Anggaran / Keuangan	Data Anggaran/keuangan daerah	Terbatas	Text	Bulanan	Badan Keuangan dan Aset Daerah	TPN-14.02. Administrasi Keuangan Perangkat Daerah	Layanan data anggaran	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-008	Data Transaksi Tuntunan Bendahara	Data Transaksi Tuntunan Bendahara	Terbatas	Text	Harian	Badan Keuangan dan Aset Daerah	TPN-14.02. Administrasi Keuangan Perangkat Daerah	Layanan Keuangan	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-009	Data Perencanaan Keuangan	Data Perencanaan Keuangan	Terbatas	Text	Harian	Badan Keuangan dan Aset Daerah	TPN-14.02. Administrasi Keuangan Perangkat Daerah	Layanan Perencanaan Dan Penganggaran	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-010	Data Logistik	Data Logistik Bantuan	Terbuka	Text	Realtime	Badan Penanggulanan Bencana Daerah	TPN-06.04. Penyiapan Tangguh Bencana	Layanan Informasi dan Bantuan	RAD 10. Data Pendukung Umum	RAD 10.04. Data Dukung Lainnya
Data-011	Data Pajak Retribusi Daerah	Data Pajak Retribusi Daerah	Terbatas	Text	Harian	Badan Pengelolaan Pajak dan Retribusi Daerah	TPN-03.05. Pengelolaan Pendapatan Daerah	Layanan keuangan	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-012	Data Penetapan dan Penerimaan Daerah	Data Penetapan dan Penerimaan Daerah	Terbatas	Text	Harian	Badan Pengelolaan Pajak dan Retribusi Daerah	TPN-03.05. Pengelolaan Pendapatan Daerah	Layanan Retribusi Daerah	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-013	Data Informasi Pelayanan Masyarakat	Landing Page (Usulan Masyarakat, Layanan Pengaduan, Layanan Konsultasi)	Terbuka	Text	Realtime	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-15.03. Pengendalian Dan Evaluasi Pembangunan Daerah	Layanan Pengaduan Masyarakat	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-014	Data Inovasi dan Berita Penelitian dan Pembangunan	Sistem Informasi Inovasi dan Berita Penelitian dan	Terbuka	Text	Realtime	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-11.02. Penelitian Dan Pengembangan Daerah	Layanan Data Inovasi	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
		Pembangunan								
Data-015	Data Perencanaan dan Penganggaran	Data Perencanaan dan Penganggaran	Terbatas	Text	Realtime	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-14.01. Perencanaan, Pengendalian Dan Evaluasi Pembangunan Daerah	Layanan Perencanaan Dan Penganggaran	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-016	Data Perencanaan Pembangunan Daerah RKPD	Data Perencanaan Pembangunan Daerah RKPD	Terbatas	Text	Realtime	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-14.01. Perencanaan, Pengendalian Dan Evaluasi Pembangunan Daerah	Layanan Perencanaan Dan Penganggaran	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-017	Data Monitoring Evaluasi	Data Monitoring Evaluasi	Terbatas	Text	Realtime	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-15.03. Pengendalian Dan Evaluasi Pembangunan Daerah	layanan evaluasi	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-018	Data DAK Fisik	Sistem Informasi DAK Fisik	Terbatas	Text	Realtime	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-15.03. Pengendalian Dan Evaluasi Pembangunan Daerah	Layanan Perencanaan Dan Penganggaran	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-019	Data Informasi Pembangunan Daerah	Data Informasi Pembangunan Daerah	Terbatas	Text	Tahunan	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-15.03. Pengendalian Dan Evaluasi Pembangunan Daerah	Layanan Perencanaan Dan Penganggaran	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-020	Data Informasi Kepemerintahan	Data Informasi Kepemerintahan	Terbuka	Text	Harian	Bagian Hubungan Masyarakat dan Protokol		Layanan Informasi Kepemerintahan	RAD 09. Informasi Pemerintahan Umum	RAD 09.03. Data Informasi
Data-021	Data Sosial	Data Sosial	Terbuka	Text	Realtime	Bagian Kesejahteraan Rakyat	TPN-09.01. Peningkatan Kualitas Kehidupan Sosial Keagamaan	Layanan informasi kepemerintahan, informasi sosial kemasyarakatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.02. Data Sosial
Data-022	Data Akuntabilitas Kinerja	Data Akuntabilitas Kinerja	Terbatas	Text	Realtime	Bagian Organisasi	TPN-08.01. Peningkatan Tata Kelola Organisasi	Layanan pelaporan dan akuntabilitas	RAD 09. Informasi Pemerintahan Umum	RAD 09.06. Data Aparatur Sipil Negara
Data-023	Data Pengadaan Barang dan Jasa	Data Pengadaan Barang dan Jasa	Terbuka	Text	Realtime	Bagian Pengadaan Barang dan Jasa	TPN-12.03. Pengadaan Barang Dan Jasa	Layanan Pengadaan Barang dan Jasa	RAD 10. Data Pendukung Umum	RAD 10.04. Data Dukung Lainnya
Data-024	Data Kebudayaan	Data Kebudayaan	Terbuka	Text	Realtime	Dinas Kebudayaan dan Pariwisata	TPN-04.02. Pelestarian Kebudayaan	Layanan Informasi, Kebudayaan, Wisata, Ekonomi Kreatif	RAD 08. Informasi Budaya dan Agama	RAD 08.02. Data Kebudayaan

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-025	Data Pariwisata	Data Pariwisata				Dinas Kebudayaan dan Pariwisata	TPN-04.03. Peningkatan Pariwisata	Layanan Informasi, Kebudayaan, Wisata, Ekonomi Kreatif	RAD 02. Informasi Ekonomi dan Industri	RAD 02.11. Data Pariwisata
Data-026	Data Survey Kepuasaan Masyarakat	Survei Kepuasan Publik	Terbuka	Text	Harian	Bagian Organisasi	TPN-07.01. Manajemen Pelayanan Publik	Layanan pengaduan masyarakat	RAD 09. Informasi Pemerintahan Umum	RAD 09.04. Data Komunikasi
Data-027	Data Kependudukan	Data Kependudukan	Terbuka	Text	Harian	Dinas Kependudukan dan Pencatatan Sipil	TPN-07.01. Manajemen Pelayanan Publik	Layanan Kependudukan	RAD 03. Pembangunan Kewilayahan	RAD 03.07. Data Kependudukan
Data-028	Data Informasi, Layanan, Kesehatan	Data Informasi, Layanan, Kesehatan	Terbuka	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-029	Data Stunting	Data Stunting	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-030	Data Gizi	Data Gizi	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-031	Data Malaria	Data Malaria	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-032	Data Ketersediaan Obat	Data Ketersediaan Obat	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-033	Data Penyakit	Data Penyakit	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-034	Data Imunisasi	Data Imunisasi	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-035	Data kesehatan Ibu dan Balita	Data kesehatan Ibu dan Balita	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-036	Data Covid	Data Covid	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Covid-19	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-037	Data Antigen dan PCR	Data Antigen dan PCR	Terbatas	Text	Harian	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Covid-19	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-038	Data Kematian	Data Kematian	Terbatas	Text	Harian	Dinas Kesehatan	TPN-07.01. Manajemen Pelayanan Publik	Layanan Kependudukan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-039	Data Harga Pangan	Data Harga Pangan	Terbuka	Text	Bulanan	Dinas Ketahanan Pangan	TPN-05.02. Peningkatan Kemandirian Pangan	Layanan Informasi Data Harga Pangan, Keamanan Pangan, Pengisian Lumbung Gabah, Dan Keamanan Pangan	RAD 02. Informasi Ekonomi dan Industri	RAD 02.03. Data Pertanian
Data-040	Data Pembangunan Lumbung	Data Pembangunan Lumbung	Terbuka	Text	Bulanan	Dinas Ketahanan Pangan	TPN-05.02. Peningkatan Kemandirian Pangan	Layanan Informasi Data Harga Pangan, Keamanan Pangan, Pengisian Lumbung Gabah, Dan Keamanan Pangan	RAD 02. Informasi Ekonomi dan Industri	RAD 02.03. Data Pertanian
Data-041	Data Pengisian Lumbung Gabah	Data Pengisian Lumbung Gabah	Terbuka	Text	Bulanan	Dinas Ketahanan Pangan	TPN-05.02. Peningkatan Kemandirian Pangan	Layanan Informasi Data Harga Pangan, Keamanan Pangan, Pengisian Lumbung Gabah, Dan Keamanan Pangan	RAD 02. Informasi Ekonomi dan Industri	RAD 02.03. Data Pertanian
Data-042	Data Keamanan Pangan	Keamanan Pangan Segar Asal Tumbuhan	Terbuka	Text	Bulanan	Dinas Ketahanan Pangan	TPN-05.02. Peningkatan Kemandirian Pangan	Layanan Informasi Data Harga Pangan, Keamanan Pangan, Pengisian Lumbung Gabah, Dan Keamanan Pangan	RAD 02. Informasi Ekonomi dan Industri	RAD 02.03. Data Pertanian

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-043	Data Pembinaan Kelompok Wanita Tani	Pembinaan Kelompok Wanita Tani	Terbuka	Text	Bulanan	Dinas Ketahanan Pangan	TPN-04.04. Peningkatan Pertanian Perikanan Dan Peternakan	Layanan Pembinaan Pengolahan Dan Pemasaran Hasil Pertanian	RAD 02. Informasi Ekonomi dan Industri	RAD 02.03. Data Pertanian
Data-044	Data Keanekaragaman Pangan	Data Keanekaragaman Pangan	Terbuka	Text	Bulanan	Dinas Ketahanan Pangan	TPN-05.02. Peningkatan Kemandirian Pangan	Layanan Informasi Data Harga Pangan, Keamanan Pangan, Pengisian Lumbung Gabah, Dan Keamanan Pangan	RAD 02. Informasi Ekonomi dan Industri	RAD 02.03. Data Pertanian
Data-045	Data Aduan	Data Aspirasi dan Pengaduan Online Rakyat	Terbatas	Text	Harian	Dinas Komunikasi dan Informatika	TPN-13.01. Pengelolaan Informasi	Layanan Pengaduan Masyarakat	RAD 09. Informasi Pemerintahan Umum	RAD 09.04. Data Komunikasi
Data-046	Data Evaluasi SPBE	Data Evaluasi SPBE	Terbatas	Text	Tahunan	Dinas Komunikasi dan Informatika	TPN-13.03. Pengelolaan Satu Data Indonesiaa	Layanan Evaluasi	RAD 10. Data Pendukung Umum	RAD 10.01. Kebijakan Pemerintah
Data-047	Data Identifikasi TIK	Data Identifikasi TIK	Terbuka	Text	Bulanan	Dinas Komunikasi dan Informatika	TPN-13.01. Pengelolaan Informasi	Layanan Identifikasi Data	RAD 09. Informasi Pemerintahan Umum	RAD 09.03. Data Informasi
Data-048	Data Profil Dinas, Kegiatan, Berita	Data Profil Dinas, Kegiatan, Berita	Terbuka	Text	Harian	Dinas Pekerjaan Umum dan Penataan Ruang	TPN-13.01. Pengelolaan Informasi	Layanan Informasi Profil Dinas	RAD 10. Data Pendukung Umum	RAD 10.02. Data Manajemen Kegiatan
Data-049	Data Laporan Jalan dan Jembatan	Data Laporan Jalan dan Jembatan	Terbuka	Text	Harian	Dinas Pekerjaan Umum dan Penataan Ruang	TPN-06.01. Pengelolaan Infrastruktur Dasar	Layanan Rekomendasi Perizinan Pemanfaatan Ruang Milik Jalan	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-050	Data Informasi dan Keuangan	Data Perencanaan Keuangan	Terbatas	Text	Realtime	Badan Keuangan dan Aset Daerah	TPN-14.02. Administrasi Keuangan Perangkat Daerah	Layanan Keuangan	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-051	Data Perkawinan Usia Di Bawah Umur, Data Usaha Rumahan, Data Kekerasan Pada Perempuan	Data Perkawinan Usia Dibawah Umur, Data Usaha Rumahan, Data Kekerasan Pada Perempuan	Terbuka	Text	Tahunan	Dinas Pemberdayaan Perempuan dan Perlindungan Anak	TPN-10.02. Perlindungan Perempuan Dan Anak Dan Penyetaraan Gender	Layanan Informasi Pusat Pembelajaran Keluarga	RAD 05. Informasi Ketertiban Umum dan Keselamatan	RAD 05.03. Data Hak Asasi Manusia

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-052	Data Kepemudaan dan Olahraga	Data Kepemudaan dan Olahraga	Terbuka	Text	Realtime	Dinas Pemuda dan Olahraga	TPN-05.03. Pembinaan Kepemudaan	Layanan Pembinaan Pengolahan Dan Pemasaran Hasil Pertanian	RAD 08. Informasi Budaya dan Agama	RAD 08.03. Data Olahraga
Data-053	Data Perizinan OSS dan Non OSS	Data Perizinan OSS dan Non OSS	Terbatas	Text	Harian	Dinas Penanaman Modal dan pelayanan Terpadu Satu Pintu	TPN-03.02. Peningkatan Perekonomian Masyarakat	Layanan Perizinan	RAD 09. Informasi Pemerintahan Umum	RAD 09.07. Data Kesekretariatan Negara
Data-054	Data Pendidikan dan Tenaga Kependidikan	Data Pendidikan, Data SK, Data Guru	Terbuka	Text	Bulanan	Dinas Pendidikan	TPN-01.01. Peningkatan Pendidikan PAUD, SD, SMP	Layanan Kependidikan	RAD 06. Informasi Pendidikan dan Tenaga Kerja	RAD 06.01. Data Pendidikan
Data-055	Data Pendaftaran Siswa Baru	Data Pendaftaran Siswa Baru	Terbuka	Text	Harian	Dinas Pendidikan	TPN-01.01. Peningkatan Pendidikan PAUD, SD, SMP	Layanan Penerimaan Siswa Baru	RAD 06. Informasi Pendidikan dan Tenaga Kerja	RAD 06.01. Data Pendidikan
Data-056	Data Perencanaan dan Informasi Kinerja Anggaran	Data Perencanaan dan Informasi Kinerja Anggaran	Terbatas	Text	Realtime	Badan Perencanaan Pembangunan Penelitian dan Pengembangan	TPN-14.02. Administrasi Keuangan Perangkat Daerah	Layanan Data Anggaran	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-057	Data Guru dan Siswa	Data Guru dan Siswa	Terbatas	Text	Realtime	Dinas Pendidikan	TPN-01.02. Fasilitasi SDM Unggul	Layanan Kependidikan	RAD 06. Informasi Pendidikan dan Tenaga Kerja	RAD 06.01. Data Pendidikan
Data-058	Data Perencanaan, Monitoring dan Evaluasi DAK	Aplikasi Pelaporan, Perencanaan, Monitoring dan Evaluasi DAK	Terbuka	Text	Realtime	Bagian Perencanaan dan Keuangan	TPN-15.03. Pengendalian Dan Evaluasi Pembangunan Daerah	Layanan Evaluasi	RAD 09. Informasi Pemerintahan Umum	RAD 09.02. Data Keuangan
Data-059	Data Pencatatan Dan Pelaporan Program Bangga Kencana	Data Pencatatan Dan Pelaporan Program Bangga Kencana	Terbatas	Text	Realtime	Dinas Pengendalian Penduduk dan Keluarga Berencana	TPN-03.06. Pemberdayaan Keluarga	Layanan Keluarga Berencana	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.03. Data Pemberdayaan Perempuan
Data-060	Data Keluarga Berencana	Data Keluarga Berencana	Terbatas	Text	Realtime	Dinas Pengendalian Penduduk dan Keluarga Berencana	TPN-03.06. Pemberdayaan Keluarga	Layanan Keluarga Berencana	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.03. Data Pemberdayaan Perempuan
Data-061	Data Kinerja PKB/PLKB	Data Kinerja PKB/PLKB	Terbatas	Text	Realtime	Dinas Pengendalian Penduduk dan Keluarga Berencana	TPN-03.06. Pemberdayaan Keluarga	Layanan Keluarga Berencana	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.03. Data Pemberdayaan Perempuan

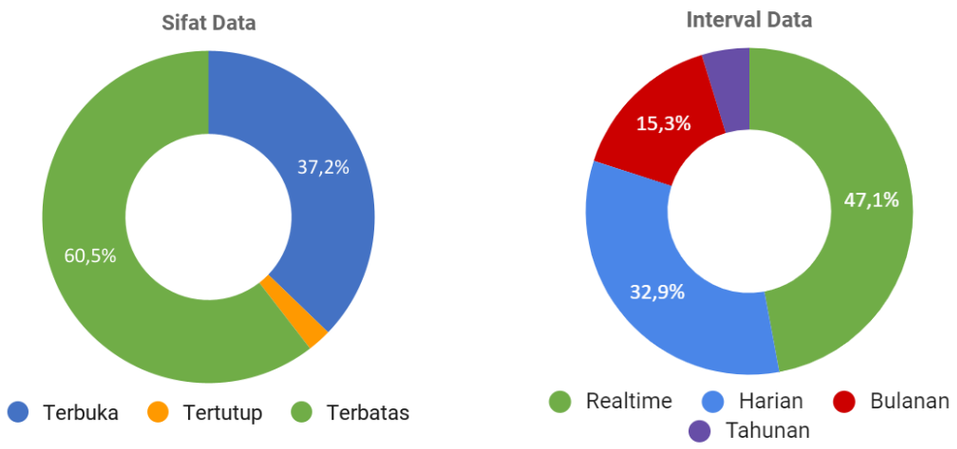
ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-062	Data Kekeluargaan	Data Kekeluargaan	Terbatas	Text	Realtime	Dinas Pengendalian Penduduk dan Keluarga Berencana	TPN-03.06. Pemberdayaan Keluarga	Layanan Konsultasi Keluarga	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.03. Data Pemberdayaan Perempuan
Data-063	Data Alat dan Obat Kontrasepsi	Data Alat dan Obat Kontrasepsi	Terbatas	Text	Realtime	Dinas Pengendalian Penduduk dan Keluarga Berencana	TPN-03.06. Pemberdayaan Keluarga	Layanan Keluarga Berencana	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.03. Data Pemberdayaan Perempuan
Data-064	Data Kampung KB	Data Statistik Kampung KB	Terbatas	Text	Realtime	Dinas Pengendalian Penduduk dan Keluarga Berencana	TPN-03.06. Pemberdayaan Keluarga	Layanan Keluarga Berencana	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.03. Data Pemberdayaan Perempuan
Data-065	Data Retribusi Pasar	Data Retribusi Pasar	Terbatas	Text	Harian	Dinas Perdagangan	TPN-03.04. Pengelolaan Perdagangan	Layanan Retribusi Pelayanan Pasar Dan Pelayanan Persampahan/Kebersihan Pasar	RAD 02. Informasi Ekonomi dan Industri	RAD 02.02. Data Perdagangan
Data-066	Data informasi Lalu Lintas dan Angkutan	Data informasi Lalu Lintas dan Angkutan	Terbuka	Text	Realtime	Dinas Perhubungan	TPN-06.01. Pengelolaan Infrastruktur Dasar	Layanan Informasi Lingkungan Perhubungan Dan Keselamatan	RAD 10. Data Pendukung Umum	RAD 10.03. Data Kewilayahan
Data-067	Data Perikanan	Data Budidaya Perikanan dan Usaha Perikanan	Terbatas	Text	Tahunan	Dinas Perikanan	TPN-04.04. Peningkatan Pertanian Perikanan Dan Peternakan	Layanan Data Informasi Perikanan	RAD 02. Informasi Ekonomi dan Industri	RAD 02.06. Data Perikanan
Data-068	Data Perpustakaan dan Katalog	Data Perpustakaan dan Katalog	Terbatas	Text	Harian	Dinas Perpustakaan dan Kearsipan	TPN-01.02. Fasilitasi SDM Unggul	Layanan Perpustakaan	RAD 09. Informasi Pemerintahan Umum	RAD 09.07. Data Kesekretariatan Negara
Data-069	Data Arsip Statis dan Arsip Dinamis	Data Arsip Statis dan Arsip Dinamis	Terbatas	Text	Harian	Dinas Perpustakaan dan Kearsipan	TPN-12.01. Pengelolaan Kearsipan	Layanan Surat Menyurat Dan Arsip Dinamis	RAD 09. Informasi Pemerintahan Umum	RAD 09.07. Data Kesekretariatan Negara
Data-070	Data Pertanian	Data Pertanian	Terbuka	Text	Harian	Dinas Pertanian	TPN-04.04. Peningkatan Pertanian Perikanan Dan Peternakan	Layanan Pelaksanaan Penyuluhan Pertanian	RAD 02. Informasi Ekonomi dan Industri	RAD 02.03. Data Pertanian
Data-071	Data Perumahan dan Komplek	Data Perumahan dan Komplek	Terbuka	Text	Realtime	Dinas Perumahan Rakyat, Kawasan Permukiman dan Pertanahan	TPN-06.03. Pemanfaatan Tata Ruang	Layanan Peningkatan Kualitas Rumah Tidak Layak Huni	RAD 03. Pembangunan Kewilayahan	RAD 03.04. Data Perumahan

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-072	Data Terpadu Kesejahteraan Sosial	Data Terpadu Kesejahteraan Sosial	Terbatas	Text	Bulanan	Dinas Sosial	TPN-09.01. Peningkatan Kualitas Kehidupan Sosial Keagamaan	Layanan DTKS(Data Terpadu Kesejahteraan Sosial)	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.02. Data Sosial
Data-073	Data Ketenagakerjaan	Data Ketenagakerjaan	Terbuka	Text	Realtime	Dinas Tenaga Kerja	TPN-01.02. Fasilitasi SDM Unggul	Layanan Terpadu Ketenagakerjaan	RAD 06. Informasi Pendidikan dan Tenaga Kerja	RAD 06.02. Data Ketenagakerjaan
Data-074	Data Tindak Lanjut	Data Pelaporan ASN dan tindak lanjut hasil pemeriksaan	Terbatas	Text	Realtime	Inspektorat	TPN-15.01. Penyelenggaraan Pengawasan	Layanan Pelaporan Dan Akuntabilitas	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional
Data-075	Data Medis	Data Medis	Tertutup	Text	Bulanan	RSUD Datu Sanggul	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-076	Data Pasien	Data Pasien	Terbatas	Text	Realtime	RSUD Datu Sanggul	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Pendaftaran Pasien	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-077	Data Produk Hukum	Data Informasi Produk Hukum	Terbuka	Text	Realtime	Sekretariat DPRD	TPN-13.01. Pengelolaan Informasi	Layanan Informasi Produk Hukum	RAD 05. Informasi Ketertiban Umum dan Keselamatan	RAD 05.01. Data Hukum
Data-078	Data TTD Elektronik	Data TTD Elektronik	Terbatas /Tertutup	Text	Realtime	Dinas Komunikasi dan Informatika	TPN-13.03. Pengelolaan Satu Data Indonesia	Layanan Identifikasi Data	RAD 09. Informasi Pemerintahan Umum	RAD 09.03. Data Informasi
Data-079	Data Informasi Keluarga	Data Informasi Keluarga	Terbatas	Text	Realtime	Dinas Pengendalian Penduduk dan Keluarga Berencana	TPN-03.06. Pemberdayaan Keluarga	Layanan Konsultasi Keluarga	RAD 03. Pembangunan Kewilayahan	RAD 03.07. Data Kependudukan
Data-080	Data Harta Kekayaan ASN	Data Harta Kekayaan ASN	Terbatas	Text	Realtime	Badan Kepegawaian dan Pengembangan Sumber Daya Manusia	TPN-08.02. Pengelolaan Kepegawaian	Layanan Profil Kepegawaian	RAD 09. Informasi Pemerintahan Umum	RAD 09.06. Data Aparatur Sipil Negara
Data-081	Data Reformasi Birokrasi	Data Reformasi Birokrasi	Terbatas	Text	Realtime	Bagian Organisasi	TPN-08.01. Peningkatan Tata Kelola Organisasi	Layanan Informasi, Birokrasi Dan Tata Laksana	RAD 09. Informasi Pemerintahan Umum	RAD 09.05. Data Perencanaan Pembangunan Nasional

ID Data	Nama Data	Uraian Data	Sifat Data	Jenis Data	Validitas Data	Produsen Data/Penanggung Jawab Data	Proses Bisnis (Dependency)	Layanan (Dependency)	→ RAD Level 1 (Dependency)	→ RAD Level 2 (Dependency)
Data-082	Data Industri	Data Industri	Terbatas	Text	Realtime	Dinas Perindustrian	TPN-03.03. Pengelolaan Perindustrian	Layanan Produk UMKM	RAD 02. Informasi Ekonomi dan Industri	RAD 02.01. Data Industri
Data-083	Data KKN	Data KKN	Terbatas	Text	Realtime	Inspektorat	TPN-15.01. Penyelenggaraan Pengawasan	Layanan Pelaporan Dan Akuntabilitas	RAD 09. Informasi Pemerintahan Umum	RAD 09.06. Data Aparatur Sipil Negara
Data-084	Data Kesehatan Haji	Data Kesehatan Haji	Terbatas	Text	Realtime	Dinas Kesehatan	TPN-02.01. Pengelolaan Kesehatan Masyarakat	Layanan Kesehatan	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.01. Data Kesehatan
Data-085	Data Ekonomi Sosial	Data Ekonomi Sosial	Terbatas	Text	Realtime	Dinas Perindustrian	TPN-03.03. Pengelolaan Perindustrian	Layanan Informasi, Birokrasi Dan Tata Laksana	RAD 04. Informasi Perlindungan Sosial dan Kesehatan	RAD 04.02. Data Sosial
Data-086	Data Pemerintahan Desa	Data Pemerintahan Desa	Terbatas	Text	Realtime	Dinas Pemberdayaan Masyarakat dan Desa	TPN-14.01. Perencanaan, Pengendalian Dan Evaluasi Pembangunan Daerah	Layanan Informasi Keuangan Desa	RAD 03. Pembangunan Kewilayahan	RAD 03.05. Data Pembangunan Kawasan atau Daerah Tertinggal

B. Analisis Diagram Data

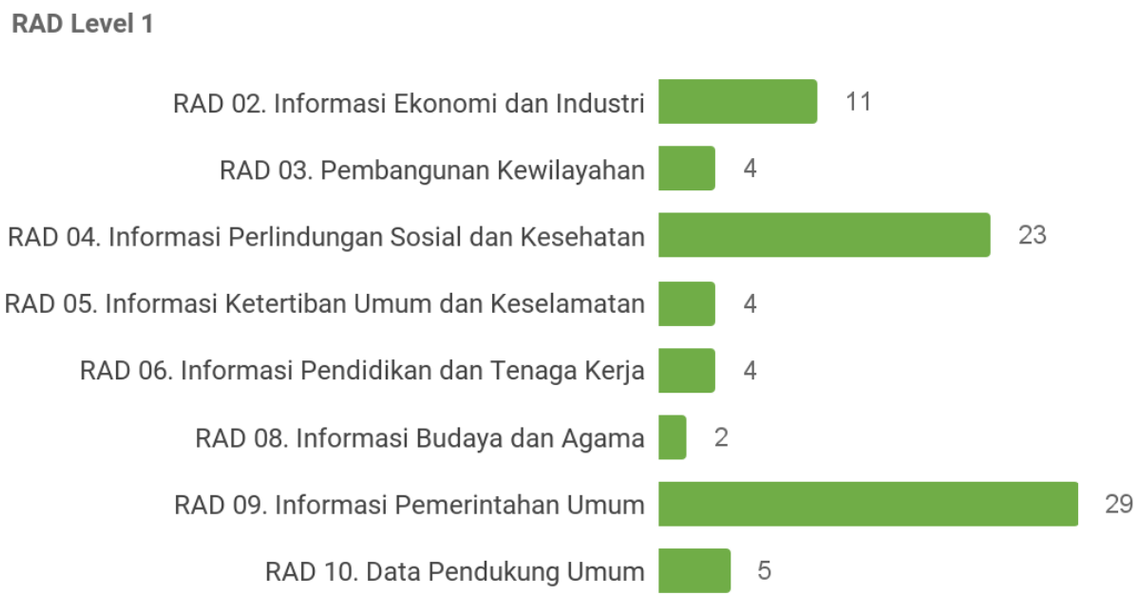
Analisa terhadap kondisi data eksisting dapat dijabarkan sebagai berikut :



Grafik 2.1.1. Kondisi Data eksisting

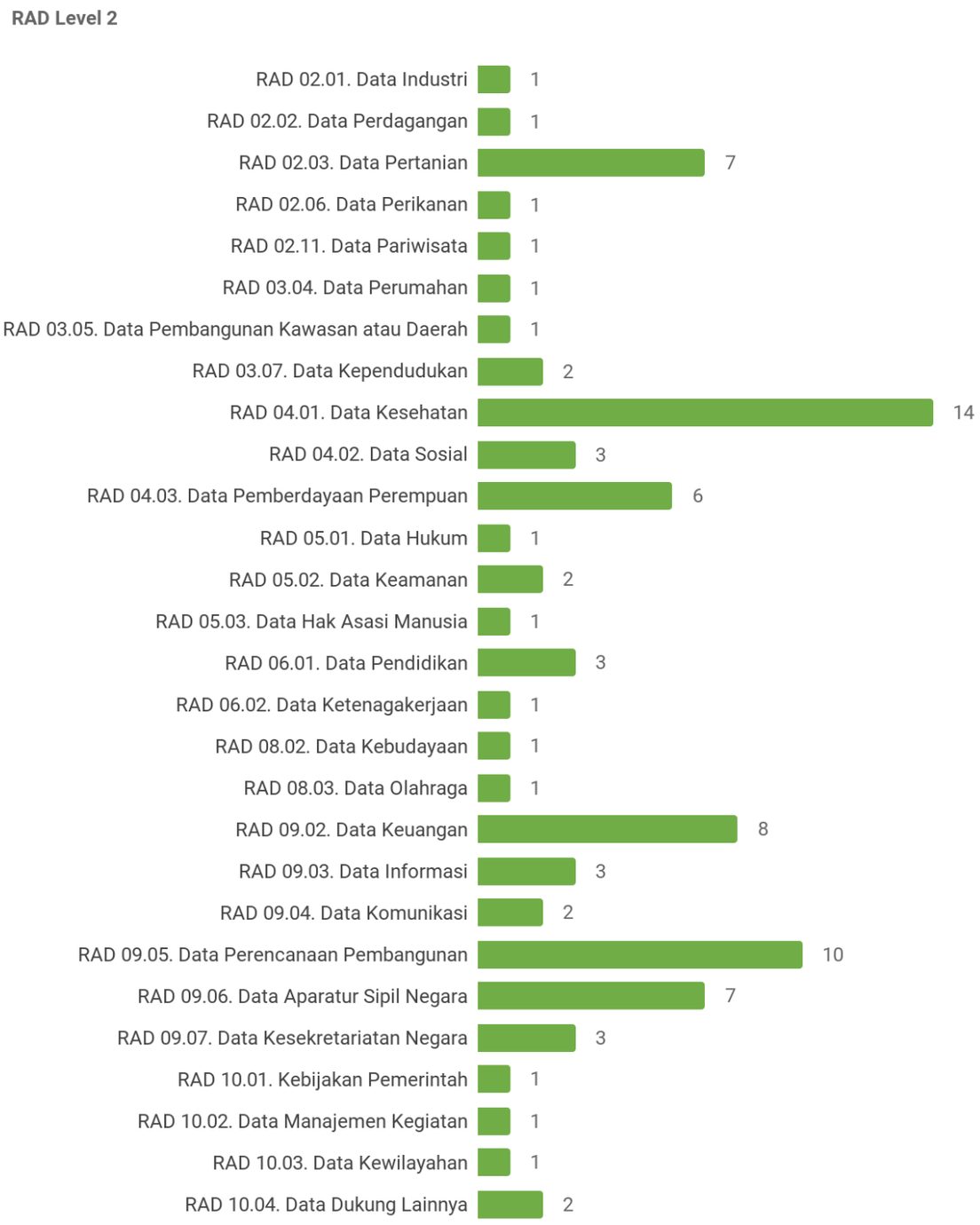
Pada grafik 2.1.1 menunjukkan 2 diagram mengenai kondisi Data eksisting sifat data dan interval data. Terdapat 87 data aplikasi eksisting yang berada di kabupaten Tapin. dari 87 data tersebut terbagi menjadi 3 sifat data dengan 37,2% (32 data) merupakan data yang bersifat terbuka atau dapat dilihat juga oleh publik, 2.3% (2 data) merupakan data yang bersifat tertutup atau rahasia, 60,5% (52 data) merupakan data yang bersifat terbatas, dan terdapat 1 data yang bersifat terbatas/tertutup.

Untuk Interval Update data eksisting di kabupaten Tapin menunjukkan 4 sifat interval data yaitu 47,1% (40 data) merupakan data dengan interval update realtime, 32.9% (28 data) merupakan data dengan interval update harian, 15,3% (13 data) merupakan data dengan interval update bulanan, dan 4,7% (4 data) merupakan data dengan interval update Tahunan.



Grafik 2.1.2. Data Pokok

Untuk Data Pokok penyesuaian dengan Standar Nasional. Dari total 82 data terbagi menjadi beberapa bagian dimana 11 Informasi Ekonomi dan Industri, 4 Informasi Ekonomi dan Industri, 23 Informasi Perlindungan Sosial dan Kesehatan, 4 Informasi Ketertiban Umum dan Keselamatan, 4 Informasi Pendidikan dan Tenaga Kerja, 2 Informasi Budaya dan Agama, 29 Informasi Pemerintahan Umum, dan 5 merupakan Data Pendukung Umum.



Grafik 2.1.3. SKPD Penanggung Jawab Data

Pada Grafik 2.1.3 dapat dilihat SKPD penanggung jawab Data. Terdapat 1 Data Industri, 1 Data Perdagangan, 7 Data Pertanian, 1 Data perikanan, 1 Data Pariwisata, 1 Data Perumahan, 1 Data Pembangunan Kawasan dan Daerah Tertinggal, 2 Data Kependudukan, 14 Data Kesehatan, 3 Data

Sosial, 6 Data Pemberdayaan Perempuan, 1 Data Hukum, 1 Data Hak Asasi Manusia, 3 Data pendidikan, 1 Data Ketenagakerjaan, 1 Dan Kebudayaan 1 Data Olahraga, 8 Data Keuangan, 3 Data Informasi, 2 Data Komunikasi, 10 Data Perencanaan Pembangunan Nasional, 7 Data Aparatur Sipil Negara, 3 Data Kesekretariatan Negara, 1 Data kebijakan Pemerintah, 1 Data Manajemen Kegiatan, 1 Data kewilayahan, dan 2 Data dukung lainnya.

C. Matriks Kewenangan Data (RACI)

Kewenangan dalam memproduksi, mengelola dan pemanfaatan data & informasi pemerintahan perlu dipetakan berdasarkan tugas dan fungsi dari masing-masing perangkat daerah. Sehingga kedepannya manajemen data di Pemerintah Daerah dapat berjalan dengan optimal. Pemetaan ini disajikan dalam bentuk Matriks Kewenangan Data dengan metode RACI (*Responsible*, *Accountable Consulted, Informed*). Penggambaran interoperabilitas data lintas Perangkat Daerah ini menggunakan diagram RACI, dengan penjelasan sebagai berikut:

- *Responsible* (R): Perangkat Daerah yang melakukan aktivitas untuk pemenuhan terhadap data yang didefinisikan.
- *Accountable* (A): Perangkat Daerah yang bertanggung jawab dan memiliki otoritas untuk memutuskan suatu perkara berdasarkan data yang didefinisikan.
- *Consulted* (C): Perangkat Daerah yang memberikan umpan balik atau saran dan berkontribusi akan data yang didefinisikan.
- *Informed* (I): Perangkat Daerah yang perlu tahu (terinformasi) terhadap data yang didefinisikan untuk mendukung tupoksinya.

Adapun matriks kewenangan data ini ditunjukkan pada **lampiran 1**.

2.2. Arsitektur Aplikasi Usulan

A. Katalog Aplikasi Usulan

Katalog aplikasi perlu mempertimbangkan inisiatif yang diusulkan oleh masing-masing SKPD Pemkab. Tapin di masa mendatang. Inisiatif-inisiatif tersebut akan berkembang dan bertambah seiring dengan kebutuhan bisnis proses di masing-masing SKPD. Berikut merupakan pendetailan inisiatif pengembangan aplikasi kedepannya di Pemkab. Tapin.

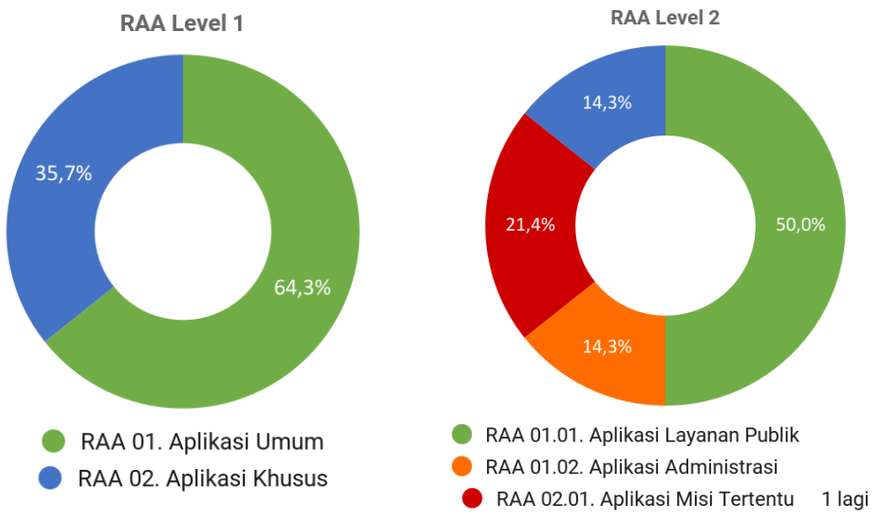
Tabel 2.2.1 Katalog Aplikasi Usulan

ID Aplikasi	Nama Aplikasi	Uraian Aplikasi	Basis Aplikasi	Tipe Lisensi Aplikasi	Nama Basis Data	→ Unit Operasional Teknologi (Dependency)	→ RAA Level 1 (Dependency)	→ RAA Level 2 (Dependency)	→ Data dan Informasi (Dependency)	→ Layanan (Dependency)
APPU-001	Sistem Informasi Profil Dinas Kesbangpol	SIstem Informasi Profil Dinas Kesbangpol	Web Based	Open Source	MySql	Badan Kesatuan Bangsa dan Politik	RAA 02. Aplikasi Khusus	RAA 02.02. Aplikasi Fungsi Tertentu	Data Profil Dinas, Kegiatan, Berita	Layanan Informasi Profil Dinas
APPU-002	Pengembangan Sistem Informasi Logistik	Pengembangan Sistem Informasi Logistik untuk Data Barang	Web Based	Open Source	MySql	Badan Penanggulangan Bencana Daerah	RAA 01. Aplikasi Umum	RAA 01.01. Aplikasi Layanan Publik	Data Logistik	Layanan Informasi dan Bantuan Logistik Kebencanaan
APPU-003	Sistem Informasi Sertifikasi Beras	Aplikasi Layanan Sertifikasi Beras yang berfungsi untuk memudahkan masyarakat dalam membuat sertifikasi penjualan beras	Web Based	Open Source	MySql	Dinas Ketahanan Pangan	RAA 02. Aplikasi Khusus	RAA 02.02. Aplikasi Fungsi Tertentu	Data Keamanan Pangan	Layanan Informasi Data Harga Pangan, Keamanan Pangan, Pengisian Lumbung Gabah, Dan Keamanan Pangan
APPU-004	Pengembangan e-SAKIP	e-SAKIP v2	Web Based	Open Source	MySql	Dinas Komunikasi dan Informatika	RAA 01. Aplikasi Umum	RAA 01.02. Aplikasi Administrasi Pemerintahan	Data Akuntabilitas Kinerja	Layanan Pelaporan Dan Akuntabilitas
APPU-005	Pengembangan Sipenari	Aplikasi pengelola pajak	Mobile	Open Source	MySql	Dinas Komunikasi dan	RAA 02. Aplikasi	RAA 02.02. Aplikasi	Data Pajak Retribusi	Layanan Pajak

	Japin	dan retribusi daerah				Informatika	Khusus	Fungsi Tertentu	Daerah	Daerah
APPU-006	Sistem Informasi Profile DP3A	Sistem Informasi Profile DP3A	Web Based	Open Source	MySql	Dinas Pemberdayaan Perempuan dan Perlindungan Anak	RAA 02. Aplikasi Khusus	RAA 02.01. Aplikasi Misi Tertentu	Data Perkawinan Usia Di Bawah Umur, Data Usaha Rumahan, Data Kekerasan Pada Perempuan	Layanan Kesejahteraan Sosial
APPU-007	Sistem Informasi Profil Dispora	Data informasi dinas	Web Based	Open Source	MySql	Dinas Pemuda dan Olahraga	RAA 01. Aplikasi Umum	RAA 01.01. Aplikasi Layanan Publik	Data Kepemudaan dan Olahraga	Layanan Informasi Profil Dinas
APPU-008	Sistem Informasi Profile Dinas Pendidikan	Informasi dinas pendidikan	Web Based	Open Source	MySql	Dinas Pendidikan	RAA 01. Aplikasi Umum	RAA 01.01. Aplikasi Layanan Publik	Data Pendidikan dan Tenaga Kependidikan	Layanan Informasi Profil Dinas
APPU-009	Sistem Informasi Pembinaan Kader	Website pembinaan kader	Web Based	Open Source	MySql	Dinas Pengendalian Penduduk dan Keluarga Berencana	RAA 02. Aplikasi Khusus	RAA 02.01. Aplikasi Misi Tertentu	Data Keluarga Berencana	Layanan Informasi Kepemerintahan, Informasi Sosial Kemasyarakatan
APPU-010	Sistem Informasi Profile Dinas Perhubungan	Data informasi dinas	Web Based	Open Source	MySql	Dinas Perhubungan	RAA 01. Aplikasi Umum	RAA 01.01. Aplikasi Layanan Publik	Data Profil Dinas, Kegiatan, Berita	Layanan Informasi Profil Dinas
APPU-011	Sistem Informasi Profile Dinas Perikanan	Informasi dinas	Web Based	Open Source	MySql	Dinas Perikanan	RAA 01. Aplikasi Umum	RAA 01.01. Aplikasi Layanan Publik	Data Profil Dinas, Kegiatan, Berita	Layanan Informasi Profil Dinas
APPU-012	Sistem Informasi Profile Dinas Perindustrian	Informasi kegiatan dan berita dinas	Web Based	Open Source	MySql	Dinas Perindustrian	RAA 01. Aplikasi Umum	RAA 01.01. Aplikasi Layanan Publik	Data Profil Dinas, Kegiatan, Berita	Layanan Informasi Profil Dinas
APPU-013	Sistem Informasi Profil Dinas Perpustakaan dan Kearsipan	Informasi dinas	Web Based	Open Source	MySql	Dinas Perpustakaan dan Kearsipan	RAA 01. Aplikasi Umum	RAA 01.01. Aplikasi Layanan Publik	Data Profil Dinas, Kegiatan, Berita	Layanan Informasi Profil Dinas
APPU-014	Sistem Informasi Pemindaian Keabsahan Data	Keabsahan pindai data	Web Based	Open Source	MySql	Rumah Sakit Umum Daerah	RAA 01. Aplikasi Umum	RAA 01.02. Aplikasi Administrasi Pemerintahan	Data Identifikasi TIK	Layanan Identifikasi Data
APPU-015	Sistem Informasi Jadwal Kegiatan DPRD	Jadwal kegiatan atau rapat DPRD	Mobile	Open Source	MySql	Sekretariat DPRD	RAA 02. Aplikasi Khusus	RAA 02.01. Aplikasi Misi Tertentu	Data Profil Dinas, Kegiatan, Berita	Layanan Profil Kepegawaian

B. Analisis Diagram Aplikasi Usulan

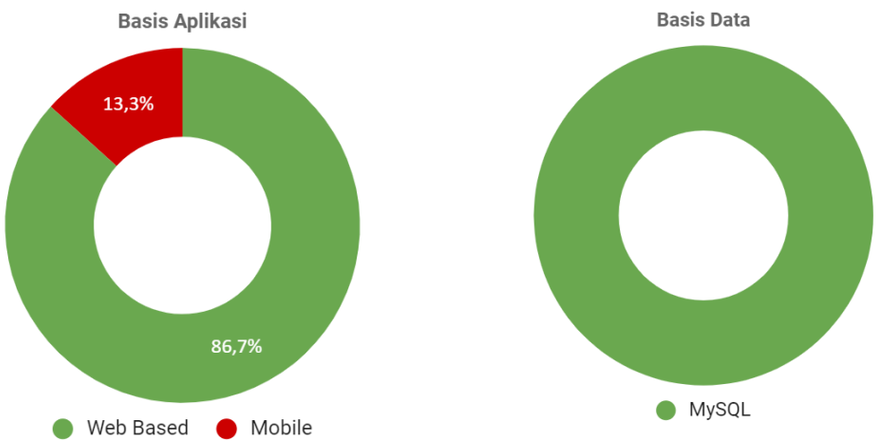
Analisa terhadap kondisi aplikasi eksisting dapat dijabarkan sebagai berikut:



Grafik 2.2.1 Referensi Arsitektur Aplikasi

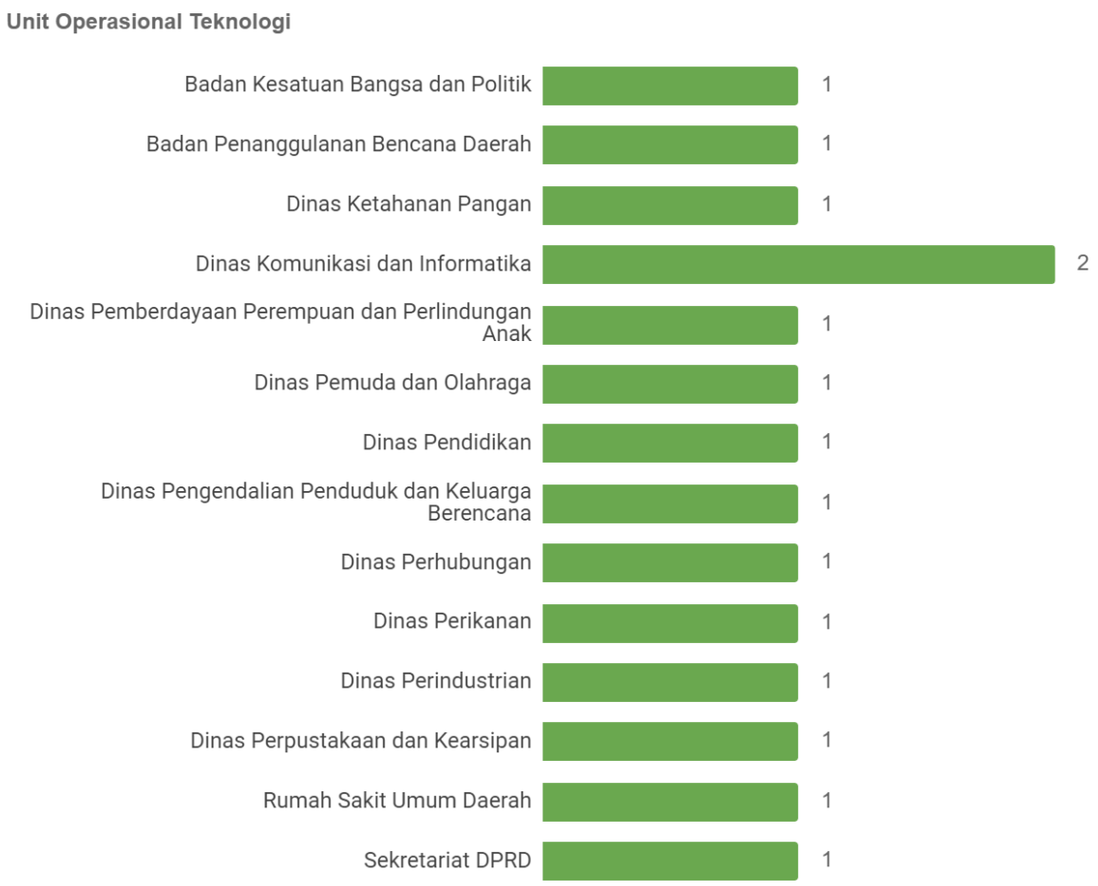
Grafik 2.2.1 menunjukkan referensi arsitektur aplikasi usulan pada RAA Level 1 dan RAA Level 2. Dari grafik tersebut dapat dilihat bahwa sesuai dengan Referensi Arsitektur Level 1 terdapat 14 aplikasi usulan. 14 Aplikasi tersebut terbagi menjadi 2, 64,3% merupakan RAA 01. Aplikasi Umum dan 35,7% merupakan RAA 02. Aplikasi Khusus.

Untuk Referensi Arsitektur Level 2 Aplikasi usulan terbagi menjadi empat yaitu 50,0% (7 Aplikasi) merupakan RAA 01.01 Aplikasi Layanan Publik, 14,3% (2 Aplikasi) merupakan RAA 01.02 Aplikasi Administrasi Pemerintahan, 21,4% (3 Aplikasi) merupakan Aplikasi RAA 02.01 Misi Tertentu, dan yang terakhir 14,3% (2 Aplikasi) merupakan Aplikasi RAA 02.02 Fungsi Tertentu di Perangkat Daerah.



Grafik 2.2.2 Kondisi Teknologi Sistem Informasi (ii)

Kemudian untuk Basis aplikasi yang digunakan dalam aplikasi usulan terdapat 2 basis. 86,7%(39 Aplikasi usulan) menggunakan web based dan 13,3%(2 Aplikasi usulan) menggunakan aplikasi berbasis Mobile. Sedangkan untuk basis yang digunakan sebagai aplikasi usulan menggunakan satu basis data yaitu MySQL.



Grafik 2.2.3 SKPD Pengelola Aplikasi Usulan

Pada Grafik 3.5.4 dapat dilihat SKPD Pengelola Aplikasi Usulan. Untuk Badan Kesatuan Bangsa dan Politik, Badan Penanggulangan Bencana Daerah, Dinas Ketahanan Pangan, Dinas Pemberdayaan Perempuan dan Perlindungan Anak, Dinas Pemuda dan Olahraga, Dinas Pendidikan, Dinas Pengendalian Penduduk dan Keluarga Berencana, Dinas Perhubungan, Dinas Perikanan, Dinas Perindustrian, Dinas Perpustakaan dan Kearsipan, Rumah Sakit Umum Daerah, dan Sekretariat DPRD memiliki masing masing satu usulan aplikasi. Kemudian untuk Dinas Komunikasi dan Informatika memiliki 2 aplikasi Usulan Aplikasi.

C. Analisis Effort Impact

Usulan perencanaan teknologi informasi yang direkomendasikan dapat dijadikan dasar untuk pengelolaan teknologi informasi yang sesuai dengan kebutuhan perusahaan dan memberikan arah bagi pengembangan teknologi informasi yang mampu memberikan kontribusi positif bagi penyelesaian berbagai permasalahan pemerintah di Kabupaten Tapin.

Berdasarkan usulan kebutuhan aplikasi yang telah dijelaskan sebelumnya. Selanjutnya perlu dilakukan analisis untuk strategi implementasinya dengan pertimbangan arahan strategis dan kapabilitas anggaran Kabupaten Tapin. 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 2.2.1. Matriks Effort - Impact

2.3. Arsitektur Infrastruktur dan Keamanan

A. Tren Teknologi dan Praktek Terbaik (Best Practice)

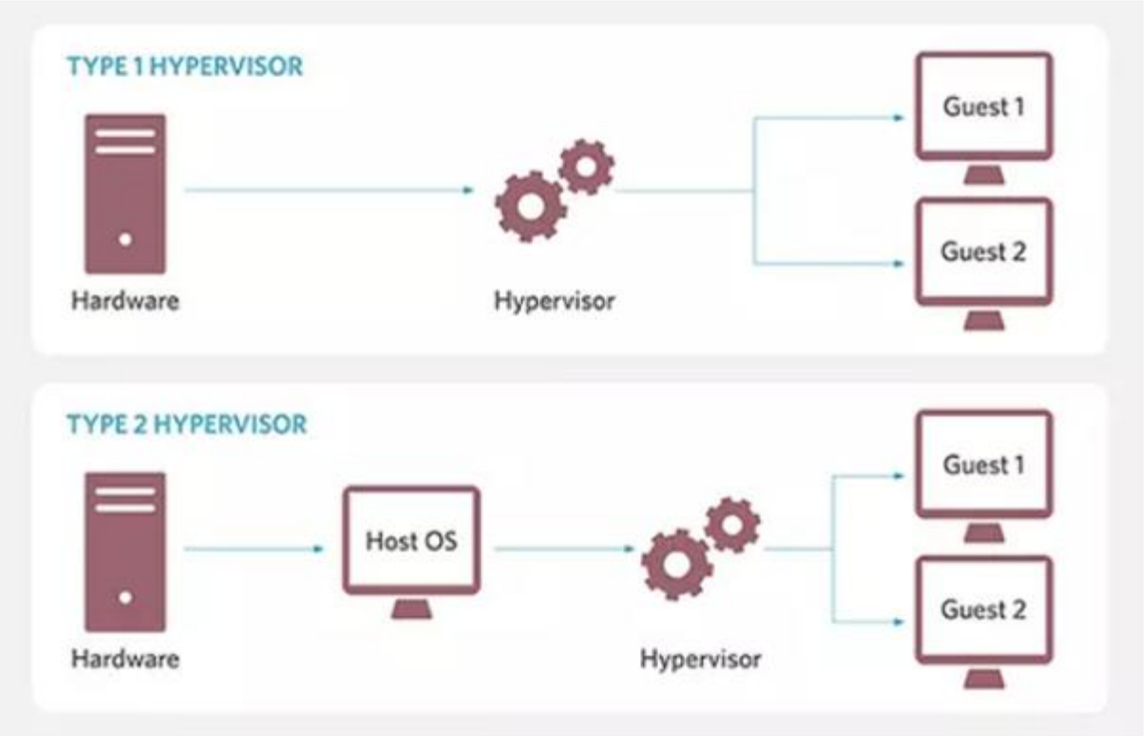
1. Teknologi Virtualisasi

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

Dalam sebuah server fisik bisa dibuat banyak virtual server, 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 server fisik dapat dimanfaatkan secara optimal karena kita bisa menginstall beberapa sistem operasi yang akan dikonfigurasi menjadi server sesuai kebutuhan tanpa membeli hardware baru.

Untuk mendukung implementasi virtualisasi server, CPU dari sebuah server harus mendukung teknologi virtualisasi, dan hardware saat ini sudah mendukung teknologi virtualisasi bahkan untuk komputer biasa pun sudah mendukung teknologi virtualisasi.

Dalam teknologi virtualisasi sebuah server dipecah ke dalam virtual environment, dan setiap virtual environment dapat diinstall sistem operasi yang berbeda dari sistem operasi server fisik atau sistem operasi dari virtual environment lainnya. Ketika virtual environment berjalan dia tidak tahu tentang resource yang digunakan 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 server yang mengimplementasikan teknologi virtualisasi untuk mengatur virtual environment.



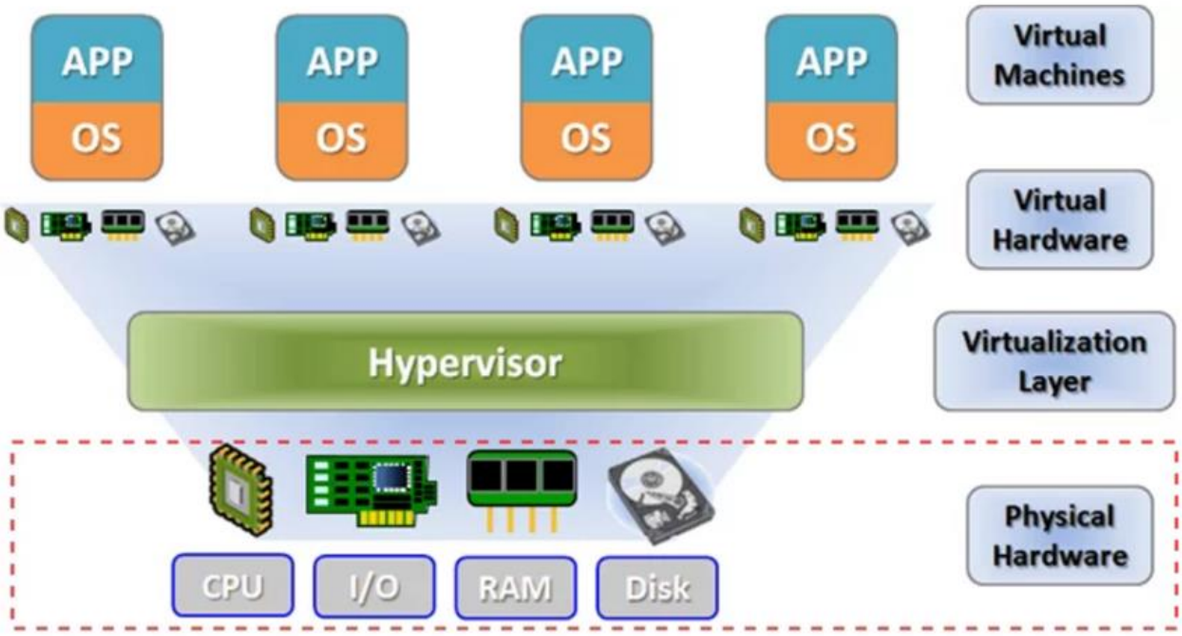
Gambar 2.3.1. Dua Jenis Hypervisor

Terdapat 2 jenis Hypervisor dalam dunia virtualisasi saat ini (Error! Reference source not found.) :

1. 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 XenServer, Hyper-V,V Mware vSphere/ESXi.
2. Hypervisor Tipe 2 (Hosted Hypervisor)
   Jenis Hypervisor ini memerlukan sistem operasi untuk berjalan, karena jenis hyper visor ini berjalan diatas sistem operasi. Contoh Hypervisor Type 2 diantaranya : Vmware Work station, VMware Player, dan Virtualbox.

a. Virtualisasi Server

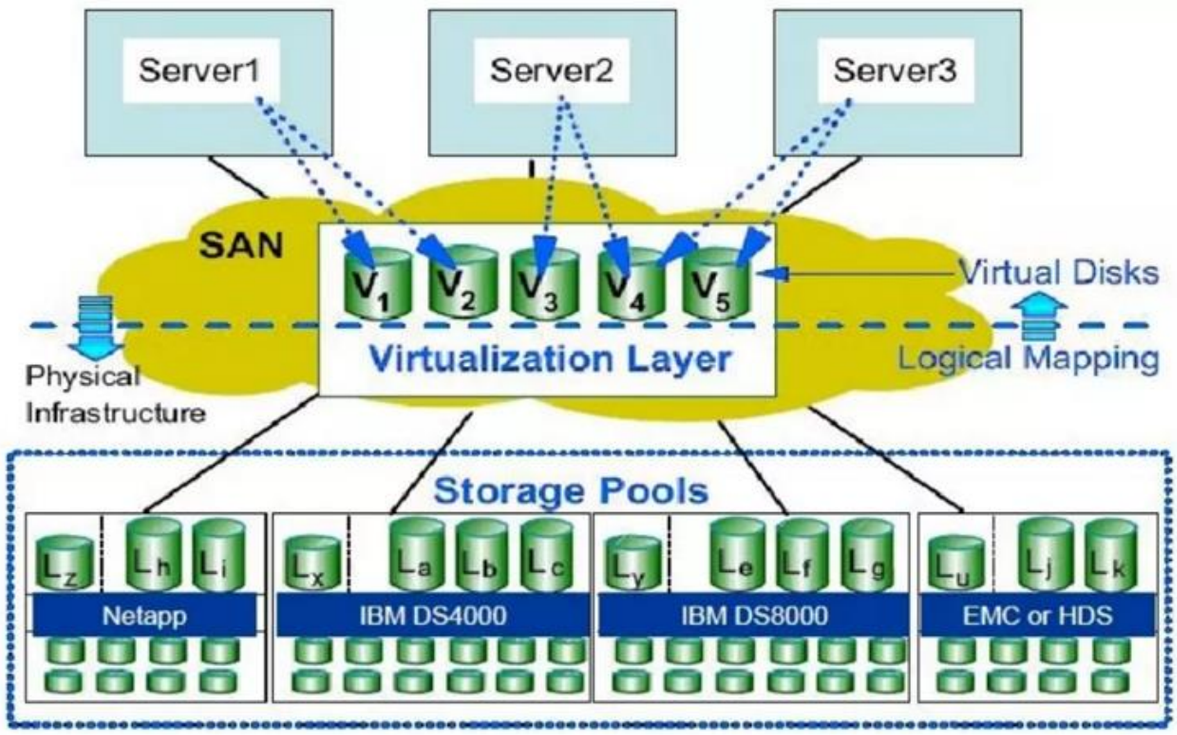
Adalah penggunaan teknologi virtualisasi dengan tujuan untuk memecah resource fisik server kedalam beberapa virtual server yang nantinya akan diinstall berbagai macam sistem operasi sesuai kebutuhan atau bisa juga virtual server ini dijual /disewakan oleh pihak hosting. Kita sering mendengarnya dengan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



Gambar 2.3.2. Lapisan – lapisan Teknologi Virtualisasi Server

b. 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 user bisa mengakses storage kapanpun dan dimanapun.

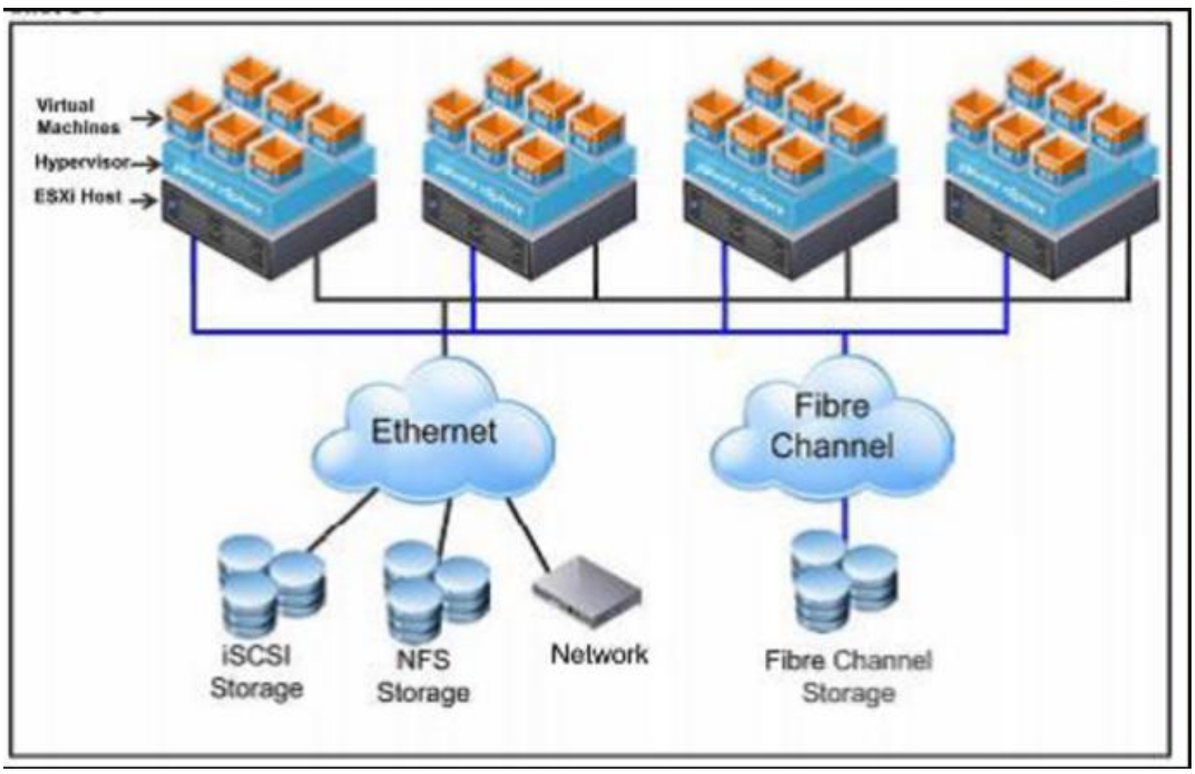


Gambar 2.3.3. Virtualisasi Storage

c. Virtualisasi Data Center

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

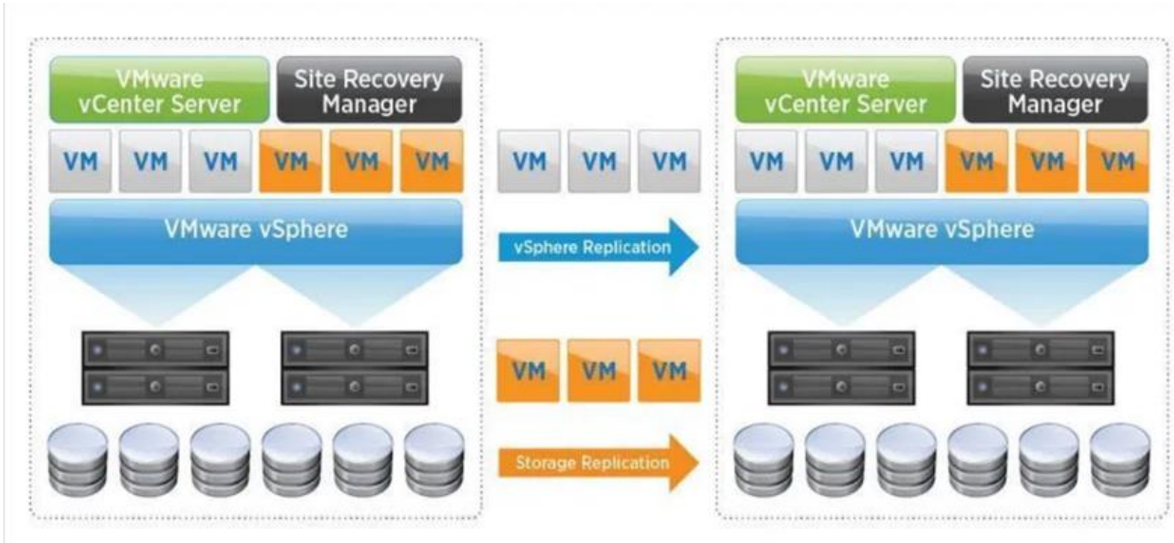
Virtualisasi memudahkan dalam perancangan pusat data dengan tingkat ketersediaan yang tinggi (high-availability) dengan teknik clustering, redundansi, dan replikasi.



Gambar 2.3.4. Topologi Virtualisasi Server dan Storage di Pusat Data

d. Virtualisasi DC-DRC

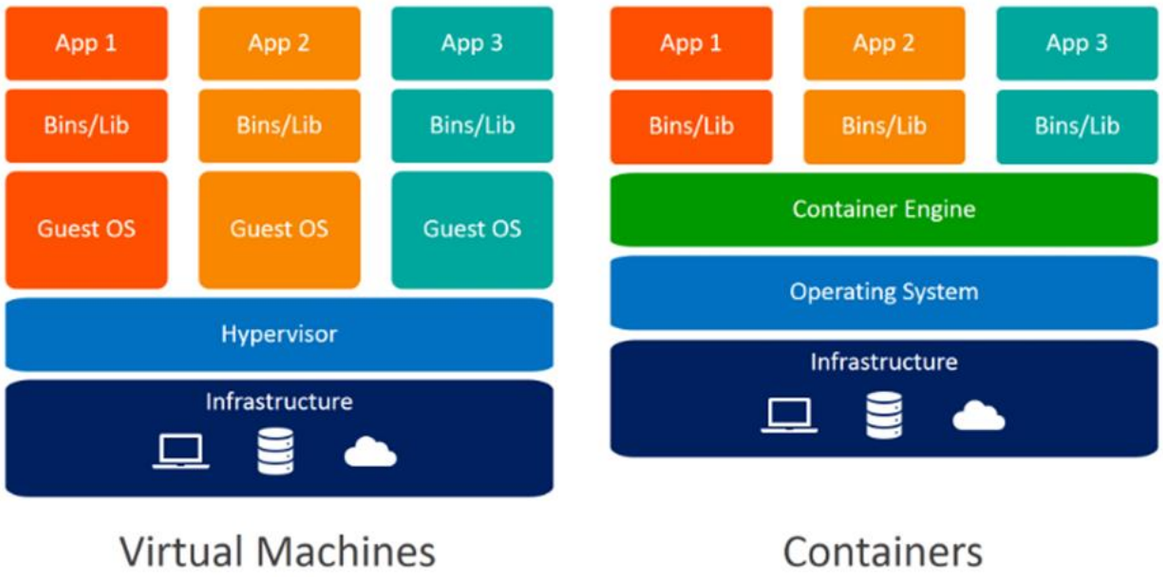
Penggunaan teknologi virtualisasi di DC dan DRC akan memudahkan dalam proses backup, replikasi, dan migrasi server dan aplikasi. Virtualisasi juga memudahkan dalam melakukan scale-up atau scale-down server sesuai dengan kebutuhan bisnis.



Gambar 2.3.5. Replikasi Server di DC-DC dengan Teknologi Virtualisasi

e. Container

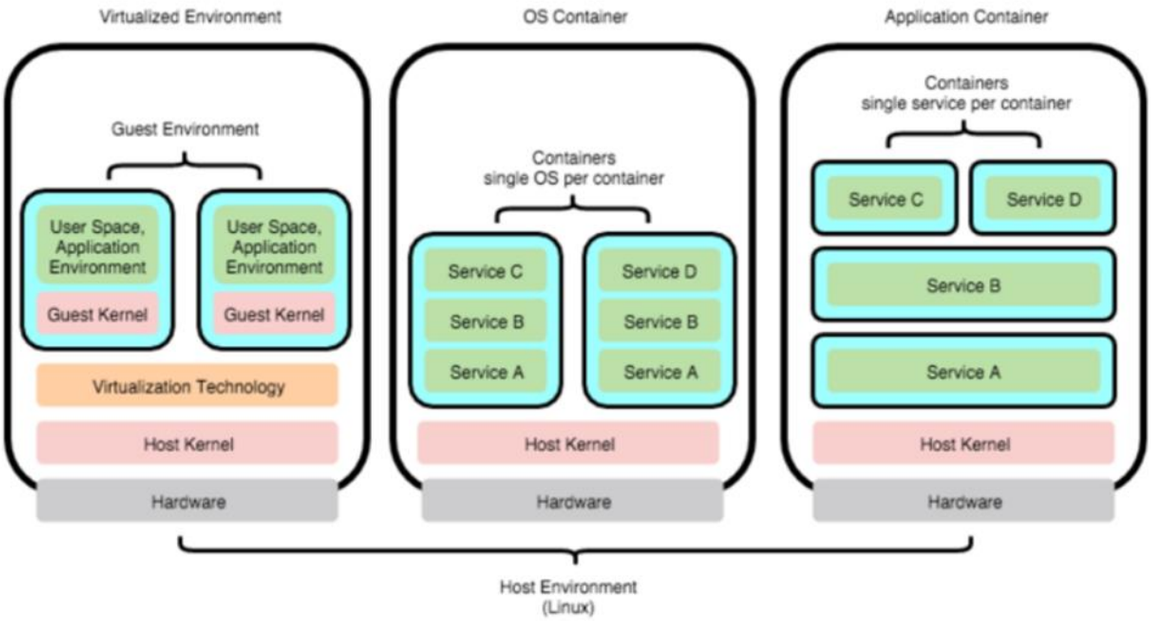
Perkembangan dari teknologi virtualisasi yakni container yang mengenkapsulasi aplikasi dengan dependensinya sehingga dapat memberikan sistem yang terisolasi (isolated environment) pada level OS yang dijalankan pada satu induk linux kernel (host). Teknologi container merubah cara mengembangkan, mendistribusikan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



Gambar 2.3.6. Perbandingan Teknologi Virtual Machines dan Containers

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

a. Kontainer berbasis sistem operasi (OS Container), yakni kontainer yang memberikan isolasi pada level sistem operasi dan memanfaatkan kernel yang sama dari suatu induk, contohnya adalah LXC, OpenVZ, Linux VServer, BSD Jails and Solaris zones.
b. Kontainer berbasis aplikasi (Application Container), yakni kontainer yang memberikan isolasi pada level aplikasi dengan memanfaatkan beberapa komponen yang ada pada sistem operasi induk, ditambah beberapa komponen pada kontainer-kontainer lain yang menjadi basis dari berjalannya sebuah aplikasi, contohnya adalah Docker dan Rocket (rkt).



Gambar 2.3.7. Perbandingan Teknologi Virtualisasi dan Container (sumber: https://blog.andi.dirgantara.co/teknologi-kontainer-pengantar-pengenalan-docker-706eafe03269)

Virtualisasi

Pada lingkungan virtualisasi, penyedia aplikasi virtualisasi melakukan abstraksi untuk lapisan hardware dan kernel, sehingga mesin yang berjalan pada virtualisasi seolah-olah merupakan mesin terpisah yang hanya memanfaatkan hardware yang tersedia pada lingkungan induk dengan kernelnya sendiri.

Kontainer berbasis Sistem Operasi

Kontainer berbasis sistem operasi merupakan teknologi kontainer yang memperlakukan kontainer-kontainer di dalamnya sebagai satu kesatuan sistem secara utuh seolah-olah dalam satu sistem operasi tersendiri secara terisolasi.

Teknologi ini banyak dipakai sebagai infrastruktur pada shared hosting dan virtual private server karena sifatnya yang high performance serta memiliki lingkungan yang terisolasi antara kontainer satu dengan yang lain.

Kontainer berbasis Aplikasi

Kontainer berbasis aplikasi adalah teknologi yang belakangan ini ramai diperbincangkan, karena adanya vendor yakni Docker yang menawarkan teknologi ini dengan fitur-fitur tambahan yang sangat mudah dan nyaman digunakan, khususnya bagi development and operations (dev ops).

Kontainer berbasis aplikasi ini sangat cocok untuk desain arsitektur sistem dengan pendekatan microservice, karena masing-masing service memiliki lingkungan yang terisolasi namun tetap dapat berkomunikasi satu sama lain.

Penggunaan teknologi container mempunyai banyak keuntungan, antara lain:

a. Ringan

Container menyediakan virtualisasi yang berbeda konsep dengan virtualisasi perangkat keras yang tersedia di VM. Menggunakan host dan kernel yang sama container berbagi manajemen memori, management proses, I/O dll, sementara proses pada tiap kontainer terisolasi dan mempunyai dependensi terpisah.

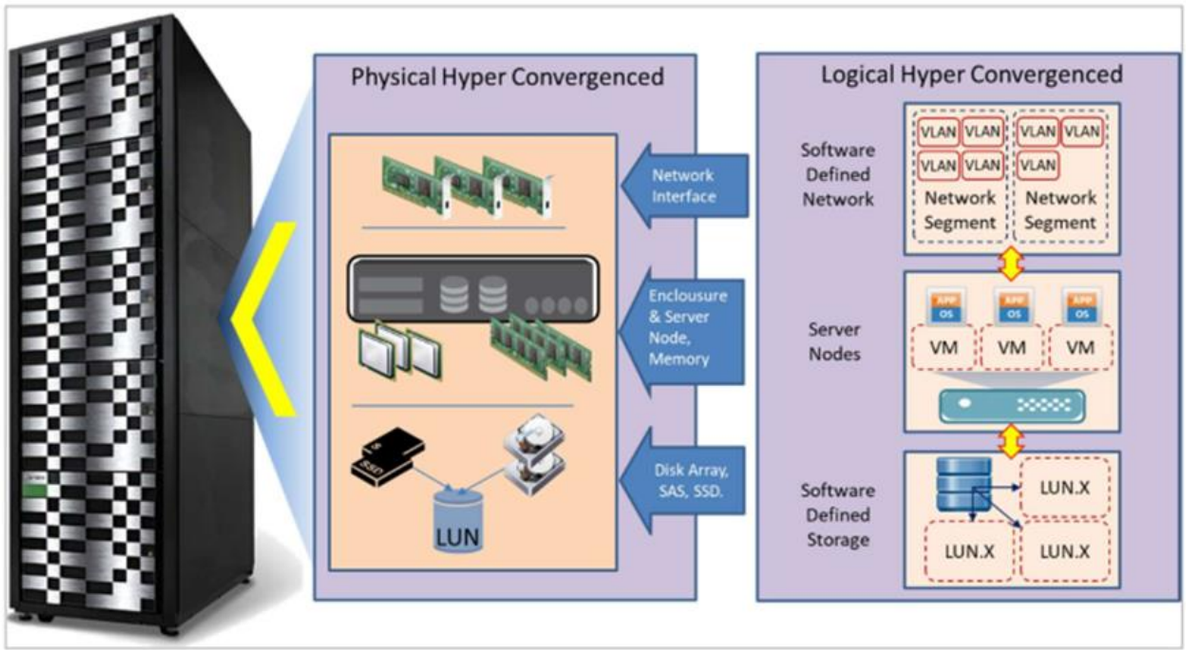
b. Kinerja Maksimal
   Karena container dikelola pada host yang sama, proses pada container dijalankan dengan kinerja sama seperti host, setiap proses yang dijalankan dalam container sebenarnya adalah proses dalam host yang di isolasi.
c. Konsumsi Sumber Daya Lebih Rendah
   Karena container tidak membutuhkan virtualisasi perangkat keras yang penuh, satu host dapat mempunyai banyak container dibanding VM.
d. Cepat
   Proses booting dalam kontainer hampir sama dengan proses booting pada host, dibanding virtual machine yang menjalankan proses tunggal namun harus melakukan booting pada sistem operasi secara penuh.

2. Hyper Converged Infrastructure (HCI) Server

Teknologi hyper-convergence ini menggabungkan teknologi jaringan (network), teknologi server 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 konsol 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.

Dalam console enclosure 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 server, enclosure ini menyediakan x86-based servers 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 2.3.8. Arsitektur Server Hyper Converged Infrastructure (HCI)

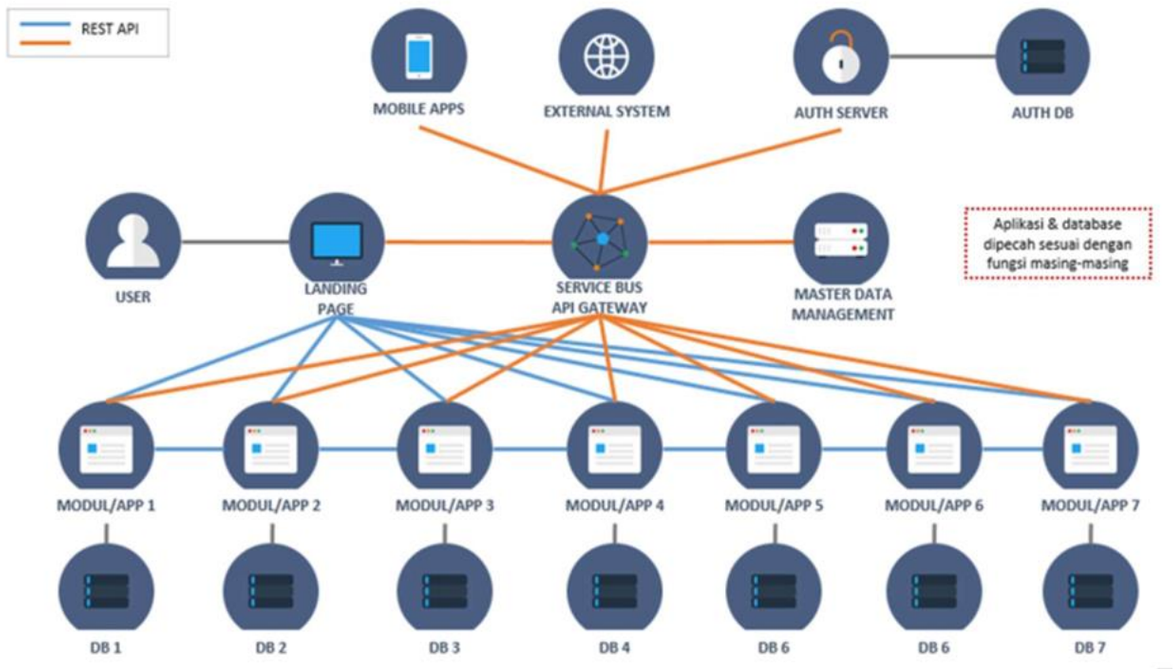
3. *Microservices*

Secara sederhana, arsitektur aplikasi microservices ini menggunakan desain yang memecah aplikasi berdasarkan fungsinya secara spesifik. Tidak sekedar dengan 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 itu 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. Alih-alih berbagi skema database tunggal dengan services lainnya, masing-masing services memiliki skema database tersendiri. Di satu sisi, pendekatan ini bertentangan dengan gagasan model data enterprise-wide. Selain itu, sering kali menghasilkan duplikasi beberapa data. Namun, 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.

Pada intinya microservices yaitu 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. Dimana 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 akan dibangun dengan menggunakan arsitektur microservices dimana setiap modul yang dimiliki akan dibangun engine masing-masing dan memiliki basis data masing masing, sehingga akan berdampak terhadap peningkatan kinerja aplikasi yang signifikan. Di samping itu keamanan aplikasi akan lebih terjamin dengan melakukan pengamanan aplikasi melalui REST API, sehingga transaksi dan pertukaran data yang dilakukan akan lebih terjaga.



Gambar 2.3.9. Arsitektur Microservices

Kelebihan Arsitektur Microservices meliputi:

1. Komponen Terpisah

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

2. Pemahaman yang Lebih Mudah

   Dibagi menjadi komponen yang lebih kecil dan lebih sederhana, aplikasi microservices lebih mudah dipahami dan dikelola. Developer aplikasi hanya berkonsentrasi pada layanan spesifik yang terkait dengan tujuan bisnis yang telah ditentukan sebelumnya.

3. Skalabilitas yang Lebih Baik

   Keuntungan lain dari pendekatan microservices adalah bahwa setiap elemen dapat diskalakan secara independen. Jadi seluruh proses lebih efektif dari segi biaya dan waktu dibandingkan dengan dengan monolith ketika seluruh aplikasi harus ditingkatkan meskipun tidak diperlukan. Selain itu, setiap monolitik arsitektur memiliki batasan dalam hal skalabilitas, sehingga semakin banyak, maka semakin banyak masalah yang berpotensi muncul. Oleh karena itu, banyak perusahaan, akhirnya membangun kembali arsitektur monolitik mereka.

Kekurangan Arsitektur Microservices meliputi:

1. Kompleksitas Ekstra

   Karena arsitektur layanan microservices adalah sistem terdistribusi, maka harus memilih dan mengatur koneksi antara semua modul dan database. Juga, selama aplikasi tersebut termasuk layanan independen, semuanya harus dikerahkan secara independen.

2. Distribusi Sistem

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

3. Cross-Functional Bertambah

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

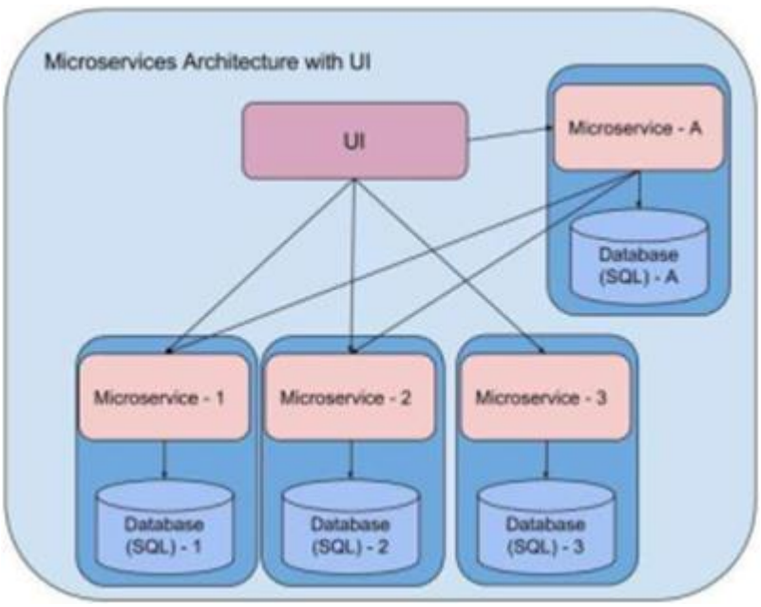
4. Pengujian

   Sejumlah besar komponen yang dapat digunakan secara terpisah membuat pengujian solusi berbasiskan layanan jauh lebih sulit.

Arsitektur Pangkalan Data (Database) Microservices

Arsitektur basis data yang akan diterapkan pada arsitektur aplikasi microservices adalah menggunakan two-tier architecture, dimana dalam setiap modul aplikasi tersebut memiliki pangkalan

data masing-masing sesuai dengan perannya, seperti terlihat pada gambar berikut:



Gambar 2.3.10. Arsitektur Pangkalan Data Microservices

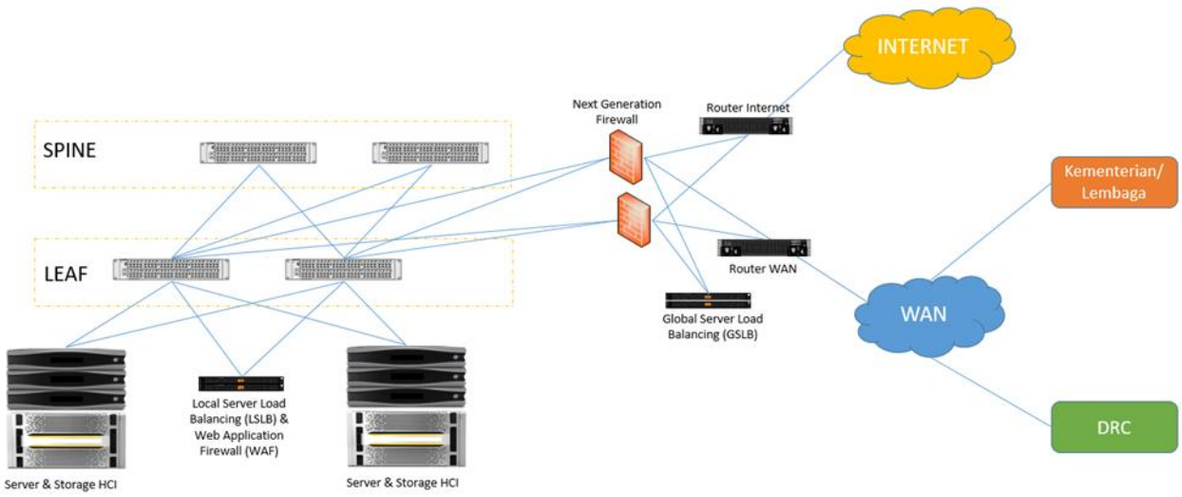
4. Arsitektur Network Spine-Leaf Datacenter

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 server dan terhubung langsung ke Spine Layer atau jaringan inti. Switch Spine – Leaf menghubungkan semua switch leaf dalam topologi penuh ke switch core.

Dengan prevalensi infrastruktur cloud dan container di pusat data modern, lalu lintas jaringan terus meningkat. Lalu lintas di jaringan bergerak menyamping dari satu server ke server lainnya.

Perubahan ini terutama disebabkan oleh fakta bahwa aplikasi modern memiliki komponen yang didistribusikan di lebih banyak server atau mesin virtual.

Dengan latensi rendah, lalu lintas jaringan yang dioptimalkan sangat penting untuk kinerja jaringan, terutama untuk aplikasi yang sensitif terhadap waktu atau intensif data. Arsitektur Lapisan Spine – Leaf membantu hal ini dengan memastikan bahwa lalu lintas selalu mengambil jumlah lompatan yang sama dari tujuan berikutnya, sehingga memprediksi latensi yang lebih rendah.



Gambar 2.3.11. Arsitektur Network Spine-Leaf Datacenter

5. 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 yang tidak efektif untuk memaksa otorisasi hak akses bekerja sesuai fungsinya. Misalnya, apabila *user* berhasil melewati halaman *login*, mereka 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 bagaimana web aplikasi memberikan akses fungsi ataupun konten kepada beberapa user, dan tidak kepada user yang lain. Proses ini terjadi setelah otentikasi atau lebih umum dikenal dengan proses login.

   Kebanyakan Access Control tidak dibentuk dan di desain jadi dari awal melainkan adalah berkembang mengikuti website nya sendiri. Dalam hal ini aturan dari Access control

disisipkan pada setiap fungsi mengikuti berkembangnya suatu website. Pada akhir pengembangan fungsi dari access control akan terkumpul dan rumit sehingga sulit untuk 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*, dikarenakan data yang tidak terenkripsi kerap kali data tersebut dimanfaatkan oleh *attacker* untuk mengakses data yang lebih tinggi lagi.

c. A03:2021-Injection
Sistem / program memproses sebuah data yang tidak valid, yang mengakibatkan attacker dapat menginputkan kode tertentu kepada program lalu kode tersebut akan membuat program menjalankan perintah yang salah.

d. A04:2021-Insecure Design
Sebuah kerentanan yang berfokus pada kelemahan pada konsep / desain dari sebuah arsitektur program, sebelum melakukan koding, pengembang diharuskan menerapkan beberapa prinsip salah satunya adalah *Secure By Design*.

Secure By Design dalam dunia software engineering adalah sebuah software yang seharusnya memiliki kapabilitas di design cukup aman secara fundamental.

Attacker mendapatkan sebuah informasi sensitif yang terdapat pada pesan error, hal tersebut terjadi dikarenakan pengembang tidak menggunakan error handler dengan baik.

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

e. A05:2021-Security Misconfiguration
Pengembang tidak mengikuti dokumentasi sebuah library, framework atau komponen aplikasi, tidak menerapkan standar konfigurasi yang ada, maka aplikasi tersebut akan memiliki beberapa lobang kecil yang akan bisa dimanfaatkan oleh attacker.

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 untuk 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 server/aplikasi tidak termonitoring dengan baik, biasanya disebabkan karena log management yang buruk, log yang tidak terformat dengan baik, namun ada halnya faktor human error, ketika SOC team tidak melakukan pemeriksaan lanjutan atau melakukan analisis log secara proaktif terhadap alert.

j. A10:2021-Server-Side Request Forgery
Sebuah kerentanan yang disebabkan oleh 2 layer (aplikasi & network) dimana request URL oleh user diizinkan untuk berinteraksi langsung melewati firewall dengan internal network, yang menyebabkan permintaan URL apapun ke internal network dari user akan diproses oleh Internal network, begitu pula dari sisi internal network tidak melakukan validasi data apa yang direquest oleh user, hal tersebut mengakibatkan request URL external dapat diproses oleh internal network.

B. Infrastruktur SPBE

1. Prinsip – prinsip Pengembangan Infrastruktur Teknologi Informasi

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

a. Pengembangan Kapasitas (*Scalable)*
Kemampuan infrastruktur TI Diskominfo Kabupaten Tapin 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 akan tuntutan bisnis tersebut.

b. Keamanan (*Secure*)
Kemampuan infrastruktur TI Diskominfo Kabupaten Tapin untuk melindungi data dan sistem dalam aspek kerahasiaan dan integritas. Faktor keamanan tidak hanya berkaitan

pencegahan orang mengakses data atau sistem yang tidak sesuai dengan haknya, tetapi juga kemampuan untuk menjaga data yang dikirim melalui infrastruktur TI terjaga integritasnya. Sebagai contoh otentikasi dan otorisasi kepada seluruh pengguna sebelum pengguna mengakses sistem untuk memastikan pengguna yang akses adalah pengguna sebenarnya dan memiliki hak akses terhadap fungsi-fungsi yang akan digunakan. Menjaga integritas data dapat menggunakan *digital signature* untuk memastikan pengiriman data adalah memang benar dan data tidak mengalami perubahan selama proses pengiriman/transfer.

c. Ketersediaan (*Available*)
   Kemampuan infrastruktur TI Diskominfo Kabupaten Tapin beroperasi pada interval waktu tertentu. Ketersediaan infrastruktur TI Diskominfo Kabupaten Tapin untuk tetap beroperasi sesuai dengan *Service Level Agreement* (SLA). 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 Pengelolaan (*Manageable*)
   Kemampuan infrastruktur TI Diskominfo Kabupaten Tapin untuk dikelola dengan mudah. Kemudahan tidak hanya berkaitan dengan tersedianya *management tools* terhadap infrastruktur TI tetapi juga kemudahan dalam mempelajari infrastruktur tersebut. Contoh kemudahan dalam pengelolaan adalah *IP Address*, memanfaatkan DHCP (*Domain Host Control Protocol*) memudahkan sistem administrator untuk mengalokasikan *IP Address* komputer pengguna dalam jumlah besar.

e. Kemudahan dalam Perbaikan (*Serviceable*)
   Kemampuan infrastruktur TI Diskominfo Kabupaten Tapin 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 dapat diperoleh dengan memilih teknologi yang sudah teruji di industri dan memiliki dukungan teknis *vendor* dapat diandalkan.

2. Pusat Data

Pusat Data (*data center*) adalah suatu fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

Pusat Pemulihan Bencana (*disaster recovery center*) adalah suatu fasilitas yang digunakan 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.

Prinsip dan kriteria perancangan sebuah Pusat Data secara umum 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. Data center harus dibuat sebisa mungkin mendekati zero-failure untuk seluruh komponennya.

b. Skalabilitas (*Scalability*)
   Pusat Data harus mampu beradaptasi dengan pertumbuhan kebutuhan yang cepat atau ketika adanya 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 server, jaringan, dan lain - lain maupun non fisik (intangible) yakni data – data dan informasi. Oleh karenanya sistem keamanan dibuat seketat mungkin meliputi pengamanan secara fisik maupun pengamanan non-fisik.

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

e. Kemudahan *Deployment*
   Server 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 server seperti ketika ingin memindah, merubah *resource* bahkan ketika kita ingin melakukan *live migration* atau memindahkan server dalam keadaan hidup tanpa mengalami *down*. Proses penginstalan dan pemulihan (*recovery*) juga tidak memakan waktu yang lama jika terjadi kerusakan/*error* pada server.

g. Redudansi (*Redundancy*)
   Untuk menjamin ketersediaan dan kinerja aplikasi maka diperlukan redudansi aplikasi, basis data (*database*) dengan menggunakan teknik *clustering* dan duplikasi server. *Clustering server* aplikasi dapat membagi beban kerja server (*load sharing*) dan duplikasi server 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 memindahkan server aplikasi ke tempat lain dapat dilakukan dengan mudah dan cepat.

i. Penghematan

Prinsip penghematan yang dimaksud meliputi:

1. Optimalisasi server

   Server fisik dengan kapasitas besar, sedangkan aplikasi server yang akan dibangun hanya memerlukan *resource* yang kecil maka diperlukan teknologi yang dapat mengoptimalkan server tersebut sehingga dapat dimanfaatkan untuk membangun aplikasi lain di server fisik tersebut.

2. Hemat Listrik dan *Hardware*

   Server fisik dengan kapasitas besar dapat digunakan untuk berbagi resource untuk menjalankan banyak aplikasi server. Sehingga tidak diperlukan banyak server fisik yang dapat menghemat penggunaan listrik dan pendingin. Jika *resource* kurang maka tidak perlu beli server baru cukup *upgrade part* yang perlu *diupgrade* saja (misal RAM,CPU,Storage).

   Berkurangnya jumlah perangkat otomatis mengurangi panasnya ruang server/data center. Ini akan berimbas pada pengurangan biaya pendinginan/AC dan pada akhirnya mengurangi biaya penggunaan listrik.

3. Hemat Space/Rack Server

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

4. Tidak Terikat pada Satu Vendor

   Tidak harus terikat pada satu vendor tertentu, jenis server dan platform. Sehingga memudahkan dalam pengembangan dan pemulihan (*recovery*) 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 server yang ada.

6. Keamanan

   Jika terjadi kasus server di hack dan data penting dalam server dihapus/dirusak maka proses mengembalikan server 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/*data center* harus memperhatikan:

1) Memilih lokasi Pusat Data yang aman dari bencana, mudah diakses dan mudah melakukan pengembangan/pembangunan Pusat Data;

2) Merancang dan membangun Pusat Data sesuai dengan standar topologi yang dipilih sesuai kebutuhan berdasarkan kajian kebutuhan bisnis dan analisis dampak bisnis (*business impact analysis*);
3) 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)*;
4) Menyediakan 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) Memiliki sistem *monitoring* lingkungan pusat data (*environment monitoring system*) yang meliputi antara lain monitoring temperatur, kelembaban, asap, kebakaran, kebocoran air, dan tegangan listrik.
6) Mempunyai dan menjalankan standar operasional prosedur untuk operasi dan perawatan; dan
7) Memiliki rencana keberlangsungan usaha (*business continuity plan*) dan rencana pemulihan bencana (*disaster recovery plan*) yang komprehensif serta proses pemulihan bencana yang cepat dan adaptif.

A. SNI Pusat Data

Saat ini telah terbit Standar Nasional Indonesia (SNI) tentang pusat data yakni :

1. SNI No 8799-1:2019 tentang Panduan Spesifikasi teknis pusat data;
2. SNI No 8799-2:2019 tentang Panduan Manajemen Pusat data;
3. SNI No 8799-3:2019 beserta amandemennya tentang Panduan Audit Pusat Data

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

Standar ini merinci persyaratan spesifikasi teknis pusat data sebagai berikut:

a. Spesifikasi gedung
   1. 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 pada atau kumuh, jarak dengan arteri lalu lintas (jalan raya utama dan jalur kereta api) minimal 91 m.

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

3. 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.

4. Pembagian ruangan

   Pembagian ruangan meliputi area perkantoran (area publik, pribadi, ruang fasilitas penunjang), area telekomunikasi, dan area server.

5. Ketahanan material gedung

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

6. 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, pengelolaan energi.

b. Spesifikasi sistem kelistrikan

1. Catu daya listrik

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

2. 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.

3. Persediaan bahan bakar

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

4. *Uninterruptible Power Supply (UPS)*

   Pusat data memiliki UPS untuk menjaga ketersedian kelistrikan tidak terputus, Kapasitas UPS minimum sama dengan 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 dalam keadaan ketiadaan catu daya listrik dari sumber utama.

   Tersedia sambungan langsung otomatis atau manual untuk sistem kelistrikan yang diperlukan dalam perawatan jaringan kelistrikan.

5. 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.

6. Konstruksi panel listrik

   Persyaratan konstruksi panel listrik, khususnya untuk panel induk, untuk masing-masing kategori strata pusat data.

7. 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.

8. 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.

9. 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 server dan area telekomunikasi harus memenuhi pengukuran:

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

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

   Bagian pada rak server yang kosong harus ditutup untuk menjaga pendinginan maksimal. Insulasi diperlukan untuk mencegah terjadinya pengembunan yang disebabkan oleh perbedaan temperatur antara ruang server 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 mempergunakan 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

Sistem pemadam kebakaran meliputi seluruh pusat data dan terbagi dalam area-area yang berdiri independen, artinya apabila terjadi kebakaran area A maka hanya area tersebut yang terpadamkan. Sistem pemadam kebakaran sekurang-kurangnya dilakukan tes setahun sekali. Pusat data 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 stabilitas tegangan arus listrik dan penggunaan daya listrik yang dapat memberikan peringatan sebelum terjadi kelebihan beban. Pusat data memiliki sistem monitoring suhu perangkat serta kelembaban relatif ruangan di dalam area server dan area telekomunikasi. Pusat data memiliki sistem pemipaan dengan fitur *monitoring* kebocoran pipa air atau genangan di bawah *raised floor*.

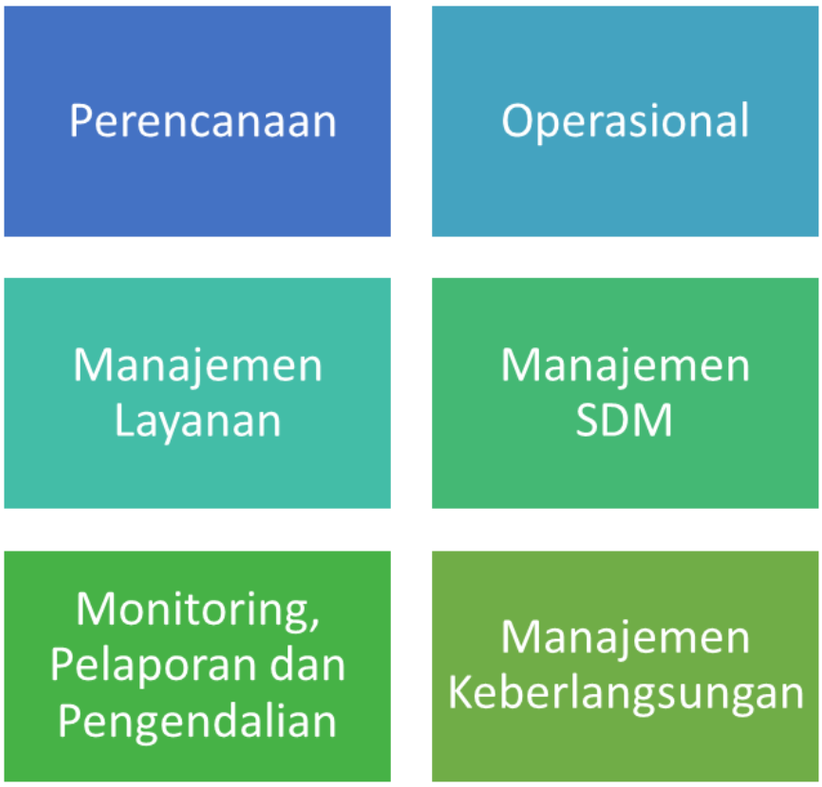
g. Spesifikasi sistem keamanan fisik

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. 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 ini dapat digunakan oleh penyelenggara yang bertanggung jawab atas manajemen Pusat data di dalam suatu Penyelenggara pusat data / lembaga. Spesifikasi manajemen pusat data ini berlaku untuk semua pusat data.



Gambar 2.3.14. SNI No 8799-2:2019 - Panduan Manajemen Pusat Data

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.

3) SNI No 8799-3:2019 beserta amandemennya tentang Panduan Audit Pusat Data

Bagian seri standar pusat data menyediakan panduan audit pusat data yang efektif di dalam suatu penyelenggaraan pusat data. Standar ini digunakan untuk melakukan audit terhadap pusat data yang sudah berlangsung atau beroperasi meliputi:

a. Spesifikasi teknis pusat data
b. Manajemen pusat data

Hasil yang didapat dari audit pusat data adalah:

a. Memenuhi atau tidak terhadap standar pusat data, dan
b. Tingkat strata dari pusat data.
    - Pada SNI No 8799-1:2019, pusat data dikategorikan dalam 4 strata untuk menunjukkan spesifikasi teknis dan tingkat ketersediaan layanan pusat data.
    - Pada SNI No 8799-2:2019, pusat data dikategorikan dalam 4 strata untuk menunjukkan manajemen pusat data terhadap tingkat layanan.

B. Pengembangan Pusat Data

a. Topologi Data Center

Terdiri dari sistem – sistem pendukung, infrastruktur utama, dan infrastruktur pendukung DC. Berikut ini adalah rincian topologi Data Center :

a. Sistem – sistem pendukung DC meliputi :
    - Sistem kelistrikan;
    - Sistem pendingin dan kelembaban;
    - Sistem pemadam kebakaran;
    - Sistem pengkabelan;
    - Desain ruang komputer meliputi raised floor, cable tray, dan lokasi rack server;
    - Sistem Keamanan;
    - Sistem Pencahayaan;
    - Sistem Pemantau Lingkungan;
b. Infrastruktur Utama DC meliputi :
    - Infrastruktur Jaringan;
    - Infrastruktur Server & Storage;
    - Model DC;
    - Aplikasi pendukung (Software)
c. Infrastruktur Pendukung DC meliputi :
    - Local Area Network
    - Wireless LAN
    - WAN
    - Remote Access dan VPN
    - Internet
    - Telekomunikasi

b. Ruang Pendukung

Ruang pendukung DC adalah ruangan – ruangan untuk menempatkan perangkat – perangkat pendukung operasional DC seperti ruang perangkat sistem pendingin & kelembaban, ruang perangkat fire suppression dll. Ruang operasional dan pemantauan DC juga termasuk ruang pendukung DC. Rincian ruang pendukung DC yang direkomendasikan antara lain sesuai dengan label gambar di atas adalah :

1. Lobby
   Lokasi ruang tunggu tamu, rekanan, penukaran kartu identitas dengan kartu akses.
2. Security
   Lokasi ruang operasi keamanan meliputi pemantauan CCTV, kontrol akses ke ruangan.
3. Office
   Ruang kerja administrasi DC termasuk ruang kepala DC.
4. Facility Control
   Ruang kontrol fasilitas DC seperti kontrol suhu & kelembaban, power, listrik dan lain – lain.
5. Hall
   Ruang serba guna yang bisa digunakan untuk kegiatan meeting dalam jumlah besar atau lainnya.
6. Operations Command Center
   Petugas memonitor server pusat data melalui dashboard yang ditayangkan dalam layar lebar.
7. Network Room
   Lokasi rak perangkat jaringan dan keamanan jaringan. Semua struktur kabel data baik UTP maupun Fiber optic berakhir di ruang jaringan.
8. Meet Me Room
   Ruang terminasi (akhir) kabel jaringan dari provider internet (ISP), dan telekomunikasi.
9. Network Operating Center
   Ruang pemantauan kinerja jaringan DC yang ditayangkan melalui dashboard.
10. Meeting Room
    Ruang pertemuan untuk rapat atau diskusi dari pengelola DC.
11. Fire Suppression System
    Ruang untuk menempatkan perangkat – perangkat pendukung sistem pemadam kebakaran (fire suppression).
12. UPS
    Ruang untuk perangkat UPS pendukung catu daya cadangan ruang server, lampu, cctv, access control dll.
13. UPS Battery
    Ruang battery UPS yang terpisah dari UPS sehingga mudah untuk perawatan dan penggantian battery.
14. Loading Dock
    Tempat untuk menerima peralatan yang baru datang untuk pusat data.
15. Build Room/Staging Area

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

16. Chiller
    Ruang untuk perangkat chiller pendingin suhu.
17. Warehouse
    Ruang untuk perangkat listrik.
18. Genset Room
    Ruang untuk meletakkan perangkat generator pembangkit listrik cadangan (genset).
19. Trafo
    Ruang untuk meletakkan trafo listrik dari PLN.
20. Solar Tank
    Ruang untuk menyimpan solar sebagai bahan bakar genset.
21. Ruang Mekanik
    Ruang kerja mechanical engineering (ME).
22. Ruang Spare Part
    Ruang gudang penyimpanan suku cadang *(sparepart)* perangkat mechanical dan listrik DC.

c. Sistem Kelistrikan

Sistem kelistrikan meliputi catu daya utama dan catu daya cadangan. Catu daya utama berasal dari listrik PLN dan catu daya cadangan berasal dari generator, dan UPS. Beberapa ketentuan tentang sistem kelistrikan di DC antara lain :

1. Kabel daya masuk ke dalam bangunan pusat data (data center) determinasi di ruang kendali penyambungan listrik yang handal;
2. Daya listrik utama paling sedikit 20% lebih besar dari proyeksi beban puncak di mana pusat data (data center)berada;
3. Tersedianya catu daya listrik alternatif (seperti generator standby) dengan kapasitas yang memadai untuk operasional minimal 3 jam selama kejadian gangguan listrik utama;
4. Perangkat server, storage, jaringan, keamanan server & jaringan, CCTV, access control, penerangan harus diproteksi dengan Uninterruptible Power Supply (UPS) atau catu daya cadangan lainnya;
5. UPS atau catu daya cadangan lainnya harus memiliki kapasitas memadai untuk memasok beban DC sampai catu daya alternatif mampu memikul beban perangkat DC (steady-state);
6. Kapasitas UPS harus lebih besar dari proyeksi beban puncak perangkat DC. Kapasitas beban rata-rata tidak lebih besar dari 80% kapasitas UPS;
7. UPS memiliki sistem pelaporan, pemantauan kinerja, dan sistem peringatan;
8. UPS yang digunakan telah memiliki jaminan dari pabrikan untuk dapat berfungsi sesuai spesifikasinya;
9. Bangunan harus dilengkapi dengan sistem proteksi petir;
10. Kabel komunikasi tembaga dari luar gedung diproteksi dengan peredam tegangan lebih (surge suppressor) sebelum ke ruang pusat data (data center);

11. Ruang pusat data (data center) memiliki terminal pembumian (grounding) tembaga yang menjadi titik acuan pembumian ruangan tersebut.
12. Sistem grounding untuk peralatan data center harus dibedakan dengan peralatan lainnya seperti sistem penangkal petir pada bangunan data center.
13. Semua benda logam harus terikat ke tanah termasuk lemari, rak, PDU, CRAC (AC Ruangan Server), jalur kabel, dan setiap raised floor dengan resistansi grounding kurang dari 1 Ohm

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

Listrik utk Peralatan IT	Listrik utk Pendukung DRC
• UPS • PDU • Cabling • Network Devices • Servers • Storage	• Sistem Pendingin • Pencahayaan • Fire Suppression • Keamanan – Access Door & CCTV • Generator

Gambar 2.3.15. Kebutuhan Listrik DC

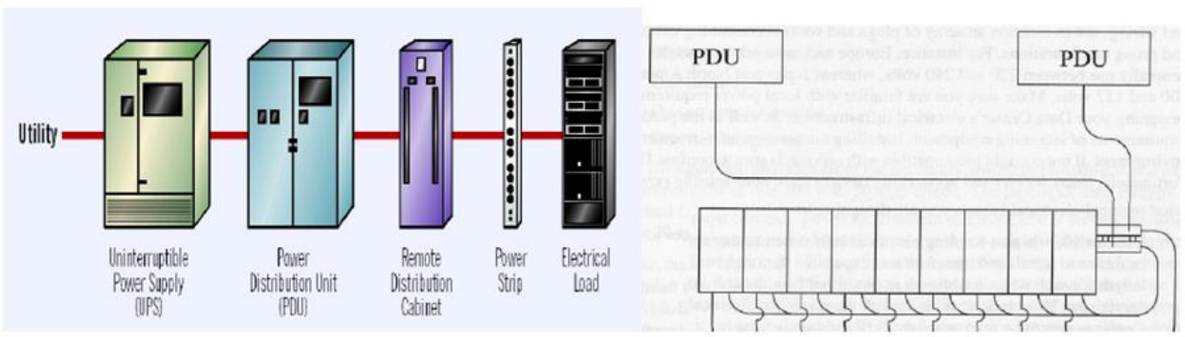
d. Distribusi Listrik Ruang Server

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

1. Distribusi secara langsung dari PDU (Power Distribution Units)

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

   PDU akan menuju ke panel circuit kemudian dari tempat tersebut akan didistribusikan ke masing-masing lokasi kabinet. Jauh lebih efisien dari segi pengkabelan karena untuk jarak yang jauh antara lokasi kabinet server dengan PDU, hanya membutuhkan satu kabel yang panjang, baru kemudian dari panel sirkuit disalurkan ke masing – masing kabinet server dengan kabel yang berjarak pendek.

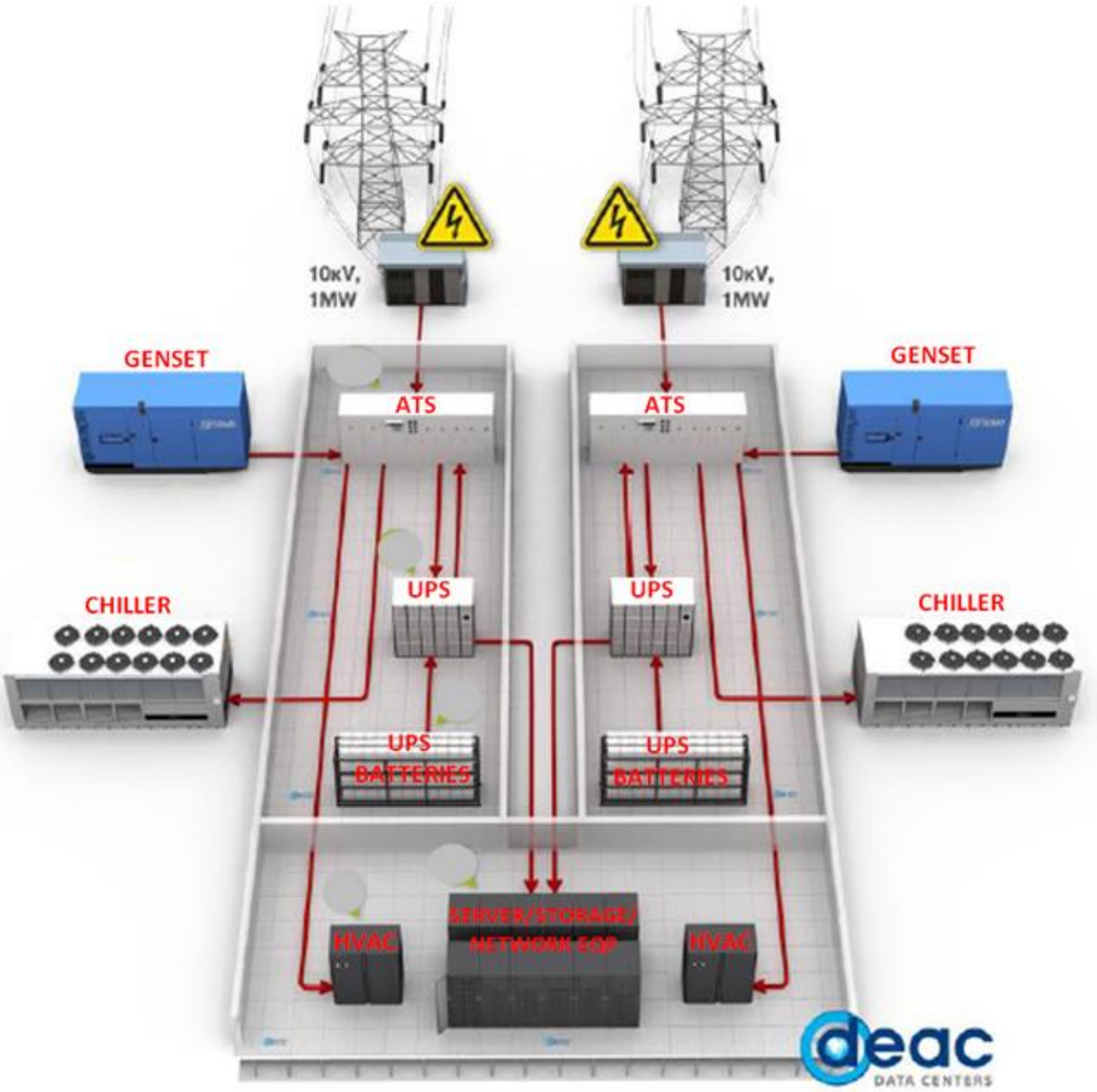


Gambar 2.3.16. Distribusi Listrik dari PDU melalui Panel Circuit

Gambar di atas adalah distribusi listrik dengan menggunakan panel circuit yang tersebar di Remote 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).

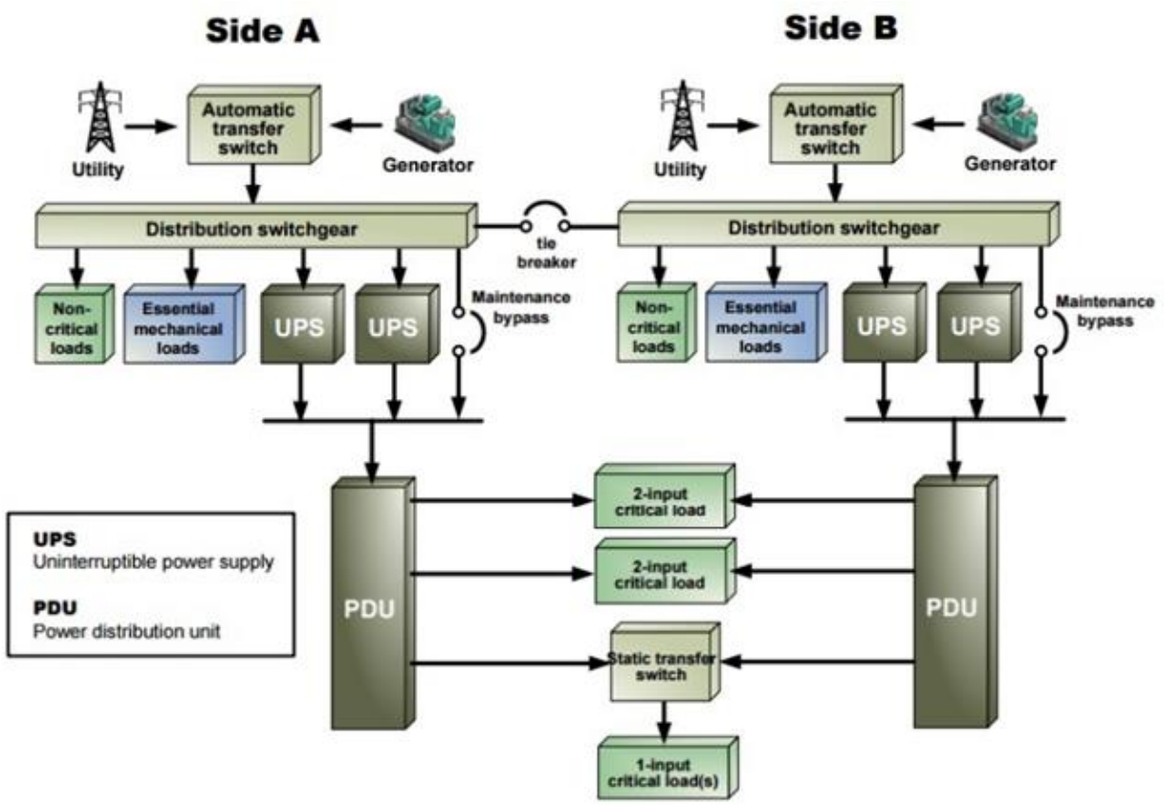
e. Redudansi Sumber Listrik

Untuk mencapai tingkat reliabilitas yang tinggi maka diperlukan redundansi pada perangkat utama maupun cadangan dan jalur masuk ke DC. Saluran listrik ke lokasi DC berasal dari sumber gardu listrik yang berbeda. Selain itu, jalur masuk ke DC dari arah yang berbeda juga. Redundansi sumber listrik utama (PLN) dan sumber listrik cadangan diperlukan untuk menjamin keberlangsungan dan kehandalan dari DC. Redundansi meliputi sumber listrik PLN dari gardu listrik yang berbeda, jalur (lintasan) aliran listrik dari gardu menuju kawasan DC. Selain itu juga redundansi dari perangkat sumber listrik cadangan seperti generator, UPS, dan automatic transfer switch (ATS).



Gambar 2.3.17. 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 server akan memiliki dua power strip dan akan ada receptacle yang berbeda juga disetiap server.
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 2.3.18. Instalasi Logik dari Sistem Kelistrikan

f. Listrik Cadangan (Standby Power)

Sistem listrik yang berperan sebagai standby power pada DC merupakan sumber tenaga back-up-an ketika sistem listrik utama mengalami kegagalan. Standby power yang dibuat mempertimbangkan 3 aspek yaitu redundansi, kesederhanaan, dan biaya. Berbagai perangkat terkait dengan standby power pada data center 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.

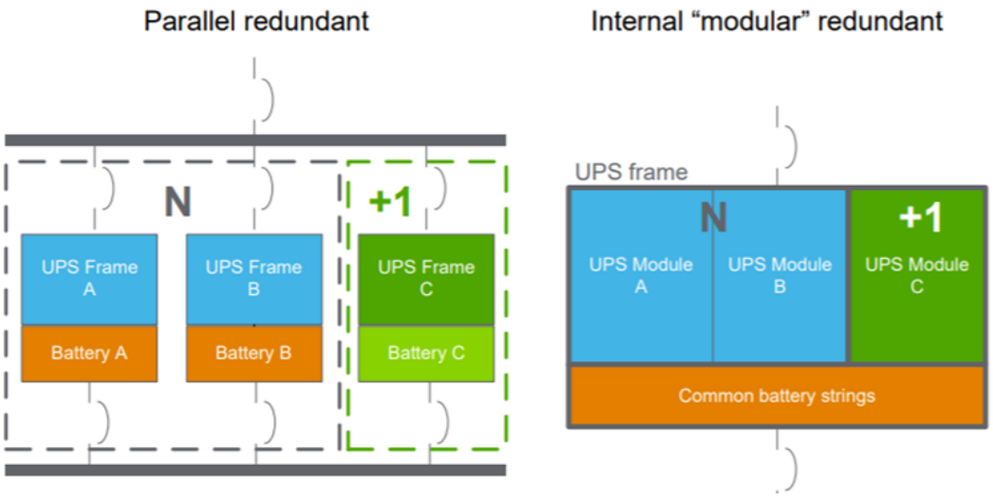
Selain lamanya waktu perpindahan, yang perlu dicatat adalah kehandalan dari masing-masing tipe terhadap kemampuan menangani permasalahan yang timbul dari jaringan listrik PLN, yaitu antara lain adalah kemampuan menangani tegangan naik atau turun, harmonik, Sag (mati sesaat atau berkedip), swell (lonjakan 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;
- Perhitungan kapasitas UPS adalah lebihkan 25% dari beban puncak;

Contoh perhitungan kebutuhan kapasitas UPS :
Konsumsi listrik untuk full rack sekitar 600 watt untuk perangkat server, perangkat jaringan seperti switch, load balance, storage server, fan dan lainnya. Untuk rack server 4U dengan konfigurasi tergolong padat, kebutuhan listrik dapat mencapai 1000 watt. Dari total kebutuhan konsumsi listrik tersebut, diberikan rentang 25% untuk faktor redundancy.
Untuk kebutuhan listrik 600 watt dan dengan kemampuan runtime 60 menit, maka UPS yang memiliki kapasitas diatas 600 watt / 600 VA (1 Watt nyaris = 1 VA jika power factor 0.9%). Sehingga UPS terbaik untuk Server tersebut adalah yang berkapasitas 125% x 600 watt atau 750 watt atau 1000 VA, maksimum 1500 VA. Sehingga kesimpulannya untuk satu rack server full load, kebutuhan UPS nya adalah 1 kV.

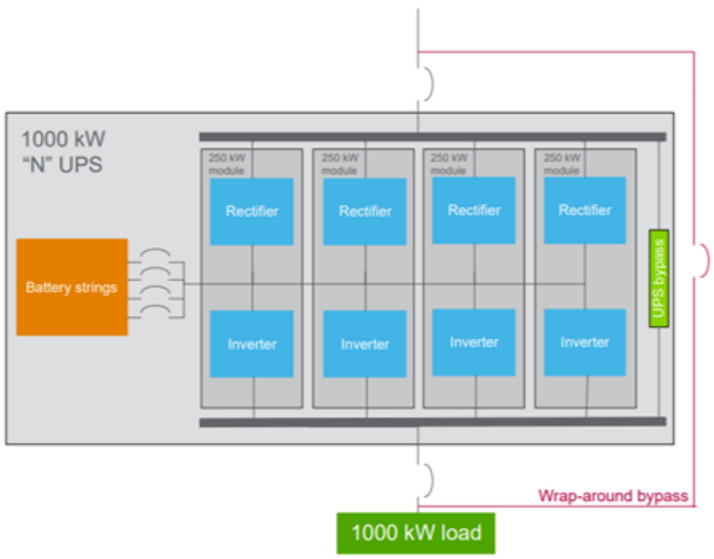
1. Redudansi UPS

   Redundansi UPS terdiri dari dua model yakni parallel redundant atau internal modular redundant. Parallel redundant berarti perangkat UPS yang terdiri dari UPS Module dan battery-nya redundan dengan perhitungan N+1. N adalah jumlah UPS pada beban puncak. Sedangkan internal modular redundant adalah jumlah modulnya saja yang redundant sedangkan battery-nya tidak. Gambar di bawah memberikan informasi topologi perangkat UPS dengan dua model yakni parallel redundant dan internal modular redundant.



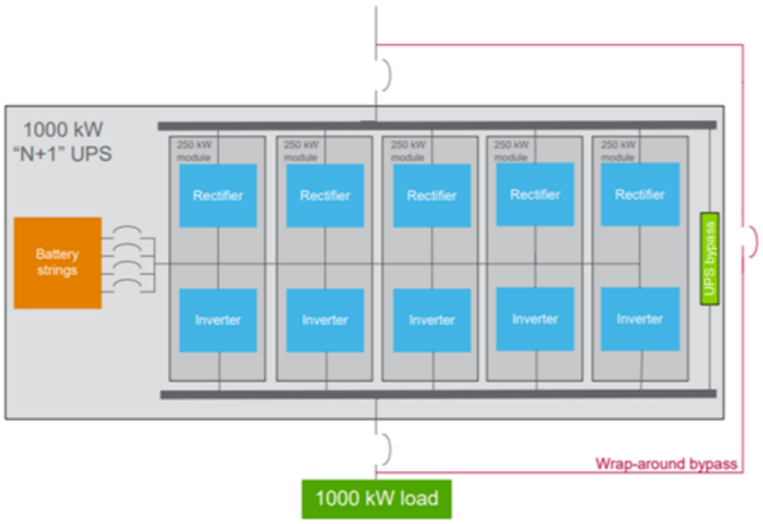
Gambar 2.3.19. Perbandingan Dua Model UPS DC

Di bawah ini adalah tiga contoh topologi perangkat UPS dengan kapasitas 1000kW yang terdiri dari 4 modul masing – masing 250kW. Baseline 1N configuration adalah satu UPS dengan empat modul tanpa redundant.



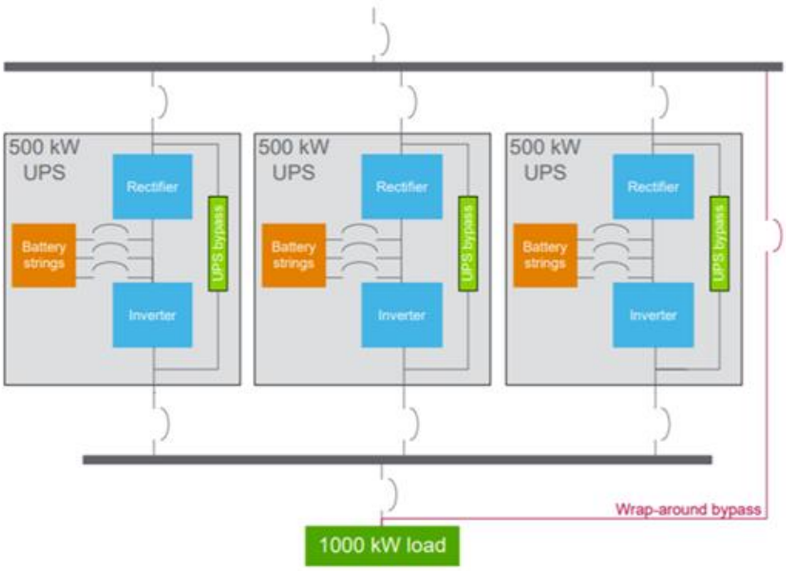
Gambar 2.3.20. UPS dengan Empat Modul Tanpa Redundansi

Gambar selanjutnya adalah topologi UPS dengan model internally ‘modular’ redundant N+1 configuration. Modul UPS terdiri dari lima buah yakni 4 buah modul utama dan satu buah untuk cadangan.



Gambar 2.3.21. UPS dengan Internally Modular Redundancy

Gambar terakhir adalah topologi UPS dengan model Parallel redundant N+1 configuration. UPS utama terdiri dari dua modul yakni masing – masing 500 kW dan satu buah modul untuk cadangan sebesar 500 kW.



Gambar 2.3.22 UPS dengan Parallel redundant N+1

2. Fault Tolerance UPS

Fault Tolerance adalah apa yang memungkinkan suatu sistem untuk terus beroperasi (dalam hal ini, mendukung beban TI) jika terjadi kegagalan beberapa komponennya. Dengan itu mengatakan, beberapa UPS dirancang dengan tingkat toleransi kesalahan yang lebih tinggi daripada yang lain. Saat memilih UPS, penting untuk mempertimbangkan atribut desain toleransi kesalahan kotak; terutama jika arsitektur yang dipilih terdiri dari satu bingkai UPS (seperti pada konfigurasi 1 dan 2). Di bawah ini adalah contoh atribut desain toleransi kesalahan:

- Redundansi modul daya (inverter / penyearah)
- Redundansi penggemar
- Redundansi catu daya pada pengontrol
- Redundansi string baterai

- Redundansi bus komunikasi
- Redundansi dalam sistem kontrol
- Saklar statis berukuran lebih besar dari beban maksimum yang diharapkan untuk mengakomodasi muatan in-rush/step peralatan IT.

g. Sistem Pendingin & Kelembaban

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

Kriteria umum untuk sistem pendingin dan & kelembaban adalah :

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

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

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

a) 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 dibuat oleh suatu kelompok perangkat yang dalam hal ini terletak di data center. Temperatur yang rendah sangat diperlukan untuk efisiensi operasi server dan perangkat jaringan untuk menghindarkan dari fluktuasi. Sistem pendingin pada data center pada prinsipnya adalah sistem aliran udara dingin, yang terbagi menjadi tiga perangkat utama yaitu air handler, chiller, dan cooling towers. Selain itu, juga ada perangkat pendingin tambahan.

Redundansi sistem pendingin adalah memasang lebih dari satu air handler, kemudian juga tersedia menara pendingin tambahan untuk setiap chiller. Selain itu, persediaan air yang dibutuhkan untuk menciptakan udara dingin harus diamankan secara ekstra antara lain dengan membangun kontainer penyimpan air.

b) Tekanan Udara

Tekanan udara pada data center harus dijaga pada level tertentu yang disebut sebagai tekanan statis. DC didesain untuk memiliki tekanan antara 0.2-0.5 in. wc. Untuk menjaga agar tekanan udara tetap stabil maka periksa seluruh ruangan apakah telah tertutup dengan baik

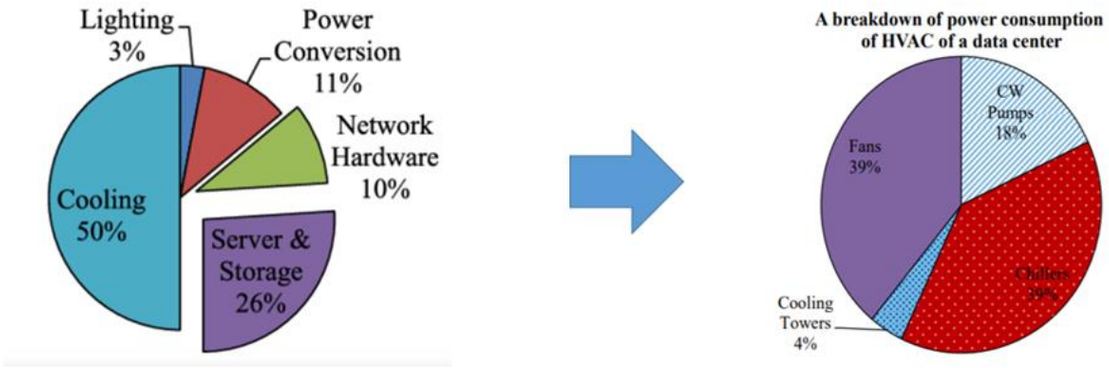
dan yakin bahwa tidak ada lubang sedikit pun. Jangan letakkan perforated tile dekat-dekat dengan DC air handler, karena kebanyakan handler membutuhkan buffer sekitar 36-42 in (91.4-106.7 cm).

c) Kelembaban

Kelembaban sendiri merupakan konsentrasi uap air di udara, yang penting untuk dijaga terkait dengan sistem HVAC data center adalah kelembaban relatif dalam ruangan data center. Kelembaban relatif adalah persentase perbandingan dari jumlah uap air yang ada di udara dengan jumlah uap air di udara kering. Perangkat server 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 karatan pada beberapa perangkat di data center karena penguapan (kelembaban tinggi) atau mencegah munculnya elektrostatis pada beberapa perangkat metal (kelembaban yang rendah). Cara yang dilakukan adalah melengkapi AH dengan kemampuan humidification atau melalui penggunaan unit-unit humidification yang terpisah dari AH. Kelembaban relatif yang memungkinkan untuk suatu ruangan data center 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.

d) Konsumsi Listrik Sistem Pendingin

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



Gambar 2.3.23. Grafik Konsumsi Listrik di DC

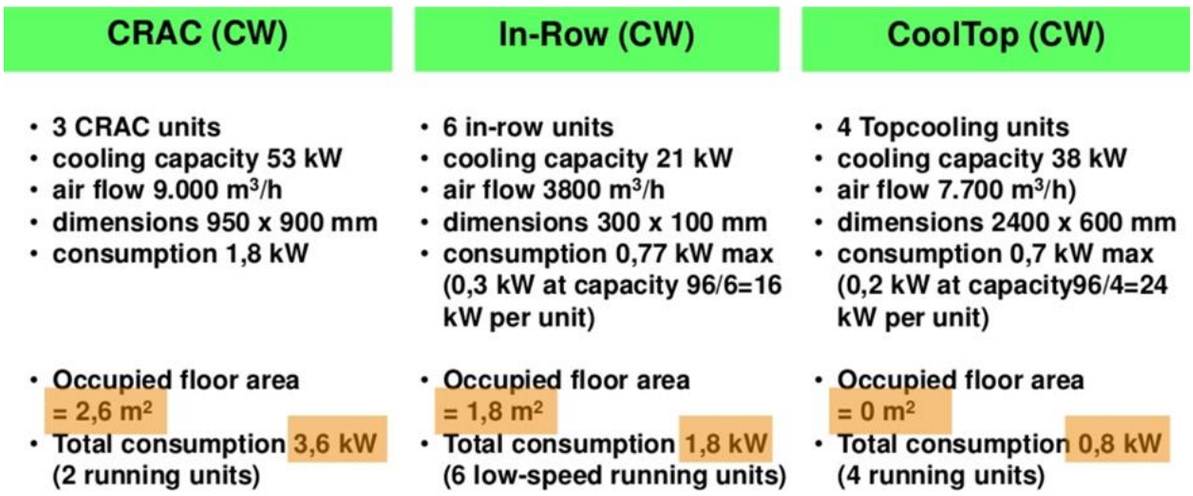
Dari informasi di atas, maka diperlukan sistem pendingin & kelembaban yang efisien dan efektif serta dukungan dari perangkat yang ada. Sistem pendingin & kelembaban berfungsi untuk mendinginkan perangkat server, storage, dan perangkat jaringan. Jika kapasitas ruang server belum maksimal, maka diperlukan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

e) Teknik Pendinginan Ruangan/Server

Saat ini terdapat tiga teknik pendinginan ruangan server atau rak server yakni Room Cooling atau Cooling Room Air Conditioner (CRAC), IN-ROW, dan TOP Cooling.

Gambar 2.3.24. Perbandingan Keuntungan dari Tiga Model Sistem Pendinginan DC

1) ROOM-COOLING
   - Fungsi mendinginkan seluruh ruangan server secara merata;
   - CRAC/PAC disebar di sisi-sisi ruang data center;
   - Jalur udara dingin (cold aisle) mengalir dari bawah raised floor naik ke atas melalui lubang – lubang kecil di papan raised floor arah depan rack server;
   - Jalur udara panas (hot aisle) yang berasal dari belakang rack server akan mengalir ke perangkat CRAC;
   - Kurang efisien jika ruang server belum terisi penuh;
2) IN-ROW
   - CRAC/PAC tidak lagi disebar di sisi-sisi ruang data center tapi sudah disebar di barisan rack servernya;
   - CRAC/PAC sudah disebar di barisan rack servernya, di dalam barisan rack-rack server ini di sisipkan cooling system yang mendinginkan udara panas di belakang server dan menghembuskan ke sisi depan server;
   - 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 server;
   - Tingkat efisiensi tinggi karena pembangunan bisa secara bertahap tergantung kebutuhan rack server;
3) TOP-COOLING
   - CRAC/PAC tidak lagi disebar di sisi-sisi ruang data center tapi diletakkan di atas rack server;
   - Di atas rack-rack server ini di sisipkan cooling system yang menghembuskan udara dingin ke sisi depan server dan mendinginkan udara panas di belakang server;
   - Tingkat efisiensi tinggi paling tinggi karena tempat yang dibutuhkan paling kecil, konsumsi daya listrik paling kecil juga di bandingkan dua teknik lainnya;



Gambar 2.3.25. Perbandingan Tiga Model Sistem Pendingin DC

Dari gambar perbandingan teknik pendinginan ruang server diatas, 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 server, tidak menambah ruang di bawah. Kesimpulannya teknik CoolTop memiliki tingkat efisiensi paling tinggi untuk mendinginkan rack server. Pada kondisi ruang server yang belum terisi penuh, teknik ini juga sebagai solusi menekan biaya listrik.

h. Fire Suppression System

Perlindungan DC dari api mempunyai tiga tujuan utama yakni : identifikasi adanya api (detection), pemberitahuan adanya api ke seluruh penghuni DC 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 :

1. Gas System

   Sistem gas tidak merusak perangkat server dll, efektif tetapi waktu singkat.

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

2. Water sprinklers

   Sistem air dapat merusak perangkat server dll, dapat digunakan untuk melindungi bangunan dan memadamkan api.

   Kriteria Fire Suppression System untuk DC adalah sebagai berikut :

   a) QUICK

      Sistem dapat memberikan respon cepat jika terjadi kebakaran untuk meminimalkan terjadinya kerusakan pada perangkat server dll.

   b) CLEAN

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

c) ODORLESS

Gas yang dikeluarkan tidak menimbulkan bau yang menyengat.

d) NON-TOXIC

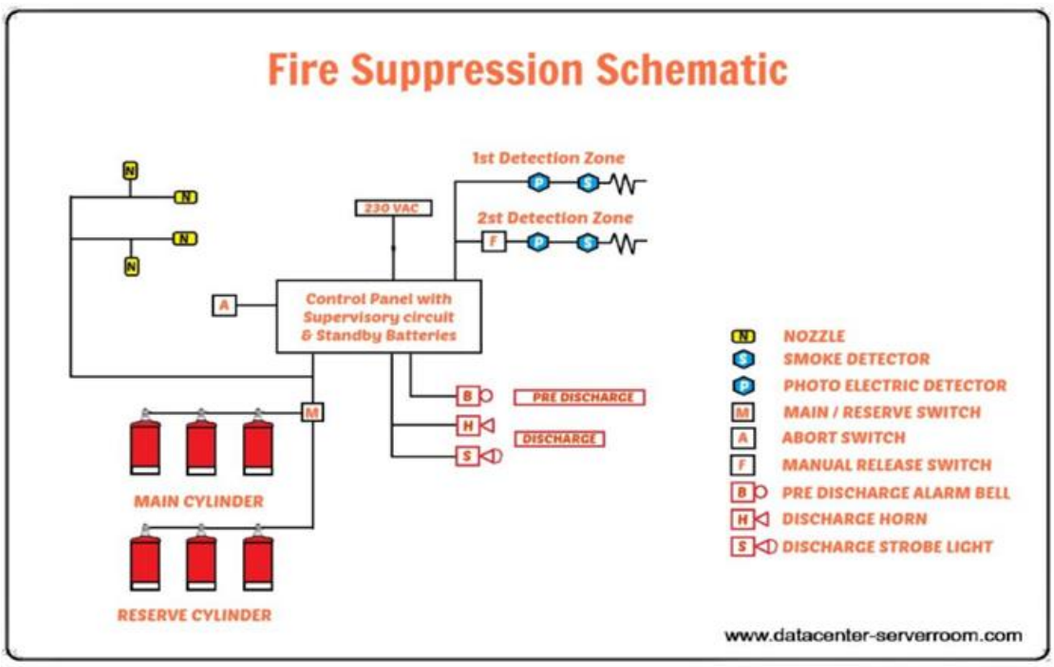
Gas yang dikeluarkan tergolong aman untuk manusia (tidak beracun).

e) NON-CONDUCTIVE

Gas yang dikeluarkan bukan penghantar panas atau elektrik karena dapat menyebabkan kerusakan.

f) LOW STORAGE SPACE

Perangkat utama dan pendukung hanya membutuhkan tempat yang kecil.



Gambar 2.3.26. Skema Fire Suppression System DC

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

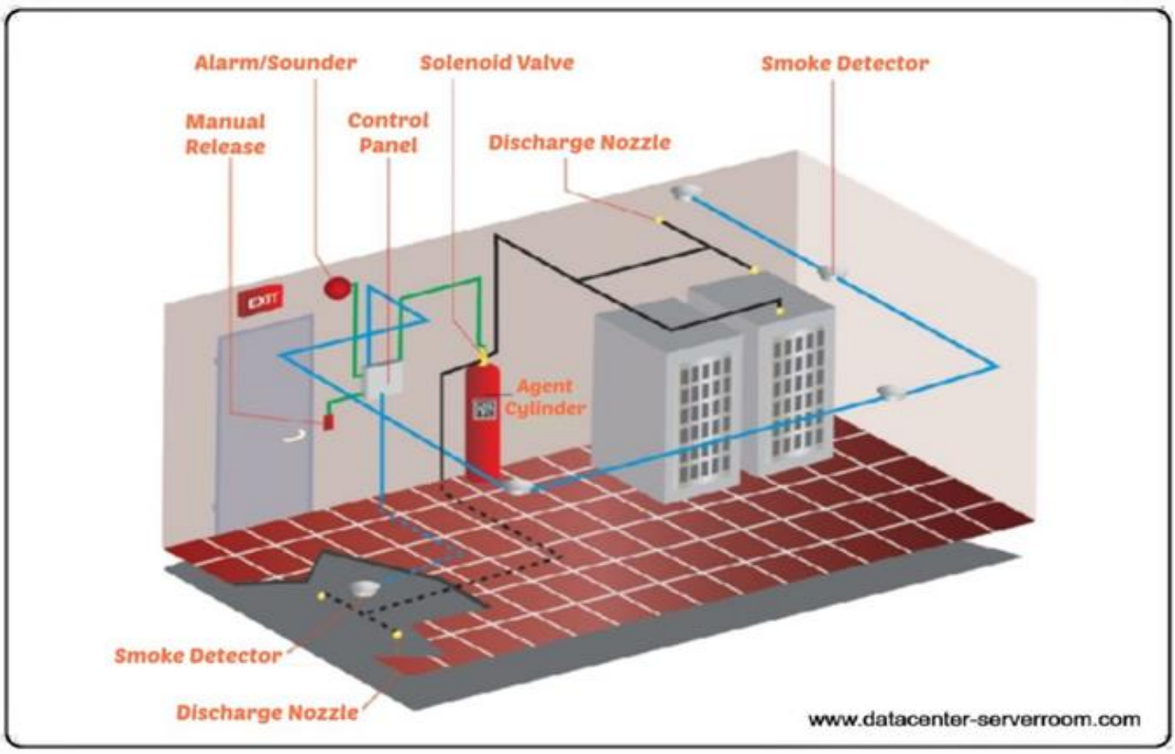
1. Deteksi panas yang linier (kabel sensor panas), ditempatkan sepanjang tray wire dan jalur elektrik baik diatas maupun dibawah raised-floor. Alarm pada sensor dibunyikan pada sistem kontrol bukan untuk memicu bekerjanya sistem fire suppression.
2. Deteksi tipe spot secara intelligent (photoelectric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

Dari lima kelas handheld extinguisher, yang paling tepat untuk dipasang pada pusat data adalah handheld extinguisher tipe C (untuk kebakaran yang diakibatkan oleh sistem listrik). Material CO2 dan halogenated adalah material suppression yang dipilih karena meninggalkan sedikit sisa ketika sudah tidak digunakan lagi. Komponen minimum fire suppression yang harus digunakan pada pusat data sederhana sekalipun adalah sebuah sistem sprinkler biasa (yang bertindak

sebagai pre-action sprinkler) dengan clean-agent fire extinguishers yang cocok. Kemudian meningkat pada level yang lebih tinggi, maka sistem fire suppression yang lebih canggih akan meliputi air sampling smoke detection systems, pre-action sprinkler systems, dan clean agent suppression systems.

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 itu juga disediakan sebagai pengganti smoke detectors biasa, karena kesensitifannya dan kapabilitas deteksinya jauh melampaui detektor konvensional.

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



Gambar 2.3.27. Instalasi Fire Suppression System DC

Beberapa ketentuan dalam pembangunan fire suppression system DC sebagai berikut :

1. Jumlah dan lokasi pintu darurat kebakaran sesuai dengan peraturan perundang-undangan;
2. Pintu darurat kebakaran dapat dibuka ke arah luar;
3. Lampu darurat dan tanda keluar diletakkan pada lokasi sesuai dengan peraturan perundang-undangan;

4. Titik panggil manual harus dipasang sesuai dengan peraturan perundang-undangan;
5. Dinding dan pintu ke ruang server, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan ruangan penting lainnya memiliki tingkat terbakar (fire-rating) sesuai dengan peraturan perundang-undangan;
6. Ruang komputer harus diproteksi dengan sistem pendeteksi asap. Seluruh sistem deteksi asap bangunan harus diintegrasikan ke dalam satu alarm bersama;
7. Catatan pemeliharaan yang mencakup seluruh aspek yang berkaitan dengan deteksi api dan pemadaman harus tersedia untuk keperluan pemeriksaan;
8. Bukti pelatihan staf pada simulasi pengendalian kebakaran harus tersedia;
9. Ruang pusat data (data center) harus dilindungi dengan sistem pemadam kebakaran. Sistem pemadam kebakaran otomatis harus dapat diaktifkan secara manual;
10. Alat pemadam kebakaran harus ditempatkan sesuai ketentuan peraturan perundangan-undangan;
11. Semua tanda peringatan kebakaran harus ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan;
12. Seluruh sistem pendeteksi dan pemadam kebakaran harus didesain dan dipasang oleh berkualifikasi sesuai standar internasional/nasional atau regulasi nasional;
13. Jika ruang server, ruang telekomunikasi, dan ruang mekanikal dan kelistrikan memiliki sistem pemadam api otomatis (sprinkler), maka sistem tersebut harus tipe preaction;
14. Jika ruang atau bangunan yang berdekatan dengan lokasi pusat data (data center) tidak memiliki sistem pemadam api otomatis (sprinkler), maka risiko kebakaran harus dikaji.

i. Sistem Pengkabelan

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

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

Yang patut diketahui bahwa betapa pentingnya kualitas kabel yang akan digunakan yaitu :

1. Kabel menyumbang kurang dari 10 persen dari total biaya infrastruktur jaringan;
2. Rentang hidup dari sistem kabel yang khas adalah 16 tahun ke atas, sehingga kabel adalah komponen yang terpenting dalam sistem pengkabelan terstruktur;
3. Hampir 70 persen dari semua jaringan yang bermasalah berasal dari pemasangan kabel yang tak memenuhi standar dan komponen kabel itu sendiri.

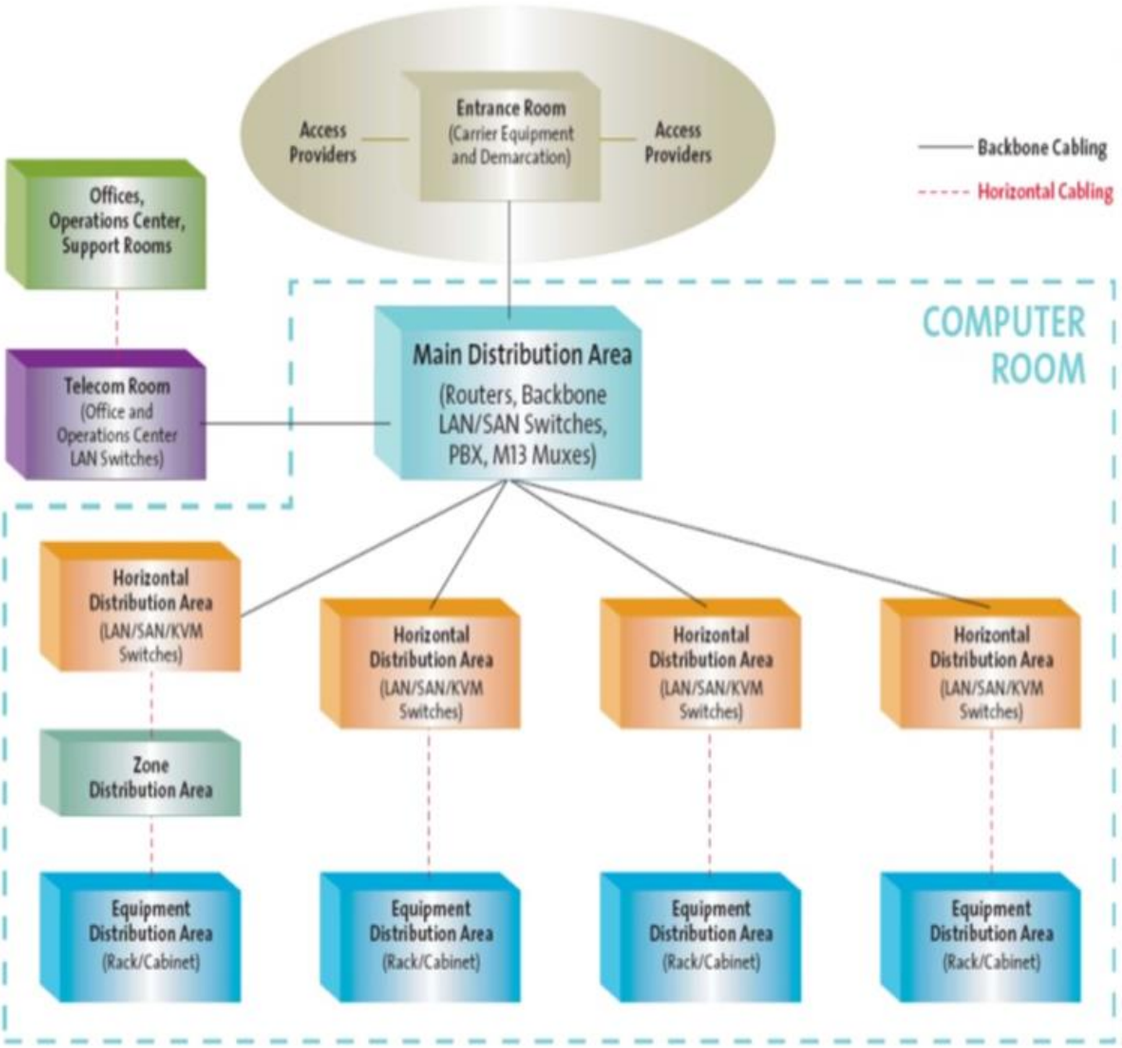
Beberapa ketentuan umum sistem pengkabelan listrik dan data di DC antara lain :

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

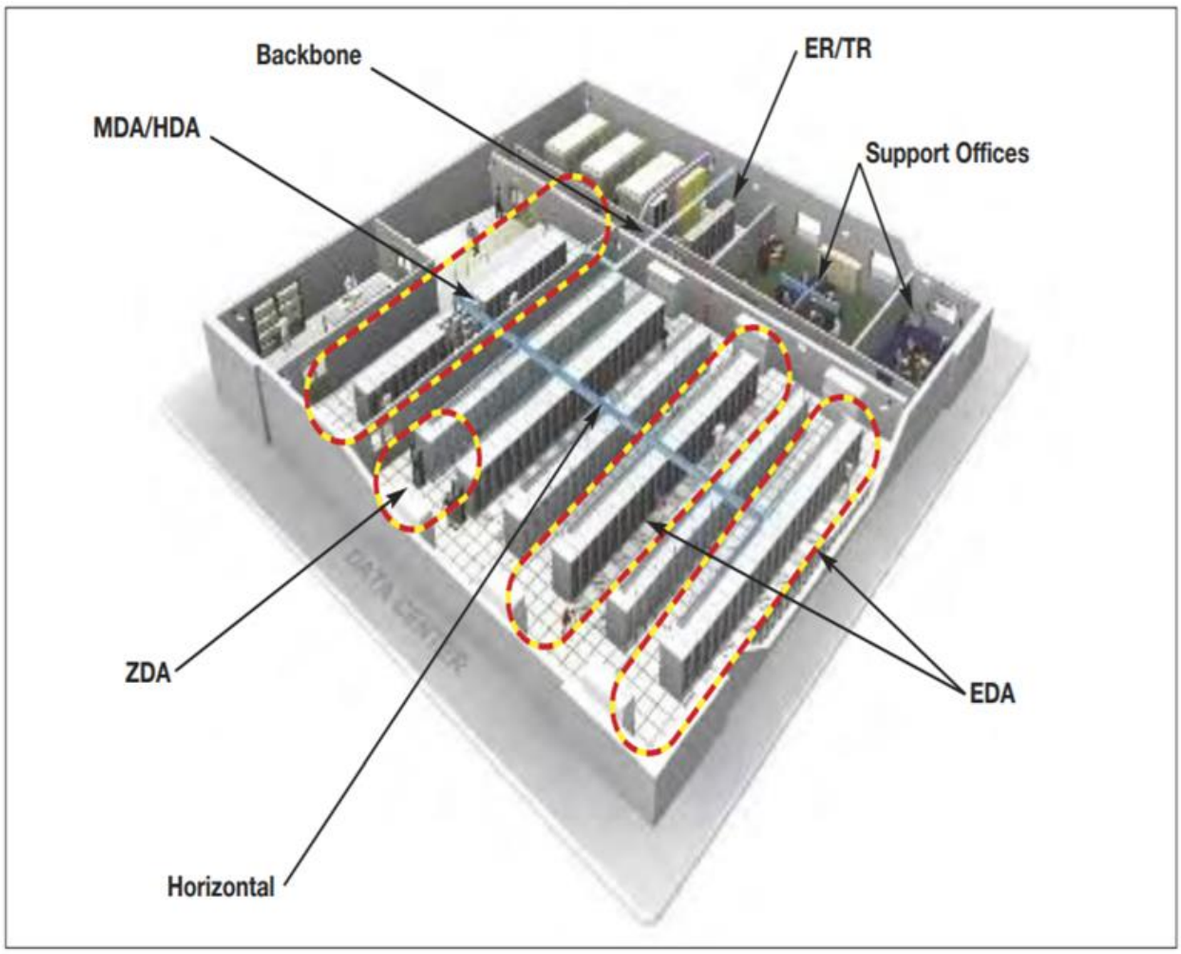
Standar ANSI/TIA/EIA-568-B berisi elemen dasar dari struktur sistem pengkabelan pada data center adalah sebagai berikut:

1. Sistem pengkabelan horizontal (horizontal cabling)
2. Sistem pengkabelan backbone (backbone cabling)
3. Cross-connect pada pintu masuk (entrance room) atau (main distribution area) atau area kerja
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
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 data center



Gambar 2.3.28. Topologi Sistem Pengkabelan DC



Gambar 2.3.29 Arsitektur Instalasi Sistem Pengkabelan DC

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 server, atau bahkan ruang telekomunikasi lainnya untuk konektivitas utama dengan seluruh jaringan.

   a. Pengkabelan horizontal meliputi :
   b. Kabel dari patch panel ke area kerja
   c. Outlet telekomunikasi
   d. Kabel penghentian
   e. Cross-connections(jika diizinkan)
   f. Pembatasan maksimal pada satu titik transisi
   g. Komponen jaringan yang spesifik (switch, router) tidak harus dipasang sebagai bagian dari kabel dengan sistem horizontal (dalam dinding). Ini harus dipasang di ruang telekomunikasi atau area kerja.

h. 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. Ini 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 untuk menjadi fleksibel, tapi masih memerlukan manajemen hati-hati. Prosedur pemasangan kabel instalasi standar terstruktur harus diamati ketika menginstal outlet area kerja, dan terminasi kabel harus dilakukan dengan menggunakan standar yang sama (T568A atau T568B) di seluruh sistem untuk menghindari masalah seperti pasangan menyeberang yang mungkin timbul jika standar dicampur. T568B standar yang lebih umum digunakan dalam aplikasi data. Standar ini mengharuskan dua outlet harus disediakan di setiap piring dinding - satu untuk suara, dan satu untuk data.

4. Telecom Room (Telekomunikasi)

   Daerah tertutup, seperti ruang atau lemari, peralatan telekomunikasi perumahan, frame distribusi, terminasi kabel dan lintas menghubungkan. Dengan kata lain, semua perangkat keras yang diperlukan untuk menghubungkan kabel horizontal untuk kabel vertikal. Daerah ini sering juga rumah peralatan bantu, termasuk berkas server 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)

   Ruang yang rumah membangun sistem telekomunikasi seperti PBXs, server, switch dll, dan penghentian mekanik dari sistem kabel telekomunikasi. Hal ini dianggap berbeda dari lemari telekomunikasi karena kompleksitas komponen itu rumah. Ruang peralatan baik dapat mengambil tempat dari lemari telekomunikasi atau menjadi fasilitas terpisah.Fungsi ruang peralatan bahkan mungkin 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. Dalam lingkungan kampus, setiap bangunan dapat memiliki ruang sendiri peralatan, yang peralatan lemari telekomunikasi terhubung, dan peralatan di ruangan ini kemudian dapat

terhubung ke fasilitas kampus pusat yang menyediakan utama lintas menghubungkan untuk seluruh kampus.

6. Entrance Room (Fasilitas Pintu Masuk)

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

7. Administrasi Kabel

   Ini adalah proses yang meliputi seluruh aspek kegiatan premis kabel yang berhubungan dengan mendokumentasikan, mengelola, dan pengujian sistem, serta kompilasi dan mempertahankan rencana arsitektur untuk sistem.

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 2.3.30. Kategori Kabel UTP – Ethernet

B. Fiber Optic

Standar ANSI/TIA/EIA-568-B memperbolehkan secara single-mode dan multimode dengan kabel serat optik. 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 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. Juga, Standar ANSI/TIA/EIA-568-B sekarang mengakui small-form factor konektor seperti konektor MT-RJ.Gambar 3.19 Spesifikasi dari 00-Ohm Unshielded Twisted-Pair Cabling
Tabel dibawah ini memberikan gambaran singkat mengenai standar industry pengkabelan mengakui serat optik yang digunakan pada pengkabelan premis. Empat tipe dari serat optik di spesifikasikan untuk menyokong beragam kelas aplikasi, Tipe tipe serat optik multimode (OM1, OM2, OM3) dan satu tipe singlemode (OS1) , OS1 merujuk pada serat singlemode standar, ITU-T G.652.

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 2.3.31 Kategori Tipe Kabel Serat Optik

j. Desain Ruang Server

1. Desain Raised Floor

Disebut juga access floor atau raised access floor

FUNGSI

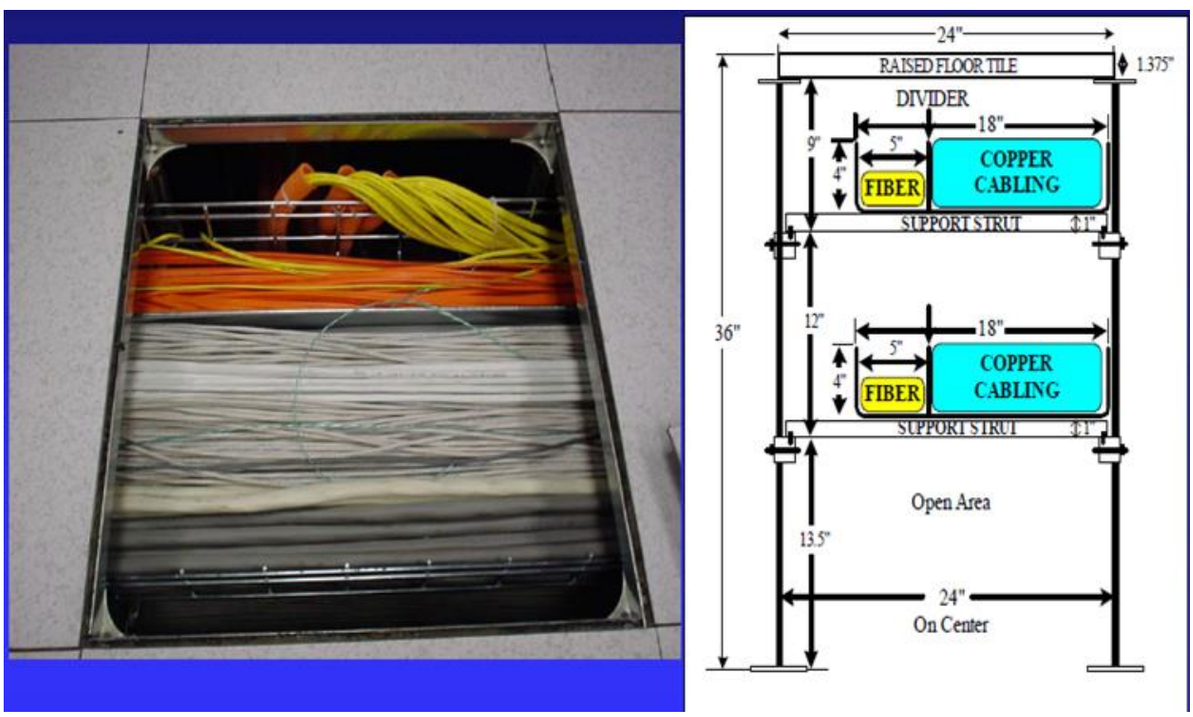
- Sistem distribusi udara dingin untuk mendinginkan peralatan IT
- Jalur kabel data
- Jalur kabel listrik
- Jaringan kabel tembaga untuk grounding peralatan
- Lokasi untuk mengalirkan air dingin (chilled water) atau pipa utilitas lainnya

Ukuran

- Panel : 60x60cm
- Tebal : 28-42 mm
- Tinggi penyangga : 35cm

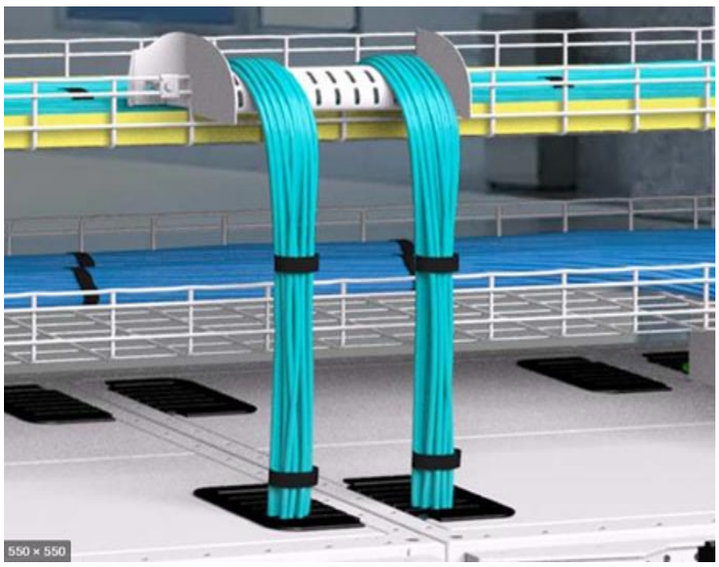
Gambar 2.3.32 Komponen Pendukung Raised Floor

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

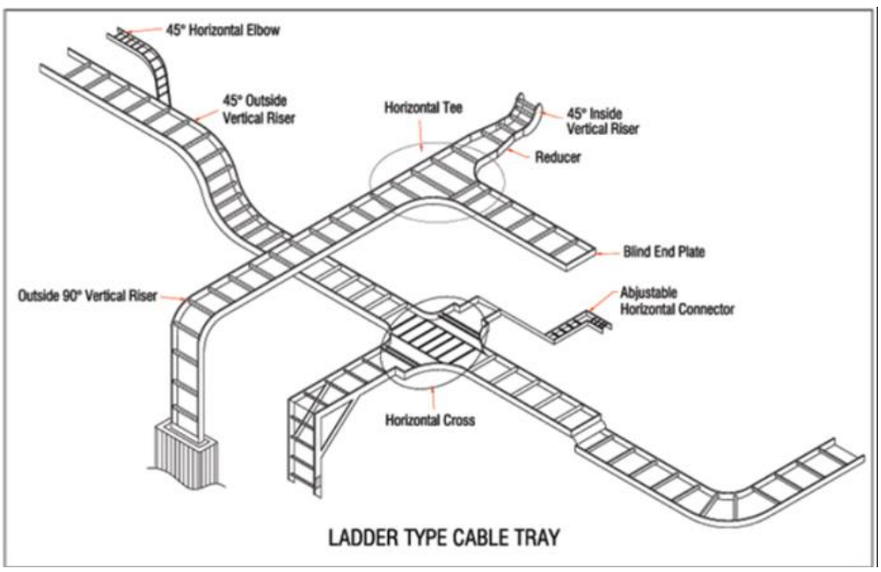


Gambar 2.3.33 Instalasi Kabel Data & Power di Bawah Raised Floor

   b. Atas Rack Server



Gambar 2.3.34 Instalasi Kabel Data di Atas Rack Server dengan Cable Tray

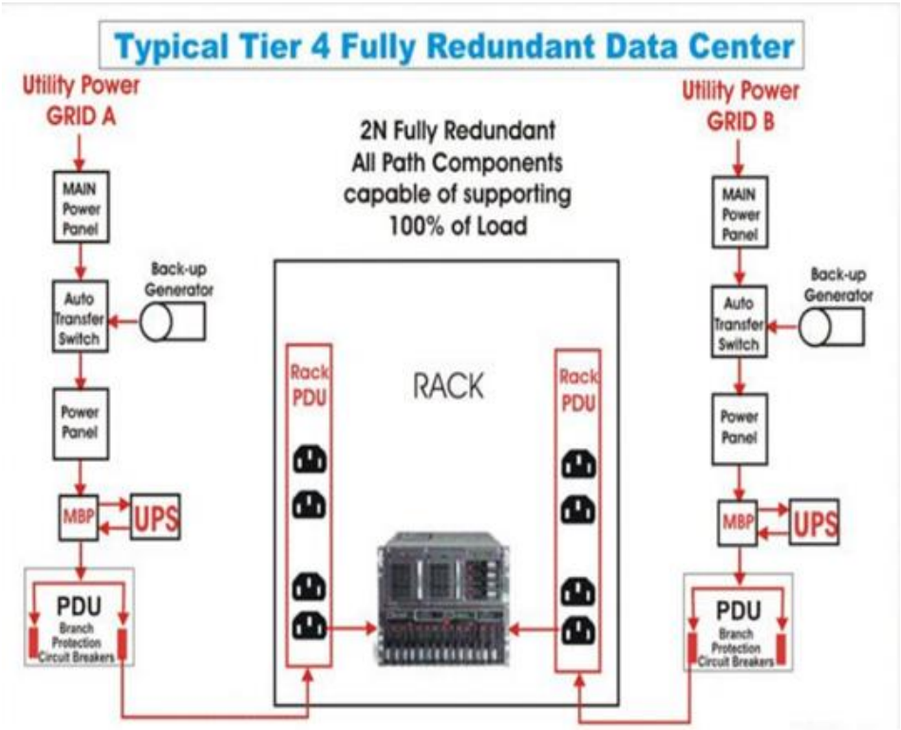


Gambar 2.3.35 Type Kabel Tray Untuk Instalasi Sistem Pengkabelan

c. Rack Location Unit

- Rack server 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 server dapat lebih terkendali.
- Seluruh perangkat server dan peralatan lainnya yang besar diletakan dibagian paling bawah rack server.
- Setiap rack server memiliki dua strip power dengan sumber listrik dari sumber yang berbeda.

Gambar dibawah ini adalah topologi redundansi sistem kelistrikan untuk tipe Tier 4 dengan mode aktif-aktif. Dua buah power strip yang ada di rak server di-supply oleh sumber listrik yang berbeda.



Gambar 2.3.36 Instalasi Sistem Kelistrikan Tier-4 - Fully Redundant

k. Sistem Keamanan Fisik

Terdiri dari sistem pengamanan fisik dan non-fisik pada data center. Fitur sistem pengamanan fisik meliputi akses user ke data center berupa kunci akses memasuki ruangan (kartu akses atau biometrik) dan segenap petugas keamanan yang mengawasi keadaan data center (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 DC terdiri dari keamanan gedung, keamanan ruang komputer, dan kebijakan serta prosedur keamanan.

Gambar 2.3.37 Keamanan DC

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

Gambar 2.3.38 Perangkat Pendukung Keamanan Fisik DC

l. Sistem Pencahayaan

Sistem pencahayaan DC diperlukan untuk menerangi ruang server 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 DC dibagi menjadi tiga lapisan yakni :

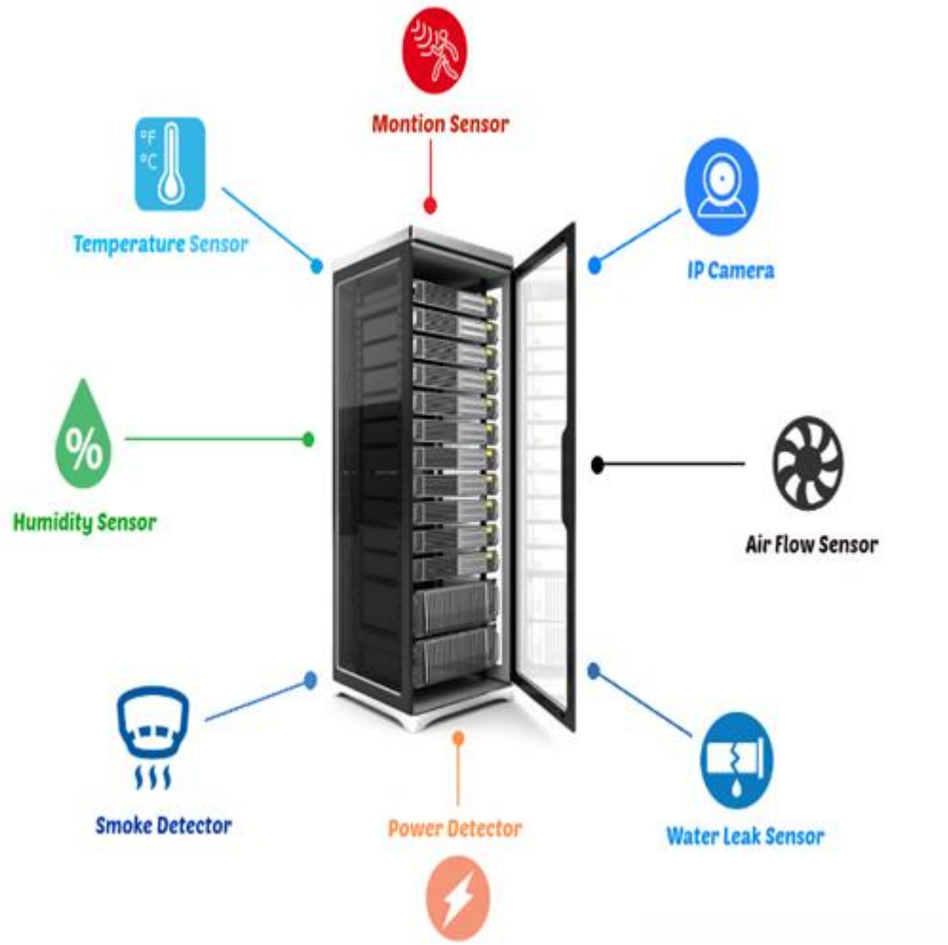
- Level 1 : untuk lokasi yang tidak dihuni. Pencahayaan tidak perlu untuk mendukung kejelasan penglihatan manusia tetapi peralatan pengawas video harus tetap dapat bekerja dengan baik.
- Level 2: untuk lokasi menuju ruang DC – Server Farm berupa gang-gang dan lorong-lorong yang cukup diterangi untuk pergerakan yang aman dan kamera keamanan dapat bekerja dengan baik.
- Level 3: lokasi utama DC – Server Fam dll dan ditempati di mana karyawan akan bekerja. Tingkat cahaya bidang horizontal : 500 lux dan bidang vertikal: 200 lux.

m. Sistem Pemantau Lingkungan

Fungsi utama dari EMS (Environment Monitoring System) adalah memonitor operasional data center dari ancaman lingkungan yang ada disekitarnya. Oleh karena operasional data center yang non-stop maka perlindungan dan monitoring pada fasilitas ini harus diutamakan. Pada umumnya gangguan yang dimonitor oleh EMS ini adalah suhu & kelembaban pada server 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 data center, 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
- mendapatkan alert melalui email / SMS terintegrasi dengan NMS yang ada.



Gambar 2.3.39 Komponen Lingkungan yang akan di Pantau di DC

Gambar 2.3.40 Metode Notifikasi Sistem Pemantauan Lingkungan DC

C. 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 ini, sehingga ketika terjadi bencana, data tetap aman. 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
   Memiliki 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. DRC akan meminimalkan terjadinya

   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 server 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.

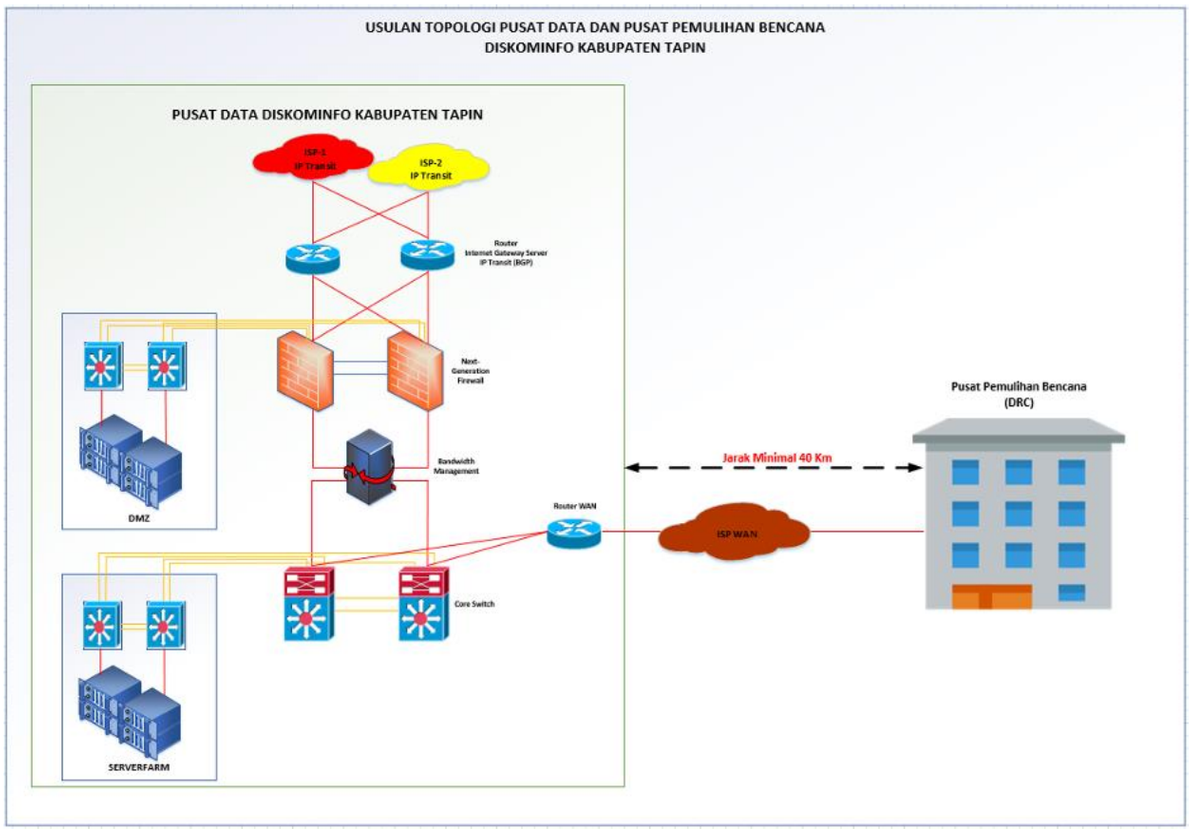
3. *Hot DRC*

   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 data center lama.

D. Usulan Topologi Pusat Data (DC) dan Pusat Pemulihan Bencana (DRC)

Kondisi saat ini, Diskominfo Kabupaten Tapin belum memiliki Pusat Pemulihan Bencana atau DRC. Pengembangan Pusat Pemulihan Bencana dapat menggunakan jasa dari pihak ketiga yakni penyedia layanan colocation server atau Virtual Private Server (VPS).

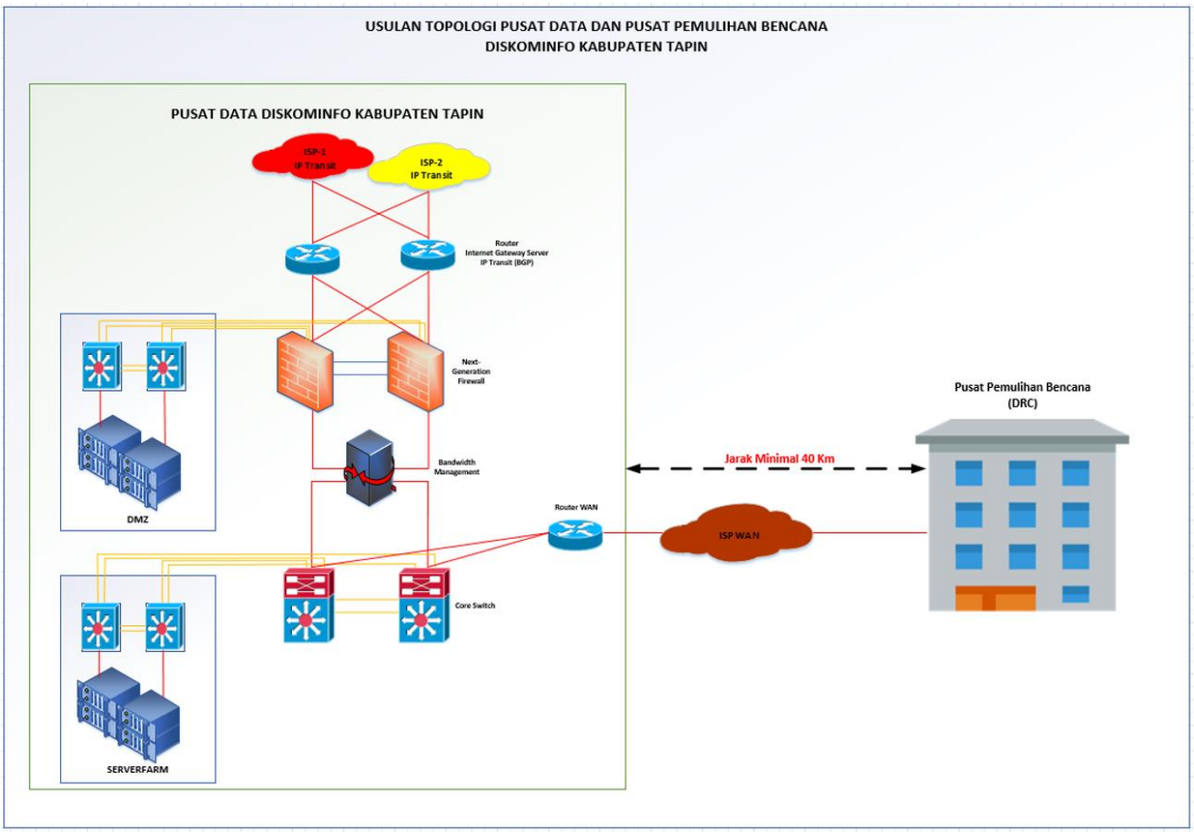
Jika Diskominfo akan melakukan Colocation Server untuk DRC berikut ini usulan untuk topologi dan jarak DRC.



Gambar 2.3.41 Usulan Topologi DC-DRC

Berdasarkan gambar topologi di atas, jarak antara Pusat Data dan Pusat Pemulihan Bencana minimal 40 km dan koneksi jaringan menggunakan layanan jaringan WAN seperti Metro-E atau VPN-IP dari pihak ketiga (provider).

Selain jarak fisik lokasi Pusat Data dan Pusat Pemulihan Bencana, tipe Pusat Pemulihan Bencana yang dipilih yakni Hot DRC untuk menjaga tingkat ketersediaan dan keandalan dari aplikasi, dan data. Berikut ini adalah gambar usulan sinkronisasi Pusat Data dan Pusat Pemulihan Bencana .



Gambar 2.3.42. Usulan Sinkronisasi DC - DRC

Berikut ini adalah konfigurasi sinkronisasi DC – DRC:

a. Router WAN

Menghubungkan DC dan DRC menggunakan layanan WAN yakni Metro-E atau VPN-IP dari pihak ketiga (*provider*);

b. *Load Balancer* Aplikasi (HA Proxy)

Jika server aplikasi lebih dari satu unit, maka digunakan load balancer untuk membagi beban kerja dan juga menjaga ketersediaan aplikasi. Jika salah satu server aplikasi mengalami kegagalan, maka server satunya masih dapat melayani pengguna.

c. Application Server (Server Aplikasi)

File aplikasi (.php), file hasil olah aplikasi, atau file yang diunggah oleh pengguna (.xls, .pdf, .doc) ditempatkan di file server dengan metode folder sharing (*Network File Sharing* – NFS).

d. Database Server (Server Pangkalan Data)

Pangkalan data dikonfigurasi dengan sistem *cluster* (lebih dari satu *instance*) yang tersinkronisasi secara otomatis. Selain itu dengan sistem cluster jika terjadi kegagalan pada satu server maka server lainnya akan menggantikannya secara otomatis.

Server aplikasi akan mengakses ke *load balancer* atau HA Proxy Database Server dengan IP Virtual.

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 Diskominfo Kabupaten Tapin 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. Menggunakan model hirarkis dapat membantu untuk memaksimalkan kinerja jaringan, mengurangi waktu untuk mengimplementasikan dan memecahkan masalah desain, dan meminimalkan biaya.

Desain jaringan redundant 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. Redundansi juga memfasilitasi pembagian beban, yang meningkatkan kinerja jaringan. Redudansi menambah kompleksitas dan biaya pada jaringan, dan harus dirancang dengan hati-hati.

Desain keamanan jaringan dengan menambahkan satu atau lebih perangkat firewall ke topologi jaringan untuk melindungi jaringan Diskominfo Kabupaten Tapin dari penyerang luar.

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)

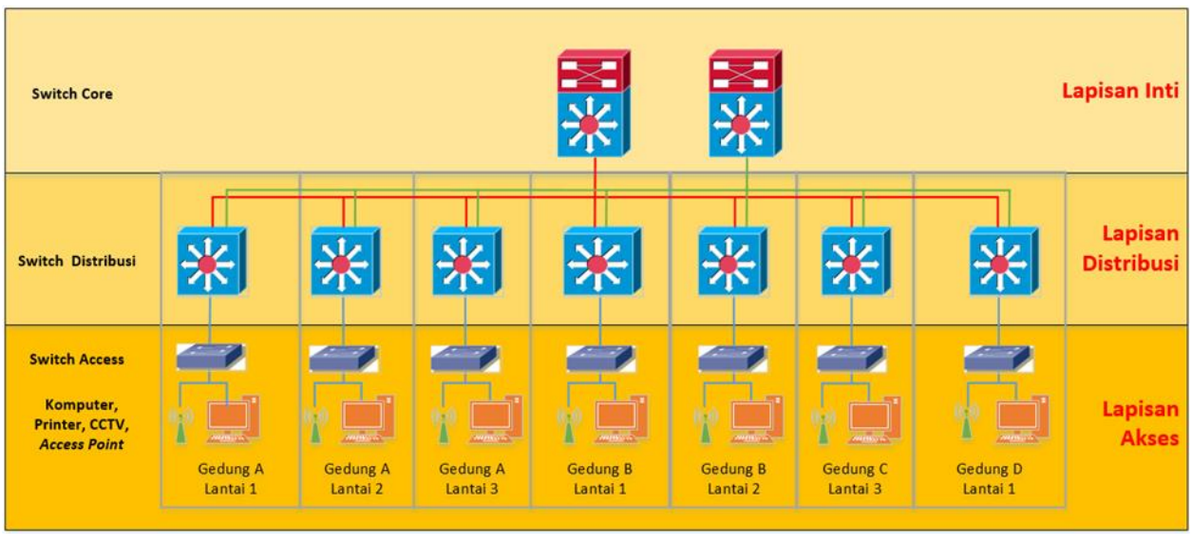
Model desain jaringan berjenjang atau hirarki untuk membantu dalam mengembangkan topologi di lapisan diskrit. Setiap lapisan atau *tier*, dalam hirarki menyediakan fungsi tertentu yang mendefinisikan perannya dalam jaringan secara keseluruhan. Setiap lapisan dapat difokuskan pada fungsi tertentu, memungkinkan 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 redundant. Lapisan inti harus sangat andal dan harus beradaptasi dengan perubahan dengan cepat.

2. Lapisan distribusi (Distribution Layer)
   Lapisan distribusi akan menghubungkan layanan jaringan ke lapisan akses dan implementasi kebijakan tentang keamanan, pemuatan lalu lintas, dan perutean (*routing*). Di jaringan desain yang mencakup LAN virtual (VLAN), lapisan distribusi dapat dikonfigurasi untuk rute antara VLAN.

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



Gambar 2.3.43 Topologi Jaringan 3-*Tier Hierarchy*

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

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.

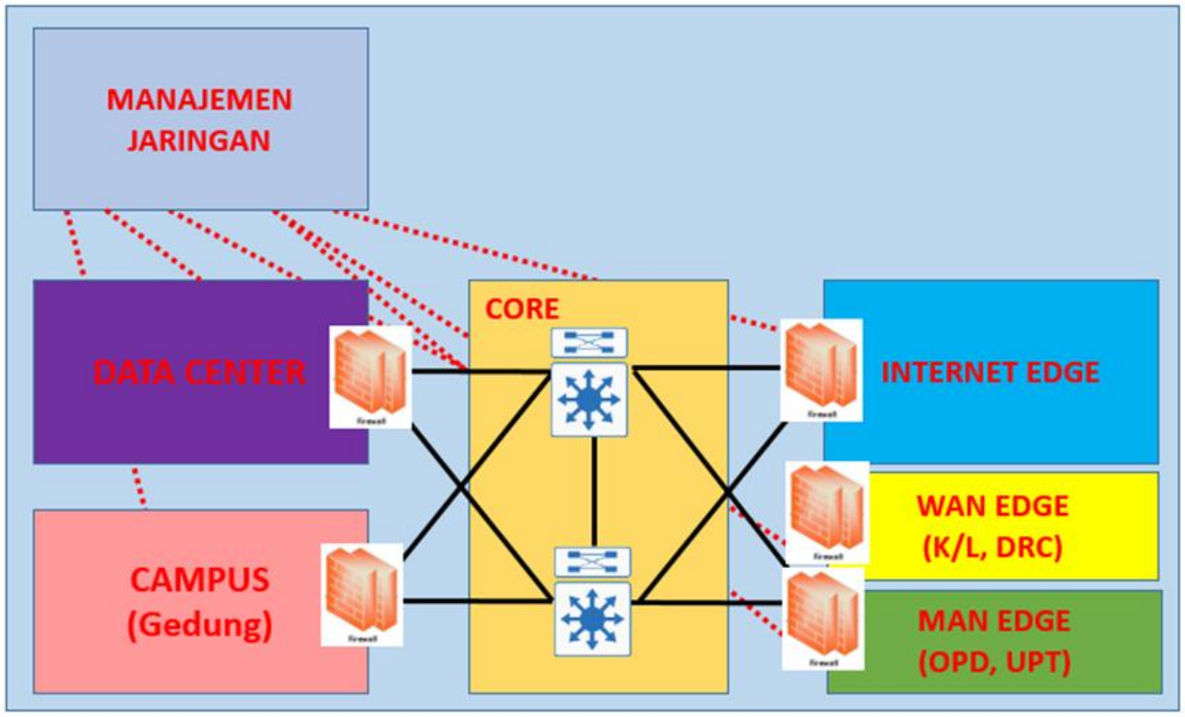
Tabel 2.3.1. Penerapan 3 (Tiga) Lapisan Jaringan Berjenjang (3-Tier Hierarchy)

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*)	
	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:
	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 data center, 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.
	Jaringan Pusat Data
	Jaringan data center memberikan akses jaringan untuk semua server 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.
	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 2.3.44 Arsitektur Jaringan Berbasis Zonasi (*Zoning*)

Arsitektur 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 (*Data Center*)
   Pusat data menampung server, aplikasi, dan perangkat penyimpanan untuk digunakan oleh pengguna internal. Pusat data juga menghubungkan infrastruktur jaringan. Pusat data tidak dapat diakses langsung dari Internet untuk masyarakat umum.

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*). Server manajemen mendukung RADIUS, Kerberos, Protokol Waktu Jaringan (*Network Time Protocol*), Protokol Manajemen Jaringan Sederhana (*Simple Network Management Protocol*), dan lalu lintas *syslog*.

Tabel 2.3.2. Aplikasi Server Manajemen Jaringan

No	Aplikasi Server	Fungsi
1	*Dynamic Host Configuration Protocol* (DHCP)	Server 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 Server* (DNS) Lokal	Sistem yang menghubungkan *Uniform Resource Locator* (URL) dengan *IP Address*. Server DNS berisi *database* alamat IP privat dan nama *host* terkait. Server 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*	Server 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 server yakni *Active Directory Domain Service* (ADDS) pada Windows Server, *Lightweight Directory Access Protocol* (LDAP) pada distro Linux.
4	*Network Time Protocol* (NTP)	Server 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)	Server yang digunakan untuk melayani service *Authentication, Authorization,* dan *Accounting* (AAA) di dalam sebuah jaringan. Singkatnya RADIUS Server ini menyimpan kumpulan *user* dimana *user-user* tersebut dapat digunakan oleh *client* atau *user* yang berada dalam satu jaringan dengan RADIUS Server tersebut.
6	*Network Monitoring System*(NMS)	Suatu server 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 server tertentu, yang disebut server syslog. Ini terutama digunakan untuk mengumpulkan berbagai log perangkat dari beberapa mesin berbeda di lokasi pusat untuk pemantauan dan peninjauan.

5. Jaringan Antar Kota (*Wide Area Network*)
   WAN adalah bagian dari jaringan yang menghubungkan beberapa kantor Kementerian/Lembaga/Pusat Pemulihan Bencana (DRC) yang jauh secara geografis dengan pusat data.

6. Jaringan Dalam Kota (*Metropolitan Area Network*)
   MAN adalah bagian dari jaringan yang menghubungkan beberapa kantor cabang, SKPD, UPT yang cukup jauh secara geografis dengan pusat data tetapi masih dalam satu area kota/kabupaten.

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 Tapin, dan akses jarak jauh *Virtual Private Network* (VPN).

D. Redudansi (Redundancy)

Desain jaringan redundant 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 redundansi 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 cetak biru teknik, 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 ini harus dilindungi dari disengaja atau tidak disengaja kerusakan. Beberapa aset jaringan yang paling penting adalah perangkat jaringan itu sendiri, termasuk server, saklar dan router, dan terutama firewall dan deteksi intrusi sistem (IDS) yang menyediakan layanan keamanan untuk pengguna jaringan. Perangkat-perangkat ini target yang menarik bagi peretas dan harus diperkeras (diperkuat) terhadap intrusi.

2. Menganalisis Risiko Keamanan *(Analyzing Security Risk)*
   Menganalisa ancaman potensial dan mendapatkan pemahaman tentang kemungkinan dan dampak bisnis mereka. Analisis risiko dan konsekuensinya membangun kebijakan keamanan dan desain jaringan yang aman adalah proses yang berkelanjutan, karena risiko berubah dalam tingkat keparahan dan probabilitas.

3. Membangun Kebutuhan Keamanan (*Developing Security Requirements)*
   Masalah keamanan seharusnya tidak mengganggu kemampuan organisasi untuk melakukan bisnis.Itulah 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. 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 server, dan lainnya.

b. Zona Jaringan Antar Gedung (*Campuss Network*)
   Jaringan lokal yang ada di setiap gedung – gedung di komplek perkantoran Pemerintah Kabupaten Tapin yang berdekatan dengan kantor Kominfo dapat dikelola dalam satu jaringan lokal yakni jaringan antar gedung (*Campuss Network*).

c. Zona Data Center (Server Farm)
   Server – server *database, file server, storage* yang tidak langsung diakses oleh pengguna ditempatkan di zona Server Farm.

d. Zona Internet (*Internet Edge*)
   Zona internet adalah zona yang melayani akses internet pengguna atau akses ke aplikasi web internet Pemerintah Kabupaten Tapin.

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

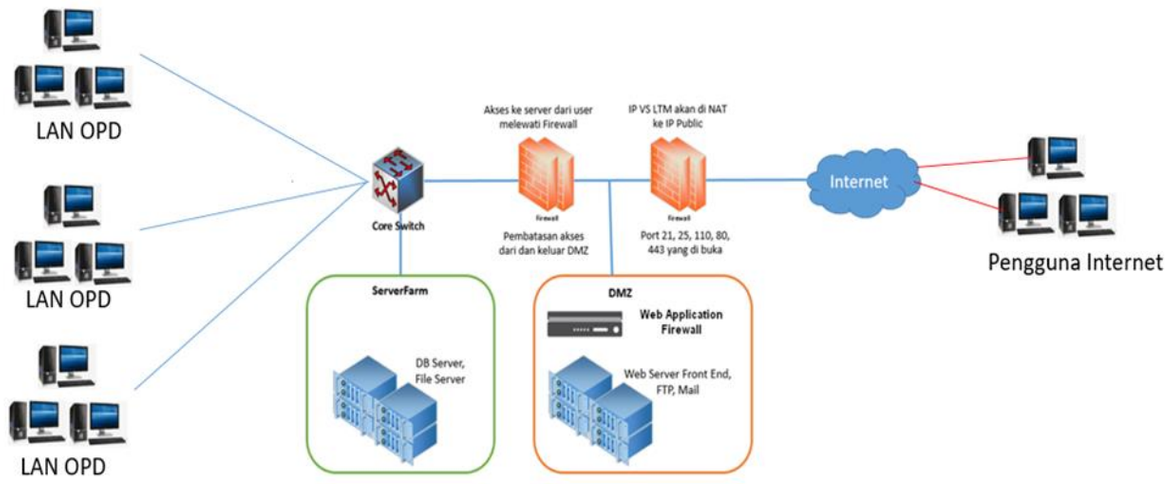
e. Zona Jaringan Antar SKPD (MAN)

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

f. Zona Jaringan Antar Kementerian/Lembaga (WAN)

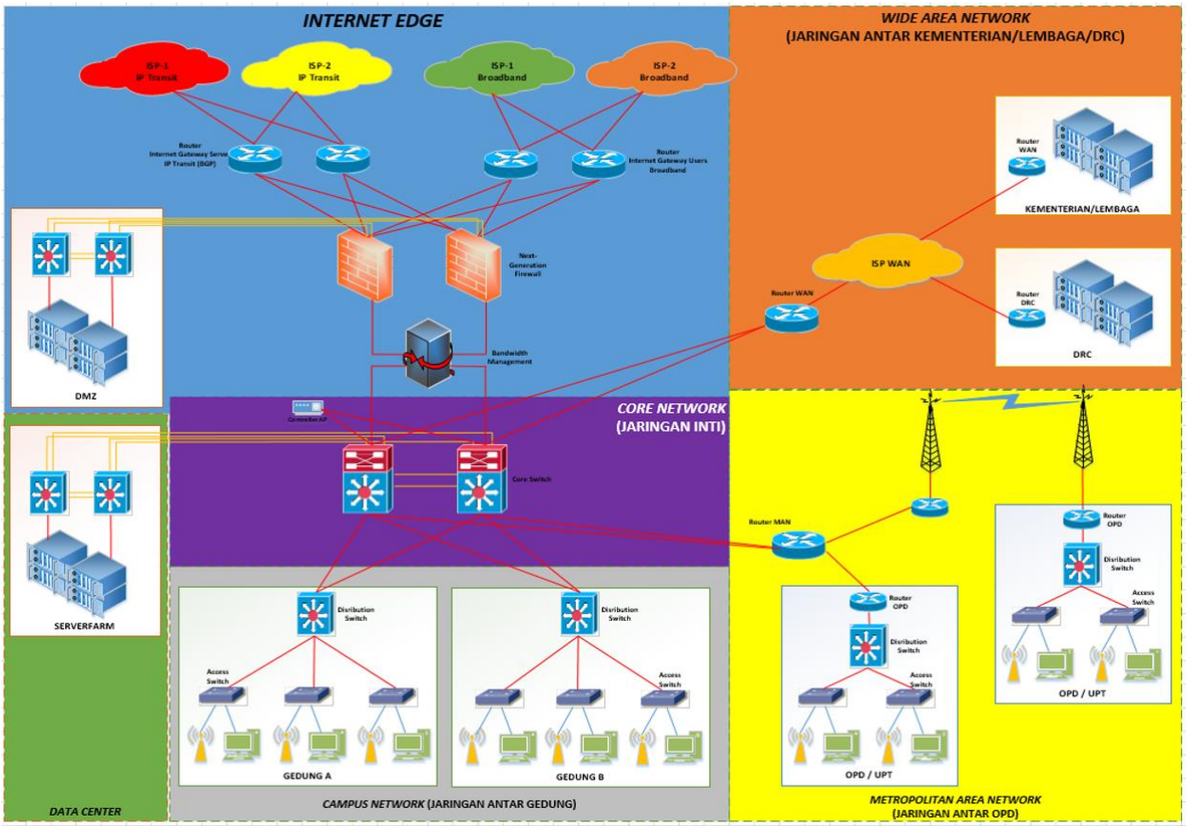
Interkoneksi antara pusat data dengan kementerian atau lembaga lainnya berada di zona Wide Area Network (WAN). Interkoneksi ini menggunakan jaringan Metro-E atau VPN-IP dari penyedia layanan WAN (*provider*). Pembatasan akses ke server – server di Pusat Data seperti alamat IP, port, dan lainnya akan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

Berikut ini adalah topologi Server Farm dengan DMZ.



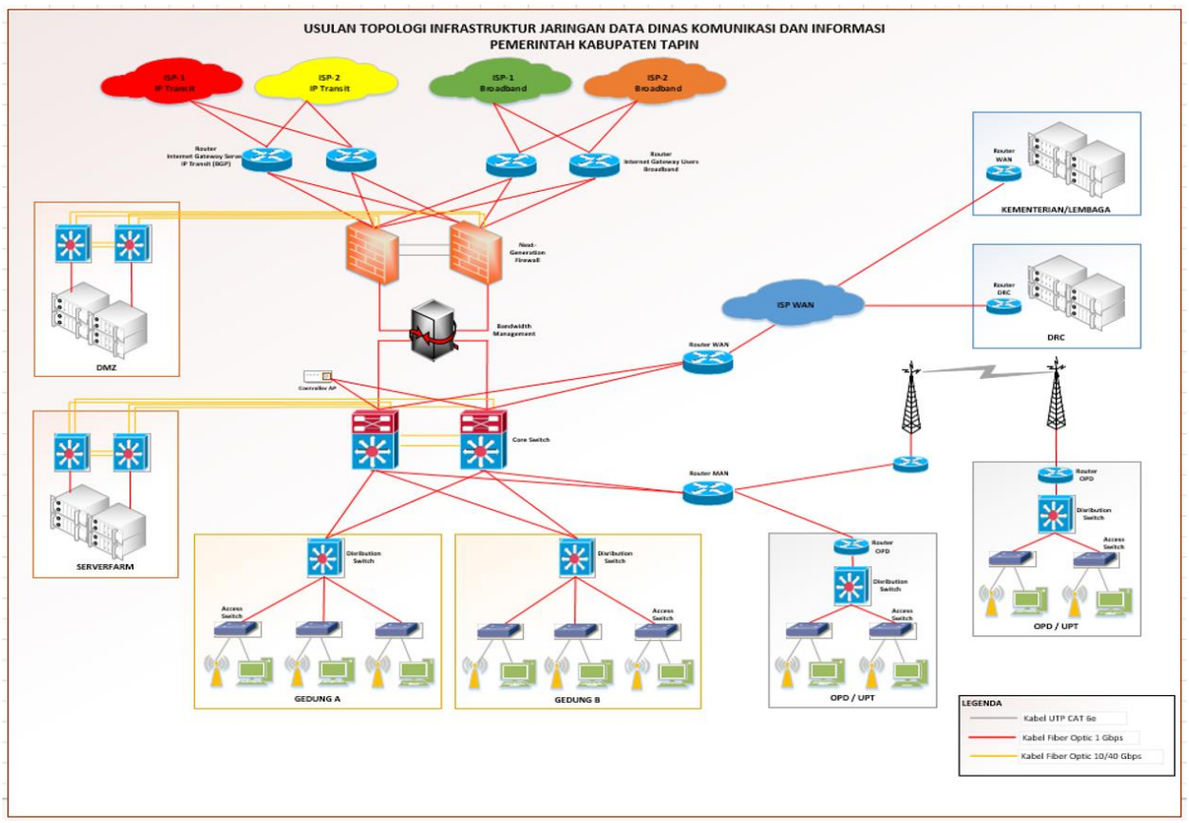
Gambar 2.3.45 Pemisahan Logik Server Farm dengan DMZ

Berdasarkan gambar di atas terlihat bahwa antara Server Farm dan DMZ dipisahkan oleh perangkat firewall dan Core Switch. Pengguna – pengguna di SKPD/UPT akan dibatasi akses ke server – server di Server Farm melalui konfigurasi di router MAN. Akses aplikasi web dari pengguna di SKPD/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 Server 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 Kabupaten Tapin berbasis Zonasi.



Gambar 2.3.46. Usulan Arsitektur Jaringan Data Diskominfo Kabupaten Tapin Berbasis Zonasi

Berikut ini adalah usulan topologi jaringan data Diskominfo Kabupaten Tapin.

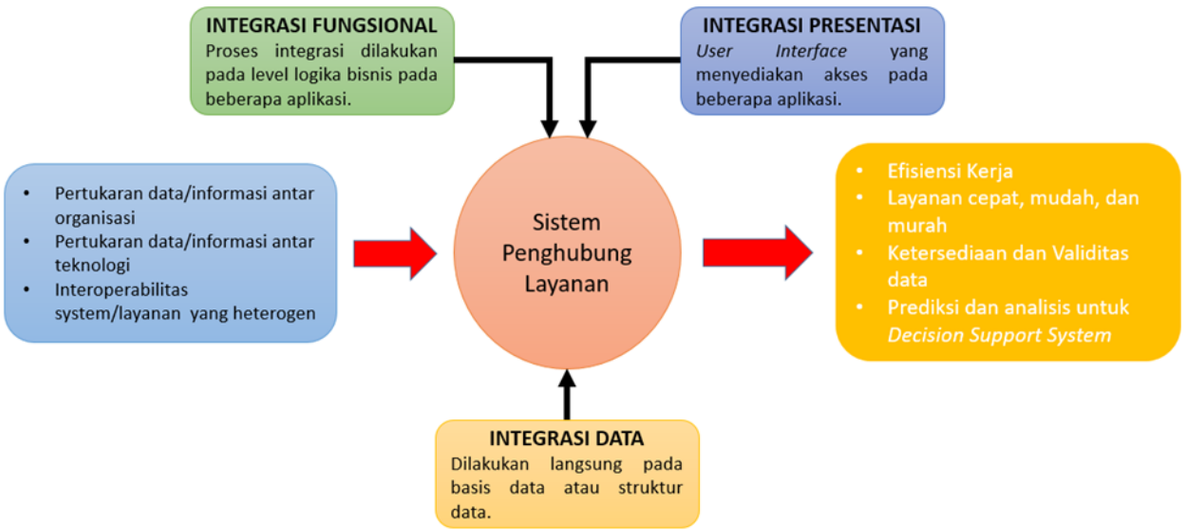


Gambar 2.3.47. Usulan Topologi Infrastruktur Jaringan Data

4. Sistem Penghubung Layanan

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. 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;
d. dapat melakukan prediksi dan analisis untuk sistem pengambil keputusan (*Decision Support System*).



Gambar 2.3.48. Sistem Penghubung Layanan Pemerintah

Sistem Penghubung Layanan Pemerintah terdiri dari:

1. Integrasi Data
   Proses integrasi dilakukan langsung pada basis data atau struktur data dari aplikasi dengan mengabaikan presentasi atau *business logic* ketika membuat integrasi.
2. Integrasi Presentasi
   Proses integrasi dengan membuat antarmuka pengguna (*user interface*) yang menyediakan akses pada beberapa aplikasi.
3. Integrasi Fungsional
   Proses integrasi dilakukan pada level logika bisnis pada beberapa aplikasi.

A. Integrasi Data

Integrasi data memusatkan 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 *tool* 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 dan analisis, dalam 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 kebutuhan:

a. Data yang sama (misalnya: data penduduk) dapat dipakai bersama antar bagian organisasi (antar instansi);
b. Data suatu instansi dapat dipakai bersama oleh instansi-instansi lain yang memerlukan (tidak perlu ada duplikasi data dalam suatu lingkungan organisasi);
c. Meskipun fokus integrasi adalah data, tapi perlu juga integrasi hal-hal lain yang terkait;
d. Integrasi data perlu dilakukan secara cermat karena kesalahan pada integrasi data bisa menghasilkan output/keluaran yang menyimpang dan bahkan menyesatkan pengambilan keputusan nantinya;
e. Syarat integrasi data dapat dipenuhi dengan berbagai cara seperti konsisten dalam penamaan variabel, konsisten dalam ukuran variabel, konsisten dalam struktur pengkodean dan konsisten dalam atribut fisik dari data. Masalah-masalah yang ada pada integrasi data yaitu heterogenitas data, otonomi sumber data, kebenaran dan kinerja query/permintaan.

***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 (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:

1. SOAP (Simple Object Access Protocol)

Gambar 2.3.49. Arsitektur SOAP

Komunikasi data model SOAP dilakukan antara Aplikasi Client/Request (SOAP-Client) dengan Web-API/Provider (SOAP-Server) melalui alamat Web-API dengan protokol HTTPs (Hypertext Transfer Protocol/Secure). Informasi Metadata yang disediakan SOAP-Server 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-Server dalam format dokumen XML SOAP-Envelope yang dibentuk oleh fungsi SOAP-Server pada Web-API.

2. REST (Representational State Transfer)

Gambar 2.3.50. 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 dengan membuat antarmuka pengguna dengan sistem data yang berbeda. Misalnya menggunakan pintu untuk berinteraksi dengan data dan sistem intelegensi bisnis yang berbeda. Jadi bisa dikatakan aplikasi yang terintegrasi sehingga pengguna dapat melakukan operasi tanpa disadari sebenarnya pengguna sedang menjalankan dua aplikasi sekaligus.

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 ti sehingga integrasi proses bisnis semakin lebih mudah dilakukan.

D. API Gateway

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.

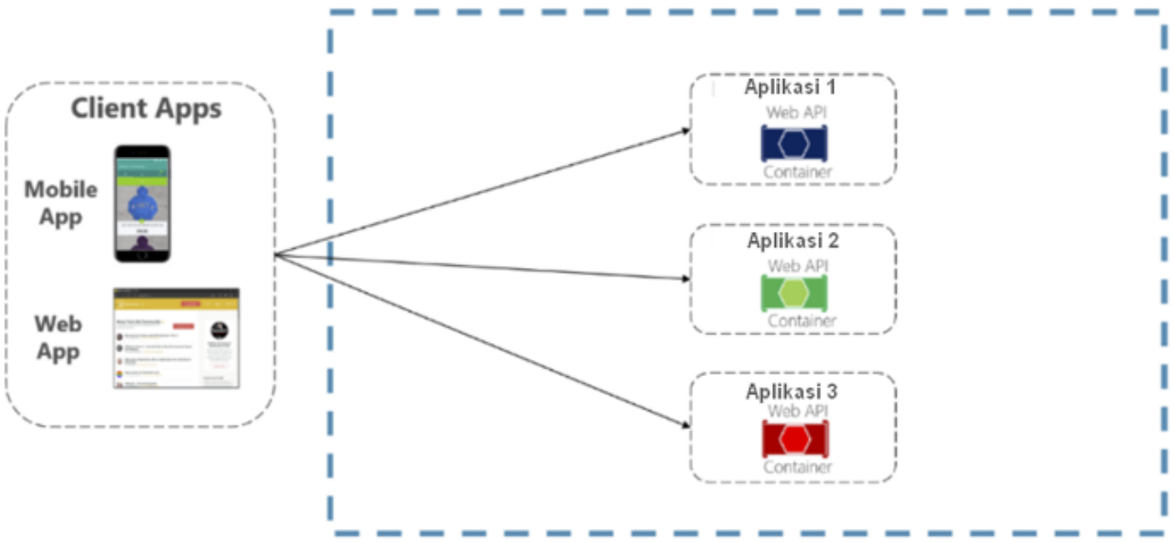
Akses langsung pada Web API Aplikasi

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 servicenya.

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 servicenya.



Gambar 2.3.51 Akses Langsung Antar API

Penggunaan *direct acces* pada service ini mungkin akan cukup baik dan efektif untuk sistem yang kecil. Akan tetapi, untuk sistem yang sudah sangat besar dimana banyak sekali service-service yang digunakan maka penggunaan *direct acces* ini tidak disarankan untuk digunakan.

Akses ke API Gateway

Cara kedua untuk mengakses service-service pada suatu aplikasi adalah dengan menggunakan API *Gateway*. API Gateway merupakan gerbang dari beberapa API (service), bertugas sebagai manajemen API, *merge* beberapa API, otentikasi API dan lain - lain. Kelebihan dari pemakaian API Gateway yakni:

1. **Loose Coupling**

   Dengan adanya API Gateway kita dapat menurunkan tingkat ketergantungan *client* terhadap service-servive yang ada. Apabila kita melakukan *refactoring* dan *maintenance* akan membuat dampak pada client kita secara langsung. Dimungkinkan terjadi *breaking* pada client yang mengkonsumsi service-service kita. API Gateway dapat membuat yang asalnya sangat *coupled* menjadi *loose coupling*.

2. **Terlalu banyak Round Trip**

   Suatu halaman front end atau mobile app terkadang memerlukan banyak sekali pemanggilan ke beberapa service yang berbeda. Atau jika service yang dibuat tidak terlalu bagus, bisa saja terjadi banyak pemanggilan pada service yang sama. Dengan adanya API Gateway kita dapat menurunkan tingkat latency dengan membuat agregate pada API Gateway untuk menggabungkan beberapa pemanggilan API yang terjadi. Biasanya untuk keperluan ini kita mesti dapat melakukan customize pada API Gateway yang kita gunakan.

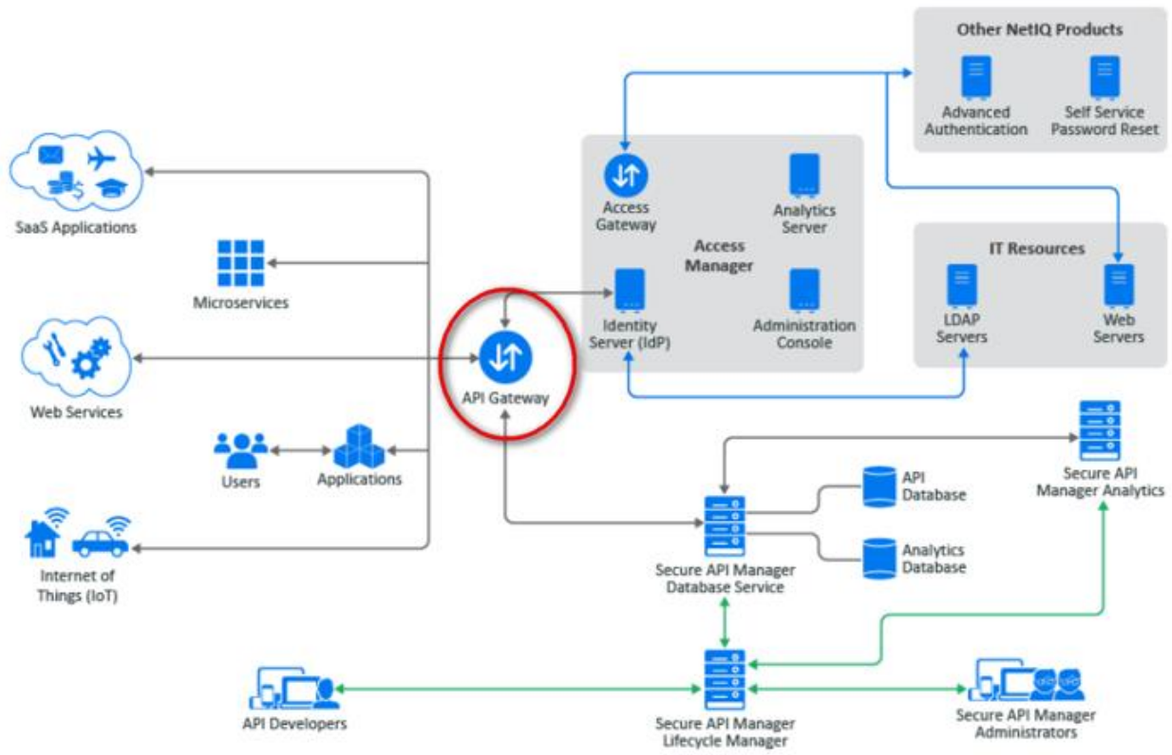
3. **Security**

   Tanpa API Gateway, apabila kita akan menerapkan security maka kita harus membuat dan mengimplementasikannya di setiap service yang ada. Hal ini menjadi tidak efisien dan terlalu banyak usaha yang harus dikorbankan. Dengan API Gateway kita hanya perlu melakukan implement security di level API Gateway dan setiap service kita tempatkan di lingkungan private yang tidak terekspose secara langsung dari luar.

4. **Cross-cutting concern.**

   Proses penerapan authorization, SSL, dan hal-hal lainya yang berhubungan tetapi bukan proses utama atau pendukung dapat kita implementasikan di bagian gateway sehingga membuat setiap service menjadi lebih sederhana.

API Gateway adalah suatu service yang dibuat khusus dan dijadikan sebagai pintu utama atau entry point dari dunia luar untuk masuk ke dalam service-service kita. API gateway akan berada di antara client dan service-service kita. Ini berfungsi sebagai reverse proxy untuk me routing request dari client ke server-service.



Gambar 2.3.52 Arsitektur API Gateway

Jika kita lihat dari 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*
- *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 perusahaan, 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.

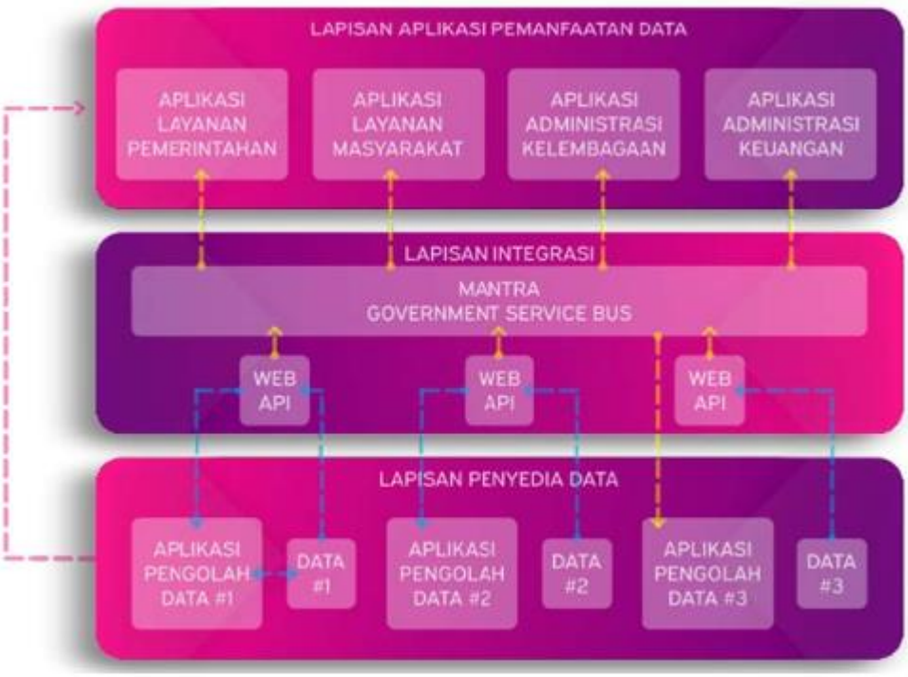
Platform API Management

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)
6. MANTRA (Manajemen Integrasi Informasi dan Pertukaran Data) - Kominfo

   Sejak 2011, Kemkominfo telah mengembangkan 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.

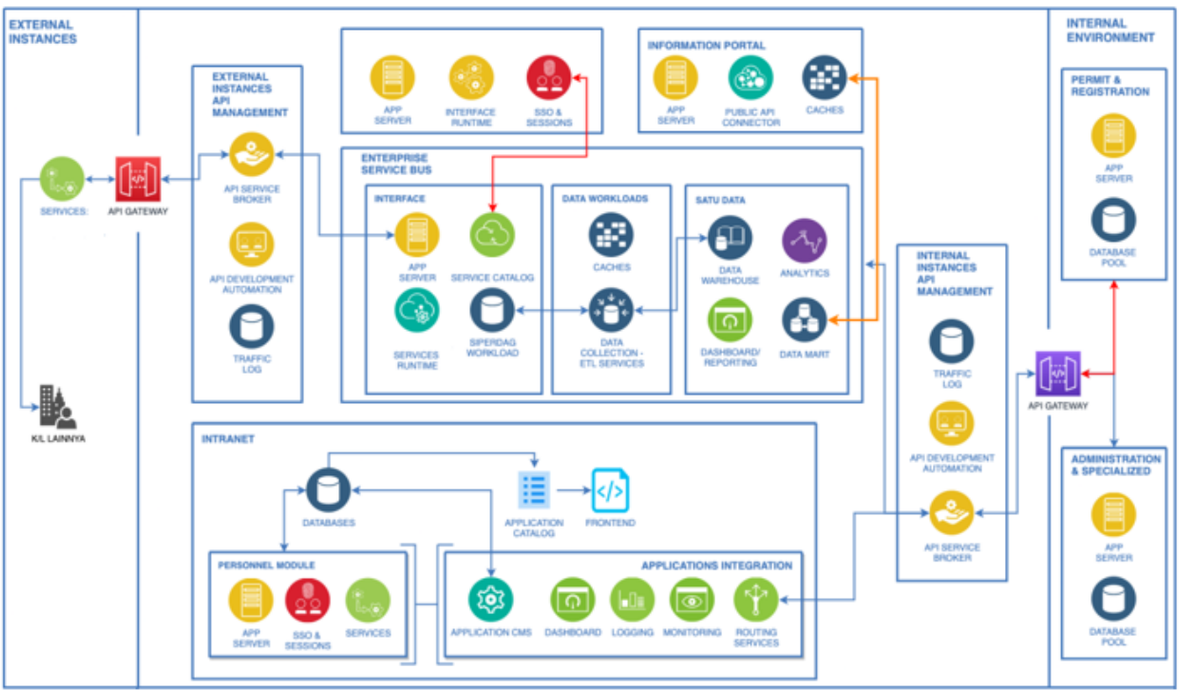
Aplikasi MANTRA dikembangkan dengan menerapkan teknologi dan pemrograman berbasis standar terbuka (open standard), antara lain PHP, SOAP (Simple Object Access Protocol), REST (Representational State Transfer), HTTP (Hypertext Transfer Protocol), dan menggunakan format data XML (Extensible Markup Language)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



Gambar 2.3.53. Arsitektur API Gateway MANTRA

API Gateway Internal dan Eksternal

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 melalui melalui jalur internet.



Gambar 2.3.54. Arsitektur API Gateway Internal dan Eksternal

Pada gambar di atas, terlihat ada dua API Gateway yakni API Gateway Eksternal untuk melayani akses ke Kementerian/Lembaga dan API Gateway Internal untuk melayani akses service internal/intranet.

C. Keamanan Informasi SPBE

1. Arsitektur Keamanan SPBE

Arsitektur keamanan merupakan aspek vital dalam usaha organisasi untuk melindungi aset-aset penting yang dimilikinya. 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. Ia 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 tersebut juga mengandung risiko keamanan. Mengingat kondisi yang berbeda-beda antara satu organisasi dengan organisasi lainnya, maka analisis dan desain arsitekturnya mesti mempertimbangkan variabel dan risiko spesifik yang mungkin terjadi pada masing-masing organisasi.

Gambar 2.3.55. Arsitektur Keamanan SPBE

Arsitektur Keamanan Informasi SPBE bertujuan untuk mendukung Visi dan Misi Diskominfo Kabupaten Tapin. Perancangan arsitektur keamanan menggunakan model *Sherwood Applied Business Security Architecture* (SABSA) yang merupakan metodologi pengembangan arsitektur keamanan informasi tingkat enterprise yang berdasarkan risiko. Dari 6 (enam) layer arsitektur keamanan SABSA, pada Arsitektur Keamanan Informasi Diskominfo Tapin menggunakan 4 (empat) layer yakni:

1. Kontekstual Keamanan Informasi, terdiri dari:
    a. Konsep Arsitektur Keamanan,
    b. Standarisasi Keamanan,
    c. Manajemen Risiko,
    d. Kebijakan Dan Regulasi
    e. Ruang Lingkup Keamanan
    f. Komitmen Organisasi
    g. Sumber Daya Organisasi
2. Arsitektur Logis Keamanan Informasi, terdiri dari:
    a. Manajemen Perangkat Keamanan
    b. *Teleworking*
    c. Akses Kontrol
    d. Kriptografi
    e. Perlindungan terhadap Malware
    f. Akuisisi Pengembangan dan Pemeliharaan
3. Arsitektur Fisik Keamanan Informasi, terdiri dari:
    a. Manajemen Aset
    b. Pengamanan Aset
    c. Peralatan Keamanan
    d. Hubungan dengan Pihak Ketiga
4. Komponen Arsitektur Keamanan Informasi, terdiri dari:
    a. Manajemen Insiden
    b. Evaluasi Kinerja dan Kepatuhan
    c. Peningkatan Berkesinambungan
    d. Manajemen Layanan

e. Blueprint TI

Komponen Arsitektur keamanan terdiri dari Standar Keamanan, Penerapan Keamanan, dan Kelaikan Keamanan.

2. Manajemen Keamanan Informasi SPBE

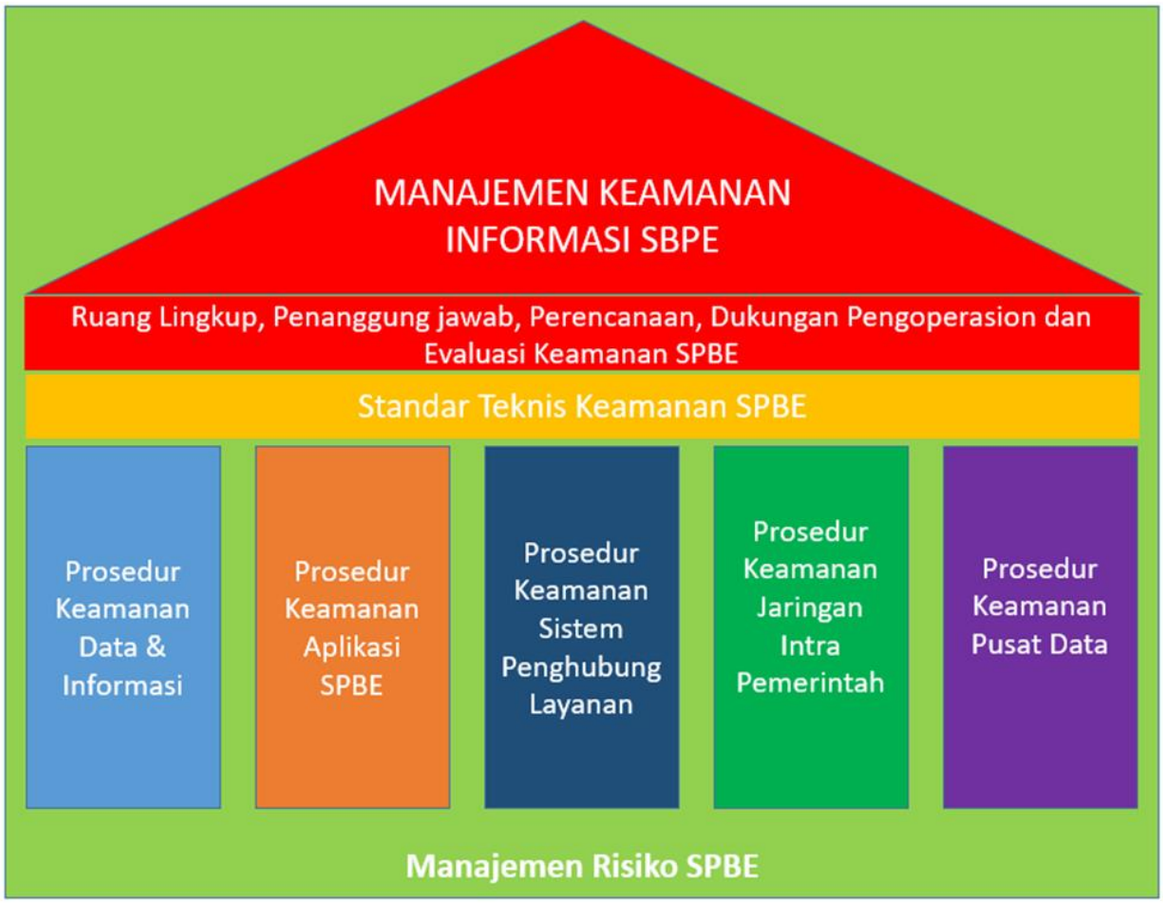
Dasar hukum dari Manajemen Keamanan Informasi SPBE yakni:

a. Perpres 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
b. Permenpan-RB 59 tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
c. Perban BSSN no 4 tahun 2021 tentang Pedoman Manajemen Keamanan SPBE dan Standar Teknis & Prosedur Keamanan SPBE;
d. Permendagri no 18 tahun 2020 tentang Peraturan Pelaksanaan Peraturan Pemerintah no 13 tahun 2019 tentang Laporan dan Evaluasi Penyelenggaraan Pemerintah Daerah.

Seuai dengan Perpres 95 tahun 2018 disebutkan bahwa Manajemen Keamanan Informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi. Selanjutnya, di dalam Perban BSSN no 4 tahun 2021 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

Selain pedoman manajemen terdapat juga standar teknis dan prosedur keamanan sebagai acuan persyaratan minimal keamanan dalam bentuk standar nasional, internasional serta regulasi peraturan terkait 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 2.3.56. Pilar Manajemen dan Standar Teknis Keamanan SPBE

Dalam proses penyusunan manajemen keamanan SPBE dapat menggunakan acuan gambar di bawah ini.

Gambar 2.3.57. Proses Manajemen Keamanan Informasi SPBE

b. SNI ISO 27001:2013 – 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 2.3.3. 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 dari SNI ISO 27001:2013 meliputi:

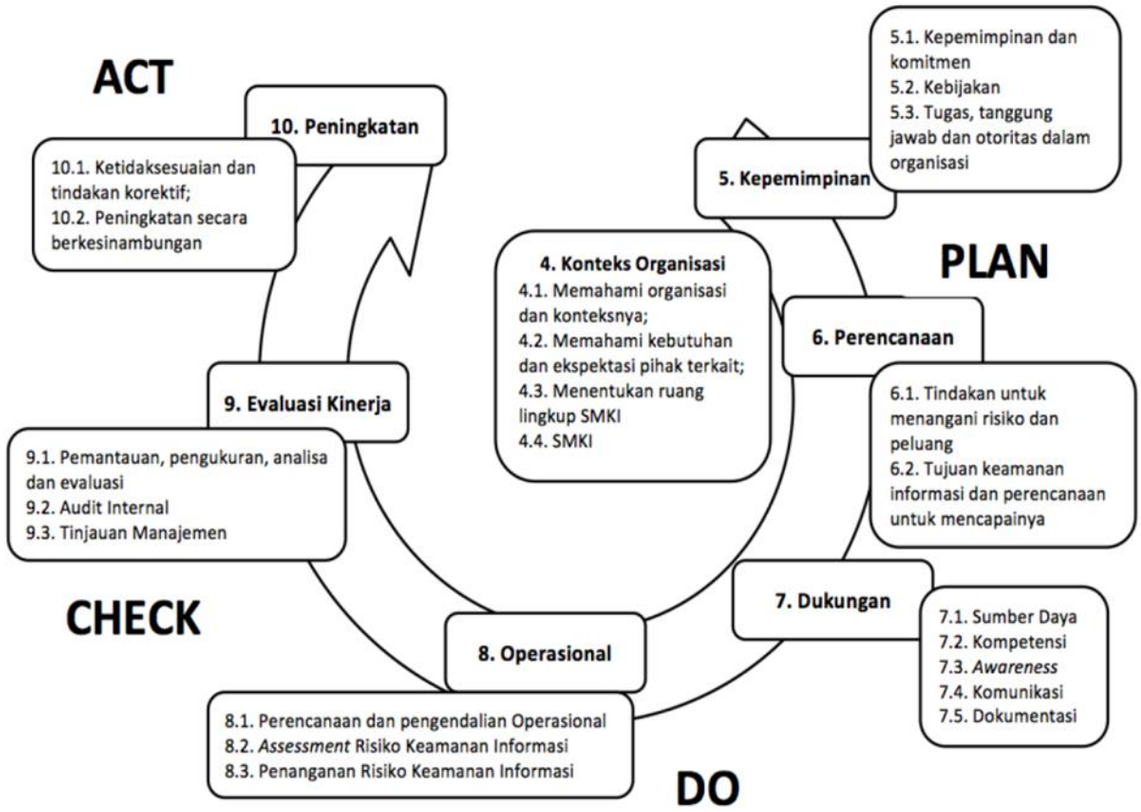
a. Mendefinisikan persyaratan untuk menetapkan, menerapkan, memelihara, meningkatkan secara berkesinambungan terhadap sistem manajemen keamanan informasi;
b. Persyaratan dalam standar ini bersifat umum dimaksudkan agar dapat diterapkan oleh organisasi tanpa membatasi jenis, ukuran, serta sifat organisasi;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

SNI ISO 27001:2013 mensyaratkan penetapan sasaran kontrol dan kontrol keamanan informasi meliputi 14 area pengamanan sebagai berikut:

1. Kebijakan Keamanan Informasi
   Untuk memberikan arahan dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi serta hukum yang relevan.
2. Organisasi Keamanan Informasi

Untuk membentuk kerangka kerja manajemen untuk mengendalikan implementasi, dan operasi keamanan informasi serta untuk menjamin keamanan teleworking dalam organisasi.

3. Sumber Daya Manusia Menyangkut Keamanan Informasi
   Untuk memastikan bahwa setiap pegawai memahami peran dan tanggung jawab mereka di dalam organisasi.
4. Manajemen Aset
   Untuk mengenali aset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai dengan organisasi.
5. Kendali Akses
   Untuk memastikan pengendalian dari setiap informasi.
6. Kriptografi
   Untuk memastikan penggunaan kriptografi secara tepat dan efektif dalam melindungi kerahasian,
7. keaslian dan keutuhan sebuah informasi.
   Keamanan Fisik dan Lingkungan Untuk mencegah akses fisik dari pihak yang tidak berkewenangan sehingga dapat menimbulkan kerusakan terhadap informasi dan fasilitas pengolah informasi di dalam organisasi.
8. Keamanan Operasi
   Untuk menjamin operasi fasilitas pengolahan informasi yang baik dan benar.
9. Keamanan Komunikasi
   Untuk menjamin perlindungan keamanan informasi dalam jaringan dan fasilitas pendukung pengolah informasi.
10. Pengadaan/Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi
    Untuk memastikan bahwa keamanan merupakan bagian yang utuh dari informasi.
11. Hubungan dengan Pemasok
    Untuk memastikan perlindungan dari aset organisasi yang dapat diakses oleh pemasok.
12. Manajemen Insiden Keamanan Informasi
    Untuk memastikan kejadian dan kelemahan keamanan sistem informasi terkait dengan sistem
    informasi dilakukan sinkronisasi sehingga dimungkinkan tindakan koreksi yang tepat waktu.
13. Manajemen Keberlangsungan Bisnis (*Business Continuity Management*)
    Untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek
    kegagalan utama SI atau bencana dan untuk memastikan keberlanjutannya secara tepat waktu.
14. Kepatuhan
    Untuk mencegah pelanggaran terhadap undang undang atau kewajiban kontrak dan setiap persyaratan keamanan.



Gambar 2.3.58. Struktur SNI ISO 27001:2013

3. 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.

a. Keamanan Data dan Informasi

Standar teknis keamanan data dan informasi meliputi aspek:

1. Kerahasiaan (*Confidentiality*);
2. Keaslian (*Authentication*);
3. Keutuhan (*Integrity*);
4. Kenirsangkalan (*Non-Repudiation*); dan
5. Ketersediaan (*Availability*).

Berikut ini adalah rincian beberapa prosedur untuk memenuhi aspek – aspek standar teknis.

a. Kerahasiaan dengan menerapkan:
   - Klasifikasi informasi
   - Enkripsi dengan sistem kriptografi
   - 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 2.3.4 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.

Standar Kriptografi untuk Enkripsi

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 2.3.59. Standar Kriptografi untuk Enkripsi

b. Keaslian
   - Mekanisme verifikasi;
   - Mekanisme validasi; dan

- Menerapkan sistem *hash function*.

c. Keutuhan
   - Penerapan pendeteksian modifikasi
   - 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.

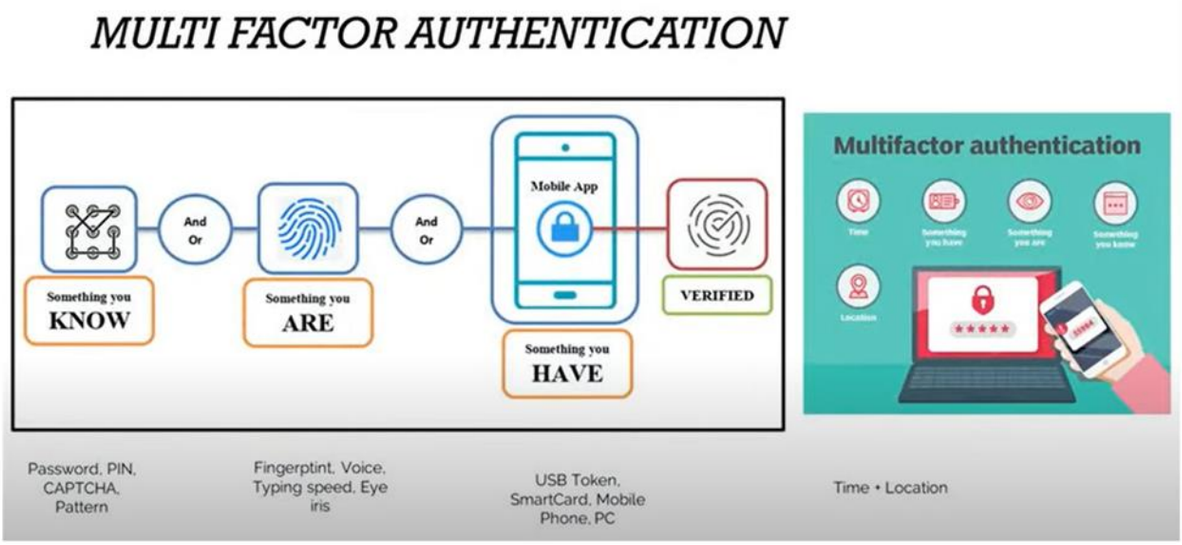
b. Keamanan Aplikasi SPBE

Keamanan aplikasi SPBE meliputi aplikasi berbasis web dan aplikasi berbasis *mobile*. 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

Untuk pemenuhan beberapa aspek standar keamanan aplikasi berbasis web diperlukan prosedur – prosedur seperti berikut ini.

a. Autentikasi
   1. menggunakan manajemen kata sandi untuk proses autentikasi;
   2. menerapkan verifikasi kata sandi pada sisi server;
   3. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
   4. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
   5. mengatur mekanisme pemulihan kata sandi;
   6. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
   7. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.



Gambar 2.3.60. Multi Factor Authentication

b. 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.

c. 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.

d. Validasi input
   - menerapkan fungsi validasi input pada sisi server;
   - 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.

e. 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.

f. Penanganan error dan pencatatan log
- mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
- menggunakan metode penanganan error untuk mencegah kesalahan terprediksi dan tidak terduga
- serta 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.

g. 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.

h. 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.

i. 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.

j. 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.

k. 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 server untuk mengunduh file sesuai ekstensi yang ditentukan.

l. 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.

m. Keamanan konfigurasi
- mengkonfigurasi server sesuai rekomendasi server 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 server 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 server, 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 server* 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 ini 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.

Untuk pemenuhan beberapa aspek standar keamanan 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 server perantara saat client mengakses server 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;
   - 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.
   - 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.
   - Memenuhi persyaratan ketahanan material gedung meliputi ketahanan api, dan pengembunan.

d. Perangkat Pengamanan dan Pendukung
   - *CCTV*
   - *Access Door*
   - Sistem Pemadam Kebakaran
   - Sistem Pendinginan
   - 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.
   - 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 server dan perangkat jaringan utama tidak boleh dilakukan secara remote.

4. Aktivitas Keamanan Informasi

Dalam menjalankan keamanan SPBE, Diskominfo 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.

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
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
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
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
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
3. Komunikasi

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.

Gambar 2.3.61 Fungsi dan Kategori Aktivitas Keamanan Informasi

LAMPIRAN