BUPATI TEGAL
PROVINSI JAWA TENGAH

PERATURAN BUPATI TEGAL
NOMOR 45 TAHUN 2022

TENTANG

ARSITEKTUR SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA
BUPATI TEGAL,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 10 Peraturan Daerah Kabupaten Tegal Nomor 2 Tahun 2020 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Tegal, perlu menetapkan Peraturan Bupati tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten Dalam Lingkungan Propinsi Djawa Tengah (Berita Negara Repubik Indonesia Tahun 1950 Nomor 42);
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843); sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara

Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
5. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143);
6. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali, terakhir dengan Undang Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245);
7. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189) sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor185);

8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
10. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembuatan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2018 Nomor 157);
11. Peraturan Menteri Negara Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2018 tentang Pedoman Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 154) sebagaimana telah diubah dengan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
12. Peraturan Badan Siber 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 (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
13. Peraturan Daerah Kabupaten Tegal Nomor 11 Tahun 2009 tentang Organisasi dan Tata Kerja Lembaga Lain Kabupaten Tegal (Lembaran Daerah Kabupaten Tegal Tahun 2009 Nomor 11, Tambahan Lembaran Daerah Kabupaten Tegal Nomor 35);
14. Peraturan Daerah Kabupaten Tegal Nomor 2 Tahun 2020 tentang Penyelenggaraan Sistem Pemerintahan

Berbasis Elektronik di Kabupaten Tegal (Lembaran Daerah Kabupaten Tegal Tahun 2020 Nomor 2, Tambahan Lembaran Daerah Kabupaten Tegal Nomor 133);

15. Peraturan Daerah Kabupaten Tegal Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Tegal (Lembaran Daerah Kabupaten Tegal Tahun 2016 Nomor 12, Tambahan Lembaran Daerah Kabupaten Tegal Nomor 110) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Daerah Kabupaten Tegal Nomor 10 Tahun 2021 tentang Perubahan Kedua Atas Peraturan Daerah Kabupaten Tegal Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Tegal (Lembaran Daerah Kabupaten Tegal Tahun 2021 Nomor 10, Tambahan Lembaran Daerah Kabupaten Tegal Nomor 153);
16. Peraturan Daerah Kabupaten Tegal Nomor 3 Tahun 2019 tentang Rencana Pembangunan Jangka Menengah Daerah Kabupaten Tegal Tahun 2019-2024 (Lembaran Daerah Kabupaten Tegal Tahun 2019 Nomor 3, Tambahan Lembaran Daerah Kabupaten Tegal Nomor 129) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Tegal Nomor 2 Tahun 2021 tentang Perubahan Atas Peraturan Daerah Kabupaten Tegal Nomor 3 Tahun 2019 tentang Rencana Pembangunan Jangka Menengah Daerah Kabupaten Tegal Tahun 2019-2024 (Lembaran Daerah Kabupaten Tegal Tahun 2021 Nomor 3, Tambahan Lembaran Daerah Kabupaten Tegal Nomor 147);
17. Peraturan Bupati Tegal Nomor 82 Tahun 2021 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Perangkat Daerah dan Staff Ahli Bupati di Lingkungan Pemerintah Kabupaten Tegal (Berita Daerah Kabupaten Tegal Tahun 2021 Nomor 82).

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG ARSITEKTUR SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Tegal.
2. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Dewan Perwakilan Rakyat Daerah yang selanjutnya disebut DPRD adalah Lembaga Perwakilan Rakyat Daerah sebagai unsur Penyelenggara Pemerintahan Daerah.
4. Bupati adalah Bupati Tegal.
5. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintahan oleh pemerintah daerah dan dewan perwakilan rakyat daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
6. Anggaran Pendapatan dan Belanja Daerah yang selanjutnya disingkat APBD adalah rencana keuangan tahunan Daerah yang ditetapkan dengan Peraturan Daerah.
7. Peraturan Presiden yang selanjutnya diringkas Perpres adalah Peraturan Perundang-undangan yang dibuat oleh Presiden.
8. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
9. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang berkaitan dengan pemrosesan, pengelolaan dan penyampaian atau pemindahan informasi antar sarana/media.
10. Pengguna SPBE adalah instansi pusat, pemerintah daerah, pegawai Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan Layanan SPBE.

11. Tata Kelola SPBE adalah kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu.
12. Rencana Induk SPBE Daerah, selanjutnya disebut Rencana Induk SPBE, adalah dokumen perencanaan pembangunan SPBE untuk jangka waktu 5 (lima) tahun.
13. 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.
14. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi instansi pusat dan Pemerintah Daerah masing-masing.
15. Data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar, peta, tanda, isyarat, tulisan, suara, dan/atau bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi.
16. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
17. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data,pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
18. Infrastruktur SPBE Pemerintah Daerah adalah infratsruktur SPBE yang diselenggarakan oleh Daerah.
19. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.
20. Aplikasi umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau Pemerintah Daerah.
21. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh instansi pusat atau Pemerintah Daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.
22. Audit Teknologi Informasi dan Komunikasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.

23. Data Center adalah ruang khusus yang disediakan oleh Perangkat Daerah yang membidangi urusan komunikasi dan informatika yang digunakan untuk menyimpan server, media penyimpanan data, dan perangkat lain milik unit kerja lain yang terhubung melalui jaringan dengan sistem informasi kedinasan.
24. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
25. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
26. Sistem Penghubung Layanan adalah perangkat integrasi atau penghubung untuk melakukan pertukaran Layanan SPBE.
27. *Standar Operasional Prosedur* yang selanjutnya disingkat SOP adalah panduan yang digunakan untuk memastikan kegiatan operasional organisasi atau perusahaan berjalan dengan lancar.
28. Tim Pengarah SPBE Daerah yang selanjutnya disebut Tim Pengarah, adalah tim lintas Perangkat Daerah yang memiliki fungsi untuk melakukan koordinasi dan penerapan kebijakan SPBE di Daerah.

BAB II
ARSITEKTUR SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAERAH
Pasal 2

(1) Arsitektur SPBE Daerah dimaksudkan untuk memberikan panduan dalam pelaksanaan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terpadu.
(2) Arsitektur SPBE Daerah sebagaimana dimaksud pada ayat (1) memuat :
    a. Referensi Arsitektur SPBE; dan
    b. Domain Arsitektur SPBE.
(3) Referensi Arsitektur SPBE sebagaimana dimaksud pada ayat (2) huruf a mendeskripsikan komponen dasar arsitektur baku yang digunakan sebagai acuan untuk penyusunan setiap Domain Arsitektur SPBE.
(4) Domain Arsitektur SPBE sebagaimana dimaksud pada ayat (2) huruf b mendeskripsikan substansi arsitektur yang memuat :
    a. domain arsitektur proses bisnis;
    b. domain arsitektur data dan informasi;
    c. domain arsitektur layanan SPBE;
    d. domain arsitektur aplikasi SPBE;
    e. domain arsitektur infrastruktur SPBE; dan
    f. domain arsitektur keamanan SPBE.

(5) Arsitektur SPBE Daerah sebagaimana dimaksud pada ayat (1) dipetakan dan diselaraskan berdasarkan Referensi Arsitektur SPBE nasional.
(6) Arsitektur SPBE Daerah sebagaimana dimaksud pada ayat (1) disusun dengan berpedoman pada Arsitektur SPBE nasional dan Rencana Pembangunan Jangka Menengah Daerah.
(7) Penyusunan Arsitektur SPBE Daerah dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang Komunikasi dan Informatika.
(8) Dalam menyusun Arsitektur SPBE Daerah, Perangkat Daerah sebagaimana dimaksud pada ayat (7) dapat melakukan konsultasi dengan Tim Koordinasi SPBE Nasional.
(9) Arsitektur SPBE Daerah sebagaimana dimaksud pada ayat (1) menjadi pedoman dalam proses integrasi Layanan SPBE Daerah dengan Pemerintah Daerah lain dan/atau Instansi Pusat.

Pasal 3

(1) Arsitektur SPBE Daerah disusun dalam jangka waktu tahun 2022 sampai dengan tahun 2026.
(2) Arsitektur SPBE Daerah sebagaimana dimaksud pada ayat (1) dilakukan reviu pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.
(3) Reviu sebagaimana dimaksud pada ayat (2) dilakukan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang Komunikasi dan Informatika.
(4) Reviu sebagaimana dimaksud pada ayat (2) dilakukan berdasarkan:
    a. perubahan Arsitektur SPBE nasional;
    b. hasil Pemantauan SPBE dan Evaluasi SPBE;
    c. perubahan pada unsur SPBE di Daerah; dan/atau
    d. perubahan Rencana Pembangunan Jangka Menengah Daerah
(5) Hasil reviu Arsitektur SPBE Daerah sebagaimana dimaksud pada ayat (2) disampaikan kepada Tim Koordinasi SPBE Daerah.
(6) Arsitektur SPBE Daerah sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 4

Guna mendukung terlaksananya Arsitektur SPBE Daerah ini, diperlukan :

a. komitmen Pemangku Kepentingan; dan
b. dukungan anggaran sesuai kebutuhan yang diprioritaskan dalam Anggaran Pendapatan dan Belanja Daerah Kabupaten Tegal.

BAB III

PENUTUP

Pasal 5

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahui, memerintahkan Pengundangan Peraturan Bupati ini dengan menempatkannya dalam Berita Daerah Kabupaten Tegal.

Ditetapkan di Slawi
pada tanggal 10 JUNI 2022

BUPATI TEGAL,

UMI AZIZAH

Diundangkan di Slawi
pada tanggal 10 JUNI 2022
SEKRETARIS DAERAH,

WIDODO JOKO MULYONO

BERITA DAERAH KABUPATEN TEGAL TAHUN 2022 NOMOR 45

LAMPIRAN
PERATURAN BUPATI TEGAL
NOMOR 45 TAHUN 2022
TENTANG
ARSITEKTUR SISTEM PEMERINTAHAN
BERBASIS ELEKTRONIK
PEMERINTAH KABUPATEN TEGAL

ARSITEKTUR SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH KABUPATEN TEGAL

DAFTAR ISI

BAB I
PENDAHULUAN

1.1. Latar Belakang

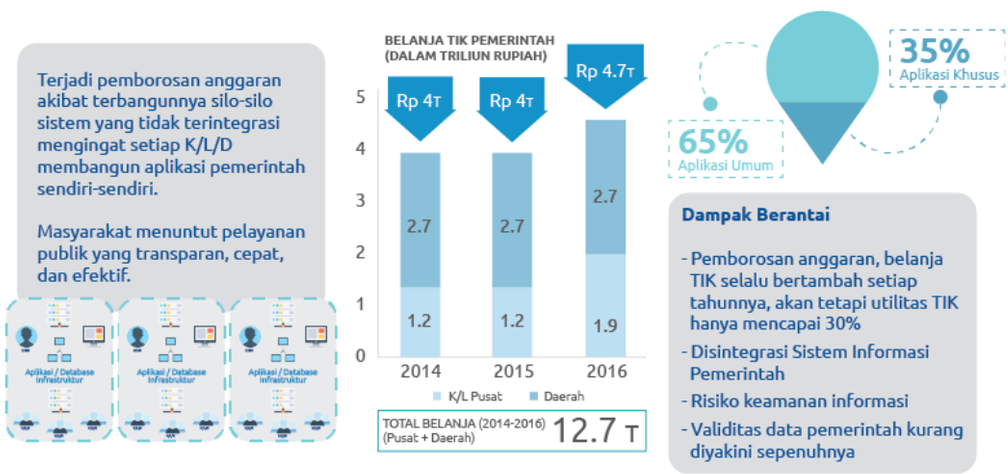
Kabupaten Tegal, adalah salah satu kabupaten di Provinsi Jawa Tengah. Ibukotanya adalah Slawi, sekitar 14 km sebelah selatan Kota Tegal. Kabupaten Tegal terdiri atas 18 kecamatan, yang dibagi lagi atas sejumlah desa dan kelurahan. Luas wilayah Kabupaten Tegal adalah 876,10 km2 dari wilayah Provinsi Jawa Tengah, dengan luas sebesar ini teknologi informasi untuk mendukung reformasi birokrasi menjadi sebuah keharusan agar pelayanan publik dapat tersampaikan dengan maksimal. Pada tahun 2019 Kabupaten Tegal menjadi kabupaten terbaik dalam pelayanan sistem pemerintahan berbasis elektronik (SPBE) oleh Kementerian Pendayagunaan dan Administrasi Negara dan Reformasi Birokrasi (KemenpanRB). Hal ini terbukti dengan adanya Berdasarkan dokumen RPJMD Kabupaten Tegal Tahun 2019-2024 telah ditetapkan visi yang merupakan gambaran kondisi atau keadaan Kabupaten Tegal yang akan diwujudkan setelah tahun 2019. Sedangkan misi untuk mewujudkan visi. Visi pembangunan Kabupaten Tegal untuk lima tahun mendatang adalah sebagai berikut:

"Terwujudnya Masyarakat Kabupaten Tegal yang Sejahtera, Mandiri, Unggul, Berbudaya, dan Berakhlak Mulia"

Berdasarkan dengan visi tersebut, maka perlu adanya peningkatan pelayanan publik untuk sektor kesehatan, pendidikan dan ekonomi kreatif. Saat ini Revolusi Industri 4.0 sebagai perkembangan peradaban modern telah kita rasakan dampaknya pada berbagai sendi kehidupan, penetrasi teknologi yang serba disruptif, menjadikan perubahan semakin cepat, sebagai konsekuensi dari fenomena Internet untuk segalanya (*Internet of Things* or IoT), kumpulan himpunan data dalam jumlah yang sangat besar dan kompleks sehingga menjadikannya sulit untuk ditangani atau diproses jika hanya menggunakan manajemen basis data biasa atau aplikasi (*Big Data*), teknologi yang menjadikan internet sebagai pusat pengelolaan data dan aplikasi (*Cloud Computing*), hingga kecerdasan buatan (*Artificial Intelligence*). Perubahan pada lanskap ekonomi politik dan relasi organisasi sebagai konsekuensi Revolusi Industri 4.0 menjadikan transformasi organisasi pemerintah sebagai suatu keniscayaan dalam berbagai skala ruang lingkup, dan kompleksitasnya. Transformasi organisasi pemerintah ini menjadi kata kunci yang harus terus diupayakan sebagai instrumen bagi aparat

pemerintah agar responsif terhadap perubahan. Perubahannya ini dapat diimplementasikan pada reformasi di kegiatan pemerintahan.

Di satu sisi dalam mewujudkan reformasi organisasi pemerintah, perlu didukung dengan komitmen dan perencanaan di bidang TIK. Salah satu upaya guna mewujudkan tujuan dari Reformasi Birokrasi adalah dengan memodernisasi birokrasi pemerintahan yang memfokuskan pada orientasi pelayanan publik kepada kepuasan masyarakat melalui optimalisasi pemanfaatan TIK. Saat ini pemanfaatan TIK di sektor pemerintahan (*Smart Government*) atau yang saat ini lebih dikenal dengan istilah SPBE dimanfaatkan untuk mendukung fungsi dan layanan pemerintahan di lingkungan Pemerintah Kabupaten Tegal. Aktivitas pemerintahan ini sudah sejak lama dilakukan dengan intensitas yang semakin meningkat. Baik Dinas Komunikasi dan Informatika sebagai "*leading sector*" di bidang pengembangan dan pemanfaatan TIK maupun perangkat daerah saat ini mengelola berbagai sistem aplikasi yang mana pertumbuhannya terus meningkat. Ketidakseragaman dalam proses pengembangan aplikasi SPBE yang digunakan menjadi permasalahan tersendiri dalam melakukan proses pemeliharan. Hal ini dikarenakan belum tersedianya kebijakan, panduan dan standar yang jelas terkait dengan implementasi *Smart Government* sehingga membuat proses pengelolaan tidak berjalan dengan efektif.



Gambar 1.1.1. Kondisi Pengelolaan Belanja TIK Pemerintah
(Sumber: Paparan KemenpanRB)

Faktanya, kini masyarakat menuntut pelayanan publik yang transparan, birokrasi yang cepat dan efektif sehingga SPBE menjadi tuntutan dan harus diterapkan dengan serius. Akan tetapi sejauh ini implementasi sistem informasi pemerintahan di Kab. Tegal masih belum terpadu, mengingat perangkat daerah masih membangun aplikasi pemerintahan sendiri-sendiri serta mengacu pada Nilai indeks SPBE Kab. Tegal dimana pada aspek Strategi & Perencanaan nilainya masih di angka 2.8. Fakta ini mengindikasikan bahwa kurangnya koordinasi antar instansi pemerintah daerah

di dalam pengembangan SPBE membuat operasional menjadi tidak efisien dan berdampak pada pemborosan anggaran belanja TIK dan kapasitas TIK yang melebihi kebutuhan. Pemborosan anggaran belanja TIK ini selalu bertambah setiap tahunnya. Berdasarkan Inpres Nomor 3 Tahun 2003 tentang kebijakan dan strategi nasional pengembangan *e-Government*, disebutkan bahwa setiap Pemerintah Daerah dapat mengambil langkah-langkah yang diperlukan sesuai dengan tugas pokok, fungsi, dan kewenangannya untuk melaksanakan pengembangan pelayanan pemerintahan berbasis Teknologi Informasi dan Komunikasi (TIK) secara nasional. Pelayanan yang dikenal dengan sebutan SPBE diharapkan mampu mendongkrak kualitas Pemerintah Daerah kepada masyarakat karena dapat menghemat waktu layanan, percepatan proses, menyederhanakan birokrasi, serta adanya transparansi terhadap proses, biaya, maupun waktu pelayanan. Oleh karena itu, peningkatan kualitas pelayanan merupakan prasyarat terwujudnya *Good Governance of Government.*

Gambar 1.1.2. Kebijakan Pengembangan SPBE

Untuk memastikan SPBE baik yang akan dibangun maupun yang sudah ada benar-benar mendukung proses bisnis di lingkungan Pemerintah Kabupaten Tegal berjalan dengan baik maka diperlukan suatu kajian terkait SPBE di lingkungan Pemerintah Kabupaten Tegal.

Diharapkan permasalahan-permasalahan yang ada saat ini terkait dengan proses pembangunan dan pemeliharaan layanan SPBE di lingkungan Pemerintah Kabupaten Tegal dapat terselesaikan dan mampu diimplementasikan dengan baik menyesuaikan proses bisnis yang ada di Pemerintah Kabupaten Tegal. Dalam rangka membangun panduan yang dimaksud, maka Pemerintah Kabupaten Tegal menyusun Arsitektur SPBE Daerah. Harapan yang ingin dicapai di masa mendatang dengan adanya

kajian ini maka pengembangan SPBE dapat dilaksanakan dengan lebih sistematik dan terpadu. Keterpaduan ini ditujukan untuk memanfaatkan sumber daya SPBE secara optimal dan mencegah timbulnya duplikasi inisiatif dan anggaran dalam pelaksanaan SPBE.

1.2. Maksud dan Tujuan

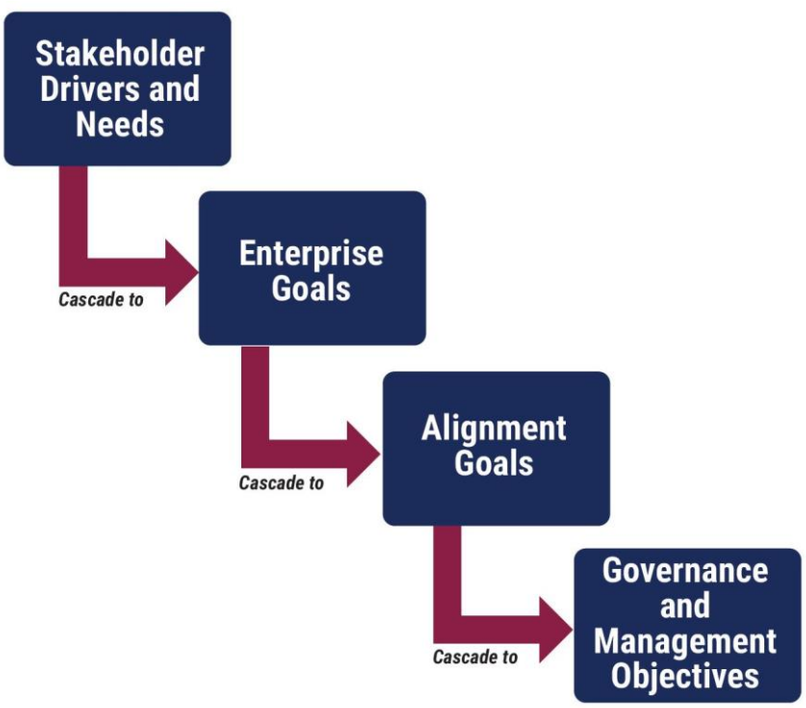
Maksud penyusunan Arsitektur SPBE Daerah di Kabupaten Tegal 2022-2026 ini adalah agar terciptanya perencanaan dan implementasi SPBE di Kabupaten Tegal yang terintegrasi antar pemangku kepentingan.

Sementara tujuan dari penyusunan Arsitektur SPBE Daerah di Kabupaten Tegal 2022-2026 ini adalah sebagai berikut :

a. menyusun kerangka kerja (*framework*) tata kelola pemerintahan dan pelayanan masyarakat berbasis sistem elektronik yang efektif dan efisien;
b. memberikan arahan strategis pengelolaan dan pengembangan sistem informasi Kabupaten Tegal agar dapat terlaksana secara efektif dan efisien;
c. menyusun dokumen Arsitektur SPBE Kabupaten Tegal 2022-2026 yang berfungsi sebagai pedoman untuk pengembangan dan pengelolaan layanan SPBE di Kabupaten Tegal.

1.3. Landasan Teori

1. Framework COBIT 5 untuk Pemenuhan Tata Kelola TIK

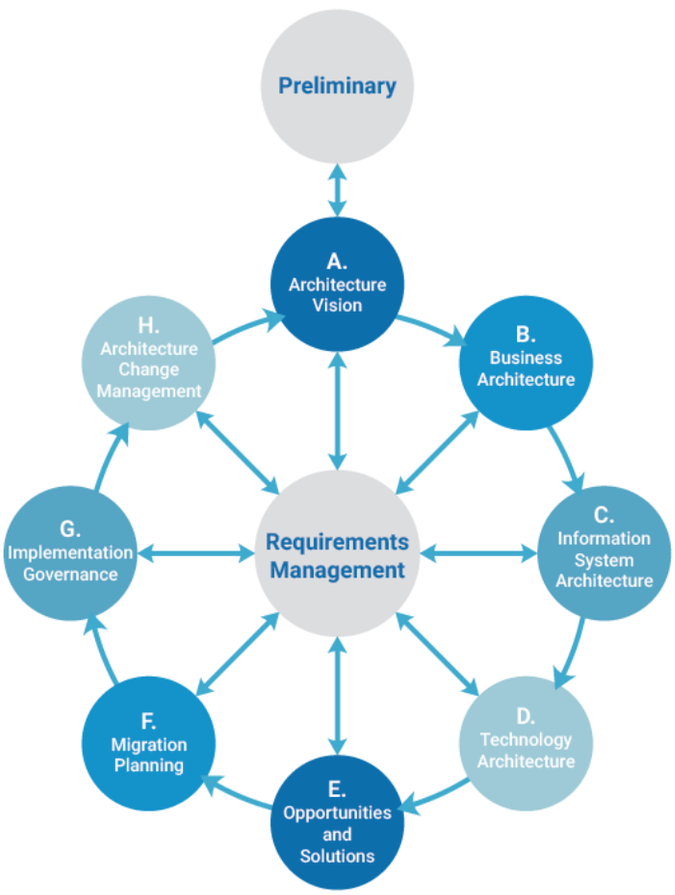


Gambar 1.3.1. Tata Kelola (COBIT)

Tahapan untuk mendesain tata kelola TIK yang tepat untuk mendukung implementasi layanan SPBE, bermula dari analisis kondisi eksisting

lingkungan, teknologi dan kebijakan pemangku kepentingan (*stakeholder drivers*) yang diturunkan menjadi analisis kebutuhan dari pemangku kepentingan pemerintah daerah (masyarakat, pemerintah pusat, kepala daerah dan seterusnya). Selanjutnya diturunkan menjadi tujuan organisasi (*Enterprise Goals*) pemerintah daerah. Tujuan organisasi harus dapat dipastikan tingkat pencapaiannya. Oleh karena itu perlu adanya keselarasan antara tujuan organisasi pemerintah daerah dengan tujuan teknologi informasi dan komunikasi (*Enabler Goals*) yang berperan menjadi pendukungnya agar implementasi TIK dapat tercapai.

2. TOGAF 9.1 *Framework* untuk Arsitektur Data, Infrastruktur, Aplikasi dan Keamanan TIK

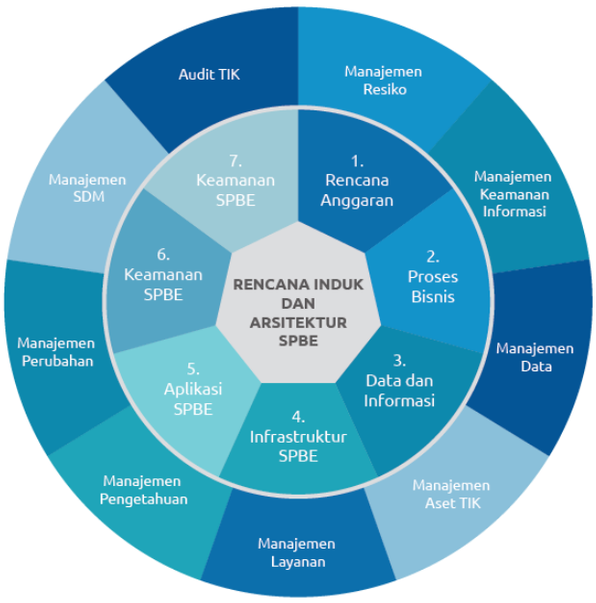


Gambar 1.3.2. Tata Kelola (TOGAF)

Penyusunan arsitektur teknologi informasi dan komunikasi mengadopsi dari konsep Arsitektur Pengembangan IT (*Architecture Development Method*) yang ada dalam *framework* TOGAF 9.1 konsep ini mendefinisikan arsitektur dimulai dengan mendefinisikan visi arsitektur dilanjutkan dengan menentukan arsitektur bisnis, arsitektur sistem dan data, arsitektur teknologi (infrastruktur TIK). Visi arsitektur yang dibangun harus mampu memenuhi tujuan dari perkembangan teknologi/kebijakan yang ingin diadopsi oleh pemerintah daerah di masa mendatang dan mempertimbangkan evaluasi atas arsitektur TIK yang telah dibangun sebelumnya.

3. Sistem Pemerintahan Berbasis Elektronik

Merujuk kepada Perpres 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE. Dalam perencanaan pembangunan dan pengembangan aplikasi harus didasarkan pada arsitektur SPBE pemerintah daerah agar SPBE menjadi terpadu dan diharapkan akan menciptakan proses bisnis pemerintahan yang terintegrasi antara instansi pusat dan pemerintah daerah sehingga akan membentuk satu-kesatuan pemerintahan yang utuh dan menyeluruh serta menghasilkan birokrasi pemerintahan dan pelayanan publik yang berkinerja tinggi.



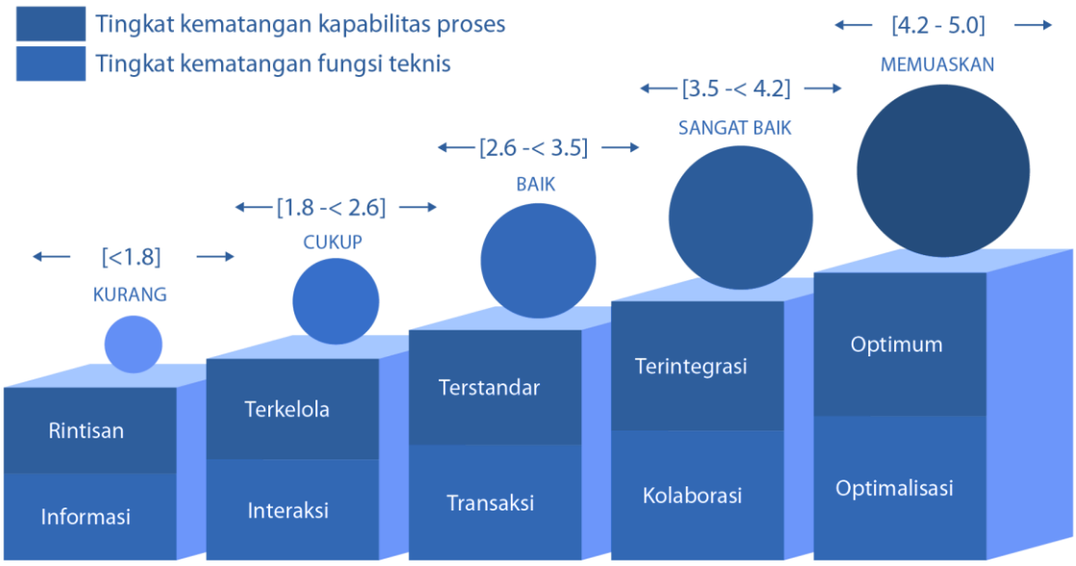
Gambar 1.3.3. Ruang Lingkup Rencana Induk dan Arsitektur SPBE

Untuk mengimplementasikan Rencana Induk Nasional dan Arsitektur SPBE, setiap perangkat daerah Pemerintah Daerah perlu melakukan transformasi paradigma dan proses dalam konteks penyelenggaraan pemerintahan, pelayanan publik berbasis elektronik, dukungan TIK, dan SDM. Terdapat 3 tahapan penting dalam kesuksesan SPBE:

1. Perencanaan: Rencana Induk dan Arsitektur SPBE, Kerangka Acuan Kerja (KAK), Kontrak.
2. Pelaksanaan: Manajemen Proyek/Kegiatan, Manajemen Rekanan, dan Tim Pelaksana (jumlah & kompetensi).
3. Evaluasi: *Monitoring* dan evaluasi setiap tahun untuk mengetahui capaian progress implementasi Rencana Induk khususnya *Roadmap*, Kondisi permasalahan eksisting SPBE, Inisiatif perbaikan program.

Untuk mengetahui kondisi penerapan SPBE di Pemerintah Kabupaten Tegal saat ini, dapat menggunakan konsep tingkat kematangan SPBE yang merupakan kerangka kerja yang mengukur derajat pengembangan

SPBE. Tingkatan kematangan mengarahkan pengembangan SPBE pada keluaran dan dampak yang lebih baik. Tingkat kematangan yang rendah menunjukkan kapabilitas dan keberhasilan yang rendah, sedangkan tingkat kematangan yang tinggi menunjukkan kapabilitas dan keberhasilan yang lebih tinggi.



Gambar 1.3.4. Tingkat Kematangan Proses SPBE

Tabel 1.3.1. Tingkat Kematangan pada Domain Tata Kelola SPBE dan Kebijakan Internal SPBE

Tingkat (Level)	Karakteristik
1 - Rintisan	Proses tata kelola dilaksanakan sewaktu-waktu, tidak terorganisasi dengan baik, tanpa pemantauan, dan hasil tidak terprediksi. Kebijakan internal belum tersedia atau masih berbentuk konsep.
2 - Terkelola	Proses tata kelola dilaksanakan dengan dasar-dasar manajemen yang telah didefinisikan dan didokumentasikan, dilaksanakan berdasarkan standar masing-masing unit organisasi. Kebijakan internal telah dilegalisasi, namun pengaturannya bersifat parsial atau sektoral.
3 - Terstandarisasi	Proses tata kelola dilaksanakan sepenuhnya dengan standarisasi oleh semua unit organisasi terkait. Kebijakan internal telah mengatur standar proses tata kelola bagi semua unit organisasi terkait, tetapi belum mengatur keselarasan antar proses tata kelola.
4 - Terintegrasi	Proses tata kelola dilaksanakan terintegrasi dengan proses tata kelola lain dan terukur kinerjanya secara Kuantitatif. Kebijakan internal telah mengatur integrasi antar proses tata kelola dan mekanisme pengukuran kinerja proses tata

	kelola tersebut.
5 - Optimum	Proses tata kelola dilaksanakan dengan peningkatan kualitas secara berkesinambungan. Kebijakan internal telah mengatur mekanisme evaluasi berkelanjutan dan manajemen perubahan.

Tabel 1.3.2. Tingkat Kematangan pada Domain Layanan SPBE

Tingkat (Level)	Kriteria
1 - Informasi	Layanan SPBE diberikan dalam bentuk informasi satu arah.
2 - Interaksi	Layanan SPBE diberikan dalam bentuk interaksi dua arah.
3 - Transaksi	Layanan SPBE diberikan melalui pertukaran informasi dan layanan.
4 - Kolaborasi	Layanan SPBE diberikan melalui integrasi dengan layanan SPBE lain.
5 - Optimalisasi	Layanan SPBE dapat beradaptasi terhadap perubahan kebutuhan di lingkungan internal dan eksternal

BAB II
VISI, MISI, TUJUAN DAN SASARAN SPBE, DAN STRATEGI PENINGKATAN INDEKS SPBE SERTA INISIATIF STRATEGIS SPBE

2.1. Visi Misi, Tujuan dan Sasaran SPBE

Visi Misi SPBE Nasional adalah :

> ***"Terwujudnya sistem pemerintahan berbasis elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi."***

Visi dan misi SPBE nasional perlu diselaraskan, disinkronisasikan, dan diharmonisasikan dengan visi dan misi Pemerintah Kabupaten Tegal dan visi misi Rencana Induk SPBE Kabupaten Tegal.

Visi Misi Pemerintah Daerah

> ***"Terwujudnya Masyarakat Kabupaten Tegal yang Sejahtera, Mandiri, Unggul, Berbudaya, dan Berakhlak Mulia"***

Visi Misi Rencana Induk SPBE Daerah

> **" Terwujudnya layanan Smart Government prima menuju birokrasi yang profesional dan inovatif ".**

Dengan mengacu pada tiga hal pondasi strategi dalam arsitektur SPBE Daerah Pemerintah Kabupaten Tegal Tahun 2022-2026 berfokus pada peningkatan perekonomian dan peningkatan kualitas sumberdaya manusia untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi.

Visi tersebut menjadi acuan dalam mewujudkan pelaksanaan SPBE yang terpadu di Instansi Pemerintah Daerah untuk menghasilkan birokrasi pemerintah yang integratif, dinamis, transparan, dan inovatif, serta peningkatan kualitas pelayanan publik yang terpadu, efektif, responsif, dan adaptif. Dalam rangka mencapai visi SPBE, maka misi SPBE adalah:

a. melakukan penataan dan penguatan organisasi dan tata kelola sistem pemerintahan berbasis elektronik yang terpadu;
b. mengembangkan pelayanan publik berbasis elektronik yang terpadu, menyeluruh, dan menjangkau masyarakat luas;
c. membangun fondasi teknologi informasi dan komunikasi yang terintegrasi, aman, dan andal; dan

d. membangun SDM yang kompeten dan inovatif berbasis teknologi informasi dan komunikasi.

Berdasarkan visi dan misi SPBE, tujuan SPBE adalah:

a. mewujudkan tata kelola pemerintahan yang bersih, efektif, efisien, transparan, dan akuntabel.
b. mewujudkan pelayanan publik yang berkualitas dan terpercaya; dan
c. mewujudkan sistem pemerintahan berbasis elektronik yang terpadu.

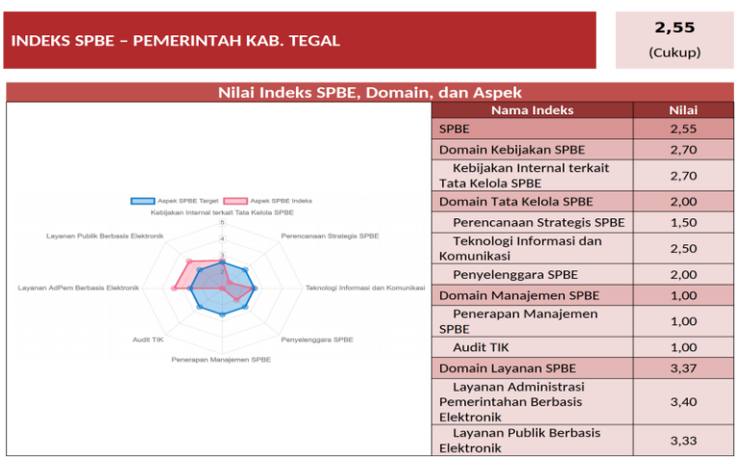
Berdasarkan visi, misi, dan tujuan SPBE, sasaran SPBE adalah:

a. terwujudnya tata kelola dan manajemen TIK yang efektif dan efisien;
b. terwujudnya layanan SPBE yang terpadu dan berorientasi kepada pengguna;
c. terselenggaranya infrastruktur SPBE yang terintegrasi; dan
d. meningkatnya kapasitas SDM TIK.

Gambar 2.1.1. Unsur-unsur dalam SPBE

2.2. Strategi Peningkatan Indeks SPBE

Meningkatkan domain tata kelola agar bisa mencapai level maksimal



Nama Indeks	Nilai
SPBE	2,55
Domain Kebijakan SPBE	2,70
Kebijakan Internal terkait Tata Kelola SPBE	2,70
Domain Tata Kelola SPBE	2,00
Perencanaan Strategis SPBE	1,50
Teknologi Informasi dan Komunikasi	2,50
Penyelenggara SPBE	2,00
Domain Manajemen SPBE	1,00
Penerapan Manajemen SPBE	1,00
Audit TIK	1,00
Domain Layanan SPBE	3,37
Layanan Administrasi Pemerintahan Berbasis Elektronik	3,40
Layanan Publik Berbasis Elektronik	3,33

Gambar 2.2.1. Indeks SPBE Kab. Tegal Tahun 2021

2.3. Inisiatif Strategis SPBE

Berdasarkan telaah visi misi SPBE dan analisa hasil survei diperoleh sepuluh inisiatif sebagai prioritas pengembangan SPBE di Kabupaten Tegal yaitu:

a. Penyesuaian Tim Pengarah SPBE;
b. Pembentukan Komite/Forum Manajemen SPBE;
c. Melakukan penerapan manajemen dan audit SPBE;
d. Peningkatan kompetensi dan jumlah SDM dengan kualifikasi TI secara terencana dan berkesinambungan;
e. Optimalisasi Sistem Informasi guna mendukung implementasi layanan SPBE, antara lain:
    1. sistem Informasi Perencanaan
    2. sistem Informasi Penganggaran
    3. sistem Informasi Keuangan
    4. Sistem Informasi Pengadaan
    5. Sistem Informasi Kepegawaian
    6. Sistem Informasi Kearsipan
    7. Sistem Informasi Barang Milik Daerah
    8. Sistem Informasi Pengawasan Internal Pemerintah
    9. Sistem Informasi Akuntabilitas Kinerja Organisasi
    10. Sistem Informasi Kinerja Pegawai
    11. Sistem Informasi Pengaduan Publik
    12. Sistem Informasi Data Terbuka
    13. Sistem Informasi JDIH
    14. Sistem Informasi Publik Sektor

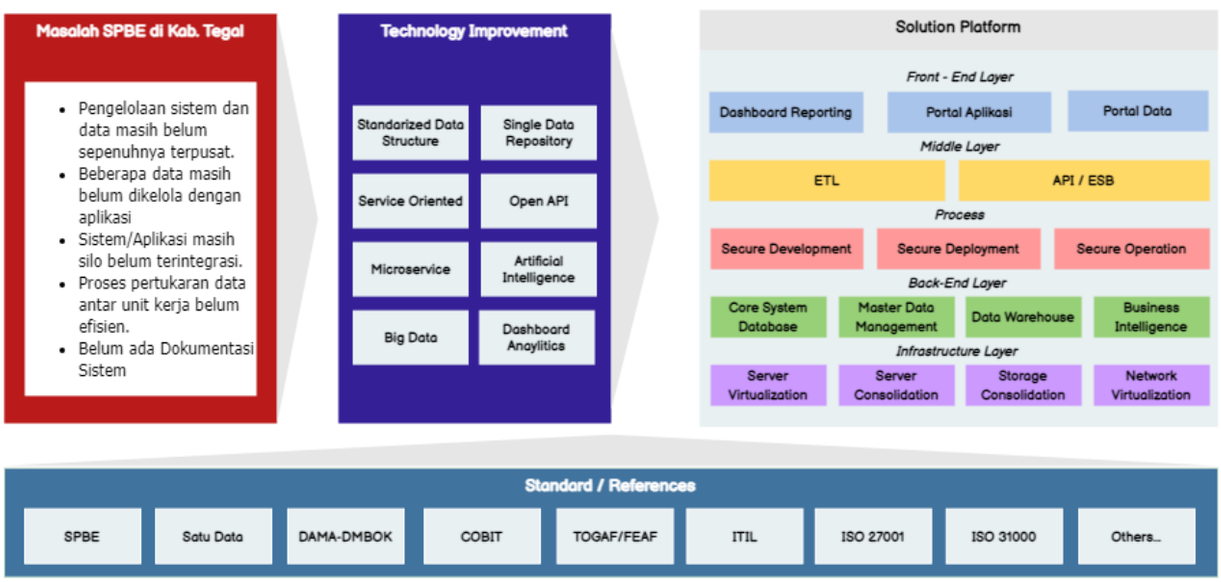
    Sistem Informasi ini minimal harus memenuhi syarat indeks layanan SPBE di level 4 (empat), dimana sistem informasi harus dapat terintegrasi dengan sistem informasi lain-lain baik yang dikelola oleh internal pemda maupun yang dikelola oleh kementerian; serta direkomendasikan untuk menggunakan aplikasi umum dari Instansi Pusat;
f. Melakukan integrasi layanan SPBE Internal dengan mengembangkan API Library dan Monitoring sebagai sistem penghubung antar layanan;
g. Melakukan penataan standar pengembangan aplikasi;
h. Melakukan analisis kelayakan operasional dan keamanan SPBE;

i. Menyediakan kebijakan implementasi TIK yang menyeluruh dan menjangkau seluruh perangkat daerah seperti: SOP Pembangunan Aplikasi oleh pihak ketiga;
   Penambahan dan peremajaan perangkat komputer dan perangkat pendukung

BAB III
KONDISI IDEAL LAYANAN SPBE

3.1. Diagram Konsep Solusi SPBE

Setiap permasalahan pasti mempunyai solusi. Namun tidak semua solusi dapat menyelesaikan permasalahan, sebab bisa saja solusi tersebut tidak cukup efektif dalam menyelesaikan permasalahan tersebut. Solusi yang baik adalah solusi yang sesuai dengan kebutuhan dan bisa meminimalisasi permasalahan tanpa menimbulkan permasalahan baru. Perencanaan SPBE harus mengakomodasi solusi-solusi yang terbaik untuk permasalahan SPBE yang terjadi di Kab. Tegal. *Solution concept* adalah hasil dari usulan pengembangan teknologi yang akan menjadi solusi bagi permasalahan yang dihadapi oleh user. *Solution concept* awalnya berangkat dari masalah yang terjadi di Pemkab. Tegal kemudian dikaji solusi yang dibutuhkan oleh Pemkab. Tegal untuk mengatasi masalah terkait pengelolaan SPBE.



Gambar 3.1.1. Solution Konsep Diagram SPBE

Perbaikan dari sisi teknologi yaitu kedepan teknologi untuk mendukung operasional SPBE harus memiliki komponen berikut:

Komponen	Deskripsi
Service Oriented	Menyediakan *service (backend)* sebagai penghubung untuk konektivitas aplikasi-aplikasi ke database sektoral pemerintahan.

	Aplikasi pemerintahan bersifat modular sehingga aplikasi dapat menggunakan *service* dari aplikasi lainnya seperti mengorkestrasikan beberapa API yang ada untuk membangun sebuah aplikasi dan tentunya ini dapat mengefisienkan waktu dalam proses pengembangan aplikasi.
Integrated System	Aplikasi harus terintegrasi dengan aplikasi lainnya, baik integrasi ke aplikasi internal maupun kementerian.
Sustainability	Infrastruktur harus redundan untuk memastikan sistem dapat berjalan 24x7 jam.
Security	Melakukan audit atas infrastruktur dan aplikasi untuk memastikan keamanan informasi terjaga.
Standardized Data Structure	Perlu adanya standarisasi struktur data dari masing-masing data sektoral.
Big Data	Pemanfaatan data dari berbagai sumber untuk melakukan analisis pengambilan keputusan atau penyusunan kebijakan.
Standardized Platform	Menggunakan platform yang standar sesuai dengan kompetensi developer internal Kab. Tegal. Sehingga kedepan aplikasi dapat di maintain oleh internal tanpa perlu ketergantungan dengan pihak ketiga.
Dashboard Analytics	Dashboard informasi yang dapat memberikan informasi secara *real-time* mengenai kondisi yang ada di Kab. Tegal sehingga memudahkan pejabat daerah untuk dalam merespon suatu kejadian di Kab. Tegal.

Kedepan solusi yang ada untuk mendukung operasional SPBE harus memiliki komponen berikut :

Komponen	Deskripsi
Front-End Layer	Pada layer ini terdapat platform untuk *reporting* terkait urusan pemerintahan secara *realtime* dan notifikasi *approval* untuk mempercepat proses birokrasi, notifikasi ini bisa dikirim melalui email maupun *whatsapp* dan telegram. selain itu juga terdapat platform portal aplikasi dan data untuk

Komponen	Deskripsi
	memudahkan aksesibilitas ke berbagai aplikasi dan data yang dikelola Pemkab. Tegal.
Middle Layer	Pada layer ini terdapat platform untuk API untuk memudahkan proses integrasi antar sistem Pemkab. Tegal dan juga terdapat teknologi ETL (*Extract Transform Load*) yang memungkinkan untuk melakukan ***ekstraksi*** data dari berbagai sumber *database*, selanjutnya data tersebut di *cleansing* dan di ***transform*** untuk menghasilkan informasi yang sesuai kebutuhan pengguna, selanjutnya melakukan ***load*** informasi tersebut ke data *warehouse* sebagai bahan untuk ditampilkan pada *Dashboard Analytics*.
Process	Dalam pengembangan aplikasi SPBE harus memastikan mulai dari proses *development*, *deployment* dan operasionalnya aman.
Back-End Layer	Dalam layer ini terdapat platform *Core System Database, Artificial Intelligence* guna mengotomatisasi proses analisis pada sistem, *Data Warehouse* dan *Business Intelligence* untuk mendapatkan *insight* mengenai tren saat ini dan memprediksi kejadian kedepan.
Infrastructure Layer	Memastikan infrastruktur sudah optimal dan available 24x7 jam dengan melakukan *Server Virtualization, Server Consolidation, Storage Consolidation, Network Virtualization.*

3.2 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:

3.2.1 Kondisi Ideal Kelembagaan

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

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

a. memberikan arahan dan persetujuan terhadap seluruh inisiatif program dan kegiatan SPBE di lingkungan Pemerintah Kabupaten Tegal, khususnya yang bersifat kebijakan dan anggaran/investasi.
b. memfasilitasi proses koordinasi, kerjasama, atau integrasi penerapan SPBE dengan Instansi Pusat/Pemerintah Daerah lain.

c. memfasilitasi penerapan tata kelola dan manajemen SPBE.
d. melakukan pemantauan dan evaluasi berkala atas penerapan SPBE.
e. melakukan perbaikan dan pengembangan atas hasil rekomendasi pemantauan dan evaluasi penerapan SPBE.

Tim Pelaksana dalam Tim Koordinasi Sistem Pemerintahan Berbasis Elektronik Kabupaten Tegal 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:

a. mengkoordinasikan perencanaan, realisasi, operasional, dan evaluasi SPBE khususnya terkait dengan inisiatif SPBE prioritas Pemerintah Kabupaten Tegal, bekerja sama dengan perangkat daerah pengelola SPBE dan perangkat daerah pemilik proses bisnis maupun pengguna TIK lainnya;
b. mengkoordinasikan Tim SPBE perangkat daerah;
c. memfasilitasi perencanaan dan implementasi inisiatif SPBE lintas perangkat daerah di tingkat Pemerintah Daerah, khususnya inisiatif SPBE prioritas Pemerintah Kabupaten Tegal;
d. memfasilitasi tata kelola SPBE yang baik di Pemerintah Kabupaten Tegal melalui penerbitan kebijakan, standar, prosedur, atau panduan yang relevan;
e. mengkoordinasikan perencanaan dan pelaksanaan inisiatif dan portofolio SPBE Pemerintah Kabupaten Tegal;
f. melakukan *review* berkala atas pelaksanaan implementasi SPBE di Pemerintah Kabupaten Tegal.

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

a. perumusan konsep, pelaksanaan kebijakan pengkoordinasian dan pemantauan informasi publik;
b. perumusan dan pengkoordinasian dalam pengelolaan domain dan subdomain bagi lembaga pelayanan publik;

c. perumusan regulasi tata kelola teknologi dan informasi menuju SPBE;
d. perumusan konsep, pelaksanaan kebijakan, pemantauan dan evaluasi pusat data, jaringan teknologi informasi serta pengembangan sistem informasi dan keamanan informasi
e. 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 Tegal 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. Tegal harus berdasarkan pada asas:

a. 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.

b. 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.

c. 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.

d. Keterpaduan;

   Asas keterpaduan sebagai landasan bahwa penyelenggaraan SPBE harus mengedepankan adanya keterpaduan dan

integrasi dari berbagai komponen dan sumber daya SPBE di Daerah.

e. 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.

f. Akuntabilitas

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

g. 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.

h. 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.

i. 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.

A. Tim Koordinasi SPBE

Gambar 3.2.1.1. Skema Susunan Tim Koordinasi SPBE

SUSUNAN TIM KOORDINASI SPBE

Kabupaten Tegal

No	Posisi dalam Tim	Pengisi Posisi
#	Ketua Tim Pengarah	Sekretariat Daerah
1	Koordinator Pelaksana Layanan Perencanaan	Kepala Bappeda dan Litbang
2	Koordinator Pelaksana Layanan Penganggaran	Kepala BPKAD
3	Koordinator Pelaksana Layanan Keuangan	Kepala BPKAD
4	Koordinator Pelaksana Layanan Pengadaan	Kepala Bagian PBJ
5	Koordinator Pelaksana Layanan Kepegawaian	Kepala BKPSDM
6	Koordinator Pelaksana Layanan Kearsipan	Kepala Dinas Perpusip
7	Koordinator Pelaksana Layanan Pengelolaan BMD	Kepala BPKAD
8	Koordinator Pelaksana Layanan Pengawasan Internal	Inspektur
9	Koordinator Pelaksana Layanan Akuntabilitas Kinerja Organisasi	Kepala Bagian Organisasi
10	Koordinator Pelaksana Layanan Kinerja Pegawai	Kepala BKPSDM
11	Koordinator Pelaksana Layanan Pengaduan Publik	Kepala Dinas Kominfo
12	Koordinator Pelaksana Layanan Data Terbuka	Kepala Dinas Kominfo
13	Koordinator Pelaksana Layanan JDIH	Kepala Bagian Hukum
14	Koordinator Pelaksana Layanan Publik Sektor	Kepala Dinas terkait Layanan Publik
15	Tim Pelaksana	Dinas Kominfo

B. Kebijakan SPBE

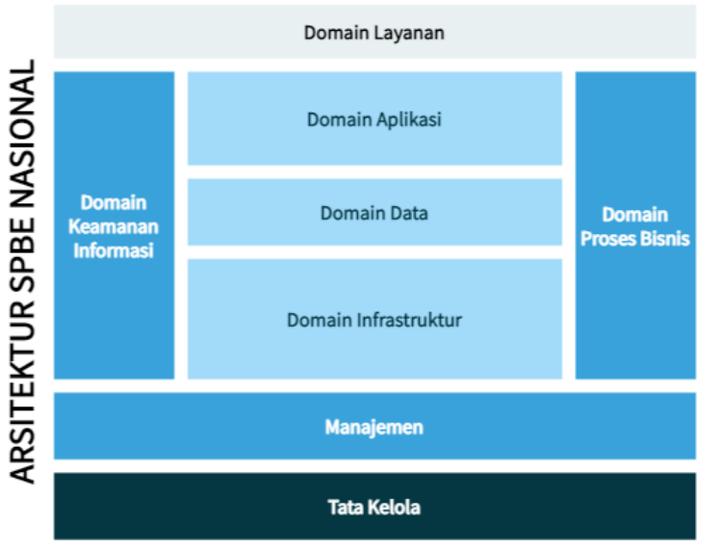
Penyusunan kebijakan dan SOP perlu dilakukan untuk mendukung pengembangan, penggunaan, maupun pemeliharaan sumber daya TIK. Berikut kebijakan yang diundangkan melalui peraturan dan SOP yang perlu disusun.

1) Kebijakan internal arsitektur SPBE Instansi Pusat/Pemerintah Daerah
2) Kebijakan internal peta rencana SPBE Instansi Pusat/Pemerintah Daerah
3) Kebijakan internal manajemen data
4) Kebijakan internal pembangunan aplikasi SPBE
5) Kebijakan internal layanan Pusat Data
6) Kebijakan internal layanan jaringan intra Instansi Pusat/Pemerintah Daerah
7) Kebijakan internal penggunaan sistem penghubung layanan Instansi Pusat/Pemerintah Daerah
8) Kebijakan internal manajemen keamanan informasi
9) Kebijakan internal audit teknologi informasi dan komunikasi

   Kebijakan internal tim koordinasi SPBE Instansi Pusat/Pemerintah Daerah

3.2.2 Tata Kelola Arsitektur SPBE

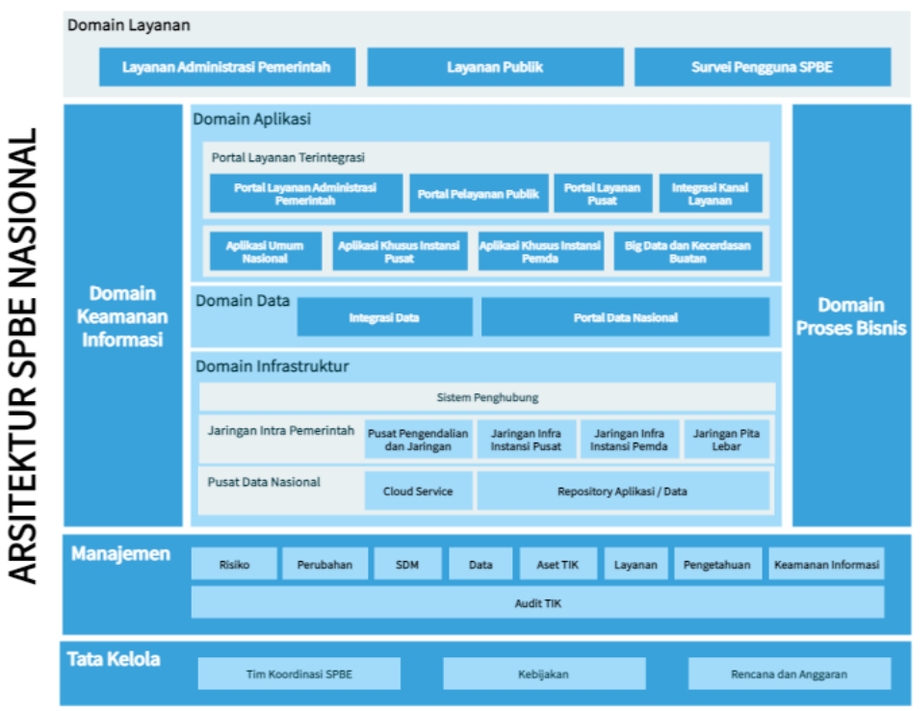
Arsitektur dan Peta Jalan SPBE merupakan panduan dalam pelaksanaan integrasi Proses Bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terpadu. Arsitektur memuat beberapa domain yang dijelaskan sebagai berikut:



Gambar 3.2.2.1. 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 3.2.2.2.



Gambar 3.2.2.2. Detailing Domain Arsitektur SPBE

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

aparatur negara. Arsitektur SPBE 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 Tegal;
3. Perubahan substansi kondisi Arsitektur SPBE.

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

3.2.3 Penganggaran SPBE

Anggaran dan belanja SPBE disusun dengan berpedoman pada Arsitektur SPBE Pemerintah Kab. Tegal yang kemudian dituangkan dalam Peta Rencana SPBE. Anggaran dan belanja SPBE disusun dalam bentuk inventarisasi kebutuhan anggaran dan belanja Perangkat Daerah dan lembaga tenis lainnya. Penyusunan anggaran dan belanja SPBE dikoordinasikan oleh Bappeda dan dibantu dengan Diskominfo .

Koordinasi dalam proses penyusunan anggaran dan belanja SPBE dilakukan dengan cara melakukan peninjauan terhadap rencana anggaran dan belanja SPBE untuk memastikan keterpaduan perencanaan anggaran dan belanja SPBE di seluruh Perangkat Daerah dan lembaga tenis lainnya.

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

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.

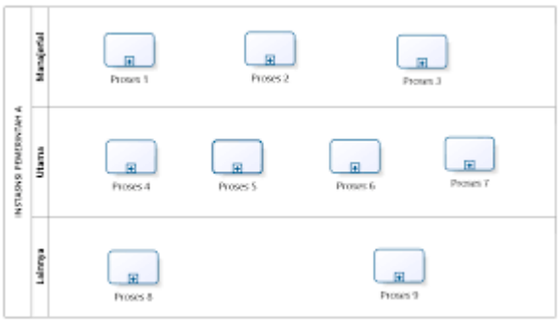
3.2.4 Tata Kelola Kebijakan SPBE

Penyusunan kebijakan perlu dilakukan untuk mendukung pengembangan dan operasional SPBE. Berikut ini dijelaskan kebijakan SPBE yang kedepan perlu disusun.

1) Kebijakan internal arsitektur SPBE
2) Kebijakan internal peta rencana SPBE
3) Kebijakan internal manajemen data
4) Kebijakan internal pembangunan aplikasi SPBE
5) Kebijakan internal layanan Pusat Data
6) Kebijakan internal layanan jaringan intra Instansi Pusat
7) Kebijakan internal penggunaan sistem penghubung layanan Instansi Pusat
8) Kebijakan internal manajemen keamanan informasi
9) Kebijakan internal audit teknologi informasi dan komunikasi
10) Kebijakan internal tim koordinasi SPBE Instansi Pusat

3.2.5 Tata Kelola Proses Bisnis

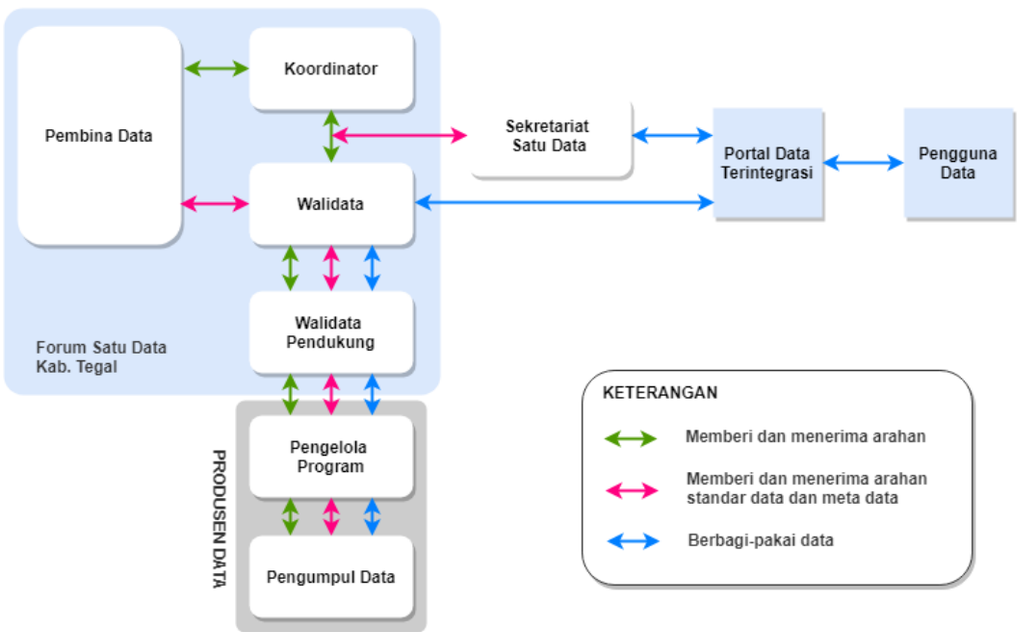
Proses bisnis di seluruh Perangkat Daerah dan lembaga tenis lainnya perlu dipetakan dengan mengacu pada Permenpan-RB 19/2018 tentang pedoman penyusunan peta proses bisnis dimana mensyaratkan dalam menyusun peta proses bisnis perlu menggunakan standar BPMN versi 2.0; Selain itu dokumen peta proses bisnis ini merupakan living dokumen artinyaa ketikaa ada perubahaan pada visi misi daerah peta proses bisnisnya juga perlu di update untuk diselaraskan. Mengacu pada pedoman evaluasi SPBE Dokumen Peta Bisnis Proses ini juga perlu dilakukan Monev secara berkala guna memastikan serangkaian aktivitas yang terdapat dalam peta bisnis proses tersebut bisa di simplifikasi untuk efisiensi waktu pekerjaan sehingga dapat meningkatkan kualitas dari pelayanan publik pemerintah Kabupaten Tegal.



Gambar 4.2.8.1. Ilustrasi Peta Bisnis Proses

3.2.6 Tata Kelola Data

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



Gambar 4.2.9.1. Forum Satu Data Kab. Tegal

Penugasan:

Koordinator	Sekda
Pembina Data	Bappeda dan Litbang dan BPS
Walidata	Dinas Kominfo
Walidata Pendukung	Masing-masing Perangkat daerah (Bag. Program)
Produsen Data	Masing-masing Perangkat daerah (Seluruh Bidang)

Tugas Pembina Data Tingkat Daerah :

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

Tugas Produsen Data Tingkat Daerah:

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

3.2.7 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.

Gambar 4.2.10.1. Layanan SPBE

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

3.2.11 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 Dinas Kominfo dipetakan dalam matriks sebagai berikut:

Gambar 4.2.11.1. Matrix Easy Implementation

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

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

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

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

Sehingga secara ringkas, urutan prioritas pengembangan sistem dapat diurutkan sebagai berikut:

	High - Easy
1	Pengaduan kependudukan
2	Antrian online
3	MODALKU

4	Sistem Informasi Harga Barang Pokok
5	SKP Online

	Low - Easy
1	CEK NIK ONLINE
2	SIM PERLENGKAPAN JALAN
3	SIM DAERAH RAWAN KECELAKAAN
4	SIMOLE (Soybean Integrated Manual for Economy and Labour)
5	i-Tegal

	High - Hard
1	Database dan marketplace UMKM
2	Wisata Tegal
3	APLIKASI MONITORING LALU LINTAS JALAN MELALUI SMARTPHONE
4	INTELLIGENT TRANSPORTATION SYSTEM
5	Tegal Smart City

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

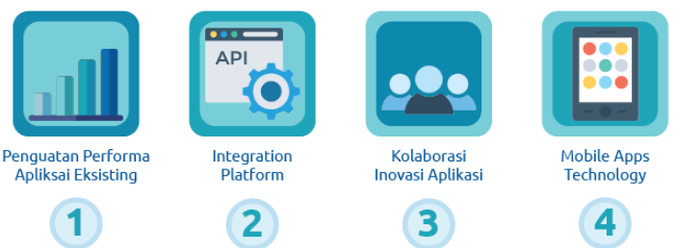
Gambar 4.2.11.2. Bagan Strategi Prioritasisasi Pengembangan Aplikasi

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 4.2.11.3. 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 Tegal 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 Tegal harus dapat meningkatkan fleksibilitas pemanfaatan teknologi dan kemudahan bagi masyarakat.

3. *Agile*

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

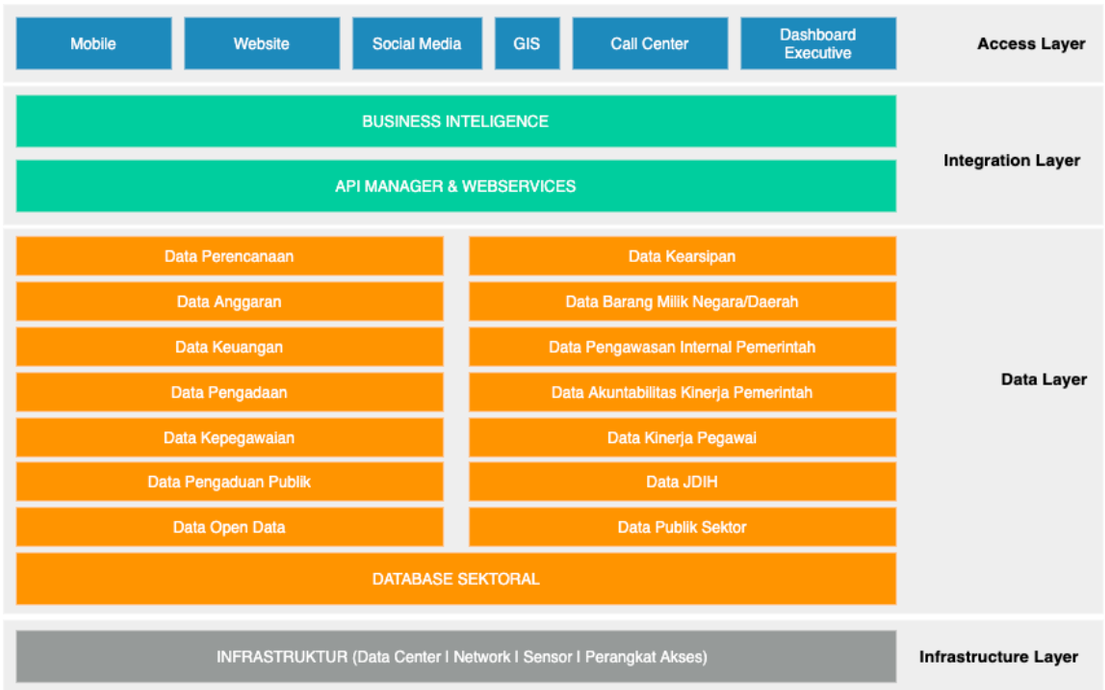
4. *Reliability*

   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 Tegal agar tercipta pelayanan prima kepada masyarakat.

B. Desain Arsitektur Sistem Informasi



Gambar 4.2.11.4. Desain Arsitektur Sistem Informasi

Arsitektur Sistem Informasi dijabarkan sebagai berikut:

a. *Operational Application Layer*

Pada bagian ini akan terdapat aplikasi-aplikasi yang akan mendukung perangkat daerah dalam proses operasional utama di unit kerjanya. Masing-masing Perangkat Daerah akan memiliki aplikasi dengan alur proses (proses bisnis) yang beragam sesuai dengan tugas dan fungsi Perangkat Daerah tersebut. Untuk mempermudah mengelola pertumbuhan aplikasi di masa mendatang, pada *layer* operasional, aplikasi dikategorikan sesuai dengan klaster SPBE dan dimensi *Smart City* sesuai dengan gambar di atas.

b. *Integration Layer*

Bagian ini ditujukan untuk aplikasi, *platform*, *module*, *services* yang berfungsi menjadi mediasi antara *layer* operasional dengan *layer* akses. Proses pengaturan terhadap akses data juga dikelola oleh layanan pada *layer* ini.

Pada *layer* ini akan terdapat *data warehouse* yang akan memiliki konten data primer dari masing-masing aplikasi yang berjalan pada *layer* operasional. Juga pada *layer* ini akan terdapat *web services* yang akan mengelola akses data antar aplikasi.

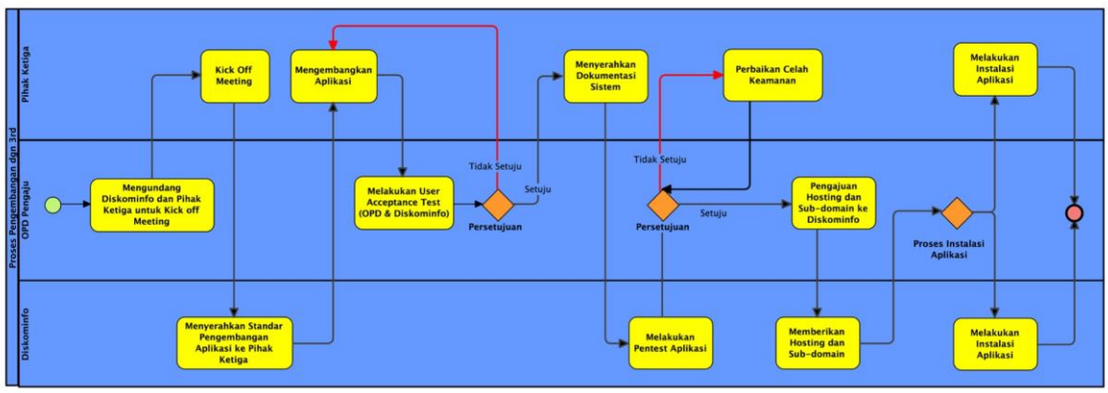
c. *Access Layer*

Pada bagian akses *layer* ini ditujukan untuk aplikasi-aplikasi yang akan mengkonsumsi, memanfaatkan data secara komprehensif dari masing-masing aplikasi pada *operasional layer*. Beberapa aplikasi yang dapat dikembangkan di sini contohnya adalah *website* dan *mobile apps,* yang dapat digunakan untuk membangun *engagement* masyarakat dengan Pemerintah Daerah, *messaging center,* digunakan untuk memberikan pesan langsung (*broadcast*) kepada masyarakat maupun pegawai, dan *dashboard apps,* yang dapat digunakan untuk melakukan proses *monitoring* kinerja Perangkat Daerah maupun sebagai alat bantu pengambil keputusan oleh Kepala Daerah.

d. Layer Arsitektur

Pada bagian ini terdapat *database* milik masing-masing aplikasi dan juga perangkat jaringan dan *server* yang akan dijabarkan lebih detail dalam bagian selanjutnya.

C. Alur Pengembangan Aplikasi dengan Pihak



Gambar 4.2.11.5. Alur Pengembangaan Aplikasi dengan Pihak ketiga

Dalam pengembaangan aplikasi dengan pihak ketiga yang dilakukan oleh seluruh perangkat daerah perlu dilakukan dengan koordinasi dengan Diskominfo; sebagaimana yang telah dijelaskan pada gambar diatas. hal ini untuk mengantisipasi pengembangan aplikasi yang tidak sesuai dengan prosedur atau standar keamanan informasi yang ditetapkan oleh Diskominfo Pemerintah Kabupaten Tegal.

D. 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 4.2.11.6. Data Urusan Pemerintahan

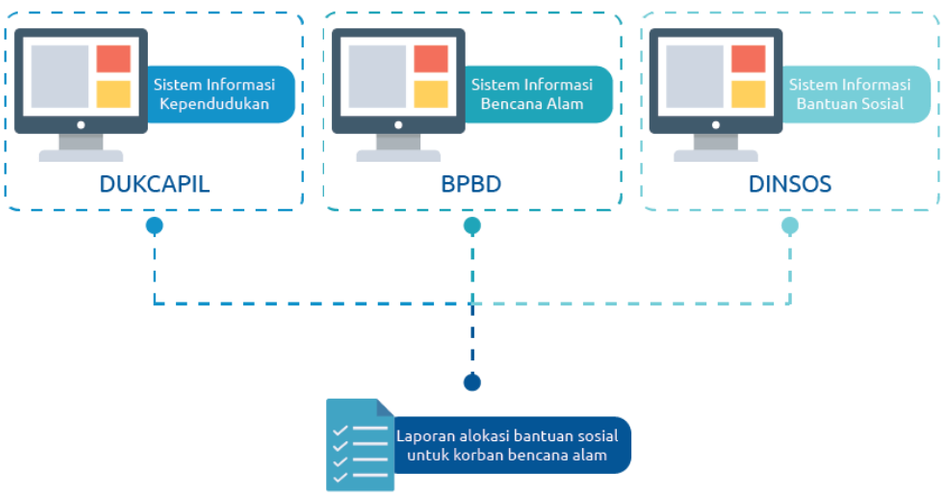
Sistem informasi yang dikembangkan dapat diintegrasikan dengan menggunakan *Application Programming Interface* (API), API adalah kumpulan fungsi-fungsi untuk menggantikan bahasa yang digunakan dalam *system call* dengan bahasa yang terstruktur. API menyediakan fungsi untuk menghubungkan koneksi antar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

E. 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 4.2.11.7. 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 4.2.11.8. Ilustrasi Model Integrasi Sistem

F. Pilihan Teknologi

a. *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 4.2.11.9. 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.

b. ***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.

c. ***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 4.2.11.10. 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.

d. **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.

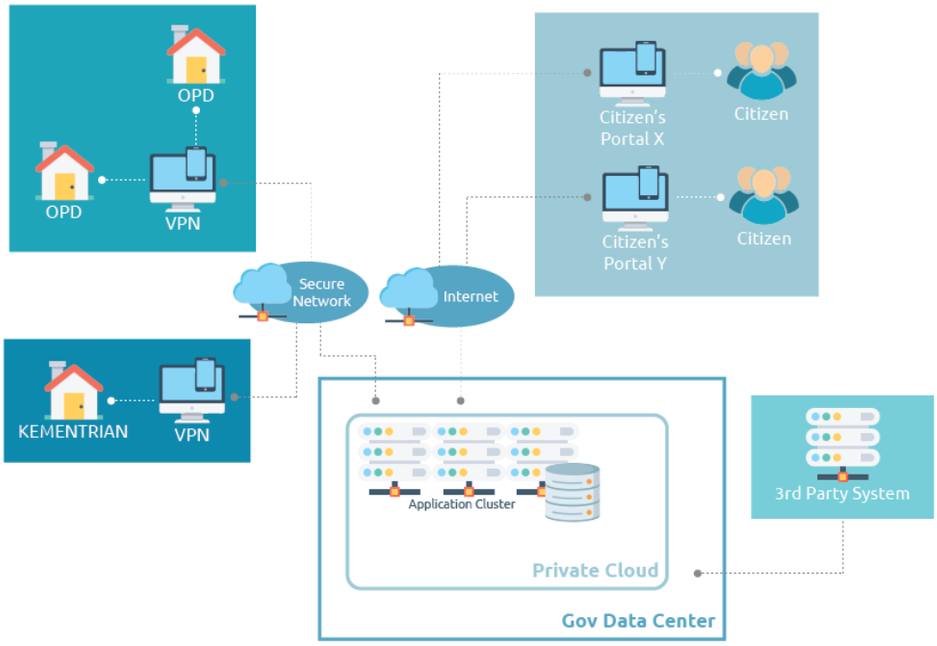
Dalam penerapan konsep *single sign on* diperlukan sebuah *protokol* untuk menyimpan *account* pengguna beserta hak aksesnya yang lintas aplikasi. Nantinya setiap aplikasi yang terhubung pada *server* tersebut akan selalu merujuk pada *account* pengguna yang tunggal. Protocol tersebut dinamai *Lightweight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

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

e. **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 4.2.11.11. 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.

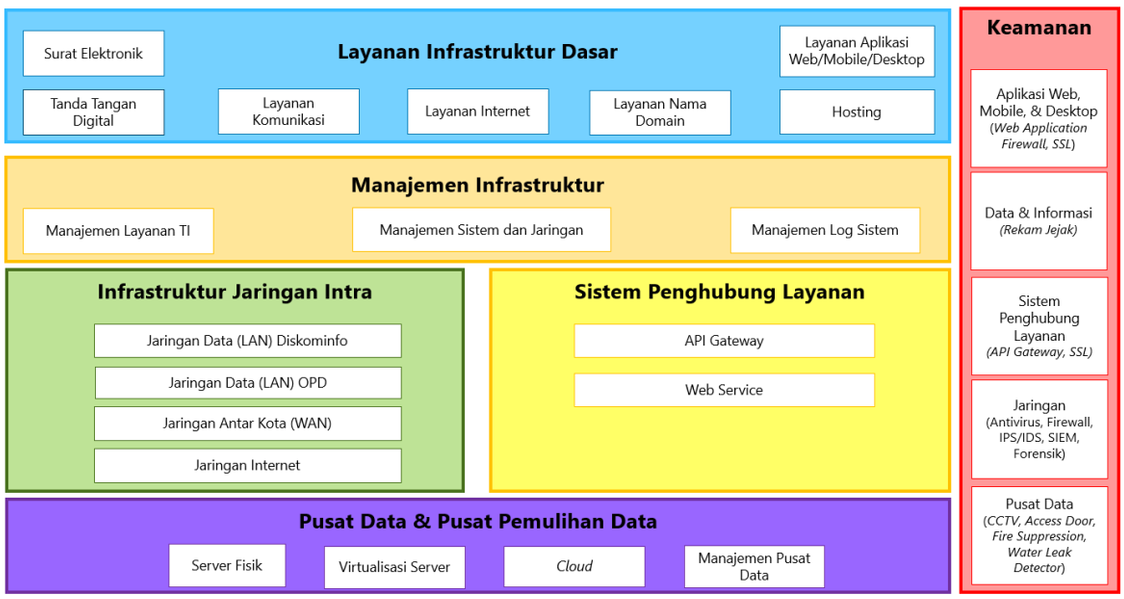
3.2.12 Tata Kelola Infrastruktur

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. Target Arsitektur Infrastruktur TIK



Gambar 4.2.11.12. Arsitektur Infrastruktur SPBE Kabupaten Tegal

Arsitektur Infrastruktur terdiri dari zona Layanan infrastruktur dasar, manajemen infrastruktur, infrastruktur jaringan data, infrastruktur komunikasi, pusat data dan pusat pemulihan data, dan keamanan. Setiap zona memiliki layanan masing – masing seperti pada zona layanan infrastruktur dasar terdapat layanan surat elektronik, tanda tangan digital, layanan komunikasi, layanan internet, layanan nama domain, layanan aplikasi web/mobile, dan layanan direktori pengguna.

Zona Manajemen infrastruktur berfungsi untuk tata kelola, pemantauan, dan pengendalian layanan infrastruktur dasar. Manajemen infrastruktur terdiri dari manajemen layanan ti yang berisi katalog layanan dan SLA-nya, manajemen sistem dan jaringan berupa konfigurasi dan pemantauan kesehatan dan kinerja, serta manajemen log sistem untuk proses audit dan *troubleshooting*.

Infrastruktur Jaringan Data meliputi jaringan data lokal (LAN) di kantor Diskominfo, LAN kantor perangkat daerah, jaringan antar kota (WAN) interkoneksi dengan Kementerian/Lembaga Negara/Lembaga Swasta, dan jaringan internet.

Infrastruktur Komunikasi meliputi penyediaan perangkat mesin PBX di simpan di salah satu kantor atau dalam bentuk awan (cloud PBX), jaringan telepon Telkom (PSTN).

Pusat Data dan Pusat Pemulihan Data dalam bentuk fisik atau *colocation server* di pihak ketiga. Teknologi di pusat data dapat berupa virtualisasi atau container. Untuk pengelolaan diperlukan Manajemen Pusat Data.

Semua layanan dan infrastruktur perlu dilindungi keamanannya meliputi keamanan Sistem Informasi (aplikasi, basis data, sistem operasi, dan platform), keamanan infrastruktur (antivirus, Firewall, IPS/IDS, SIEM, dan forensik), dan keamanan Fisik (*CCTV, access door, Fire Suppression, dan Water Leak Detector.*

B. Pusat Data

Gambar 4.2.11.13. 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 4.2.11.14. SNI No 8799-1:2019 tentang Panduan Manajemen Pusat Data

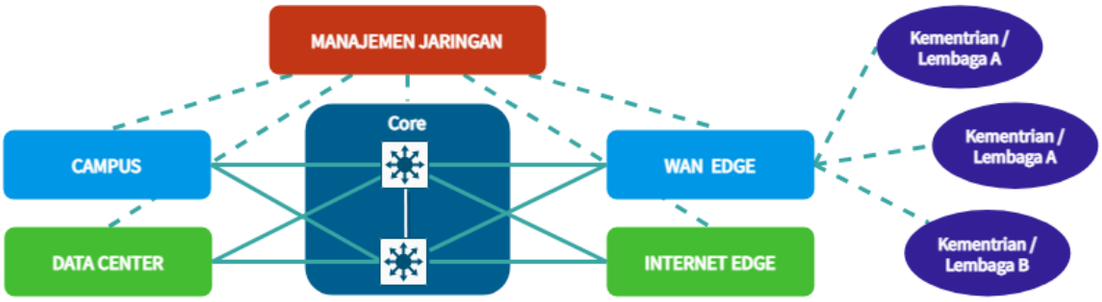
a. Perencanaan
1. Analisis kebutuhan
2. Manajemen risiko dan kesesuaian

b. Operasional
   1. Organisasi penyelenggara pusat data
   2. Sistem manajemen layanan operasional pusat data
   3. Infrastruktur
c. Manajemen layanan
   1. Sistem manajemen layanan tingkat lanjut (STML)
   2. Manajemen keselamatan
   3. Manajemen keamanan
   4. Manajemen proyek
d. Manajemen SDM
   1. Pengelolaan kompetensi
   2. Pelatihan
   3. Manajemen kinerja
e. *Monitoring*, pelaporan dan pengendalian
f. Manajemen keberlangsungan
   1. Manajemen keberlangsungan kegiatan
   2. 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

C. Jaringan Intra Pemerintah

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

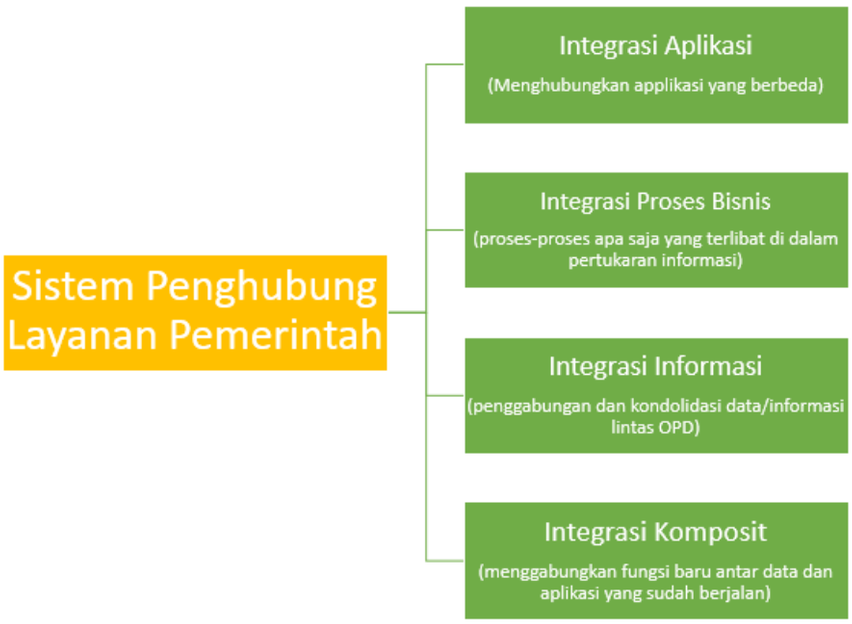


Gambar 4.2.11.15. Arsitektur Jaringan Intra Diskominfo Kabupaten Tegal

Dari gambar arsitektur di atas diperoleh informasi bahwa untuk koneksi jaringan intra pemerintah antara jaringan Diskominfo Kabupaten Tegal 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.

D. Sistem Penghubung Layanan Pemerintah

Sistem penghubung layanan pemerintah adalah integrasi kolaborasi.

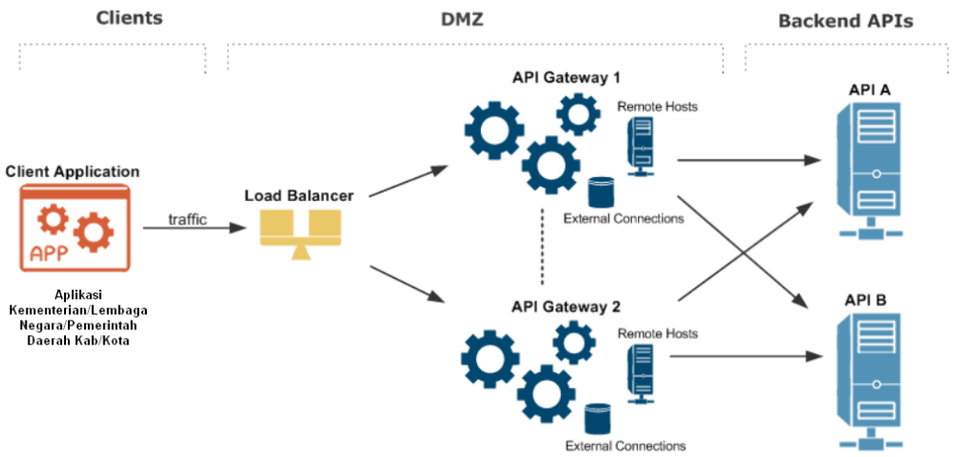


Gambar 4.2.11.16. Sistem Penghubung Layanan Pemerintah

***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 4.2.11.17. Arsitektur API Gateway dengan konfigurasi High Availability (Sumber: https://docs.oracle.com/cd/E55956_01/doc.11123/administrator_guide/content/high_availability.html)

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).

3.3 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 3.3.1. Lingkup Manajemen SPBE

#	Lingkup	Referensi
a.	Manajemen Risiko	PermenpanRB 05/2020, ISO 31000, 27005
b.	Manajemen Keamanan Informasi	ISO 27001, Indeks KAMI
c.	Manajemen Data	Perpres 39/2019, SNI 8799:2019, ISO 11179
d.	Manajemen Aset TIK	ISO 55001
e.	Manajemen SDM	PermenPANRB 38/2017, SFIA Framework
f.	Manajemen Pengetahuan	ISO 30401
g.	Manajemen Perubahan	COBIT 2019
h.	Manajemen Layanan	ITIL

3.3.1 Manajemen Risiko SPBE

Gambar 4.3.1.1. 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:

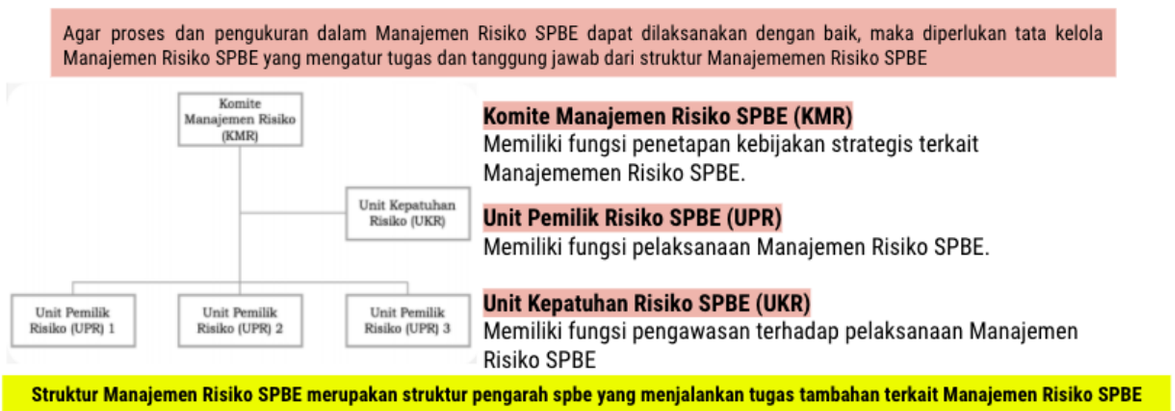
1. Meningkatkan kemungkinan pencapaian tujuan penerapan SPBE di Pemerintah Daerah.
2. Memberikan dasar yang kuat untuk perencanaan dan pengambilan.
3. keputusan melalui penyajian informasi Risiko SPBE yang memadai di Pemerintah Daerah dalam penerapan SPBE.
4. Meningkatkan optimalisasi pemanfaatan sumber 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.

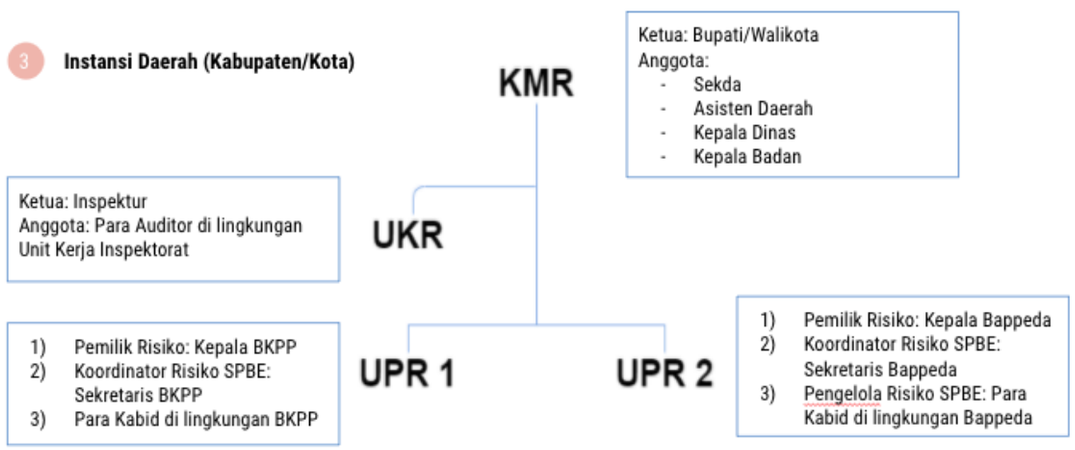
2. Mewujudkan penerapan SPBE yang terpadu di Instansi Pemerintah Daerah.
3. Meningkatkan kinerja pemerintahan di Instansi Pemerintah Daerah.
4. Meningkatkan reputasi dan kepercayaan pemangku kepentingan kepada Pemerintah Daerah.
5. Mewujudkan budaya kerja yang profesional dan berintegritas di Pemerintah Daerah.

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



Gambar 4.3.1.2. Pedoman Struktur Manajemen Risiko SPBE Daerah (sumber: paparan KemenpanRB)

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



Gambar 4.3.1.3. Struktur Manajemen Risiko SPBE Kab. Tegal

Merujuk pada *best practices* yang ada dalam PermenpanRB 05/2020 terdapat beberapa aktivitas yang dapat dilakukan oleh pemerintah daerah dalam upaya menajemen SPBE.

Gambar 4.3.1.4. Beberapa aktivitas yang dapat dilakukan oleh pemerintah daerah dalam upaya menajemen SPBE

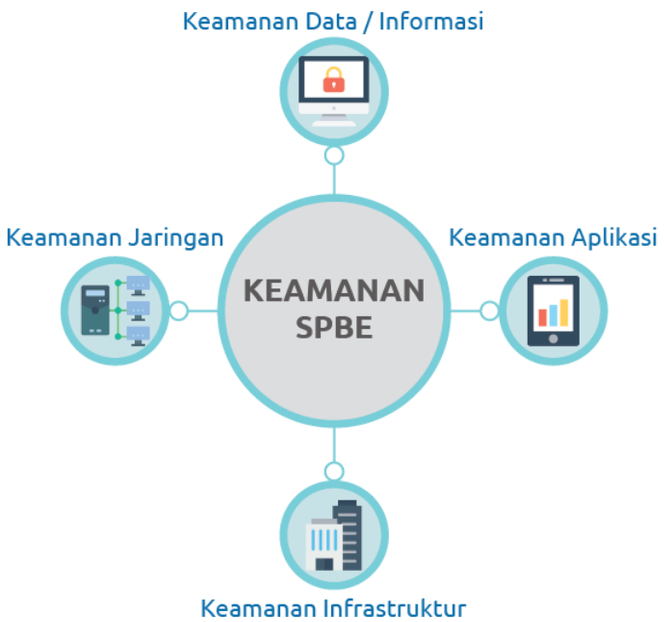
Secara teknis pemerintah daerah perlu menyusun Kajian dan SOP terkait manajemen risiko dengan lingkup sebagai berikut :

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

3.3.2 Manajemen Keamanan Informasi

Gambar 4.3.2.1. 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 4.3.2.2. Keamanan 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.

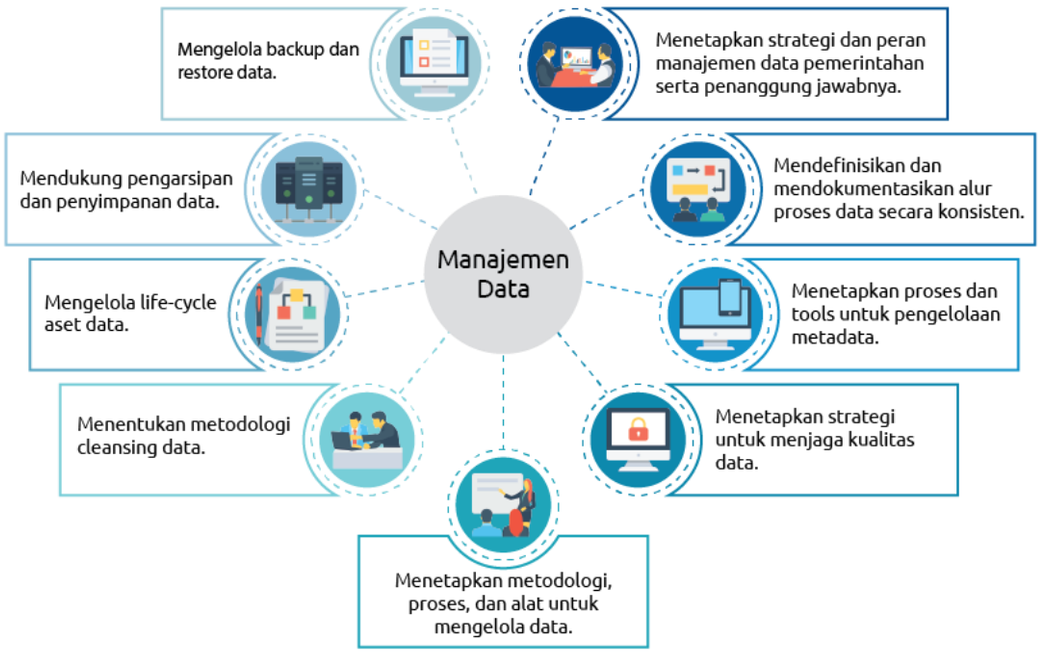
4. mendapatkan otorisasi dari pejabat struktural untuk menerapkan dan mengoperasikan atau mengubah manajemen keamanan informasi.
5. mempersiapkan dan memelihara pernyataan penerapan yang menggambarkan ruang lingkup manajemen keamanan informasi.
6. menetapkan serta mengkomunikasikan peran dan tanggung 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

3.3.3 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 4.3.3.1. 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 perangkat daerah. Menetapkan peran dan tanggung jawab masing-masing perangkat daerah 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 perangkat daerah.
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 perangkat daerah 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 perangkat daerah 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.

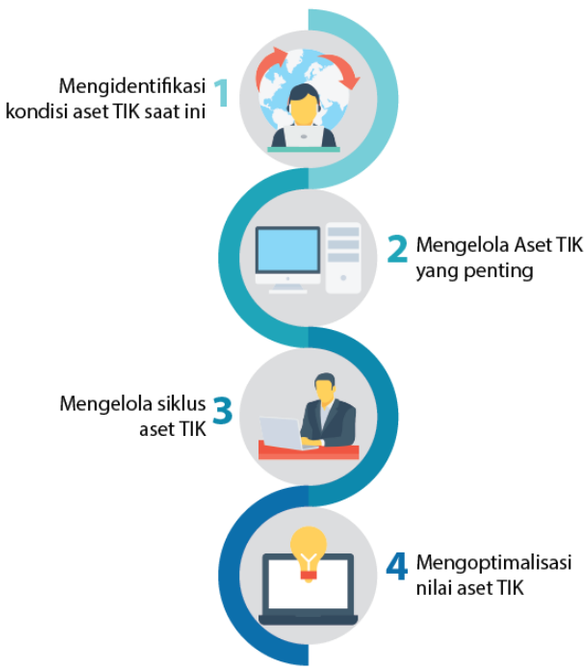
Secara teknis pemerintah daerah perlu menyusun kebijakan / SOP terkait manajemen data dengan lingkup sebagai berikut:

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

3.3.4 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 COBIT 2019, Berikut aktivitas-aktivitas yang perlu dilakukan dalam manajemen Aset TIK yaitu:



Gambar 4.3.4.1. 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.

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

4 SOP Pembuatan dan perubahan pengkodean Aset TIK.
5 SOP Inventarisasi dan konfigurasi Aset TIK.
6 SOP Pemeliharaan dan Perbaikan Aset TIK.
7 SOP Penghentian dan Pembuangan Aset TIK.

3.3.5 Manajemen SDM

Manajemen SDM perlu dilakukan guna menjamin keberlangsungan dan peningkatan mutu layanan SPBE dan memastikan ketersediaan kompetensi SPBE. Mengacu pada Peraturan Menteri PANRB Nomor 38 Tahun 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.

Gambar 4.3.5.1. Manajemen SDM

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

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

3.3.6 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. sembentukan Pokja beberapa unit-kerja untuk koordinasi implementasi manajemen dipimpin oleh pimpinan pemerintah daerah.
3. sefinisikan 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.

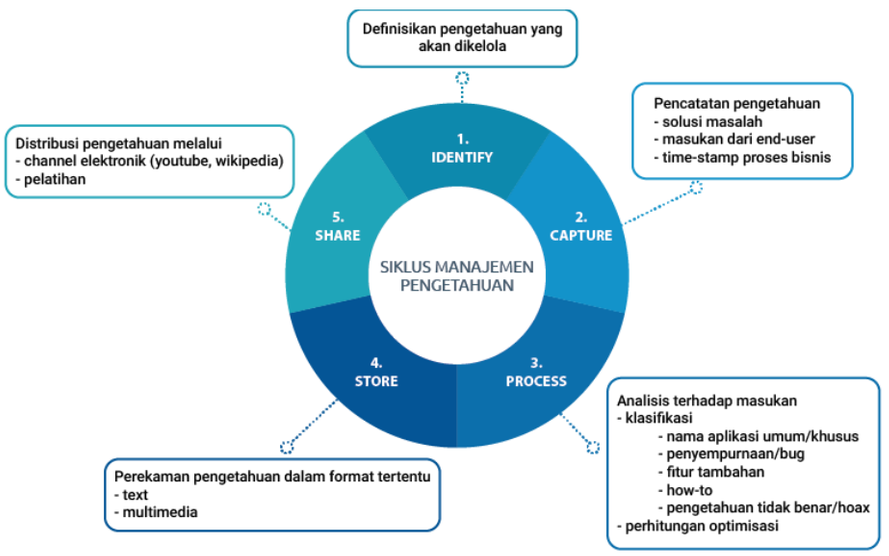
6. budayakan "*sharing & re-use*" sebagai cara bekerja yg efektif dan efisien.

Gambar 4.3.6.1. 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 4.3.6.2. Siklus Manajemen Pengetahuan

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

1. SOP Pencatatan pengalaman dan *lesson learned* untuk setiap perangkat daerah

3.3.7 Manajemen Perubahan

SPBE merubah cara kerja pemerintahan dari yang konvensional menjadi berbasis elektronik oleh karenanya pemerintah daerah perlu menerapkan manajemen perubahan yang bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan SPBE dan pengendalian perubahan pada penerapan SPBE. Mengacu pada Peraturan Menteri PANRB Nomor 10 Tahun 2011 tentang pedoman pelaksanaan program manajemen perubahan terdapat 3 tahapan yang dijelaskan sebagai berikut :

Gambar 4.3.7.1. Manajemen Perubahan

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

1. SOP Manajemen perubahan

3.3.8 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:

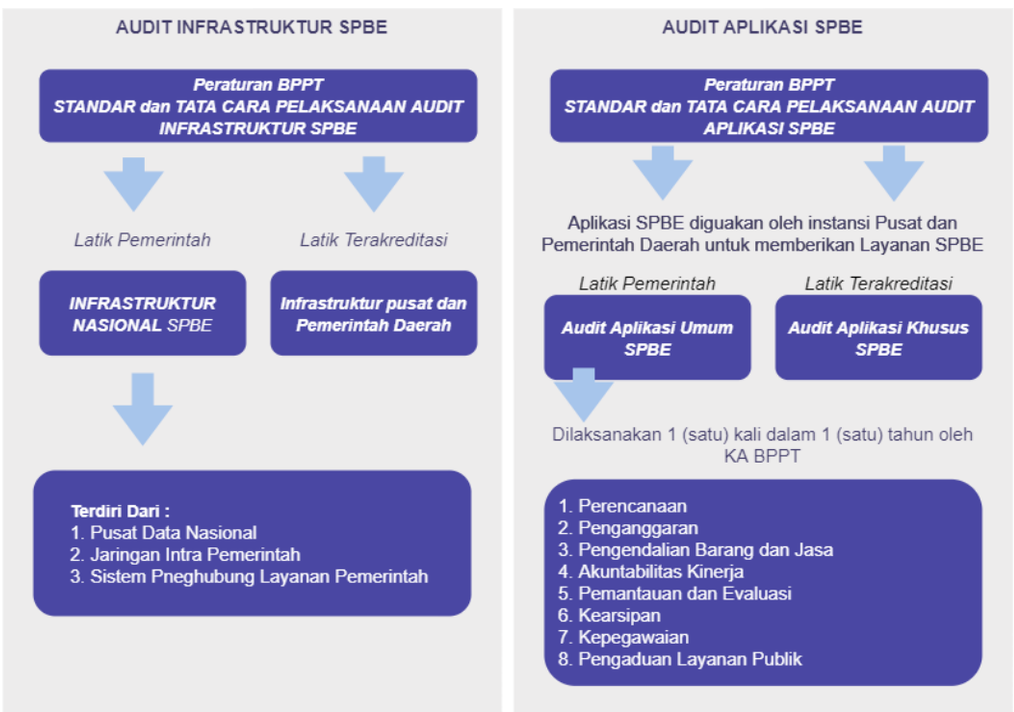
Gambar 4.3.8.1. Manajemen Layanan

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.

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

A. SOP Pengajuan layanan (Helpdesk)

3.3.9 Audit TIK



Gambar 4.3.9.1. Lingkup Audit TIK

(sumber: Paparan KemenpanRB)

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

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 Nomor 95 Tahun 2018 pasal 55 disebutkan:
   a. Infrastruktur SPBE Nasional diaudit setiap tahun oleh BPPT;
   b. Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah diaudit setiap dua tahun oleh lembaga audit TIK atau perusahaan audit TIK;
   c. 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 Pemda 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.

A. Kondisi Ideal Sumber Daya Manusia Tim Pelaksana Teknis

   Dalam kondisi ideal setiap pegawai Pemerintah Daerah diharapkan memiliki kemampuan penggunaan 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 perangkat daerah 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 sumber daya manusia 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 merencanakan, menganalisis, merancang, mengimplementasikan, mengembangkan dan atau mengoperasikan sistem informasi berbasis komputer.

3.4 Arsitektur SPBE

3.4.1 Layanan SPBE

A. Katalog Layanan

Berdasarkan dari hasil survei untuk saat ini belum ada perencanaan untuk penambahan jenis layanan baru, hanya saja kedepan memungkinkan bagi Pemerintah Kab. Tegal untuk membuat jenis layanan baru ketika ada arahan strategis maupun regulasi baru. Untuk saat ini yang menjadi mandatory dalam SPBE bagi Pemerintah Kab. Tegal yaitu melakukan integrasi antar layanan yang ada, serta melakukan evaluasi secara periodik atas implementasi layanan tersebut. Berikut ini disajikan daftar layanan SPBE yang ada di Pemerintah Kab. Tegal.

Tabel 4.4.1.1. Katalog Target Layanan

#	Layanan	Aplikasi
1	Layanan Perencanaan	SIPD
2	Layanan Penganggaran	SIPD
3	Layanan Keuangan	SIMDA Keuangan
4	Layanan Pengadaan Barang dan Jasa	SPSE
5	Layanan Kepegawaian	SIMPEG
6	Layanan Kearsipan Dinamis	e-Arsip
7	Layanan Pengelolaan Barang Milik Daerah	SIMBADA
8	Layanan Pengawasan Internal Pemerintah	SIM-HP
9	Layanan Akuntabilitas Kinerja Organisasi	e-SAKIP Reviu
10	Layanan Kinerja Pegawai	e-Kinerja
11	Layanan Pengaduan Pelayanan Publik	SPAN Lapor
12	Layanan Data Terbuka	Open Data

13	Jaringan Dokumentasi dan Informasi Hukum (JDIH)	JDIH
14	Layanan Publik Sektor Kesehatan	SIMRS dan BPJS
15	Layanan Publik Sektor Perizinan	OSS dan Si Cantik

3.4.2 Aplikasi SPBE

A. Katalog Aplikasi Usulan

Diagram target arsitektur aplikasi perlu mempertimbangkan inisiatif pengembangan aplikasi yang diusulkan oleh masing-masing perangkat daerah Pemkab Tegal di masa mendatang. Inisiatif-inisiatif tersebut akan berkembang dan bertambah seiring dengan kebutuhan proses operasional di masing-masing perangkat daerah. Berdasarkan dari diagram target arsitektur aplikasi yang menjadi prioritas utama yaitu mengubah layanan yang telah ada menjadi *smart services.* Berikut merupakan detail inisiatif pengembangan aplikasi tahun 2022 - 2026 di Kabupaten Tegal.

Tabel 4.4.2.1. Katalog Aplikasi Usulan

No	Kode	Domain Aplikasi	Kode	Area Aplikasi	Aplikasi	Deskripsi	Unit Pemilik	Platform	Layanan SPBE
1	RAA 02	Aplikasi Khusus	RAA 02.01	Aplikasi Misi Tertentu	ESAKIP	Aplikasi untuk peningkatan kualitas pelaksanaan akuntabilitas kinerja di lingkungan instansi pemerintah guna meningkatkan efektivitas dan efisiensi pelaporan penggunaan anggaran.	Bagian Organisasi	Web	Layanan Akuntabilitas Kinerja Organisasi
2	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	JIPP (Jaringan Inovasi Pelayanan Publik)	Aplikasi untuk mendokumentasikan dan mempromosikan inovasi pelayanan publik pada Masing-Masing Perangkat Daerah dan melaksanakan Kompetisi Inovasi Pelayanan Publik agar menumbuhkan semangat berinovasi sebagaimana kebijakan Pemerintah "one agency one innovation".	Bagian Organisasi	Web	Layanan Publik Sektor
3	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi	SIKODA (Sistem Informasi	Aplikasi untuk menilai kematangan Perangkat Daerah dengan mendasari	Bagian Organisasi	Web	Layanan Administrasi

				Tertentu	Kematangan Organisasi Daerah)	beberapa variabel yang ada pada Perangkat Daerah.			Pemerintah Lainnya
4	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Website Bagian Organisasi	Aplikasi untuk menampilkan aplikasi yang akan tersedia di Bagian Organisasi, materi rapat, dan berita mengenai kegiatan di Bagian Organisasi.	Bagian Organisasi	Web	Layanan Administrasi Pemerintah Lainnya
5	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Tanda Daftar Kelompok Perikanan Tangkap	Aplikasi untuk Menerbitkan Tanda Daftar Kelompok	Dinas Perikanan	Desktop	Layanan Administrasi Pemerintah Lainnya
6	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Tanda Daftar Kelompok Perikanan Budidaya dan Pengolahan Pemasaran	Aplikasi untuk Menerbitkan Tanda Daftar Pelaku Usaha Perikanan Budidaya dan Pengolahan Pemasaran	Dinas Perikanan	Desktop	Layanan Administrasi Pemerintah Lainnya
7	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Rekomendasi TDUP (Tanda Daftar Usaha Pariwisata)	Aplikasi untuk memberikan Rekomendasi Izin Tanda Daftar Usaha Pariwisata	Dinas Kepemudaan, Olah Raga dan Pariwisata	Web	Layanan Publik Sektor
8	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Database Kepariwisataan	Aplikasi untuk pusat sistem Informasi Kepariwisataan	Dinas Kepemudaan, Olah Raga dan Pariwisata	Web	Layanan Publik Sektor
9	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Sistem Informasi Kepemudaan	Aplikasi untuk pusat sistem Informasi Kepemudaan	Dinas Kepemudaan, Olah Raga dan Pariwisata	Web	Layanan Administrasi Pemerintah Lainnya

10	RAA 01	Aplikasi Umum	RAA 01.02	Aplikasi Administrasi Pemerintahan	E-Presensi	Aplikasi untuk melakukan presensi ASN menggunakan deteksi wajah dan titik koordinat sesuai perangkat daerah berbasis mobile	Badan Kepegawaian dan Pengembangan Sumber Daya Manusia	Mobile	Layanan Kepegawaian
11	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	SISKA (Sistem Informasi Surat Keterangan Penelitian)	Aplikasi untuk pelayanan bagi pemohon yang akan melaksanakan penelitian	Dinas Penanaman Modal dan pelayanan Terpadu Satu Pintu	Web	Layanan Administrasi Pemerintah Lainnya
12	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	SI REKEBARU (Sistem Informasi Rencana Kebutuhan Barang Unit)	Aplikasi untuk Rencana Kebutuhan Barang Unit yg terintegrasi dengan perencanaan	Dinas Penanaman Modal dan pelayanan Terpadu Satu Pintu	Web	Layanan Perencanaan
13	RAA 02	Aplikasi Khusus	RAA 02.01	Aplikasi Misi Tertentu	SIKOPI	Aplikasi untuk informasi publikasi koperasi	Dinas Koperasi, Usaha Kecil dan Menengah dan Perdagangan	Web	Layanan Administrasi Pemerintah Lainnya
14	RAA 02	Aplikasi Khusus	RAA 02.01	Aplikasi Misi Tertentu	Tracing space aplikasi layanan member co-Walking	Aplikasi untuk data member co - walking	Dinas Koperasi, Usaha Kecil dan Menengah dan Perdagangan	Web	Layanan Administrasi Pemerintah Lainnya
15	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	SIMPURNA 1.1	Aplikasi Untuk Pengembangan aplikasi SIMPURNA (perbaikan dashboard dan framework) dan penambahan / perbaikan fitur	Dinas Perumahan Rakyat dan Kawasan Permukiman, serta Pertanahan	Web	Layanan Administrasi Pemerintah Lainnya

16	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Layanan IUJK	Aplikasi Izin Usaha Jasa Konstruksi	Bidang Jasa Konstruksi	Web	Layanan Akuntabilitas Kinerja Organisasi
17	RAA 01	Aplikasi Umum	RAA 01.02	Aplikasi Administrasi Pemerintahan	Simantap (Sistem Pemantauan Tahapan Pengadaan)	Aplikasi Untuk Mengetahui Proses Tahapan Pengadaan Dari Proses Di Perangkat Daerah Sampai Dengan Tayang Di Spse 4.4	Bagian Pengadaan Barang dan Jasa	Web	Layanan Pengadaan
18	RAA 01	Aplikasi Umum	RAA 01.02	Aplikasi Administrasi Pemerintahan	E-ARSIPSPJ	Aplikasi untuk mengarsipkan data surat pertanggungjawaban untuk mempermudah dalam proses penyimpanan dokumen serta akses dokumen tersebut keuangan	Dinas Lingkungan Hidup	Web	Layanan Kearsipan
19	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	E-STOCK BARANG (Masuk dan Keluar)	Aplikasi untuk mengetahui persediaan barang habis pakai yang ada di gudang	Dinas Lingkungan Hidup	Web	Layanan Pengelolaan Barang Milik Negara/Daerah
20	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	SIPEMAS (Sistem Penyajian Data Pemantauan Air Sungai berbasis wibsite)	Aplikasi untuk mengetahui sejauh mana kondisi sungai di Kab.Tegal tentang pencemarannya	Dinas Lingkungan Hidup	Web	Layanan Administrasi Pemerintah Lainnya
21	RAA 02	Aplikasi Khusus	RAA 02.01	Aplikasi Misi Tertentu	Indeks Kepuasan Masyarakat dengan aplikasi elektronik	Aplikasi untuk mengetahui jumlah kepuasan masyarakat dr pelayanan laboratorium	Dinas Lingkungan Hidup	Web	Layanan Administrasi Pemerintah Lainnya

22	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	e-Retribusi Sampah	Aplikasi Monitoring dan Pembuatan ID Billing untuk Pembayaran nontunai retribusi sampah	Dinas Lingkungan Hidup	Web	Layanan Administrasi Pemerintah Lainnya
23	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Go Ploong (Permintaan Penyedotan Lumpur Tinja secara elektronik)	Aplikasi untuk mempermudah permintaan pelayanan jasa penyedotan (tidak terpatok oleh waktu)	Dinas Lingkungan Hidup	Web	Layanan Publik Sektor
24	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	SAMRETA	Aplikasi untuk melihat timbulan sampah yang masuk ke TPA	Dinas Lingkungan Hidup	Web	Layanan Publik Sektor
25	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Sistem Informasi Lingkungan Hidup	Aplikasi Rencana Untuk Perda RPPLH Daerah	Dinas Lingkungan Hidup	Web	Layanan Administrasi Pemerintah Lainnya
26	RAA 01	Aplikasi Umum	RAA 01.01	Aplikasi Layanan Publik	SIPERLING (Sistem Pelaporan Persetujuan Teknis dan Persetujuan Lingkungan)	Aplikasi untuk memberikan kemudahan bagi pelaku usaha dalam menyampaikan laporan kewajiban dan ketentuan dalam persetujuan teknis (Pertek) dan persetujuan lingkungan (Perling)	Dinas Lingkungan Hidup	Web	Layanan Publik Sektor
27	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Aplikasi Tabungan Sampah	Aplikasi bagi nasabah bank sampah yang akan menjual sampah anorganiknya ke Bank Sampah	Dinas Lingkungan Hidup	Web	Layanan Administrasi Pemerintah Lainnya

28	RAA 01	Aplikasi Umum	RAA 01.01	Aplikasi Layanan Publik	RUBIKON (Rumah Bina Keluarga Online)	Aplikasi untuk pusat informasi, pembelajaran dan konsultasi berbasis online bagi keluarga dan masyarakat	Dinas Pemberdayaan Perempuan, Perlindungan Anak, Pengendalian Penduduk dan Keluarga Berencana	Web	Layanan Administrasi Pemerintah Lainnya
29	RAA 01	Aplikasi Umum	RAA 01.01	Aplikasi Layanan Publik	SIPER KPA (Sistem Pelaporan Kasus kekerasan Perempuan dan Anak)	Aplikasi untuk memberi laporan pengaduan kasus kekerasan Perempuan dan anak	Dinas Pemberdayaan Perempuan, Perlindungan Anak, Pengendalian Penduduk dan Keluarga Berencana	Web	Layanan Publik Sektor
30	RAA 01	Aplikasi Umum	RAA 01.02	Aplikasi Administrasi Pemerintahan	SIGA (Sistem Informasi Gender dan Anak) Kabupaten Tegal	Aplikasi untuk mengetahui data terpilah Gender dan Anak	Dinas Pemberdayaan Perempuan, Perlindungan Anak, Pengendalian Penduduk dan Keluarga Berencana	Web	Layanan Administrasi Pemerintah Lainnya
31	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Aplikasi Pencapaian Akseptor	Aplikasi untuk mengetahui capaian akseptor KB di tiap Desa dan Penyuluh	Dinas Pemberdayaan Perempuan, Perlindungan Anak, Pengendalian Penduduk dan Keluarga Berencana	Mobile	Layanan Administrasi Pemerintah Lainnya
32	RAA 01	Aplikasi	RAA	Aplikasi	Sistem Data	Aplikasi untuk mengakses capaian	Dinas	Web	Layanan

		Umum	01.02	Administrasi Pemerintahan	satu Perangkat Daerah	kinerja Dinas P3AP2 dan KB	Pemberdayaan Perempuan, Perlindungan Anak, Pengendalian Penduduk dan Keluarga Berencana		Administrasi Pemerintah Lainnya
33	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Sistem Pengelolaan Stuting	Aplikasi untuk mengetahui capaian penanganan stunting	Dinas Pemberdayaan Perempuan, Perlindungan Anak, Pengendalian Penduduk dan Keluarga Berencana	Web	Layanan Administrasi Pemerintah Lainnya
34	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	SINOKE (Aplikasi *New Order* Sembako)	Aplikasi untuk pencairan program SEMBAKO	Dinas Sosial	Web	Layanan Administrasi Pemerintah Lainnya
35	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Simda BLUD RSUD Suradadi	Aplikasi untuk pemberitahuan keadaan Keuangan BLUD Rsud Suradadi	Bagian Perencanaan dan Keuangan RSUD Suradadi	Desktop	Layanan Administrasi Pemerintah Lainnya
36	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Host to Host RSUD Suradadi dengan Bank Jateng	Aplikasi Host to Host RSUD Suradadi dengan Bank Jateng	Bagian Perencanaan dan Keuangan RSUD Suradadi	Web	Layanan Administrasi Pemerintah Lainnya
37	RAA 01	Aplikasi Umum	RAA 01.02	Aplikasi Administrasi Pemerint	SILAPERKASA (Sistem Layanan Permohonan	Aplikasi SILAPERKASA yang merupakan aplikasi reresmi yang digunakan untuk pendataan permohonan kerja sama daerah di lingkungan Pemerintah	Bagian Pemerintahan	Web	Layanan Administrasi Pemerintah Lainnya

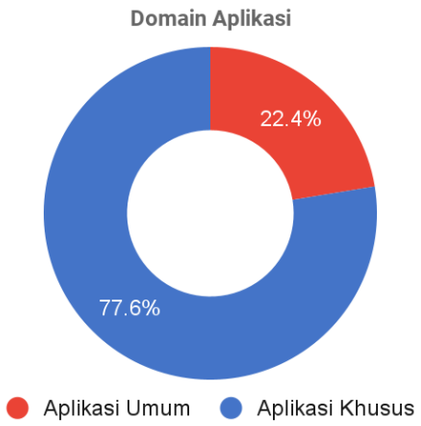
				ahan	Kerjasama)	KabupatenTegal yang dapat digunakan oleh instansi/badan daerah lain, pihak ketiga dan institusi pusat maupun institusi luar negeri yang terkait.			
38	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Sistem Informasi Pengelolaan Alsintan	Aplikasi untuk memantau data alat dan mesin pertanian yang ada dan pemanfaatannya	Dinas Ketahanan Pangan dan Pertanian	Web	Layanan Administrasi Pemerintah Lainnya
39	RAA 01	Aplikasi Umum	RAA 01.01	Aplikasi Layanan Publik	Google Form	Sistem Informasi Kepuasan Masyarakat	UPTD. Laboratorium	Web	Layanan Administrasi Pemerintah Lainnya
40	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Klinik Hukum	Aplikasi untuk konsultasi permasalahan-permasalahan hukum	Bagian Hukum	Web	Layanan Administrasi Pemerintah Lainnya
41	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Database Produk Hukum penyempurnaan dari Aplikasi ARTERI	Aplikasi Database Produk Hukum yang terintegrasi dengan Aplikasi e-SIMPUH	Bagian Hukum	Web	Layanan Administrasi Pemerintah Lainnya
42	RAA 01	Aplikasi Umum	RAA 01.01	Aplikasi Layanan Publik	Pendaftaran Online Pasien Rawat Jalan	Aplikasi Pendaftaran pasien rawat jalan secara online	RSUD dr. Soeselo Kab. Tegal	Mobile	Layanan Publik Sektor
43	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Rekam Medik Elektronik Rawat Inap	Sistem informasi kesehatan yang berisi data sosial pasien dan data medis pasien rawat inap.	RSUD dr. Soeselo Kab. Tegal	Web	Layanan Administrasi Pemerintah Lainnya

44	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Bridging Radiologi	Aplikasi untuk mengambil data/gambar hasil pemeriksaan alat-alat radiologi	RSUD dr. Soeselo Kab. Tegal	Web	Layanan Administrasi Pemerintah Lainnya
45	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	SIMPEG RS	Aplikasi Manajemen kepegawaian di RS	RSUD dr. Soeselo Kab. Tegal	Desktop	Layanan Kepegawaian
46	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Sistem Database Litbang dan InoVASI Daerah.	Pengelolaan daftar Litbang dan InoVASI Daerah	Badan Perencanaan Pembangunan Daerah, Penelitian dan Pengembangan	Web	Layanan Administrasi Pemerintah Lainnya
47	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Bank Data Desa	Digunakan untuk mengetahui jumlah dan daftar Kelembagaan Lembaga Kemasyarakatan Desa/Kelurahan (RT, RW, PKK, Posyandu, LPM, dan Karang Taruna) dan BUM Desa di masing-masing desa di Kabupaten Tegal	Dinas Pemberdayaan Masyarakat dan Desa	Web	Layanan Administrasi Pemerintah Lainnya
48	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Sistem Informasi Manajemen Pendidikan (SIMDIK)	Untuk menjamin tersedianya data dan statistik pendidikan yang lengkap, benar, mutakhir dan akurat.	Dinas Pendidikan dan Kebudayaan	Web	Layanan Administrasi Pemerintah Lainnya
49	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Aplikasi Manajemen Magang/PKL	Aplikasi untuk mengelola Siswa / Mahasiswa Magang dari proses pendaftaran, pelaksanaan penilaian harian, penilaian akhir, monitoring oleh pembimbing	Data pendaftaran siswa/mahasiswa Magang, Data penilaian siswa/mahasiswa Magang	Mobile	Layanan Administrasi Pemerintah Lainnya

50	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Aplikasi Helpdesk Aplikasi	Aplikasi untuk mengelola aduan terkait permasalahan pada aplikasi	Data pelaporan, Data permasalahan, Data Penyelesaian Permasalahan	Web	Layanan Administrasi Pemerintah Lainnya
51	RAA 01	Aplikasi Umum	RAA 01.02	Aplikasi Administrasi Pemerintahan	Aplikasi Aset TIK	Aplikasi untuk mengelola Aset TIK (software, hardware, license software, dll)	Data aplikasi, Data Hardware TIK, Data License Software	Web	Layanan Administrasi Pemerintah Lainnya
52	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Aplikasi Pelatihan / Bimtek Online	Aplikasi untuk memberikan pelatihan / bimtek secara online menggunakan video / materi tertulis	Data peserta pelatihan, data pelatihan, data materi pelatihan	Desktop	Layanan Administrasi Pemerintah Lainnya
53	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	PEPRIBAGUM	Melayani pinjam tempat, kendaraan dinas, dan pelayanan bagian umum lainnya secara online	Melayani pinjam tempat, kendaraan dinas, dan pelayanan bagian umum lainnya secara online	Web	Layanan Administrasi Pemerintah Lainnya
54	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Upgrade SIAP LAJU	Menambahkan fitur pengajuan andalalin	Data Analisis Dampak Lalu Lintas	Web	Layanan Administrasi Pemerintah Lainnya
55	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Website Profile	Website Profile Satpol PP	Data Profile Satpol PP	Web	Layanan Administrasi Pemerintah Lainnya

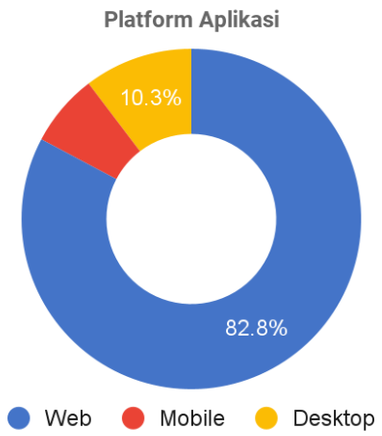
56	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Aplikasi Survey Management	Penginputan Data Kegiatan Lapangan Satpol PP	Data Survey Lapangan	Web	Layanan Administrasi Pemerintah Lainnya
57	RAA 02	Aplikasi Khusus	RAA 02.02	Aplikasi Fungsi Tertentu	Aplikasi Alih Media Arsip	Aplikasi Alih Media Arsip untuk pengelolaan arsip masyarakat, industri dan ormas.	Data Alih media arsip	Web	Layanan Kearsipan
58	RAA 01	Aplikasi Umum	RAA 01.02	Aplikasi Administrasi Pemerintahan	SIMPEL POK (Sistem Pelaporan Pengendalian Operasional Kegiatan)	Digunakan untuk mencatat laporan pelaksanaan APBD per bulan dari masing-masing bagian di Setda sebagai bahan pelaporan ke Bappeda, Rapat Komisi DPRD dan bahan Rakorpok Intern Setda	Realisasi keuangan dan fisik, hambatan pelaksanaan dan rencana tindak lanjut	Desktop	Layanan Administrasi Pemerintah Lainnya

Analisa aplikasi yang diusulkan oleh perangkat daerah adalah sebagai berikut:



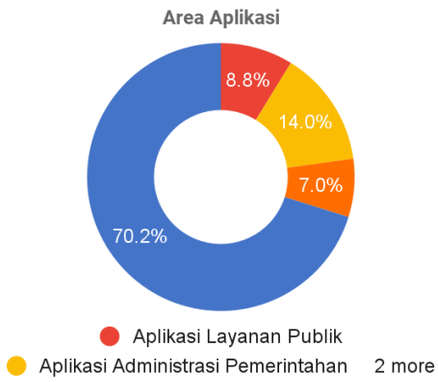
Grafik 4.4.2.1. Rencana Pengembangan Sistem Informasi

Sebanyak 58 aplikasi yang diusulkan dimana 77,6% (45 aplikasi) merupakan aplikasi khusus yang hanya dapat digunakan pada Perangkat Daerah yang mengusulkan, dan 22,4% (13 aplikasi) merupakan aplikasi umum yang dapat digunakan lebih dari satu Perangkat Daerah.



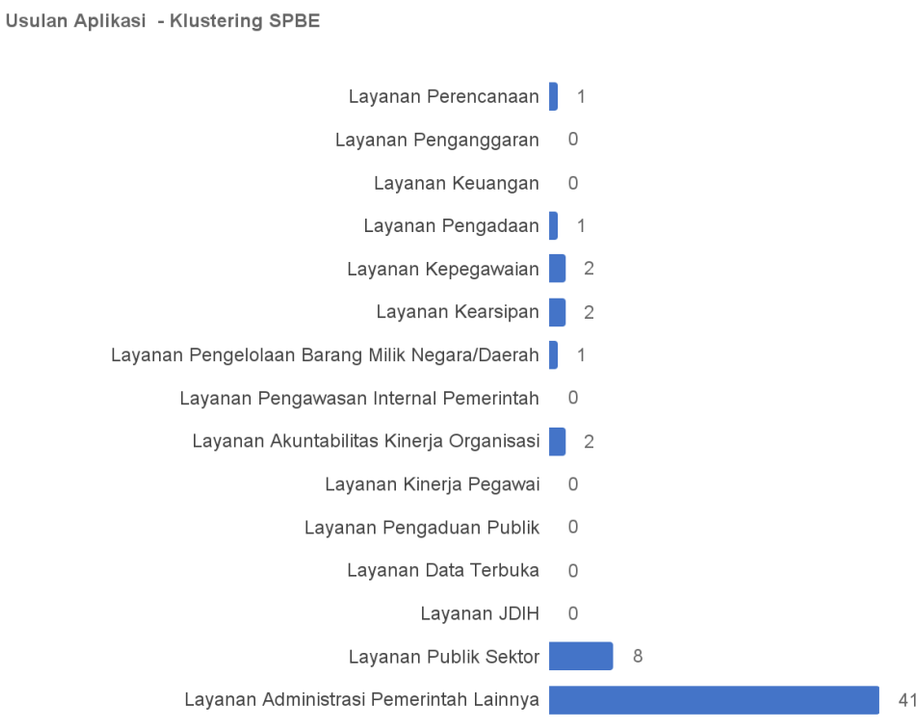
Grafik 4.4.2.2. Rencana Pengembangan Platform Teknologi

Untuk platform aplikasi yang diusulkan dimana platform web sebanyak 82,8% (48 aplikasi), dilanjut dengan platform mobile sebanyak 6,9% (4 aplikasi), lalu platform Desktop sebanyak 10,3% (6 aplikasi), jadi dengan total aplikasi sejumlah 58 tersebut akan bisa berjalan pada platform Web, Mobile dan Desktop.



Grafik 4.4.2.3. Rencana Pengembangan Area Aplikasi

Untuk area aplikasi pada aplikasi usulan dimana sejumlah 8.6% (5 aplikasi) merupakan aplikasi layanan publik, 13,8% (8 aplikasi) merupakan aplikasi administrasi pemerintahan, 6,9% (4 aplikasi) merupakan aplikasi misi tertentu, 70.7% (41 aplikasi) merupakan aplikasi fungsi tertentu.



Grafik 4.4.2.4. Klastering Aplikasi Usulan sesuai Dimensi SPBE

Pada Grafik 3.7 dapat dilihat bahwa aplikasi yang diusulkan sesuai dimensi SPBE didominasi oleh aplikasi untuk mendukung layanan Perencanaan 1 aplikasi, layanan Pengadaan 1 aplikasi, layanan kepegawaian 2 aplikasi, layanan kearsipan 2 aplikasi, layanan pengelolaan barang milik negara/daerah 1 aplikasi, layanan akuntabilitas kinerja

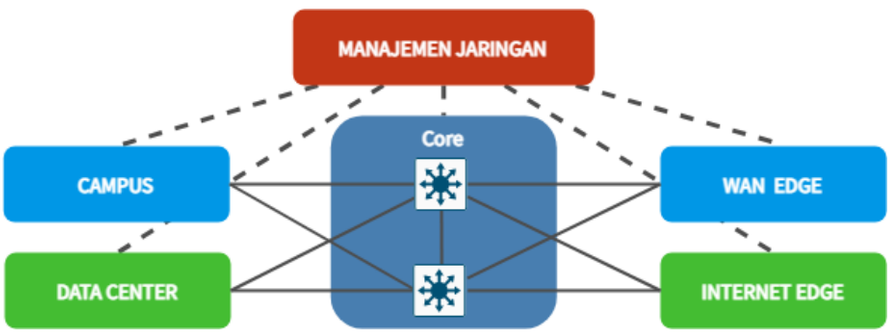
organisasi 2 aplikasi, layanan publik sektor 8 aplikasi, layanan administrasi pemerintahan lainya 41 aplikasi. Sedangkan pada klaster layanan lainnya tidak ada aplikasi yang diusulkan.

Selanjutnya selain perlu mengembangkan berbagai aplikasi baru ke depan juga perlu melakukan integrasi antar aplikasi yang merupakan mandatory dalam evaluasi SPBE. Berikut ini dijelaskan inisiatif integrasi antar aplikasi.

3.4.3 Arsitektur Infrastruktur Jaringan Intra Pemerintah

Segmentasi Jaringan

Infrastruktur jaringan data Dinas Kominfo Kabupaten Tegal perlu dirancang secara sistematis supaya dapat mengakomodasi pengembangan tugas pokok Dinas Kominfo Kabupaten Tegal. Pendekatan dengan melakukan segmentasi jaringan dan penerapan hierarki sesuai dengan fungsinya dapat menjadi solusi.



Gambar 4.4.3.1 Segmentasi Jaringan Dinas Kominfo Kabupaten Tegal

Segmentasi jaringan yang dibutuhkan Dinas Kominfo Kabupaten Tegal adalah sebagai berikut:

Core: Jaringan Core adalah jaringan inti yang menghubungkan antara segmen/ fungsi jaringan satu dengan lainnya. Di dalam jaringan inti terjadi lalu lintas jaringan yang cukup tinggi sehingga diperlukan perangkat jaringan berupa switch Layer 3 (L3) dengan spesifikasi tinggi;

Internet: Segmen jaringan yang bersinggungan langsung dengan internet disebut sebagai internet zone/ edge. Disini terdapat

pintu gerbang (gateway) utama dan cadangan untuk terhubung ke intranet maupun internet.

MAN/WAN: Segmen jaringan yang menghubungkan antara jaringan dengan beberapa lokasi kantor/ gedung di luar area komplek perkantoran Kabupaten Tegal disebut sebagai jaringan antar kota (Metropolitan Area Network). Segmen ini juga dapat digunakan untuk interkoneksi jaringan Kementerian/ Lembaga lain.

Campus Network: Pada segmen campus network merupakan jaringan internal dimana di dalamnya terdapat berbagai perangkat pengguna akhir (end user) seperti PC, laptop, mobile device, network printer, CCTV dan perangkat lainnya yang menggunakan IP Address protokol. Campus Network merupakan jaringan lokal yang ada di gedung kantor pemerintahan di komplek kantor Pemerintah Kabupaten Tegal yang dikelola oleh Dinas Kominfo Kabupaten Tegal.

Data Center: Pada segmen Data Center zone server-server yang melayani permintaan data dari jaringan internal (LAN) maupun internet. Pusat data menampung server, aplikasi, dan perangkat penyimpanan untuk digunakan oleh pengguna internal. Pusat data juga menghubungkan infrastruktur jaringan yang ini perangkat memerlukan, termasuk router, switch, load balancers, perangkat pengiriman konten, dan perangkat akselerasi aplikasi.

Manajemen Jaringan: Pada segmen network management (manajemen jaringan) zone terdapat proses untuk mengelola lalu-lintas komunikasi data, menentukan skala prioritas komunikasi, pengelolaan jaringan nirkabel dan lain sebagainya. Tools atau perangkat yang ada di dalam network management antara lain DNS Server, DHCP Server, Directory Service Server, WiFi Controller, pemantauan jaringan (Network Management System), dan lain - lain.

Hirarki Tiga Lapisan (3-Tier Hierarchy)

Desain hirarkis memfasilitasi perubahan. Karena elemen dalam jaringan memerlukan perubahan, maka biaya untuk melakukan

peningkatan terkandung dalam sebagian kecil dari keseluruhan jaringan. Di besar arsitektur jaringan datar atau menyatu, perubahan cenderung berdampak sejumlah besar sistem. Mengganti satu perangkat dapat memengaruhi banyak jaringan karena kompleksnya interkoneksi.

Setiap lapisan model hirarkis memiliki peran spesifik:

- Lapisan inti

  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, Anda harus mendesain lapisan inti dengan komponen redundan. Lapisan inti harus sangat andal dan harus beradaptasi dengan perubahan dengan cepat.

- Lapisan distribusi

  Menghubungkan layanan jaringan ke lapisan akses dan implementasi kebijakan tentang keamanan, pemuatan lalu lintas, dan rute/ jalur data. Lapisan distribusi seringkali merupakan lapisan yang menggambarkan broadcast (penyiaran) domain. (Meskipun ini dapat dilakukan pada lapisan akses juga.) Di jaringan desain yang mencakup LAN virtual (VLAN), lapisan distribusi dapat dikonfigurasi untuk rute antara VLAN.

- Lapisan Akses

  Lapisan akses memberi pengguna di segmen lokal akses ke internetwork. Itu lapisan akses dapat mencakup router, sakelar, jembatan, hub media bersama, dan nirkabel titik akses. Seperti yang disebutkan, switch access sering diterapkan pada lapisan akses di kampus jaringan untuk membagi domain bandwidth untuk memenuhi tuntutan aplikasi itu membutuhkan banyak bandwidth atau tidak dapat menahan penundaan variabel yang ditandai oleh shared bandwidth.

High Availability (HA)

Untuk menjamin kualitas dan keberlangsungan layanan, Dinas Kominfo Kabupaten Tega perlu mengadopsi skema High Availability (HA) dimana seluruh perangkat jaringan dan infrastruktur pendukungnya memiliki cadangan yang terpasang secara bersamaan. Perangkat utama dan cadangannya dapat dipasang dengan dua skenario yaitu pertama adalah active-active dimana kedua perangkat bekerja secara aktif, dan kedua adalah active-passive atau active - standby dimana kedua perangkat menyala dengan salah satu bekerja aktif sedangkan satunya pasif/ standby dan menjadi aktif jika terjadi kegagalan di perangkat yang aktif sebelumnya.

Skema HA pada jalur koneksi yakni dengan menyediakan koneksi internet yang redundan atau minimal dua provider internet (ISP). Redudansi untuk memenuhi persyaratan ketersediaan jaringan elemen duplikat dalam jaringan. Redundansi berusaha menghilangkan titik tunggal dari kegagalan pada jaringan. Pada jalur jaringan utama (backbone link) juga dapat dilakukan konfigurasi untuk berpindah jalur secara otomatis apabila terjadi gangguan koneksi dari ISP yang utama ke ISP cadangan (auto switching / auto routing).

3.4.4 Keamanan SPBE

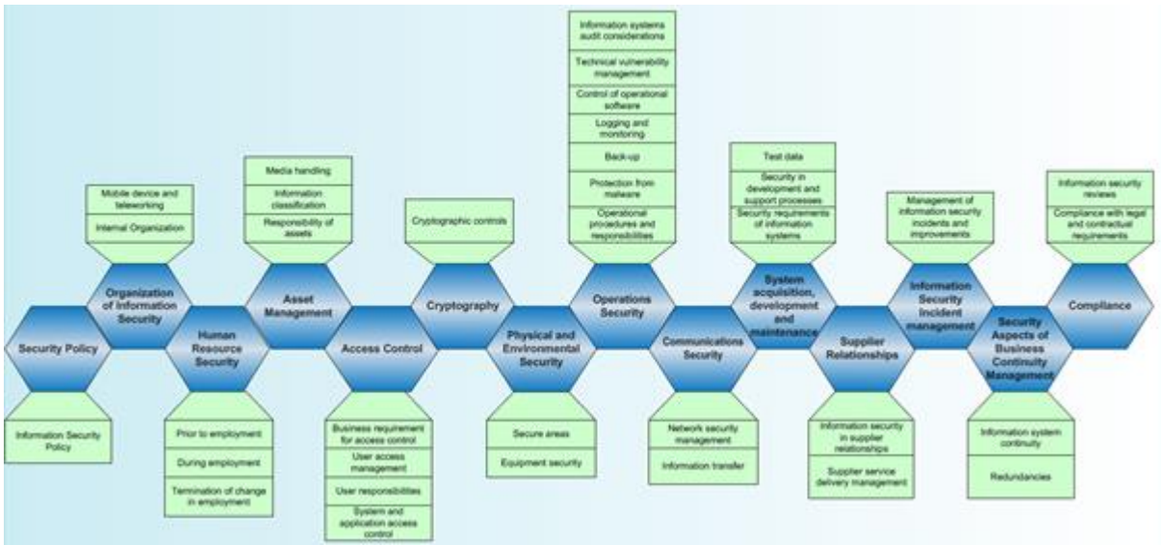
Pengembangan arsitektur Keamanan Informasi harus mempertimbangkan aspek teknis dan non-teknis karena kedua aspek tersebut sama pentingnya. Arsitektur Keamanan Informasi diperlukan karena adanya kebutuhan antara lain :

a. Untuk menjamin Integritas dari informasi (Integrity)
b. Untuk menjaga kerahasiaan informasi (Confidentiality)
c. Untuk memastikan kesiagaan sistem informasi (Availability)
d. Untuk memastikan pemenuhan peraturan, hukum, dan bakuan yang berlaku (Compliance)

Sistem Manajemen Keamanan Informasi - Information Security Management System (ISMS)

Salah satu acuan atau standar dalam pengembangan arsitektur Keamanan Informasi adalah ISO27001:2013 tentang “Information

Security Management System". ISO 27001:2013 terdiri dari 14 domain atau area kontrol yang disebut sebagai Annex sebagai berikut :



Gambar 4.4.4.1. Annex A (Domain) pada ISO 27001:2013

1. A.5 Security Policies
   - Memberikan arahan dan dukungan manajemen terhadap keamanan informasi sesuai dengan kebutuhan bisnis, peraturan hukum, dan regulasi yang berlaku.

2. A.6 Organisation of Information Security
   - Membangun kerangka kerja manajemen untuk memulai dan mengontrol pelaksanaan dan operasional keamanan informasi dalam organisasi.
   - Menjamin keamanan kerja jarak jauh dan penggunaan perangkat mobile.

3. A.7 Human Resource Security
   - Memastikan bahwa karyawan dan kontraktor memahami tanggung jawab sesuai dengan tugas mereka.
   - Memastikan bahwa karyawan dan kontraktor menyadari dan memenuhi tanggung jawabnya terhadap keamanan informasi.
   - Melindungi kepentingan organisasi sebagai bagian dari proses perubahan atau pengakhiran hubungan kerja.

4. A.8 Asset Management
   - Mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang tepat.

- Memastikan bahwa aset informasi menerima perlindungan sesuai dengan tingkat kepentingannya bagi organisasi.
- Mencegah pengungkapan tidak sah, modifikasi, penghapusan atau perusakan informasi yang tersimpan pada media.

5. A.9 Access Control
   - Membatasi akses terhadap informasi dan fasilitas pengolahan informasi.
   - Menjamin akses pengguna yang berwenang dan mencegah akses tidak sah ke sistem informasi dan layanan.
   - Membuat pengguna bertanggung jawab dalam menjaga informasi yang teridentifikasi.
   - Mencegah akses tidak sah ke sistem dan aplikasi.

6. A.10 Cryptography
   - Menjamin penggunaan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keaslian, dan / atau integritas informasi.

7. A.11 Physical and Environmental Security
   - Mencegah akses fisik yang tidak sah, kerusakan dan gangguan terhadap informasi dan fasilitas pengolahan informasi.
   - Mencegah kerugian, kerusakan, pencurian, atau apapun yang membahayakan aset dan mengganggu operasional organisasi.

8. A.12 Operations Security
   - Memastikan operasional fasilitas pengolahan informasi secara benar dan aman.
   - Memastikan bahwa informasi dan fasilitas pengolahan informasi dilindungi dari malware.
   - Melindungi kemungkinan hilangnya data.
   - Merekam peristiwa dan menghasilkan bukti.
   - Memastikan integritas operasional sistem.
   - Mencegah eksploitasi kerentanan teknis.
   - Meminimalkan dampak kegiatan audit pada operasional sistem.

9. A.13 Communications Security
    - Menjamin perlindungan informasi dalam jaringan dan fasilitas pengolahan informasi pendukungnya.
    - Menjaga keamanan informasi yang ditransfer di dalam organisasi maupun ke pihak eksternal.

10. A.14 Systems Acquisition, Development and Maintenance
    - Memastikan bahwa keamanan informasi merupakan bagian integral dari sistem informasi di seluruh siklus hidup, termasuk bagi sistem informasi yang menyediakan layanan melalui jaringan publik.
    - Memastikan bahwa keamanan informasi dirancang dan dilaksanakan dalam siklus hidup pengembangan sistem informasi.
    - Menjamin perlindungan data yang digunakan untuk pengujian.

11. A.15 Supplier Relationships
    - Memastikan perlindungan aset organisasi yang dapat di akses oleh pemasok.
    - Mempertahankan tingkat keamanan informasi dan pelayanan yang disepakati sesuai dengan perjanjian pemasok.

12. A.16 Information Security Incident Management
    - Memastikan pendekatan yang konsisten dan efektif untuk pengelolaan insiden keamanan informasi, termasuk komunikasi pada peristiwa keamanan dan kelemahan yang ditemukan.

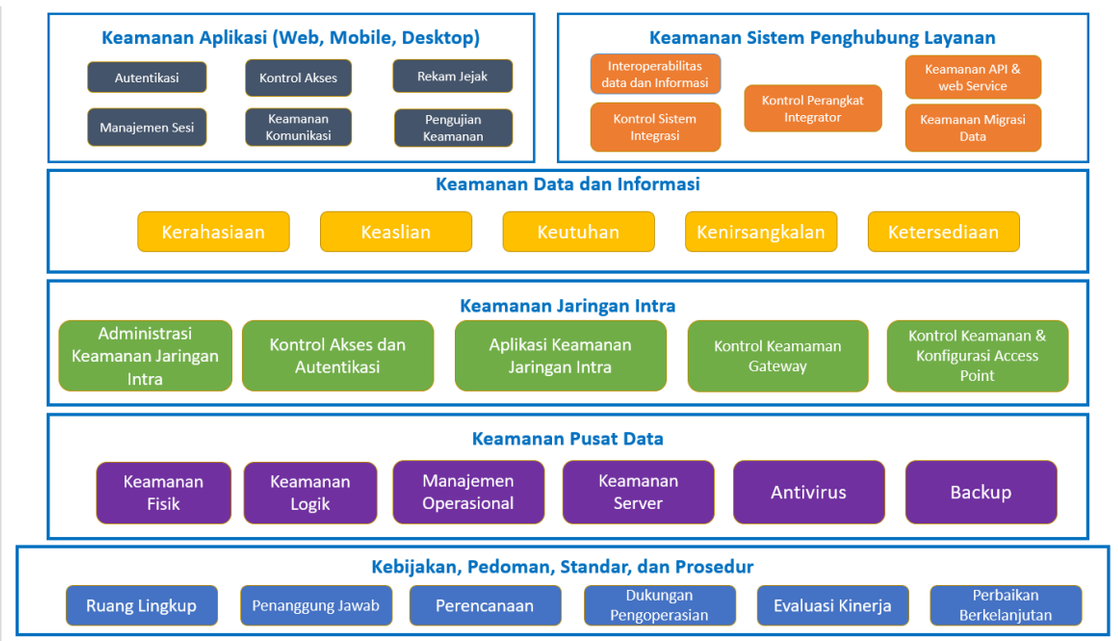
13. A.17 Information Security Aspects of Business Continuity Management
    - Kontinuitas keamanan informasi harus tertanam dalam sistem manajemen kelangsungan bisnis organisasi.
    - Memastikan ketersediaan fasilitas pengolahan informasi.

14. A.18 Compliance
    - Menghindari pelanggaran terhadap kewajiban hukum, undang – undang, peraturan atau kontrak yang terkait dengan keamanan informasi dan persyaratan keamanan.
    - Memastikan bahwa keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.

Pedoman Manajemen Keamanan Informasi SPBE

Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.

Rancangan Arsitektur Keamanan Informasi



Gambar 4.4.4.2. Rancangan Arsitektur Keamanan

1. Keamanan Aplikasi SPBE
    a. Aplikasi Web
        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.
13) keamanan konfigurasi.

b. Aplikasi Mobile
1) penyimpanan data dan persyaratan privasi.
2) kriptografi.
3) autentikasi dan manajemen sesi.
4) komunikasi jaringan.
5) interaksi platform.
6) kualitas kode dan pengaturan build.
7) ketahanan.

2. Keamanan Sistem Penghubung Layanan
a. Keamanan interoperabilitas data dan informasi.
1) menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik.
2) menerapkan sistem enkripsi data
b. Kontrol sistem integrasi;
1) menerapkan protokol secure socket layer atau protokol transport layer security versi terkini pada sesi pengiriman data dan informasi.
c. Kontrol perangkat integrator.
1) menggunakan sistem operasi dan perangkat lunak dengan security patches terkini.
2) menerapkan firewall dan host-based intrusion detection systems.

3. Keamanan Data dan Informasi
a. Kerahasiaan
1) menetapkan klasifikasi informasi.
2) menerapkan enkripsi dengan sistem kriptografi.
3) menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.

b. Keaslian.
   1) menyediakan mekanisme verifikasi.
   2) menyediakan mekanisme validasi.
   3) menerapkan sistem hash function.
c. Keutuhan.
   1) menerapkan pendeteksian modifikasi
   2) menerapkan tanda tangan elektronik tersertifikasi
d. Kenirsangkalan.
   1) menerapkan tanda tangan elektronik tersertifikasi.
   2) penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.
e. Ketersediaan
   1) menerapkan sistem pencadangan secara berkala.
   2) membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses.
   3) menerapkan sistem pemulihan.

4. Keamanan Jaringan Intra
   a. Aspek administrasi keamanan jaringan Intra
   b. Kontrol akses dan autentikasi
   c. Persyaratan perangkat dan aplikasi keamanan jaringan intra
   d. Kontrol Keamanan Gateway
   e. Kontrol keamanan access point pada jaringan nirkabel
   f. Kontrol konfigurasi access point pada jaringan nirkabel
5. Keamanan Pusat Data
   a. Persyaratan Keamanan fisik dan manajemen Pusat Data
   b. Persyaratan koneksi perangkat ke Pusat Data
      1) Memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data;
      2) Memutus akses fisik atau logic dari perangkat yang tidak terotorisasi;
      3) Memastikan akses tingkat administrator ke server dan perangkat jaringan utama tidak boleh dilakukan secara remote;
      4) Memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area Pusat Data Melakukan

backup informasi dan perangkat lunak yang berada di Pusat Data secara berkala;

5) Memastikan perangkat komputer Pusat Data terbebas dari virus dan malware;
6) Melakukan pembatasan Kerakses pembatasan akses pemanfaatan removable media di area Pusat Data;
7) Memastikan pengaktifan konfigurasi port universal serial bus telah mendapatkan izin dari personil yang berwenang;
8) Memastikan setiap perangkat yang akan terkoneksi ke infrastruktur Pusat Data menggunakan internet protocol address dan hostname yang telah ditentukan;
9) Menerapkan server perantara saat client mengakses server database dalam rangka pemeliharaan;

6. Kebijakan, Pedoman, Standar, dan Prosedur Pedoman manajemen keamanan informasi SPBE meliputi:
   a. Penetapan ruang lingkup
      1) isu internal keamanan informasi SPBE dalam organisasi
      2) isu eksternal keamanan informasi SPBE
   b. Penetapan penanggung jawab
      1) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh sekretaris Instansi Pusat dan sekretaris daerah pada Pemerintah Daerah.
      2) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, sekretaris Instansi Pusat dan sekretaris daerah pada Pemerintah Daerah disebut sebagai koordinator SPBE.
      3) Pelaksana teknis Keamanan SPBE
         a. pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada Instansi Pusat dan Pemerintah Daerah masing-masing; dan
         b. pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE.

c. Perencanaan
   1) Perencanaan dilakukan oleh pelaksana teknis Keamanan SPBE.
   2) Program kerja keamanan SPBE.
   3) edukasi kesadaran Keamanan SPBE.
   4) penilaian kerentanan Keamanan SPBE.
   5) peningkatan Keamanan SPBE.
   6) penanganan insiden Keamanan SPBE.
   7) audit Keamanan SPBE.

d. Dukungan pengoperasian
   1) Peningkatan kapasitas
      a) Sumber daya manusia Keamanan SPBE
      b) Anggaran keamanan SPBE
   2) Kompetensi
      a) Keamanan infrastruktur teknologi, informasi, dan komunikasi
      b) Keamanan aplikasi
   3) Kegiatan
      a) Pelatihan dan/ atau sertifikasi kompetensi
      b) Bimbingan teknis mengenai standar Keamanan SPBE

e. Evaluasi kinerja
   1) mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE.
   2) menetapkan indikator kinerja pada setiap area proses.
   3) memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan.
   4) menganalisis efektifitas pelaksanaan Keamanan SPBE.
   5) mendukung dan merealisasikan program audit Keamanan SPBE.
   6) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

f. Perbaikan berkelanjutan.
   1) mengatasi permasalahan dalam pelaksanaan Keamanan SPBE.
   2) memperbaiki pelaksanaan Keamanan SPBE secara periodik.

Arsitektur keamanan terbagi menjadi lima zona yakni keamanan platform, keamanan sistem informasi, keamanan jaringan data, keamanan server, dan keamanan pusat data. Keamanan platform adalah perlindungan keamanan aplikasi yang diakses oleh pengguna baik melalui internet atau jaringan lokal. Prosedur keamanan platform sebagai berikut :

1. Platform aplikasi sebagian besar berbasiskan web, *mobile*, dan sebagian kecil *desktop*. Perlindungan aplikasi web dan mobile dapat menggunakan perangkat *Web Application Firewall (WAF)* dari serangan SQL *Injection, Cross Site Scripting,* dan lain - lainya sesuai rekomendasi OWASP *(Open Web Application Security Project).*
2. Aplikasi yang menggunakan autentikasi atau *login* perlu menggunakan protokol web yang aman (HTTP Secure) dengan implementasi sertifikat SSL agar ketika data ditransmisikan sudah dalam keadaan terenkripsi dan ini akan sangat menyulitkan *hacker* untuk mengetahui informasi yang dikirimkan.
3. Pengamanan pada HTTP *header* dengan melakukan optimasi pada *web server* yang digunakan sehingga akan menyulitkan *hacker* untuk melakukan percobaan masuk ke dalam sistem secara ilegal.
4. Aktivitas *vulnerability assessment and penetration test (VAPT)* dilakukan pada saat sebelum aplikasi di-publish ke umum. Setelah production juga prosedur VAPT dilakukan secara periodik agar dapat dideteksi kelemahan sistem sejak dini sebelum kelemahan tersebut dieksploitasi secara ilegal oleh *hacker*.

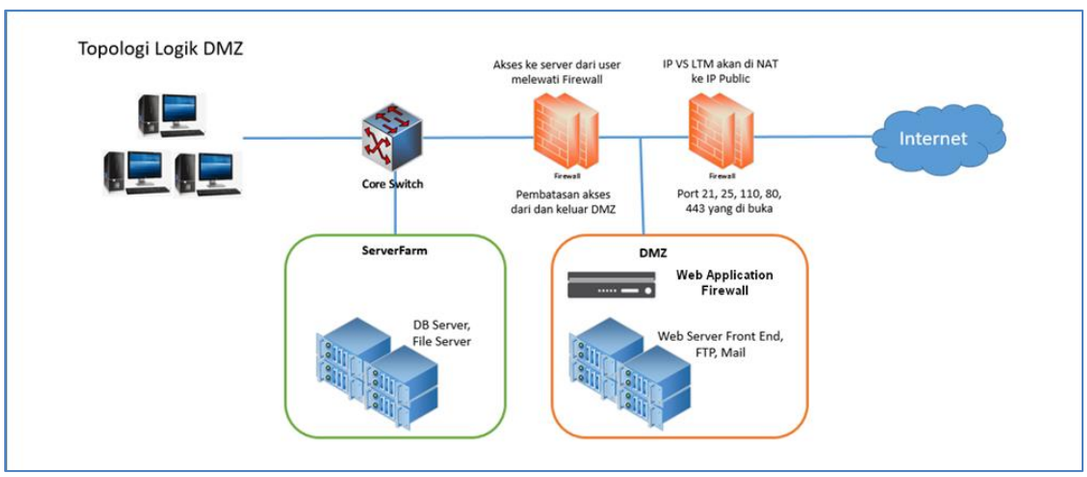
Zona kedua yakni Keamanan Sistem Informasi dengan aktivitas antara lain :

1. Prosedur keamanan aplikasi diterapkan sejak awal proses pengembangan yakni pada saat penulisan kode - kode program dengan memahami standar keamanan aplikasi dan diimplementasikan dalam *script* aplikasi yang dibuat. Beberapa *coding* dan *query* perlu dilindungi dari serangan SQL *Injection*, *brute force*, *web defacement*, dan lain-lain.

2. Keamanan basis data dengan penerapan level hak akses ke database, klasifikasi data, dan enkripsi untuk data - data dengan klasifikasi rahasia.
3. Layanan Arsitektur Berorientasi Layanan - Service Oriented Architecture (SOA) dilakukan dengan pembatasan jumlah akses, pemberian token, dan lain sebagainya.
4. Memastikan bahwa aplikasi yang dikembangkan dari pihak ketiga sudah melalui tahap pengujian kerentanan dan penetrasi.
5. Memastikan akses terhadap aplikasi hanya untuk pengguna yang terotorisasi.
6. Memastikan aplikasi memiliki *log* aktivitas yang dapat dipantau.

Zona ketiga yakni Arsitektur Keamanan Jaringan Data yakni dengan menerapkan hirarki (3-layer) dan modularitas pada topologi jaringan.

1. Perlindungan *server-server web* utama (*front end web*), mail server, FTP di dalam *De-Militerized Zone (DMZ)*.
2. Pemasangan perangkat *Web Application Firewall (WAF)* di zona DMZ.
3. Konfigurasi *firewall* yang hanya membuka *port-port* yang dibutuhkan saja.



Gambar 4.4.4.3. Topologi Logik DMZ

Secara logik web server, mail server, dan FTP server terpisah zona-nya dengan zona server farm yang didalamnya terdapat database server, file server, dan lain - lain. Akses dari pengguna, server di server farm, dan dari internet harus melalui perangkat firewall.

Firewall berfungsi untuk menyaring lalu lintas data ke DMZ berbasis alamat IP dan port.

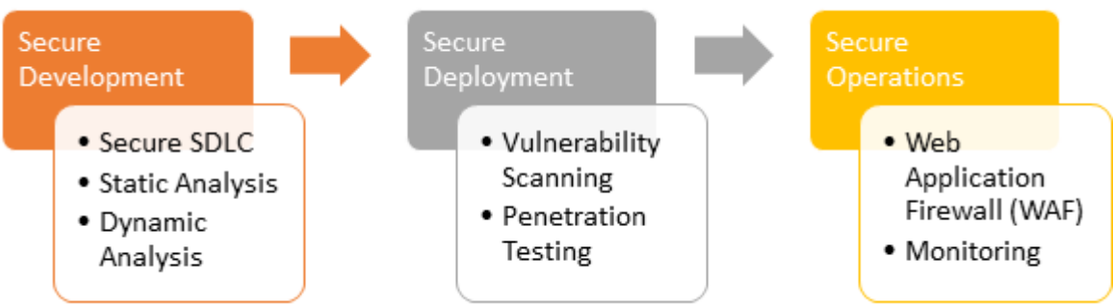
1. Pemasangan Next Generation-*Firewall* yang sudah ada modul Intrusion Prevention System (IPS) berfungsi untuk memblokir serangan dari luar serta identifikasi anomali trafik yang masuk ke jaringan internal Diskominfosandi.
2. Pemasangan alat pemantauan kinerja, kesehatan perangkat server pemakaian bandwidth internet.
3. Akses kontrol pengguna terhadap perangkat - perangkat jaringan.
4. Pemasangan analisis trafik data yang berfungsi untuk penyaringan berkas - berkas yang bisa dikirim melalui jaringan Diskominfosandi.

Zona keempat yakni Keamanan Server dengan implementasi manajemen update sistem operasi server, dan platform virtualisasi server yang digunakan.

Zona kelima yakni Keamanan Pusat Data dengan meningkatkan keamanan fisik seperti pemasangan CCTV, access control pintu ruang server, perangkat pemadam kebakaran, dan lain - lain. Keamanan Pusat data juga perlu selalu dipantau dan ada prosedur pengendalian jika terjadi insiden.

1. Keamanan Aplikasi

   Ogull dan Lane (2009) membuat daur hidup keamanan aplikasi web. Aplikasi web dibangun berdasarkan siklus daur hidup keamanan aplikasi yang dibagi menjadi 3 bagian besar seperti terlihat pada gambar di bawah ini :



Gambar 4.4.4.4. Siklus Hidup Keamanan Aplikasi Web

1. Pengembangan Keamanan *(Secure Development)*

   Secure development adalah bagaimana membangun aplikasi web dengan menerapkan prinsip keamanan. Beberapa pendekatan untuk melakukan *secure development* adalah dengan menerapkan *secure software development life cycle (SDLC), static analysis* dan *dynamic analysis.*

2. Pengujian Keamanan *(Secure Deployment)*

   Setelah semua tahap dalam pengembangan aplikasi selesai, tahap berikutnya adalah melakukan pengujian dan juga validasi. Tahap ini dilakukan untuk memastikan bahwa aplikasi tidak memiliki celah keamanan yang serius. Pengujian dan validasi dapat dilakukan dengan menggunakan metode *vulnerability assessment* dan *penetration testing.*

   Vulnerability Assessment, melakukan pemindaian (*scanning*) pada aplikasi web untuk mengetahui celah keamanan.

   Penetration Testing, adalah proses untuk membobol aplikasi untuk menentukan celah keamanan dan resiko yang ditimbulkannya. Proses *vulnerability assessment* digunakan menemukan celah keamanan sedangkan penetration testing memeriksa semua lubang untuk mengukur dampak.

3. Operasional Keamanan *(Secure Operation)*

   Bagaimana kita meningkatkan keamanan aplikasi web dengan cara mengimplementasikan perangkat keamanan seperti web *application firewall (WAF)* maupun aplikasi pemantauan lainnya pada saat aplikasi web telah dioperasikan.

***Secure* SDLC**

Software Development Life Cycle (SDLC) terdiri atas serangkaian tugas yang erat yang mengikuti langkah-langkah pendekatan sistem. Karena tugas-tugas tersebut mengikuti suatu pola yang teratur dan dilakukan secara *top-down*, SDLC sering disamakan dengan pendekatan air terjun *(waterfall approach)* walaupun pada pelaksanaannya mungkin bisa berbeda dan dapat menggunakan pendekatan lainnya.

Secara umum fase-fase dari siklus hidup pengembangan sistem informasi dapat dikelompokkan menjadi 4 fase besar seperti yang diilustrasikan pada gambar 5 yakni: Perencanaan, Analisa, Desain, dan Implementasi. Keamanan yang perlu diperhatikan dalam pengembangan sistem informasi dapat dikategorikan sesuai dengan fase/tahapan dalam pengembangan sistem informasi yakni :

1. Perencanaan

   Fase perencanaan ini dapat dilakukan investigasi awal dan kelayakan proyek (teknis, ekonomi dan operasional/organisasi) dan bagian keamanan yang perlu diperhatikan antara lain adalah: *Information security policy, Standard, legal issues, Early validation of concepts.*

2. Analisa

   Pada fase ini diperlukan hal-hal berikut ini sebagai melakukan kegiatan untuk aspek keamanan: *Threat, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, develop test plans, validation.*

3. Perancangan

   Pada fase ini juga diperlukan kegiatan-kegiatan berikut ini yang berkaitan dengan aspek keamanan yakni: *Incorporate security specifications, adjust test plans and data, determine access controls, design documentation, evaluate encryption options, design access control, consider business continuity issues, verification.*

4. Implementasi

   Pada fase implementasi biasanya terkait dengan pemrograman, instalasi dan rencana pemeliharaan , adapun kegiatan-kegiatan berikut ini yang berkaitan dengan aspek keamanan yakni: *Develop information security-related code, implement unit testing, incorporate other modules or units, support business continuity plan, develop documentation.*

Sepuluh besar Kerawanan pada Aplikasi

Open Web Application Security Project (OWASP) adalah sebuah organisasi nirlaba internasional yang memiliki visi untuk menjaga keamanan cyber termasuk website. OWASP menyediakan beberapa dokumen untuk membantu para developer membuat website dan aplikasi yang aman. Berikut ini adalah 5 dokumen sebagai panduan penting bagi para developer :

1. *OWASP Developer Guide*

   Guide ini dibuat agar para developer bisa membangun *website* atau software untuk organisasi mereka dengan menggunakan coding yang memiliki sistem yang aman. Guide ini berisikan prinsip-prinsip yang harus diikuti dalam proses codingnya.

2. *OWASP Application Security Verification Standard (ASVS)*

   ASVS adalah sebuah daftar persyaratan untuk memberi tahu para developer apakah sebuah aplikasi itu aman untuk digunakan oleh organisasi, vendor, dan *customer*.

3. *Security Knowledge Framework*

   Sebuah tool yang didesain untuk membantu developer membangun software yang aman. *Framework* ini dibangun berdasarkan standard ASVS sehingga developer bisa dengan mudah mengerti dan mengimplementasikan persyaratan keamanannya.

4. *Developer Cheat Sheet Series*

   Panduan yang dalam dan lengkap, membahas berbagai kelemahan, protokol keamanan, dan bagaimana mereka ada pada bahasa-bahasa programming terkenal. *Cheat sheet* ini didesain dengan bentuk *bullet points* jadi developer bisa mengerti *best practices* keamanan dan syarat-syaratnya dengan lebih mudah.

5. OWASP Top 10

   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.

Kelemahan-kelemahan ini memudahkan hacker untuk menanam *malware*, mencuri data, atau mengambil alih sepenuhnya website atau komputer target.

2. Keamanan Data

Data perlu diamankan dari kebocoran, penghapusan, dan kerusakan. Prinsip keamanan data antara lain :

1. Kerahasiaan (C*onfidentiality*)

Setiap data penting harus terjaga kerahasiaannya. Data atau informasi hanya boleh diakses sesuai dengan kepentingannya. Kecuali data atau informasi yang bersifat umum yang bisa diakses oleh setiap orang. Prinsip rahasia adalah menjamin data, informasi, objek dan sumber daya terbatas dari subjek yang tidak ter-otorisasi. Kerahasiaan adalah pencegahan bagi mereka yang tidak berkepentingan dapat mencapai informasi, berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Jenis ancaman serangan pada prinsip *security* ini meliputi mengintip lalu lintas *network* (biasanya dilakukan di *access point wifi public* di café atau tempat makan), mencuri *password* menggunakan *social engineering*, melakukan *port scanning* pada server, dan banyak aktifitas lainnya yang berusaha untuk mengambil data atau informasi penting.

Jika ada ancaman, tentu saja ada langkah pencegahannya, yaitu dengan menerapkan enkripsi pada informasi penting, penerapan akses control yang ketat bisa pada jaringan ataupun aplikasi, melakukan klasifikasi data, dan dapat juga berupa pelatihan karena confidentiality bisa juga terancam dikarenakan kelalaian seorang programmer, *system administrator* dan karyawan lainnya.

Privacy lebih kearah data-data yang sifatnya privat, informasi yang tepat terakses oleh mereka yang berhak dan bukan orang lain. Prinsip kerahasiaan ini tidak dapat berdiri sendiri, karena juga tergantung dengan konsep integritas. Tanpa

integritas data dijaga dengan baik, maka kerahasiaan tidak dapat dipelihara.

Usaha-usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi.

2. Integritas *(integrity)*

   Pemeliharaan data harus dapat mempertahankan kebenarannya dan modifikasi hanya dapat dilakukan oleh pihak yang memiliki kewenangan. informasi tidak boleh diubah tanpa seijin pemilik informasi, keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut. Agar *Integrity* dapat dipelihara maka kontrol harus ditempatkan untuk membatasi akses ke data, objek dan sumber daya. Kegiatan integritas data meliputi :

   a. Mencegah pihak manapun yang tidak berwenang untuk modifikasi
   b. Mencegah pihak yang berwenang dari membuat modifikasi yang tidak sesuai dengan otorisasi (hak akses)
   c. Memelihara konsistensi suatu objek agar data pada objek tersebut benar dan merefleksikan keadaan sebenarnya, dan setiap hubungan dengan objek lainnya menjadi valid, konsisten dan dapat diverifikasi.

   Beberapa contoh terkait ancaman serangan pada prinsip integritas yang dapat merubah data yaitu virus, akses yang tidak terotorisasi, *error coding* dan aplikasi yang menyebabkan data berubah, *malicious modification, backdoor* dan aktivitas lainnya yang menyebabkan suatu data dan informasi dapat berubah oleh pihak yang tidak berwenang.

   Langkah pencegahan dengan membuat akses control yang ketat, menggunakan peralatan seperti *Intrusion Detection System (IDS),* enkripsi pada objek, menggunakan *hash verification* untuk memeriksa validitas data, dan validasi pada sistem/aplikasi.

3. Ketersediaan (*availability*)

   Menjamin setiap pihak yang berwenang dapat mengakses data, objek dan sumber daya. Implementasi prinsip ketersediaan adalah dengan menyediakan *Disaster Recovery Center, Clustering* ataupun *Redundancy* pada system yang kritikal.

   Kontrol yang diperlukan dalam menjaga prinsip ini adalah untuk menjamin penanganan cepat ketika terjadi kegagalan sistem, menyediakan *redundancy*, memelihara *backup*, mencegah data hilang atau rusak.

   Ancaman serangan pada prinsip ini biasanya berupa kegagalan perangkat/mesin, error pada *software*, masalah pada lingkungan seperti banjir, kebakaran, mati listrik, dan juga ancaman hacker seperti DOS *Attack* juga termasuk yang mengancam prinsip *Integrity*.

   Sejumlah pencegahan yang dapat dilakukan terhadap ancaman tersebut seperti dengan menggunakan *firewall* atau *security tools* lainnya untuk mencegah DOS, implementasi *redundancy* untuk system yang kritikal, pemeliharaan backup dan *testing backup* yang baik dan juga memonitor kinerja lalu lintas jaringan dan system/server

4. Keautentikan (*authentication*)

   Autentikasi adalah proses verifikasi atau menguji apakah identitas yang diberikan adalah benar. Contoh implementasi pada sistem IT adalah dengan penerapan *password* pada halaman login.

5. Otorisasi (*authorization*)

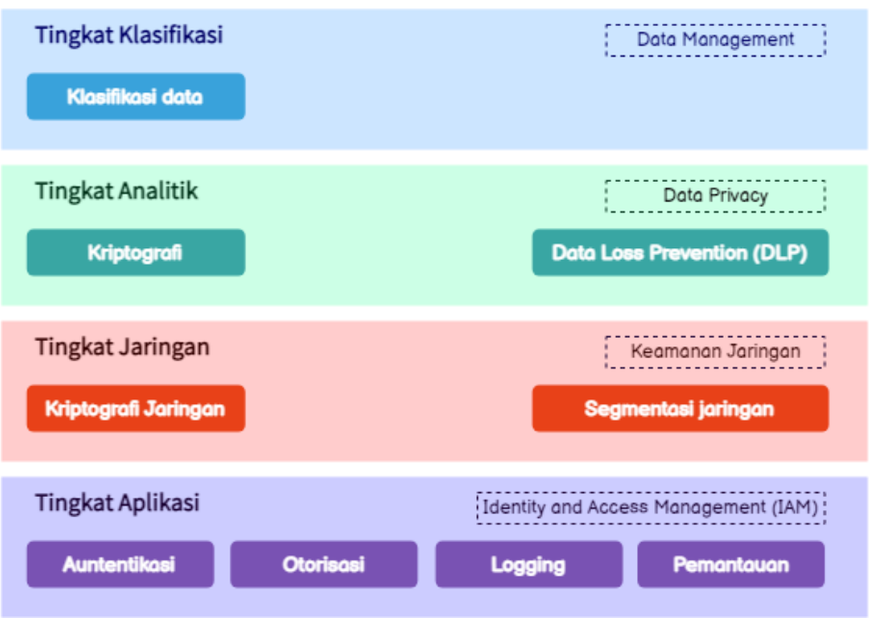
   Otorisasi adalah memastikan aktivitas request atau akses terhadap suatu objek sesuai dengan kewenangannya atau *privilege*. Jadi suatu akses yang berhasil masuk harus sesuai dengan pengaturan *privilege* yang berlaku. Pada sistem biasanya terdapat *Access Control* Matrix yang mengatur *privilege* suatu user.

6. Kenirsangkalan (*nonrepudiation*)

Setiap aktivitas subjek pada sistem tidak bisa disangkal lagi. Sehingga tidak bisa lagi subjek mengatakan bahwa bukan saya yang melakukan input pada sistem tersebut ataupun aktifitas lainnya. Non Repudiation dapat dilakukan jika konsep AAA *Services* sudah dijalankan dengan baik.

Salah satu langkah untuk *Non Repudiation* adalah seperti menerapkan sertifikat digital dalam otentikasi, otentikasi menggunakan *biometrics*, membuat *log* transaksi, setiap aktivitas direkam didalam *log*. Biasa banyak terjadi kegagalan dalam *Nonrepudiation* karena kebijakan *IT Security* masih belum diterapkan dengan baik, contohnya masih banyak yang melakukan *sharing password* untuk masuk ke sistem, dll.

Prosedur pengamanan data dapat menggunakan pendekatan kerangka kerja *Big Data (Big Data Framework).* Kerangka kerja ini dibagi menjadi empat tingkat yakni klasifikasi, analitik, jaringan, dan aplikasi seperti ditunjukkan gambar di bawah ini :



Gambar 4.4.4.5. Kerangka Kerja Keamanan Big Data

1. Tingkat Klasifikasi

Aset Informasi yang dikelola harus dapat diklasifikasikan berdasarkan asas risiko. Pedoman Tata Naskah Dinas Instansi Pemerintah Nomor 80 Tahun 2012 membagi data

menjadi tiga klasifikasi berdasarkan kekritisan data yakni :

- Sangat Rahasia

  Aset informasi yang bersifat strategis dan berisiko tinggi yang pembocoran atau akses tanpa izin terhadapnya mempunyai konsekuensi hukum. Informasi ini hanya dapat diakses secara sangat terbatas oleh pihak ketiga dan hanya dapat digunakan untuk kepentingan tertentu dengan syarat pihak ketiga menandatangani Kesepakatan Menjaga Rahasia *(Non-Disclosure Agreement – NDA)*

- Rahasia

  Aset informasi yang sangat peka dan berisiko tinggi atau yang menurut peraturan perundang – undangan dinyatakan rahasia yang pembocoran atau penyalahgunaan akses terhadapnya dapat mengganggu kelancaran kegiatan, citra dan reputasi lembaga. Informasi ini hanya dapat diakses secara terbatas oleh pihak ketiga dan hanya dapat digunakan untuk kepentingan tertentu dengan syarat syarat pihak ketiga menandatangani Kesepakatan Menjaga Rahasia *(Non-Disclosure Agreement – NDA.*

- Terbatas

  Aset informasi yang telah terdistribusi secara luas di lingkungan internal DJP yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik aset informasi dan risiko penyebarannya oleh pihak yang tidak berwenang tidak menimbulkan kerugian berarti. Informasi ini dapat diberikan kepada pihak ketiga oleh pemiliknya untuk kepentingan dinas melalui prosedur serah terima resmi.

- Biasa atau public

  Aset informasi yang secara sengaja disediakan untuk dapat diketahui masyarakat umum.

2. Tingkat Analitik

   Data Privasi adalah perlindungan terhadap kerahasiaan informasi dari semua pihak, kecuali yang memiliki wewenang. Perlindungan bisa dilakukan dengan teknik kriptografi, dan pemasangan perangkat *Data Loss Prevention (DLP)* untuk mendeteksi adanya berkas – berkas dengan klasifikasi terbatas sampai sangat rahasia yang akan di cetak, atau di kirim melalui jaringan internal.

3. Tingkat Jaringan

   Pengelolaan keamanan jaringan dengan melakukan segmentasi jaringan untuk memisahkan antara jaringan LAN, Server Farm, DMZ, dan Internet. Keamanan jaringan memastikan data ditransfer secara aman dan nyaman *(safe and secure)*. Proteksi keamanan bisa dilakukan pada komunikasi antar segmen. Akses jaringan nirkabel menggunakan protokol enkripsi.

4. Tingkat Aplikasi

   Pengelolaan aplikasi di awali dengan kontrol terhadap akses aplikasi dan data.

3. Keamanan Jaringan

Arsitektur Keamanan Informasi secara teknis bisa dibagi menjadi dua kategori yakni keamanan infrastruktur jaringan dan keamanan server. Prinsip pengembangan arsitektur keamanan infrastruktur jaringan data Kab. Tegal mengikuti 3 kaidah, yaitu:

1. Desain Keamanan Jaringan (*Network Security Design*)
2. Mekanisme Keamanan (*Security Mechanism*)
3. Desain Keamanan Modula (*Modularizing Security Design*)

Desain Keamanan Jaringan *(Network Security Design)*

Kegiatan dalam merancang keamanan jaringan meliputi:

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

   Aset jaringan dapat mencakup host jaringan (termasuk sistem operasi, aplikasi, dan data host), perangkat yang bekerja di internet (seperti router dan *switch*), dan data jaringan yang melintasi jaringan. Aset yang kurang jelas,

tetapi masih penting, termasuk intelektual properti, dan reputasi perusahaan.

2. Analisa Risiko Keamanan (*Analyzing Security Risks*)
   Risiko dapat berkisar dari penyusup yang bermusuhan (*hostile intruders*) hingga pengguna yang tidak terlatih yang mengunduh aplikasi Internet yang memiliki virus. Pengganggu yang bermusuhan dapat mencuri data, mengubah data, dan menyebabkan layanan ditolak untuk pengguna yang sah. Serangan *Denial-of-service (DoS)* semakin meningkat umum dalam beberapa tahun terakhir.

3. Menganalisis Persyaratan Keamanan dan Pengorbanan Kompromi (*Analyzing Security Requirements and Tradeoffs*)
   Kerahasiaan data, sehingga hanya pengguna yang berwenang yang dapat melihat informasi sensitif. Integritas data, sehingga hanya pengguna yang berwenang yang dapat mengubah informasi sensitive. Ketersediaan sistem dan data, sehingga pengguna memiliki akses tidak terputus ke penting sumber daya komputasi.

4. Mengembangkan Rencana Keamanan (*Developing a Security Plan*)
   Rencana harus didasarkan pada tujuan pelanggan dan analisis jaringan aset dan risiko. Rencana keamanan harus merujuk topologi jaringan dan memasukkan daftar layanan jaringan yang akan disediakan (misalnya, FTP, web, email, dan sebagainya). Daftar ini harus ditentukan siapa yang menyediakan layanan, siapa yang memiliki akses ke layanan, bagaimana akses diberikan, dan siapa yang mengelola layanan.

   Agar rencana keamanan bermanfaat, perlu mendapat dukungan dari semua tingkatan karyawan dalam organisasi. Sangat penting bahwa manajemen perusahaan mendukung sepenuhnya rencana keamanan. Staf teknis di kantor pusat dan lokasi terpencil harus setuju rencana, sebagaimana seharusnya pengguna akhir.

5. Mengembangkan Kebijakan Keamanan (*Developing a Security Policy*)

   Kebijakan keamanan memberitahu pengguna, manajer, dan staf teknis tentang kewajiban mereka untuk melindungi aset teknologi dan informasi. Kebijakan harus menentukan mekanisme dengan dimana kewajiban ini dapat dipenuhi. Seperti halnya dengan rencana keamanan, keamanan kebijakan harus diterima dari karyawan, manajer, eksekutif, dan tenaga teknis.

Komponen Kebijakan Keamanan

Secara umum, suatu kebijakan setidaknya harus mencakup item-item berikut:

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).

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.

Kebijakan otentikasi yang membangun kepercayaan melalui kebijakan kata sandi yang efektif dan mengatur pedoman untuk otentikasi lokasi jauh.

Kebijakan privasi yang menetapkan ekspektasi privasi yang wajar mengenai pemantauan surat elektronik, pencatatan penekanan tombol, dan akses ke file pengguna.

Pedoman pembelian teknologi komputer yang menentukan persyaratan untuk memperoleh, mengkonfigurasi, dan mengaudit sistem dan jaringan komputer untuk kepatuhan dengan kebijakan tersebut.

1. Mengembangkan Prosedur untuk implementasi kebijakan keamanan (*Develop procedures for applying security policies*)

   Prosedur keamanan menerapkan kebijakan keamanan. Prosedur menentukan konfigurasi, login, proses audit, dan pemeliharaan. Prosedur keamanan harus ditulis untuk pengguna akhir, administrator jaringan, dan administrator keamanan. Prosedur keamanan harus menentukan bagaimana menangani insiden yaitu, apa yang harus dilakukan dan siapa yang harus dihubungi jika intruksi terdeteksi.

   Prosedur keamanan dapat dikomunikasikan kepada pengguna dan administrator di instruktur dan kelas pelatihan mandiri.

2. Memelihara Keamanan (*Maintain security*)

   Keamanan harus dijaga dengan menjadwalkan audit independen berkala, membaca audit log, menangani 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.

4. Keamanan Infrastruktur

   Terdapat dua teknik pengamanan yang harus berjalan secara simultan, yaitu pengamanan fisik yang meliputi pengamanan mesin dan lokasi, serta pengamanan logik yang meliputi otentikasi, otorisasi, firewall, dan *intrusion detection system (IDS)*.

   Untuk pengembangan desain jaringan yang aman terdapat beberapa kriteria yang harus dipenuhi, yaitu:

   A. Keamanan Fisik (*Physical Security*)

      Keamanan fisik mengacu pada membatasi akses ke sumber daya jaringan utama dengan mempertahankan sumber daya di balik pintu yang terkunci dan dilindungi dari bencana alam dan buatan manusia.

Keamanan fisik dapat melindungi jaringan dari penyalahgunaan peralatan jaringan yang tidak disengaja oleh karyawan dan kontraktor yang tidak terlatih. Itu juga dapat melindungi jaringan dari peretas, pesaing, dan teroris mengganti peralatan konfigurasi.

B. Otentikasi (*Authentication*)

Otentikasi mengidentifikasi siapa yang meminta layanan jaringan. Istilah otentikasi biasanya merujuk pada mengautentikasi pengguna tetapi juga dapat merujuk pada mengotentikasi perangkat atau perangkat lunak proses.

Sebagian besar kebijakan keamanan menyatakan bahwa untuk mengakses jaringan dan layanannya, pengguna harus memasukkan ID login ID dan kata sandi yang diautentikasi oleh server keamanan. Untuk memaksimalkan keamanan, kata sandi satu kali (dinamis) dapat digunakan. Dengan sistem kata sandi satu kali, pengguna kata sandi selalu berubah.

Banyak sistem menggunakan otentikasi dua faktor, yang mengharuskan pengguna memiliki dua bukti identitas. Contohnya adalah sistem kontrol akses yang memerlukan kartu keamanan dan kata sandi. Dengan otentikasi dua faktor, kompromi dari satu faktor tidak mengarah ke kompromi dari sistem. Seorang penyerang bisa belajar kata sandi, tetapi kata sandi itu tidak berguna tanpa kartu keamanan. Sebaliknya, jika kartu keamanan dicuri, tidak dapat digunakan tanpa kata sandi.

C. Otorisasi (*Authorization*)

Otorisasi adalah apa yang dapat mereka lakukan setelah mereka mengakses sumber daya. Otorisasi memberikan hak istimewa untuk proses dan pengguna. Otorisasi memungkinkan administrator keamanan mengontrol bagian-bagian jaringan (misalnya, direktori dan file di server).

D. Akuntansi dan Audit (*Accounting & Auditing*)

Prosedur harus ditetapkan untuk mengumpulkan data aktivitas jaringan untuk selanjutnya dilakukan analisis keamanan jaringan dan untuk menanggapi insiden

keamanan, Mengumpulkan data adalah disebut akuntansi atau audit. Data yang dikumpulkan harus mencakup nama pengguna dan host untuk upaya masuk dan keluar, dan hak akses sebelumnya dan baru untuk perubahan hak akses. Setiap entri dalam log audit harus diberi cap waktu.

Proses audit sebaiknya tidak mengumpulkan kata sandi. Mengumpulkan kata sandi menciptakan potensi untuk pelanggaran keamanan jika catatan audit diakses secara tidak benar. Tidak benar juga kata sandi yang salah harus dikumpulkan. Kata sandi yang salah sering berbeda dari kata sandi yang valid hanya dengan satu karakter atau transposisi karakter.

E. Enkripsi Data (*Data Encryption*)

Enkripsi adalah proses yang mengacak data untuk melindunginya agar tidak dibaca oleh siapa pun kecuali penerima yang dituju. Perangkat enkripsi mengenkripsi data sebelum menempatkannya di jaringan. Perangkat dekripsi mendekripsi data sebelum meneruskannya ke aplikasi. Sebuah router, server, sistem akhir, atau perangkat khusus dapat bertindak sebagai enkripsi atau dekripsi alat. Data yang dienkripsi disebut data yang dienkripsi (atau hanya data yang dienkripsi). Data yang tidak dienkripsi disebut teks biasa atau teks jelas.

F. Pembatasan Paket (*Packet Filters*)

Filter paket dapat diatur pada router, firewall, dan server untuk menerima atau menolak paket dari alamat atau layanan tertentu. Filter paket menambah otentikasi dan otorisasi mekanisme. Mereka membantu melindungi sumber daya jaringan dari penggunaan yang tidak sah, pencurian, kehancuran, dan serangan DoS.

Kebijakan keamanan harus menyatakan apakah filter paket menerapkan satu atau yang lain dari kebijakan berikut:

1) *Deny* - tolak tipe paket tertentu dan terima semuanya
2) *Accept* - terima jenis paket tertentu dan tolak semua yang lain

G. Firewalls

Firewall adalah perangkat yang memberlakukan kebijakan keamanan di Internet batas antara dua atau lebih jaringan. Firewall dapat berupa router dengan ACL, *dedicated* alat perangkat keras, atau perangkat lunak yang berjalan pada PC atau sistem UNIX. *Firewall* adalah terutama penting pada batas antara jaringan perusahaan dan Internet. *Firewall* memiliki seperangkat aturan yang menentukan lalu lintas mana yang harus diizinkan atau ditolak.

H. Sistem Deteksi Intrusi dan Sistem Pencegahan Intrusi *(Intrusion Detection and Prevention Systems)*

Sistem deteksi intrusi (IDS) mendeteksi peristiwa berbahaya dan memberi tahu administrator, menggunakan email, paging, atau login kejadian. IDS juga dapat melakukan statistic dan analisis anomali. Beberapa perangkat IDS dapat melaporkan ke database pusat yang berkorelasi informasi dari beberapa sensor untuk memberi administrator pandangan keseluruhan waktu nyata keamanan jaringan. Sistem pencegahan intrusi (IPS) dapat secara dinamis memblokir lalu lintas dengan menambahkan aturan ke *firewall* atau dengan dikonfigurasi untuk memeriksa (dan menolak atau mengizinkan) lalu lintas saat memasuki *firewall*. IPS adalah IDS yang dapat mendeteksi dan mencegah serangan.

5. Fungsi dan Kategori Aktivitas Keamanan Informasi

Gambar 4.4.4.6. Fungsi dan Kategori Aktivitas Keamanan Informasi

Operasional Keamanan informasi berdasar kerangka kerja NIST Cybersecurity terdiri dari 5 (lima) domain yakni Identifikasi, Proteksi, Deteksi, Respon dan Pemulihan. Setiap domain memiliki kategori seperti gambar di 4.37. Operasional Keamanan Informasi didukung oleh SIstem Manajemen Keamanan Informasi (SMKI), penyelenggara Security Operation Center (SOC), dan CSIRT.

Bab IV

Penutup

Arsitektur SPBE Kabupaten Tegal disusun guna memberikan gambaran sementara kondisi implementasi TIK untuk layanan SPBE (Sistem Pemerintahan Berbasis Elektronik) di Pemerintah Kabupaten Tegal.

Arsitektur SPBE Kabupaten Tegal ini akan dijadikan sebagai landasan dalam implementasi layanan Sistem Pemerintahan Berbasis Elektronik yang sesuai bagi Pemerintah Kabupaten Tegal selama 5 (lima) tahun mendatang.

BUPATI TEGAL,

UMI AZIZAH