Dinas komunikasi dan Informatika
Kabupaten Natuna

DOKUMEN MANAJEMEN SPBE

Pekerjaan:

Pendampingan Monitoring
dan Evaluasi SPBE

DOKUMEN MANAJEMEN SPBE

PEKERJAAN PENDAMPINGAN MONITORING DAN EVALUASI SPBE

DINAS KOMUNIKASI DAN INFORMATIKA

KABUPATEN NATUNA

TAHUN 2024

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Implementasi SPBE yang efektif memerlukan dokumen manajemen yang komprehensif dan terstruktur, memastikan semua aspek dari perencanaan, pelaksanaan, hingga evaluasi berjalan sesuai dengan tujuan yang ditetapkan.

1.1 Latar Belakang

Kebijakan penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) telah ditetapkan sejak tahun 2018 berdasarkan Peraturan tahun 2018 Nomor 95 tentang Penyelenggaraan SPBE. Dalam rangka pelaksanaan lebih lanjut juga ditetapkan Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia, dan Peraturan Presiden Nomer 132 Tahun 2023 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional.

Mencermati dan memperhatikan dinamika pelaksanaan SPBE dilingkungan Pemerintah Kabupaten Natuna, serta permasalahan-permasalahan yang ada maka perlu dilakukan penguatan koordinasi dan sinergi antar instansi, untuk kesepahaman yang lebih baik tentang isu-isu krusial, menganalisis dan memahami tantang yang dihadapi, serta mendorong partisipasi semua pihak untuk kontribusi solusi efektif dan berkelanjutan terhadap masalah-masalah dalam pelaksanaan SPBE ini.

Sehubungan dengan hal tersebut maka dipandang perlu salah satu ruang lingkup pengaturan dalam pelaksanaan SPBE yang harus diformulasikan adalah Manajemen SPBE yang meliputi terkait manajemen resiko, Manajemen keamanan informasi, Manajemen data, Manajemen data, Manajemen aset TIK, Manajemen pengetahuan, Manajemen perubahan, dan Manajemen layanan SPBE Pemda yang harus diformulasikan secara tepat.

Dokumen Manajemen SPBE (Sistem Pemerintahan Berbasis Elektronik) merupakan panduan penting bagi instansi pemerintah dalam menyelenggarakan SPBE secara efektif, efisien, dan akuntabel. Dokumen ini memuat strategi, kebijakan, rencana, dan panduan yang harus dipedomani oleh seluruh pemangku kepentingan.

1.2 Maksud dan Tujuan

Penyusunan dokumen Manajemen SPBE (Sistem Pemerintahan Berbasis Elektronik) memiliki beberapa maksud penting, yaitu:

1. Menyelaraskan SPBE dengan Visi, Misi, dan Tujuan Organisasi
2. Memandu Pelaksanaan SPBE
3. Meningkatkan Akuntabilitas dan Transparansi
4. Mendukung Pemantauan dan Evaluasi SPBE
5. Mempermudah Audit SPBE

Adapun Tujuan utama penyusunan Dokumen Manajemen SPBE adalah untuk

- Memandu instansi pemerintah dalam menyelenggarakan SPBE secara efektif, efisien, dan akuntabel.
- Meningkatkan kualitas layanan publik melalui pemanfaatan TIK.
- Mewujudkan tata kelola pemerintahan yang baik.
- Meningkatkan transparansi dan akuntabilitas penyelenggaraan pemerintahan.

BAB II
PENDEKATAN DAN METODOLOGI PELAKSANAAN PEKERJAAN

2.1 Pendekatan Teknis

2.1.1 Tentang SPBE

SPBE merupakan singkatan dari Sistem Pemerintahan Berbasis Elektronik, Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE. Hal ini seperti yang tertuang pada Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. SPBE ditujukan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya. Tata kelola dan manajemen sistem pemerintahan berbasis elektronik secara nasional juga diperlukan untuk meningkatkan keterpaduan dan efisiensi sistem pemerintahan berbasis elektronik.

SPBE dilaksanakan dengan prinsip sebagai berikut :

a. Efektivitas, merupakan optimalisasi pemanfaatan sumber daya yang mendukung SPBE yang berhasil guna sesuai dengan kebutuhan.
b. Keterpaduan, merupakan pengintegrasian sumber daya yang mendukung SPBE.
c. Kesinambungan, merupakan keberlanjutan SPBE secara terencana, bertahap, dan terus menerus sesuai dengan perkembangannya.
d. Efisiensi, merupakan optimalisasi pemanfaatan sumber daya yang mendukung SPBE yang tepat guna
e. Akuntabilitas, merupakan kejelasan fungsi dan pertanggungjawaban dari SPBE.
f. Interoperabilitas, merupakan koordinasi dan kolabolasi antar Proses Bisnis dan antar sistem elektronik, dalam rangka pertukaran data, informasi, atau Layanan SPBE.
g. Keamanan, merupakan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan *(nonrepudiation)* sumber daya yang mendukung SPBE.

2.1.2 Regulasi SPBE Nasional

Upaya penerapan Sistem Pemerintahan Berbasis Elektronilk (SPBE) di instansi pemerintah saat ini di pandang belum berhasil, sehingga menimbulkan pemborosan anggaran. Hal itu terjadi antara lain disebabkan pembangunan SPBE bersifat parsial. Untuk itu instansi pemerintah, baik pusat maupun daerah, di dorong untuk dapat memperbaiki tata kelola

penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) guna mewujudkan keterpaduan dan efektivitas dalam penyelenggaraan pemerintahan.

Kehadiran Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) serta Peraturan Presiden (Perpres) Nomor 39 Tahun 2019 tentang Satu Data Indonesia merupakan babak baru bagi tata kelola atau manajemen pemerintahan di Indonesia. Berdasarkan kebijakan tersebut, seluruh instansi pemerintah wajib menerapkan SPBE atau yang lebih dikenal dengan e-government.

Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE bertujuan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel. Selain itu juga untuk mewujudkan pelayanan publik yang berkualitas dan terpercaya. Kebijakan tersebut juga diharapkan dapat meningkatkan keterpaduan dan efisiensi dalam pelaksanaan SPBE di dalam dan antar instansi pemerintah. Penerapan SPBE yang terpadu akan mentransformasi sistem pemerintahan, baik dari segi tata kelola pemerintahan, tata kelola aplikasi, dan infrastruktur, serta manajemen pelaksanaan dari kedua hal tersebut yang mengedepankan prinsip berbagi sumber daya, kolaborasi, dan integrasi antar instansi pemerintah.

Unsur-unsur SPBE sebagaimana tertuang dalam Pasal 4 Peraturan Presiden Nomor 95 tahun 2018 adalah sebagai berikut:

1. Arsitektur SPBE
   a. Arsitektur SPBE terdiri dari:
      - Arsitektur SPBE Nasional
      - Arsitektur SPBE Instansi Pusat dan
      - Arsitektur SPBE Pemerintah Daerah.
   b. Domain Arsitektur yang digambarkan terdiri dari:
      - Domain arsitektur Proses Bisnis;
      - Domain arsitektur data dan informasi;
      - Domain arsitektur Infrastruktur SPBE;
      - Domain arsitektur Aplikasi SPBE;
      - Domain arsitektur Keamanan SPBE; dan
      - Domain arsitektur Layanan SPBE.

Gambar 2. 1 Domain Arsitektur SPBE

2. Peta Rencana SPBE

   Peta Rencana SPBE memuat rancangan perencanaan untuk :

   a. Tata Kelola SPBE
   b. Manajemen SPBE
   c. Layanan SPBE
   d. Infrastruktur SPBE
   e. Aplikasi SPBE
   f. Keamanan SPBE dan
   g. Audit Teknologi Informasi dan Komunikasi

3. Rencana dan anggaran SPBE
4. Proses Bisnis
   a. Penyusunan Proses Bisnis bertujuan untuk memberikan pedoman dalam penggunaan data dan informasi serta penerapan Aplikasi SPBE, Keamanan SPBE, dan Layanan SPBE.
   b. Proses Bisnis yang saling terkait disusun secara terintegrasi untuk mendukung pembangunan atau pengembangan Aplikasi SPBE dan Layanan SPBE yang terintegrasi.
5. Data dan informasi
   a. Data dan informasi mencakup semua jenis data dan informasi yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah, dan/atau yang diperoleh dari masyarakat, pelaku usaha, dan/atau pihak lain.
   b. Penggunaan data dan informasi mengutamakan bagi pakai data dan informasi antar Instansi Pusat dan/atau Pemerintah Daerah dengan berdasarkan tujuan dan cakupan, penyediaan akses data dan informasi, dan pemenuhan standar interoperabilitas data dan informasi.
   c. Standar interoperabilitas data dan informasi ditetapkan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

d. Penyelenggaraan tata kelola data dan informasi antar Instansi Pusat dan/atau Pemerintah Daerah dikoordinasikan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional.

6. Infrastruktur SPBE
   a. Infrastruktur SPBE Nasional terdiri dari:
      - Pusat Data nasional;
      - Jaringan Intra pemerintah; dan
      - Sistem Penghubung Layanan pemerintah
   b. Penggunaan Infrastruktur SPBE Nasional bertujuan untuk meningkatkan efisiensi, keamanan, dan kemudahan integrasi dalam rangka memenuhi kebutuhan Infrastruktur SPBE bagi Instansi Pusat dan Pemerintah Daerah.
   c. Pembangunan dan pengembangan Infrastruktur SPBE Nasional harus didasarkan pada Arsitektur SPBE Nasional.
7. Aplikasi SPBE
   a. Aplikasi SPBE sebagaimana dimaksud terdiri atas :
      - Aplikasi Umum dan Aplikasi Khusus.
   b. Keterpaduan pembangunan dan pengembangan Aplikasi SPBE dikoordinasikan oleh menteri yang menyelenggarakan urusan pemerintahan
   c. Pembangunan dan pengembangan Aplikasi SPBE mengutamakan penggunaan kode sumber terbuka
   d. Dalam hal pembangunan dan pengembangan Aplikasi SPBE menggunakan kode sumber tertutup, Instansi Pusat dan Pemerintah Daerah harus mendapatkan pertimbangan dari menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika
   e. Aplikasi Umum ditetapkan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur Negara
   f. Pembangunan dan pengembangan Aplikasi Umum didasarkan pada Arsitektur SPBE Nasional.
   g. Setiap Instansi Pusat dan Pemerintah Daerah harus menggunakan Aplikasi Umum
   h. Dalam hal Instansi Pusat dan Pemerintah Daerah tidak menggunakan Aplikasi Umum, Instansi Pusat dan Pemerintah Daerah dapat menggunakan aplikasi sejenis dengan Aplikasi Umum.
   i. Telah mengoperasikan aplikasi sejenis sebelum Aplikasi Umum ditetapkan
   j. Melakukan kajian biaya dan manfaat terhadap penggunaan dan pengembangan aplikasi sejenis

k. Melakukan pengembangan aplikasi sejenis yang disesuaikan dengan Proses Bisnis dan fungsi pada Aplikasi Umum
l. Mendapatkan pertimbangan dari menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika
m. Instansi Pusat dan Pemerintah Daerah dapat melakukan pembangunan dan pengembangan Aplikasi Khusus
n. Pembangunan dan pengembangan Aplikasi Khusus sebagaimana dimaksud didasarkan pada Arsitektur SPBE Instansi Pusat dan Arsitektur SPBE Pemerintah Daerah masing-masing
o. Ketentuan lebih lanjut mengenai standar teknis dan cprosedur pembangunan dan pengembangan Aplikasi Khusus diatur dengan Peraturan Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

8. Keamanan SPBE
   a. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE
   b. Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan SPBE
   c. Dalam menerapkan Keamanan SPBE dan menyelesaikan permasalahan Keamanan SPBE, pimpinan Instansi Pusat dan kepala daerah dapat melakukan konsultasi dan atau koordinasi dengan kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber
   d. Penerapan Keamanan SPBE harus memenuhi standar teknis dan prosedur Keamanan SPBE. (Ketentuan lebih lanjut mengenai standar teknis dan prosedur Keamanan SPBE diatur dengan Peraturan Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber)
9. Layanan SPBE
   a. Layanan SPBE terdiri atas:
      - layanan administrasi pemerintahan berbasis elektronik dan
      - layanan publik berbasis elektronik.
   b. Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud merupakan Layanan SPBE yang mendukung tata laksana internal birokrasi dalam rangka meningkatkan kinerja dan akuntabillitas pemerintah di Instansi Pusat dan Pemerintah Daerah.
   c. Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud meliputi layanan yang mendukung kegiatan di bidang perencanaan, penganggaran,

keuangan, pengadaan barang dan jasa, kepegawaian, kearsipan, pengelolaan barang milik negara, pengawasan, akuntabilitas kinerja, dan layanan lain sesuai dengan kebutuhan internal birokrasi pemerintahan.

d. Layanan administrasi pemerintahan berbasis elektronik diterapkan dengan pembangunan dan pengembangan Aplikasi Umum.
e. Layanan publik berbasis elektronik sebagaimana dimaksud meliputi layanan yang mendukung kegiatan di sektor pendidikan, pengajaran, pekerjaan dan usaha, tempat tinggal, komunikasi dan informasi, lingkungan hidup, kesehatan, jaminan sosial, energi, perbankan, perhubungan, sumber daya alam, pariwisata, dan sektor strategis lainnya.
f. Layanan publik berbasis elektronik sebagaimana dimaksud dapat dikembangkan sesuai dengan kebutuhan pelayanan publik di Instansi Pusat dan Pemerintah Daerah.
g. Dalam hal layanan publik berbasis elektronik memerlukan Aplikasi Khusus, Instansi Pusat dan Pemerintah Daerah dapat melakukan pembangunan dan pengembangan Aplikasi Khusus.
h. Integrasi Layanan SPBE merupakan proses menghubungkan dan menyatukan beberapa Layanan SPBE ke dalam satu kesatuan alur kerja Layanan SPBE.
i. Instansi Pusat menerapkan integrasi Layanan SPBE didasarkan pada Arsitektur SPBE Instansi Pusat.
j. Pemerintah Daerah menerapkan integrasi Layanan SPBE didasarkan pada Arsitektur SPBE Pemerintah Daerah.
k. Integrasi Layanan SPBE antar Instansi Pusat dan/atau Pemerintah Daerah dikoordinasikan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.

2.1.3 Manajemen SPBE Nasional

Adapun aspek manajemen yang diatur dalam regulasi SPBE ini melingkupi praktek manajemen sebagai berikut :

1. Manajemen risiko;
   a. Manajemen risiko sebagaimana dimaksud bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam SPBE.
   b. Manajemen risiko dilakukan melalui serangkaian proses identifikasi, analisis, pengendalian, pemantauan, dan evaluasi terhadap risiko dalam SPBE.
   c. Manajemen risiko sebagaimana dimaksud dilaksanakan berdasarkan pedoman manajemen risiko SPBE.
2. Manajemen keamanan informasi;

a. Manajemen keamanan informasi sebagaimana dimaksud bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi.
b. Manajemen keamanan informasi dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE.
c. Manajemen keamanan informasi sebagaimana dilaksanakan berdasarkan pedoman manajemen keamanan informasi SPBE.

3. Manajemen data;
   a. Manajemen data bertujuan untuk menjamin terwujudnya data yang akurat, mutakhir,terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan nasional.
   b. Manajemen data dilakukan melalui serangkaian proses pengelolaan arsitektur data, data induk, data referensi, basis data, dan kualitas data.
   c. Manajemen data sebagaimana dimaksud dilaksanakan berdasarkan pedoman manajemen data SPBE.
   d. Dalam pelaksanaan manajemen data, pimpinan Instansi Pusat dan kepala daerah berkoordinasi dan dapat melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional.
4. Manajemen aset teknologi informasi dan komunikasi;
   a. Manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud huruf d bertujuan untuk menjamin ketersediaan dan optimalisasi pemanfaatan aset teknologi informasi dan komunikasi dalam SPBE
   b. Manajemen aset teknologi informasi dan komunikasi dilakukan melalui serangkaian proses perencanaan, pengadaan, pengelolaan, dan penghapusan perangkat keras dan perangkat lunak yang digunakan dalam SPBE.
   c. Manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud dilaksanakan berdasarkan pedoman manajemen aset teknologi informasi dan komunikasi SPBE.
   d. Dalam pelaksanaan manajemen aset teknologi informasi dan komunikasi, pimpinan Instansi Pusat dan kepala daerah berkoordinasi dan dapat melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

5. Manajemen sumber daya manusia;
    a. Manajemen sumber daya manusia sebagaimana dimaksud bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE.
    b. Manajemen sumber daya manusia dilakukan melalui serangkaian proses perencanaan, pengembangan, pembinaan, dan pendayagunaan sumber daya manusia dalam SPBE.
    c. Manajemen sumber daya manusia memastikan ketersediaan dan kompetensi sumber daya manusia untuk pelaksanaan Tata Kelola SPBE dan Manajemen SPBE.
    d. Manajemen sumber daya manusia sebagaimana dimaksud dilaksanakan berdasarkan pedoman manajemen sumber daya manusia SPBE.
    e. Dalam pelaksanaan manajemen sumber daya manusia, pimpinan Instansi Pusat dan kepala daerah berkoordinasi dan dapat melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.
6. Manajemen pengetahuan;
    a. Manajemen pengetahuan sebagaimana dimaksud bertujuan untuk meningkatkan kualitas Layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE.
    b. Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam SPBE.
    c. Manajemen pengetahuan sebagaimana dimaksud dilaksanakan berdasarkan pedoman manajemen pengetahuan SPBE.
    d. Dalam pelaksanaan manajemen pengetahuan, pimpinan Instansi Pusat dan kepala daerah berkoordinasi dan dapat melakukan konsultasi dengan kepala lembaga pemerintah non kementerian yang menyelenggarakan tugas pemerintahan di bidang pengkajian dan penerapan teknologi.
7. Manajemen perubahan;
    a. Manajemen perubahan sebagaimana dimaksud bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE melalui pengendalian perubahan yang terjadi dalam SPBE.
    b. Manajemen perubahan dilakukan melalui serangkaian proses perencanaan, analisis, pengembangan, implementasi, pemantauan dan evaluasi terhadap perubahan SPBE.
    c. Manajemen perubahan sebagaimana dimaksud dilaksanakan berdasarkan pedoman manajemen perubahan SPBE.

d. Dalam pelaksanaan manajemen perubahan, pimpinan Instansi Pusat dan kepala daerah berkoordinasi dan dapat melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.

8. Manajemen Layanan SPBE
   a. Manajemen Layanan SPBE sebagaimana dimaksud bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE kepada Pengguna SPBE.
   b. Manajemen Layanan SPBE dilakukan melalui serangkaian proses pelayanan Pengguna SPBE, pengoperasian Layanan SPBE, dan pengelolaan Aplikasi SPBE.
   c. Pelayanan Pengguna SPBE sebagaimana dimaksud pada ayat 21 merupakan kegiatan pelayanan terhadap keluhan, gangguan, masalah, permintaan, dan perubahan Layanan SPBE dari Pengguna SPBE.
   d. Pengoperasian Layanan SPBE sebagaimana dimaksud pada ayat 21 merupakan kegiatan pendayagunaan dan pemeliharaan Infrastruktur SPBE dan Aplikasi SPBE.
   e. Pengelolaan Aplikasi SPBE sebagaimana dimaksud merupakan kegiatan pembangunan dan pengembangan aplikasi yang berpedoman pada metodologi pembangunan dan pengembangan Aplikasi SPBE.
   f. Manajemen Layanan SPBE sebagaimana dimaksud dilaksanakan berdasarkan pedoman manajemen Layanan SPBE.
   g. Dalam pelaksanaan manajemen Layanan SPBE, pimpinan Instansi Pusat dan kepala daerah berkoordinasi dan dapat melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

Pelaksanaan Manajemen SPBE Nasional ini mempertimbangkan hal-hal berikut ini :

1. Instansi Pusat dan Pemerintah Daerah melaksanakan Manajemen SPBE berpedoman pada Standar Nasional Indonesia.
2. Dalam hal Standar Nasional Indonesia sebagaimana dimaksud belum tersedia, pelaksanaan Manajemen SPBE dapat berpedoman pada standar internasional.

Penyelenggaraan SPBE di setiap daerah diatur sebagai berikut :

1. Setiap kepala daerah mempunyai tugas melakukan koordinasi dan menetapkan kebijakan SPBE di Pemerintah Daerah.
2. Setiap kepala daerah menetapkan koordinator SPBE Pemerintah Daerah.
3. Koordinator SPBE Pemerintah Daerah sebagaimana dimaksud mempunyai tugas melakukan koordinasi dan penerapan kebijakan SPBE di Pemerintah Daerah.

4. Koordinator SPBE Pemerintah Daerah dijabat oleh sekretaris daerah

2.1.4 Rencana Induk SPBE Nasional

Rencana Induk SPBE nasional tertuang dalam Peraturan Presiden No 95 Tahun 2018 yang menetapkan rencana strategis untuk kurun waktu 2019 – 2025.

Visi SPBE adalah "Terwujudnya sistem pemerintahan berbasis elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan publik yang berkinerja tinggi".

Adapun Misi dari SPBE yang ditetapkan adalah sebagai berikut:

1. Melakukan penataan dan penguatan organisasi dan tata kelola sistem pemerintahan berbasis elektronik yang terpadu;
2. Mengembangkan pelayanan publik berbasis elektronik yang terpadu, menyeluruh, dan menjangkau masyarakat luas;
3. Membangun fondasi teknologi informasi dan komunikasi yang terintegrasi, aman, dan andal; dan
4. Membangun SDM yang kompeten dan inovatif berbasis teknologi informasi dan komunikasi.

Adapun tujuan dari SPBE adalah sebagai berikut:

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.

Sasaran yang ingin dicapai adalah:

1. Terwujudnya tata kelola dan manajemen SPBE yang efektif dan efisien;
2. Terwujudnya layanan SPBE yang terpadu dan berorientasi kepada pengguna;
3. Terselenggaranya infrastruktur SPBE yang terintegrasi; dan
4. Meningkatnya kapasitas SDM SPBE.

Rencana strategis memuat inisiatif strategis secara garis besar adalah :

A. Tata Kelola SPBE
    1. Pembangunan Arsitektur SPBE
    2. Pembentukan dan Penguatan Kapasitas Tim Koordinasi SPBE

3. Penguatan Kebijakan SPBE
4. Evaluasi Penerapan Kebijakan SPBE

B. Layanan SPBE
1. Survei Pengguna SPBE
2. Portal Pelayanan Publik yang terintegrasi
3. Portal Pelayanan Administrasi Pemerintahan Yang Terintegrasi
4. Penyelenggaraan Manajemen Layanan

C. Teknologi Informasi dan Komunikasi
1. Pusat Data Nasional
2. Penyediaan Jaringan Intra Pemerintah
3. Penyediaan Sistem Penghubung Layanan Nasional Pemerintah
4. Penyediaan Akses Berkualitas Terhadap Layanan SPBE di Seluruh Wilayah Indonesia
5. Pengembangan Layanan Berbasis Teknologi Layanan berbagi Pakai
6. Pembangunan Portal Data Nasional
7. Pembangunan Sistem Keamanan Informasi Nasional
8. Pengembangan Teknologi Kecerdasan Buatan untuk Pengambilan Keputusan Yang Cepat Dan Akurat

D. Sumber Daya Manusia SPBE
1. Promosi Literasi SPBE
2. Peningkatan Kapasitas ASN Penyelenggara SPBE
3. Pembangunan Forum Kolaborasi SPBE antara Pemerintah dan Non Pemerintah

Tabel 2. 1 Inisiatif Strategis Pengembangan SPBE Nasional

No	Inisiatif Strategis	Keluaran	Target Waktu
A	**Tata Kelola SPBE**		
1	Pembangunan Arsitektur SPBE	Arsitektur SPBE Pemerintah Daerah	2020 – 2021
2	Pembentukan dan Penguatan Kapasitas Tim Koordinasi SPBE	Tim Koordinasi SPBE Daerah	2018 – 2019
3	Penguatan Kebijakan SPBE	Kebijakan Mikro SPBE	2019 – 2025
4	Evaluasi Penerapan Kebijakan SPBE	• Evaluasi SPBE Instansi Pemerintah Daerah • Audit TIK	2018 – 2025
B	**Layanan SPBE**		
1	Survei Pengguna SPBE	Survei Kebutuhan dan Kepuasan Pengguna	2019 – 2025

No	Inisiatif Strategis	Keluaran	Target Waktu
2	Portal Pelayanan Publik yang terintegrasi	• Integrasi Proses Bisnis Pelayanan Publik Pemerintah Daerah • Portal Pelayanan Publik Pemerintah Daerah	2018 - 2025
3	Portal Pelayanan Administrasi Pemerintahan yang terintegrasi	• Integrasi Perencanaan, Penganggaran dan Penganggaran Barang dan Jasa • Integrasi Kepegawaian • Integrasi Kearsipan • Intergasi Pengaduan Publik • Portal Pelayanan • Administrasi Pemerintahan	2018 – 2020
4	Penyelenggaran Manajemen Layanan	• Manajemen Layanan SPBE • Portal Pusat Layanan	2019 - 2021
C	**Teknologi Informasi**		
1	Penyediaan Pusat Data Nasional	Pusat Data Nasional	2018 – 2022
2	Penyediaan Jaringan Intra Pemerintah	Jaringan Intra Pemerintah Daerah Kabupaten/Kota/ Kabupaten	2018 – 2022
3	Penyediaan Sistem Penghubung Layanan	Sistem Penghubung Layanan Pemerintah	2018 – 2022
4	Penyediaan Akses Berkualitas Terhadap Layanan SPBE di seluruh wilayah Indonesia	Jaringan Pita Lebar Berkualitas	2018 – 2025
5	Pengembangan Layanan Berbasis Teknologi Layanan Berbagi Pakai	Cloud Service	2018 – 2025
6	Pembangunan Portal Data Nasional	• Dukungan TIK Portal Data Nasional • Integrasi Data dan Pengelolaan Portal Data Nasional	2019 - 2025
7	Pembangunan Sistem Keamanan Informasi Nasional	• Manajemen Keamanan Informasi • Teknoogi Keamanan Informasi • Budaya Keamanan Informasi	2018 – 2020
8	Pengembangan Teknologi Kecerdasan Buatan untuk Pengambilan Keputusan Yang Cepat dan Akurat	• Kajian Teknologi Kecerdasan Buatan • Penerapan Big Data Pemerintah	2019 – 2025
D	**Sumber Daya Manusia SPBE**		
1	Peningkatan Kapasitas ASN Penyelenggara SPBE	• Standar Kompetensi Teknis SPBE • Pelatihan dan Sertifikasi Kompetensi SPE	2018 – 2022

No	Inisiatif Strategis	Keluaran	Target Waktu
2	Pembangunan Forum Kolaborasi SPBE antara Pemerintah dan Non Pemerintah	Forum Kolaborasi SPBE	2019 – 2020

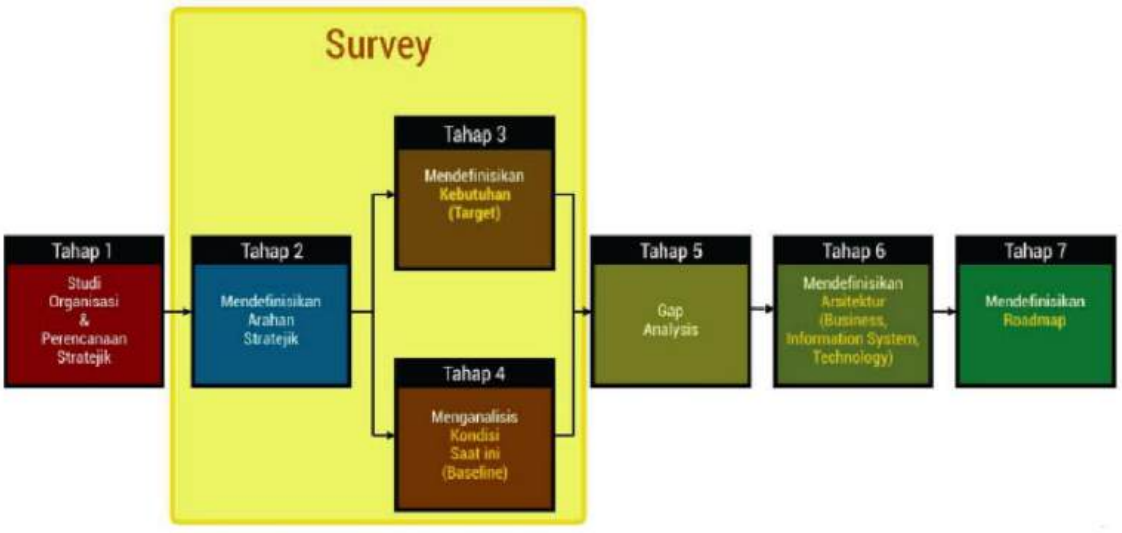
2.2 Metodologi & Tahapan

Metodologi yang digunakan dalam penyusunan Tata Kelola dan Manajemen SPBE di Pemerintah Daerah mengadopsi referensi dari Arsitektur dan Peta Rencana Induk SPBE Nasional. Selain itu juga untuk perencanaan program kerja SPBE mengadopsi lingkup yang ada didalam lingkup SPBE yang meliputi: Proses Bisnis, Data dan Informasi, Infrastruktur SPBE, Aplikasi SPBE, Keamanan SPBE dan Layanan SPBE.

Kegiatan ini dilaksanakan dengan menerapkan metode :

- Studi Pustaka (literature review) untuk referensi metodologi, perangkat pengumpulan data, pengukuran, dan analisisnya.
- Survei online
- Observasi bukti pendukung (dokumen, peralatan, dan lain-lain)
- Wawancara dan Questionnaire
- Focus Group Discussion dan Desk Evaluation untuk konfirmasi dan rekomendasi akhir.

Mengadopsi metode penyusunan tata kelola dan penyusunan arsitektur dari teori diatas, tahapan pekerjaan yang digunakan dalam penyusunan Rencana Induk dan Arsitektur adalah sebagai berikut:



Gambar 2. 2 Tahapan Pekerjaan dalam Penyusunan Tata Kelola dan Manajemen SPBE

Berikut uraian metodologi yang akan digunakan dalam melaksanakan penyusunan Tata Kelola dan Manajemen SPBE di Pemerintah Daerah.

1. **Tahap 1 – Studi Organisasi dan Perencanaan Strategik**

   Tahap pertama yang dilakukan adalah mempelajari profil organisasi, yang mencakup visi, misi, dan nilai yang dicanangkan organisasi, sehingga diketahui arah dan target utama/prioritas organisasi dalam melakukan aktivitas sehari-hari, serta proses bisnis organisasi. Agar tingkat pencapaian visi dan misi dapat tercapai dan dimonitor, maka sudah seharusnya apabila suatu organisasi memiliki objektif dan indikator bisnis sebagai tolok ukur. Dalam hal ini, setidaknya terdapat dua peranan teknologi informasi yang penting, yaitu sebagai pemicu (*driver*) supaya dapat mencapai objektif yang dicanangkan, dan sebagai alat bantu untuk melihat kinerja organisasi melalui pengumpulan dan penyampaian informasi yang berkaitan dengan indikator bisnis.

2. **Tahap 2 – Mendefinisikan Arahan Strategik**

   Apabila hasil studi organisasi telah diketahui, maka dapat dilakukan perencanaan strategik tujuan. Aktivitas yang dilakukan diproses ini adalah mengadakan kajian terhadap hubungan organisasi dengan seluruh *stakeholder*-nya. Pada dasarnya, hasil/output dari kajian ini adalah definisi tentang peranan teknologi/sistem informasi yang sesuai dengan kebutuhan operasional organisasi.

Tabel 2. 2 Tahap 1 & 2

Kegiatan Tahap 1 & 2	Hasil
Analisis Internal: Arahan Strategis Organisasi	Arahan Strategis Organisasi
Analisis Eksternal Organisasi	Hasil Analisis Eksternal Organisasi
Penyelarasan Organisasi dan TI	Hasil penyelarasan TI terhadap kebutuhan organisasi
IT Strategy and Goals	Kebutuhan TI untuk mendukung organisasi

Tabel 2. 3 Tahap 3 & 4

Kegiatan Tahap 3 & 4	Keluaran
Asesmen kebutuhan proses bisinis dan tata kelola eksisting TIK	Hasil Asesmen proses bisinis dan tata kelola existing TIK
Asesmen kondisi eksisting infrastruktur dan keamanan TI	Hasil Asesmen kondisi eksisting infrastruktur dan keamanan TI

3. Tahap 5 – Gap Analysis SPBE

Gap Analysis SPBE adalah tahapan untuk menganalisa hasil olahan data-data dari analisa hasil data survei, sistem yang sudah ada, dibandingkan dengan kebutuhan kedepannya, sehingga akan nampak kesenjangan yang nantinya hal tersebut menjadi dasar untuk program kerja dan peta rencana pengembangan SPBE.

Tabel 2. 4 Tahap 5

Kegiatan Tahap 5	Hasil
Analisis Kesenjangan Proses Bisnis	Hasil Analisis Kesenjangan Proses Bisnis
Analisis Kesenjangan Data dan Informasi	Hasil Analisis Kesenjangan Data dan Informasi
Analisis Kesenjangan Infrastruktur	Hasil Analisis Kesenjangan Infrastruktur
Analisis Kesenjangan Aplikasi	Hasil Analisis Kesenjangan Aplikasi
Analisis Kesenjangan Keamanan	Hasil Analisis Kesenjangan Keamanan
Analisis Kesenjangan Layanan SPBE	Hasil Analisis Kesenjangan Layanan SPBE

4. Tahap 6 – Perumusan Arsitektur

Dalam tahap ini dilakukan perumusan arsitektur SPBE sebagai bagian dari perencanaan Sistem Pemerintahan Berbasis Elektronik dengan mengacu pada referensi arsitektur SPBE nasional. Selanjutnya merumuskan proses rutin penerapan, pemeliharaan, dan pengembangan sistem yang dilakukan bersamaan dengan dieksekusinya sejumlah program kerja, sehingga diperlukan strategi dan skenario yang jelas dalam menggabungkan kedua jenis aktivitas dengan basis yang berbeda tersebut. Profil sumber daya manusia dan struktur organisasi akan menjadi penentu tipe pengguna (user) dan karakteristik hak akses yang diperkenankan. Selain itu juga dilakukan perumusan manajemen tata kelola dan tata kelola (*governance*) yang efektif, efisien, dan terkontrol untuk menjalankan aktivitas berbasis TIK serta mengelola aspek-aspek teknologi informasi yang akan dibangun. Salah satu hal yang harus dilakukan adalah menentukan sebuah tim yang bertanggung jawab untuk melakukan sejumlah proses penerapan dan pemeliharaan teknologi informasi yang dimiliki organisasi (people – process – technology). Keluaran yang dihasilkan pada tahap ini akan sangat menentukan keberhasilan eksekusi dari rencana pengembangan teknologi informasi agar memberikan nilai sesuai dengan harapan organisasi.

Tabel 2. 5 Tahap 6

Kegiatan Tahap 6	Hasil
Desain Arsitektur Tata Kelola SPBE	Arsitektur Tata Kelola SPBE
Desain Arsitektur Manajemen SPBE	Arsitektur Manajemen SPBE
Penyusunan Penyelenggara SPBE	Organisasi dan personel yang bertanggung jawab atas penyelenggaraan SPBE

5. Tahap 7 – Mendefinisikan Peta Rencana SPBE

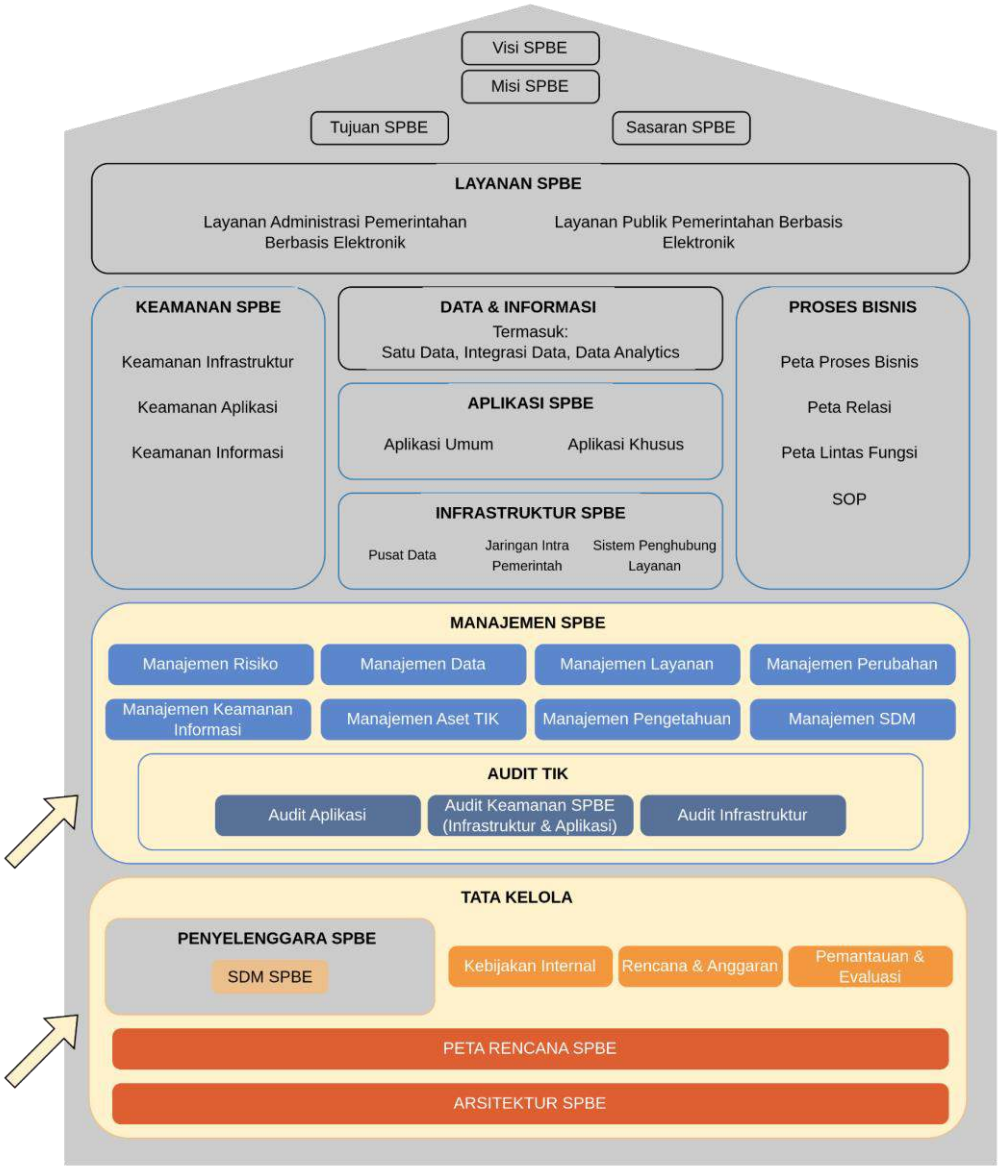
Tahap ini bertujuan untuk mengidentifikasi tema prioritas untuk peningkatan SPBE setiap tahun. Tema prioritas dapat ditentukan dengan mempertimbangkan strategi prioritas dan kondisi SPBE yang ada saat ini. Dengan memaparkan peta rencana spbe yang mencakup beberapa domain, yaitu domain tata kelola SPBE, manajemen SPBE, proses bisnis, data dan informasi serta layanan, aplikasi SPBE, Infrastruktur SPBE, Keamanan SPBE, dan Audit TIK.

Tabel 2. 6 Tahap 7

Kegiatan 7	Keluaran
Penyusunan Jadwal Pelaksanaan SPBE	Jadwal Pelaksanaan SPBE
Penyusunan Program SPBE	Program SPBE

BAB III
TATA KELOLA DAN MANAJEMEN SERTA PENYELENGARA SPBE

Berdasarkan Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018, untuk mencapai SPBE yang terpadu diperlukan Rencana Induk SPBE Nasional yang disusun dengan memperhatikan arah kebijakan, strategi, dan inisiatif pada bidang tata kelola SPBE, layanan SPBE, TIK, dan SDM. Tata kelola SPBE diarahkan untuk melakukan perbaikan dengan memperkuat kapasitas pengelolaan, sistem koordinasi pelaksanaan SPBE dan kebijakan SPBE untuk mewujudkan SPBE yang terpadu dan menyeluruh. Dalam Penyusunan Tata Kelola dan Manajemen SPBE di Pemerintah Daerah berfokus pada domain kebijakan internal SPBE, domain tata kelola SPBE dan domain manajemen SPBE sebagaimana digambarkan berikut:



Gambar 3. 1 Keterhubungan Tata Kelola, Manajemen, dan Penyelenggara dengan Arsitektur SPBE

3.1 Penjelasan Tata Kelola dan Manajemen, serta Penyelenggara SPBE

Tata kelola SPBE sendiri merupakan kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu. Perlunya melakukan penataan dan penguatan organisasi dan tata kelola sistem pemerintahan berbasis elektronik yang terpadu agar sesuai dengan sasaran SPBE yang pertama yaitu terwujudnya tata kelola dan manajemen SPBE yang efektif dan efisien.

Manajemen SPBE merupakan serangkaian proses untuk mewujudkan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas. SPBE yang efektif, efisien, dan berkesinambungan dapat mendukung penyelenggaraan pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya.

Penyelenggara SPBE yaitu Pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada lembaga pemerintah, aparatur sipil negara, pelaku bisnis, masyarakat, dan pihak lainnya. Selain itu perlunya peningkatan ASN penyelenggara SPBE karena kualitas layanan SPBE ditentukan oleh kapasitas ASN. Peningkatan kapasitas ASN pelaksana SPBE dapat dilakukan antara lain melalui pengembangan pola rekruitmen, pengembangan standar kompetensi, pengembangan pola karir pegawai ASN, pengembangan pola remunerasi dan pengembangan kompetensi teknis. Untuk terwujudnya tata kelola SPBE yang efektif dan efisien diperlukan perbaikan tata kelola dengan pembentukan tim koordinasi SPBE tingkat nasional, di Instansi Pusat, dan di Pemerintah Daerah, pembangunan arsitektur SPBE. Tujuan dari arsitektur SPBE adalah memberikan arahan pada saat integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan pengamanan SPBE untuk mewujudkan layanan SPBE yang terpadu. Arsitektur SPBE Administrasi Daerah yang disusun oleh masing-masing pemerintah daerah dan digunakan sebagai panduan untuk melakukan integrasi SPBE di masing-masing Pemerintah Daerah.

3.2 Tata Kelola SPBE

Tata kelola SPBE di pemerintah daerah merupakan kerangka kerja yang memastikan terlaksananya peraturan, pengarahan dan pengendalian dalam penerapan SPBE secara terpadu. Tata kelola SPBE di pemerintah daerah bertujuan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya.

Tata kelola SPBE di pemerintah daerah meliputi aspek-aspek berikut:

- Kebijakan SPBE
- Pembentukan unit kerja SPBE
- Perencanaan SPBE
- Pembangunan SPBE
- Pemeliharaan dan pengembangan SPBE
- Penggunaan SPBE
- Penilaian SPBE

Kebijakan SPBE

Kebijakan SPBE merupakan dasar bagi pelaksanaan SPBE di pemerintah daerah. Kebijakan SPBE harus disusun secara komprehensif dan terintegrasi dengan kebijakan-kebijakan lainnya di pemerintah daerah. Kebijakan SPBE harus mencakup aspek-aspek berikut:

- Visi, misi, dan tujuan SPBE
- Sasaran dan strategi SPBE
- Prinsip-prinsip SPBE
- Kerangka kerja SPBE
- Proses penerapan SPBE

Pembentukan unit kerja SPBE

Pembentukan unit kerja SPBE merupakan hal penting untuk mengkoordinasikan dan melaksanakan kegiatan-kegiatan SPBE. Unit kerja SPBE dapat dibentuk di tingkat provinsi, kabupaten/kota, atau kecamatan. Unit kerja SPBE dapat terdiri dari unsur pemerintah daerah, akademisi, atau praktisi.

Perencanaan SPBE

Perencanaan SPBE merupakan proses penyusunan rencana SPBE yang meliputi visi, misi, tujuan, sasaran, dan strategi SPBE. Rencana SPBE harus disusun secara terukur, realistis, dan dapat dicapai.

Pembangunan SPBE

Pembangunan SPBE merupakan proses pengadaan, implementasi, dan pengelolaan sistem dan infrastruktur SPBE. Pembangunan SPBE harus dilakukan secara terencana, bertahap, dan terukur.

Pemeliharaan dan pengembangan SPBE

Pemeliharaan dan pengembangan SPBE merupakan proses untuk menjaga agar sistem dan infrastruktur SPBE tetap berfungsi dengan baik dan sesuai dengan kebutuhan. Pemeliharaan dan pengembangan SPBE harus dilakukan secara berkelanjutan.

Penggunaan SPBE

Penggunaan SPBE merupakan proses pemanfaatan sistem dan infrastruktur SPBE untuk penyelenggaraan pemerintahan dan pelayanan publik. Penggunaan SPBE harus dilakukan secara efektif dan efisien.

Penilaian SPBE

Penilaian SPBE merupakan proses untuk mengukur tingkat keberhasilan pelaksanaan SPBE. Penilaian SPBE dapat dilakukan secara internal atau eksternal.

Penyelenggaraan tata kelola SPBE di pemerintah daerah harus dilaksanakan secara terintegrasi dan berkelanjutan. Hal ini penting untuk memastikan bahwa SPBE dapat memberikan manfaat yang optimal bagi penyelenggaraan pemerintahan dan pelayanan publik.

Berikut adalah beberapa contoh tata kelola SPBE yang dapat dilaksanakan di pemerintah daerah:

- Pembentukan Tim Koordinasi SPBE
- Pengembangan kebijakan SPBE
- Penyelenggaraan pelatihan dan sosialisasi SPBE
- Pelaksanaan audit SPBE

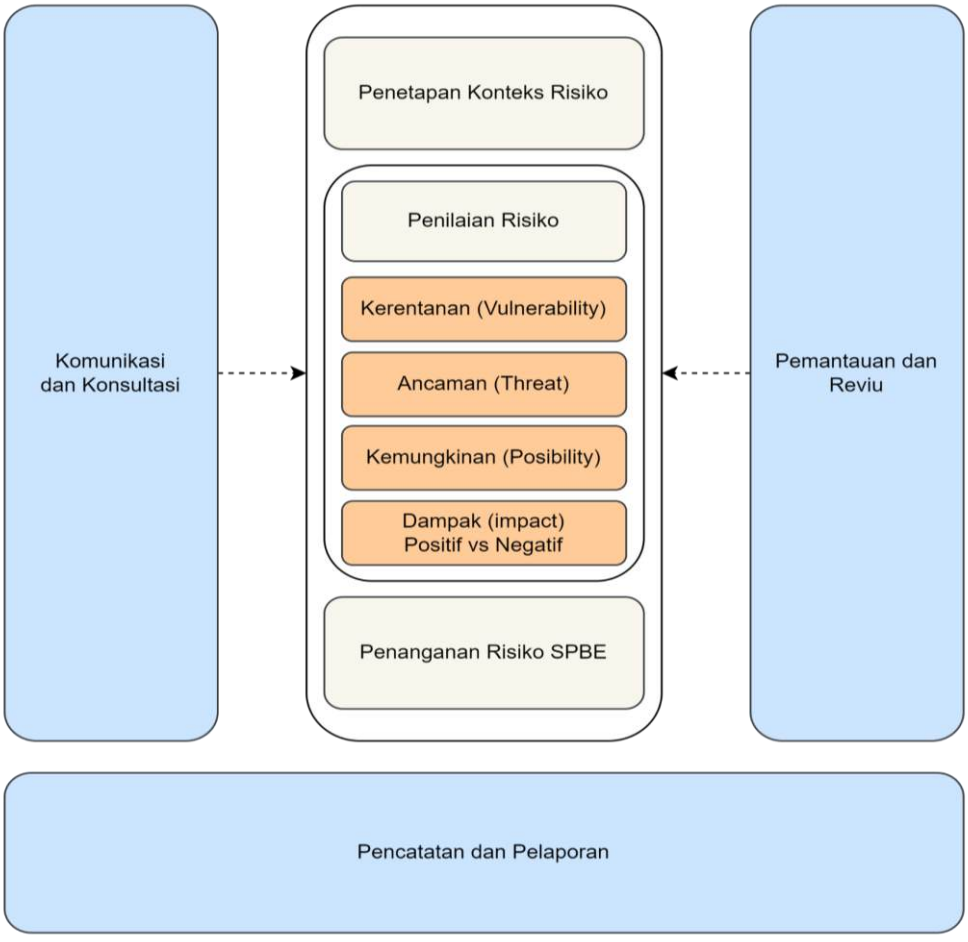
Pembentukan Tim Koordinasi SPBE dapat membantu pemerintah daerah untuk mengkoordinasikan dan melaksanakan kegiatan-kegiatan SPBE. Pengembangan kebijakan SPBE dapat membantu pemerintah daerah untuk menetapkan arah dan tujuan pelaksanaan SPBE. Penyelenggaraan pelatihan dan sosialisasi SPBE dapat membantu meningkatkan pemahaman dan keterampilan aparatur sipil negara (ASN) dalam penggunaan SPBE. Pelaksanaan audit SPBE dapat membantu pemerintah daerah untuk mengukur tingkat kematangan SPBE dan mengidentifikasi area-area yang perlu ditingkatkan.

Pemerintah daerah dapat mengadaptasi contoh-contoh tersebut sesuai dengan kebutuhan dan kondisi masing-masing daerah.

3.3 Manajemen SPBE

Manajemen SPBE merupakan serangkaian proses untuk mewujudkan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas. SPBE yang efektif, efisien, dan berkesinambungan dapat mendukung penyelenggaraan pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya. Manajemen SPBE meliputi 8 area kelompok, yaitu:

- **Manajemen Risiko**



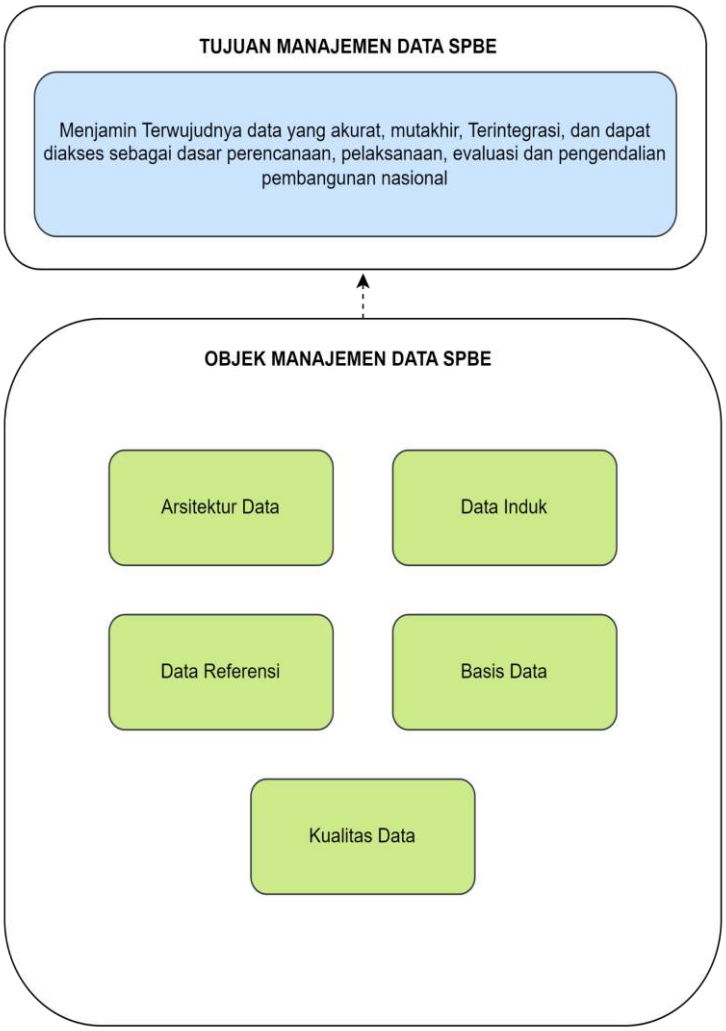
Gambar 3. 2 Diagram Proses Manajemen Risiko

Gambar diatas menunjukkan diagram proses manajemen risiko. Diagram tersebut menunjukkan langkah-langkah proses manajemen risiko, yang terdiri dari:

Tabel 3. 1 Proses Manajemen Risiko

Proses Manajemen Risiko	
Penetapan konteks risiko	Langkah ini dilakukan untuk menentukan ruang lingkup, konteks, dan kriteria penerapan manajemen risiko. Ruang lingkup menentukan aspek-aspek yang akan dipertimbangkan dalam proses manajemen risiko, sedangkan konteks menentukan faktor-faktor internal dan eksternal yang dapat mempengaruhi risiko. Kriteria penerapan manajemen risiko digunakan untuk menentukan tingkat risiko yang perlu ditangani
Identifikasi risiko	Langkah ini dilakukan untuk mengidentifikasi semua risiko yang mungkin terjadi, baik risiko positif maupun risiko negatif. Risiko positif adalah risiko yang dapat memberikan manfaat bagi organisasi, sedangkan risiko negatif adalah risiko yang dapat menimbulkan kerugian bagi organisasi
Analisis Risiko	Langkah ini dilakukan untuk menilai setiap risiko yang telah diidentifikasi berdasarkan kemungkinan dan dampak terjadinya. Kemungkinan adalah ukuran seberapa sering risiko tersebut diperkirakan akan terjadi, sedangkan dampak adalah ukuran seberapa besar kerugian yang mungkin ditimbulkan oleh risiko tersebut
Evaluasi Risiko	Langkah ini dilakukan untuk menentukan tingkat risiko yang dihadapi organisasi. Tingkat risiko ditentukan berdasarkan hasil analisis risiko
Penanganan Risiko	Langkah ini dilakukan untuk mengurangi atau menghilangkan risiko yang telah diidentifikasi. Penanganan risiko dapat dilakukan dengan berbagai cara, seperti : ▪ Menghindari risiko ▪ Mengurangi kemungkinan terjadinya risiko ▪ Mengurangi dampak risiko ▪ Menerima risiko
Pemantauan dan Review	Langkah ini dilakukan untuk memantau dan mengevaluasi efektivitas proses manajemen risiko. Monitoring dilakukan untuk memastikan bahwa risiko tetap terkendali, sedangkan review dilakukan untuk menilai apakah proses manajemen risiko perlu diperbaiki

- **Manajemen Data**



Gambar 3. 3 Diagram Tujuan Manajemen Data SPBE

Gambar diatas menunjukkan diagram tujuan manajemen data SPBE. Diagram tersebut menunjukkan bahwa tujuan manajemen data SPBE adalah untuk memastikan terwujudnya data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan nasional.

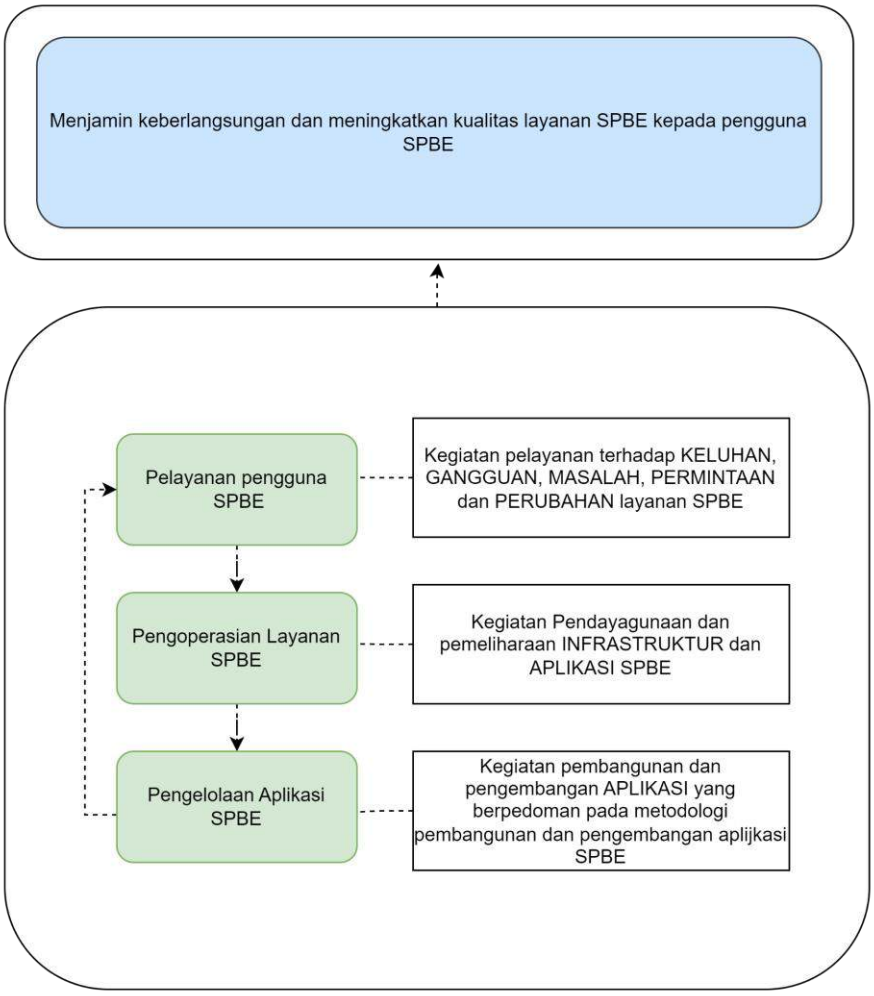
Tabel 3. 2 Tujuan Manajemen Data SPBE

Tujuan Manajemen Data SPBE	
Akurat	Data yang akurat diperlukan untuk memastikan bahwa keputusan yang dibuat berdasarkan data tersebut adalah tepat
Mutakhir	Data yang mutakhir diperlukan untuk memastikan bahwa keputusan yang dibuat berdasarkan data tersebut adalah relevan dengan kondisi terkini
Terintegrasi	Data yang terintegrasi diperlukan untuk memastikan bahwa data dapat digunakan secara efektif untuk berbagai tujuan
Dapat diakses	Data yang dapat diakses diperlukan untuk memastikan bahwa data dapat digunakan oleh semua pihak yang membutuhkan

Tabel 3. 3 Objek Manajemen Data SPBE

Objek Manajemen Data SPBE	
Arsitektur	Kerangka kerja yang mengatur bagaimana data dikelola dalam organisasi. Arsitektur data yang baik diperlukan untuk memastikan bahwa data dikelola secara efektif dan efisien
Data induk	Data yang merupakan dasar dari data lainnya. Data induk yang akurat dan mutakhir diperlukan untuk memastikan bahwa data lainnya juga akurat dan mutakhir
Data referensi	Data yang digunakan untuk menjelaskan atau melengkapi data lainnya. Data referensi yang akurat dan mutakhir diperlukan untuk memastikan bahwa data lainnya dapat digunakan secara efektif
Basis data	Sistem penyimpanan data. Basis data yang baik diperlukan untuk memastikan bahwa data dapat disimpan dan diakses dengan cepat dan mudah
Kualitas data	Tingkat akurasi, kelengkapan, dan relevansi data. Kualitas data yang tinggi diperlukan untuk memastikan bahwa data dapat digunakan untuk berbagai tujuan

- **Manajemen Layanan**



Gambar 3. 4 Diagram Manajemen Layanan SPBE

Gambar diatas menunjukkan diagram yang menggambarkan langkah-langkah yang terlibat dalam menjaga dan meningkatkan kualitas layanan SPBE kepada pengguna SPBE. Diagram tersebut terdiri dari tiga komponen utama, yaitu:

1. Pelayanan pengguna SPBE, yang mencakup kegiatan pelayanan terhadap keluhan, gangguan, masalah, permintaan, dan perubahan layanan SPBE.
2. Pengoperasian layanan SPBE, yang mencakup kegiatan pendayagunaan dan pemeliharaan infrastruktur dan aplikasi SPBE.
3. Pengelolaan aplikasi SPBE, yang mencakup kegiatan pembangunan dan pengembangan aplikasi yang berpedoman pada metodologi pembangunan dan pengembangan aplikasi SPBE.

Pelayanan pengguna SPBE bertujuan untuk memastikan kepuasan pengguna SPBE dengan layanan yang diberikan. Komponen ini mencakup kegiatan berikut:

1. Penanganan keluhan, yaitu kegiatan untuk menyelesaikan keluhan pengguna SPBE secara cepat dan memuaskan.
2. Penanganan gangguan, yaitu kegiatan untuk mengatasi gangguan layanan SPBE secara cepat dan efektif.
3. Penanganan masalah, yaitu kegiatan untuk menyelesaikan masalah layanan SPBE secara permanen.
4. Penanganan permintaan, yaitu kegiatan untuk memenuhi permintaan pengguna SPBE terkait layanan SPBE.
5. Penanganan perubahan, yaitu kegiatan untuk menyesuaikan layanan SPBE sesuai dengan kebutuhan pengguna.

Pengoperasian layanan SPBE bertujuan untuk memastikan ketersediaan dan keandalan layanan SPBE. Komponen ini mencakup kegiatan berikut :

1. Pendayagunaan infrastruktur SPBE, yaitu kegiatan untuk memanfaatkan infrastruktur SPBE secara optimal untuk mendukung layanan SPBE.
2. Pemeliharaan infrastruktur SPBE, yaitu kegiatan untuk menjaga infrastruktur SPBE agar tetap dalam kondisi baik dan dapat berfungsi secara optimal.
3. Pendayagunaan aplikasi SPBE, yaitu kegiatan untuk memanfaatkan aplikasi SPBE secara optimal untuk mendukung layanan SPBE.
4. Pemeliharaan aplikasi SPBE, yaitu kegiatan untuk menjaga aplikasi SPBE agar tetap dalam kondisi baik dan dapat berfungsi secara optimal.

Pengelolaan aplikasi SPBE bertujuan untuk memastikan kualitas aplikasi SPBE. Komponen ini mencakup kegiatan berikut:

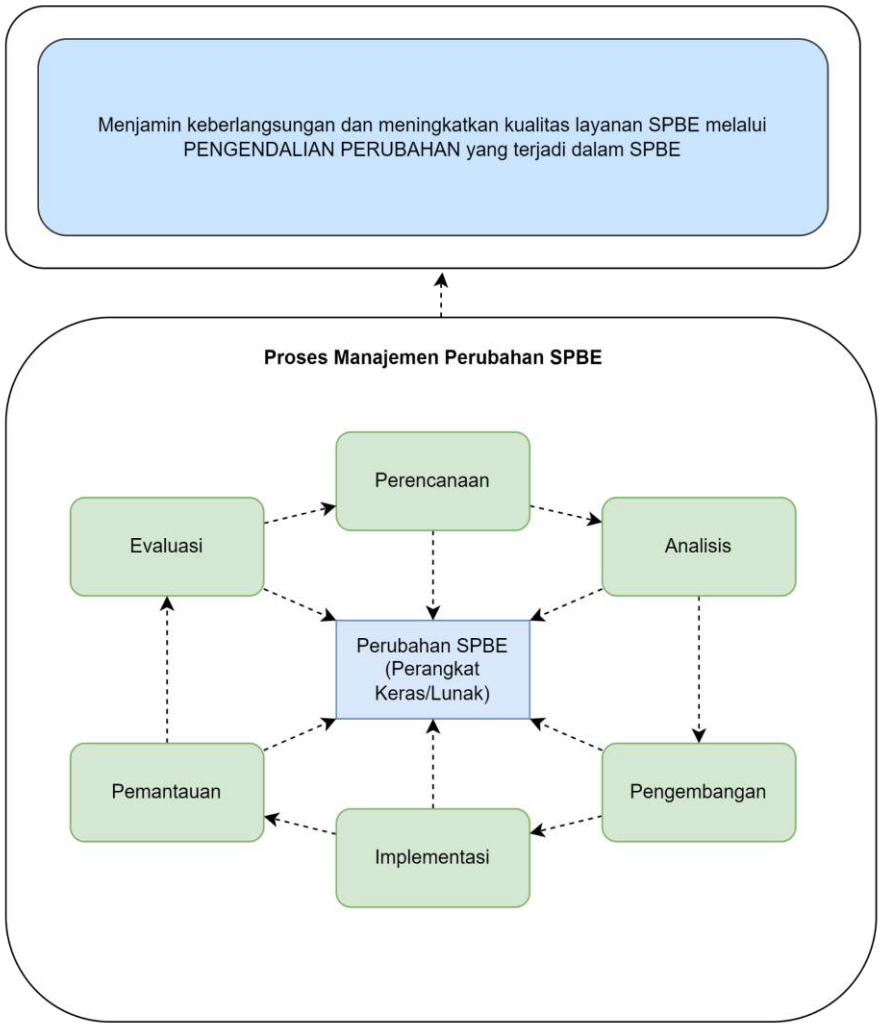
1. Pembangunan aplikasi SPBE, yaitu kegiatan untuk menciptakan aplikasi SPBE baru yang memenuhi kebutuhan pengguna.
2. Pengembangan aplikasi SPBE, yaitu kegiatan untuk meningkatkan kualitas aplikasi SPBE yang telah ada.

Diagram tersebut menunjukkan bahwa menjaga dan meningkatkan kualitas layanan SPBE adalah sebuah proses yang kompleks dan melibatkan berbagai komponen. Proses ini harus dilakukan secara berkelanjutan untuk memastikan kepuasan pengguna SPBE dan

keberlangsungan layanan SPBE. Berikut adalah penjelasan lebih lanjut tentang masing-masing komponen dalam diagram tersebut:

1) Pelayanan pengguna SPBE merupakan komponen yang paling penting dalam menjaga dan meningkatkan kualitas layanan SPBE. Hal ini karena kepuasan pengguna SPBE merupakan salah satu faktor yang menentukan keberhasilan layanan SPBE. Untuk memastikan kepuasan pengguna SPBE, penyelenggara layanan SPBE harus memiliki sistem pelayanan yang efektif dan efisien. Sistem pelayanan ini harus mampu menangani berbagai keluhan, gangguan, masalah, permintaan, dan perubahan yang disampaikan oleh pengguna SPBE.
2) Pengoperasian layanan SPBE merupakan komponen yang penting dalam memastikan ketersediaan dan keandalan layanan SPBE. Hal ini karena infrastruktur dan aplikasi SPBE merupakan komponen utama yang mendukung layanan SPBE. Untuk memastikan ketersediaan dan keandalan layanan SPBE, penyelenggara layanan SPBE harus memiliki sistem pengelolaan infrastruktur dan aplikasi SPBE yang memadai. Sistem pengelolaan ini harus mampu memastikan bahwa infrastruktur dan aplikasi SPBE selalu dalam kondisi baik dan dapat berfungsi secara optimal.
3) Pengelolaan aplikasi SPBE merupakan komponen yang penting dalam memastikan kualitas aplikasi SPBE. Hal ini karena aplikasi SPBE merupakan salah satu komponen utama yang menentukan kualitas layanan SPBE. Untuk memastikan kualitas aplikasi SPBE, penyelenggara layanan SPBE harus memiliki sistem pembangunan dan pengembangan aplikasi SPBE yang memadai. Sistem pembangunan dan pengembangan ini harus mampu menghasilkan aplikasi SPBE yang memenuhi kebutuhan pengguna dan memiliki kualitas yang baik.

- **Manajemen Perubahan**



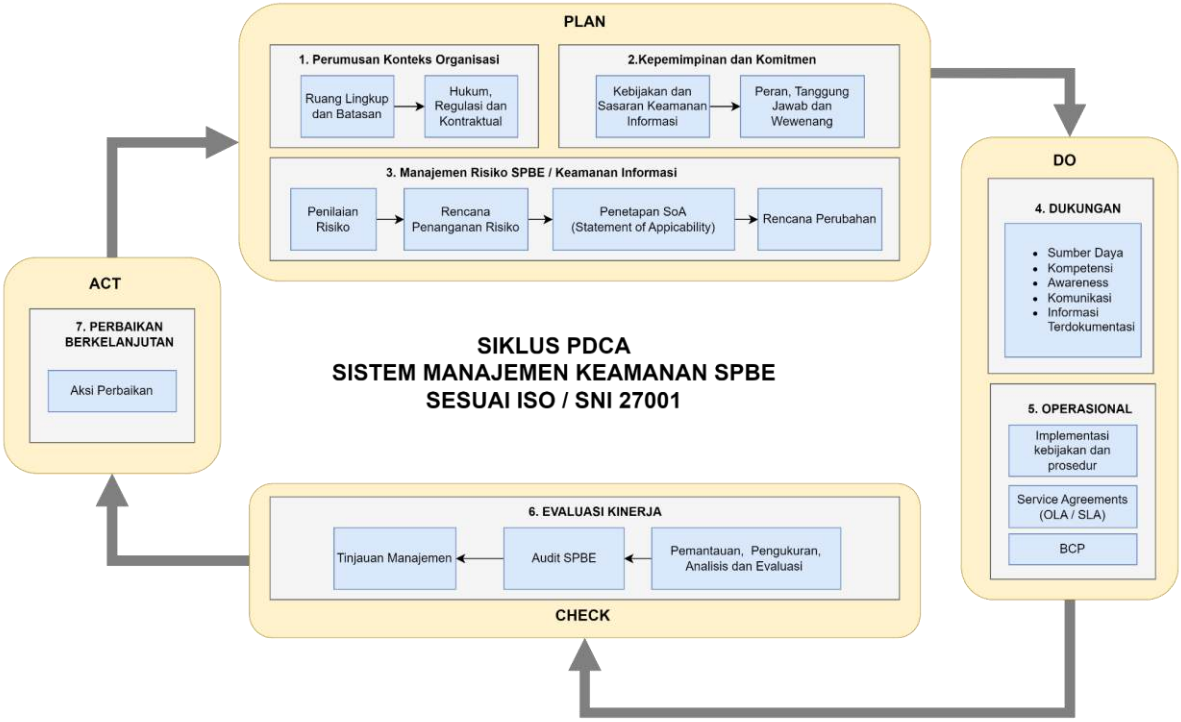
Gambar 3. 5 Diagram Manajemen Perubahan SPBE

Gambar diatas menunjukkan bahwa proses manajemen perubahan SPBE dimulai dengan adanya usulan perubahan. Usulan perubahan tersebut kemudian dianalisis untuk menentukan apakah perubahan tersebut perlu dilakukan atau tidak. Jika perubahan tersebut perlu dilakukan, maka akan dilanjutkan ke tahap pengembangan solusi perubahan. Solusi perubahan tersebut kemudian diimplementasikan ke dalam sistem yang ada. Setelah perubahan diterapkan, maka akan dilakukan pemantauan untuk memastikan bahwa perubahan tersebut berjalan sesuai rencana. Terakhir, perubahan tersebut akan dievaluasi untuk menilai keberhasilannya. Berdasarkan gambar diatas, dapat disimpulkan bahwa proses manajemen perubahan SPBE adalah proses yang penting untuk memastikan bahwa perubahan yang terjadi dalam SPBE dapat berjalan dengan lancar dan mencapai tujuan yang diinginkan.

Tabel 3. 4 Langkah Proses Manajemen Perubahan SPBE

Langkah Proses Manajemen Perubahan SPBE	
Perencanaan	Langkah ini bertujuan untuk menetapkan tujuan dan sasaran perubahan, serta menyusun rencana pelaksanaan perubahan. Tujuan dan sasaran perubahan harus jelas dan spesifik agar dapat diukur keberhasilannya. Rencana pelaksanaan perubahan harus realistis dan dapat diimplementasikan
Analisis	Langkah ini bertujuan untuk menganalisis dampak perubahan terhadap berbagai aspek, seperti proses bisnis, sistem informasi, dan sumber daya manusia. Analisis dampak perubahan penting dilakukan untuk memastikan bahwa perubahan tersebut tidak menimbulkan masalah baru
Pengembangan	Langkah ini bertujuan untuk mengembangkan solusi perubahan yang sesuai dengan hasil analisis. Solusi perubahan harus dapat mengatasi masalah yang ada dan memenuhi kebutuhan pengguna
Implementasi	Langkah ini bertujuan untuk menerapkan solusi perubahan ke dalam sistem yang ada. Implementasi perubahan harus dilakukan secara hati-hati dan bertahap untuk menghindari masalah
Pemantauan	Langkah ini bertujuan untuk memantau pelaksanaan perubahan dan melakukan penyesuaian jika diperlukan. Pemantauan perubahan penting dilakukan untuk memastikan bahwa perubahan tersebut berjalan sesuai rencana
Evaluasi	Langkah ini bertujuan untuk menilai keberhasilan perubahan dan memberikan umpan balik untuk perbaikan di masa depan. Evaluasi perubahan penting dilakukan untuk memastikan bahwa perubahan tersebut telah mencapai tujuan yang diinginkan

- **Manajemen Keamanan Informasi**



Gambar 3. 6 Diagram Siklus PDCA Sistem Manajemen Keamanan SPBE Sesuai ISO/SNI 27001

Gambar diatas menunjukkan diagram siklus PDCA untuk sistem manajemen keamanan SPBE sesuai ISO/SNI 27001. Siklus PDCA terdiri dari empat fase, yaitu :

1. Plan (Perencanaan): Pada fase ini, organisasi menetapkan ruang lingkup, tujuan, dan kontrol keamanan informasi.
2. Do (Pelaksanaan): Pada fase ini, organisasi melaksanakan kontrol keamanan informasi yang telah ditetapkan.
3. Check (Evaluasi): Pada fase ini, organisasi mengevaluasi efektivitas kontrol keamanan informasi yang telah dilaksanakan.
4. Act (Tindakan): Pada fase ini, organisasi mengambil tindakan untuk meningkatkan efektivitas kontrol keamanan informasi.

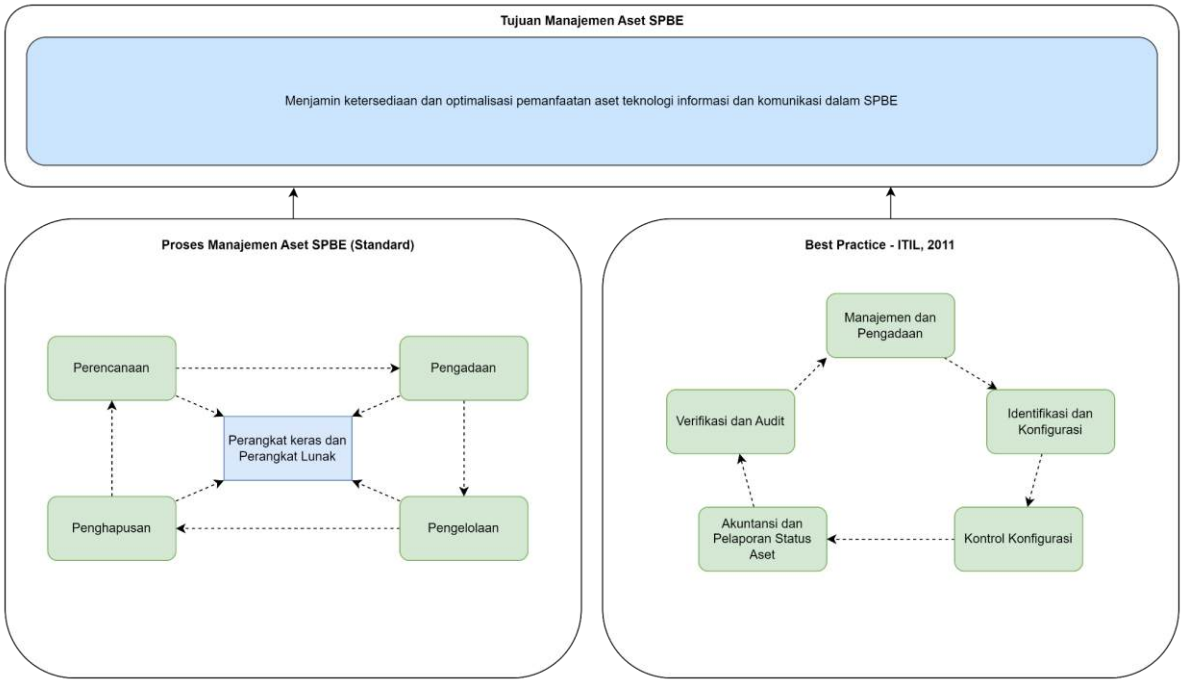
Gambar diatas juga menunjukkan 7 langkah yang dilakukan dalam setiap fase siklus PDCA. Langkah-langkah tersebut adalah sebagai berikut:

Tabel 3. 5 Langkah Pada Fase Siklus PDCA

Langkah Pada Fase Siklus PDCA	
Plan (Perencanaan)	
Perumusan Konteks Organisasi	langkah ini bertujuan untuk mengidentifikasi konteks organisasi, termasuk lingkungan internal dan eksternal yang dapat berdampak pada keamanan informasi. Lingkungan internal meliputi faktor-faktor seperti budaya organisasi, struktur organisasi, dan proses bisnis. Lingkungan eksternal meliputi faktor-faktor seperti peraturan pemerintah, tren teknologi, dan ancaman keamanan informasi
Kepemimpinan dan Komitmen	langkah ini bertujuan untuk menetapkan kebijakan dan sasaran keamanan informasi, serta menetapkan peran, tanggung jawab, dan wewenang dalam pengelolaan keamanan informasi. Kebijakan keamanan informasi adalah pernyataan tujuan dan komitmen organisasi dalam pengelolaan keamanan informasi. Sasaran keamanan informasi adalah hasil yang ingin dicapai oleh organisasi dalam pengelolaan keamanan informasi. Peran, tanggung jawab, dan wewenang dalam pengelolaan keamanan informasi harus didefinisikan dengan jelas agar memastikan bahwa sistem manajemen keamanan informasi dapat berjalan efektif
Manajemen Risiko SPBE / Keamanan Informasi	langkah ini bertujuan untuk mengidentifikasi, menganalisis, dan menilai risiko keamanan informasi. Risiko keamanan informasi adalah kemungkinan terjadinya suatu peristiwa yang dapat menyebabkan kerugian bagi organisasi. Risiko keamanan informasi dapat dikategorikan menjadi risiko teknis, risiko operasional, dan risiko hukum
Do (Pelaksanaan)	
Dukungan	langkah ini bertujuan untuk menyediakan sumber daya, kompetensi, dan dokumentasi yang diperlukan untuk mendukung sistem manajemen keamanan informasi. Sumber daya yang diperlukan meliputi sumber daya manusia, sumber daya finansial, dan sumber daya teknologi informasi. Kompetensi yang diperlukan meliputi kompetensi teknis dan kompetensi manajerial. Dokumentasi yang diperlukan meliputi kebijakan, prosedur, dan instruksi kerja
Operasional	langkah ini bertujuan untuk menerapkan kebijakan dan prosedur keamanan informasi. Kebijakan dan prosedur keamanan informasi harus diimplementasikan secara konsisten agar dapat memberikan perlindungan yang efektif terhadap keamanan informasi
Check (Evaluasi)	

Langkah Pada Fase Siklus PDCA	
Evaluasi Kinerja	langkah ini bertujuan untuk melakukan pemantauan, pengukuran, analisis, dan evaluasi terhadap sistem manajemen keamanan informasi. Evaluasi kinerja dilakukan untuk memastikan bahwa sistem manajemen keamanan informasi tetap efektif dan memenuhi kebutuhan organisasi
Act (Tindakan)	
Perbaikan Berkelanjutan	langkah ini bertujuan untuk mengambil tindakan untuk meningkatkan efektivitas sistem manajemen keamanan informasi. Tindakan perbaikan dapat berupa perubahan pada kebijakan, prosedur, atau kontrol keamanan informasi

- **Manajemen Aset TIK**



Gambar 3. 7 Diagram Manajemen Aset SPBE

Berdasarkan gambar diatas, proses manajemen aset SPBE diawali dengan tahap perencanaan. Tahap ini bertujuan untuk menetapkan kebutuhan aset TIK yang akan diperoleh. Setelah kebutuhan aset TIK ditetapkan, maka tahap selanjutnya adalah pengadaan. Tahap ini dapat dilakukan dengan cara pembelian, sewa, atau hibah. Setelah aset TIK diperoleh, maka tahap selanjutnya adalah verifikasi dan audit. Tahap ini bertujuan untuk memastikan bahwa aset TIK yang diperoleh telah sesuai dengan spesifikasi yang telah ditetapkan. Setelah aset TIK diverifikasi dan diaudit, maka tahap selanjutnya adalah identifikasi dan konfigurasi. Tahap ini

bertujuan untuk memberikan identitas dan informasi konfigurasi yang unik untuk setiap aset TIK. Aset TIK yang telah diidentifikasi dan dikonfigurasi kemudian dapat digunakan.

Pada tahap pengelolaan, aset TIK yang telah tersedia harus dikelola secara optimal agar dapat dimanfaatkan secara maksimal. Pengelolaan aset TIK meliputi akuntansi dan pelaporan status aset, serta kontrol konfigurasi.

Proses manajemen aset SPBE yang baik akan membantu memastikan ketersediaan dan optimalisasi pemanfaatan aset TIK dalam SPBE. Hal ini akan berdampak pada peningkatan efektivitas dan efisiensi penyelenggaraan SPBE.

Berikut adalah beberapa penjelasan tambahan tentang gambar tersebut:

1. Tujuan Manajemen Aset SPBE

   Tujuan manajemen aset SPBE adalah untuk memastikan ketersediaan dan optimalisasi pemanfaatan aset TIK dalam SPBE. Hal ini dapat dicapai dengan menerapkan proses manajemen aset SPBE yang baik.
2. Proses Manajemen Aset SPBE (Standard)

   Proses manajemen aset SPBE yang ditunjukkan dalam gambar tersebut merupakan proses yang standar. Proses ini dapat digunakan sebagai acuan untuk penerapan manajemen aset SPBE di berbagai instansi pemerintah.
3. Best Practice ITIL, 2011

   Proses manajemen aset SPBE yang ditunjukkan dalam gambar tersebut didasarkan pada best practice ITIL, 2011. ITIL merupakan framework yang digunakan untuk manajemen layanan TI.
4. Perangkat Keras dan Perangkat Lunak

   Aset TIK yang dikelola dalam proses manajemen aset SPBE meliputi perangkat keras dan perangkat lunak. Perangkat keras adalah komponen fisik dari sistem TI, sedangkan perangkat lunak adalah program yang digunakan untuk mengoperasikan sistem TI.
5. Verifikasi dan Audit

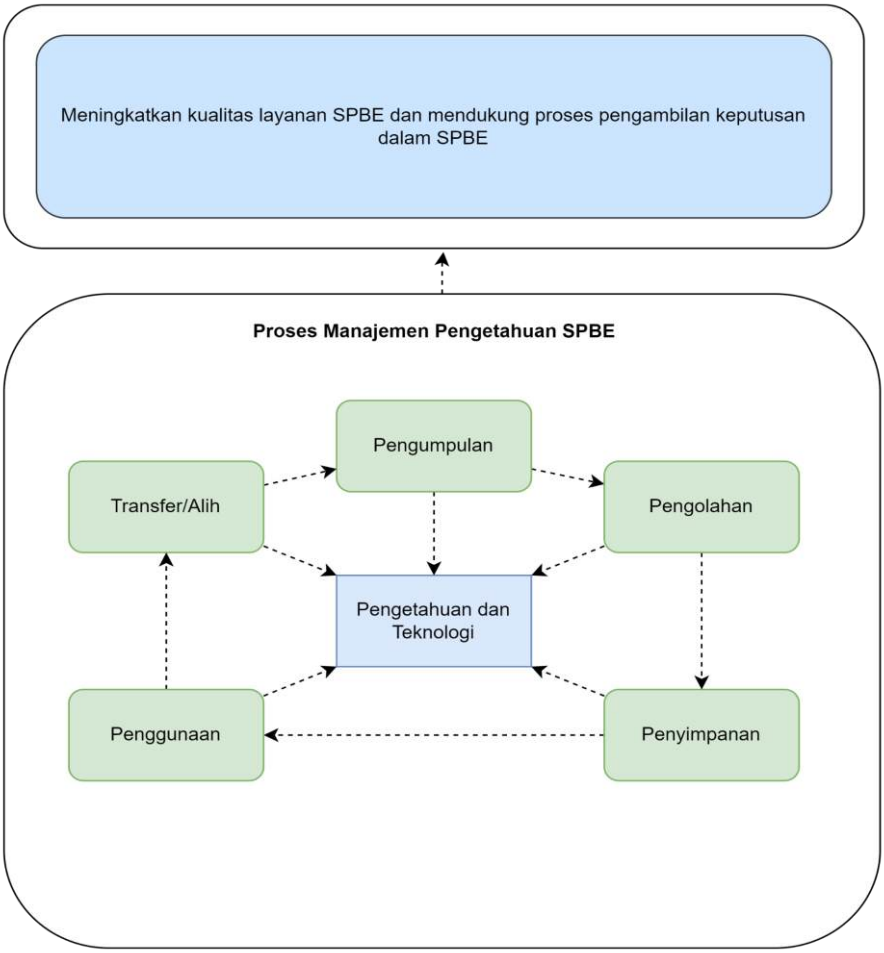
   Verifikasi dan audit merupakan proses yang penting untuk memastikan bahwa aset TIK yang diperoleh telah sesuai dengan spesifikasi yang telah ditetapkan. Verifikasi dilakukan oleh pihak yang independen, sedangkan audit dilakukan oleh pihak internal instansi pemerintah.
6. Identifikasi dan Konfigurasi

Identifikasi dan konfigurasi merupakan proses yang penting untuk memastikan bahwa aset TIK dapat dikelola secara efektif. Identitas aset TIK harus unik agar dapat dilacak dengan mudah. Informasi konfigurasi aset TIK harus akurat dan mutakhir agar dapat digunakan untuk pengelolaan aset TIK.

7. Penghapusan

   Penghapusan merupakan proses yang penting untuk memastikan bahwa aset TIK yang sudah tidak digunakan atau tidak memenuhi kebutuhan dapat dikelola dengan baik. Aset TIK yang akan dihapus harus didokumentasikan dengan baik agar dapat digunakan sebagai referensi di masa mendatang.

- **Manajemen Pengetahuan**



Gambar 3. 8 Diagram Proses Manajemen Pengetahuan SPBE

Gambar tersebut menunjukkan bahwa manajemen pengetahuan SPBE bertujuan untuk meningkatkan kualitas layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE dan alur proses manajemen pengetahuan SPBE yang terdiri dari lima tahapan, yaitu :

1. Pengumpulan

Pengetahuan dan teknologi yang dihasilkan dalam SPBE dapat dikumpulkan dari berbagai sumber, baik internal maupun eksternal. Sumber-sumber internal antara lain dokumen, laporan, hasil penelitian, dan hasil pengembangan. Sumber-sumber eksternal antara lain jurnal, buku, konferensi, dan media massa.

2. Pengolahan

   Pengetahuan dan teknologi yang telah dikumpulkan perlu diolah agar dapat digunakan secara efektif. Proses pengolahan dapat berupa klasifikasi, penataan, dan penyuntingan. Klasifikasi dilakukan untuk mengelompokkan pengetahuan dan teknologi berdasarkan kategori tertentu, seperti jenis, tema, atau tingkat kepentingan. Penataan dilakukan untuk menyusun pengetahuan dan teknologi agar mudah ditemukan dan digunakan. Penyuntingan dilakukan untuk memperbaiki kesalahan atau ketidakakuratan pada pengetahuan dan teknologi.

3. Penyimpanan

   Pengetahuan dan teknologi yang telah diolah perlu disimpan dalam sistem manajemen pengetahuan agar dapat diakses dengan mudah. Sistem manajemen pengetahuan dapat berupa portal, repositori, atau database. Portal adalah sistem manajemen pengetahuan yang dapat diakses melalui web browser. Repositori adalah sistem manajemen pengetahuan yang dapat digunakan untuk menyimpan dan berbagi file. Database adalah sistem manajemen pengetahuan yang dapat digunakan untuk menyimpan dan mengelola data dalam jumlah besar.

4. Penggunaan

   Pengetahuan dan teknologi yang telah disimpan dapat digunakan untuk meningkatkan kualitas layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE. Pengetahuan dan teknologi dapat digunakan untuk :

   1. Mengembangkan layanan SPBE baru
   2. Menyempurnakan layanan SPBE yang ada
   3. Meningkatkan efisiensi dan efektivitas layanan SPBE
   4. Meningkatkan kepuasan pengguna layanan SPBE
   5. Mendukung proses pengambilan keputusan dalam SPBE

5. Transfer/Alih

   Pengetahuan dan teknologi yang telah dimiliki dapat ditransfer atau dialihkan kepada pihak lain, baik internal maupun eksternal. Transfer/alih pengetahuan dan teknologi dapat dilakukan melalui berbagai cara, seperti pelatihan, seminar, dan konferensi. Transfer/alih pengetahuan dan teknologi dapat bermanfaat untuk :

   1. Meningkatkan pengetahuan dan keterampilan pegawai

2. Meningkatkan daya saing organisasi
3. Mempercepat pengembangan teknologi

- **Manajemen SDM**

Gambar 3. 9 Diagram Proses Manajemen SDM SPBE

Gambar diatas menunjukkan diagram proses manajemen SDM SPBE. Diagram tersebut terdiri dari empat tahap, yaitu:

1. Rekrutmen dan Seleksi

   Tahap ini bertujuan untuk mencari dan memilih pegawai yang memenuhi persyaratan untuk bekerja di bidang SPBE. Persyaratan tersebut meliputi :

   1. Pendidikan
   2. Pengalaman kerja
   3. Kompetensi teknis
   4. Kompetensi manajerial
   5. Kompetensi kepemimpinan

   Proses rekrutmen dan seleksi dapat dilakukan melalui berbagai cara, seperti :

   1. Seleksi administrasi
   2. Seleksi tertulis

3. Seleksi wawancara
4. Seleksi psikologi

2. Kompetensi

Tahap ini bertujuan untuk meningkatkan kompetensi pegawai SPBE agar dapat menjalankan tugas dan fungsinya dengan baik. Kompetensi pegawai SPBE meliputi :

1. Kompetensi teknis: pengetahuan dan keterampilan yang dibutuhkan untuk menjalankan tugas dan fungsi di bidang SPBE, seperti pemrograman, desain grafis, dan manajemen database.
2. Kompetensi manajerial: kemampuan untuk mengelola sumber daya, seperti manusia, uang, dan waktu.
3. Kompetensi kepemimpinan: kemampuan untuk mempengaruhi dan menggerakkan orang lain untuk mencapai tujuan bersama.

Peningkatan kompetensi pegawai SPBE dapat dilakukan melalui berbagai cara, seperti:

- Pelatihan
- Seminar
- Workshop
- On-the-job training

3. Learning dan Development

Tahap ini bertujuan untuk mengembangkan pengetahuan dan keterampilan pegawai SPBE agar dapat mengikuti perkembangan teknologi dan perubahan lingkungan. Pengembangan ini dapat dilakukan melalui berbagai cara, seperti :

- Pelatihan
- Seminar
- Workshop
- Rotasi jabatan
- Penghargaan

4. Pengembangan dan Budaya Organisasi

Tahap ini bertujuan untuk mengembangkan budaya organisasi yang mendukung penerapan SPBE. Budaya organisasi yang mendukung penerapan SPBE adalah budaya yang terbuka, kolaborasi, dan inovatif.

Pengembangan budaya organisasi dapat dilakukan melalui berbagai cara, seperti :

- Pelatihan
- Seminar
- Workshop
- Pembentukan tim kerja

- Pengembangan kebijakan dan prosedur kerja

Berdasarkan informasi yang tertera dalam gambar, manajemen SDM SPBE bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE. Dengan menerapkan proses manajemen SDM SPBE yang baik, instansi pemerintah dapat memiliki pegawai SPBE yang kompeten dan profesional, sehingga dapat memberikan layanan SPBE yang berkualitas kepada masyarakat.

Manajemen SPBE di pemerintah daerah merupakan proses yang kompleks dan berkelanjutan yang melibatkan berbagai pihak. Manajemen SPBE yang efektif dapat membantu pemerintah daerah untuk mencapai tujuan SPBE, yaitu:

- Peningkatan efisiensi dan efektivitas penyelenggaraan pemerintahan
- Peningkatan transparansi dan akuntabilitas pemerintahan
- Peningkatan partisipasi masyarakat
- Peningkatan kualitas pelayanan publik

BAB IV
POTENSI DAN REKOMENDASI INISIATIF PERBAIKAN MANAJEMEN SPBE

4.1 Manajemen Risiko

Kondisi ideal yang diharapkan dalam praktek manajemen risiko SPBE adalah penerapan sesuai dengan permen PAN RB no 5 tahun 2020, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 1 Manajemen Risiko SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. penerapan pedoman manajemen risiko SPBE 2. reviu dan evaluasi pelaksanaan manajemen risiko SPBE 3. perbaikan tindak lanjut dari hasil evaluasi risiko SPBE	1. penyelenggaraan Pelatihan Awareness dan Readiness Manajemen Risiko SPBE 2. penerapan Manajemen Risiko sesuai dengan hasil asesmen pada pelatihan awareness dan readiness 3. pengembangan Solusi atau platform untuk monitoring pelaksanaan manajemen risiko lingkup Pemkab. Natuna	1. rutin minimal 1 kali per semester 2. bertahap tiap semester untuk setiap satuan kerja yang sudah mendapatkan pelatihan Awareness dan Readiness 3. awal tahun depan untuk memastikan profil dan registrasi risiko sudah dipetakan sesuai kemen PAN RB no 5 tahun 2020

4.2 Manajemen Sumber Daya Manusia

Kondisi ideal yang diharapkan dalam praktek manajemen SDM SPBE adalah adanya kebijakan strategis manajemen SDM SPBE serta keterpenuhan kompetensi SDM SPBE (kompetensi di bidang Proses Bisnis Pemerintahan, Arsitektur SPBE, Data dan Informasi, Keamanan SPBE, Aplikasi SPBE, dan Infrastruktur SPBE), tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 2 Manajemen SDM SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. kebijakan strategis manajemen SPBE 2. pemetaan kompetensi SDM SPBE 3. program peningkatan kompetensi SDM SPBE	1. penyusunan Rencana Aksi Manajemen SDM SPBE 2. pelaksanaan dan Penyusunan Peta Kompetensi dan Peta Karir Fungsional SPBE 3. pelaksanaan dan penyusunan analisis jabatan fungsional SPBE 4. penyusunan rencana	1. awal Tahun Depan dan berlaku untuk 5 tahun 2. awal Tahun Depan dan berlaku mengikuti perkembangan kebutuhan SDM SPBE 3. awal tahun depan

Potensi Perbaikan	Usulan	Sifat Usulan
	pengembangan dan pelaksanaan peningkatan kapabilitas SDM SPBE sesuai dengan peta kompetensi dan analisis jabatan fungsional SPBE	mengikuti pola kegiatan kedua Setiap tahun

4.3 Manajemen Keamanan

Kondisi ideal yang diharapkan dalam praktek manajemen keamanan SPBE adalah pendekatan sistematis sesuai dengan standar SMKI (Sistem Manajemen Keamanan Informasi) berdasarkan ISO 27001 pengendalian keamanan informasi yang dilaksanakan pada seluruh unit kerja, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 3 Manajemen Keamanan SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. penguatan tim dan implementasi teknologi terkait pengamanan informasi 2. Pembuatan dan penetapan pedoman manajemen keamanan SPBE / Implementasi Dokumen dan Audit Survailen Keamanan Informasi dan Sertifikasi ISO 27001 3. reviu dan evaluasi pelaksanaan manajemen keamanan SPBE 4. perbaikan tindak lanjut perbaikan dari hasil evaluasi keamanan SPBE	1. penyusunan Kebijakan (Perbup, pedoman, SOP) terkait keamanan siber 2. uji keamanan siber berkala 3. pendampingan implementasi SNI 27001 oleh implementator tersertifikasi 4. audit keamanan informasi independent 5. pendampingan pra-sertifikasi ISO 27001	1. awal tahun depan 2. bertahap tiap semester

4.4 Manajemen Pengetahuan

Kondisi ideal yang diharapkan dalam praktek manajemen pengetahuan SPBE adalah adanya pedoman manajemen pengetahuan mendokumentasi pengalaman dan pengetahuan dalam perencanaan, implementasi, dan evaluasi SPBE, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 4 Manajemen Pengetahuan SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. pembuatan pedoman manajemen pengetahuan 2. membuat mekanisme secara teknologi yang mudah digunakan untuk mendokumentasikan	1. penyelenggaraan Pelatihan Awareness dan Readiness Manajemen Pengetahuan SPBE 2. penerapan Manajemen Pengetahuan sesuai	1. awal tahun depan dan berlaku mengikuti perkembangan kebutuhan 2. bertahap tiap

Potensi Perbaikan	Usulan	Sifat Usulan
pengalaman dan pengetahuan SPBE	dengan hasil asesmen pada pelatihan Awareness dan Readiness 3. pengembangan Solusi atau platform untuk manajemen pengetahuan dilingkup Kabupaten Natuna	semester untuk setiap satuan kerja yang sudah mendapatkan pelatihan Awareness dan Readiness

4.5 Manajemen Perubahan

Kondisi ideal yang diharapkan dalam praktek manajemen perubahan SPBE adalah adanya pedoman dan prosedur untuk mengelola perubahan, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 5 Manajemen Perubahan SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. pembuatan dokumen pedoman manajemen perubahan 2. implementasi tools ataupun mekanisme standard untuk mencatat dan mengelola perubahan	1. penyelenggaraan Pelatihan Awareness dan Readiness Manajemen Perubahan SPBE 2. penerapan Manajemen Perubahan sesuai dengan hasil asesmen pada pelatihan Awareness dan Readiness 3. pengembangan Solusi atau platform untuk manajemen perubahan dilingkup Kabupaten Natua.	1. awal tahun depan dan berlaku mengikuti perkembangan kebutuhan 2. Bertahap tiap semester untuk setiap satuan kerja yang sudah mendapatkan pelatihan Awareness dan Readiness

4.6 Manajemen Layanan

Kondisi ideal yang diharapkan dalam praktek manajemen layanan SPBE adalah dengan membangun dan mengelolah portal pusat layanan, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 6 Manajemen Layanan SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. penguatan manajemen layanan yang berkesinambungan (*continuous improvement*) untuk implementasi yang sudah baik	1. redesign pengalaman pengguna dalam akses layanan publik yang user centric 2. pengembangan layanan helpdesk untuk layanan publik	1. awal Tahun Depan dan berlaku mengikuti perkembangan kebutuhan layanan

Potensi Perbaikan	Usulan	Sifat Usulan
	3. pengembangan layanan helpdesk TIK untuk internal pegawai	

4.7 Manajemen Aset TIK

Kondisi ideal yang diharapkan dalam praktek manajemen aset TIK yaitu dilakukan dengan serangkain proses (perencanaan, pengadaan, pengelolaan dan penghapusan perangkat keras) untuk menjamin ketersediaan dan optimalisasi pemanfaatan aset teknologi informasi dan komunikasi dalam SPBE, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 7 Manajemen Aset TIK

Potensi Perbaikan	Usulan	Sifat Usulan
1. pencatatan aset TIK yang terkelola baik dan menyeluruh, termasuk aspek tingkat utilisasinya, usia, dan kondisinya 2. pedoman terkait manajemen kapasitas dan availabilitas aset TIK	1. Implementasi manajemen aset TIK	1. awal tahun depan dan berlaku untuk 5 tahun

4.8 Manajemen Data

Kondisi ideal yang diharapkan dalam praktek manajemen data SPBE adalah Penerapan Kebijakan Satu Data Pemerintah Kabupaten Natuna, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 8 Manajemen Data SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. penerapan Kebijakan Satu Data Pemkab. Natuna 2. perlunya integrasi arsitektur dan manajemen data dengan Satu Data Indonesia 3. optimasi kemampuan interoperabilitas data	1. penyelenggaraan Pelatihan Awareness dan Readiness Manajemen Data SPBE 2. penerapan Satu Data Pemkab. Natuna 3. pengembangan detail arsitektur data Pemkab. Natuna 4. pengembangan inter-connectivity untuk integrasi data di level database	1. awal tahun depan dan berlaku untuk 5 tahun

4.9 Manajemen Audit TIK

Kondisi ideal yang diharapkan dalam praktek manajemen audit SPBE adalah penerapan kebijakan internal Audit TIK, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

Tabel 4. 9 Manajemen Audit TIK

Potensi Perbaikan	Usulan	Sifat Usulan
1. integrasi program audit TIK dengan proses bisnis audit Inspektorat Jenderal 2. peningkatan kompetensi dan formasi tim pelaksana audit TIK	1. audit internal SPBE oleh Tim Assessor SPBE 2. penguatan organisasi terkait SPBE	1. setiap tahun 2. awal Tahun Depan dan berlaku mengikuti perkembangan kebutuhan SDM SPBE

4.10 Manajemen Tata Kelola

Kondisi ideal yang diharapkan dalam praktek manajemen tata kelola SPBE yaitu dengan melaksanakan Keputusan Menteri Dalam Negeri terkait penerapan SPBE, tetapi kondisi saat ini seperti hasil survey terdapat beberapa gap yang perlu ditutup atau diselesaikan. Adapun potensi perbaikan dan inisiatif yang diusulkan adalah sebagai berikut:

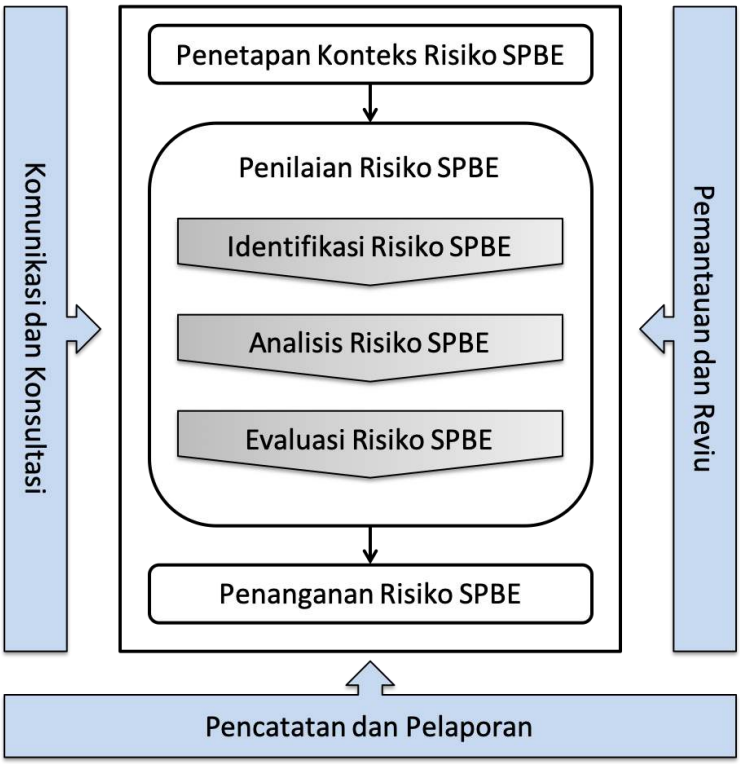
Tabel 4. 10 Manajemen Tata Kelola SPBE

Potensi Perbaikan	Usulan	Sifat Usulan
1. kelengkapan kebijakan sampai pada level pedoman manajemen SPBE	Implementasi siklus manajemen SPBE, antara lain dengan: • Memastikan semua program SPBE yang sudah ditetapkan menjadi bagian dari perencanaan SPBE • Memperkuat monitoring dan reviu pimpinan yang terjadwal berkala untuk melihat perkembangan SPBE • Memperbaiki dan mendokumentasikan atas rekomendasi tindakan perbaikan / corrective action yang diperlukan sebagai output dari reviu berkala SPBE	1. Rutin minimal 1 kali per semester 2. Bertahap tiap semester untuk setiap satuan kerja yang sudah mendapatkan pelatihan Awareness dan Readiness

BAB V
STANDAR DAN KEBIJAKAN UMUM PENERAPAN MANAJEMEN SPBE

5.1 Manajemen Risiko

Berdasarkan Peraturan Menteri PAN RB No 5 Tahun 2020 tentang Manajemen Risiko SPBE secara konseptual manajemen risiko digambarkan sebagai berikut:



Gambar 5. 1 Manajemen Risiko SPBE

Proses Manajemen Risiko SPBE merupakan rangkaian proses yang sistematis dan menjadi bagian dari proses pelaksanaan tugas dan fungsi Instansi Pusat dan Pemerintah Daerah untuk pengambilan keputusan di tingkat strategis, operasional, dan pelaksanaan proyek. Proses Manajemen Risiko SPBE yang dilaksanakan oleh Instansi Pusat dan Pemerintah Daerah terdiri atas proses:

1. komunikasi dan konsultasi;
2. penetapan konteks Risiko SPBE;
3. penilaian Risiko SPBE, yang terdiri atas identifikasi Risiko SPBE, analisis Risiko SPBE, dan evaluasi Risiko SPBE;
4. penanganan Risiko SPBE;
5. pemantauan dan reviu;
6. pencatatan dan pelaporan.

Sedangkan, tata kelola Manajemen Risiko SPBE merupakan mekanisme untuk mengatur kewenangan dan memastikan akuntabilitas pelaksanaan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Dalam hal ini, tata kelola Manajemen Risiko SPBE dibangun dengan menyusun struktur Manajemen Risiko SPBE dan membangun budaya sadar Risiko SPBE. Struktur Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah sedikitnya terdiri atas fungsi yang terkait dengan strategi dan kebijakan, pelaksanaan, dan pengawasan Manajemen Risiko SPBE. Selain itu, budaya sadar Risiko SPBE perlu dibangun dan dikembangkan oleh Instansi Pusat dan Pemerintah Daerah melalui perencanaan, pelaksanaan, dan pemantauan dan evaluasi kegiatan budaya sadar Risiko SPBE.

A. Komunikasi dan Konsultasi

Komunikasi dan konsultasi merupakan proses yang berkelanjutan dan berulang untuk menyediakan, membagikan, ataupun mendapatkan informasi dan menciptakan dialog dengan para pemangku kepentingan mengenai Risiko SPBE. Komunikasi dilakukan untuk meningkatkan kesadaran dan pemahaman mengenai Risiko SPBE. Sementara konsultasi dilakukan untuk mendapatkan umpan balik dan informasi dalam rangka mendukung pengambilan keputusan.

Bentuk kegiatan komunikasi dan konsultasi antara lain :

1. Rapat berkala, merupakan rapat yang diadakan secara rutin;
2. Rapat insidental, merupakan rapat yang diadakan sewaktu-waktu; dan
3. *Focus Group Discussion* (FGD), merupakan kelompok diskusi yang terarah untuk membahas topik tertentu.

B. Penetapan Konteks Risiko SPBE

Penetapan konteks Risiko SPBE bertujuan untuk mengidentifikasi parameter dasar dan ruang lingkup penerapan Risiko SPBE yang harus dikelola dalam proses Manajemen Risiko SPBE.

Tahapan penetapan konteks meliputi :

1. Inventarisasi Informasi Umum

   Inventarisasi informasi umum bertujuan untuk mendapatkan gambaran umum mengenai unit kerja yang menerapkan Manajemen Risiko SPBE. Informasi yang dicantumkan meliputi nama Unit Pemilik Risiko (UPR) SPBE, tugas UPR SPBE, fungsi

UPR SPBE, dan periode waktu pelaksanaan Manajemen Risiko SPBE dalam kurun waktu satu tahun.

2. Identifikasi Sasaran SPBE

   Identifikasi sasaran SPBE bertujuan untuk menentukan sasaran SPBE beserta Indikator dan targetnya yang mendukung sasaran unit kerja sebagai UPR SPBE.

3. Penentuan Struktur Pelaksana Manajemen Risiko SPBE

   Penentuan struktur pelaksana Manajemen Risiko SPBE bertujuan untuk menentukan unit kerja yang bertanggung jawab atas pelaksanaan Manajemen Risiko SPBE.

4. Identifikasi Pemangku Kepentingan

   Identifikasi pemangku kepentingan bertujuan untuk mendapatkan informasi dan memahami pihak-pihak yang melakukan interaksi dengan UPR SPBE dalam rangka pencapaian sasaran SPBE. Pihak-pihak tersebut meliputi unit kerja internal, unit kerja eksternal, instansi pemerintah, atau non instansi pemerintah. Hubungan kerja antara UPR SPBE dan setiap pihak pemangku kepentingan yang terkait dengan penerapan SPBE perlu dideskripsikan dengan jelas.

5. Identifikasi Peraturan Perundang-Undangan

   Identifikasi peraturan perundang-undangan bertujuan untuk memahami kewenangan, tanggung jawab, tugas dan fungsi, serta kewajiban hukum yang harus dilaksanakan oleh UPR SPBE. Informasi yang perlu dijelaskan dalam melakukan identifikasi peraturan perundang-undangan meliputi nama peraturan dan amanat dalam peraturan tersebut.

6. Penetapan Kategori Risiko SPBE

   Penetapan Kategori Risiko SPBE bertujuan untuk menjamin agar proses identifikasi, analisis, dan evaluasi Risiko SPBE dapat dilakukan secara komprehensif. Kategori Risiko SPBE meliputi:

   a. Rencana Induk SPBE Nasional, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan perencanaan pembangunan SPBE Nasional;
   b. Arsitektur SPBE, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pemanfaatan arsitektur SPBE yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, dan keamanan SPBE;
   c. Peta Rencana SPBE, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan Peta Rencana SPBE;
   d. Proses Bisnis, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan penerapan proses bisnis SPBE;

e. Rencana dan Anggaran, merupakan Risiko SPBE yang berkaitan dengan proses perencanaan dan penganggaran SPBE;
f. Inovasi, merupakan Risiko SPBE yang berkaitan dengan ide baru atau pemikiran kreatif yang memberikan nilai manfaat dalam penerapan SPBE;
g. Kepatuhan terhadap Peraturan, merupakan Risiko SPBE yang berkaitan dengan kepatuhan unit kerja di lingkungan Instansi Pusat dan Pemerintah Daerah terhadap peraturan perundang-undangan, kesepakatan internasional, maupun ketentuan lain yang berlaku;
h. Pengadaan Barang dan Jasa, merupakan Risiko SPBE yang berkaitan dengan proses pengadaan dan penyediaan barang dan jasa;
i. Proyek Pembangunan/Pengembangan Sistem, merupakan Risiko SPBE yang berkaitan dengan proyek pembangunan ataupun pengembangan sistem pada penerapan SPBE;
j. Data dan Informasi, merupakan Risiko SPBE yang berkaitan dengan semua data dan informasi yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah;
k. Infrastruktur SPBE, merupakan Risiko SPBE yang berkaitan dengan pusat data, jaringan intra pemerintah, dan sistem penghubung layanan pemerintah termasuk perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama;
l. Aplikasi SPBE, merupakan Risiko SPBE yang berkaitan dengan program komputer yang diterapkan untuk melakukan tugas atau fungsi layanan SPBE;
m. Keamanan SPBE, merupakan Risiko SPBE yang berkaitan dengan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya yang mendukung SPBE;
n. Layanan SPBE, merupakan Risiko SPBE yang berkaitan dengan pemberian layanan SPBE kepada Pengguna SPBE;
o. Sumber Daya Manusia SPBE, merupakan Risiko SPBE yang berkaitan dengan SDM yang bekerja sebagai penggerak penerapan SPBE di Instansi Pusat dan Pemerintah Daerah; dan
p. Bencana Alam, merupakan Risiko SPBE yang berkaitan dengan peristiwa yang disebabkan oleh alam.

7. Penetapan Area Dampak Risiko SPBE

Penetapan Area Dampak Risiko SPBE bertujuan untuk mengetahui area mana saja yang terkena efek dari Risiko SPBE di Instansi Pusat dan Pemerintah Daerah.

Penetapan Area Dampak Risiko SPBE diawali dengan melakukan identifikasi dampak Risiko SPBE. Area Dampak Risiko SPBE yang menjadi fokus penerapan Manajemen Risiko SPBE meliputi:

a. Finansial, dampak Risiko SPBE berupa aspek yang berkaitan dengan keuangan;
b. Reputasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan tingkat kepercayaan pemangku kepentingan;
c. Kinerja, dampak Risiko SPBE berupa aspek yang berkaitan dengan pencapaian sasaran SPBE;
d. Layanan Organisasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan pemenuhan kebutuhan atau jasa kepada pemangku kepentingan;
e. Operasional dan Aset TIK, dampak Risiko SPBE berupa aspek yang berkaitan dengan kegiatan operasional TIK dan pengelolaan aset TIK;
f. Hukum dan Regulasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan peraturan perundang-undangan dan kebijakan; dan g. Sumber Daya Manusia, dampak Risiko SPBE berupa aspek yang berkaitan dengan fisik dan mental pegawai.

8. Penetapan Kriteria Risiko SPBE

Penetapan Kriteria Risiko SPBE bertujuan untuk mengukur dan menetapkan seberapa besar kemungkinan kejadian dan dampak Risiko SPBE yang dapat terjadi. Kriteria Risiko SPBE ini ditinjau secara berkala dan perlu melakukan penyesuaian dengan perubahan yang terjadi. Penetapan Kriteria Risiko SPBE ini terdiri atas:

a. Kriteria Kemungkinan SPBE

Penetapan Kriteria Kemungkinan Risiko SPBE dilakukan berdasarkan penetapan level kemungkinan dan penetapan kriteria dari setiap level kemungkinan terhadap Risiko SPBE.

Instansi Pusat dan Pemerintah Daerah dapat menggunakan level kemungkinan dengan 3 level, 4 level, 5 level, atau level lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Untuk 5 level kemungkinan, dapat diuraikan sebagai berikut:

1) Hampir Tidak Terjadi;
2) Jarang Terjadi;
3) Kadang-Kadang Terjadi;
4) Sering Terjadi;
5) Hampir Pasti Terjadi.

6) Sedangkan, penetapan kriteria kemungkinan dilakukan melalui pendekatan persentase probabilitas statistik, jumlah frekuensi terjadinya suatu Risiko SPBE dalam satuan waktu, ataupun berdasarkan expert judgement.

Tabel 5. 1 Kriteria Kemungkinan SPBE

Level Kemungkinan		Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi	X ≤ 5%	X < 2 kali
2	Jarang Terjadi	5% < X ≤ 10%	2 ≤ X ≤ 5 kali
3	Kadang-Kadang Terjadi	10% < X ≤ 20%	6 ≤ X ≤ 9 kali
4	Sering Terjadi	20% < X ≤ 50%	10 ≤ X ≤ 12 kali
5	Hampir Pasti Terjadi	X > 50 %	> 12 kali

b. Kriteria Dampak SPBE

Penetapan Kriteria Dampak Risiko SPBE dilakukan dengan kombinasi antara Area Dampak Risiko SPBE (sebagaimana dijelaskan pada angka 7 di atas tentang Penetapan Area Dampak Risiko SPBE) dan level dampak. Instansi Pusat dan Pemerintah Daerah dapat menggunakan 3 level, 4 level, 5 level, atau level dampak lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Untuk 5 level dampak, dapat diuraikan sebagai berikut:

1) Tidak Signifikan;
2) Kurang Signifikan;
3) Cukup Signifikan;
4) Signifikan;
5) Sangat Signifikan.

Tabel 5. 2 Kriteria Dampak SPBE

Area Dampak		Level Dampak				
		1	2	3	4	5
		Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Kinerja	Positif	Peningkatan kinerja < 20%	Peningkatan kinerja 20% s.d < 40%	Peningkatan kinerja 40% s.d < 60%	Peningkatan kinerja 60% s.d < 80%	Peningkatan kinerja - 80%
	Negatif	Penurunan kinerja < 20%	Penurunan kinerja 20% s.d < 40%	Penurunan kinerja 40% s.d < 60%	Penurunan kinerja 60% s.d < 80%	Penurunan kinerja - 80%

9. Matriks Analisis Risiko SPBE dan Level Risiko SPBE

Matriks analisis Risiko SPBE berisi kombinasi antara level kemungkinan dan level dampak untuk dapat menetapkan Besaran Risiko SPBE yang direpresentasikan dalam bentuk angka.

Tabel 5. 3 Matriks Analisis Risiko SPBE dan Level Risiko SPBE

Matriks Analisis Risiko 5 x 5			**Level Dampak**				
			1	**2**	**3**	**4**	**5**
			Tidak Signifikan	**Kurang Signifikan**	**Cukup Signifikan**	**Signifikan**	**Sangat Signifikan**
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang-Kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

Besaran Risiko SPBE ini selanjutnya dikelompokkan ke dalam Level Risiko SPBE dimana setiap Level Risiko SPBE memiliki rentang nilai Besaran Risiko SPBE. Pemilihan Level Risiko SPBE dapat menggunakan 3 level, 4 level, 5 level, atau Level Risiko SPBE lainnya yang disesuaikan dengan kompleksitas Risiko SPBE. Setiap level tersebut direpresentasikan dengan warna sesuai dengan preferensi masing-masing Instansi Pusat dan Pemerintah Daerah. Untuk 5 Level Risiko SPBE, dapat diuraikan sebagai berikut:

a. Sangat Rendah, direpresentasikan dengan warna biru;
b. Rendah, direpresentasikan dengan warna hijau;
c. Sedang, direpresentasikan dengan warna kuning;
d. Tinggi, direpresentasikan dengan warna jingga;
e. Sangat Tinggi, direpresentasikan dengan warna merah.

Tabel 5. 4 Besaran Risiko SPBE

Level Risiko		Rentang Besaran Risiko	Keterangan Warna
1	Sangat Rendah	1-5	Biru
2	Rendah	6-10	Hijau
3	Sedang	11-15	Kuning
4	Tinggi	16-20	Jingga
5	Sangat Tinggi	21-25	Merah

10. Selera Risiko SPBE

    Selera Risiko SPBE bertujuan untuk memberikan acuan dalam penentuan ambang batas minimum terhadap Besaran Risiko SPBE yang harus ditangani untuk setiap Kategori Risiko SPBE baik Risiko SPBE Positif maupun Risiko SPBE Negatif. Penentuan Selera Risiko SPBE ini dapat disesuaikan dengan kompleksitas Risiko SPBE serta konteks internal dan eksternal masing-masing Instansi Pusat dan Pemerintah Daerah

C. Penilaian Risiko SPBE

Penilaian Risiko SPBE pada penerapan SPBE dilakukan melalui proses identifikasi, analisis, dan evaluasi Risiko SPBE. Penilaian Risiko SPBE bertujuan untuk memahami penyebab, kemungkinan, dan dampak Risiko SPBE yang dapat terjadi di Instansi Pusat dan Pemerintah Daerah. Penilaian Risiko SPBE dilakukan pada setiap Sasaran SPBE. Tahapan penilaian Risiko SPBE meliputi:

1. Identifikasi Risiko SPBE

   Identifikasi Risiko SPBE merupakan proses menggali informasi mengenai kejadian, penyebab, dan dampak Risiko SPBE. Informasi yang dicantumkan meliputi:

   a. Jenis Risiko SPBE

      Jenis Risiko SPBE terbagi menjadi Risiko SPBE positif dan Risiko SPBE negatif. Dalam melakukan identifikasi Risiko SPBE, Risiko SPBE dituliskan ke dalam masing-masing jenis Risiko SPBE.

   b. Kejadian

      Kejadian dapat diidentifikasi dari terjadinya suatu peristiwa yang menimbulkan Risiko SPBE yang diperoleh dari riwayat peristiwa dan/atau prediksi terjadinya peristiwa di masa yang akan datang. Kejadian selanjutnya disebut sebagai Risiko SPBE.

   c. Penyebab

      Penyebab dapat diidentifikasi dari akar masalah yang menjadi pemicu munculnya Risiko SPBE. Penyebab dapat berasal dari lingkungan internal maupun eksternal

Instansi Pusat dan Pemerintah Daerah. Identifikasi penyebab akan membantu menemukan tindakan yang tepat untuk menangani Risiko SPBE.

d. Kategori

Penentuan Kategori Risiko SPBE didasarkan pada penyebab dari munculnya Risiko SPBE. Kategori Risko SPBE telah dijelaskan pada bagian huruf B angka 6 tentang Penetapan Kategori Risiko SPBE.

e. Dampak

Dampak dapat diidentifikasi dari pengaruh atau akibat yang timbul dari Risiko SPBE.

f. Area Dampak

Penentuan Area Dampak Risiko SPBE didasarkan pada dampak yang telah teridentifikasi. Area Dampak Risiko telah dijelaskan pada bagian huruf B angka 7 tentang Penetapan Area Dampak.

2. Analisis Risiko SPBE

Analisis Risiko SPBE merupakan proses untuk melakukan penilaian atas Risiko SPBE yang telah diidentifikasi sebelumnya. Analisis Risiko SPBE dilakukan dengan cara menentukan sistem pengendalian, level kemungkinan, dan level dampak terjadinya Risiko SPBE. Informasi yang dicantumkan pada analisis Risiko SPBE meliputi:

a. Sistem Pengendalian

1) Sistem pengendalian internal mencakup perangkat manajemen yang dapat menurunkan/meningkatkan level Risiko SPBE dalam rangka pencapaian sasaran SPBE.
2) Sistem pengendalian internal dapat berupa Standard Operating Procedure (SOP), pengawasan melekat, reviu berjenjang, regulasi, dan pemantauan rutin yang dilaksanakan terkait Risiko SPBE tersebut.

b. Level Kemungkinan

Penentuan level kemungkinan dilakukan dengan mengukur persentase probabilitas atau frekuensi peluang terjadinya Risiko SPBE dalam satu periode yang dicocokkan dengan Kriteria Kemungkinan Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka 8 huruf a. Penentuan level kemungkinan harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level kemungkinan tersebut.

c. Level Dampak

Penentuan level dampak dilakukan dengan mengukur besar dampak dari terjadinya Risiko SPBE yang dicocokan dengan Kriteria Dampak Risiko SPBE sebagaimana telah dijelaskan pada bagian huruf B angka 8 huruf b. Level dampak harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level dampak tersebut.

d. Besaran Risiko SPBE dan Level Risiko SPBE

Penentuan Besaran Risiko SPBE dan Level Risiko SPBE didapat dari kombinasi Level Kemungkinan dan Level Dampak dengan menggunakan rumusan dalam Matriks Analisis Risiko SPBE

3. Evaluasi Risiko SPBE

Evaluasi Risiko SPBE dilakukan untuk mengambil keputusan mengenai perlu tidaknya dilakukan upaya penanganan Risiko SPBE lebih lanjut serta penentuan prioritas penanganannya. Pengambilan keputusan mengacu pada Selera Risiko SPBE yang telah ditentukan sebagaimana telah dijelaskan pada bagian huruf B angka 10. Prioritas penanganan Risiko SPBE diurutkan berdasarkan Besaran Risiko SPBE. Apabila terdapat lebih dari satu Risiko SPBE yang memiliki besaran yang sama maka cara penentuan prioritas berdasarkan *expert judgement*.

D. Penanganan Risiko SPBE

Penanganan Risiko SPBE merupakan proses untuk memodifikasi penyebab Risiko SPBE. Penanganan Risiko SPBE dilakukan dengan mengidentifikasi berbagai opsi yang mungkin diterapkan dan memilih satu atau lebih opsi penanganan Risiko SPBE. Informasi yang dicantumkan pada penanganan Risiko SPBE meliputi :

1. Prioritas Risiko

Prioritas Risiko SPBE diurutkan berdasarkan Besaran Risiko SPBE. Risiko SPBE yang memiliki prioritas lebih tinggi ditunjukkan dengan nilai Besaran Risiko SPBE yang lebih tinggi.

2. Rencana Penanganan Risiko SPBE

Rencana penanganan Risiko SPBE merupakan agenda kegiatan untuk menangani Risiko SPBE agar mencapai Selera Risiko SPBE yang telah ditetapkan. Rencana penanganan Risiko SPBE dilakukan dengan mengidentifikasi hal-hal sebagai berikut:

a. Opsi Penanganan Risiko SPBE

Opsi penanganan Risiko SPBE, berisikan alternatif yang dipilih untuk menangani Risiko SPBE. Opsi penanganan Risiko SPBE dilakukan dengan mengidentifikasi berbagai opsi yang mungkin untuk diterapkan. Opsi penanganan Risiko SPBE

terbagi menjadi dua, yaitu penanganan Risiko SPBE Positif dan penanganan Risiko SPBE Negatif.

Adapun opsi yang ditentukan pada pedoman ini meliputi:

1) Opsi Penanganan Risiko Positif
   a) Eskalasi Risiko

      Eskalasi risiko dipilih jika Risiko SPBE berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan Risiko SPBE ke unit kerja yang lebih tinggi.
   b) Eksploitasi Risiko

      Eksploitasi risiko dipilih jika Risiko SPBE dapat dipastikan terjadi. Opsi ini dilakukan dengan cara memanfaatkan Risiko SPBE tersebut semaksimal mungkin.
   c) Peningkatan Risiko

      Peningkatan risiko dilakukan dengan cara meningkatkan level kemungkinan dan/atau level dampak dari Risiko SPBE.
   d) Pembagian Risiko

      Pembagian risiko dipilih jika Risiko SPBE tidak dapat ditangani secara langsung dan membutuhkan pihak lain untuk menangani Risiko SPBE tersebut. Pembagian risiko dilakukan dengan bekerja sama dengan dengan pihak lain.
   e) Penerimaan Risiko

      Penerimaan risiko dipilih jika upaya penanganan lebih tinggi dibandingkan manfaat yang didapat atau kemungkinan terjadinya kecil. Opsi ini dilakukan dengan cara membiarkan Risiko SPBE terjadi apa adanya.
2) Opsi Penanganan Risiko Negatif
   a) Eskalasi Risiko

      Eskalasi risiko dipilih jika Risiko SPBE berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan Risiko SPBE ke unit kerja yang lebih tinggi.
   b) Mitigasi Risiko

      Mitigasi risiko dilakukan dengan cara mengurangi level kemungkinan dan/atau level dampak dari Risiko SPBE.
   c) Transfer Risiko

Transfer risiko dipilih jika terdapat kekurangan sumber daya untuk mengelola Risiko SPBE. Opsi ini dilakukan dengan cara mengalihkan kepemilikan risiko kepada pihak lain untuk melakukan pengelolaan dan pertanggungjawaban terhadap Risiko SPBE.

d) Penghindaran Risiko

Penghindaran risiko dilakukan dengan mengubah perencanaan, penganggaran, program, dan kegiatan, atau aspek lainnya untuk mencapai sasaran SPBE.

e) Penerimaan Risiko

Penerimaan risiko dipilih jika biaya dan usaha penanganan lebih tinggi dibandingkan manfaat yang didapat, kemungkinan terjadinya sangat kecil atau dampak sangat tidak signifikan. Opsi ini dilakukan dengan cara membiarkan risiko terjadi apa adanya.

b. Rencana Aksi Penanganan Risiko

Rencana aksi penanganan risiko merupakan rancangan kegiatan tindak lanjut untuk menangani Risiko SPBE.

c. Keluaran

Keluaran merupakan hasil dari rencana aksi penanganan Risiko SPBE.

d. Jadwal Implementasi

Jadwal implementasi merupakan jadwal pelaksanaan dari setiap rencana aksi penanganan Risiko SPBE.

e. Penanggung Jawab

Penanggung jawab berisikan nama unit yang bertanggung jawab dan unit pendukung dari setiap rencana aksi penanganan Risiko SPBE.

3. Risiko Residual

Risiko residual merupakan Risiko SPBE yang tersisa dari Risiko SPBE yang telah ditangani. Dalam melakukan penanganan terhadap risiko residual, dilakukan pengulangan proses penilaian risiko sampai dengan risiko residual tersebut berada di bawah Selera Risiko SPBE. Penetapan risiko residual ini dapat ditetapkan berdasarkan *expert judgement*.

E. Pemantauan dan Reviu

Pemantauan bertujuan untuk memonitor faktor-faktor atau penyebab yang mempengaruhi Risiko SPBE dan kondisi lingkungan Instansi Pusat dan Pemerintah

Daerah. Selain itu, pemantauan dilakukan guna memonitor pelaksanaan rencana aksi penanganan Risiko SPBE. Hasil pelaksanaan pemantauan dapat menjadi dasar untuk melakukan penyesuaian kembali proses Manajemen Risiko SPBE. Pemantauan dilakukan berdasarkan setiap triwulan, semester, tahun, atau sewaktu-waktu (insidental) sesuai dengan kesepakatan dari Instansi Pusat dan Pemerintah Kabupaten Natuna.

Reviu bertujuan untuk mengontrol kesesuaian dan ketepatan seluruh pelaksanaan proses Manajemen Risiko SPBE sesuai dengan ketentuan yang berlaku. Reviu dilakukan sesuai dengan kesepakatan dari masing-masing Instansi Pusat dan Pemerintah Daerah.

F. Pencatatan dan Pelaporan

Pencatatan merupakan kegiatan atau proses pendokumentasian suatu aktivitas dalam bentuk tulisan dan dituangkan dalam dokumen. Pelaporan merupakan kegiatan yang dilakukan untuk menyampaikan hal-hal yang berhubungan dengan hasil pekerjaan yang telah dilakukan selama satu periode tertentu.

Proses Manajemen Risiko SPBE dan keluaran yang dihasilkan perlu dicatat dan dilaporkan dengan mekanisme yang tepat. Pencatatan dan pelaporan bertujuan untuk mengkomunikasikan aktivitas Manajemen Risiko SPBE serta keluaran yang dihasilkan, menyediakan informasi untuk pengambilan keputusan, meningkatkan kualitas aktivitas Manajemen Risiko SPBE, serta mengawal interaksi dengan pemangku kepentingan termasuk tanggung jawab serta akuntabilitas terhadap Manajemen Risiko SPBE.

Pencatatan dan pelaporan Manajemen Risiko SPBE terdiri dari:

1. Pencatatan dan Pelaporan Periodik

   Pencatatan dan pelaporan periodik merupakan kegiatan yang dilakukan secara berulang pada waktu yang telah ditentukan.
2. Pencatatan dan Pelaporan Insidental

   Pencatatan dan pelaporan insidental merupakan kegiatan yang dilakukan pada waktu tertentu sesuai dengan kebutuhan.

G. Dokumen Manajemen Risiko SPBE

1. Pakta Integritas Manajemen Risiko SPBE

Pakta Integritas Manajemen Risiko SPBE merupakan dokumen pernyataan atau janji untuk berkomitmen menjalankan Manajemen Risiko SPBE di Pemerintah Kabupaten Natuna. Dokumen Pakta Integritas dapat dilihat pada Formulir 1.0 Pakta Integritas.

2. Dokumen Proses Risiko SPBE

   Dokumen Proses Risiko SPBE merupakan dokumen pendukung pelaksanaan proses penetapan konteks, penilaian, dan penanganan Risiko SPBE. Dokumen Proses Risiko SPBE terdiri dari:

   a. Formulir Konteks Risiko SPBE

      Formulir Konteks Risiko SPBE merupakan dokumen dari aktivitas penetapan konteks pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 2.0.

   b. Formulir Penilaian Risiko SPBE

      Formulir Penilaian Risiko SPBE merupakan dokumen dari aktivitas penilaian Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 3.0.

   c. Formulir Rencana Penanganan Risiko SPBE

      Formulir Rencana Penanganan Risiko SPBE merupakan dokumen dari aktivitas penanganan Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 4.0.

3. Dokumen Proses Pengendalian Risiko SPBE

   Dokumen Proses Pengendalian Risiko SPBE merupakan dokumen pendukung pelaksanaan proses komunikasi dan konsultasi, serta pelaporan Risiko SPBE. Dokumen Proses Pengendalian Risiko SPBE terdiri dari:

   a. Dokumen Kegiatan Komunikasi dan Konsultasi

      Dokumen Kegiatan Komunikasi dan Konsultasi merupakan dokumen dari aktivitas pelaksanaan kegiatan komunikasi dan konsultasi. Dokumen dapat berbentuk notulensi dan laporan atau dokumen lainnya yang dihasilkan dari pelaksanaan kegiatan komunikasi dan konsultasi.

   b. Dokumen Laporan Pemantauan

      Dokumen Laporan Pemantauan merupakan dokumen dari aktivitas pelaksanaan kegiatan pemantauan Risiko. Dalam pedoman ini menggunakan 2 format laporan yaitu laporan pemantauan triwulan dan laporan pemantauan tahunan.

      Laporan pemantauan triwulan menggambarkan kondisi pelaksanaan dalam waktu setiap tiga bulan terkait rencana aksi penanganan yang meliputi besaran/level

Risiko SPBE saat ini dan proyeksi Risiko SPBE, penanganan yang telah dilakukan, rencana penanganan, penanggung jawab, dan waktu pelaksanaan.

Laporan pemantauan tahunan merangkum laporan triwulan I sampai dengan triwulan IV dengan berfokus pada tendensi besaran Risiko SPBE dan memberikan rekomendasi penanganan Risiko SPBE yang dapat digunakan sebagai masukan pelaksanaan proses Manajemen Risiko SPBE pada tahun selanjutnya.

Pada alur proses pelaksanaan manajemen resiko, terdapat 4 pilihan penanganan terhadap risiko potensial, yaitu:

1. Take: Jika risiko yang ada dirasakan cukup besar dan tidak dapat dihindari, sehingga perusahaan dapat mengalami dampak yang mengganggu dan bersifat merusak secara alamiah, maka diambil tindakan "*Take*" atau menerima risiko tersebut.
2. Treat: Jika risiko yang ada dirasakan dapat ditanggapi dengan tindakan untuk menurunkan tingkat risikonya, maka diambil tindakan "*Treat*" untuk mengontrol risiko tersebut. Tindakan nyatanya adalah dengan menerapkan kontrol atau mitigasi terhadap risiko yang ada sehingga risiko tersebut dapat diturunkan levelnya.
3. *Terminate* : Jika risiko yang ada dirasakan terlalu besar, maka dapat diambil tindakan "*Terminate*" terhadap risiko tersebut, artinya kita harus menghindar dan tidak mau mengambil risiko dengan membuat produk baru tersebut, sehingga tindakan nyatanya adalah membatalkan rencana pembuatan produk.
4. Transfer: Jika risiko yang ada dianggap akan lebih baik jika dialihkan ke pihak lain yang sesuai dengan bidang ahlinya, maka dapat diambil tindakan "*Transfer*" terhadap risiko tersebut.

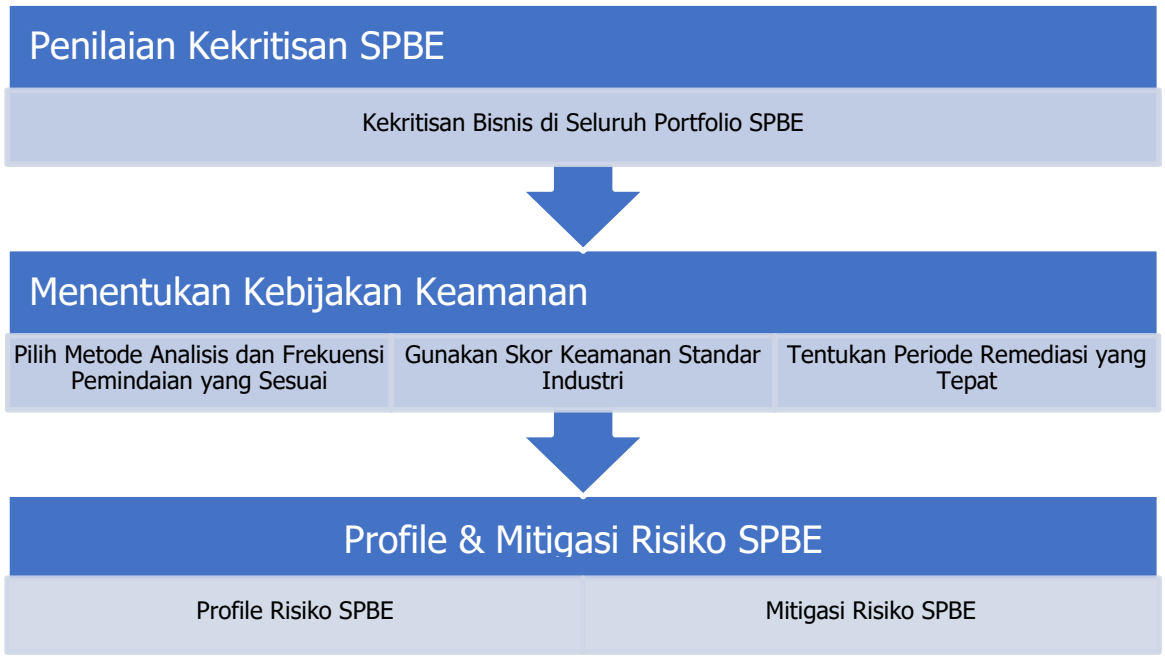
Langkah yang dilakukan dalam pengelolaan risiko terdiri dari:

1. Penilaian Risiko SPBE: Menilai Kekritisan Bisnis di Seluruh Portfolio SPBE
2. Menentukan Kebijakan Keamanan Aplikasi

Kekritisan bisnis yang dipilih untuk suatu aplikasi menentukan kebijakan keamanan aplikasi yang diperlukan untuk aplikasi tersebut. Mendefinisikan kebijakan keamanan aplikasi terdiri dari langkah-langkah berikut:

1. Pilih Metode Analisis dan Frekuensi Pemindaian yang Sesuai
2. Gunakan Skor Keamanan Standar Industri
3. Tentukan Periode Remediasi yang Tepat

Uraian diatas dapat digambarkan dalam diagram berikut ini:



Gambar 5. 2 Pengelolaan Risiko Kebijakan Keamanan Informasi

5.2 Manajemen Keamanan Informasi

Manajemen Keamanan Informasi sekurang-kurang meliputi:

1. **Kebijakan Keamanan Informasi**

   Kebijakan Keamanan Informasi akan memberikan panduan dalam membangun, mengimplementasikan, mengoperasikan, memonitor, memelihara dan meningkatkan SMKI di Pemerintah Daerah.

   Ruang Lingkup Kebijakan Sistem Manajemen Keamanan Informasi adalah mencakup semua proses yang terangkum dalam proses implementasi SMKI yang dijalankan di Pemerintah Daerah.

2. **Standar Keamanan Informasi**

   Standard keamanan informasi dirancang dan diimplementasikan untuk mengurangi kemungkinan dan/atau mengurangi dampak dari risiko keamanan informasi. Perancangan dan implementasi dari Standard tersebut dilakukan dengan menimbang metode untuk menjaga aspek kerahasiaan, integritas dan ketersediaan dari informasi organisasi.

   Standard ini dibuat sebagai panduan dan arahan untuk kontrol keamanan informasi yang diimplementasikan di Pemerintah Daerah

Standard Keamanan Informasi ini berlaku bagi seluruh personil, informasi, aset pengolahan informasi beserta sarana pendukungnya dalam ruang lingkup SMKI di Pemerintah Daerah

3. **Prosedur Tinjauan Manajemen**

   Untuk menjamin kesesuaian, kecukupan dan efektifitas dari SMKI di organisasi, manajemen puncak Pemerintah Daerah perlu untuk secara periodik memantau dan meninjau kondisi dan operasi dari SMKI di organisasi. Prosedur ini ditetapkan untuk memberikan panduan untuk proses tinjauan manajemen SMKI di Pemerintah Daerah. Prosedur ini berlaku untuk proses tinjauan manajemen SMKI di Pemerintah Daerah berdasarkan ISO/IEC 27001:2013 - Klausul 9.3. Tinjauan Manajemen.

4. **Prosedur Penanganan Ketidaksesuaian dan Peningkatan SMKI**

   Untuk memastikan pengelolaan ketidaksesuaian SMKI dengan baik, dokumen ini dibuat sebagai pedoman formal dalam proses indentifikasi, analisis ketidaksesuaian dan pengambilan tindakan korektif dan peningkatan yang tepat. Hal ini diperlukan untuk memastikan kesesuaian dari prasyaratan SMKI perusahaan serta untuk memastikan peningkatan yang berkelanjutan pada Pemerintah Daerah. Kebijakan dan prosedur ini berlaku untuk proses penanganan ketidaksesuaian dan peningkatan SMKI di Pemerintah Daerah. Referensi yang digunakan adalah:

   - ISO/IEC 27001:2013 Klausul 10.1.Ketidaksesuaian dan tindakan korektif.
   - ISO/IEC 27001:2013 Klausul 10.2. Peningkatan secara berkesinambungan. Kebijakan SMKI Pemerintah Daerah

5. **Prosedur Peningkatan Komunikasi SMKI**

   Prosedur ini ditetapkan sebagai panduan untuk menjaga tingkat pemahaman SMKI yang memadai dan mengelola komunikasi terkait SMKI. Kebijakan dan prosedur ini berlaku untuk proses peningkatan pemahaman SMKI dan proses komunikasi SMKI di Pemerintah Daerah. Referensi yang digunakan adalah:

   - ISO/IEC 27001:2013 Klausul 7.2. Kompetensi.
   - ISO/IEC 27001:2013 Klausul 7.3. Kesadaran/Pemahaman (Awareness)
   - ISO/IEC 27001:2013 Klausul 7.4. Komunikasi.

6. **Prosedur Pengendalian Dokumen**

   Untuk menjamin pengendalian yang memadai dari dokumentasi SMKI, prosedur ini disusun sebagai panduan dalam pengelolaan dokumentasi SMKI. Prosedur ini berlaku untuk seluruh dokumentasi SMKI dalam bentuk hardcopy maupun softcopy. Referensi : ISO/IEC 27001:2013-Klausul 7.5. Documented information.

7. **Prosedur Audit Internal**

Untuk menjamin kepatuhan dan efektifitas dari SMKI, proses audit internal SMKI harus dilakukan. Prosedur ini ditetapkan untuk memberikan panduan untuk proses audit internal SMKI di Pemerintah Daerah. Prosedur ini berlaku untuk proses audit internal SMKI di LPSE, Referensi yang digunakan adalah ISO/IEC 27001:2013 - Klausul 9.2. Audit Internal.

8. **Prosedur Pengelolaan Ruang Server**

Prosedur ini bertujuan untuk mencapai dan memelihara sistem perlindungan yang tepat terhadap aset server dan sarana pendukung pada Ruang Server di Pemerintah Daerah. Prosedur ini mengatur pengelolaan Ruang Server yang terdapat di Pemerintah Daerah yang meliputi pengamanan akses fisik Ruang Server, pemeliharaan Ruang Server. Referensi yang digunakan adalah:

- ISO/IEC 27001:2013 Annex A.11.1.2 – Pengendalian Akses Masuk Secara Fisik.
- ISO/IEC 27001:2013 Annex A.11.1.5 - Bekerja di Wilayah Aman.
- ISO/IEC 27001:2013 Annex A.11.2.1 – Penempatan dan Perlindungan Perangkat.
- ISO/IEC 27001:2013 Annex A.11.2.4 – Pemeliharaan Perangkat.
- ISO/IEC 27001:2013 Annex A.11.2.2 – Utilitas Pendukung.

9. **Prosedur Instalasi Software**

Prosedur ini bertujuan untuk mengatur mengenai pengelolaan Software dalam rangka kebutuhan pelaksanaan tugas pokok pegawai di Pemerintah Daerah.

Prosedur ini mengatur bagaimana melakukan permohonan instalasi Software pada PC/notebook pegawai dan memonitor Software yang berlisensi atau yang terotorisasi di Pemerintah Daerah. Software yang diatur dalam prosedur ini mencakup Software berlisensi, driver, freeware, dan Software trial. Referensi yang digunakan adalah:

- ISO/IEC 27001:2013 – Annex A.12.5.1. Instalasi Perangkat Lunak pada Sistem Operasional.
- ISO/IEC 27001:2013 – Annex A.18.1.2. Hak atas kekayaan intelektual.

10. **Prosedur Pengelolaan Insiden**

Prosedur ini bertujuan sebagai pedoman dalam menangani insiden keamanan informasi yang terjadi di Pemerintah Daerah agar dampak terjadinya insiden dapat diminimalisir dan mencegah terulangnya insiden. Prosedur ini mengatur bagaimana melakukan penanganan dan evaluasi insiden keamanan informasi di Pemerintah Daerah yang mempengaruhi proses bisnis. Referensi yang digunakan adalah:

- ISO/IEC 27001:2013 Annex A.16.1.1 – Tanggung Jawab dan Prosedur
- ISO/IEC 27001:2013 Annex A.16.1.2 – Pelaporan Kejadian (event) Keamanan Informasi.
- ISO/IEC 27001:2013 Annex A.16.1.3 – Pelaporan Kelemahan dan Keamanan Informasi.

11. Prosedur Manajemen Perubahan

Prosedur ini bertujuan untuk memastikan bahwa setiap pengubahan terhadap perangkat infrastruktur dan aplikasi di Pemerintah Daerah dilakukan secara terkendali. Ruang lingkup dalam prosedur ini adalah proses mulai dari pencatatan hingga persetujuan pengubahan perangkat dan aplikasi di Pemerintah Daerah. Referensi yang digunakan adalah ISO/IEC 27001:2013 – Annex A.12.1.2 – Manajemen Perubahan.

12. Prosedur Pengamanan Pihak Ketiga

Tujuan dari prosedur ini adalah untuk mengatur pelaksanaan layanan yang diberikan pihak ketiga kepada Pemerintah Daerah agar terkendali. Ruang lingkup dari penerapan prosedur ini adalah untuk mengatur pengamanan personil pihak ketiga dan monitoring pelayanan pihak ketiga yang melakukan pekerjaan di lingkungan Pemerintah Daerah. Referensi yang digunakan adalah:

- ISO 27001:2013 – Annex A.15.1.1 – Kebijakan keamanan informasi dalam hubungan dengan pemasok.
- ISO 27001:2013 – Annex A.15.2.1 – Pemantauan dan peninjauan layanan dari pemasok.

13. Prosedur Penanganan Informasi

Prosedur ini bertujuan untuk memberikan arahan dalam perlindungan dan penanganan informasi khususnya yang bersifat rahasia di lingkungan Pemerintah Daerah. Prosedur ini mengatur proses inventarisasi, distribusi, pemusnahan, peminjaman, dan back-up informasi yang bersifat rahasia. Referensi yang digunakan adalah:

- ISO/IEC 27001:2013 - Annex 8.2.2 Pelabelan Informasi.
- ISO/IEC 27001:2013 - Annex 8.2.3 Pengendalian aset.
- ISO/IEC 27001:2013 - Annex 13.2.1 Prosedur dan Kebijakan transfer informasi.

14. **Prosedur Pengelolaan Aset**

Untuk memberikan arahan dalam pengelolaan dan perlindungan terhadap aset pengolahan informasi di lingkungan Pemerintah Daerah. Prosedur ini mengatur proses pencatatan, pemeliharaan, perbaikan, dan pemusnahan aset di Pemerintah Daerah Aset yang diatur untuk pengolahan informasi meliputi PC, Notebook, Flashdisk. Referensi yang digunakan adalah:

- ISO/IEC 27001:2013 – Annex 8.3.2 Pembuangan Media.
- ISO/IEC 27001:2013 – Annex 8.1.1 Inventarisasi Aset.
- ISO/IEC 27001:2013 – Annex 8.3.1 Management Removable Media.
- ISO/IEC 27001:2013 – Annex 8.2.3 Penanganan Aset

15. **Prosedur Pengembangan Aplikasi**

Prosedur ini disusun sebagai panduan dalam pengelolaan keamanan informasi dalam proses akuisisi, pengembangan dan pemeliharaan dari aplikasi perusahaan. Kebijakan dan prosedur ini berlaku untuk seluruh akuisisi, pengembangan dan pemeliharaan dari aplikasi dalam ruang lingkup SMKI di Pemerintah Daerah. Referensi yang digunakan adalah:

- ISO 27001:2013 Annex 14.1. Prasyarat keamanan dari sistem informasi.
- ISO 27001:2013 Annex 14.2. Pengamanan dari proses pengembangan dan support
- ISO 27001:2013 Annex 14.3. Data pengujian. Kebijakan SMKI Pemerintah Daerah

16. **Matriks Pengendalian Akses**

Prosedur ini bertujuan sebagai panduan dalam pengendalian dan pengalokasian akses pengguna ke sistem informasi milik Pemerintah Daerah. Matriks ini berlaku untuk sistem informasi dalam ruang lingkup SMKI di Pemerintah Daerah. Referensi yang digunakan adalah:

- ISO/IEC 27001:2013 Annex A.9.1.1 – Kebijakan pengendalian akses
- Standard Keamaan Informasi.

5.3 Manajemen Data

Manajemen Data meliputi beberapa praktek yaitu:

1. **Pengaturan**

Pengaturan dalam pengelolaan data didasarkan pada Undang-undang No 82 tahun 2012.

2. **Administrasi**

Praktek Administrasi Data terdiri dari beberapa praktek yaitu:

A. Kepemilikan Data

1. Data yang dikumpulkan oleh Unit Organisasi manapun pada akhirnya menjadi milik organisasi seperti harus tersedia untuk berbagi dengan Unit Organisasi lainnya, dalam batasan-batasannya undang-undang, kebijakan dan peraturan yang ada.
2. Unit Organisasi Pemilik Sumber Data harus memasukkan proses pemeliharaan data termasuk menangani pembaruan data dan penyebarluasan data kepada Pengguna Data pada Unit Organisasi lainnya.
3. Untuk memastikan integritas data di seluruh Direktorat Jenderal Pemerintah, Unit Organisasi harus mengumpulkan data terlebih dahulu yang diperlukan untuk menyelesaikan transaksi layanan yang dilakukan, jika tersedia. Jika tidak ada, maka Unit Organisasi yang memerlukan data dapat mengumpulkan data dari sumber lain yang valid.

B. Pengumpulan Data

1. Unit Organisasi harus memastikan bahwa semua informasi atau catatan disimpan secara elektronik sistem mereka, diklasifikasikan dan diamankan sesuai Peraturan yang berlaku dan memenuhi standar serta kesesuaian dengan Arsitektur Enterprise. Unit Organisasi juga harus membuat dan memelihara daftar tersebut data kunci dan aset informasi.
2. Unit Organisasi harus memastikan bahwa data dikumpulkan dengan cara yang sah dan adil, dan terbatas pada apa yang diperlukan sesuai persyaratan pemenuhan kebutuhan tugas pokok dan fungsi. Kebijakan ini mengatur apakah sumber data yang diperlukan harus bersumber dari Unit Organisasi lainnya atau harus mengumpulkan dari sumber lainnya yang sah.
3. Unit Organisasi harus meminta informasi atau dokumen pendukung yang berasal dari individu atau bisnis yang diperlukan untuk memproses layanan transaksi hanya jika informasi tersebut tidak tersedia secara elektronik atau tidak tersedia di lokasi berbagi data dari unit organisasi pemerintah lainnya.
4. Unit Organisasi harus memastikan bahwa informasi data pribadi yang bersifat individu sudah dipahami oleh individu tersebut dan memberikan persetujuan atas pengumpulan, penggunaan atau pengungkapan Data Pribadi tersebut ke Pihak Ketiga atau Badan lain untuk tujuan pelayanan pemrosesan transaksi.

5. Unit Organisasi harus melakukan tinjauan untuk mengidentifikasi layanan di mana pengajuan dokumen dan pengisian formulir oleh individu dan bisnis dapat dihilangkan atau dikurangi menjadi minimal:
    a. melakukan review untuk menentukan apakah informasi atau dokumen diperlukan memproses layanan atau transaksi tertentu;
    b. mempertimbangkan cara alternatif sumber informasi melalui:
        i. sumber informasi yang dibutuhkan secara internal dari repositori dan database;
        ii. mencari verifikasi yang dibutuhkan dan / atau data yang dibutuhkan secara eksternal dari sumber data yang berasal dari Unit Organisasi lainnya;
        iii. mengotomatisasi proses tersebut dari sumber informasi internal atau eksternal;

C. Standar Data

Standar data adalah dasar untuk interoperabilitas. Penerapan satu set data standar untuk penggunaan di seluruh Unit Organisasi Pemerintah akan menghilangkan ambiguitas dan ketidakkonsistenan penggunaan data dan memungkinkan penggunaan dan pertukaran data yang lebih efektif.

1. Setiap Unit Organisasi bertanggung jawab untuk menetapkan dan memelihara katalog standar data yang harus menyertakan informasi metadata dan standar untuk datanya dalam format standar Katalog standar data juga membantu membentuk Unit Organisasi pemilik bisnis untuk data tertentu.
2. Unit Organisasi harus menyebarkan katalog standar data kepada petugas yang berwenang di Unit Organisasi Pemerintah lainnya untuk mengetahui ketersediaan data dan metadata informasi dan standar.
3. Pengguna Data harus menggunakan standar data dari Unit Organisasi Pemilik Sumber data sesuai dengan elemen data yang diberikan.
4. Unit Organisasi Pemilik Sumber Data bertanggung jawab untuk memperbarui standar datanya katalog dengan atribut baru atau yang diperbarui dan beri tahu pemangku kepentingan di seluruh Kementerian Keuangan untuk semua revisi.

D. Akses Data

Akses data hanya diberikan kepada individu dan Unit Organisasi yang memiliki legitimasi dan alasan yang dapat dibenarkan untuk akses, dalam batas-batas hukum, kebijakan dan kebijakan serta peraturan yang relevan:

1. Unit Organisasi harus membedakan secara jelas antara item data untuk akses terkontrol dari item untuk akses terbuka yang tergolong publik sesuai dengan undang-undang dan peraturan yang berlaku.
2. Unit Organisasi harus menempatkan kontrol untuk memastikan akses terhadap data yang terkendali hanya diberikan kepada individu, badan atau lembaga lain yang memiliki legitimasi dan alasan yang dapat dibenarkan untuk akses semacam itu, serta izin persetujuan yang tepat.

E. Perlindungan

1) Perlindungan Informasi dan Data

1. Unit Organisasi harus melindungi semua informasi dan data yang dimilikinya (termasuk data diterima dari Lembaga lain), atau saat mengungkapkan data ke Pihak Ketiga atau pihak lainnya Unit Organisasi. Pengaman keamanan harus dilakukan untuk melindungi data terhadap apapun akses tidak sah, dan pengungkapan atau modifikasi.
2. Unit Organisasi harus mematuhi Undang-undang. Peraturan dan Kebijakan yang berlaku untuk memastikan pengamanan yang memadai tersedia untuk melindungi sistem dan elektronik apa pun media penyimpanan yang menangani data untuk mencegah akses yang tidak sah, atau modifikasi data.
3. Unit Organisasi harus melakukan penelaahan berkala terhadap kebijakan dan proses mereka untuk memastikannya pengamanan data yang memadai, dan melakukan audit berkala untuk memastikan bahwa Langkah-langkah untuk menjaga data sesuai dengan kebijakan.
4. Unit Organisasi harus memastikan bahwa proses telah dilakukan untuk melindungi kerahasiaan dan integritas data yang diperoleh dari Unit Organisasi lain.
5. Unit Organisasi harus memastikan bahwa semua aset data dan informasi diklasifikasikan dan disimpan sesuai dengan tingkat keamanan mereka (rujukan dapat dilakukan pada Undang-undang. Peraturan dan Kebijakan yang berlaku).

2) Perlindungan Data Pribadi

Unit Organisasi harus mematuhi prinsip privasi informasi dan hukum yang berlaku mulai dari proses pengumpulan, pengolahan dan pembagian.

1. Unit Organisasi juga harus memastikan kebijakan dan proses untuk melindungi Data Pribadi terbaru dan dipatuhi secara ketat untuk semua pemrosesan data di dalam Unit Organisasi dan saat mentransfer atau berbagi data dengan Unit Organisasi lain atau ke Pihak Ketiga.
2. Unit Organisasi harus memastikan bahwa kebijakan dan proses yang ditetapkan terkait dengan pemrosesan Data Pribadi meliputi:
   (a) Data Pribadi yang dimiliki oleh Badan atau yang disediakan untuk Lembaga lain diperlukan untuk memenuhi persyaratan hukum atau peraturan, atau untuk kepentingan layanan publik;
   (b) Informasi lebih rinci dari data pribadi yang diperlukan oleh Unit Organisasi atau pengungkapan data pribadi oleh Unit Organisasi lainnya
   (c) Rincian kontak staff yang bertanggung jawab atas informasi yang bersifat pribadi
3. Unit Organisasi harus menerbitkan/menyampaikan syarat dan ketentuan untuk penayangan data pribadi dalam situs web yang dimiliki.
4. Unit Organisasi harus menerapkan proses untuk membuang atau menghancurkan Data Pribadi secara aman sehingga mencegah pihak yang tidak berwenang memperoleh akses terhadap data ini.

F. Pemanfaatan dan Berbagi Data

1) Berbagi Data

Unit Organisasi tidak boleh mengumpulkan data dari masyarakat jika data tersedia dari Unit Organisasi pemerintah lainnya. Ini akan memastikan bahwa masyarakat hanya perlu menyediakan data hanya sekali kepada unit organisasi pemerintah untuk mendapatkan berbagai layanan; sehingga memastikan satu sumber kebenaran, dan akurasi data dan integritas.

1. Unit Organisasi Pemilik Sumber Data harus membagikan data yang diambil atau dibuat dengan Lembaga lain sesuai dengan kewajiban hukum dan privasi, jika ada tujuan berbagi yang jelas dan benar.

2. Unit Organisasi harus mendapatkan persetujuan dari orang-orang dalam bentuk Salinan hard copy atau layanan online, untuk kepentingan penggunaan kembali dan berbagi data pribadi untuk tujuan penyediaan layanan pemerintah kepada mereka. Persetujuan tersebut dapat berupa pernyataan bahwa dengan mengajukan permohonan layanan yang diminta, pemohon selanjutnya mengizinkan untuk berbagi dan menggunakan kembali data pribadinya antara Unit Organisasi.
3. Untuk penggunaan kembali atau berbagi data tersebut untuk tujuan selain penyediaan layanan, Unit Organisasi harus mencari persetujuan individu untuk tujuan tertentu tersebut.
4. Unit Organisasi pemilik Sumber Data harus memfasilitasi dan memungkinkan pembagian data dengan pengguna data Unit Organisasi lainnya sehingga masyarakat dapat:
   (a) Memberikan kenyamanan yang lebih besar kepada individu dan masyarakat (sehingga hanya perlu memasok data sekali ke Unit Organisasi di Pemerintah untuk mendapatkan berbagai layanan publik, daripada harus menyediakan data yang sama ke berbagai Lembaga untuk berbagai transaksi);
   (b) mengembangkan kebijakan yang lebih tepat sasaran dan informasi melalui akses terhadap data kualitas yang lebih baik dan lebih baik; dan
   (c) meningkatkan efisiensi dan mengurangi biaya melalui peningkatan berbagi data.

2) Tujuan Pemanfaatan Data

Unit Organisasi harus berbagi data satu sama lain hanya untuk tujuan yang jelas dan benar.

1. Unit Organisasi Pengguna Data harus menetapkan tujuan yang jelas ke Unit Organisasi pemilik Sumber Data, kecuali pemanfaatan Data telah disetujui sebelumnya untuk digunakan untuk tujuan bersama.
2. Unit Organisasi Pengguna Data hanya menggunakan data untuk tujuan yang ditentukan.
3. Apabila sesuai, kesepakatan berbagi data harus dibuat untuk mengikat semua pihak yang terlibat dalam berbagi. Seperti kesepakatan berbagi data harus mencakup: tujuan berbagi data, organisasi yang terlibat,

kumpulan data / item yang akan dibagi, peraturan untuk retensi dan penghapusan item data bersama, prosedur untuk menangani penghentian perjanjian berbagi data.

3) Berbagi di Internal Pemerintah

1. Data yang dikumpulkan atau dihasilkan oleh Unit Organisasi harus dibagi dengan Lembaga lain, sesuai batas yang diizinkan oleh hukum yang berlaku dan prinsip privasi data, untuk memungkinkan Unit Organisasi pemerintah mencapai tujuan:
   (a) memberikan layanan *customer-centric*;
   (b) mencapai perumusan kebijakan mutu;
   (c) memfasilitasi analisis dan penelitian.
2. Untuk data sensitif, Unit Organisasi pemilik Sumber Data harus bekerja dengan Unit Organisasi Pengguna Data untuk menentukan jumlah minimum data yang diperlukan untuk memenuhi kebutuhan pengguna sambil memastikan perlindungan yang memadai tersedia untuk melindungi data; misalnya dengan menentukan apakah tujuannya bisa dicapai dengan menganonimkan mereka.
3. Data yang akan dibagi harus dibatasi sesuai dengan spesifikasi dana permintaan.
4. Bila memungkinkan, Unit Organisasi Pengguna Data harus mematuhi standar data. Unit Organisasi pemilik Sumber data harus memastikan ketersediaan data secara mudah.
5. Standar data dari Unit Organisasi pemilik Sumber Data apabila terjadi ketidaksesuaian dalam proses pertukaran atau pengiriman layanan kepada Unit Organisasi Pengguna Data berdasarkan alasan yang sah dan dapat dibenarkan, pihak pertama harus memperbarui standar data yang berlaku dan sesegera mungkin menyediakan data dalam format yang disepakati. Dalam jangka waktu yang ditentukan.
6. Unit Organisasi yang terlibat dalam berbagi data harus menerapkan proses penanganan pembaruan data dan umpan balik terkait kualitas data.
7. Unit Organisasi harus menetapkan dengan jelas kondisi penggunaan, penanganan dan pembuangan data sebelum data dimanfaatkan oleh Unit

Organisasi Pengguna Data, termasuk periode retensi dan pengaturan penghapusan data baik yang dikirim ataupun yang diterima.

8. Unit Organisasi Pengguna Data tidak boleh berbagi data dengan Unit Organisasi lain tanpa persetujuan eksplisit dari Unit Organisasi Pemilik Sumber Data, kecuali jika diberi wewenang atau yang disahkan oleh undang-undang atau keputusan, atau data telah disetujui sebelumnya untuk digunakan untuk semua keperluan oleh Unit Organisasi pemilik sumber data.
9. Unit Organisasi pemilik Sumber Data akan membagikan semua data yang sudah disetujui sebelum untuk digunakan berbagai tujuan melalui Platform Integrasi Data sebagai layanan pertukaran data yang dapat digunakan kembali oleh Unit Organisasi.

4) Berbagi Data Publik

1. Unit Organisasi hanya membagikan Data non-pribadi dengan masyarakat umum dalam lingkup undang-undang, kebijakan, dan peraturan yang relevan.
2. Jika data tersebut tidak dimiliki oleh Unit Organisasi, maka sebelumnya harus meminta persetujuan dari Unit Organisasi Pemilik Sumber Data sebelum menayangkan data tersebut ke masyarakat umum kecuali jika diberi wewenang atau disahkan oleh undang-undang atau keputusan.

G. Pusat Pertukaran

1. Organisasi harus membuat dan memelihara Platform Pertukaran/Integrasi Data yang memungkinkan Unit Organisasi untuk berbagi dan mengakses data yang tersedia untuk memberikan layanan publik, dan yang terdiri dari komponen inti berikut:
   (a) Infrastruktur TI - platform pertukaran data pemerintah yang aman yang memungkinkan Unit Organisasi pemilik Sumber Data membagikan data, lalu Unit Organisasi Pengguna Data dapat mencari dan meminta data yang tersedia;
   (b) Katalog Standar Data - menyusun dan memperbaharui kamus data yang ada dari semua Unit Organisasi, sebagaimana didefinisikan arsitektur data, yang mencakup informasi dan standar metadata;

(c) Manajemen & Tata Kelola Platform - menetapkan struktur dan proses pemerintahan untuk mengawasi penggunaan data yang efektif dan efisien antar Unit Organisasi pemerintah termasuk Persyaratan Penggunaan dan Akses yang Berlaku, SLA, dll.

2. Semua Unit Organisasi harus berbagi dan bertukar data dengan Unit Organisasi lainnya melalui Platform Pertukaran/Integrasi dengan pengaturan saat dan kapan pelaksanaannya berjalan, mematuhi proses dan standar yang berlaku.

H. Pengawasan dan Evaluasi

Pemilik Kebijakan Pengelolaan Data akan memantau penerapan dan kepatuhan lembaga terhadap Kebijakan ini dan akses ke Platform Pertukaran/Integrasi Data.

1. Unit Organisasi harus berusaha sekuat tenaga untuk berbagi data antara Unit Organisasi lainnya sehingga dapat memberikan layanan yang terintegrasi untuk melayani masyarakat dengan lebih baik.
2. Dapat menerbitkan prosedur, pedoman, dan praktik terbaik tambahan atau tambahan dari waktu ke waktu untuk mendukung Kebijakan Pengelolaan Data.

I. Prosedur Umum Pengelolaan Data

1) Pembuatan dan Perekaman

Tahap pertama melibatkan pembuatan atau perekaman data dalam bentuk digital. Beberapa data mungkin terlahir digital, misalnya keluaran seperti file xml dari suatu sistem atau data yang tersedia dalam format digital seperti spreadsheet yang diterima dari sumber lain. Sementara data non-digital dari sumber lain seperti dokumen kertas dapat didigitasi melalui input manual ke dalam sistem atau solusi pemindaian.

Proses untuk merekam dan menyimpan data bersumber secara digital relatif lebih mudah dibandingkan dengan membuat data digital dari sumber non-digital. Solusi teknis untuk membantu dalam proses pembuatan dan perekaman data meliputi bentuk digital, solusi pengelolaan dokumen, pemindaian dan pemecahan gambar, dan solusi integrasi sistem.

2) Penyimpanan dan Pengelolaan

Begitu data dikumpulkan dan dibuat, data harus disimpan dengan cara yang paling mendukung proses bisnis. Tahap kedua melibatkan pengelolaan data yang diambil dan disimpan dalam infrastruktur TI organisasi sesuai kebijakan operasionalnya.

1. Klasifikasi data

Dasar pemikiran untuk mengklasifikasikan informasi ke dalam kelas adalah memungkinkan nilai yang sesuai untuk dipastikan untuk item informasi, risikonya harus ditentukan, dan perlindungan yang sesuai untuk diterapkan. Semua data yang dibuat dan ditangkap harus diklasifikasikan sesuai dengan Peraturan Perundang-undangan yang berlaku.

2. Keamanan data dan aksesibilitas

Keamanan fisik, keamanan jaringan dan keamanan sistem komputer dan file semua perlu dipertimbangkan untuk menjamin keamanan data dan mencegah akses yang tidak sah, perubahan pada data, pengungkapan atau penghancuran data. Pengaturan keamanan harus sesuai dengan sifat data dan risiko yang terkait.

Langkah penting lainnya dalam proses ini untuk membantu penemuan dan aksesibilitas adalah mengindeks data dan mengungkap metadata penemuan melalui antarmuka yang dapat ditelusuri**.**

Tercantum di bawah ini adalah praktik keamanan data tertentu:

- Keamanan data fisik memerlukan:
  - ✓ Mengontrol akses ke ruangan dan bangunan tempat data, komputer atau media diadakan
  - ✓ Membongkar penghapusan, dan akses ke, media atau materi hardcopy di ruang penyimpanan
  - ✓ Mengangkut data sensitif hanya dalam keadaan luar biasa, bahkan untuk tujuan perbaikan, misalkan Memberikan hard drive yang gagal yang berisi data sensitif ke produsen komputer dapat menyebabkan pelanggaran keamanan
- Keamanan jaringan berarti:
  - ✓ Tidak menyimpan data rahasia seperti yang berisi informasi pribadi pada server atau komputer yang terhubung ke jaringan eksternal, terutama server yang meng-host layanan internet
  - ✓ Perlindungan firewall dan upgrade terkait keamanan dan tambalan ke sistem operasi untuk menghindari virus dan kode berbahaya

- Keamanan sistem dan file komputer bisa meliputi:
  - ✓ Mengunci sistem komputer dengan password dan memasang sistem firewall
  - ✓ Melindungi server dengan sistem proteksi tenaga listrik melalui sistem catu daya tak terputus (interactive-interinterible power supply / UPS)
  - ✓ menerapkan proteksi password, dan akses terkontrol ke, file data, mis. tidak ada akses, baca saja, baca dan tulis atau hanya izin administrator
  - ✓ Mengontrol akses ke materi yang dibatasi dengan enkripsi
  - ✓ menerapkan perjanjian non-pengungkapan untuk manajer atau pengguna data rahasia
  - ✓ Tidak mengirimkan data pribadi atau rahasia melalui email atau sarana transfer file lainnya tanpa terlebih dahulu mengenkripsi mereka
  - ✓ Menghancurkan data secara konsisten bila diperlukan
  - ✓ Tidak menggunakan layanan file sharing seperti Google Docs atau Dropbox yang mungkin tidak aman
  - ✓ memungkinkan jejak audit dan kontrol versi untuk melacak modifikasi pada sistem dan basis data
- Keamanan data pribadi:

  Data yang berisi informasi pribadi harus ditangani dengan tingkat keamanan yang lebih tinggi daripada data yang tidak. Keamanan bisa dibuat lebih mudah dengan:
  - ✓ Menganonimkan atau menggabungkan data
  - ✓ Menghapus informasi pribadi, seperti nama dan alamat, dari file data dan menyimpannya secara terpisah
  - ✓ Mengenkripsi data yang berisi informasi pribadi sebelum disimpan - enkripsi pastinya diperlukan sebelum pengiriman data tersebut.

  Instansi terkait harus mendefinisikan proses dan prosedur keamanan informasi sesuai dengan Peraturan dan Perundang-undangan yang berlaku.

3. Kualitas data

Data dianggap berkualitas baik jika sudah lengkap, akurat, tersedia dan tepat waktu. Kesalahan umum yang mempengaruhi kualitas data termasuk catatan master duplikat, tidak adanya standar umum dan tidak adanya hubungan antara elemen transaksional.

Langkah-langkah utama dari proses kualitas data adalah:

- Penilaian data:

  Tahap penilaian data terdiri dari analisis struktur data dan pemetaan ujung ke ujung antara sistem sumber dan tujuan. Tahap ini mendefinisikan persyaratan pembersihan data dan menetapkan prioritas.

- Kontrol kualitas data:

  Fase ini memfokuskan pada koreksi dan standardisasi data untuk mengendalikan integritas data dari waktu ke waktu, dan terutama melibatkan tiga langkah: standardisasi data, pembersihan data dan konsolidasi data. Sementara standardisasi data memastikan konsistensi data antar sistem, pembersihan data dilakukan untuk memastikan integritas data dan untuk mempersiapkan data kebutuhan migrasi spesifik. Konsolidasi data mengurangi duplikat dan informasi yang tidak perlu dalam repositori data.

- Verifikasi kualitas data:

  Uji siklis harus dilakukan untuk memeriksa kesalahan data. Validasi data memberi jarak pandang terhadap kesalahan, penyebab dan kemungkinan tindakan perbaikannya.

  Instansi terkait harus menetapkan kerangka kualitas data yang terus menerus dan berulang untuk mengendalikan kualitas data.

4. Cadangan data

Tujuan utama backup adalah untuk memulihkan data setelah kehilangannya, baik itu dengan penghapusan data atau korupsi. Cadangan umumnya merupakan bagian dari rencana pemulihan bencana organisasi. Dinas Komunikasi, Informatika dan Statistik harus menerapkan proses pencadangan sesuai peraturan dan perundang-undangan yang berlaku dan kebijakan dan prosedur pemulihan bencana yang ditetapkan.

5. Pembuangan data dan arsip

Pembuangan data berarti dengan aman menghapus data yang telah usang atau berlebihan dan tidak diperlukan untuk dipertahankan atau dipertahankan; sementara arsip mengacu pada proses mengidentifikasi dan memindahkan data tidak aktif dari sistem produksi saat ini dan ke dalam sistem penyimpanan arsip jangka panjang yang khusus.

Salah satu langkah kunci dalam proses ini adalah menentukan kebijakan retensi data organisasi. Berikut adalah beberapa ketentuan hukum dan peraturan yang berlaku yang berkaitan dengan retensi rekaman:

- Catatan yang berkaitan dengan identifikasi pengguna layanan harus dipelihara selama waktu yang telah ditetapkan/didefinisikan oleh Direktorat Jenderal Pemerintah Daerah
- Wajib Pajak yang melakukan suatu kegiatan di Pemerintah diminta untuk menyimpan catatan akuntansi sesuai dengan peraturan dan perundang-undangan yang berlaku.

3) Distribusi dan Transaksi

Selama tahap ini, data yang pernah ditangkap dan disimpan sering dikirim ke alur kerja untuk routing dan tindakan sebagai bagian dari proses bisnis. Untuk mengolah data, secara aktif diakses dan dimiliki oleh instansi pemerintah dan karyawan mereka pada tahap ini. Aturan untuk siapa yang dapat mengakses setiap record akan ditentukan pada tahap sebelumnya, memberikan lingkungan yang tepat untuk memudahkan akses informasi tepat waktu, akurat dan tersedia dalam pedoman keamanan dan privasi. Instansi harus menetapkan proses untuk memudahkan penemuan dan akses data masukan, dan pengelolaan data keluaran.

5.4 Manajemen Aset TIK

Praktek manajemen asset SPBE dapat digunakan 2 referensi utama yaitu:

1. Peraturan Menteri Dalam Negeri Nomor 47 Tahun 2021

Ruang lingkup manajemen Asset SPBE dalam hal ini adalah Barang Milik Daerah atau BMD meliputi praktek:

a. Pembukuan

Kegiatan pendaftaran dan pencatatan BMD ke dalam daftar barang yang ada pada Kuasa Pengguna Barang, Pengguna Barang atau Pengelola Barang menurut penggolongan dan kodefikasi barang.

b. Inventarisasi

merupakan kegiatan untuk melakukan pendataan, pencatatan, dan pelaporan hasil pendataan BMD pada Daftar Barang Aset Tetap, Daftar Barang Aset Lainnya, Daftar Aset Bersejarah

c. Pelaporan

Hasil transaksi pencatatan pembukuan menghasilkan laporan. Adapun laporan tersebut meliputi Laporan perolehan/penerimaan, penggunaan, penerimaan internal pengguna barang, pengeluaran internal pengguna barang, pemanfaatan, reklasifikasi, koreksi, penambahan masa manfaat atau kapasitas manfaat, penyusutan atau amortisasi, persediaan, pemeliharaan, pengamanan, dan penghapusan pada Kuasa Barang, Pengguna Barang, Pengelola Barang dan gabungan Kuasa Barang, Pengguna Barang, Pengelola Barang.

2. Praktek Manajemen Konfigurasi dalam IT Infrastructure Library

Dalam praktek ini asset SPBE atau IT disebut dengan Item Konfigurasi. Lingkup pengelolaan Manajemen Aset adalah sebagai berikut:

A. Pengelolaan Item Konfigurasi

Organisasi perlu mendefinsikan kebijakan dan prosedur terkait dengan pengelolaan konfigurasi TIK. Pengelolaan konfigurasi tersebut menjelaskan hubungan komponen-komponen TIK yang disebut dengan Item Konfigurasi (Configuration Item) dalam suatu Configuration Management Database (CMDB).

CMDB membantu dalam mengelola komponen-komponen infrastruktur TIK, memfasilitasi ketersediaan sistem untuk meminimalkan terjadinya masalah pada lingkungan produksi, serta dapat membantu menyelesaikan masalah dengan cepat.

Aspek yang diatur dalam pengelolaan konfigurasi TIK adalah sebagai berikut:

1. Instalasi hardware, software,dan network;
2. Pengaturan parameter (hardening) hardware, software,dan network;
3. Inventarisasi dan pemutakhiran dokumentasi konfigurasi hardware, software, network, media penyimpan dan perangkat pendukung lainnya.

Adapun infrastruktur yang akan dikelola dalam manajemen konfigurasi (CMDB) adalah sebagai berikut:

1. Hardware

Inventarisasi hardware harus dilakukan secara menyeluruh termasuk inventarisasi hardware yang dimiliki oleh Penyedia Barang dan Jasa. Informasi

yang perlu didokumentasikan adalah sebagai berikut, namun tidak terbatas pada:

a. Nama Penyedia Barang dan Jasa;
b. Tanggal pembelian dan instalasi;
c. Kapasitas prosesor;
d. Memori utama;
e. Kapasitas penyimpanan;
f. Sistem operasi;
g. Fungsi;
h. Lokasi.

2. Software

Informasi yang harus ada dalam inventarisasi software mencakup hal-hal berikut, namun tidak terbatas pada:

a. Sistem operasi;
b. Sistem aplikasi atau sistem utilitas;
c. Nama pembuat atau Penyedia Barang dan Jasa;
d. Tanggal instalasi;
e. Nomor versi dan keluaran (release);
f. Pemilik software;
g. Setting parameter dan service yang aktif;
h. Jumlah lisensi yang dimiliki;
i. Jumlah yang diinstal dan jumlah user.

3. Perangkat Jaringan

Informasi yang harus ada dalam inventarisasi perangkat jaringan mencakup hal-hal berikut, namun tidak terbatas pada:

a. Diagram jaringan;
b. Identifikasi seluruh koneksi internal dan eksternal Pemerintah Daerah;
c. Daftar dan kapasitas peralatan jaringan seperti switch, router, hub, gateway, firewall, dan lain-lain;
d. Identifikasi Penyedia Jasa Telekomunikasi;
e. Rencana perluasan dan perubahan konfigurasi jaringan;
f. Gambaran sistem pengamanan jaringan.

4. Media

Informasi yang harus ada dalam inventarisasi media penyimpan mencakup hal-hal berikut, namun tidak terbatas pada:

a. Jenis dan kapasitas;
b. Lokasi penyimpanan, baikon-site maupun off-site;
c. Tipe dan klasifikasi data yang disimpan;
d. Source system;
e. Masa retensi backup.

5. Perangkat Pendukung Data Center

Inventarisasi perangkat pendukung Data Center harus dilakukan, antara lain pada UPS dan power control, fire detection and extinguisher, air conditioning, pengukur suhu dan kelembaban udara

B. Manajemen Kapasitas

Perencanaan kapasitas hendaknya disusun untuk jangka waktu cukup panjang dan selalu dikinikan untuk mengakomodir perubahan yang ada. Pemerintah Daerah perlu memiliki kebijakan dan prosedur pengelolaan kapasitas. Kebijakan dan prosedur tersebut bertujuan sebagai pedoman untuk memastikan bahwa hardware dan software yang digunakan Pemerintah Daerah telah sesuai dengan kebutuhan operasional dan dapat mengantisipasi pertumbuhan data. Hal-hal yang harus diperhatikan dalam pengelolaan kapasitas adalah sebagai berikut, namun tidak terbatas pada:

1. Pemantauan dan pengukuran kapasitas perangkat hardware dan jaringan komunikasi yang ada di Data Center dilakukan secara rutin sesuai dengan periode yang telah ditentukan;
2. Hasil pemantauan dan pengukuran kapasitas perangkat hardware dan jaringan komunikasi dijadikan dasar untuk memprediksikan kebutuhan hardware dan jaringan komunikasi di masa yang akan datang.

C. Migrasi Data

Migrasi data diperlukan dalam manajemen konfigurasi agar semua item konfigurasi bisa tersimpan dalam satu CMDB. Dalam aplikasi yang akan diimplementasikan fitur pengelolaan manajemen konfigurasi sudah tersedia dengan beberapa fitur yang

sudah memenuhi syarat yang dibutuhkan. Adapun skema migrasi data yang diimplementasikan setidaknya terdiri dari beberapa kriteria berikut:

1. Adanya tipologi item konfigurasi yang akan didefinisikan
2. Adanya klasifikasi item konfigurasi yang akan didefinisikan.
3. Struktur data item konfigurasi yang spesifik untuk setiap kelas item konfigurasi
4. Proses migrasi dilakukan untuk setiap kelas item konfigurasi.

D. Klasifikasi Item Konfigurasi

Adapun kelas-kelas yang sudah didefinisikan dalam kajian ini berdasarkan sumber informasi dari Pemerintah Daerah dalam asset register terdiri dari:

1. Information
2. Physical
3. People
4. Software
5. Services
6. Intangible

E. Kebijakan Umum dalam Manajemen Konfigurasi

1) Perbaharuan/Update Item Konfigurasi
    1. Setiap permohonan update item konfigurasi harus diajukan kepada penanggung jawab Manajemen Konfigurasi.
    2. Update item konfigurasi dapat dilakukan untuk kegiatan instalasi, update atau upgrade yang harus disertai dokumentasi yang diperlukan.
    3. Penanggung Jawab Manajemen Konfigurasi memberikan penomoran/pengkodean item konfigurasi yang akan dilakukan proses update.
    4. Proses update yang dilakukan merupakan perubahan minor dan tidak diperlukan untuk diproses dalam prosedur Manajemen Perubahan.
    5. Dalam pelaksanaan update item konfigurasi, Penanggung Jawab Manajemen Konfigurasi dapat mendelegasikan kepada IT Support.
    6. Setiap proses yang telah dilaksanakan harus direkam ke CMDB dan Penanggung Jawab Manajemen Konfigurasi harus mendapatkan notifikasi atas update yang dilakukan.

2) Pengaturan Parameter Item Konfigurasi

1. Perubahan parameter perangkat pada item konfigurasi diajukan oleh IT Support ke Penanggung Jawab Manajemen Konfigurasi melalui sebuah form perubahan parameter perangkat item konfigurasi yang diajukan kepada Penanggung Jawab Manajemen Konfigurasi .
2. Setiap perubahan parameter perangkat item konfigurasi harus disertai dokumentasi yang diperlukan.
3. Untuk permohonan perubahan parameter perangkat yang disetujui, Penanggung Jawab Manajemen Konfigurasi memberikan penomoran/pengkodean item konfigurasi.
4. Setiap permohonan yang tidak disetujui akan diberitahukan langsung pada IT Support.
5. Setiap perubahan parameter perangkat item konfigurasi harus dicatat dan di-update ke CMDB.
6. Penanggung Jawab Manajemen Konfigurasi mendapatkan notifikasi atas perubahan parameter perangkat item konfigurasi yang dilakukan oleh IT Support.

3) Update dan Inventarisasi Item Konfigurasi

1. *Review* terhadap *database* konfigurasi dilakukan sedikitnya setiap 6 (enam) bulan atau pada saat diperlukan.
2. *Review* dilakukan oleh IT *Support* dan dievaluasi serta dinilai oleh Penanggung Jawab Manajemen Konfigurasi .
3. Jika diperlukan update database konfigurasi maka IT *Support* mengajukan permohonan kepada Penanggung Jawab Manajemen Konfigurasi .
4. IT *Support* melakukan update database konfigurasi dengan persetujuan dan pengawasan Penanggung Jawab Manajemen Konfigurasi .
    a. Pada setiap *update* pada *database* konfigurasi pihak Penanggung Jawab Manajemen Konfigurasi mendapatkan notifikasi dari IT *Support* setelah dilakukan perekaman pada CMDB.

F. Prosedur Dalam Manajemen Konfigurasi

Adapun prosedur dalam manajemen konfigurasi setidaknya memuat aktivitas-aktivitas sebagai berikut:

i. Perbaharuan item konfigurasi

ii. Pengaturan parameter item konfigurasi
iii. Inventarisasi item konfigurasi
iv. Analisis kapasitas dan kebutuhan konfigurasi
v. Pengendalian dan Pelaporan item konfigurasi

5.5 Manajemen SDM

Manajemen SDM SPBE adalah untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE. Tujuan manajemen SDM SPBE tersebut dibentuk dari proses sebagai berikut:

1. Rekrutmen dan seleksi
2. Kompetensi
3. Learning and Development
4. Pengembangan dan budaya organisasi

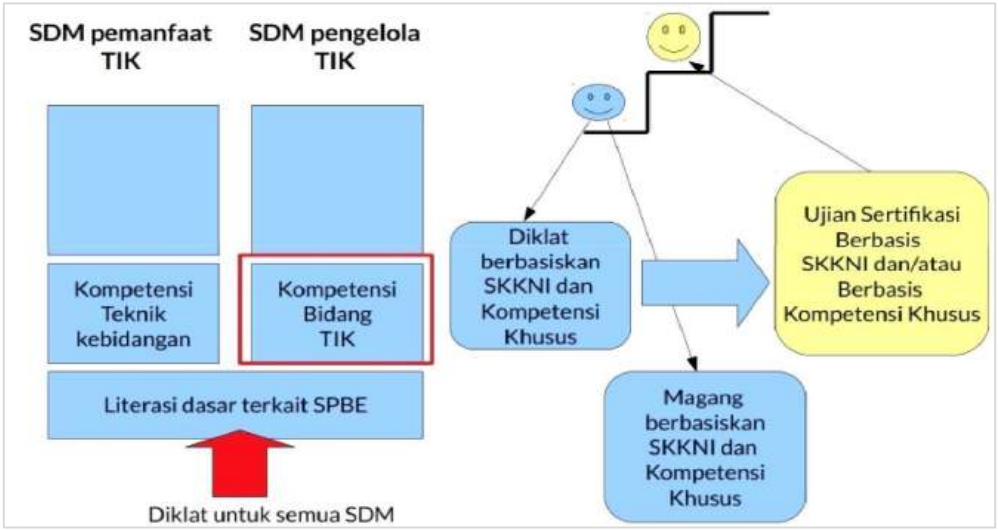
Aspek yang harus diperhatikan dalam management SDM SPBE antara lain:

1. Sumber daya manusia SPBE dikelola secara fungsional oleh OPD urusan SDM. Sumber daya manusia setiap organisasi harus dikelola secara memadai untuk memastikan terpenuhinya aspek jumlah, kompetensi, integritas, dan kepedulian personel.
2. SPBE harus mempunyai matriks kompetensi untuk setiap jabatan. Penilaian kinerja dilakukan secara rutin namun belum mencakup penilaian atas gap kompetensi yang ada.
3. Perencanaan training masih belum berdasarkan pada suatu proses Analisis Kebutuhan Pelatihan. Kegiatan pengembangan kompetensi personel dipersiapkan jika terdapat inisiasi permintaan dari unit kerja dan anggaran pelaksanaan tersedia.
4. Penilaian atas kegiatan pengembangan kompetensi baru mencakup penilaian atas pelaksanaan pelatihan, dan belum mencakup nilai dari pelatihan itu dalam meningkatkan performa personel.
    a. Promosi Literasi SPBE: Bimtek SPBE berbasis Perpres No 95 Tahun 2018 ke seluruh OPD.
    b. Peningkatan Kapasitas ASN Penyelenggara SPBE melalui SKKNI

Adapun secara keseluruhan kebutuhan umum kompetensi SDM TIK dalam penyelenggaran SPBE sekurang-kurang pemenuhan kompetensi tersebut berdasarkan kurikulum generic sebagai berikut:

Gambar 5. 3 Kurikulum Global Skill TIK

Adapun implementasi pengembangan kompetensi SDM TIK dapat dilaksanakan dengan model seperti berikut ini:



Gambar 5. 4 Model Implementasi Pengembangan SDM TIK

Area Peta Okupasi yang dapat dipetakan sebagai berikut:

- Sistem Manajemen Data (Data Management System)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam merancang, membangun, dan mengimplementasikan system basis data dan/atau informasi (kontendigital). Ruang lingkup dan jenis model database dimaksud beraneka ragam, seperti berbasis struktur, relasional, objek,dan lain sebagainya.Termasuk didalam domain ini adalah kemampuan

mengolah data tidak terstruktur seperti yang dikembangkan dalam konsep bigdata dan business intelligence.

- Pengembangan Perangkat Lunak dan Pemrograman (Programming and Software Development)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam merancang, mendesain, mengkonfigurasi, dan membuat perangkat lunak (software) maupun aplikasi yang dijalankan/dioperasikan dalam lingkungan komputer, piranti digital, maupun jaringan. Spektrum kemampuan ini berhubungan erat dengan metodologi atau life cycle pembuatan perangkat lunak, yaitu: perencanaan, perancangan, pemrograman, pengujian, perbaikan, penerapan, dan penilaian. Disamping itu,aspek ini berkaitan pula dengan kemampuan seorang individu dalam membuat atau mengembangkan program komputer yang dapat dijalankan dalam berbagai lingkungan komputasi (standal one maupun network), baik menggunakan Bahasa tingkat rendah (low level language) hingga tingkat tinggi (high level language) – baik yang bersifat terbuka (opensource) maupun tertutup(proprietary).
- Perangkat Keras dan Piranti Digital (Hardware and Digital Peripherals)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam merancang, mendesain, merakit, mengoperasikan, mengendalikan, dan memelihara perangkat keras komputer maupun piranti digital lainnya (hardware). Yang dimaksud dengan piranti digital lain adalah notebook, tablet, telepon pintar (smartphone), dan beraneka ragam gawai lainnya.
- Infrastruktur dan Jaringan (Network and Infrastructure)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam merancang, membangun, mengoperasikan, dan mengawasi berbagai komponen teknis jaringan infrastruktur dan telekomunikasi. Yang dimaksud dengan infrastruktur telekomunikasi di sini adalah medium transmisi atau koneksi berbasis digital/elektronik, yang beroperasi melalui darat (terestrial), laut (kabel laut), maupun udara (satelit).
- Sistem Operasi dan Aplikasi Pendukung (Operation and System Tools)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam mengembangkan, menginstalasi, mengkonfigurasi, menggunakan, dan memelihara sistem operasi komputer – baik untuk sistem mandiri (stand-alone) maupun dalam bentuk jaringan (network). Sistem operasi yang dimaksud melingkupi berbagai jenis baik yang bersifat terbuka (open source) maupun tertutup (proprietary).
- Pengembangan Sistem dan Teknologi Informasi (Information System and Technology Development)

Aspek ini berkaitan dengan kemampuan seorang individu dalam merencanakan, merancang, membangun, mengujicoba, menerapkan, mengembangkan, menilai, dan mengendalikan sistem informasi. Sistem informasi pada dasarnya dibangun oleh sejumlah komponen yang saling terkait satu dan lainnya, dimana elemen pembentuknya terdiri dari tiga bagian utama, yaitu: manusia (organisasi), proses, dan teknologi. Dalam tataran implementasinya, terdapat berbagai jenis variasi sistem dimaksud, misalnya: sistem informasi keuangan, sistem informasi sumber daya manusia, sistem informasi korporat, sistem informasi rumah sakit, sistem informasi pengendalian, dan lain sebagainya.

- Manajemen dan Tata Kelola Teknologi Informasi (Information Technology Governance and Management)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam hal merencanakan, merancang, mengadakan, membangun, menerapkan, menjalankan, dan mengendalikan tata kelola sistem dan teknologi informasi dalam organisasi. Hal utama yang menjadi fokus pada elemen ini terkait dengan isu seputar governance dan manajemen.
- Manajemen Proyek Teknologi Informasi (Information Technology Project Management)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam hal merencanakan, mempersiapkan, menjalankan, mengelola, menilai, mengawasi, dan mengendalikan aktivitas proyek sistem dan teknologi informasi. Adapun fokus utamanya adalah pada manajemen ruang lingkup, kualitas, waktu, biaya, risiko, komunikasi, pengadaan, sumber daya manusia, pemangku kepentingan, dan integrasi.
- Arsitektur Teknologi Informasi Korporasi (Information Technology Enterprise Architecture)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam hal merencanakan, merancang, mendesain, menerapkan/mengimplementasikan, mengkaji, mereviu, menilai, mengelola, dan mengendalikan arsitektur enterprise beserta sub-sistem pembentuknya. Adapun sub-sistem pembentuknya berupa arsitektur bisnis (proses), arsitektur aplikasi, arsitektur informasi, arsitektur teknologi, arsitektur organisasi, dan arsitektur kebijakan (policy).
- Keamanan Teknologi Informasi dan Kepatuhan (Information Technology Security and Compliance)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam hal merencanakan, merancang, membangun, menerapkan, mengelola, menilai, mengukur, dan mengendalikan sistem keamanan data, informasi, sistem, dan/atau internet. Spektrum ruang lingkup kapabilitas ini bervariasi dari yang sangat konseptual hingga teknis, dan mulai dari yang teoritis hingga terapan. Disamping itu, aspek ini berkaitan pula dengan

kemampuan organisasi dalam memenuhi atau mematuhi beragam peraturan/regulasi teknis di bidang keamanan informasi.

- Sistem Manajemen Layanan Teknologi Informasi (Information Technology Services Management System)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam hal merencanakan, merancang, mendesain, menerapkan, mengendalikan, dan mengevaluasi beragam layanan teknologi informasi dalam sebuah organisasi. Layanan dimaksud melingkupi aspek-aspek utama seperti: ketersediaan/availabilitas, dukungan bantuan/helping support, kualitas, keberlanjutan, kebersinambungan, dan lain sebagainya.

- Sistem Manajemen Fasilitas Teknologi Informasi (Information Technology and Computing Facilities Management)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam hal merencanakan, merancang,mendesain, membangun, menjalankan/menerapkan/mengimplementasikan, mengelola, dan mengendalikan beragam fasilitas, sarana prasarana, dan teknologi pendukung sistem informasi. Fasilitas maupun sarana prasarana dimaksud antara lain: data center, call center, disaster recovery center, server room, cloud computing facilities, dan lain sebagainya.

- Multimedia (IT Multimedia)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam merancang, membuat, mengembangkan, dan menerapkan aplikasi dan/atau konten berbasis multimedia dalam platform antarmuka (user interface) yang beragam. Multimedia merupakan representasi digital dalam berbagai format media seperti: teks, gambar/citra/grafis, suara/audio, film/video, atau kombinasi di antaranya. Beragam media ini dikembangkan untuk kebutuhan pengguna yang menginginkan adanya model navigasi aplikasi (input maupun output) yang menarik, mudah digunakan (user friendly), dan ergonomis.

- Teknologi Mobile dan Internet-Of-Things (Information Technology Mobility and Internet-Of-Things)

  Aspek ini berkaitan dengan kemampuan seorang individu dalam merancang, membuat, mengembangkan, mengkonfigurasi, menerapkan, dan mengendalikan teknologi yang berhubungan dengan kanal akses (access channels atau distribution channels). Belakangan ini telah dikenal sejumlah teknologi kanal akses yang dikenal masyarakat seperti: ATM, kios, TV digital, tablet, smart phone, gadget, kamera, dan lain sebagainya – baik yang berdiri sendiri maupun yang telah dirakit (embedded) dalam entitas lain seperti: mobil, pesawat, kereta api, motor, mesin cuci, lemari es, dan lain sebagainya (internet-of-things).

- Sistem Informasi Terintegrasi (Integration Application System)

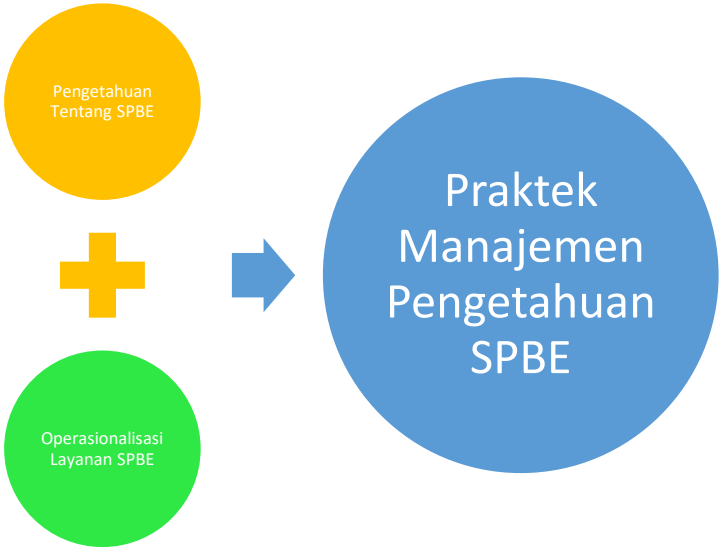
  Aspek ini berkaitan dengan kemampuan eorang individu dalam merencanakan, merancang, membangun, menerapkan, mengendalikan, dan mengembangkan sistem informasi terintegrasi dan terpadu yang di dalamnya terdiri dari berbagai komponen penting berupa komponen teknologi, proses, dan manusia. Ruang lingkup yang ditangani sangatlah luas, mulai yang bersifat strategis hingga teknis – termasuk di dalamnya isu-isu penting seperti: manajemen perubahan, dinamika sosial, strategi implementasi, dan lain sebagainya.
- Konsultasi dan Layanan Jasa SDM Teknologi Informasi (IT Consultancy and Advisory)

  Aspek ini berkaitan erat dengan kemampuan seorang individu dalam memberikan beragam jasa layanan terkait dengan teknologi informasi, seperti konsultasi, pendampingan, pelatihan, penelitian, dan lain sebagainya. Termasuk di dalamnya mereka yang ingin menekuni bidang *digital entrepreneurship*.

5.6 Manajemen Pengetahuan

A. Ruang Lingkup Manajemen Pengetahuan

Manajemen pengetahuan atau knowledge management SPBE mempunyai lingkup penyelenggaran layanan SPBE. Keterkaitan Manajemen Layanan ini dapat digambarkan sebagai berikut:



Gambar 5. 5 Ruang Lingkup Manajemen Pengetahuan

1. Pengetahuan tentang SPBE
2. Operasionalisasi Layanan SPBE
3. Praktek Manajemen Pengetahuan SPBE

Adapun cakupan pengetahuan dari manajemen pengetahuan berasal dari:

1. Resolusi Insiden

   Setiap insiden yang dinyatakan selesai oleh support teknis harus mencantumkan paparan langkah solusi yang dilaksanakan.

2. Resolusi Problem

   Setiap problem yang dinyatakan selesai oleh support teknis harus mencantumkan paparan langkah solusi yang dilaksanakan.

3. Resolusi Workaround

   Workaround adalah langkah penyelesaian secara spesifik dalam rangka menghilangkan pengaruh atau meminimalkannya dari sebuah insiden atau problem

4. Riwayat Tiket

   Riwayat tiket memapakah penanganan tiket permintaan dan dari paparan riwayat perlu dilakukan analisis untuk mendapatkan pengetahuan

Berdasarkan hasil aktivitas penanganan permintaan pengguna untuk berbagai manajemen maka implementasi dari manajemen pengetahuan yang dapat direalisasikan dalam aplikasi adalah sebagai berikut:

a. Known Error Database
b. Frequently Ask Question

B. Kebijakan Umum Manajemen Pengetahuan

Adapun kebijakan umum dalam manajemen pengetahuan adalah sebagai berikut:

1. Dalam pelaksanaan penanganan penyelesaian insiden/problem, setiap support teknis direkomendasikan mempunyai referensi dari known error database atau data resolusi penanganan insiden/problem sebelumnya.
2. Pembelajaran penyelesaian penanganan insiden harus dilakukan oleh setiap Tier support penanganan insiden/problem.
3. Mekanisme pembelajaran diatur secara otonomi oleh setiap Tier support penanganan insiden/problem.
4. Manajer Support Teknis dan pimpinan Diskominfotik dapat dijadikan mitra atau nara sumber Pembelajaran Penyelesaian Penanganan Insiden/problem.
5. Pembelajaran Penyelesaian Penanganan Insiden/problem menjadi landasan peningkatan mutu layanan dan usulan perubahan layanan.
6. Setiap pelaporan Problem setidaknya memuat perihal berikut ini:

7. Pelaporan atas penanganan problem dilakukan secara berkala yang memuat hal-hal berikut:
    i. Uraian rangkuman problem yang terselesaikan, laporan ini setidaknya mencantumkan problem yang terjadi, waktu penanganan sampai tuntas dan solusi apa yang diberikan.
    ii. Status atas problem yang terbuka adalah uraian problem yang belum terselesaikan dengan menguraikan kapan problem tersebut terjadi dan alasan tindakan yang dilakukan tidak dapat menyelesaikan permasalahan.
    iii. Laporan Problem Root Cause meliputi problem yang terjadi, alasan terjadinya problem dan tindakan pencegahan agar problem tidak terulang lagi.
    iv. Rencana tindakan berikutnya untuk peningkatan tindakan penanganan problem terkait tren problem yang terjadi dan waktu penyelesaian permasalahan.
    v. Analisa problem harus dibuat sebagai masukan bagi manajemen.

C. Prosedur dalam Manajemen Pengetahuan

Prosedur yang ada dalam manajemen pengetahuan setidaknya memuat aktifitas-aktifitas berikut ini:

1. Aktifitas pendokumentasian resolusi penanganan insiden/problem
2. Aktifitas pendokumentasian Workaround
3. Aktifitas perekaman item konfigurasi dan analis pengaruhnya terhadap item konfigurasi lainnya.
4. Aktifitas perekamana Known Error Database
5. Aktifitas perekaman Frequently Ask Question

5.7 Manajemen Perubahan

Manajemen perubahan (*Management of Change*) adalah sebuah proses dan pendekatan terstruktur dan sistematis yang digunakan untuk membantu individu, tim maupun organisasi dengan menerapkan pengetahuan, sarana dan sumber daya untuk merealisasikan perubahan dari kondisi saat ini menuju kondisi baru yang lebih baik secara efektif dan efisien guna memperkecil dampak dari proses perubahan tersebut.

Adapun praktek Manajemen Perubahan berdasarkan 7R yaitu:

1. The REASON behind the change? (Alasan dibalik perubahan)
2. RISKS involved in the requested change? (Risiko yang terlibat dalam permintaan perubahan)

3. RESOURCES required to deliver the change? (Resource yang disyaratkan dalam pelaksanaan perubahan)
4. Who RAISED the change request? (Pihak yang menginisiasi permintaan perubahan)
5. RETURN required from the change? (Balikan yang disyaratkan dari perubahan)
6. Who is RESPONSIBLE for creating, testing, and implementing the change? (Penanggung jawab dalam pelaksanaan perubahan)
7. RELATIONSHIP between suggested change and other changes? (Relasi atau hubungan antara perubahan yang disarankan dan perubahan lainnya)

Pemerintah Daerah harus memiliki pengendalian dalam proses Manajemen Perubahan atau Manajemen Perubahan. Manajemen Perubahan adalah prosedur yang mengatur penambahan, penghapusan, maupun modifikasi objek di lingkungan produksi. Objek yang dimaksud dapat berupa data, program, menu, aplikasi, perangkat komputer, perangkat jaringan, dan proses serta layanan SPBE.

A. Kebijakan Umum Manajemen Perubahan

Kebijakan umum dalam melakukan manajemen perubahan adalah sebagai berikut, namun tidak terbatas pada:

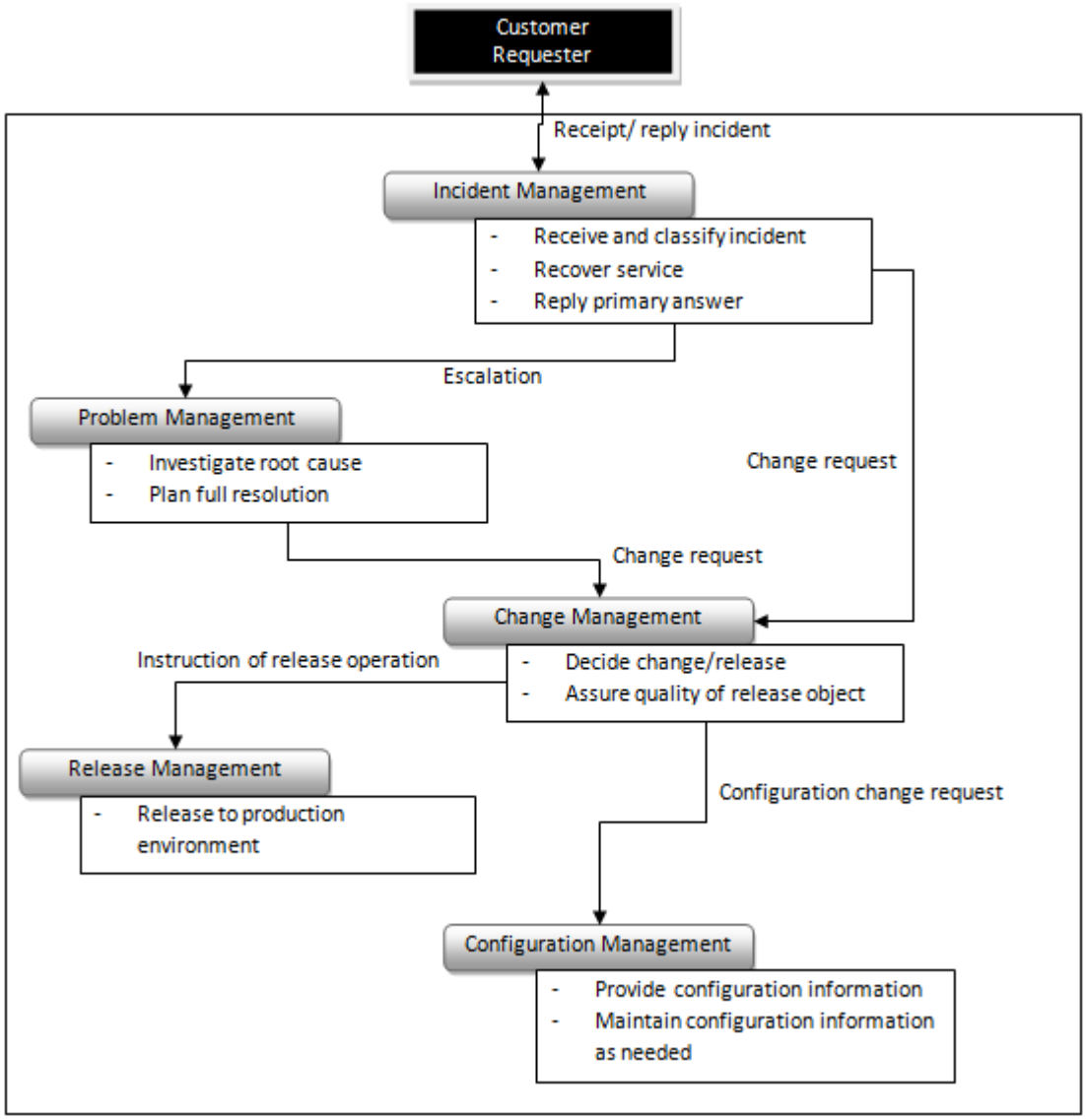
1. Pengajuan perubahan dilakukan oleh pengguna dan disetujui oleh pihak yang memiliki otorisasi di Pemerintah Daerah;
2. Pelaksana Perubahan melakukan perubahan pada lingkungan pengembangan yang terpisah dari lingkungan produksi;
3. Pelaksana Perubahan melakukan pengujian untuk memastikan integrasi antar modul pada saat melakukan perubahan;
4. Pengujian dilakukan di lingkungan pengujian yang terpisah dari lingkungan produksi dan data yang digunakan bukan data asli. Jika menggunakan data asli, data tersebut harus disamarkan;
5. Pengujian dilakukan berdasarkan skenario yang telah dibuat pengguna;
6. Hasil perubahan yang akan diimplementasikan, harus mendapatkan persetujuan fungsi IT Quality Assurance;
7. Dokumentasi perubahan harus disimpan dan dikelola dengan baik untuk mempermudah dalam melakukan penelusuran kembali jika terjadi gangguan pada sistem/infrastruktur TIK.

B. Prosedur dalam Manajemen Perubahan

Prosedur dalam Manajemen perubahan setidaknya meliputi aktivitas-aktivitas berikut ini:

1. Permintaan perubahan dalam bentuk dokumen RFC
2. Analisis Permintaan Perubahan oleh Manajer Perubahan
3. Proses Persetujuan oleh Komite Penasehat Perubahan (Change Advisory Board)
4. Proses Pelaksanaan Perubahan
5. Pelaporan Hasil Pelaksanaan perubahan

Prosedur dalam manajemen perubahan akan terkait dengan prosedur dalam manajemen insiden, manajemen permasalahan, manajemen rilis dan manajemen konfigurasi. Keterkaitan ini dapat digambarkan sebagai berikut:



Gambar 5. 6 Prosedur Manajemen Perubahan

5.8 Manajemen Layanan

Manajemen Layanan SPBE dalam prakteknya dikhususkan pada bagaimana penyelenggaran layanan SPBE dapat diberikan kepada pengguna.

A. Katalog Layanan

Rancangan awal dari manajemen layanan yang perlu didefinisikan adalah pendefinisian Paket Layanan yang dipaparkan dalam bentuk katalog layanan. Paket Layanan yang didefinisikan adalah sebagai berikut:

1. Layanan Data
    a. Akses Data
    b. Pertukaran Data
    c. Insiden Keamanan Data
2. Layanan Aplikasi
    a. Permintaan Akses Aplikasi
    b. Insiden Aplikasi tidak bisa diakses
    c. Insiden Aplikasi Rusak
3. Layanan Infrastruktur
    a. Personal Computer
    b. Jaringan Lokal/Internet
    c. Perangkat Server
    d. Perangkat Jaringan
    e. Perangkat Keras Bergerak
4. Layanan Publik SPBE
    a. Perijinan
    b. Surat Keterangan
    c. Kependudukan dan Catatan Sipil
    d. Pajak dan Retribusi
    e. Sertifikasi
    f. Layanan Publik Lainnya
5. Layanan Administrasi Pemerintahan
    a. Kepegawaian
    b. Keuangan
    c. Layanan Administrasi Lainnya

B. Format Katalog Layanan

Berikut adalah contoh format katalog layanan

Tabel 5. 5 Format Katalog Layanan

Nama Layanan	Layanan Data
Uraian	Layanan ini ditujukan untuk masyarakat umum pengguna SPBE. Layanan ini terdiri penanganan permasalahan dan kebutuhan: 1. Download tidak berhasil 2. Data Rusak Setiap layanan yang diberikan akan mendapatkan penanganan sesuai dengan prioritas dan dampak yang dapat ditimbulkan. Dampak dan prioritas yang harus dipertimbangkan terdiri dari: • Gangguan berdampak pada kegagalan pengguna mendapatkan data yang diinginkan melalui proses download • Gangguan berdampak pada data tidak bisa dibuka atau diakses setelah melalui proses download • Gangguan berdampak pada tidak terpenuhinya kualitas layanan data kepada pengguna • Gangguan berdampak pada terhentinya proses download peta mendapatkan prioritas sangat tinggi • Gangguan berdampak pada terhentinya akses ke web services mendapatkan prioritas tinggi
Pengguna Layanan	Masyarakat Umum
Waktu Pelaksanaan Layanan	Layanan Offline: 08:00 – 16:00 Setiap Hari Kerja Layanan Online: 24 jam melalui saluran aplikasi Web dan Mobile
Kriteria Keberhasilan Layanan	Kesukseskan pelaksanaan layanan terdiri dari indikator berikut ini: • Waktu respon terhadap laporan pertama kali • Waktu penyelesaian layanan yang dimulai dari waktu respon terhadap laporan pertama kali.
Kapasitas Layanan	Waktu layanan disediakan selama hari kerja dan jam kerja, permintaan layanan di luar waktu tersebut akan ditindaklanjuti sesuai dampak dan prioritas yang melekat. Pelaporan layanan dilakukan melalui kontak tunggal dengan kapasitas penerimaan laporan secara bersamaan maksimum 3 layanan. Penerimaa layanan melalui e-Ticketing dapat dilakukan 24 jam x 365 hari dalam setahun. Waktu respon terhadap layanan disesuaikan dengan ketentuan waktu layanan yang disediakan kecuali untuk prioritas tinggi dan sangat tinggi. Penanganan layanan secara remote dilaksanakan maksimum 1 layanan pada satu saat dengan waktu layanan konsultasi maksimum 1 jam. Penanganan layanan secara langsung di tempat dilaksanakan maksimum 2 hari dari waktu pertama kali kedatangan di lokasi. Kapasitas total layanan per periode waktu (hari/bulan/tahun) ditentukan oleh jumlah tim support yang ditugaskan dans sewaktu-waktu kapasitas ini dapat berubah.

C. Organisasi Pengelola Layanan

Organisasi Pengelola Layanan di Diskominfotik untuk SPBE ini didasarkan pada struktur organisasi Diskominfotik. Berikut ini adalah pemetaan pengelola layanan.

Tabel 5. 6 Pemetaan Pengelola Layanan

Pengelola	Nama Kontak	Jabatan	Tanggung Jawab
Pemilik Layanan	Pejabat Sekretaris Daerah	Pemilik Layanan	• Pembuat Keputusan Kunci • Bertanggung jawab atas proses Service Desk
Manager Operasional Layanan	Pejabat Dinas Kominfo	Manajer Operasional Layanan	• Sebagai pelaksana manajemen Layanan • Berfungsi sebagai kontak utama layanan
Pemilik Teknikal Layanan	Pejabat atau personil yang berkompeten dalam hal teknis layanan	Pemilik Teknis Layanan	• Pembuat Keputusan Teknis Utama • Bertanggung jawab atas pelaksanaan layanan pada tingkat yang disepakati
Manager Teknikal Layanan	Pejabat atau personil yang berkompeten dalam mengelola teknis layanan	Koordinator Pelaksana Teknis Layanan	• Sebagai pelaksana dalam kegiatan layanan pada tingkat yang disepakati • Berfungsi sebagai kontak utama layanan
Pelaksana Teknis	Personil atau tim yang pertama kali menerima permintaan layanan dari pengguna	Personil yang menerima kontak laporan ke service desk dan sebagai Support Teknis Level - 0 (Tier-1)	• Menerima laporan dan melayani kebutuhan pengguna serta melakukan eskalasi penugasan laporan permintaan layanan, insiden atau problem jika diperlukan
	Personil yang memahami masing-masing bidang teknis layanan	Support Teknis Level-1 (Tier-2)	• Menerima dan menyelesaikan eskalasi laporan insiden dan problem dari level 0 • Menerima penugasan dari service desk dan melakukan eskalasi jika diperlukan dari setiap laporan insiden dan problem • Melakukan penyelesaian insiden/problem • Melakukan workaround yang diminta oleh support teknis level 2
		Support Teknis Level-2	• Menerima Eskalasi laporan insiden dan problem dari level 1

Pengelola	Nama Kontak	Jabatan	Tanggung Jawab
	Narasumber Teknis di masing-masing bidang layanan Vendor TIK	(Tier-3)	• Melakukan analisis penyelesaian insiden/problem untuk membantu support teknis level-1 • Jika diperlukan menyelesaikan insiden/problem • Membuat tiket perubahan jika insiden atau problem perlu dieskalasikan ke manajemen perubahan

C. Pendefinisian Level Layanan

Pendefinisian level layanan ditujukan untuk mengukur pencapaian kinerja layanan yang diberikan kepada pengguna. Paket level layanan ini perlu didefinisikan sebagai baseline kinerja service desk.

Sebelum didefinisikan paket level layanan perlu dipaparkan dahulu metrik yang digunakan dalam pengukuran kinerja layanan yang diberikan oleh Pemerintah Daerah baik kepada masyarakat atau internal Pemerintah Daerah sendiri. Adapun metric tersebut adalah sebagai berikut:

1. Waktu respon terhadap pelaporan atau permintaan layanan dan akan dinamai atau diistilahkan Time to Respond (TTR)
2. Waktu penugasan terhadap pelaporan atau permintaan layanan dan akan dinamai atau diistilahkan dengan Time to Owned (TTO).
3. Waktu Penyelesaian Tindak Lanjut Laporan adalah ukuran kinerja yang dihitung mulai dari penugasan sampai laporan/permintaan pengguna dinyatakan selesai dan ditutup.

Setiap metrik ini akan didefinisikan dengan nilai yang berbeda berdasarkan prioritas pelaksanaan layanan yang diberikan. Prioritas ini akan diputuskan melalui sebuah analisa atau perhitungan secara objektif. Adapun prioritas tersebut adalah sebagai berikut:

1. Urgent atau mendesak
2. High atau tinggi
3. Medium atau sedang
4. Low atau rendah.

Ukuran kinerja secara rinci merupakan kombinasi dari masing-masing metric dengan prioritas yang ditetapkan. Kinerja tersebut berlaku pada tataran proses pelaksanaan layanan secara normal atau tidak ada pelanggaran atas kesepakatan layanan (Service Level Aggreement). Pelanggaran terhadap metric tersebut akan berimplikasi munculnya metric tambahan sebagai kontrol atas pelanggaran yaitu:

1. Escalated TTR atau TTR tereskalasi
2. Escalated TTO atau TTO tereskalasi

D. Pelaksanaan dan Penyelesaian Layanan

Pelaksanaan dan penyelesaian layanan diuraikan dalam tabel berikut:

Tabel 5. 7 Pelaksanaan dan Penyelesaian Layanan

Target Pelaksaanaan & Penyelesaian Layanan berdasarkan Prioritas	Pelaksanaan dan penyelesaian layanan dilakukan selama waktu kerja yang berlaku di Pemerintah Daerah dengan interval yang tersedia yaitu: • Hari: Senin – Jum'at • Waktu 08:00 – 17:00 Waktu pelaksanaan dan penyelesaian layanan tidak tersedia pada hari libur nasional dan akhir pekan kecuali jika ditetapkan pada prioritas mendesak yang ditetapkan dan disetujui oleh pimpinan organisasi Pemerintah Daerah.		
Prioritas	**TTR**	**TTO**	**Penyelesaian**
Urgent	5 menit	15 menit	1 hari kerja
Tinggi	10 menit	30 menit	Maksimum 3 hari
Sedang	15 menit	45 menit	Maksimum 5 hari
Rendah	30 menit	60 menit	Maksimum 10 hari

E. Prosedur Dukungan, Komunikasi dan Eskalasi

Prosedur dukungan, komunikasi dan eskalasi diuraikan dalam tabel berikut:

Tabel 5. 8 Prosedur Dukungan, Komunikasi dan Eskalasi

Dukungan	Setiap laporan akan ditindaklanjuti mulai dari penugasa, pelaksanaan penyelesaian dan pelaporan penyelesaian tindakan. Pelaksana tindakan adalah Technical Support yang telah ditetapkan sesuai dengan kompetensi dan tanggung jawabnya.
Komunikasi	Ruang lingkup komunikasi yang harus dibangun dalam pelaksanaan tindakan pelayanan adalah sebagai berikut: • Status laporan akan diperbaharui dan tertera dalam log tiket layanan dalam aplikasi e-ticketing. • Pengguna/pelapor dapat melakukan komunikasi dalam proses pelaksanaan tindakan baik melalui aplikasi, telpon atau pun email.

	• Pengguna akan mendapatkan email pemberitahuan tindakan pelaksanaan layanan. • Media social akan digunakan untuk mendukung komunikasi pelaksanaan layanan.
Eskalasi	Eskalasi akan dilakukan jika suatu tindakan tidak dapat dilanjutkan oleh personil yang ditugaskan dengan kondisi-kondisi berikut: 1. Kompleksitas laporan dari pengguna memerlukan kompentesi yang lebih tinggi daripada kompetensi technical support yang ditugaskan saat itu. 2. Perlunya pengambilan keputusan dari technical support diatasnya atau pimpinan Pemerintah Daerah. 3. Tindakan lanjutan yang dilaksanakan memerlukan keterlibatan pihak ketiga.

F. Tindakan pada Sebuah Event atau Gangguan Terencana

Tindakan pada sebuah event atau gangguan terencana diuraikan dalam tabel berikut:

Tabel 5. 9 Tindakan pada sebuah Event atau Gangguan Terencana

Gangguan Terencana atau Event	Pelaksana layanan sudah menyepakati dengan pengguna adanya gangguan terencana atau event yang dapat menurunnya kualitas layanan sementara waktu. Adapun tindakan yang perlu dilakukan oleh pelaksana layanan untuk meminimalkan dampak dari gangguan terencana atau even tersebut adalah: • Menjadwalkan tindakan di luar jam kerja layanan • Pemberitahuan gangguan disampaikan kepada pengguna selambat-lambatnya 1 hari sebelumnya atau jika prioritasnya mendesak dilakukan pemberitahuan selambat-lambatnya 2 jam sebelumnya. Karakteristik dari gangguan terencana atau event yang harus dipenuhi adalah sebagai berikut: 1. Adanya pendefinisian frekuensi, lama dan jumlah gangguan terencana atau event yang akan terjadi 2. Adanya perkiraan jadwal atau waktu dan durasi waktu gangguan terencana atau event yang akan terjadi. Berikut ini adalah contoh gangguan terencana atau event: • Pelaksanaan bug fixing • Update atau patch aplikasi • Perawatan rutin infrastruktur
Komunikasi	Ruang lingkup komunikasi yang harus dibangun dalam pelaksanaan tindakan terhadap gangguan terencana atau even adalah sebagai berikut: • Pemberitahuan dilakukan melalui beberapa saluran komunikasi seperti email, web ataupun social media. • Pengguna akan mendapatkan email pemberitahuan tindakan pelaksanaan layanan.

BAB VI
RENCANA AKSI PENERAPAN MANAJEMEN SPBE

6.1 Pendahuluan

Rencana Aksi ini dibuat sebagai panduan untuk menerapkan Dokumen Manajemen SPBE di lingkungan Pemerintah Kabupaten Natuna. Rencana Aksi ini memuat langkah-langkah strategis dan terukur yang akan dilaksanakan dalam jangka waktu tertentu untuk mencapai tujuan penerapan SPBE yang efektif, efisien, dan akuntabel

6.2 Tujuan Rencana Aksi

- Mewujudkan penyelenggaraan SPBE di Pemda yang efektif, efisien, akuntabel, dan berkelanjutan.
- Meningkatkan kualitas layanan publik berbasis elektronik di Pemerintah Kabupaten Natuna.
- Mendukung pencapaian Visi dan Misi Pemerintah Kabupaten Natuna.

6.3 Sasaran Rencana Aksi

- Tercapainya target Indeks SPBE Pemerintah Kabupaten Natuna.
- Meningkatnya kematangan penyelenggaraan SPBE di seluruh OPD di Pemkab. Natuna
- Meningkatnya kepuasan masyarakat terhadap layanan publik berbasis elektronik.
- Terwujudnya interoperabilitas dan integrasi sistem SPBE di Pemerintah Kabupaten Natuna.
- Meningkatnya kapasitas dan kompetensi SDM dalam pengelolaan SPBE di Pemerintah Kabupaten Natuna.

6.4 Ruang Lingkup Kegiatan Rencana Aksi

Rencana Aksi ini akan dilaksanakan dengan metode sebagai berikut:

- Penguatan Kelembagaan
- Perencanaan dan Pengembangan SPBE
- Pengembangan Infrastruktur SPBE
- Pengembangan Aplikasi dan Layanan SPBE
- Pengembangan SDM SPBE
- Pengelolaan Keamanan SPBE
- Pengelolaan Data dan Informasi SPBE
- Pengelolaan Anggaran SPBE
- Komunikasi dan Edukasi SPBE

- Monitoring dan Evaluasi SPBE

6.5 Metode Pelaksanaan Rencana Aksi

Rencana Aksi ini akan dilaksanakan dengan metode sebagai berikut:

- Pembentukan Tim Koordinasi SPBE Pemkab. Natuna dan Tim SPBE OPD.
- Penyusunan Peta Jalan SPBE Pemkab. Natuan dan Peta Jalan SPBE Perangkat Daerah.
- Sosialisasi dan edukasi SPBE kepada seluruh pemangku kepentingan.
- Pelatihan dan sertifikasi SDM SPBE.
- Pengadaan infrastruktur SPBE.
- Pengembangan aplikasi dan layanan SPBE.
- Penerapan langkah-langkah pengamanan SPBE.
- Penerapan tata kelola data dan informasi SPBE.
- Pengelolaan anggaran SPBE secara efektif dan efisien.
- Monitoring dan evaluasi pelaksanaan SPBE secara berkala.

6.6 Rencana Aksi 2024

Rencana aksi tahun 2024 diuraikan dalam tabel berikut:

Tabel 6. 1 Rencana Aksi Tahun 2024

Tahun	Komponen	Aktivitas	Target
2024	Penguatan Kelembagaan	- Pembentukan Tim Koordinasi SPBE Pemkab. Natuna dan Tim SPBE OPD - Penyusunan Dokumen Manajemen SPBE Pemkab. Natuna	- Tim SPBE Daerah dan Tim SPBE Perangkat Daerah terbentuk dan terstruktur. - Dokumen Manajemen SPBE Daerah tersusun dan disepakati.
	Perencanaan dan Pengembangan SPBE	- Review Peta Jalan SPBE Pemkab. Natuna - Analisis kebutuhan dan kesenjangan SPBE Kab. Natuan	- Evaluasi dan Penyesuain Peta Jalan SPBE. - Analisis kebutuhan dan kesenjangan SPBE Pemkab. Natuna selesai dilaksanakan.
	Pengembangan Infrastruktur SPBE	- Evaluasi desain infrastruktur SPBE Pemkab. Natuna - Pengadaan infrastruktur SPBE Pemkab. Natuna	- Perbaikan/Penyesuaian infrastruktur SPBE Pemkab. Natuna - Infrastruktur SPBE Pemkab. Natuna terbangun/ter-upgrade dan operasional.

6.7 Rencana Aksi 2025

Rencana aksi tahun 2025 diuraikan dalam tabel berikut:

Tabel 6. 2 Rencana Aksi Tahun 2025

Tahun	Komponen	Aktivitas	Target
2025	Pengembangan Aplikasi dan Layanan SPBE	- Penyusunan roadmap pengembangan aplikasi dan layanan SPBE Daerah - Pengembangan aplikasi dan layanan SPBE prioritas	- Roadmap pengembangan aplikasi dan layanan SPBE Daerah tersusun dan disepakati. - Aplikasi dan layanan SPBE prioritas terbangun dan operasional.
	Pengembangan SDM SPBE	- Penyusunan program pelatihan dan sertifikasi SDM SPBE - Pelaksanaan pelatihan dan sertifikasi SDM SPBE	- Program pelatihan dan sertifikasi SDM SPBE tersusun dan disepakati. - Pelatihan dan sertifikasi SDM SPBE selesai dilaksanakan.
	Pengelolaan Keamanan SPBE	- Penyusunan kebijakan dan prosedur keamanan SPBE Pemkab. Natuna - Implementasi langkah-langkah pengamanan SPBE Pemkab. Natuna	- Kebijakan dan prosedur keamanan SPBE Pemkab. Natuna tersusun dan disepakati. - Langkah-langkah pengamanan SPBE Pemkab. Natuna terimplementasi.
	Pengelolaan Data dan Informasi SPBE	- Penyusunan/Perbaikan kebijakan dan tata kelola data dan informasi SPBE Daerah - Implementasi pengelolaan data dan informasi SPBE Daerah	- Kebijakan dan tata kelola data dan informasi SPBE Daerah tersusun dan disepakati. - Pengelolaan data dan informasi SPBE Daerah terimplementasi.