BUPATI NATUNA
PROVINSI KEPULAUAN RIAU

PERATURAN BUPATI NATUNA
NOMOR 19 TAHUN 2024
TENTANG
PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENNGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI NATUNA,

Menimbang : a. bahwa untuk mewujudkan tata kelola, manajemen, layanan pemerintahan dan publik yang bersih, efektif, transapan, akuntabel, berkualitas dan terpercaya diperlukan sistem pemerintahan berbasis elektronik;

b. bahwa untuk menyelenggarakan sistem pemerintahan berbasis elektronik diperlukan pengelolaan dan pemanfaatan teknologi informasi dan komunikasi yang handal;

c. bahwa berdasarkan ketentuan dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik guna optimalisasi pelaksanaan penyelenggaraan sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Natuna, maka Peraturan Bupati ini mulai berlaku, Peraturan Bupati Natuna Nomor 60 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Natuna sebagaimana telah diubah dengan Peraturan Bupati Nomor 17 Tahun 2023 tentang Perubahan Atas Peraturan Bupati Natuna Nomor 60 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Natuna perlu diganti;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Undang-Undang Nomor 53 Tahun 1999 tentang Pembentukan Kabupaten Pelalawan, Kabupaten Rokan Hulu, Kabupaten Rokan Hilir, Kabupaten Siak, Kabupaten Karimun, Kabupaten Natuna, Kabupaten Kuantan Singingi, dan Kota Batam (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 181, Tambahan Lembaran Negara Republik Indonesia Nomor 3902) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 34 Tahun 2008 tentang Perubahan Ketiga

Atas Undang-Undang Nomor 53 Tahun 1999 tentang Pembentukan Kabupaten Pelalawan, Kabupaten Rokan Hulu, Kabupaten Rokan Hilir Kabupaten Siak, Kabupaten Karimun, Kabupaten Natuna, Kabupaten Kuantan Singingi, dan Kota Batam (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 107, Tambahan Lembaran Negara Republik Indonesia Nomor 4880);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 224, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 238, Tambahan Lembaran Negara Republik Indonesia Nomor 6841);
4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
5. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
6. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
8. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 215, Tambahan Lembaran Negara Republik Indonesia Nomor 5357);
9. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
10. Peraturan Presiden Nomor 81 Tahun 2010 tentang Grand Design Reformasi Birokrasi 2010-2025;

11. Peraturan Menteri Pendayagunaan Aparatur Negara Reformasi Birokrasi Nomor 10 Tahun 2011 tentang Pedoman Pelaksanaan Program Manajemen Perubahan;
12. Peraturan Menteri Pendayagunaan Aparatur Negara Reformasi Birokrasi Nomor 14 Tahun 2011 tentang Pedoman Pelaksanaan Program Manajemen Pengetahuan (*Knowledge Management*);
13. Peraturan Kepala Badan Pengkajian dan Penerapan Teknologi Nomor 007a Tahun 2017 tentang Pelaksanaan Audit Teknologi;
14. Peraturan Menteri Pendayagunaan Aparatur Negara Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
15. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
16. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
17. Peraturan Menteri Perencanaan Pembangunan/Kepala Badan Perencanaan Pembangunan Nasional Nomor 16 Tahun 2020 tentang Manajemen Data Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1573);
18. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE;

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG SISTEM PEMERINTAHAH BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Natuna.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Natuna.
3. Bupati adalah Bupati Natuna.
4. Perangkat Daerah adalah unsur pembantu kepala daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
5. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi

dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.

6. Tata Kelola SPBE adalah kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu.
7. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas.
8. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
9. Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, Data dan informasi, infrastruktur SPBE, aplikasi SPBE dan keamanan SPBE untuk menghasilkan Layanan SPBE yang terintegrasi.
10. Arsitektur SPBE Pemerintah Daerah adalah Peta Rencana SPBE yang diterapkan di Pemerintah Daerah.
11. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan pelaksanaan SPBE yang terintegrasi.
12. Peta Rencana SPBE Pemerintah Daerah adalah Peta Rencana SPBE yang diterapkan di Pemerintah Daerah.
13. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi instansi pusat dan Pemerintah Daerah masing-masing.
14. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi Data, pengolahan dan penyimpanan Data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
15. Infrastruktur SPBE Pemerintah Daerah adalah Infrastruktur SPBE yang diselenggarakan oleh Pemerintah Daerah masing-masing.
16. Pengguna SPBE adalah instansi pusat, Pemerintah Daerah, pegawai aparatur sipil negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan Layanan SPBE Pemerintah Daerah.
17. Manajemen Risiko adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE.
18. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
19. Tim Pelaksana Teknis Keamanan SPBE adalah Tim yang bertugas dalam melaksanakan keamanan SPBE di lingkungan Pemerintah Daerah.
20. Teknologi Informasi dan Komunikasi adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, pemindahan informasi antar media yang menggunakan media elektronik.
21. Aset Informasi adalah semua sumber daya yang dimiliki pemerintah daerah dalam bentuk Data dasar, Data informasi hasil proses sistem informasi, dokumen dalam

bentuk kertas dan digital, sumber kode sistem informasi, dokumen desain, perencanaan, hasil monitoring dan Evaluasi.

22. Evaluasi adalah proses pemeriksaan terhadap sistem, proses, program, dan produk dalam rangka untuk memastikan keabsahan, kehandalan, dan kesesuaian dengan standar yang berlaku atas permintaan Perangkat Daerah.
23. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
24. Aplikasi Umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh Pemerintah Daerah.
25. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh pemerintah daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.
26. Data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar, peta, tanda. Isyarat, tulisan, suara dan/atau bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi atau situasi.
27. Metadata adalah informasi dalam bentuk struktur dan format yang baku untuk menggambarkan Data, menjelaskan Data, serta memudahkan pencairan, penggunaan dan pengelolaan informasi Data.
28. Interoperabilitas Data adalah kemampuan Data untuk dibagipakaikan antar Sistem Elektronik yang saling berinteraksi.
29. Data Referensi adalah komponen yang mendeskripsikan substansi Data yang berupa spesifikasi dan kategorisasi, dan ketentuan mengenai Data, serta mengintegrasikannya dengan domain Arsitektur SPBE yang lain.
30. Kode Referensi adalah tanda berisi karakter yang mengandung atau menggambarkan makna, maksud atau norma tertentu sebagai rujukan identitas Data yang bersifat unik.
31. Data Induk adalah Data yang mempresentasikan objek dalam Proses Bisnis pemerintah sesuai dengan Peraturan Bupati Natuna tentang Indonesia Tingkat Kabupaten Natuna.
32. Manajemen Data adalah proses pengelolaan Data mencakup perencanaan, pengumpulan, pemeriksaan dan penyebarluasan yang dilakukan secara efektif dan efisien sehingga diperoleh Data yang akurat, mutakhir dan terintegrasi.
33. Arsitektur Data adalah model yang mengatur dan menentukan jenis Data yang dikumpulkan, disimpan, dikelola dan diintegrasikan dalam SPBE.
34. Manajemen Basis Data adalah proses pengelolaan kumpulan Data yang disimpan di Open Data Natuna.
35. Daftar Data adalah usulan Data yang disampaikan oleh WaliData sebagai bahan penyusunan Data prioritas dalam Forum Satu Data Indonesia Tingkat Kabupaten Natuna.

36. Audit Teknologi Informasi dan Komunikasi adalah proses yang sistematis untuk memperoleh dan mengEvaluasi bukti secara objektif terhadap aset Teknologi Informasi dan Komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara Teknologi Informasi dan Komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
37. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
38. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.
39. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan Sistem Elektronik.
40. Audit Infrastruktur SPBE adalah proses yang sistematis untuk memperoleh dan mengEvaluasi bukti secara objektif terhadap aset Infrastruktur SPBE dengan tujuan untuk menetapkan tingkat kesesuaian antara Infrastruktur SPBE dengan kriteria dan/atau standar yang telah ditetapkan.
41. Audit Aplikasi SPBE adalah proses yang sistematis untuk memperoleh dan mengEvaluasi bukti secara objektif terhadap aset Aplikasi SPBE dengan tujuan untuk menetapkan tingkat kesesuaian antara Aplikasi SPBE dengan kriteria dan/atau standar yang telah ditetapkan.
42. Auditor adalah orang yang memiliki kompetensi pengetahuan dan keterampilan khusus dengan tugas utama melakukan Evaluasi atas pengendalian Sistem Elektronik yang dapat dipertanggungjawabkan secara akademis maupun praktis.
43. Pusat Data adalah fasilitas yang digunakan untuk penempatan Sistem Elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan Data, serta pemulihan Data.
44. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
45. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
46. Pusat Data Nasional adalah sekumpulan pusat Data yang digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah, dan saling terhubung.
47. Jaringan Intra Pemerintah adalah jaringan interkoneksi tertutup yang menghubungkan antar jaringan intra instansi pusat dan pemerintah daerah.
48. Sistem Penghubung Layanan Pemerintah adalah perangkat terintegrasi yang terhubung dengan sistem penghubung layanan instansi pusat dan pemerintah

daerah untuk pertukaran layanan SPBE antar instansi pusat dan/atau pemerintah daerah.

49. *Auditee* adalah instansi pusat dan pemerintah daerah yang menjadi objek dari pelaksanaan Audit Infrastruktur SPBE dan Audit Aplikasi SPBE.
50. Kesepakatan Tingkat Layanan (*Service Level Agreement*) yang selanjutnya disingkat SLA adalah sasaran tingkat layanan yang disepakati antara perangkat daerah dengan pihak ketiga.
51. Rencana Pemulihan Bencana (*Disaster recovery plans*) adalah perencanaan terperinci mengenai prosedur pemulihan layanan pasca bencana.

Pasal 2

Maksud Peraturan Bupati ini adalah sebagai pedoman untuk mengatur penyelenggaraan SPBE oleh Pemerintah Daerah.

(1) Tujuan Peraturan Bupati ini adalah:
   a. memberikan landasan hukum bagi pelaksanaan SPBE di Pemerintah Daerah secara terpadu;
   b. mendorong pelaksana SPBE di Pemerintah Daerah untuk melaksanakan tugas dan fungsinya secara profesional;
   c. meningkatkan sinkronisasi dalam proses dan penjaminan kualitas pelaksanaan layanan pemerintah dan publik;
   d. meningkatkan transparansi dan akuntabilitas kinerja Pemerintah Daerah;
   e. mendukung proses pemantauan dan Evaluasi SPBE Pemerintah Daerah serta Audit Teknologi Informasi dan Komunikasi;
   f. memenuhi kebutuhan akses dan ketersediaan Data dan/atau informasi; dan
   g. meningkatkan kualitas pelaksanaan pemerintahan yang memanfaatkan Teknologi Informasi dan Komunikasi secara efektif, efisien, dan berkesinambungan.

Pasal 3

(1) SPBE di Pemerintah Daerah dilaksanakan berdasarkan prinsip:
   a. efektivitas;
   b. keterpaduan;
   c. kesinambungan;
   d. efisiensi;
   e. akuntabilitas;
   f. interoperabilitas; dan
   g. keamanan.
(2) Efektivitas sebagaimana dimaksud pada ayat (1) huruf a merupakan optimalisasi pemanfaatan sumber daya yang mendukung SPBE yang berhasil guna sesuai dengan kebutuhan.
(3) Keterpaduan sebagaimana dimaksud pada ayat (1) huruf b merupakan pengintegrasian sumber daya yang mendukung SPBE.

(4) Kesinambungan sebagaimana dimaksud pada ayat (1) huruf c merupakan keberlanjutan SPBE secara terencana, bertahap, dan terus menerus sesuai dengan perkembangannya.
(5) Efisiensi sebagaimana dimaksud pada ayat (1) huruf d merupakan optimalisasi pemanfaatan sumber daya yang mendukung SPBE yang tepat guna.
(6) Akuntabilitas sebagaimana dimaksud pada ayat (1) huruf e merupakan kejelasan fungsi dan pertanggungjawaban dari SPBE.
(7) Interoperabilitas sebagaimana dimaksud pada ayat (1) huruf f merupakan koordinasi dan kolaborasi antar Proses Bisnis dan antar Sistem Elektronik, dalam rangka pertukaran Data, Informasi, atau Layanan SPBE.
(8) Keamanan sebagaimana dimaksud pada ayat (1) huruf g merupakan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya yang mendukung SPBE.

Pasal 4

Ruang lingkup dalam Peraturan Bupati ini meliputi:
a. tata kelola SPBE;
b. Manajemen SPBE;
c. Audit Teknologi Informasi dan Komunikasi;
d. penyelenggara SPBE;
e. percepatan SPBE; dan
f. pemantauan dan Evaluasi SPBE.

BAB II
TATA KELOLA
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Bagian Kesatu
Umum

Pasal 5

(1) Tata kelola SPBE sebagaimana dimaksud dalam Pasal 4 huruf a, bertujuan untuk memastikan penerapan unsur-unsur SPBE di Pemerintah Daerah secara terpadu.
(2) Unsur-unsur SPBE sebagaimana dimaksud pada ayat (1) meliputi:
    a. Arsitektur SPBE;
    b. Peta Rencana SPBE;
    c. rencana dan anggaran SPBE;
    d. Proses Bisnis;
    e. Data dan informasi;
    f. Infrastruktur SPBE;
    g. Aplikasi SPBE;
    h. Keamanan SPBE; dan
    i. Layanan SPBE.

Bagian Kedua
Arsitektur Sistem Pemerintah Berbasis Elektronik

Pasal 6

(1) Arsitektur SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a disusun untuk memberikan panduan dalam pelaksanaan:
   a. referensi arsitektur; dan
   b. domain arsitektur.
(2) Referensi arsitektur sebagaimana dimaksud pada ayat (1) huruf a mendeskripsikan komponen dasar arsitektur baku yang digunakan sebagai acuan untuk penyusunan setiap domain arsitektur.
(3) Domain arsitektur SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (1) huruf b terdiri atas:
   a. domain arsitektur Proses Bisnis;
   b. domain Arsitektur Data dan informasi;
   c. domain arsitektur infrastruktur SPBE;
   d. domain arsitektur Aplikasi SPBE;
   e. domain arsitektur Keamanan SPBE; dan
   f. domain arsitektur Layanan SPBE.

Pasal 7

(1) Arsitektur SPBE Pemerintah Daerah disusun dengan berpedoman pada Arsitektur Nasional dan Rencana Pembangunan Jangka Menengah Daerah Kabupaten Natuna.
(2) Arsitektur SPBE Pemerintah Daerah disusun untuk jangka waktu 5 (lima) tahun sekali.
(3) Arsitektur SPBE sebagaimana dimaksud pada ayat (1) disusun oleh Tim Koordinasi.
(4) Arsitektur SPBE ditetapkan dengan Keputusan Bupati.
(5) Tim sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Bupati.

Pasal 8

(1) Arsitektur SPBE Pemerintah Daerah dilakukan reviu paling singkat 1 (satu) kali dalam 1 (satu) tahun atau sewaktu-waktu sesuai dengan kebutuhan.
(2) Reviu Arsitektur SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan:
   a. perubahan Arsitektur SPBE Nasional;
   b. hasil pemantauan dan Evaluasi SPBE Pemerintah Daerah;
   c. perubahan pada unsur SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf c sampai dengan huruf i; /atau
   d. perubahan Rencana Pembangunan Jangka Menengah Daerah Kabupaten Natuna.
(3) Reviu Arsitektur SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Tim Koordinasi SPBE Pemerintah Daerah dengan Persetujuan Bupati.

Bagian Ketiga
Peta Rencana Sistem Pemerintah Berbasis Elektronik

Pasal 9

(1) Peta Rencana SPBE Pemerintah Daerah disusun dalam bentuk program dan kegiatan SPBE Pemerintah Daerah untuk pembangunan, pengembangan, dan penerapan SPBE Pemerintah Daerah.
(2) Peta Rencana SPBE Pemerintah Daerah disusun untuk jangka waktu 5 (lima) tahun.
(3) Peta Rencana SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (1) memuat:
    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.
(4) Peta Rencana SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b disusun oleh Tim Koordinasi SPBE dengan berpedoman pada Peta Rencana SPBE Nasional, Arsitektur SPBE Pemerintah Daerah, Rencana Pembangunan Jangka Menengah Daerah, dan Rencana Strategis Perangkat Daerah Pemerintah Daerah.
(5) Peta Rencana SPBE ditetapkan dengan Keputusan Bupati.
(6) Peta Rencana SPBE, dilakukan reviu paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau berdasarkan:
    a. perubahan Peta Rencana SPBE;
    b. perubahan Rencana Pembangunan Jangka Menengah Daerah Pemerintah;
    c. perubahan Arsitektur SPBE; dan/atau
    d. hasil pemantauan dan Evaluasi SPBE.
(7) Reviu Peta Rencana SPBE sebagaimana dimaksud pada ayat (4) dilakukan oleh Tim Koordinasi SPBE.

Bagian Keempat
Rencana dan Anggaran Sistem Pemerintahan Berbasis Elektronik

Pasal 10

(1) Rencana dan anggaran SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf c berpedoman pada Arsitektur SPBE Pemerintah Daerah dan Peta Rencana SPBE Pemerintah Daerah serta dengan mempertimbangkan usulan dan kebutuhan anggaran SPBE dari seluruh Perangkat Daerah.
(2) Penyusunan rencana dan anggaran SPBE sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Perangkat Daerah yang melaksanakan fungsi penunjang urusan pemerintahan di bidang Perencanaan Pembangunan Daerah.
(3) Penyusunan rencana dan anggaran SPBE dikoordinasikan dengan Perangkat Daerah yang melaksanakan fungsi penunjang urusan pemerintahan di bidang perencanaan pembangunan daerah dan di bidang keuangan.

Bagian Kelima
Proses Bisnis

Pasal 11

(1) Proses Bisnis sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf d disusun berdasarkan pada Arsitektur SPBE Pemerintah Daerah.
(2) Penyusunan Proses Bisnis untuk memberikan pedoman dalam penggunaan Data dan informasi, pengembangan, dan penerapan Aplikasi SPBE, Keamanan SPBE dan Layanan SPBE.
(3) Dokumen hasil penyusunan Proses Bisnis ditetapkan selaras dengan Penetapan Pengaturan Rencana Pembangunan Jangka Menengah Daerah.

Pasal 12

(1) Proses Bisnis disusun oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang penatalaksanaan administrasi, yang berkoordinasi dengan Tim Koordinasi SPBE.
(2) Proses Bisnis sebagaimana dimaksud pada ayat (1) disusun dengan mempertimbangkan integrasi antar:
    a. Aplikasi SPBE; dan
    b. Layanan SPBE.

Bagian Keenam
Data dan Informasi

Pasal 13

(1) Data dan informasi sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf e mencakup semua jenis Data dan informasi yang dimiliki oleh Pemerintah Daerah melalui Perangkat Daerah dan/atau yang diperoleh dari Masyarakat, pelaku usaha, dan/atau pihak lain.
(2) Perangkat Daerah sebagaimana dimaksud pada ayat (2) adalah Perangkat Daerah yang menyelenggarakan urusan di bidang komunikasi dan informatika yang bertanggung jawab atas keakuratan Data dan informasi yang disediakan serta keamanan Data dan informasi yang bersifat strategis dan/atau rahasia.
(3) Data dan Informasi sebagaimana dimaksud pada ayat (2) harus memenuhi kriteria:
    a. berdasarkan standar Data dan informasi;
    b. berbagi pakai Data dan informasi;
    c. mudah diakses; dan
    d. selaras dengan Arsitektur SPBE.

Pasal 14

(1) Data dan informasi sebagaimana dimaksud dalam Pasal 13 ayat (1) diintegrasikan dalam bentuk Sistem Elektronik oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

(2) Pemerintah Daerah menggunakan Data dan informasi didasarkan pada Arsitektur SPBE Pemerintah Daerah.
(3) Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika, bertanggung jawab menjamin keamanan, kerahasiaan, keutuhan, keaslian, dan kenirsangkalan Data dan informasi sesuai dengan standar berdasarkan ketentuan Peraturan Perundang-undangan.
(4) Data dan informasi disediakan dan dikelola oleh Perangkat Daerah sesuai dengan tugas dan fungsinya berdasarkan prinsip Satu Data Indonesia.
(5) Data dan informasi merupakan bagian dan digunakan dalam penyelenggaraan SPBE.
(6) Penggunaan Data dan Informasi dilakukan dengan mengutamakan bagi pakai Data dan Informasi antar Perangkat Daerah di Pemerintah Daerah, Instansi Pusat, dan/atau Pemerintah Daerah dengan berdasarkan tujuan dan cakupan, penyediaan akses Data dan Informai, dan pemenuhan standar Interoperabilitas Data dan Informasi.

Bagian Ketujuh
Infrastruktur Sistem Pemerintah Berbasis Elektronik

Pasal 15

(1) Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf f digunakan untuk meningkatkan efisiensi, keamanan, dan kemudahan integrasi dalam rangka memenuhi kebutuhan Infrastruktur SPBE bagi Pemerintah Daerah.
(2) Infrastruktur SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. perangkat Teknologi Informasi dan Komunikasi;
    b. Pusat Data yang memanfaatkan Pusat Data Nasional;
    c. pusat pemulihan Data Pemerintah; dan
    d. perangkat jaringan dan komunikasi Data Pemerintah Daerah.
(3) Infrastruktur SPBE Pemerintah Daerah diselenggarakan dan dikelola oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
(4) Infrastruktur SPBE sebagaimana dimaksud pada ayat (2) harus dimanfaatkan secara bagi pakai oleh seluruh Perangkat Daerah.
(5) Pembangunan dan pengembangan Infrastruktur SPBE Pemerintah Daerah didasarkan pada Arsitektur SPBE Pemerintah Daerah.
(6) Infrastruktur SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (1) sesuai dengan standar perangkat, standar interoperabilitas, standar keamanan sistem informasi, dan standar lainnya berdasarkan ketentuan Peraturan Perundang-undangan.

Pasal 16

(1) Perangkat Teknologi Informasi dan Komunikasi dalam Tata Kelola Data dan Pusat Informasi dalam bentuk Sistem Elektronik, merupakan semua peralatan yang mendukung jalannya SPBE Pemerintah Daerah, meliputi:
   a. server;
   b. *storage*;
   c. *router* dan *switch*;
   d. *unit power supply*;
   e. media koneksi jaringan;
   f. ruang Pusat Data serta perangkat pendukungnya; dan/atau
   g. ruangan *network operation center* sebagai pengendali atau pemantauan Pusat Data Pemerintah Daerah.

(2) Penatausahaan perangkat Teknologi Informasi dan Komunikasi sebagaimana dimaksud pada ayat (1) meliputi:
   a. perencanaan;
   b. pengadaan;
   c. pengelolaan;
   d. penghapusan.

(3) Penatausahaan perangkat Teknologi Informasi dan Komunikasi sebagaimana dimaksud pada ayat (2) dilakukan oleh Perangkat Daerah di lingkungan Pemerintah Daerah dan berkoordinasi dengan Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika dan Tim Koordinasi SPBE Pemerintah Daerah.

(4) Pengelolaan sebagaimana dimaksud pada ayat (2) huruf c sesuai dengan standar dan mekanisme yang ditetapkan oleh Perangkat Daerah yang menyelenggarakan tugas dan urusan pemerintahan komunikasi dan informatika.

Pasal 17

(1) Pusat Data Pemerintah Daerah sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b merupakan beberapa Pusat Data yang saling terhubung dan digunakan secara bagi pakai oleh Perangkat Daerah di lingkungan Pemerintah Daerah.

(2) Pusat Data Pemerintah Daerah sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. Pusat Data yang diselenggarakan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika; dan
   b. Pusat Data lainnya yang diizinkan oleh ketentuan Peraturan Perundang-undangan.

(3) Pusat Data Pemerintah Daerah sebagaimana dimaksud pada ayat (1) berfungsi untuk:
   a. mengelola kelancaran layanan dan Infrastruktur SPBE Pemerintah Daerah;
   b. mengelola penyimpanan dan kelancaran lalu lintas Data dan informasi yang diperlukan Pengguna SPBE; dan

c. mengatur akses Data dan/atau informasi sesuai dengan kewenangan Perangkat Daerah di lingkungan Pemerintah Daerah.

(4) Desain dan manajemen Pusat Data Pemerintah Daerah sebagaimana dimaksud pada ayat (1) harus memenuhi standar nasional Indonesia.

(5) Dalam hal standar nasional Indonesia sebagaimana dimaksud pada ayat (4) belum tersedia, dapat menggunakan standar internasional.

Pasal 18

(1) Pusat pemulihan Data Pemerintah Daerah sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c merupakan cadangan dari Pusat Data Pemerintah Daerah dalam rangka menjamin keamanan Data pada saat Pusat Data Pemerintah Daerah tidak berfungsi.

(2) Pusat pemulihan Data Pemerintah Daerah sebagaimana dimaksud pada ayat (1) diselenggarakan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

Pasal 19

Perangkat jaringan dan komunikasi Data Pemerintah Daerah sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf d merupakan semua/peralatan yang mendukung jaringan komunikasi Data yang digunakan secara berbagi pakai meliputi:

a. Jaringan Intra Pemerintah Daerah;
b. sistem penghubung layanan Pemerintah Daerah; dan
c. *bandwidth.*

Pasal 20

(1) Jaringan Intra Pemerintah Daerah sebagaimana dimaksud dalam Pasal 19 huruf a merupakan Jaringan Intra yang diselenggarakan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika untuk menghubungkan antar simpul jaringan dalam Pemerintah Daerah.

(2) Penggunaan Jaringan Intra Pemerintah Daerah bertujuan untuk menjaga keamanan dalam melakukan pengiriman Data dan informasi antar simpul jaringan di lingkungan Pemerintah Daerah.

(3) Penggunaan Jaringan Intra Pemerintah Daerah sebagaimana dimaksud pada ayat (1) harus memenuhi ketentuan sebagai berikut:
   a. membuat keterhubungan dengan Jarinan Intra pemerintah;
   b. mendapatkan pertimbangan kelaikan operasi dari kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika; dan

c. mendapatkan pertimbangan kelaikan keamanan dari kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(4) Pelaksanaan Jaringan Intra Pemerintah Daerah sebagaimana dimaksud pada ayat (1) dapat menggunakan jaringan fisik yang dibangun oleh Pemerintah Daerah dan/atau penyedia jasa layanan jaringan.

Pasal 21

(1) Sistem Penghubung Layanan Pemerintah Daerah sebagaimana dimaksud dalam Pasal 19 huruf b merupakan perangkat integrasi yang terhubung dengan Sistem Penghubung Layanan Pemerintah Daerah yang diselenggarakan oleh Perangkat Daerah yang menyelenggarakan tugas dan urusan pemerintahan di bidang komunikasi dan informatika untuk melakukan pertukaran Layanan SPBE dalam Pemerintah Daerah.

(2) Dalam menggunakan Sistem Penghubung Layanan Pemerintah Daerah sebagaimana dimaksud pada ayat (1), harus:
   a. membuat keterhubungan dan akses Jaringan Intra Pemerintah Daerah;
   b. memenuhi standar interoperabilitas antar Layanan SPBE Pemerintah Daerah sesuai dengan ketentuan Peraturan Perundang-undangan;
   c. mendapatkan pertimbangan kelaikan operasi sesuai dengan ketentuan Peraturan Perundang-undangan; dan
   d. mendapatkan pertimbangan kelaikan keamanan sesuai dengan ketentuan Peraturan Perundang-undangan.

(3) Pengaturan/norma penggunaan sistem penghubung Layanan Perangkat Daerah di lingkungan Pemerintah Daerah.

Pasal 22

(1) *Bandwidth* sebagaimana dimaksud dalam Pasal 19 huruf c merupakan kapasitas transfer Data yang dapat digunakan pada perangkat jaringan dan komunikasi Data.

(2) Kebutuhan *bandwidth* diusulkan oleh Perangkat Daerah dan ditetapkan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika berdasarkan skala prioritas.

(3) Pemantauan dan Evaluasi penggunaan *bandwidth* dilakukan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika, melalui sistem otomatis dan diEvaluasi setiap bulan.

(4) Hasil Evaluasi sebagaimana dimaksud pada ayat (3) disampaikan kepada Tim Koordinasi SPBE Pemerintah Daerah sebagai bahan perencanaan kebutuhan *bandwidth* di lingkungan Pemerintah Daerah.

Bagian Kedelapan
Aplikasi Sistem Pemerintahan Berbasis Elektronik

Pasal 23

Aplikasi SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf g digunakan oleh Perangkat Daerah di lingkungan Pemerintah Daerah untuk memberikan Layanan SPBE kepada Pengguna SPBE.

Pasal 24

(1) Aplikasi SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 22 terdiri atas:
    a. Aplikasi Umum; dan
    b. Aplikasi Khusus.
(2) Pembangunan dan pengembangan Aplikasi SPBE Pemerintah Daerah mengutamakan penggunaan kode sumber terbuka yang dilaksanakan berdasarkan siklus pengembangan sistem yang meliputi tahap:
    a. perencanaan;
    b. analisis;
    c. pembangunan dan/atau pengembangan;
    d. penerapan; dan
    e. pemeliharaan.
(3) Pembangunan dan pengembangan Aplikasi SPBE Pemerintah Daerah secara terpadu dikoordinasikan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
(4) Standar dan teknis tata kelola Aplikasi SPBE sebagaimana tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 25

(1) Aplikasi Umum sebagaimana dimaksud dalam Pasal 23 ayat (1) huruf a dibangun dan dikembangkan:
    a. selaras dengan Arsitektur SPBE Nasional; dan
    b. berpedoman pada Rencana Induk SPBE Nasional;
    c. memenuhi standar teknis dan prosedur pembangunan; dan
    d. pengembangan Aplikasi Umum sesuai dengan ketentuan Peraturan Perundang-undangan.
(2) Aplikasi Umum dan kode sumbernya didaftarkan dan disimpan pada repositori Aplikasi SPBE.
(3) Repositori Aplikasi SPBE sebagaimana dimaksud pada ayat (1) dikelola oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
(4) Setiap Perangkat Daerah di lingkungan Pemerintah Daerah harus menggunakan Aplikasi Umum.

Pasal 26

(1) Aplikasi Khusus sebagaimana dimaksud dalam Pasal 23 ayat (1) huruf b dibangun dan dikembangkan:
    a. selaras dengan Arsitektur SPBE Pemerintah Daerah;
    b. sesuai dengan tugas dan fungsi Pemerintah Daerah;

c. berpedoman kepada Rencana Induk SPBE Pemerintah Daerah; dan
d. memenuhi standar teknis dan prosedur yang telah ditetapkan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

(2) Sebelum melakukan pembangunan dan pengembangan Aplikasi Khusus sebagaimana dimaksud pada ayat (1), Perangkat Daerah harus mendapatkan pertimbangan dari Perangkat Daerah yang menyelenggarakan tugas dan fungsi di bidang komunikasi dan informatika dan menteri yang menyelenggarakan urusan pemerintahan di bidang aparat negara.

(3) Pembangunan dan pengembangan Aplikasi Khusus sebagaimana dimaksud pada ayat (1) harus memenuhi standar teknis dan prosedur pembangunan dan pengembangan Aplikasi Khusus sesuai dengan ketentuan Peraturan Perundang-undangan.

Bagian Kesembilan
Keamanan Sistem Pemerintahan Berbasis Elektronik

Pasal 27

(1) Keamanan SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf h, mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait Data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.

(2) Penjaminan Kerahasiaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan lainnya.

(3) Penjaminan keutuhan sebagaimana dimaksud pada ayat (1) dilakukan melalui pendeteksian modifikasi.

(4) Penjaminan ketersediaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penyediaan cadangan dan pemulihan.

(5) Penjaminan keaslian sebagaimana dimaksud pada ayat (1) dilakukan melalui penyediaan mekanisme verifikasi dan validasi.

(6) Penjaminan kenirsangkalan sebagaimana dimaksud pada ayat (1) dilakukan melalui penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital sesuai dengan ketentuan Peraturan Perundang-undangan.

(7) Penerapan Keamanan SPBE Pemerintah Daerah dilaksanakan dengan memenuhi standar teknis dan prosedur Keamanan SPBE sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 28

(1) Setiap Perangkat Daerah harus menerapkan Keamanan SPBE Pemerintah Daerah dalam penyelenggaraan SPBE Pemerintah Daerah.
(2) Dalam menerapkan Keamanan SPBE Pemerintah Daerah dan menyelesaikan permasalahan Keamanan SPBE Pemerintah Daerah, kepala Perangkat Daerah dapat melakukan konsultasi dan/atau koordinasi dengan Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika dan Tim Koordinasi SPBE Pemerintah Daerah.
(3) Penyelesaian permasalahan Keamanan SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (2) dilakukan sesuai dengan ketentuan Peraturan Perundang-undangan.

Bagian Kesepuluh
Layanan Sistem Pemerintahan Berbasis Elektronik

Pasal 29

Layanan SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf i terdiri atas:
a. layanan administrasi pemerintahan berbasis elektronik; dan
b. layanan publik berbasis elektronik.

Pasal 30

(1) Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 29 huruf a merupakan Layanan SPBE Pemerintah Daerah yang mendukung tata laksana internal birokrasi dalam rangka meningkatkan kinerja dan akuntabilitas Pemerintah Daerah.
(2) Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud pada ayat (1) meliputi layanan:
    a. perencanaan;
    b. penganggaran;
    c. keuangan;
    d. pengadaan barang dan jasa;
    e. kepegawaian;
    f. kearsipan;
    g. pengelolaan barang milik negara;
    h. pengawasan;
    i. akuntabilitas kinerja; dan
    j. layanan lain sesuai dengan kebutuhan internal Pemerintah Daerah.
(3) Penerapan layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud pada ayat (2) dilakukan dengan pembangunan dan pengembangan Aplikasi Umum sebagaimana dimaksud dalam Pasal 25.

Pasal 31

(1) Layanan publik berbasis elektronik sebagaimana dimaksud dalam Pasal 29 huruf b merupakan Layanan

SPBE yang mendukung pelaksanaan pelayanan publik sesuai dengan tugas dan fungsi Pemerintah Daerah.

(2) Layanan publik berbasis elektronik diterapkan dengan mengutamakan penggunaan Aplikasi Umum sebagaimana dimaksud dalam Pasal 25.

(3) Dalam hal layanan publik berbasis elektronik sebagaimana dimaksud pada ayat (2) memerlukan Aplikasi Khusus, Perangkat Daerah dapat melakukan pembangunan dan pengembangan Aplikasi Khusus sebagaimana dimaksud dalam Pasal 26.

(4) Penanggung jawab layanan publik berbasis elektronik sebagaimana dimaksud pada ayat (1) adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

Pasal 32

(1) Integrasi Layanan SPBE sebagaimana dimaksud dalam Pasal 21 merupakan proses yang menghubungkan Data dan informasi dari beberapa Layanan SPBE ke dalam satu kesatuan alur kerja Layanan SPBE.

(2) Integrasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

Pasal 33

(1) Perangkat Daerah yang menyelenggarakan Layanan SPBE sebagaimana dimaksud dalam Pasal 22, dapat membentuk pusat informasi dan bantuan.

(2) Pusat informasi dan bantuan sebagaimana dimaksud pada ayat (1) mempunyai tugas memberikan layanan kepada Pengguna SPBE dengan memberikan solusi permasalahan secara cepat dan tepat, dalam rangka mengatasi keluhan dan/atau permintaan Pengguna SPBE.

(3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), pusat informasi dan bantuan menyelenggarakan fungsi:
   a. narahubung;
   b. mencatat laporan gangguan layanan;
   c. mencatat permintaan layanan;
   d. memantau dan menginformasikan status gangguan dan permintaan layanan; dan
   e. menyediakan informasi, solusi, dan edukasi kepada Pengguna SPBE.

(4) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (3) pusat informasi dan bantuan dapat berkoordinasi dengan Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

BAB III
MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Bagian Kesatu
Umum

Pasal 34

(1) Manajemen SPBE meliputi:
   a. Manajemen Risiko;
   b. manajemen Keamanan Informasi;
   c. Manajemen Data;
   d. manajemen aset Teknologi Informasi dan Komunikasi;
   e. manajemen sumber daya manusia;
   f. manajemen pengetahuan;
   g. manajemen perubahan; dan
   h. manajemen Layanan SPBE.
(2) Manajemen SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan Peraturan Perundang-undangan.
(3) Standar dan Mekanisme Manajemen SPBE sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Bagian Kedua
Manajemen Risiko

Pasal 35

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf a bertujuan untuk menjamin keberlangsungan SPBE Pemerintah Daerah dengan mengurangi dampak risiko dalam SPBE Pemerintah Daerah.
(2) Manajemen Risiko dilakukan melalui serangkaian proses identifikasi, analisis, pengendalian, pemantauan, dan Evaluasi terhadap risiko dalam SPBE Pemerintah Daerah.
(3) Dalam pelaksanaan Manajemen Risiko, Perangkat Daerah berkoordinasi dengan Tim Koordinasi SPBE Pemerintah Daerah.
(4) Manajemen Risiko dilaksanakan sesuai dengan ketentuan Peraturan Perundang-undangan.

Bagian Ketiga
Mananajemen Keamanan Informasi

Pasal 36

(1) Manajemen Keamanan Informasi sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf b bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko Keamanan Informasi.
(2) Manajemen Keamanan Informasi dilakukan melalui rangkaian proses yang meliputi
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;

c. perencanaan;
d. pengoperasian;
e. Evaluasi kinerja; dan
f. perbaikan berkelanjutan terhadap Keamanan Informasi dalam SPBE.

(3) Ketentuan lain untuk mendukung kebijakan internal manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi :
a. Manajemen Risiko;
b. penetapan prosedur pengendalian Keamanan Informasi SPBE; dan
c. pengelolaan pihak ketiga.

(4) Dalam pelaksanaan manajemen Keamanan Informasi, Perangkat Daerah berkoordinasi dengan Tim Koordinasi SPBE Pemerintah Daerah.

Pasal 37

(1) Penetapan ruang lingkup manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 36 ayat (2) huruf a meliputi:
a. Data dan informasi SPBE;
b. Aplikasi SPBE; dan
c. Infrastruktur SPBE.

(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 38

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 36 ayat (2) huruf b dilaksanakan oleh Bupati.

(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh sekretaris daerah Kabupaten Natuna.

(3) Sekretaris daerah Kabupaten Natuna sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan Peraturan Perundang-undangan.

Pasal 39

(1) Sekretaris daerah sebagai penanggung jawab manajemen Keamanan Informasi SPBE dan koordinator SPBE sebagaimana dimaksud dalam Pasal 38 ayat (3) menunjuk pelaksana teknis Keamanan SPBE.

(2) Pelaksana teknis Keamanan SPBE sebagai dimaksud pada ayat (1) terdiri atas:
a. ketua tim; dan
b. anggota tim.

(3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh pimpinan Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan Perangkat Daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah.

Pasal 40

(1) Ketua tim sebagaimana dimaksud dalam Pasal 39 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:
   a. menetapkan prosedur pengendalian Keamanan Informasi SPBE;
   b. mengEvaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Pemerintah Daerah;
   c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan Peraturan Perundang-undangan;
   d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
   e. memutuskan dan merancang langkah kelangsungan layanan Teknologi Informasi dan Komunikasi dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
   f. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE pada koordinator SPBE.
(2) Anggota tim sebagaimana dimaksud dalam Pasal 39 ayat (2) huruf b mempunyai tugas:
   a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian Keamanan Informasi SPBE pada Perangkat Daerah masing-masing;
   b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan Peraturan Perundang-undangan;
   c. melaksanakan dan mengelola langkah kelangsungan layanan Teknologi Informasi dan Komunikasi yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
   d. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 41

(1) Perencanaan sebagaimana dimaksud dalam Pasal 36 ayat (2) huruf c disusun oleh ketua Tim Pelaksana Teknis Keamanan SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
   a. program kerja Keamanan SPBE; dan
   b. target realisasi program kerja Keamanan SPBE.

Pasal 42

(1) Program kerja Keamanan SPBE sebagaimana dimaksud pada Pasal 41 ayat (2) huruf a paling sedikit meliputi:
   a. edukasi kesadaran Keamanan SPBE;
   b. penilaian kerentanan Keamanan SPBE;
   c. peningkatan Keamanan SPBE;
   d. penanganan insiden Keamanan SPBE; dan
   e. audit Keamanan SPBE.

(2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada Pasal 41 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 43

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 36 ayat (2) huruf d dilakukan oleh koordinator SPBE.

(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
   a. sumber daya manusia Keamanan SPBE;
   b. teknologi Keamanan SPBE; dan
   c. anggaran Keamanan SPBE.

(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen Keamanan Informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 44

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada Pasal 43 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
   a. keamanan Teknologi Komunikasi dan Informatika; dan
   b. keamanan aplikasi.

(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
   a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan Teknologi Informasi dan Komunikasi; dan/atau
   b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.

(3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.

(4) Teknologi Keamanan Informasi sebagaimana dimaksud pada Pasal 43 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada Pasal 43 ayat (2) huruf c disusun berdasarkan

perencanaan yang telah ditetapkan sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 45

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 36 ayat (2) huruf e dilakukan oleh koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
    b. menetapkan indikator kinerja pada setiap area proses;
    c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
    d. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
    e. mendukung dan merealisasikan program audit Keamanan SPBE.
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 46

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 36 ayat (2) huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil Evaluasi kinerja.
(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
    a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE;
    b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
    c. tindak lanjut hasil audit Keamanan SPBE.

Pasal 47

(1) Manajemen Risiko sebagaimana dimaksud dalam Pasal 36 ayat (3) huruf a dilakukan oleh setiap Perangkat Daerah.
(2) Manajemen Risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (*risk register*) dengan ketentuan subtansi meliputi:
    a. inventarisasi aset SPBE;
    b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
    c. penilaian risiko keamanan terhadap aset SPBE;
    d. penentuan prioritas risiko;
    e. analisa dampak jika terjadi risiko;

f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
g. rekomendasi kontrol keamanan.

(3) Prosedur pelaksanaan Manajemen Risiko mengacu sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 48

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada Pasal 36 ayat (3) huruf b sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

(2) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah dengan cangkupan aspek dapat meliputi:
a. keamanan perangkat teknologi informasi komunikasi;
b. keamanan jaringan;
c. keamanan Pusat Data;
d. keamanan perangkat *end point*;
e. keamanan *remote working*;
f. keamanan penyimpanan elektronik;
g. pengelolaan akses kontrol;
h. pengendalian keamanan dari ancaman virus dan *malware*;
i. persayaratan keamanan terkait pembangunan dan pengembangan Aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi Data;
l. konfigurasi perangkat *IT Security*;
m. perlindungan Data pribadi;
n. keamanan komunikasi;
o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
p. pengendalian Keamanan Informasi terhadap pihak ketiga;
q. penerapan kriptografi;
r. penanganan insiden Keamanan Informasi;
s. kelangsungan bisnis atau layanan TIK (*business continuity*);
t. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
u. audit internal Keamanan SPBE; dan/atau
v. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya.

(3) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 49

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada Pasal 48 ayat (3).
(2) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Informasi SPBE.

Pasal 50

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 36 ayat (3) huruf c dilakukan oleh setiap Perangkat Daerah.
(2) Perangkat Daerah harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
(3) Perangkat Daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
(4) Perangkat Daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan kerjasama dengan pihak ketiga.
(5) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian *service level aggreement* dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

Bagian Keempat
Manajemen Data

Pasal 51

(1) Manajemen Data sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf c bertujuan untuk menjamin terwujudnya Data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, Evaluasi, dan pengendalian pembangunan daerah.
(2) Manajemen Data dilakukan melalui rangkaian proses pengelolaan Arsitektur Data, Data Induk, Data Referensi, basis Data, dan kualitas Data.
(3) Dalam pelaksanaan Manajemen Data, Perangkat Daerah berkoordinasi dengan Tim Koordinasi SPBE Pemerintah Daerah.

Bagian Kelima
Manajemen Aset Teknologi Informasi dan Komunikasi

Pasal 52

(1) Manajemen aset Teknologi Informasi dan Komunikasi sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf d bertujuan untuk menjamin ketersediaan dan optimalisasi

pemanfaatan aset Teknologi Informasi dan Komunikasi dalam SPBE.

(2) Manajemen aset Teknologi Informasi dan Komunikasi dilakukan melalui serangkaian proses perencanaan, pengadaan, pengelolaan, dan penghapusan perangkat keras dan perangkat lunak yang digunakan dalam SPBE.

(3) Manajemen aset Teknologi Informasi dan Komunikasi dilaksanakan oleh seluruh Perangkat Daerah di lingkungan Pemerintah Daerah.

(4) Dalam pelaksanaan manajemen aset Teknologi Informasi dan Komunikasi, Perangkat Daerah berkoordinasi dengan Tim Koordinasi SPBE Pemerintah Daerah.

Bagian Keenam
Manajemen Sumber Daya Manusia

Pasal 53

(1) Manajemen Sumber Daya Manusia sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf e bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE dalam rangka memastikan ketersediaan dan peningkatan kompetensi sumber daya manusia untuk pelaksanaan Tata Kelola SPBE Pemerintah Daerah serta Manajemen SPBE Pemerintah Daerah.

(2) Manajemen sumber daya manusia dilakukan melalui serangkaian proses perencanaan, pengembangan, pembinaan, dan pendayagunaan sumber daya manusia dalam SPBE.

(3) Dalam pelaksanaan manajemen sumber daya manusia, Perangkat Daerah berkoordinasi dengan Perangkat Daerah yang melaksanakan fungsi penunjang urusan pemerintah di bidang aparatur Pemerintah Daerah.

(4) Manajemen sumber daya manusia memastikan ketersediaan dan kompetensi sumber daya manusia untuk pelaksanaan Tata Kelola SPBE dan Manajemen SPBE.

Bagian Ketujuh
Manajemen Pengetahuan

Pasal 54

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf f bertujuan untuk meningkatkan kualitas Layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE.

(2) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam SPBE.

(3) Manajemen pengetahuan dilaksanakan oleh seluruh Perangkat Daerah di lingkungan Pemerintah Daerah.

(4) Dalam pelaksanaan manajemen pengetahuan, Perangkat Daerah berkoordinasi dengan Tim Koordinasi SPBE Pemerintah Daerah.

Bagian Kedelapan
Manajemen Perubahan

Pasal 55

(1) Manajemen perubahan sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf g bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE melalui pengendalian perubahan yang terjadi dalam SPBE.
(2) Manajemen perubahan dilakukan melalui serangkaian proses perencanaan, analisis, pengembangan, implementasi, pemantauan dan Evaluasi terhadap perubahan SPBE.
(3) Manajemen perubahan sebagaimana dimaksud pada ayat (1) dilaksanakan oleh seluruh Perangkat Daerah yang menyelenggarakan Layanan SPBE.
(4) Dalam pelaksanaan manajemen perubahan, Perangkat Daerah berkoordinasi dengan Tim Koordinasi SPBE Pemerintah Daerah.

Bagian Kesembilan
Manajemen Layanan Sistem Pemerintahan Berbasis Elektronik

Pasal 56

(1) Manajemen Layanan SPBE sebagaimana dimaksud dalam Pasal 34 ayat (1) huruf h bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE Pemerintah Daerah kepada Pengguna SPBE.
(2) Manajemen Layanan SPBE dilakukan melalui serangkaian proses pelayanan Pengguna SPBE, pengoperasian Layanan SPBE, dan pengelolaan Aplikasi SPBE.
(3) Dalam pelaksanaan Manajemen Layanan SPBE, Perangkat Daerah berkoordinasi dengan Tim Koordinasi SPBE Pemerintah Daerah.

BAB IV
PENYELENGGARA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Pasal 57

(1) Penyelenggara SPBE Pemerintah Daerah terdiri atas:
    a. Tim Koordinasi; dan
    b. Tim Assesor.
(2) Tim Koordinasi dan Tim Assesor sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Bupati.

Pasal 58

(1) Tim Koordinasi SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 57 ayat (1) huruf a diketuai oleh sekretaris daerah.
(2) Tim Koordinasi sebagaimana dimaksud pada ayat (1) beranggotakan semua Perangkat Daerah yang bertugas menyelenggarakan koordinasi layanan administrasi pemerintahan berbasis elektronik dan Perangkat Daerah.

(3) Tim Koordinasi SPBE sebagaimana dimaksud pada ayat (1) mempunyai tugas:
   a. mengarahkan, memantau, dan mengEvaluasi pelaksanaan SPBE;
   b. melakukan koordinasi dengan Tim Koordinasi SPBE Nasional untuk pelaksanaan SPBE yang melibatkan lintas instansi Pusat dan Pemerintah Daerah;
   c. memfasilitasi proses koordinasi, kerja sama, atau integrasi penerapan SPBE dengan pihak-pihak eksternal dalam dan luar negeri;
   d. mengatur pemantauan, penillaian dan Evaluasi kebijakan SPBE secara berkala terhadap perubahan peraturan perkembangan teknologi dan/atau kebutuhan daerah; dan
   e. mengatur pelaksanaan manajemen perubahan kebijakan SPBE.

Pasal 59

(1) Tim Assesor SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 57 ayat (1) huruf b diketuai oleh kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
(2) Tim Assesor sebagaimana dimaksud pada ayat (1) beranggotakan semua Perangkat Daerah yang bertugas menyelenggarakan koordinasi layanan administrasi pemerintahan berbasis elektronik dan Perangkat Daerah terkait.
(3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (2), Tim Koordinasi menyelenggarakan fungsi:
   a. memfasilitasi perencanaan dan implementasi melalui program dan kegiatan SPBE;
   b. memfasilitasi peras koordinasi, kerja sama dan Manajemen SPBE; dan
   c. memfasilitasi proses koordinasi, kerja sama, atau integrasi penerapan SPBE dengan pihak-pihak terkait.

BAB V
AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

Pasal 60

(1) Dalam rangka memastikan kehandalan dan keamanan sistem Teknologi Informasi dan Komunikasi di lingkungan Pemerintah Daerah perlu dilakukan Audit Teknologi Informasi dan Komunikasi secara berkala.
(2) Audit Teknologi Informasi dan Komunikasi sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. audit Infrastruktur SPBE;
   b. Audit Aplikasi SPBE; dan
   c. audit Keamanan SPBE.
(3) Audit Teknologi Informasi dan Komunikasi dilakukan dengan melakukan pemeriksaan hal pokok teknis pada:
   a. penerapan tata kelola dan manajemen Teknologi Informasi dan Komunikasi;
   b. fungsionalitas Teknologi Informasi dan Komunikasi;

c. kinerja Teknologi Informasi dan Komunikasi yang dihasilkan; dan
d. aspek Teknologi Informasi dan Komunikasi lainnya.

(4) Audit Teknologi Informasi dan Komunikasi sebagaimana dimaksud pada ayat (2) dilaksanakan oleh lembaga pelaksana Audit Teknologi Informasi dan Komunikasi pemerintah atau lembaga pelaksana Audit Teknologi Informasi dan Komunikasi yang terakreditasi sesuai dengan ketentuan Peraturan Perundang-undangan.

(5) Sebagai persiapan pelaksanaan Audit Teknologi Informasi dan Komunikasi sebagaimana dimaksud pada ayat (4), satuan kerja yang menyelenggarakan tugas dan fungsi bidang komunikasi dan informatika melakukan audit internal paling lambat (1) satu bulan sebelumnya.

(6) Standar dan Teknis pelaksanaan Audit Teknologi Informasi dan Komunikasi sebagaimana tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 61

(1) Audit Teknologi Informasi dan Komunikasi Kabupaten Natuna dilaksanakan oleh Tim Auditor di bawah koordinasi Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang pengawasan dan pengendalian internal Pemerintah Daerah.

(2) Tim Auditor sebagaimana dimaksud pada ayat (1) ditetapkan dengan keputusan Bupati.

(3) Audit Teknologi Informasi dan Komunikasi dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun.

(4) Audit Teknologi Informasi dan Komunikasi dilaksanakan berdasarkan ketentuan Peraturan Perundang-undangan.

BAB VI
PEMANTAUAN DAN EVALUASI

Pasal 62

(1) Pemantauan SPBE dan Evaluasi SPBE bertujuan untuk:
a. mengetahui capaian kemajuan pelaksanaan SPBE; dan
b. memberikan saran perbaikan yang berkesinambungan untuk peningkatan kualitas pelaksanaan SPBE di Pemerintah Daerah.

(2) Pemantauan SPBE dan Evaluasi SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

(3) Pemantauan SPBE dan Evaluasi SPBE didasarkan pada pedoman dan Evaluasi SPBE.

(4) Pemantauan SPBE dan Evaluasi SPBE dilaksanakan oleh Tim Koordinasi.

(5) Dalam pelaksanaan teknis Pemantauan SPBE dan Evaluasi SPBE sebagaimana dimaksud pada ayat (4), dibentuk Tim Assesor internal yang ditetapkan dengan Keputusan Bupati.

(6) Hasil Pemantauan SPBE dan Evaluasi SPBE sebagaimana dimaksud pada ayat (2) disampaikan kepada Bupati melalui Tim Koordinasi SPBE.

BAB VII
KETENTUAN PENUTUP

Pasal 63

Pada saat Peraturan Bupati ini mulai berlaku, Peraturan Bupati Natuna Nomor 60 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Natuna (Berita Daerah Kabupaten Natuna Tahun 2022 Nomor 145) sebagaimana telah diubah dengan Peraturan Bupati Nomor 17 Tahun 2023 tentang Perubahan Atas Peraturan Bupati Natuna Nomor 60 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Natuna (Berita Daerah Kabupaten Natuna Tahun 2023 Nomor 257) dicabut dan dinyatakan tidak berlaku.

Pasal 64

Peraturan Bupati ini mulai berlaku pada tanggal ditetapkan.

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

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM

EFENDI, S.Sos
19810426201001101 4

Ditetapkan di Ranai
pada tanggal 31 Januari 2024

BUPATI NATUNA,

ttd

WAN SISWANDI

Diundangkan di Ranai
pada tanggal 31 Januari 2024

SEKRETARIS DAERAH KABUPATEN NATUNA,

ttd

BOY WIJANARKO VARIANTO

BERITA DAERAH KABUPATEN NATUNA TAHUN 2024 NOMOR 327

LAMPIRAN I
PERATURAN BUPATI NATUNA
NOMOR 19 TAHUN 2024
TENTANG PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

STANDAR DAN TEKNIS TATA KELOLA APLIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Pengelolaan aplikasi adalah suatu proses untuk mengelola dan memelihara aplikasi agar dapat berjalan secara optimal dan dapat memenuhi kebutuhan pengguna. Berikut adalah penjelasan lengkap mengenai pengelolaan aplikasi:

A. Pemeliharaan Aplikasi

Pemeliharaan aplikasi merupakan proses untuk menjaga agar aplikasi tetap berfungsi dengan baik, memperbaiki kesalahan atau *bug*, dan meningkatkan kinerja aplikasi. Pemeliharaan aplikasi meliputi pemantauan kinerja aplikasi, pembaruan *software* dan *hardware*, serta perbaikan *bug* atau kesalahan yang terjadi dalam aplikasi. Hal ini sangat penting untuk memastikan bahwa aplikasi berjalan dengan baik dan memenuhi kebutuhan pengguna. Berikut adalah beberapa proses dalam pemeliharaan aplikasi:

1. Identifikasi masalah : Tim Pengelola Aplikasi harus secara rutin memantau dan memeriksa aplikasi untuk mengidentifikasi masalah atau kesalahan. Masalah yang teridentifikasi harus dicatat dan dilaporkan kepada tim pengembang untuk diperbaiki.
2. Pemecahan masalah : setelah masalah diidentifikasi, Tim Pengembang akan memeriksa dan menganalisis masalah tersebut. Setelah masalah diketahui, Tim Pengembang akan mengembangkan solusi yang tepat dan mengimplementasikan perbaikan pada aplikasi.
3. Pembaruan : Aplikasi yang sudah berjalan cukup lama mungkin memerlukan pembaruan untuk meningkatkan kinerja dan stabilitasnya. Pembaruan ini dapat berupa pembaruan *software* atau hardware, dan harus dilakukan secara rutin.
4. Tes dan Evaluasi : setelah perbaikan dan pembaruan dilakukan, Tim Pengembang harus melakukan tes dan Evaluasi untuk memastikan bahwa perbaikan dan pembaruan telah berhasil diterapkan dan tidak menimbulkan masalah baru.
5. Monitoring dan pemeliharaan berkelanjutan setelah aplikasi berjalan dengan baik, penting untuk melakukan pemantauan dan pemeliharaan berkelanjutan untuk mencegah terjadinya masalah di masa depan. Hal ini dapat dilakukan dengan memperbarui aplikasi secara teratur dan memperbaiki masalah yang terjadi.

B. Manajemen Aplikasi

Manajemen aplikasi merupakan proses pengelolaan aplikasi untuk memastikan bahwa aplikasi dapat digunakan secara efektif dan efisien oleh pengguna.

Manajemen aplikasi meliputi pengelolaan dan pemantauan pengguna aplikasi, pengaturan hak akses pengguna, dan Manajemen Basis Data.

Tujuan dari manajemen aplikasi adalah untuk memastikan bahwa aplikasi dapat digunakan secara efektif dan efisien oleh pengguna. Berikut adalah beberapa proses dalam manajemen aplikasi:

1. Identifikasi kebutuhan pengguna, Manajemen aplikasi harus mengidentifikasi kebutuhan pengguna dan memastikan bahwa aplikasi dapat memenuhi kebutuhan tersebut. Ini dapat dilakukan dengan melakukan survei dan analisis Data pengguna.
2. Pengaturan hak akses pengguna dilakukan untuk mengontrol akses pengguna ke dalam aplikasi. Ini dapat dilakukan dengan memberikan izin akses yang tepat berdasarkan peran dan tanggung jawab pengguna.
3. Manajemen Basis Data meliputi pengelolaan dan pemantauan basis Data yang digunakan oleh aplikasi. Hal ini penting untuk memastikan keamanan dan ketersediaan Data.
4. Monitoring dan pemantauan dilakukan untuk memastikan bahwa aplikasi berjalan dengan baik dan memenuhi kebutuhan pengguna. Hal ini meliputi pemantauan kinerja aplikasi, pemantauan akses pengguna, dan pemantauan basis Data.
5. Evaluasi kinerja dilakukan untuk mengevaluasi penggunaan aplikasi dan mengidentifikasi area yang perlu ditingkatkan. Ini dapat dilakukan dengan menganalisis Data pengguna dan mendapatkan umpan balik dari pengguna.
6. Peningkatan aplikasi dilakukan dengan menambahkan fitur baru atau mengoptimalkan kinerja aplikasi. Tujuannya adalah untuk memastikan bahwa aplikasi selalu memenuhi kebutuhan pengguna dan tetap relevan.

Berikut adalah beberapa hal yang harus ditetapkan sebagai sebuah aplikasi yang standar menurut praktek industri terbaik:

1. Keamanan Aplikasi harus memiliki standar keamanan yang tinggi untuk melindungi Data pengguna dan menghindari serangan *cyber*. Ini meliputi penggunaan protokol keamanan, enkripsi Data, dan pengujian keamanan secara teratur.
2. Kinerja Aplikasi harus memiliki kinerja yang baik dan cepat dalam merespons permintaan pengguna. Ini meliputi waktu muat yang cepat, penggunaan memori yang efisien, dan penanganan permintaan yang baik.
3. Kemudahan penggunaan Aplikasi harus mudah digunakan oleh pengguna dengan antarmuka yang intuitif dan sederhana. Hal ini dapat dicapai dengan melakukan pengujian pengguna untuk memastikan aplikasi mudah digunakan dan memenuhi kebutuhan pengguna.
4. Skalabilitas Aplikasi harus dapat di-scaling sesuai dengan jumlah pengguna yang meningkat. Ini meliputi kemampuan aplikasi untuk menangani permintaan pengguna yang banyak dan meningkatkan kapasitas *server* saat diperlukan.

5. Portabilitas Aplikasi harus dapat dijalankan di berbagai platform dan sistem operasi. Hal ini memungkinkan pengguna untuk menggunakan aplikasi pada perangkat apa pun tanpa batasan.
6. Dokumentasi Aplikasi harus memiliki dokumentasi yang lengkap dan jelas, termasuk dokumentasi pengembang, dokumentasi pengguna, dan dokumentasi pemeliharaan. Hal ini akan memudahkan pengembang dan pengguna dalam memahami dan menggunakan aplikasi dengan tepat.
7. Pemeliharaan Aplikasi harus dapat dipelihara dengan mudah oleh tim pengembang. Ini meliputi penggunaan kode yang bersih dan terstruktur, meminimalkan penggunaan teknologi usang, dan menggunakan alat pemeliharaan dan manajemen kode yang baik.

C. Peningkatan Aplikasi

Peningkatan aplikasi dilakukan dengan cara menambahkan fitur baru, mengoptimalkan kinerja aplikasi, serta melakukan integrasi dengan aplikasi lainnya. Hal ini sangat penting untuk memastikan bahwa aplikasi selalu dapat memenuhi kebutuhan dan ekspektasi pengguna.

Berikut adalah beberapa syarat kinerja aplikasi yang harus ditetapkan menurut standar industri terbaik:

1. *Responsiveness* (Responsif) : Aplikasi harus merespons permintaan pengguna dengan cepat dan responsif. Pengguna harus dapat menavigasi antarmuka aplikasi dengan lancar dan tanpa penundaan.
2. *Scalability* (Skalabilitas) : Aplikasi harus memiliki kemampuan untuk di-scaling sesuai dengan kebutuhan, termasuk meningkatkan kapasitas server dan menangani jumlah pengguna yang meningkat.
3. *Resource Utilization* (Pemanfaatan Sumber Daya) : Aplikasi harus mengoptimalkan pemanfaatan sumber daya, seperti memori dan CPU, sehingga dapat berjalan dengan lancar tanpa membebani sistem.
4. *Load Time* (Waktu Muat) : Aplikasi harus memiliki waktu muat yang cepat untuk memastikan pengguna tidak menunggu terlalu lama untuk mengakses Data atau fungsi aplikasi.
5. *Network Performance* (Performa Jaringan) : Aplikasi harus memiliki performa jaringan yang baik, termasuk pengiriman Data yang cepat dan efisien melalui jaringan.
6. *Availability* (Ketersediaan) : Aplikasi harus tersedia untuk diakses oleh pengguna setiap saat dan memiliki mekanisme pemulihan yang cepat jika terjadi gangguan atau downtime.
7. *User Experience* (Pengalaman Pengguna) : Aplikasi harus memberikan pengalaman pengguna yang baik, termasuk antarmuka pengguna yang intuitif dan mudah digunakan, dan waktu respon yang cepat.
8. *Stability* (Stabilitas) : Aplikasi harus stabil dan dapat diandalkan, dengan minimisasi kesalahan sistem atau kerusakan.

D. Keamanan Aplikasi

Keamanan aplikasi meliputi pengaturan akses, enkripsi Data, dan pemantauan aktivitas pengguna. Tujuan dari keamanan aplikasi adalah untuk mencegah terjadinya pelanggaran Data dan menjaga kerahasiaan Data pengguna.

Berikut adalah beberapa syarat keamanan aplikasi yang harus dipenuhi menurut standar industri terbaik:

1. *Authentication* (Otentikasi) : Aplikasi harus menggunakan mekanisme otentikasi yang kuat untuk memverifikasi identitas pengguna sebelum memberikan akses ke aplikasi atau Data.

2. *Authorization* (Otorisasi) : Aplikasi harus menggunakan mekanisme otorisasi yang tepat untuk memastikan pengguna hanya memiliki akses ke Data dan fungsi aplikasi yang diperlukan untuk pekerjaannya.
3. *Encryption* (Enkripsi) : Aplikasi harus menggunakan teknik enkripsi yang kuat untuk melindungi Data dan informasi penting dari serangan hacker. Ini meliputi penggunaan enkripsi Data pada tingkat aplikasi dan database.
4. *Input Validation* (Validasi Input) : Aplikasi harus memvalidasi masukan pengguna secara menyeluruh untuk mencegah serangan injeksi SQL, XSS, dan serangan terkait input lainnya.
5. *Error Handling* (Penanganan Kesalahan) : Aplikasi harus memiliki mekanisme penanganan kesalahan yang kuat untuk mencegah serangan yang disebabkan oleh kesalahan sistem atau pengguna. Hal ini meliputi log dan pemantauan kesalahan, dan mekanisme untuk memperbaiki kesalahan sistem.
6. *Session Management* (Manajemen Sesi) : Aplikasi harus memiliki mekanisme manajemen sesi yang kuat untuk memastikan pengguna hanya memiliki akses pada waktu yang ditentukan, dan sesi pengguna diakhiri saat pengguna keluar dari aplikasi.
7. *Access Control* (Kontrol Akses) : Aplikasi harus memiliki kontrol akses yang kuat untuk memastikan bahwa hanya pengguna yang sah dan diberi otorisasi yang dapat mengakses Data dan fungsi aplikasi.
8. *Secure Configuration* (Konfigurasi Aman) Aplikasi harus dikonfigurasi dengan aman, menggunakan setelan *default* yang aman, dan memastikan bahwa pengguna tidak dapat mengubah konfigurasi yang dapat membahayakan keamanan.

E. Analisis Aplikasi

Analisis aplikasi dilakukan untuk memantau kinerja aplikasi, mengevaluasi penggunaan aplikasi, serta mengidentifikasi area yang perlu ditingkatkan. Hal ini sangat penting untuk memastikan bahwa aplikasi dapat berjalan dengan efektif dan efisien.

Melalui analisis aplikasi, dapat diperoleh informasi yang berguna tentang bagaimana aplikasi digunakan oleh pengguna, bagaimana kinerja aplikasi dalam menghadapi beban pengguna, serta bagaimana interaksi aplikasi dengan sistem dan infrastruktur lainnya. Hal ini dapat membantu pengembang dan pengelola aplikasi dalam mengambil keputusan yang tepat untuk meningkatkan kinerja dan penggunaan aplikasi.

Dalam melakukan analisis aplikasi, dapat digunakan berbagai metode dan teknologi, seperti pengumpulan Data pengguna, *monitoring* kinerja aplikasi, pengujian beban, dan analisis Data. Dengan menggunakan informasi yang diperoleh dari analisis aplikasi, pengembang dan pengelola aplikasi dapat membuat keputusan yang tepat dalam meningkatkan kinerja aplikasi dan memberikan pengalaman pengguna yang lebih baik.

Tujuannya dari analisis aplikasi adalah untuk memantau dan mengevaluasi kinerja aplikasi, serta mengidentifikasi area yang perlu ditingkatkan untuk meningkatkan efektivitas dan efisiensi aplikasi.

Ada beberapa jenis analisis aplikasi yang dapat dilakukan, di antaranya:

1. Analisis Kinerja: Dalam analisis kinerja, memeriksa seberapa baik aplikasi berfungsi. Hal-hal yang diperiksa meliputi waktu respons, waktu muat, dan kinerja keseluruhan aplikasi.

2. Analisis Pengguna: Dalam analisis pengguna, memeriksa bagaimana pengguna berinteraksi dengan aplikasi, serta mengevaluasi kebutuhan dan preferensi pengguna.
3. Analisis Kesalahan: Dalam analisis kesalahan, akan mencari kesalahan dan masalah dalam aplikasi, menemukan dan memperbaiki kesalahan untuk meningkatkan pengalaman pengguna.
4. Analisis Keamanan: Dalam analisis keamanan, memeriksa aplikasi untuk memastikan bahwa tidak ada celah keamanan yang dapat dimanfaatkan oleh orang yang tidak berwenang.

Untuk melakukan analisis aplikasi berdasarkan standar industri, ada beberapa standar yang dapat digunakan sebagai acuan, di antaranya:

1. OWASP Top 10: Standar ini berfokus pada keamanan aplikasi *web* dan menyoroti 10 celah keamanan paling umum dalam aplikasi. OWASP Top 10 mencakup celah seperti Injeksi SQL, *Broken Authentication*, dan *Cross-Site Scripting* (XSS).
2. ISO/IEC 27001: Standar ini membahas tata kelola Keamanan Informasi secara keseluruhan, termasuk untuk aplikasi. ISO/IEC 27001 menetapkan kerangka kerja untuk menerapkan, memonitor, dan memperbaiki tindakan keamanan dalam organisasi.
3. NIST Cybersecurity Framework: Standar ini menyediakan kerangka kerja untuk menerapkan dan memperbaiki program keamanan cyber dalam organisasi, termasuk untuk aplikasi. NIST Cybersecurity Framework mencakup lima area yaitu Identify, Protect, Detect, Respond, dan Recover.
4. PCI DSS: Standar ini menetapkan persyaratan keamanan yang harus dipenuhi oleh aplikasi yang memproses Data kartu kredit. PCI DSS mencakup persyaratan seperti memastikan bahwa Data kartu kredit terenkripsi dan bahwa pengujian keamanan dilakukan secara berkala.
5. HIPAA: Standar ini berfokus pada perlindungan Data medis dan keamanan aplikasi kesehatan. HIPAA menetapkan persyaratan seperti melindungi Data medis dengan enkripsi dan memastikan bahwa akses ke Data medis dibatasi hanya untuk pengguna yang sah.

Dalam melakukan analisis aplikasi berdasarkan standar industri, perlu dilakukan Evaluasi dan pengujian terhadap aplikasi untuk memastikan bahwa aplikasi memenuhi persyaratan dan standar yang ditetapkan. Hal ini dapat dilakukan dengan menggunakan alat pengujian keamanan, melakukan pengujian fungsional, serta melakukan audit terhadap kode aplikasi. Hasil dari analisis ini dapat digunakan untuk memperbaiki kelemahan keamanan aplikasi dan memastikan bahwa aplikasi aman untuk digunakan oleh pengguna.

BUPATI NATUNA,

ttd

WAN SISWANDI

LAMPIRAN II
PERATURAN BUPATI NATUNA
NOMOR 19 TAHUN 2024
TENTANG PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

STANDAR DAN MEKANISME MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
MANAJEMEN RISIKO

A. Pendahuluan

1. Latar Belakang

Berbagai penerapan SPBE telah dihasilkan oleh Instansi Pusat dan Pemerintah Daerah dan telah memberi kontribusi efisiensi dan efektivitas penyelenggaraan pemerintahan. Namun demikian, hasil pengembangan SPBE menunjukkan tingkat maturitas yang relatif rendah dan kesenjangan yang tinggi antara Instansi Pusat dan Pemerintah Daerah. Berdasarkan hasil Evaluasi SPBE tahun 2018 pada 616 Instansi Pusat dan Pemerintah Daerah, indeks SPBE Nasional mencapai nilai 1,98 dengan predikat Cukup dari target indeks SPBE sebesar 2,6 dari 5 (lima) level dengan predikat Baik. Ditinjau dari capaian Instansi Pusat dan Pemerintah Daerah, rata-rata indeks SPBE Instansi Pusat sebesar 2,6 dengan predikat Baik, sementara rata-rata indeks SPBE Pemerintah Daerah sebesar 1,87 dengan predikat Cukup. Ditinjau dari sebaran capaian target, 13,3% Instansi Pusat dan Pemerintah Daerah telah mencapai atau melebihi target indeks SPBE 2,6, sedangkan 86,7% belum mencapai target indeks SPBE 2,6. Hal ini menunjukkan adanya permasalahan dalam pengembangan SPBE secara nasional.

Permasalahan dalam pengembangan SPBE secara nasional disebabkan oleh beberapa faktor diantaranya yaitu sebagai berikut:

a. Permasalahan pertama adalah belum adanya tata kelola SPBE yang terpadu di tingkat Instansi Pusat dan Pemerintah Daerah;
b. Permasalahan kedua adalah belum optimalnya penerapan Layanan SPBE yang terpadu. Sebagaimana diketahui bahwa proses perencanaan, penganggaran, pengadaan, pelaporan keuangan, pemantauan dan Evaluasi, dan akuntabilitas kinerja adalah saling terkait antara satu proses dengan proses lainnya;
c. Permasalahan ketiga adalah terbatasnya jumlah pegawai ASN yang memiliki kompetensi Teknologi Informasi dan Komunikasi untuk mendukung penerapan SPBE.

Peningkatan kapasitas pegawai Aparatur Sipil Negara (ASN) melalui pelatihan di bidang Teknologi Informasi dan Komunikasi (TIK) belum dapat dipenuhi dikarenakan terbatasnya anggaran. Di sisi lain, permintaan Sumber Daya Manusia (SDM) TIK di pasar tenaga kerja termasuk di Instansi Pemerintah tidak diimbangi dengan ketersediaan SDM TIK itu sendiri. Hal ini dapat mengakibatkan terganggunya pengoperasian aplikasi, infrastruktur TIK, dan keamanan untuk memberikan Layanan SPBE yang terbaik.

Perkembangan tren TIK 4.0 merupakan faktor kunci eksternal yang mampu mendorong terwujudnya penerapan SPBE yang terpadu dan peningkatan kualitas Layanan SPBE yang memudahkan pengguna dalam mengakses layanan pemerintah. Beberapa tren TIK 4.0 yang berkembang antara lain:

a. Teknologi *mobile internet* dapat dimanfaatkan untuk kemudahan akses layanan pemerintah melalui gawai personal pengguna yang bebas bergerak tanpa batasan waktu dan lokasi;
b. Teknologi *cloud computing* memberikan efektivitas dan efisiensi yang tinggi untuk melakukan integrasi TIK;
c. Teknologi *internet of things (IoT)* mampu memberikan layanan yang bersifat adaptif dan responsif terhadap kebutuhan kustomisasi layanan yang diinginkan pengguna serta memperluas persediaan kanal-kanal layanan pemerintah;
d. Teknologi *big data analytics* mampu memberikan dukungan pengambilan keputusan dan penyusunan kebijakan bagi pemerintah;
e. Teknologi *artificial intelligence* dapat membantu pemerintah dalam mengurangi beban administrasi seperti penerjemahan dokumen dalam bentuk tulisan/suara serta membantu publik dalam memecahkan permasalahan yang kompleks seperti kesehatan dan keuangan.

Adanya permasalahan penerapan SPBE dan tren revolusi TIK 4.0 melahirkan sejumlah risiko yang dapat berpengaruh terhadap pencapaian tujuan SPBE. Permasalahan penerapan SPBE dapat berkontribusi pada risiko negatif yang dapat menghambat pencapaian tujuan SPBE. Sementara tren revolusi TIK 4.0 dapat berkontribusi pada risiko positif yang dapat meningkatkan peluang keberhasilan pencapaian tujuan SPBE. Oleh karena itu, berbagai risiko yang timbul dalam penerapan SPBE harus dikelola dengan baik oleh Pemerintah Daerah sebagai penyelenggara SPBE. Untuk menjamin keberlangsungan penerapan SPBE, diperlukan Manajemen Risiko SPBE yang diterapkan Pemerintah Daerah untuk mencapai tujuan SPBE sebagaimana diamanatkan dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

2. Maksud dan Tujuan

Pedoman Manajemen Risiko SPBE dimaksudkan untuk memberikan panduan bagi Pemerintah Daerah dalam melaksanakan Manajemen Risiko SPBE di lingkungannya. Sedangkan tujuan dari Manajemen Risiko SPBE adalah:

a. Meningkatkan kemungkinan pencapaian tujuan penerapan SPBE di Pemerintah Daerah;
b. Memberikan dasar yang kuat untuk perencanaan dan pengambilan keputusan melalui penyajian informasi Risiko SPBE yang memadai di Pemerintah Daerah dalam penerapan SPBE;
c. Meningkatkan optimalisasi pemanfaatan sumber daya SPBE di Pemerintah Daerah dalam penerapan SPBE;
d. Meningkatkan kepatuhan kepada peraturan dalam penerapan SPBE; dan
e. Menciptakan budaya sadar Risiko SPBE bagi pegawai ASN di lingkungan Pemerintah Daerah dalam penerapan SPBE.

3. Manfaat

Manfaat dari penerapan Manajemen Risiko SPBE dalam penerapan SPBE adalah:

a. Mewujudkan tata kelola pemerintahan yang efektif, efisien, transparan, dan akuntabel melalui penerapan SPBE di Pemerintah Daerah;
b. Mewujudkan penerapan SPBE yang terpadu di Pemerintah Daerah;
c. Meningkatkan kinerja pemerintahan di Pemerintah Daerah;
d. Meningkatkan reputasi dan kepercayaan pemangku kepentingan kepada Pemerintah Daerah; dan
e. Mewujudkan budaya kerja yang profesional dan berintegritas di Pemerintah Daerah.

4. Ruang Lingkup

Ruang lingkup Pedoman Manajemen Risiko SPBE yang menjadi fokus pembahasan mencakup:

a. Kerangka Kerja Manajemen Risiko SPBE;
b. Proses Manajemen Risiko SPBE;
c. Struktur Manajemen Risiko SPBE; dan
d. Budaya Sadar Risiko SPBE.

5. Pengertian Umum

a. Manajemen Risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE.
b. Risiko SPBE adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan penerapan.
c. SPBE Risiko SPBE Positif adalah peluang terjadinya suatu peristiwa yang akan meningkatkan keberhasilan terhadap pencapaian tujuan penerapan SPBE.
d. Risiko SPBE Negatif adalah peluang terjadinya suatu peristiwa yang akan menurunkan keberhasilan terhadap pencapaian tujuan penerapan SPBE.
e. Kategori Risiko SPBE adalah pengelompokan Risiko SPBE berdasarkan karakteristik penyebab Risiko SPBE yang menggambarkan seluruh jenis Risiko SPBE yang terdapat pada Instansi Pusat dan Pemerintah Daerah.
f. Area Dampak Risiko SPBE adalah pengelompokan area yang terkena dampak dari Risiko SPBE.
g. Kriteria Risiko SPBE adalah parameter atau ukuran secara kuantitatif atau kualitatif yang digunakan untuk menentukan Kriteria Kemungkinan Risiko SPBE dan Kriteria Dampak Risiko SPBE.
h. Kriteria Kemungkinan Risiko SPBE adalah besarnya peluang terjadinya suatu Risiko SPBE dalam periode tertentu.
i. Kriteria Dampak Risiko SPBE adalah besarnya akibat terjadinya suatu Risiko SPBE yang mempengaruhi sasaran SPBE.
j. Besaran Risiko SPBE adalah nilai Risiko SPBE yang dihasilkan dari proses analisis Risiko SPBE.
k. Level Risiko SPBE adalah pengelompokan Besaran Risiko SPBE yang mendeskripsikan tingkat Risiko SPBE.
l. Selera Risiko SPBE adalah penentuan Besaran Risiko SPBE di Instansi Pusat dan Pemerintah Daerah yang dapat diterima atau ditangani.

B. Kerangka Kerja Manajemen Risiko SPBE

Kerangka kerja Manajemen Risiko SPBE mendeskripsikan komponen dasar yang digunakan sebagai landasan penerapan Manajemen Risiko SPBE di Pemerintah Daerah. Tujuan dari kerangka kerja Manajemen Risiko SPBE adalah untuk membantu Pemerintah Kabupaten dalam mengintegrasikan Manajemen Risiko SPBE ke dalam kegiatan pelaksanaan tugas dan fungsinya.

Komponen dasar dari kerangka kerja ini terdiri atas prinsip mengenai peningkatan nilai dan perlindungan, kepemimpinan dan komitmen, serta proses dan tata kelola Manajemen Risiko SPBE sebagaimana terlihat pada Gambar di bawah ini.

Kerangka Kerja Manajemen Risiko SPBE

1. Peningkatan Nilai dan Perlindungan

Prinsip utama dari penerapan Manajemen Risiko SPBE adalah menciptakan peningkatan nilai tambah dan perlindungan bagi Pemerintah Kabupaten dalam penerapan SPBE. Prinsip utama tersebut memiliki karakteristik sebagai berikut:

a. Terintegrasi, yaitu Manajemen Risiko SPBE merupakan serangkaian proses yang terintegrasi dengan proses pelaksanaan tugas dan fungsi Pemerintah Daerah;
b. Terstruktur dan komprehensif, yaitu Manajemen Risiko SPBE dibangun secara terstruktur, sistematis, dan menyeluruh untuk memberikan kontribusi terhadap efisiensi dan konsistensi hasil yang dapat diukur dalam peningkatan kualitas penerapan SPBE;
c. Dapat disesuaikan, yaitu kerangka kerja dan proses Manajemen Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal Pemerintah dalam penerapan SPBE;

d. Inklusif, yaitu Manajemen Risiko SPBE melibatkan semua pemangku kepentingan sesuai dengan pengetahuan, pandangan, dan persepsinya untuk membangun budaya sadar Risiko SPBE di Pemerintah Daerah;
e. Dinamis, yaitu Manajemen Risiko SPBE dapat dipergunakan untuk mengantisipasi dan merespon perubahan konteks Pemerintah Daerah dengan tepat dan sesuai waktu;
f. Informasi tersedia dan terbaik, yaitu informasi yang digunakan sebagai masukan dalam proses Manajemen Risiko SPBE didasarkan pada Data historis, pengalaman, observasi, perkiraan, penilaian ahli, dan Data dukung lain yang tersedia di Pemerintah Daerah;
g. Faktor manusia dan budaya, yaitu keberhasilan penerapan Manajemen Risiko SPBE Pemerintah Daerah dipengaruhi oleh kapasitas, persepsi, kesungguhan, dan budaya kerja dari pegawai ASN yang terlibat dalam penerapan SPBE; dan
h. Perbaikan berkelanjutan, yaitu Manajemen Risiko SPBE senantiasa dikembangkan melalui strategi perbaikan manajemen secara berkelanjutan dan peningkatan kematangan penerapan Manajemen Risiko SPBE.

2. Kepemimpinan dan Komitmen

Pimpinan Pemerintah Daerah hendaknya menunjukkan kepemimpinan dan komitmen dalam penerapan kerangka kerja Manajemen Risiko SPBE melalui proses:

a. Integrasi

Kerangka kerja Manajemen Risiko SPBE hendaknya diintegrasikan dengan proses pelaksanaan tugas dan fungsi Pemerintah Daerah. Integrasi dapat dilakukan dengan memahami struktur dan konteks organisasi yang didasarkan pada tujuan, sasaran, dan kompleksitas organisasi.

Berdasarkan struktur dan konteks organisasi tersebut, tata kelola Manajemen Risiko SPBE perlu dibangun dengan menyusun struktur Manajemen Risiko SPBE beserta tugas-tugasnya untuk menjalankan, mengendalikan, dan melakukan pengawasan terhadap penerapan proses Manajemen Risiko SPBE dalam rangka mencapai sasaran dan target kinerja organisasi dalam penerapan SPBE.

b. Desain

Perancangan kerangka kerja Manajemen Risiko SPBE dilakukan dengan cara:

1) Memahami struktur dan konteks organisasi termasuk tujuan, sasaran, dan kompleksitas organisasi;
2) Mengekspresikan komitmen pimpinan terhadap penerapan kerangka kerja Manajemen Risiko SPBE dalam bentuk kebijakan, pernyataan, atau bentuk dukungan lainnya;
3) Menetapkan kewenangan, tanggung jawab, dan akuntabilitas dari setiap peran di dalam kerangka kerja Manajemen Risiko SPBE;
4) Menyediakan sumber daya yang diperlukan seperti SDM dan kompetensi, anggaran, proses dan prosedur, informasi dan pengetahuan, dan pelatihan; dan

5) Membangun komunikasi dan konsultasi untuk efektivitas implementasi kerangka kerja Manajemen Risiko SPBE.

c. Implementasi
Kerangka kerja Manajemen Risiko SPBE diterapkan dengan melibatkan semua pemangku kepentingan Pemerintah Daerah melalui penyusunan rencana, penyediaan sumber daya, pembuatan keputusan, dan pelaksanaan Manajemen Risiko SPBE.

d. Pemantauan dan Evaluasi
Untuk mengukur efektivitas implementasi kerangka kerja Manajemen Risiko SPBE, pimpinan Pemerintah Daerah perlu melakukan pemantauan dan Evaluasi secara berkala untuk pengukuran kinerja dan kesesuaian kerangka kerja Manajemen Risiko SPBE terhadap tujuan dan sasaran SPBE.

e. Perbaikan
Hasil pemantauan dan Evaluasi kerangka kerja Manajemen Risiko SPBE digunakan untuk melakukan perubahan dan perbaikan kerangka kerja Manajemen Risiko SPBE secara berkelanjutan sehingga kesesuaian, kecukupan, dan efektivitas dari kerangka kerja tersebut dapat ditingkatkan.

3. Proses dan Tata Kelola Manajemen Risiko SPBE

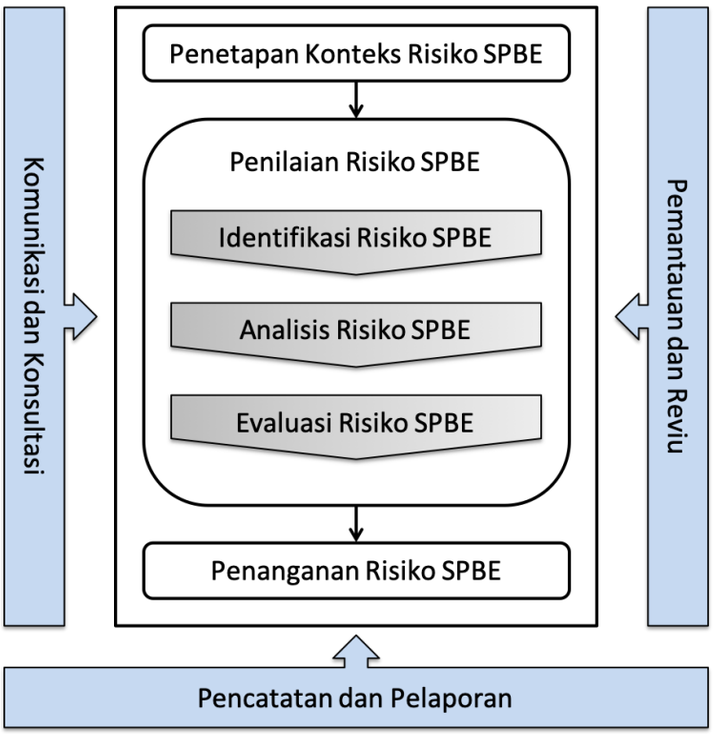
Proses Manajemen Risiko SPBE merupakan rangkaian proses yang sistematis dan menjadi bagian dari proses pelaksanaan tugas dan fungsi Pemerintah Daerah untuk pengambilan keputusan di tingkat strategis, operasional, dan pelaksanaan proyek. Proses Manajemen Risiko SPBE yang dilaksanakan oleh Pemerintah Daerah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

a. komunikasi dan konsultasi;
b. penetapan konteks Risiko SPBE;
c. penilaian Risiko SPBE, yang terdiri atas identifikasi Risiko SPBE, analisis Risiko SPBE, dan Evaluasi Risiko SPBE;
d. penanganan Risiko SPBE;
e. pemantauan dan reviu;
f. pencatatan dan pelaporan.

Sedangkan, tata kelola Manajemen Risiko SPBE merupakan mekanisme untuk mengatur kewenangan dan memastikan akuntabilitas pelaksanaan Manajemen Risiko SPBE 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 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 Pemerintah Daerah Kabupaten melalui perencanaan, pelaksanaan, dan pemantauan dan Evaluasi kegiatan budaya sadar Risiko SPBE.

C. Proses Manajemen Risiko SPBE

Proses Manajemen Risiko SPBE merupakan penerapan secara sistematis dari kebijakan, prosedur, dan praktik terhadap aktivitas komunikasi dan konsultasi, penetapan konteks, penilaian risiko (identifikasi risiko, analisis risiko, Evaluasi risiko), penanganan risiko, pemantauan dan reviu, serta pencatatan dan pelaporan. Proses Manajemen Risiko SPBE seperti gambar di bawah ini.



1. 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:

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

2. 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:

a. 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. Informasi umum dituangkan ke dalam Formulir 2.1 seperti terlihat pada Tabel 1 di bawah ini.

Tabel 1
Contoh Pengisian Formulir 2.1 Informasi Umum

Informasi Umum	
Nama UPR SPBE	Dinas Komunikasi dan Informatika
Tugas UPR SPBE	Membantu bupati dalam melaksanakan urusan pemerintahan yang menjadi kewenangan daerah dan tugas pembantuan di bidang Komunikasi dan Informatika.
Fungsi UPR SPBE	Menetapkan kebijakan teknis tentang penyelenggaraan pelayanan komunikasi, informatika.
Periode Waktu	1 Januari - 31 Desember 2024

b. Identifikasi Sasaran SPBE

Identifikasi sasaran SPBE bertujuan untuk menentukan sasaran SPBE beserta indikator dan targetnya yang mendukung sasaran unit kerja sebagai UPR SPBE. Informasi yang dicantumkan meliputi:

1) Sasaran UPR SPBE, diisi dengan sasaran unit kerja sebagai UPR SPBE yang tertuang dalam dokumen rencana strategis, rencana kerja, penetapan kinerja, atau dokumen perencanaan lainnya;
2) Sasaran SPBE, diisi dengan sasaran SPBE yang mendukung sasaran UPR SPBE;
3) Indikator Kinerja SPBE, diisi dengan indikator kinerja SPBE yang mendeskripsikan pencapaian sasaran SPBE; dan
4) Target Kinerja SPBE, diisi dengan target kinerja SPBE yang mendeskripsikan ukuran indikator kinerja untuk pencapaian sasaran SPBE.

Informasi sasaran SPBE dituangkan ke dalam Formulir 2.2 seperti terlihat pada Tabel 2 di bawah ini.

Tabel 2
Contoh Pengisian Formulir 2.2 Sasaran SPBE

No	Sasaran UPR SPBE	Sasaran SPBE	Indikator Kinerja SPBE	Target Kinerja SPBE
1	Terwujudnya tata kelola pemerintahan yang berbasis elektronik	Meningkatnya Kualitas penyelenggaraan SPBE	Indeks SPBE Pemerintah Kabupaten Natuna	4,5

c. 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. Penentuan struktur pelaksana Manajemen Risiko SPBE meliputi:

1) Unit Pemilik Risiko SPBE;
2) Pemilik Risiko SPBE;
3) Koordinator Risiko SPBE; dan
4) Pengelola Risiko SPBE.

Informasi struktur pelaksana Manajemen Risiko SPBE dituangkan ke dalam Formulir 2.3 seperti terlihat pada Tabel 3 di bawah ini.

Tabel 3
Contoh Pengisian Formulir 2.3 Struktur Pelaksana Manajemen Risiko SPBE

Struktur Pelaksana Manajemen Risiko SPBE	
Pemilik Risiko SPBE	
Koordinator Risiko SPBE	
Pengelola Risiko SPBE	

d. 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. Daftar pemangku kepentingan dituangkan ke dalam Formulir 2.4 seperti terlihat pada Tabel 4 di bawah ini.

Tabel 4
Contoh Pengisian Formulir 2.4 Daftar Pemangku Kepentingan

No	Nama Unit/Instansi	Hubungan
1	Perguruan Tinggi (Tel-U)	Pelaksana Evaluasi SPBE sebagai evaluator eksternal
2	Badan Siber dan Sandi Negara	Penyedia layanan repositori Data Evaluasi SPBE
3	Kemenpan RB	Yang menetapkan Pedoman Manajemen Risiko SPBE
4	Pemerintah Daerah	Pelaksana SPBE

e. 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. Daftar peraturan dituangkan ke dalam Formulir 2.5 seperti terlihat pada Tabel 5 di bawah ini.

Tabel 5
Contoh Pengisian Formulir 2.5 Daftar Peraturan Perundang-Undangan

No	Nama Peraturan	Amanat
1.	Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik	Pasal 70 (1) Pemantauan dan Evaluasi SPBE bertujuan untuk mengukur kemajuan dan meningkatkan kualitas SPBE di Instansi Pusat dan Pemerintah Daerah. (2) Tim Koordinasi SPBE Nasional melakukan pemantauan dan Evaluasi terhadap SPBE secara nasional dan berkala. (3) Koordinator SPBE Instansi Pusat dan Pemerintah Daerah melakukan pemantauan dan Evaluasi terhadap SPBE pada Instansi Pusat dan Pemerintah Daerah secara berkala. (4) Pelaksanaan pemantauan dan Evaluasi SPBE sebagaimana dimaksud pada ayat (3) dikoordinasikan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.
2.	Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2018 tentang Pedoman Evaluasi SPBE	Pasal 6 Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi melakukan: a. pembinaan, koordinasi, pemantauan, dan/atau supervisi terhadap Evaluasi mandiri Sistem Pemerintahan Berbasis Elektronik; dan b. penyusunan profil nasional pelaksanaan Sistem Pemerintahan Berbasis Elektronik berdasarkan hasil evaluasi eksternal.
3.	Permen PANRB Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi SPBE	Pasal 2 (1) Peraturan Menteri ini dimaksudkan untuk memberikan panduan bagi Instansi Pusat dan Pemerintah Daerah dalam: a. memahami tujuan pemantauan dan Evaluasi serta penetapan ruang lingkup penilaian penerapan SPBE; b. memahami metode penilaian Pemantauan dan Evaluasi SPBE;

		c. memahami langkah-langkah kerja yang harus dilakukan dalam proses Pemantauan dan Evaluasi SPBE; dan d. menjamin kualitas pelaksanaan Pemantauan dan Evaluasi SPBE pada Instansi Pusat dan Pemerintah Daerah. (2) Pemantauan dan Evaluasi SPBE bertujuan untuk: a. mengukur capaian kemajuan penerapan SPBE pada Instansi Pusat dan Pemerintah Daerah; b. meningkatkan kualitas penerapan SPBE pada Instansi Pusat dan Pemerintah Daerah; dan c. meningkatkan kualitas pelayanan publik pada Instansi Pusat dan Pemerintah Daerah.

f. 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:

1) Rencana Induk SPBE Nasional dan Pemerintah Daerah, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan perencanaan pembangunan SPBE Nasional dan Kabupaten;
2) 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;
3) Peta Rencana SPBE, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan Peta Rencana SPBE;
4) Proses Bisnis, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan penerapan Proses Bisnis SPBE;
5) Rencana dan Anggaran, merupakan Risiko SPBE yang berkaitan dengan proses perencanaan dan penganggaran SPBE;
6) Inovasi, merupakan Risiko SPBE yang berkaitan dengan ide baru atau pemikiran kreatif yang memberikan nilai manfaat dalam penerapan SPBE;
7) 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;
8) Pengadaan Barang dan Jasa, merupakan Risiko SPBE yang berkaitan dengan proses pengadaan dan penyediaan barang dan jasa;
9) Proyek Pembangunan/Pengembangan Sistem, merupakan Risiko SPBE yang berkaitan dengan proyek pembangunan ataupun pengembangan sistem pada penerapan SPBE;

10) Data dan Informasi, merupakan Risiko SPBE yang berkaitan dengan semua Data dan informasi yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah Kabupaten Natuna;
11) 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;
12) Aplikasi SPBE, merupakan Risiko SPBE yang berkaitan dengan program komputer yang diterapkan untuk melakukan tugas atau fungsi Layanan SPBE;
13) Keamanan SPBE, merupakan Risiko SPBE yang berkaitan dengan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya yang mendukung SPBE;
14) Layanan SPBE, merupakan Risiko SPBE yang berkaitan dengan pemberian Layanan SPBE kepada Pengguna SPBE;
15) Sumber Daya Manusia SPBE, merupakan Risiko SPBE yang berkaitan dengan SDM yang bekerja sebagai penggerak penerapan SPBE di Pemerintah Daerah Kabupaten Natuna; dan
16) Bencana Alam, merupakan Risiko SPBE yang berkaitan dengan peristiwa yang disebabkan oleh alam.

Kategori Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal di Pemerintah Daerah. Kategori Risiko SPBE dituangkan ke dalam Formulir 2.6 seperti terlihat pada Tabel 6 di bawah ini.

Tabel 6
Formulir 2.6 Kategori Risiko SPBE

No	Kategori Risiko SPBE
1	Rencana Induk SPBE Nasional dan Pemerintah Daerah
2	Arsitektur SPBE
3	Peta Rencana SPBE
4	Proses Bisnis
5	Rencana dan Anggaran
6	Inovasi
7	Kepatuhan terhadap Peraturan
8	Pengadaan Barang dan Jasa
9	Proyek Pembangunan/Pengembangan Sistem
10	Data dan Informasi
11	Infrastruktur SPBE
12	Aplikasi SPBE
13	Keamanan SPBE
14	Layanan SPBE

No	Kategori Risiko SPBE
15	SDM SPBE
16	Bencana Alam

g. 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:

1) Finansial, dampak Risiko SPBE berupa aspek yang berkaitan dengan keuangan;
2) Reputasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan tingkat kepercayaan pemangku kepentingan;
3) Kinerja, dampak Risiko SPBE berupa aspek yang berkaitan dengan pencapaian sasaran SPBE;
4) Layanan Organisasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan pemenuhan kebutuhan atau jasa kepada pemangku kepentingan;
5) Operasional dan Aset TIK, dampak Risiko SPBE berupa aspek yang berkaitan dengan kegiatan operasional TIK dan pengelolaan aset TIK;
6) Hukum dan Regulasi, dampak Risiko SPBE berupa aspek yang berkaitan dengan Peraturan Perundang-undangan dan kebijakan; dan
7) Sumber Daya Manusia, dampak Risiko SPBE berupa aspek yang berkaitan dengan fisik dan mental pegawai.

Area Dampak Risiko SPBE terdiri atas area dampak positif dan/atau negatif. Area Dampak Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal di masing-masing Instansi Pusat dan Pemerintah Daerah. Area Dampak Risiko SPBE dituangkan ke dalam Formulir 2.7 seperti terlihat pada Tabel 7 di bawah ini.

Tabel 7
Formulir 2.7 Area Dampak Risiko SPBE

No	Area Dampak Risiko SPBE
1	Finansial
2	Reputasi
3	Kinerja
4	Layanan Organisasi
5	Operasional dan Aset TIK
6	Hukum dan Regulasi
7	Sumber Daya Manusia

h. 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:

1) 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:

a) Hampir Tidak Terjadi;
b) Jarang Terjadi;
c) Kadang-Kadang Terjadi;
d) Sering Terjadi;
e) Hampir Pasti Terjadi.

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

Selanjutnya, kriteria kemungkinan dituliskan pada setiap level kemungkinan yang dituangkan ke dalam Formulir 2.8.A seperti terlihat pada Tabel 8 di bawah ini.

Tabel 8
Contoh Pengisian Formulir 2.8.A Kriteria Kemungkinan Risiko 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

2) 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:

a) Tidak Signifikan;

b) Kurang Signifikan;
c) Cukup Signifikan;
d) Signifikan;
e) Sangat Signifikan.

Kriteria Dampak Risiko SPBE dijabarkan untuk setiap Area Dampak Risiko SPBE Positif dan Area Dampak Risiko SPBE Negatif terhadap setiap level dampak ke dalam Formulir 2.8.B seperti terlihat pada Tabel 9 di bawah ini.

Tabel 9
Contoh Pengisian Formulir 2.8.B Kriteria Dampak Risiko 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%

i. 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. Besaran Risiko SPBE kemudian dimasukkan ke dalam Formulir 2.9.A seperti terlihat pada Tabel 10 di bawah ini.

Tabel 10
Contoh Pengisian Formulir 2.9.A Matriks Analisis Risiko SPBE

Matriks Analisis Risiko 5 x 5			Level Dampak				
			1	2	3	4	5
			Tidak Signikan	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 Pemerintah Daerah. Untuk 5 Level Risiko SPBE, dapat diuraikan sebagai berikut:

1) Sangat Rendah, direpresentasikan dengan warna biru;
2) Rendah, direpresentasikan dengan warna hijau;
3) Sedang, direpresentasikan dengan warna kuning;
4) Tinggi, direpresentasikan dengan warna jingga;
5) Sangat Tinggi, direpresentasikan dengan warna merah.

Nilai rentang Besaran Risiko dituangkan ke dalam Formulir 2.9.B seperti terlihat pada Tabel 11 di bawah ini.

Tabel 11
Contoh Pengisian Formulir 2.9.B Level 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

j. 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. Besaran Risiko yang ditangani pada setiap Kategori Risiko SPBE dituangkan ke dalam Formulir 2.10 seperti terlihat pada Tabel 12 di bawah ini.

Tabel 12
Contoh Pengisian Formulir 2.10 Selera Risiko SPBE

No	Kategori Risiko SPBE	Besaran Risiko Minimum yang Ditangani	
		Risiko SPBE Positif	Risiko SPBE Negatif
1	Rencana dan Anggaran	16	6
2	Pengadaan Barang dan Jasa	18	11
3	SDM SPBE	20	14

3. 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:

a. Identifikasi Risiko SPBE

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

1) 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.

2) 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.

3) 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.

4) 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.

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

6) 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.

Proses Identifikasi Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Identifikasi Risiko SPBE seperti terlihat pada Tabel 13.

Tabel 13
Contoh Pengisian Formulir 3.0
Penilaian Risiko SPBE Bagian Identifikasi Risiko SPBE

Identifikasi Risiko SPBE					
Jenis Risiko SPBE	Kejadian	Penyebab	Kategori	Dampak	Area Dampak
Positif	Respon dari K/L/D Sangat Antusias	Adanya mandat dari Peraturan Presiden No 95 Tahun 2018	Kepatuhan terhadap Peraturan	Peningkatan Kualitas Layanan SPBE	Kinerja
Negatif	Terdapat K/L/D yang tidak di Evaluasi	Kurangnya jumlah evaluator eksternal	SDM SPBE	Penurunan Kinerja	Kinerja

b. 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:

1) Sistem Pengendalian
   a) Sistem pengendalian internal mencakup perangkat manajemen yang dapat menurunkan/meningkatkan level Risiko SPBE dalam rangka pencapaian sasaran SPBE.
   b) Sistem pengendalian internal dapat berupa *Standard Operating Procedure* (SOP), pengawasan melekat, reviu berjenjang, regulasi, dan pemantauan rutin yang dilaksanakan terkait Risiko SPBE tersebut.
2) 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.
3) 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.
4) 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 sebagaimana telah dijelaskan pada bagian huruf B angka 9.

Proses Analisis Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Analisis Risiko SPBE seperti terlihat pada Tabel 14 di bawah ini.

Tabel 14
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian Analisis Risiko SPBE

Analisis Risiko SPBE						
Sistem Pengendalian	Kemungkinan		Dampak		Besaran Risiko SPBE	Level Risiko SPBE
	Level	Penjelasan	Level	Penjelasan		
Konfirmasi keikutsertaan dalam Evaluasi SPBE	Hampir Pasti Terjadi	Keikutsertaan lebih dari 80%	Sangat Signifikan	Peningkatatan kinerja Hingga 80%	25	Sangat Tinggi
Analisis beban kerja evaluator Eksternal	Kadang-Kadang Terjadi	Terjadi sekitar 15% Dalam satu periode	Cukup Signifikan	Penurunan Kinerja Hingga 50%	14	Sedang

c. 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*. Proses Evaluasi Risiko SPBE dituangkan ke dalam Formulir 3.0 pada bagian Penilaian Risiko SPBE seperti terlihat pada Tabel 15 di bawah ini.

Tabel 15
Contoh Pengisian Formulir 3.0 Penilaian Risiko SPBE Bagian Evaluasi Risiko SPBE

Evaluasi Risiko SPBE	
Keputusan Penanganan Risiko SPBE (Ya/Tidak)	Prioritas Penanganan Risiko SPBE
Ya	1
Ya	2

4. 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:

a. 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.

b. 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:
   1) 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:
      a) Opsi Penanganan Risiko Positif
         - 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.
         - Eksploitasi Risiko
           Eksploitasi risiko dipilih jika Risiko SPBE dapat dipastikan terjadi. Opsi ini dilakukan dengan cara memanfaatkan Risiko SPBE tersebut semaksimal mungkin.
         - Peningkatan Risiko
           Peningkatan risiko dilakukan dengan cara meningkatkan level kemungkinan dan/atau level dampak dari Risiko SPBE.
         - 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.
         - 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.

      b) Opsi Penanganan Risiko Negatif
         - 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.

- Mitigasi Risiko
  Mitigasi risiko dilakukan dengan cara mengurangi level kemungkinan dan/atau level dampak dari Risiko SPBE.
- 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.
- Penghindaran Risiko
  Penghindaran risiko dilakukan dengan mengubah perencanaan, penganggaran, program, dan kegiatan, atau aspek lainnya untuk mencapai sasaran SPBE.
- 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.

2) Rencana Aksi Penanganan Risiko
   Rencana aksi penanganan risiko merupakan rancangan kegiatan tindak lanjut untuk menangani Risiko SPBE.
3) Keluaran
   Keluaran merupakan hasil dari rencana aksi penanganan Risiko SPBE.
4) Jadwal Implementasi
   Jadwal implementasi merupakan jadwal pelaksanaan dari setiap rencana aksi penanganan Risiko SPBE.
5) Penanggung Jawab
   Penanggung jawab berisikan nama unit yang bertanggung jawab dan unit pendukung dari setiap rencana aksi penanganan Risiko SPBE.

Tabel 16
Contoh Pengisian Formulir 4.0 Rencana Penanganan Risiko SPBE
Bagian Rencana Penanganan

Rencana Penanganan				
Opsi Penanganan Risiko SPBE	Rencana Aksi Penanganan Risiko SPBE	Keluaran	Jadwal Implementasi	Penanggung Jawab
Eksploitasi Risiko	- Pembinaan dan pengawasan lebih ditingkatkan; - Perbaikan dan penerapan SOP yang tegas; - Memasang sumber listrik Yang tertutup;	Kemungkinan Terjadinya risiko akan dapat diminimalisir	Triwulan I dan II	Bidang Informatika

	- Akses kunci masuk area lebih diperketat/ pemasangan kunci secara - digital; - Menambah kapasitas - Membuat peraturan tata tertib dengan sangsi yang tegas			
Mitigasi Risiko	Pengadaan Barang/jasa yaitu Pengadaan *Sever* serta sarana dan Prasarana Lainnya	*Server* sesuai kebutuhan	Triwulan II	Bidang Informatika

c. 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*.

5. Pemantauan dan Reviu

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

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 Pemerintah Daerah.

6. 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:

a. Pencatatan dan Pelaporan Periodik

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

b. Pencatatan dan Pelaporan Insidental

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

7. Dokumen Manajemen Risiko SPBE

a. Pakta Integritas Manajemen Risiko SPBE

Pakta Integritas Manajemen Risiko SPBE merupakan dokumen pernyataan atau janji untuk berkomitmen menjalankan Manajemen Risiko SPBE di Instansi Pusat dan Pemerintah Daerah. Dokumen Pakta Integritas dapat dilihat pada Formulir 1.0 Pakta Integritas.

b. 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:

1) 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.
2) 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.
3) 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.

c. 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:

1) 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.
2) 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.
3) 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.
4) 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.Format laporan pemantauan triwulan dan tahunan dapat dilihat pada formulir 5.0 di bawah ini.

Formulir 5.0
Contoh Pengisian Formulir 5.0 Laporan Pemantauan Risiko SPBE Triwulan I

Laporan Pemantauan Risiko SPBE Triwulan I			
	Nama Unit	:	Dinas Komunikasi dan Informatika
	Sasaran	:	Meningkatnya penyelenggaraan pemerintahan berbasis elektronik
	Risiko	:	Terdapat beberapa kelengkapan *data center* yang kapasitasnya harus lebih memadai seperti *server* yang kapsitasnya masih kurang dibandingkan dengan kemungkinan besar bertambahnya pengguna

Laporan Pemantauan Risiko SPBE Triwulan I

Nama Unit	:	Dinas Komunikasi dan Informatika
Sasaran	:	Meningkatnya penyelenggaraan pemerintahan berbasis elektronik
Risiko	:	Terdapat beberapa kelengkapan *data center* yang kapasitasnya harus lebih memadai seperti *server* yang kapsitasnya masih kurang dibandingkan dengan kemungkinan besar bertambahnya pengguna

Besaran/Level Risiko SPBE Saat ini dan Proyeksi Risiko SPBE
Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "tinggi" dengan Besaran Risiko SPBE sebesar 19% dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 20% - 50% dalam satu periode (Sering terjadi) dan berdampak pada penurunan kinerja hingga 80% (Signifikan). Risiko SPBE tersebut pada triwulan I telah berada pada Level Risiko SPBE"tinggi" dengan Besaran Risiko SPBE sebesar 19% dimana kemungkinan terjadinya Risiko SPBE tersebut sekitar 50% dalam satu periode (Sering Terjadi) dan berdampak pada penurunan kinerja hingga 60% (Signifikan). Risiko SPBE tersebut kedepannya sangat diperlukan penanganan, karena berada di atas Selera Risiko SPBE.Penanganan

Penanganan yang telah dilakukan
Pengadaan Barang/Jasa yaitu pengadaan *server*

Rencana Penanganan	Penanggung jawab	Waktu Pelaksanaan
Melakukan pengawasan dan pengendalian serta rencana penganggaran	Bidang Informatika	Triwulan II

Contoh Pengisian Formulir 5.0 Laporan Pemantauan Risiko SPBE Tahunan

Laporan Pemantauan Risiko SPBE Tahunan

Nama Unit	:	Dinas Komunikasi dan Informatika
Sasaran	:	Meningkatnya penyelenggaraan pemerintahan berbasis elektronik
Risiko	:	Terdapat beberapa kelengkapan *data center* yang kapasitasnya harus lebih memadai seperti *server* yang kapasitasnya masih kurang dibandingkan dengan kemungkinan besar bertambahnya pengguna

Besaran/Level Risiko SPBE Saat ini
Risiko SPBE pada awal tahun berada pada Level Risiko SPBE "tinggi" dengan Besaran Risiko SPBE sebesar 19% Risiko SPBE tersebut pada triwulan I, II, III dan IV telah berada pada Level Risiko SPBE “Rendah” dengan Besaran Risiko sebesar 10%.

Penanganan yang telah dilakukan
1. Pengadaan Barang/Jasa yaitu pengadaan *server* 2. Pengawasan dan Pengendalian serta Evaluasi

Rekomendasi	Untuk mengantisipasi terjadinya Risiko SPBE yang serupa, perlu dipastikan bahwa kapasitas *server* yang memadai sangat diperlukan untuk menunjang *data center* serta perlu adanya audit infrastruktur secara berkala

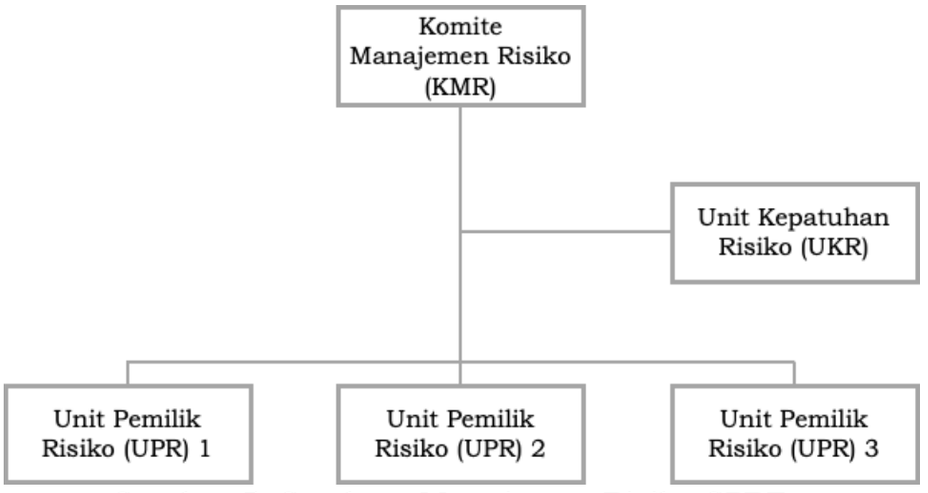
D. Struktur Manajemen dan Budaya Sadar Risiko SPBE

Manajemen Risiko SPBE merupakan tanggung jawab bersama pada semua tingkatan di lingkungan Instansi Pusat dan Pemerintah Daerah. Agar proses dan pengukuran dalam Manajemen Risiko SPBE dapat dilaksanakan dengan baik, maka diperlukan tata kelola Manajemen Risiko SPBE yang mengatur tugas dan tanggung jawab dari struktur Manajemen Risiko SPBE, dan budaya sadar Risiko SPBE yang dapat menggerakkan pegawai ASN menerapkan Manajemen Risiko SPBE.

1. Struktur Manajemen Risiko SPBE

Struktur Manajemen Risiko SPBE terdiri atas:

a. Komite Manajemen Risiko (KMR) SPBE yang memiliki fungsi penetapan kebijakan strategis terkait Manajemen Risiko SPBE.
b. Unit Pemilik Risiko (UPR) SPBE yang memiliki fungsi pelaksanaan Manajemen Risiko SPBE.
c. Unit Kepatuhan Risiko (UKR) SPBE yang memiliki fungsi pengawasan terhadap pelaksanaan Manajemen Risiko SPBE. Gambar 5 mengilustrasikan struktur Manajemen Risiko SPBE seperti di bawah ini.



Gambar 5. Struktur Manajemen Risiko SPBE

Struktur Manajemen Risiko SPBE merupakan struktur *ex-officio* yang menjalankan tugas tambahan terkait Manajemen Risiko SPBE. Apabila Pemerintah Daerah telah memiliki kebijakan Manajemen Risiko bagi organisasi, struktur Manajemen Risiko SPBE hendaknya mengadopsi struktur manajemen risiko yang telah ada tersebut untuk keterpaduan pelaksanaan Manajemen Risiko secara menyeluruh.

Di dalam penerapan Manajemen Risiko SPBE, struktur Manajemen Risiko SPBE di Pemerintah Daerah dapat memiliki struktur yang berbeda satu sama lain. Perbedaan struktur Manajemen Risiko SPBE dapat dipengaruhi oleh ukuran organisasi, kompleksitas tugas, dan/atau tingkat risiko di Pemerintah Daerah. Pemerintah Daerah yang memiliki ukuran organisasi yang besar, kompleksitas tugas yang tinggi, dan/atau tingkat risiko yang tinggi memerlukan pengendalian Risiko SPBE yang lebih ketat melalui struktur Manajemen Risiko SPBE yang lebih berjenjang.

a. Komite Manajemen Risiko (KMR) SPBE

Komite Manajemen Risiko SPBE yang disingkat KMR SPBE dibentuk dan ditetapkan oleh masing-masing pimpinan kepala daerah, dan memiliki anggota yang terdiri atas pejabat Pemerintah Daerah yang memiliki kewenangan pengambilan keputusan dan penetapan kebijakan strategis terkait Manajemen Risiko SPBE. KMR SPBE memiliki tugas menyelenggarakan perumusan dan penetapan kebijakan, pengendalian, pemantauan, dan Evaluasi penerapan kebijakan Manajemen Risiko SPBE. Dalam melaksanakan tugasnya, KMR SPBE menyelenggarakan fungsi sebagai berikut:

1) penyusunan dan penetapan kebijakan Manajemen Risiko SPBE;
2) penyusunan dan penetapan kerangka kerja dan pedoman pelaksanaan Manajemen Risiko SPBE;
3) penyusunan dan penetapan pakta integritas Manajemen Risiko SPBE;
4) penyusunan dan penetapan konteks Risiko SPBE;
5) pengendalian proses Risiko SPBE melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan Evaluasi terhadap penerapan Manajemen Risiko SPBE; dan pelaksanaan komitmen pimpinan dan penerapan budaya sadar Risiko SPBE.

b. Unit Pemilik Risiko (UPR) SPBE

Unit Pemilik Risiko SPBE yang disingkat UPR SPBE merupakan unit kerja di Pemerintah Daerah Kabupaten yang bertanggung jawab langsung kepada pimpinan Instansi Pusat dan Bupati. UPR SPBE memiliki tugas melaksanakan penerapan Manajemen Risiko SPBE pada unit kerja tertinggi sampai terendah. UPR SPBE terdiri atas unsur :

1) Pemilik Risiko SPBE merupakan pejabat yang bertanggung jawab atas pelaksanaan penerapan Manajemen Risiko SPBE di unit organisasi tersebut;
2) Koordinator Risiko SPBE merupakan pejabat/pegawai yang ditunjuk oleh Pemilik Risiko SPBE untuk bertanggung jawab atas pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan baik internal maupun eksternal UPR SPBE; dan;
3) Pengelola Risiko SPBE merupakan pejabat/pegawai yang ditunjuk oleh Pemilik Risiko SPBE untuk bertanggung jawab atas pelaksanaan operasional Manajemen Risiko SPBE pada unit-unit kerja yang berada di bawah UPR SPBE.

Dalam melaksanakan tugasnya, UPR SPBE menjalankan fungsi sebagai berikut:

1) penyusunan dan penetapan penilaian Risiko SPBE dan rencana pelaksanaan Manajemen Risiko SPBE termasuk rencana kontinjensi penanganan Risiko SPBE;
2) pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan;

3) pelaksanaan operasional Manajemen Risiko SPBE yang efektif melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan Evaluasi; dan
4) pelaksanaan pembinaan budaya sadar Risiko SPBE melalui sosialisasi, bimbingan, pelatihan, dan supervisi penerapan Manajemen Risiko SPBE.

c. Unit Kepatuhan Risiko (UKR) SPBE

Unit Kepatuhan Risiko SPBE yang disingkat UKR SPBE merupakan unit organisasi di Pemerintah Daerah yang melaksanakan fungsi pengawasan intern di Pemerintah Daerah (Aparat Pengawasan Intern Pemerintah-APIP). UKR SPBE memiliki tugas melaksanakan pengawasan terhadap penerapan kebijakan Manajemen Risiko SPBE di semua UPR SPBE. Dalam melaksanakan tugasnya, UKR SPBE menjalankan fungsi sebagai berikut:

1) penyusunan kebijakan pengawasan terhadap penerapan Manajemen Risiko SPBE;
2) pelaksanaan pengawasan intern terhadap penerapan Manajemen Risiko SPBE di semua UPR SPBE melalui audit, reviu, pemantauan, Evaluasi, dan kegiatan pengawasan lainnya;
3) pelaksanaan konsultasi dan asistensi kepada UPR SPBE dalam penerapan Manajemen Risiko SPBE;
4) penyusunan dan penyampaian rekomendasi terhadap efektivitas penerapan Manajemen Risiko SPBE kepada KMR SPBE dan UPR SPBE; dan
5) pelaksanaan konsultasi dan asistensi kepada UPR dalam pembinaan budaya sadar Risiko SPBE.

2. Budaya Sadar Risiko SPBE

Budaya sadar Risiko SPBE merupakan perilaku ASN yang mengenal, memahami, dan mengakui kemungkinan terjadinya Risiko SPBE, baik positif maupun negatif, yang ditindaklanjuti dengan upaya yang berfokus pada penerapan Manajemen Risiko SPBE di Pemerintah Daerah. ASN harus peka terhadap faktor-faktor dan peristiwa yang mungkin berpengaruh terhadap tujuan dan sasaran penerapan SPBE di Pemerintah Daerah.

Dengan menyadari adanya Risiko SPBE, ASN dapat merencanakan dan mempersiapkan tindakan atau penanganan Risiko SPBE secepatnya. Keterlibatan ASN di dalam budaya sadar Risiko SPBE akan memberikan nilai tambah dan meningkatkan efektivitas penerapan Manajemen Risiko SPBE yang pada akhirnya berdampak pada peningkatan kualitas penerapan SPBE di Pemerintah Daerah.

a. Faktor Keberhasilan

Faktor-faktor yang dapat mendukung keberhasilan dalam menciptakan budaya sadar Risiko SPBE antara lain:

1) Kepemimpinan

KMR SPBE harus dapat menunjukkan sikap kepemimpinan, yaitu konsisten dalam perkataan dan tindakan, mampu mendorong atau menggerakkan ASN dalam penerapan budaya sadar Risiko SPBE, mampu menempatkan Manajemen Risiko SPBE sebagai agenda penting di dalam setiap pengambilan keputusan yang terkait dengan penerapan SPBE, dan memiliki komitmen yang kuat

menerapkan Manajemen Risiko SPBE melalui penyediaan sumber daya yang cukup, baik anggaran, SDM, kebijakan, pedoman, maupun strategi penerapannya di Pemerintah Daerah.

2) Keterlibatan Semua Pihak
Budaya sadar Risiko SPBE melibatkan semua ASN yang terkait secara langsung maupun tidak langsung dengan penerapan SPBE, baik ASN yang berada pada KMR SPBE, UPR SPBE, maupun UKR SPBE, karena mereka yang paling memahami terjadinya Risiko SPBE dan cara penanganannya dalam level strategis maupun operasional.

3) Komunikasi
Komunikasi tentang pentingnya Manajemen Risiko SPBE harus dapat disampaikan kepada setiap ASN yang terlibat dalam penerapan SPBE melalui penyediaan saluran komunikasi yang variatif dan efektif. Tidak hanya KMR SPBE menyampaikan informasi terkait kebijakan Manajemen Risiko kepada ASN, tetapi juga ASN dapat menyampaikan informasi Risiko SPBE kepada pimpinan di setiap jenjang termasuk kepada KMR SPBE. Saluran komunikasi ini dapat diwujudkan melalui rapat-rapat pengambilan keputusan, berbagai pertemuan dalam proses Manajemen Risiko SPBE, dan penyampaian informasi melalui saluran komunikasi elektronik seperti surat elektronik, sistem naskah dinas elektronik, sistem aplikasi Manajemen Risiko, *video conference*, dan lain sebagainya.

4) Daya Responsif
Dalam budaya sadar Risiko SPBE, Risiko SPBE dieskalasi kepada pihak yang bertanggung jawab agar dapat ditangani dengan cepat. Sikap responsif ini sangat penting untuk mencegah ancaman yang dapat menghambat tercapainya tujuan penerapan SPBE ataupun meraih peluang untuk mempercepat tercapainya tujuan penerapan SPBE termasuk peningkatan kualitasnya. ASN yang responsif akan lebih siap beradaptasi terhadap perubahan dan penyelesaian masalah yang rumit dalam penerapan SPBE.

5) Sistem Penghargaan
KMR SPBE hendaknya memahami secara langsung permasalahan yang dialami oleh ASN pada pelaksanaan tugas UPR SPBE dan UKR SPBE, serta menjadikan pencapaian kinerja Risiko SPBE sebagai salah satu indikator dalam pemberian penghargaan dan sanksi.

6) Integrasi Proses
Proses Manajemen Risiko SPBE hendaknya diintegrasikan dengan proses manajemen di Pemerintah Daerah sehingga tidak dipandang sebagai tambahan beban pekerjaan. Integrasi proses dapat dilakukan dengan menyelaraskan proses Manajemen Risiko SPBE sebagai satu kesatuan dari setiap proses kegiatan, proses Manajemen Risiko, dan proses manajemen kinerja Pemerintah Daerah.

7) Program Kegiatan Berkelanjutan

Agar budaya sadar Risiko SPBE dapat diterima oleh ASN, KMR SPBE hendaknya menyusun program kegiatan budaya sadar Risiko SPBE secara sistematis dan terencana, seperti kegiatan edukasi, berbagi pengetahuan, dan kunjungan kerja/supervisi ke UPR SPBE.

b. Langkah-Langkah Pengembangan

Pengembangan budaya sadar Risiko SPBE dapat dilakukan melalui langkah-langkah berikut ini:

1) Menyusun perencanaan kegiatan budaya sadar Risiko SPBE;
2) Melaksanakan kegiatan budaya sadar Risiko SPBE; dan
3) Melakukan pemantauan dan Evaluasi pelaksanaan kegiatan budaya sadar Risiko SPBE.

Langkah-langkah pengembangan budaya sadar Risiko SPBE dapat dilihat pada Gambar di bawah ini.

Langkah Pengembangan Budaya Sadar Risiko SPBE Perencanaan kegiatan budaya sadar Risiko SPBE difokuskan pada:

1) Pemetaan pemangku kepentingan terhadap pelaksanaan Manajemen Risiko SPBE.

Tujuan dari pemetaan pemangku kepentingan adalah untuk melakukan penilaian terhadap pemangku kepentingan terkait peran dan kapasitas mereka dalam mempengaruhi keberhasilan penerapan budaya sadar Risiko SPBE, serta untuk menyusun prioritas kegiatan budaya sadar Risiko SPBE berdasarkan tingkat kekuatan, posisi penting, ataupun pengaruh dari pemangku kepentingan. Dalam hal ini, pemangku kepentingan dapat diidentifikasi dengan merujuk pada struktur Manajemen Risiko SPBE yang mencakup KMR SPBE, UPR SPBE, dan UKR SPBE.

2) Pengukuran tingkat dukungan pemangku kepentingan terhadap budaya sadar Risiko SPBE.

Hal ini menjadi penting untuk mengelola kegiatan budaya sadar Risiko SPBE secara efektif. Dukungan pemangku kepentingan dapat digolongkan ke dalam tiga kategori, yaitu: sangat mendukung secara konsisten, mendukung secara

tidak konsisten, dan tidak mendukung atau resistan terhadap budaya sadar Risiko SPBE.

3) Pengukuran tingkat kesiapan budaya sadar Risiko SPBE.
Pengukuran ini biasanya menggunakan kuesioner ang disampaikan kepada pemangku kepentingan, baik secara sampel maupun semua populasi. Pengukuran dapat difokuskan antara lain pada komitmen, manfaat/dampak, pemahaman/kesadaran, tata cara/prosedur pelaksanaan, dan partisipasi dari pemangku kepentingan terhadap penerapan Manajemen Risiko SPBE.

4) Penyusunan rencana kegiatan budaya sadar Risiko SPBE.
Rencana kegiatan yang tepat disusun dengan mempertimbangkan sumber daya yang tersedia di Pemerintah Daerah seperti anggaran, waktu, sarana dan prasarana, SDM pelaksana, peserta, dan metode pelaksanaan. Metode pelaksanaan kegiatan budaya sadar Risiko SPBE mencakup antara lain pelatihan, seminar, sosialisasi, kelompok diskusi, berbagi pengetahuan dan pengalaman, konsultansi, pembimbingan/pendampingan, dan supervisi.

Pelaksanaan kegiatan budaya sadar Risiko SPBE difokuskan pada implementasi rencana kegiatan budaya sadar Risiko SPBE, yaitu:

1) Melakukan komunikasi kepada pemangku kepentingan.
Sebelum melaksanakan rencana kegiatan budaya sadar Risiko SPBE, rencana tersebut perlu dikomunikasikan kepada pemangku kepentingan dengan memberikan alasan-alasan yang rasional agar mendapatkan dukungan pelaksanaan oleh pemangku kepentingan.

2) Mengelola hambatan/kendala.
Dalam pelaksanaan kegiatan budaya sadar Risiko SPBE, kendala- kendala yang terjadi agar dikelola dengan baik agar tujuan dari kegiatan tersebut dapat dicapai.

Pemantauan dan Evaluasi kegiatan budaya sadar Risiko SPBE ditujukan untuk meningkatkan budaya sadar Risiko SPBE melalui perbaikan berkelanjutan. Pelaksanaan pemantauan dan Evaluasi difokuskan pada:

1) Pengukuran perubahan tingkat dukungan, kesadaran, dan pemahaman dari pemangku kepentingan terhadap penerapan Manajemen Risiko SPBE.
Pengukuran terkait hal ini dapat dilakukan melalui pengumpulan dan analisis umpan balik dari pemangku kepentingan dengan cara supervisi ke unit-unit para pemangku kepentingan. Hasil analisis selanjutnya digunakan untuk memutakhirkan tingkat dukungan, kesadaran, dan pemahaman dari pemangku kepentingan, serta memberikan saran-saran perbaikan terhadap kegiatan budaya sadar Risiko SPBE.

2) Pemutakhiran rencana kegiatan budaya sadar Risiko SPBE.
Rencana kegiatan budaya sadar Risiko SPBE dilakukan pemutakhiran berdasarkan saran-saran perbaikan dengan

tetap mempertimbangkan ketersediaan sumber daya yang dimiliki oleh Instansi Pusat dan Pemerintah Daerah.

3) Pelaksanaan perbaikan berkelanjutan.
Rencana kegiatan budaya sadar Risiko SPBE yang telah dimutakhirkan dilaksanakan melalui langkah ke dua di atas sehingga mencapai peningkatan budaya sadar Risiko SPBE.

Penerapan Manajemen Risiko SPBE mutlak diperlukan untuk lebih menjamin pencapaian tujuan dan keberlangsungan dari SPBE. Pelaksanaan Manajemen Risiko SPBE diawali dengan penyusunan dan penetapan kerangka kerja Manajemen Risiko SPBE yang terintegrasi dengan proses kerja di Pemerintah Daerah. Kerangka kerja Manajemen Risiko SPBE mencakup prinsip, kepemimpinan dan komitmen, proses Manajemen Risiko SPBE, dan tata kelola Manajemen Risiko SPBE. Dalam pelaksanaannya, kerangka kerja Manajemen Risiko SPBE dapat disesuaikan dengan kondisi Pemerintah Daerah.

Agar Manajemen Risiko SPBE dapat diimplementasi dengan baik, diperlukan peran serta seluruh pihak internal Pemerintah Daerah maupun pemangku kepentingan lain. Koordinasi dan kolaborasi yang baik dengan seluruh elemen termasuk sistem yang telah berjalan di Pemerintah Daerah menjadi kunci keberhasilan pelaksanaan Manajemen Risiko SPBE.

LAMPIRAN

FORMULIR 1.0
PAKTA INTEGRITAS MANAJEMEN RISIKO SPBE

<Logo Pemerintah Daerah Kabupaten Natuna>

PAKTA INTEGRITAS MANAJEMEN RISIKO SPBE

<NOMOR PIAGAM>

<NAMA UPR>

<NAMA PEMERINTAH DAERAH>

<TAHUN PENERAPAN MANAJEMEN RISKO SPBE>

Dalam rangka pencapaian sasaran SPBE pada <Nama UPR SPBE>, saya menyatakan bahwa:

1. Penetapan konteks, identifikasi, analisis, Evaluasi, dan rencana penanganan Risiko SPBE telah sesuai dengan ketentuan Manajemen Risiko SPBE yang berlaku di <Nama Pemerintah Daerah>;
2. Rencana penanganan Risiko SPBE yang merupakan bagian yang tidak terpisahkan dari pakta integritas ini akan dilaksanakan oleh seluruh jajaran dalam unit yang saya pimpin;
3. Pemantauan dan reviu akan dilaksanakan secara berkala untuk meningkatkan efektivitas Manajemen Risiko SPBE.

<Tempat dan Tanggal Penetapan>

<Jabatan Pimpinan UPR>

<TTD>

<Nama Pimpiman UPR>

FORMULIR 2.0

KONTEKS

RISIKO SPBE

2.1. Informasi Umum

Nama UPR SPBE	:
Tugas UPR SPBE	:
Fungsi UPR SPBE	:
Periode Waktu	:

2.2. Sasaran SPBE

No	Sasaran UPR SPBE	Sasaran SPBE	Indikator Kinerja SPBE	Target Kinerja SPBE

2.3. Struktur Pelaksana Manajemen Risiko SPBE

Pemilik Risiko SPBE	:
Koordinator Risiko SPBE	:
Pengelola Risiko SPBE	:

2.4. Daftar Pemangku Kepentingan

No	Nama Unit/Instansi	Hubungan

2.5. Daftar Peraturan Perundang-Undangan

No	Nama Peraturan	Amanat

2.6. Kategori Risiko SPBE

No	Kategori Risiko SPBE

2.7. Area Dampak Risiko SPBE

No	Area Dampak Risiko SPBE

2.8. Kriteria Risiko SPBE

A. Kriteria Kemungkinan SPBE

Level Kemungkinan		Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi		
2	Jarang Terjadi		
3	Kadang-Kadang Terjadi		
4	Sering Terjadi		
5	Hampir Pasti Terjadi		

B. Kriteria Dampak SPBE

Area Dampak		Level Dampak				
		1	2	3	4	5
		Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Kinerja	Positif					
	Negatif					

2.9. Matriks Analisis Risiko SPBE dan Level Risiko SPBE

A. Matriks Analisis 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					
	4	Sering Terjadi					
	3	Kadang-Kadang Terjadi					
	2	Jarang Terjadi					
	1	Hampir Tidak Terjadi					

B. Level Risiko SPBE

Level Risiko		Rentang Besaran Risiko	Keterangan Warna
1	Sangat Rendah		
2	Rendah		
3	Sedang		
4	Tinggi		
5	Sangat Tinggi		

2.10. Selera Risiko SPBE

No	Kategori Risiko SPBE	Besaran Risiko Minimum yang Ditangani	
		Risiko SPBE Positif	Risiko SPBE Negatif

FORMULIR 3.0 PENILAIAN RISIKO SPBE

Unit Pemilik Risiko SPBE :
Periode Penerapan :

No	Sasarn SPBE	Indikatr Kinerja	Identifikasi Risiko SPBE						AnalisisRisiko SPBE							Evaluasi Risiko SPBE	
			Jenis Risiko Kejadian Penyebab Kategori Dampak Area SPBE						Kemungkinan Dampak Sistem Besaran Level							Keputusan Penanganan Risiko SPBE, Prioritas Risiko	
									pengendalian	Level Penjelasan		Level Penjelasan		Risiko	Risiko	(Ya/Tidak)	

FORMULIR 4.0
RENCANA PENANGANAN RISIKO SPBE

Unit Pemilik Risiko :
Waktu Penerapan :

Prioritas Risiko	Rencana Penanganan Risiko SPBE					Apakah Terdapat Risiko Residual (Ya/Tidak)
	Opsi Penanganan Risiko SPBE	Rencana Aksi Penanganan Risiko SPBE	Keluaran	Jadwal Implementasi	Penanggung Jawab	

FORMULIR 5.0

LAPORAN PEMANTAUAN RISIKO SPBE

Laporan Pemantauan Risiko SPBE Triwulan <I, II, atau III>

Nama Unit :

Sasaran:

Risiko :

Besaran/Level Risiko SPBE Saat ini dan Proyeksi Risiko SPBE

Penanganan yang telah dilakukan

Rencana Penanganan	Penanggung jawab	Waktu Pelaksanaan

Laporan Pemantauan Risiko SPBE Tahunan

Nama Unit :

Sasaran :

Risiko :

Besaran/Level Risiko SPBE Saat ini dan Proyeksi Risiko

Penanganan yang telah dilakukan

Rekomendasi	

BUPATI NATUNA,

ttd

WAN SISWANDI

BAB II
MANAJEMEN KEAMANAN INFORMASI

A. Pendahuluan

Sebagaimana amanat Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, bahwa Pemerintah Daerah menerapkan Keamanan SPBE. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait Data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE. Penjaminan kenirsangkalan (*nonrepudiation*) dilakukan melalui penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital. 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.

Atas amanat peraturan presiden tersebut, maka Sistem manajemen keamanan informasi Pemerintah Berbasis Elektronik terdiri atas:

1. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap Data dan informasi;
2. penjaminan ketersediaan infrastruktur yang terdiri atas Pusat Data, Jaringan Intra Pemerintah, dan Sistem Penghubung Layanan penyelenggaraan pemerintahan berbasis elektronik; dan
3. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Saat ini Pemerintah Daerah Kabupaten telah menyelenggarakan SPBE sebagaimana diamanatkan Peraturan Presiden Nomor 95 Tahun 2018, diantaranya melalui pemanfaatan aplikasi *e-Office* sebagai inovasi layanan publik yang terintegrasi untuk meningkatkan kualitas pelayanan masyarakat yang efektif, efisien, transparan dan akuntabel. Aplikasi *e-Office* dibangun berdasarkan Misi Pemerintah Daerah yan terkait misi ini yaitu misi ke-6 Menciptakan Reformasi Birokrasi yang Cerdas (SMART) dan misi ke-7 Mengoptimalkan Penggunaan Teknologi Informasi dan Komunikasi.

B. Ruang Lingkup

Penetapan ruang lingkup dilakukan dengan mendefinisikan isu internal Keamanan Informasi SPBE dalam organisasi dan isu eksternal Keamanan Informasi SPBE. Isu internal Keamanan Informasi SPBE didefinisikan berdasarkan area yang menjadi prioritas organisasi terhadap pelaksanaan Keamanan Informasi SPBE. Area yang menjadi prioritas organisasi terhadap pelaksanaan Keamanan Informasi SPBE meliputi Data dan informasi SPBE, Aplikasi SPBE, Aset Infrastruktur SPBE dan Kebijakanan Keamanan Informasi SPBE yang telah dimiliki. Isu Eksternal Keamanan Informasi SPBE didefinisikan sesuai dengan ketentuan Peraturan Perundang-undangan.

Penetapan ruang lingkup dilakukan oleh bupati. Sistem manajemen keamanan informasi Pemerintah Daerah Kabupaten memiliki ruang lingkup:

1. Data dan Informasi Pemerintah Daerah Kabupaten

Keamanan Data dan informasi Pemerintah Daerah Kabupaten dilakukan dengan memanfaatkan sertifikat elektronik, yang terdiri dari: Tanda Tangan Elektronik, Proteksi email, Proteksi dokumen dan *Secure Socket Layer* (SSL).

Seluruh ASN dan perangkat desa wajib memiliki Sertifikat elektronik, untuk pemanfaatan *e-office.* Proses untuk mendapatkan sertifikat elektronik dilakukan melalui Perangkat Daerah Kabupaten yang menyelenggarakan urusan pemerintahan bidang persandian sebagai fungsi otorisasi dari Balai Sertifikasi Elektronik (BSrE) pada Badan Siber dan Sandi Negara (BSSN) sebagaimana diatur pada Peraturan Bupati Nomor 43 Tahun 2021 tentang Penyelenggaraan Sertifikat Elektronik.

a. Tanda Tangan Elektronik

Tanda tangan elektronik memiliki kekuatan dan akibat hukum yang sah. Landasan penggunaan tanda tangan elektronik ini diperkuat dengan adanya Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mewajibkan Penyelenggara Sistem Elektronik (PSE) memiliki sertifikat elektronik yang memuat tanda tangan elektronik dan identitas lainnya sebagai status subjek hukum dalam transaksi elektronik.

Tanda tangan elektronik membantu memenuhi 3 aspek Keamanan Informasi, yakni: Autentikasi (keaslian) pengirim/penerima, memastikan bahwa informasi dikirimkan dan diterima oleh pihak yang benar, Integritas (keutuhan) Data, memastikan bahwa informasi tidak diubah/dimodifikasi selama informasi tersebut disimpan atau pada saat dikirimkan, mekanisme anti-sangkal (non-repudiasi), memastikan bahwa pemilik informasi tidak dapat menyangkal bahwa informasi tersebut adalah miliknya atau telah disahkan olehnya.

Pemerintah Daerah Kabupaten memanfaatkan tanda tangan elektronik untuk menandatangani dokumen digital dan surat elektronik pada aplikasi *e-office*. Tanda tangan elektronik melalui *e- office* akan meningkatkan efektivitas pekerjaan karena hemat waktu dapat dilakukan dimanapun berada, meningkatkan efisiensi anggaran karena mengurangi pembelian ATK, Tanda tangan elektronik aman dan legal apabila pemilik sertifikat elektronik tidak memberikan informasi *passphrase*nya kepada orang lain, tanda tangan elektronik sangat ramah lingkungan karena *paperless office*.

Keaslian dokumen yang telah ditanda tangan secara elektronik dapat diketahui dengan menggunakan aplikasi Very DS dari BSrE yaitu aplikasi verifikasi dokumen PDF.

b. Proteksi email

Sertifikat elektronik diterbitkan dengan menggunakan email resmi, dalam hal ini Pemerintah Daerah kabupaten memiliki email natunakab.go.id. untuk menjamin kerahasiaan dan integritas email dari penyadapan dan modifikasi serta menjamin autentikasi dan nir-penyangkalan pengirim email.

Seluruh ASN secara kolektif melalui SKPDnya mengajukan permohonan pembuatan email natunakab.go.id kepada Perangkat Daerah Kabupaten yang menyelenggarakan urusan pemerintahan bidang persandian.

c. Proteksi dokumen
Sertifikat elektronik menjamin keaslian dokumen, otentikasi dan nir penyangkalan pemilik dokumen serta kerahasiaan dokumen.

d. *Secure Socket Layer* (SSL)
Sertifikat elektronik menjamin kerahasiaan, otentikasi dan integritas paket Data serta nir penyangkalan *website server* (*SSL Server*) atau pengakses *website* (*SSL Client*).

2. Aset Pengolah dan Penyimpan Informasi (aplikasi dan Infrastruktur SPBE)

Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi Elektronik. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh pemerintah daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.

Infrastruktur SPBE adalah adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi Data, pengolahan dan penyimpanan Data, perangkat integrasi/penghubung, dan perangkat elektronik.

Pemerintah Daerah Kabupaten sangat banyak membangun Aplikasi Khusus baik itu yang bersifat pelayanan ataupun untuk digunakan di internal SKPD.

Untuk Identifikasi kerentanan dan penilaian risiko Keamanan Informasi Aplikasi Khusus dan jaringannya, maka dinas komunikasi dan informatika melakukan pengujian keamanan.

Pengujian keamanan terhadap aplikasi khusus dan jaringan tersebut yaitu dengan *penetration testing (pentest)* bersamaan dengan *Vulnerability Assessment (VA)*.

Pentest dan *Vulnerability Assessment (VA)* adalah sebuah proses untuk mengidentifikasi risiko dan celah kerentanan pada aplikasi, sistem, ataupun jaringan.

Dalam impelementasinya, *pentest* dapat berguna antara lain untuk menentukan seberapa baik sebuah sistem dapat menangani serangan, selain itu dapat menentukan penanggulangan yang dapat mengurangi ancaman terhadap sistem dan untuk meningkatkan keamanan pada aplikasi, sistem atau jaringan yang dimiliki. *Pentest* juga digunakan untuk mendeteksi serangan dan merespon dengan cepat dan tepat, sehingga *pentest* bertujuan untuk menganalisis risiko yang akan timbul dengan adanya kerentanan yang telah diindetifikasi pada tahap *Vulnerability Assessment (VA)* dan memberikan

rekomendasi tindakan yang perlu dilakukan apabila sistem yang diuji dapat lolos dari serangan *hacker* dan kehilangan Data.

SKPD dapat mengajukan permohonan ke dinas komunikasi dan informatika untuk dilakukan pengujian keamanan terhadap Aplikasi Khusus yang dimilikinya.

Dalam menjalankan pengujian, terdapat 4 (empat) tahapan dalam *Pentest* yaitu tahap perencanaan, *discovery*, serangan dan pelaporan. *Pentest* dilakukan menggunakan *tools*. adalah perencanaan, dilakukan identifikasi aturan dalam pengujian.

Tahapan pertama, perencanaan dilakukan identifikasi aturan dalam pengujian, selain persetujuan kedua belah pihak terkait jalannya pengujian dan ruang lingkup pengujian telah diselesaikan dan didokumentasikan kemudian menetapkan tujuan pengujian. Tahap perencanaan menentukan sukses atau tidaknya *pentest* yang dilakukan.

Tahap kedua, penemuan terdiri dari dua bagian yaitu pengumpulan informasi dan analisis potensial kerentanan (*Vulnerability Analysis*). pengumpulan informasi terkait target melalui identifikasi *port* jaringan dan layanan atau *IP address*. Analisis potensial kerentanan dilakukan dengan menggunakan *tools*.

Tahap ketiga, serangan. Mengeksekusi serangan adalah poin utama dalam *pentest*, dilakukan penentuan target, pemilihan *tools* dan metode eksploit yang tepat. Analisis potensial kerentanan yang sudah diindentifikasi sebelumnya diverifikasi dengan percobaan eksploitasi.

Tahap keempat, pelaporan. Laporan dibuat untuk menggambarkan Langkah kerja yang dilakukan, kerentanan yang teridentifikasi selama pengujian, mengidentifikasi risiko dan memberikan rekomendasi terkait untuk mengurangi kerentanan yang ditemukan dan langkah peningkatan keamanan sistem.

3. Sumber Daya Manusia

Peningkatan Sumber Daya Manusia untuk urusan Keamanan Informasi Pemerintah Daerah Kabupaten, dilakukan melalui pelaksanaan literasi, sosialisasi, bimbingan teknis dan mengutus pegawai untuk memgikuti Pendidikan dan pelatihan khusus keamanan di Lembaga terpercaya.

Dibentuk para admin sertifikat elektronik dan Keamanan Informasi di SKPD untuk mempermudah koordinasi dalam hal permasalahan Keamanan Informasi.

C. Pedoman Sistem Manajemen Keamanan Informasi

Standar Sistem Manajemen Keamanan Informasi (SMKI) adalah dengan menerapkan SNI ISO/IEC 27001:2013. Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi Aset Informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Proses SMKI menggunakan model *PLAN – DO – CHECK – ACT* (PDCA).

a) *PLAN* (Menetapkan SMKI)
Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dan sasaran.
b) *DO* (Menerapkan dan mengoperasikan SMKI)
Menerapkan dan mengoperasikan kebijakan SMKI, kontrol, proses dan prosedur-prosedur.
c) *CHECK* (Memantau dan melakukan tinjau ulang SMKI)
Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya.
d) *ACT* (Memelihara dan meningkatkan SMKI)
Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil Evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

Untuk mempersiapkan penerapan SNI ISO/IEC 27001:2013 dapat melakukan penilaian berdasarkan Indeks Keamanan Informasi (Indeks KAMI)

Indeks Keamanan Informasi (Indeks KAMI) merupakan alat Evaluasi yang dapat digunakan untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pusat maupun pemerintah daerah yang menyelenggarakan SPBE. Alat Evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja Keamanan Informasi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan Keamanan Informasi dengan ruang lingkup pembahasan yang memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013, yaitu:
1. Tata Kelola Keamanan Informasi;
2. Pengelolaan Risiko Keamanan Informasi;
3. Kerangka Kerja Keamanan Informasi;
4. Pengelolaan Aset Informasi; dan
5. Teknologi dan Keamanan Informasi.

Perangkat Daerah Kabupaten yang menyelenggarakan urusan pemerintahan bidang persandian melakukan Evaluasi Keamanan Informasi menggunakan Indeks KAMI, dengan tahapan sebagai berikut :
1. Sosialisasi
Tahap untuk mensosialisasikan kegiatan Analisis dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI bagi Perangkat Daerah penyelenggara Sistem Elektronik untuk pelayanan publik di lingkungan Pemerintah Daerah tentang substansi dari Indeks KAMI dan tata cara pengisian instrumennya
2. Pengisian *instrument*
Tahap pengisian instrumen Indeks KAMI beserta dokumen yang harus dilampirkan sebagai bukti fisiknya oleh Perangkat Daerah penyelenggara Sistem Elektronik untuk pelayanan publik di lingkungan Pemerintah Daerah.
3. Verifikasi Hasil Pengisian

Tahap untuk memverifikasi instrumen Indeks KAMI yang sudah diisi berdasarkanbukti fisik yang dilampirkan.

4. Analisis dan Evaluasi

Tahap untuk menganalisis dan mengevaluasi Indeks KAMI yang telah diverifikasi, dan menyusun rekomendasi perbaikan untuk meningkatkan kelengkapan dan kematangan aspek-aspek pengamanan informasi pada setiap area Evaluasi.

5. Pembuatan Laporan

Tahap penyusunan laporan pelaksanaan kegiatan Analisis dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI yang mencakup: Laporan Pendahuluan Laporan yang menginformasikan rencana kerja, metodologi, serta sistematika dokumen dan Laporan Akhir Laporan yang menginformasikan seluruh hasil pelaksanaan kegiatan.

D. Standar Teknis Dan Prosedur Keamanan SPBE

Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan SPBE. Penerapan Keamanan SPBE harus memenuhi standar teknis dan prosedur Keamanan SPBE. Standar teknis dan prosedur Keamanan SPBE diterapkan untuk keamanan Data dan informasi, keamanan Aplikasi SPBE, keamanan Sistem Penghubung Layanan, keamanan Jaringan Intra dan keamanan Pusat Data Nasional.

1. Data dan Informasi

Informasi diklasifikasikan menjadi 4 (empat) kategori, yaitu:

a. Informasi Rahasia

Informasi Rahasia adalah informasi yang karena sifatnya tidak dapat diungkapkan kepada pihak internal dan publik yang tidak memiliki kewenangan dan kepentingan sehingga apabila diungkapkan akan merugikan kepentingan Perseroan dan/atau Pemegang Saham, dan/atau melanggar ketentuan perundang-undangan yang berlaku.

Termasuk dalam kategori Informasi Rahasia adalah informasi-informasi yang mengandung esensi sebagaimana tersebut di bawah ini, antara lain:

- Apabila diungkapkan mengakibatkan kerugian baik secara finansial maupun non-finansial.
- Apabila diungkapkan mengakibatkan kerugian bagi pihak lain yang memiliki keterikatan kontraktual.
- Apabila diungkapkan mengakibatkan gangguan operasional.
- Apabila diungkapkan mengakibatkan gangguan tentang ketertiban, kelancaran, kesesuaian dan keserasian lingkungan kerja.
- Memuat rencana strategi Perusahaan, strategi pemasaran, dan informasi penting lainnya yang bisa mempengaruhi pengambilan keputusan bagi kompetitor.
- Menyangkut catatan dan keterangan mengenai individu Pekerja yang bersifat sensitif.
- Belum memiliki ketetapan karena sifatnya strategis dan sensitif.

b. Informasi Terbatas

Informasi Terbatas adalah informasi yang tidak termasuk kategori rahasia dan publik yang ditujukan untuk kepentingan internal dan tidak untuk diungkapkan kepada publik.

Termasuk dalam kategori Informasi Terbatas adalah informasi-informasi yang mengandung esensi sebagaimana tersebut di bawah ini, antara lain:

- Memuat materi yang hanya dapat digunakan secara internal di lingkungan Perusahaan dan tidak dimaksudkan untuk kepentingan publik.
- Berasal dari pihak di luar Perusahaan yang khusus ditujukan untuk kepentingan internal Perusahaan.

c. Informasi Publik

Informasi Publik adalah informasi yang tidak memuat kriteria sebagai Informasi Rahasia dan Informasi Terbatas serta ditujukan untuk kepentingan Publik baik karena ketentuan perundang-undangan yang berlaku maupun atas inisiatif Perseroan. Termasuk dalam kriteria Informasi Publik yaitu Informasi Biasa yang berdasarkan sifatnya apabila diungkapkan kepada Publik tidak menimbulkan dampak negatif.

Termasuk dalam kategori Informasi Publik adalah informasi-informasi yang mengandung esensi sebagaimana tersebut di bawah ini, antara lain:

- Memuat materi yang menurut peraturan perundang-undangan yang berlaku wajib disediakan untuk kepentingan Publik.
- Memuat materi yang karena kepentingan kebutuhan Pemerintah Daerah disampaikan kepada Publik, seperti brosur promosi, press release, pengumuman, *newsletter*, majalah, dan sejenisnya.
- Telah menjadi milik publik, seperti Laporan Tahunan (*Annual Report*) dan informasi- informasi lainnya yang dimuat di dalam *website* Pemerintah Daerah.

d. Informasi Tidak Terklasifikasi

Informasi-informasi lain yang berdasarkan isi, sifat dan kondisinya belum dapat dikategorikan dalam klasifikasi manapun sesuai dengan ketentuan ini ditetapkan klasifikasinya oleh Direksi atau Pejabat Satu Level di Bawah Direksi.

Standar teknis keamanan Data dan informasi terdiri atas:

a. Kerahasiaan

Terpenuhinya aspek kerahasiaan dilakukan dengan prosedur:

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

b. Keaslian
Terpenuhinya aspek keaslian dilakukan dengan prosedur:
1) menyediakan mekanisme verifikasi;
2) menyediakan mekanisme validasi; dan
3) menerapkan sistem *hash function*.

c. Keutuhan
Terpenuhinya aspek keutuhan dilakukan dengan prosedur:
1) menerapkan pendeteksian modifikasi; dan
2) menerapkan tanda tangan elektronik tersertifikasi.

d. Kenirsangkalan
Terpenuhinya aspek kenirsangkalan dilakukan dengan prosedur:
1) menerapkan tanda tangan elektronik tersertifikasi; dan
2) penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

e. Ketersediaan
Terpenuhinya aspek ketersediaan dilakukan dengan prosedur:
1) menerapkan sistem pencadangan secara berkala;
2) membuat perencanaan untuk menjamin Data dan informasi dapat selalu diakses; dan
3) menerapkan sistem pemulihan.

2. Keamanan Aplikasi SPBE
Aplikasi SPBE sebagaimana dimaksud pada ayat (1) harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:
a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan
e. menganalisis kerentanan.

Standar teknis dan prosedur keamanan Aplikasi SPBE diterapkan pada:
a. aplikasi berbasis web
Aplikasi berbasis web merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet. Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:
1) autentikasi;
Terpenuhinya fungsi autentikasi dilakukan dengan prosedur:
- menggunakan manajemen kata sandi untuk proses autentikasi;
- menerapkan verifikasi kata sandi pada sisi server;
- mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
- mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
- mengatur mekanisme pemulihan kata sandi;

- menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
- menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

2) manajemen sesi

Terpenuhinya fungsi manajemen sesi dilakukan dengan prosedur:

- menggunakan pengendali sesi untuk proses manajemen sesi;
- menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
- mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
- mengatur kondisi dan jangka waktu habis sesi;
- validasi dan pencantuman *session id*;
- pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
- pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.

3) persyaratan kontrol akses

Terpenuhinya fungsi persyaratan kontrol akses dilakukan dengan prosedur:

- menetapkan otorisasi pengguna untuk membatasi kontrol akses;
- mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
- mengatur antarmuka pada sisi administrator; dan
- mengatur verifikasi kebenaran token ketika mengakses Data dan informasi yang dikecualikan.

4) validasi input

Terpenuhinya fungsi validasi input dilakukan dengan prosedur:

- menerapkan fungsi validasi input pada sisi server;
- menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
- memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
- melakukan validasi positif pada seluruh input;
- melakukan *filter* terhadap Data yang tidak dipercaya;
- menggunakan fitur kode dinamis;
- melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
- melakukan pelindungan dari serangan injeksi basis Data.

5) kriptografi pada verifikasi statis;

Terpenuhinya fungsi kriptografi pada verifikasi statis dilakukan dengan prosedur:

- menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan Peraturan Perundang-undangan;
- melakukan autentikasi Data yang dienkripsi;
- menerapkan manajemen kunci kriptografi; dan

- membuat angka acak yang menggunakan generator angka acak kriptografi.

6) penanganan eror dan pencatatan log

Terpenuhinya fungsi penanganan eror dan pencatatan log dilakukan dengan prosedur:

- mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
- menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
- tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
- mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
- mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
- melakukan enkripsi pada Data yang disimpan untuk mencegah injeksi log; dan
- melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

7) proteksi Data

Terpenuhinya fungsi proteksi Data dilakukan dengan prosedur:

- melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
- melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
- melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
- melakukan penentuan jumlah parameter;
- memastikan Data disimpan dengan aman;
- menentukan metode untuk menghapus dan mengekspor Data sesuai permintaan pengguna; dan
- membersihkan memori setelah tidak diperlukan.

8) keamanan komunikasi

Terpenuhinya fungsi keamanan komunikasi dilakukan dengan prosedur:

- menggunakan komunikasi terenkripsi
- mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna
- mengatur jenis algoritma yang digunakan dan alat pengujiannya
- mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik

9) pengendalian kode berbahaya

Terpenuhinya fungsi pengendalian kode berbahaya dilakukan dengan prosedur:

- menggunakan analisis kode dalam kontrol kode berbahaya;

- memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
- mengatur izin terkait fitur atau sensor terkait privasi;
- mengatur pelindungan integritas; dan
- mengatur mekanisme fitur pembaruan

10) logika bisnis

Terpenuhinya fungsi logika bisnis dilakukan dengan prosedur:

- memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
- memastikan logika bisnis memiliki batasan dan validasi;
- memonitor aktivitas yang tidak biasa;
- membantu dalam kontrol antiotomatisasi; dan
- memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

11) *File*

Terpenuhinya fungsi file dilakukan dengan prosedur:

- mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah;
- melakukan validasi file sesuai dengan tipe konten yang diharapkan;
- melakukan pelindungan terhadap Metadata input dan Metadata file;
- melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya; dan
- melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan.

12) keamanan API dan *web service*

Terpenuhinya fungsi keamanan API dan web dilakukan dengan prosedur:

- melakukan konfigurasi layanan web;
- memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
- membuat keputusan otorisasi;
- menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;
- menggunakan validasi skema dan verifikasi sebelum menerima input;
- menggunakan metode pelindungan layanan berbasis web; dan
- menerapkan kontrol antiotomatisasi.

13) keamanan konfigurasi.

Terpenuhinya fungsi keamanan konfigurasi dilakukan dengan prosedur:

- mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
- mendokumentasi, menyalin konfigurasi, dan semua dependensi;
- menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;

- memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
- menggunakan respons aplikasi dan konten yang aman.

b. aplikasi berbasis *mobile*

Aplikasi berbasis *mobile* merupakan aplikasi yang dalam pengoperasiannya dapat berjalan diperangkat bergerak, dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.

Standar teknis keamanan aplikasi berbasis mobile terdiri atas terpenuhinya fungsi:

1) penyimpanan data dan persyaratan privasi

Terpenuhinya fungsi penyimpanan data dan persyaratan privasi dilakukan dengan prosedur:

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

2) Kriptografi

Terpenuhinya fungsi kriptografi dilakukan dengan prosedur:

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

3) autentikasi dan manajemen sesi

Terpenuhinya fungsi autentikasi dan manajemen sesi dilakukan dengan prosedur:

- menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
- menggunakan session identifier yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan stateful manajemen sesi;
- memastikan server menyediakan token yang telah ditandatangani menggunakan algoritme yang aman apabila menggunakan autentikasi stateless berbasis token;
- memastikan remote endpoint memutus sesi yang ada saat pengguna log out;
- menerapkan pengaturan sandi pada remote endpoint;

- membatasi jumlah percobaan log in pada remote endpoint;
- menentukan masa berlaku sesi dan masa kedaluwarsa token pada remote endpoint; dan
- melakukan otorisasi pada *remote endpoint*.

4) komunikasi jaringan

Terpenuhinya fungsi komunikasi dilakukan dengan prosedur:

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

5) interaksi platform

Terpenuhinya fungsi interaksi platform dilakukan dengan prosedur:

memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;

- melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
- menghindari pengiriman fungsionalitas sensitif melalui skema custom uniform resource locator dan fasilitas inter process communication;
- menghindari penggunaan JavaScript dalam WebView;
- menggunakan protokol hypertext transfer protocol secure pada WebView; dan
- mengimplementasikan penggunaan serialisasi API yang aman.

6) kualitas kode dan pengaturan *build*

Terpenuhinya fungsi kualitas kode dan pengaturan *build* dilakukan dengan prosedur:

- menandatangani aplikasi dengan sertifikat yang valid;
- memastikan aplikasi dalam mode rilis;
- menghapus simbol debugging dari native binary;
- menghapus kode debugging dan kode bantuan pengembang;
- mengidentifikasi kelemahan seluruh komponen third party;
- menentukan mekanisme penanganan eror;
- mengelola memori secara aman; dan
- mengaktifkan fitur keamanan yang tersedia.

7) Ketahanan

Terpenuhinya fungsi ketahanan dilakukan dengan prosedur:

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

3. Keamanan Sistem Penghubung Layanan
   Standar teknis keamanan Sistem Penghubung Layanan terdiri atas terpenuhinya fungsi:
   a. keamanan Interoperabilitas Data dan informasi;
      Terpenuhinya fungsi keamanan Interoperabilitas Data dan informasi dilakukan dengan prosedur:
      1) menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
      2) menerapkan sistem enkripsi Data;
      3) memastikan Data dan informasi selalu dapat diakses sesuai otoritasnya; dan
      4) menerapkan sistem *hash function* pada *file*.
   b. kontrol sistem integrasi;
      Terpenuhinya fungsi kontrol sistem integrasi dilakukan dengan prosedur:
      1) menerapkan protokol *secure socket layer* atau *protokol transport layer security* versi terkini pada sesi pengiriman Data dan informasi;
      2) menerapkan internet protocol security untuk mengamankan transmisi Data dalam jaringan berbasis transmission control protocol/internet protocol;
      3) menerapkan sistem anti distributed denial of service;
      4) menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung;
      5) menerapkan manajemen keamanan sesi;
      6) menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
      7) menerapkan validasi input;
      8) menerapkan kriptografi pada verifikasi statis;
      9) menerapkan sertifikat elektronik pada web authentication;
      10) menerapkan penanganan eror dan pencatatan log;
      11) menerapkan proteksi Data dan jalur komunikasi;
      12) menerapkan pendeteksi virus untuk memeriksa beberapa konten file;
      13) menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus); dan
      14) memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.
   c. kontrol perangkat integrator
      Terpenuhinya fungsi kontrol perangkat integrator dilakukan dengan prosedur:
      1) menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
      2) menggunakan anti virus dan anti-*spyware* terkini;
      3) mengaktifkan fitur keamanan pada peramban web;
      4) menerapkan *firewall* dan *host-based intrusion detection systems*;
      5) mencegah instalasi perangkat lunak yang belum terverifikasi;
      6) mencegah akses terhadap situs yang tidak sah; dan
      7) mengaktifkan sistem *recovery* dan *restore* pada perangkat integrator.

d. keamanan API dan *web service*
Terpenuhinya fungsi keamanan API dan *web service* dilakukan dengan prosedur:
1) menerapkan protokol *secure socket layer* atau protokol *transport layer security* diantara pengirim dan penerima API;
2) menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner*, *resource server* dan/atau *third party*;
3) menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;
4) melindungi layanan web RESTful yang menggunakan *cookie* dari *cross-site request forgery*; dan
5) memvalidasi parameter yang masuk oleh penerima API untuk memastikan Data yang diterima valid dan tidak menyebabkan kerusakan.

e. keamanan migrasi Data.
Terpenuhinya fungsi keamanan migrasi Data dilakukan dengan prosedur:
1) memastikan migrasi Data dilakukan secara bertahap dan terprogram oleh sistem;
2) memastikan aplikasi yang menggunakan sistem basis Data lama tetap dipertahankan sampai sistem pendukung basis Data baru dapat berjalan atau berfungsi dengan normal;
3) mendokumentasikan format sistem basis Data lama secara rinci;
4) melakukan pencadangan seluruh Data yang tersimpan pada sistem sebelum melakukan migrasi Data;
5) menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan Data; dan
6) melakukan validasi Data ketika proses migrasi Data selesai.

4. Keamanan jaringan
Standar teknis keamanan Jaringan Intra diterapkan pada:
a. Jaringan Intra pemerintah; dan
b. Jaringan Intra Instansi Pusat dan Pemerintah Daerah.

Standar teknis keamanan Jaringan Intra terdiri atas terpenuhinya:
a. aspek administrasi keamanan Jaringan Intra
Terpenuhinya aspek administrasi keamanan Jaringan Intra dilakukan dengan prosedur:
1) menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
2) mengidentifikasi seluruh aset infrastruktur jaringan;
3) menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
4) membuat laporan pengawasan keamanan jaringan secara periodik.

b. kontrol akses dan autentikasi
Terpenuhinya kontrol akses dan autentikasi dilakukan dengan prosedur:
1) menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
2) menggunakan autentikasi untuk mengakses Jaringan Intra;
3) menerapkan pembatasan akses dalam Jaringan Intra;

4) mematikan atau membatasi *protocol*, *port*, dan layanan yang tidak digunakan;
5) menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
6) menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
7) menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
8) memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
9) menerapkan *secure endpoints*;
10) memblokir layanan yang tidak dikenal;
11) menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra; dan
12) menerapkan server perantara saat client mengakses *server database* dalam rangka pemeliharaan.

c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra
Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra dilakukan dengan prosedur:
1) menggunakan perangkat *security information and event management* untuk *network logging dan monitoring*;
2) menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
3) menggunakan perangkat *firewall*;
4) menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*;
5) menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;
6) menerapkan kontrol *update patching* pada infrastruktur Jaringan Intra dan sistem komputer;
7) menggunakan perangkat *web application firewall*;
8) menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
9) memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
10) mengunduh perangkat lunak melalui *enterprise software distribution system*; dan
11) menerapkan sertifikat elektronik.

d. kontrol keamanan *gateway*
Terpenuhinya kontrol keamanan *gateway* dilakukan dengan prosedur:
1) menerapkan *content filtering*;
2) menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada Jaringan Intra;
3) menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;
4) memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;

5) melaksanakan manajemen *traffic gateway*; dan
6) memastikan *port* tidak dibuka secara *default*.

e. kontrol keamanan *access point* pada jaringan nirkabel
Terpenuhinya kontrol keamanan *access point* pada jaringan nirkabel dilakukan dengan prosedur:
1) menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
2) menerapkan media *access control* pada *address filtering*;
3) menerapkan *dedicated service set identifier*;
4) menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
5) menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
6) menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan
7) melakukan *patching firmware* secara rutin.

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

5. Keamanan Pusat Data Nasional
Standar teknis keamanan Pusat Data Nasional terdiri atas terpenuhinya:

a. persyaratan keamanan fisik dan manajemen Pusat Data Daerah
Terpenuhinya persyaratan keamanan fisik dan manajemen Pusat Data Daerah dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan Pusat Data.

b. persyaratan koneksi perangkat ke Pusat Data Daerah
Terpenuhinya persyaratan koneksi perangkat ke Pusat Data Daerah dilakukan dengan prosedur:
1) memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data Daerah;
2) memutus akses fisik atau *logic* dari perangkat yang tidak terotorisasi;
3) memastikan akses tingkat administrator ke server dan perangkat jaringan utama tidak boleh dilakukan secara *remote*;
4) memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area Pusat Data Nasional;
5) melakukan *backup* informasi dan perangkat lunak yang berada di Pusat Data Nasional secara berkala;

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

E. Penanggung Jawab Penyelenggara SMKI

Penyelenggara Sistem Manajemen Keamanan Informasi (SMKI) Pemerintah Daerah Kabupaten, terdiri dari:

1. Penanggung Jawab yaitu Sekretaris Daerah Kabupaten/Koordinator SPBE.
2. Pelaksana Teknis:
   a. Kepala Perangkat Daerah Kabupaten yang menyelenggarakan urusan pemerintahan di bidang teknologi, informasi, dan komunikasi. Kepala Perangkat Daerah melaksanakan tugas:
      1) memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
      2) merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan
      3) melaporkan pelaksanaan manajemen Keamanan Informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE.
   b. Kepala Unit Kerja yang dimaksud membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE. Kepala unit kerja bidang persandian melaksanakan tugas:
      1) menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;
      2) memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
      3) memastikan keberlangsungan Proses Bisnis SPBE; dan
      4) berkoordinasi dengan Kepala Dinas Komunikasi dan Informatika terkait perumusan program kerja dan anggaran Keamanan SPBE.

F. Perencanaan

Perencanaan dilakukan oleh pelaksana teknis Keamanan SPBE.

1. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE, terdiri dari:
   a. edukasi kesadaran Keamanan SPBE, dilaksanakan melalui sosialisasi dan pelatihan.
   b. penilaian kerentanan Keamanan SPBE yaitu terdiri dari menginventarisasi seluruh aset SPBE meliputi Data dan informasi, aplikasi, dan infrastruktur, mengidentifikasi

kerentanan dan ancaman terhadap aset SPBE, mengukur tingkat risiko Keamanan SPBE.

c. peningkatan Keamanan SPBE melalui menerapkan standar teknis dan prosedur Keamanan SPBE, menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE. Evaluasi Kinerja dilaksanakan dengan menganalisis efektifitas pelaksanaan Keamanan SPBE atau mendukung dan merealisasikan program audit Keamanan SPBE.

d. penanganan insiden Keamanan SPBE, dengan mengidentifikasi sumber serangan, menganalisis informasi yang berkaitan dengan insiden selanjutnya, memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi, mendokumentasi bukti insiden yang terjadi dan memitigasi atau mengurangi dampak risiko Keamanan SPBE.

e. audit Keamanan SPBE dilakukan sesuai peraturan yang berlaku.

2. target realisasi program kerja Keamanan SPBE disesuaikan dengan kebutuhan Pemerintah Daerah Kabupaten.

G. Penganggaran

Penganggaran Keamanan SPBE bersumber dari:

1. anggaran pendapatan dan belanja Daerah Kabupaten;
2. Sumber lain yang sah sesuai ketentuan Peraturan Perundang-undangan.

H. Monitoring Dan Evaluasi

Dalam melaksanakan monitoring dan Evaluasi keamanan SPBE dilaksanakan:

1. identifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE.
2. menetapkan indikator kinerja pada setiap area proses.
3. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan.
4. menganalisis efektivitas pelaksanaan Keamanan SPBE.
5. mendukung dan merealisasikan program audit Keamanan SPBE.

I. Perbaikan Berkelanjutan

Perbaikan berkelanjutan dilakukan dengan:

1. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE.
2. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BAB III
MANAJEMEN ASET TEKNOLOGI INFORMASI DAN KOMUNIKASI

A. Pendahuluan

1. Latar Belakang

Penyelenggaraan pemerintahan dalam rangka pelayanan publik memerlukan *Good Governance.* Implementasi *Good Governance* akan menjamin transparansi, efisiensi, dan efektivitas penyelenggaraan pemerintahan. Pada sisi lain, penggunaan Teknologi Informasi dan Komunikasi (TIK) oleh institusi pemerintahan sudah dilakukan sejak beberapa dekade lalu, dengan intensitas yang semakin meningkat. Untuk memastikan penggunaan TIK tersebut benar- benar mendukung tujuan penyelenggaraan pemerintahan, dengan memperhatikan efisiensi penggunaan sumber daya dan pengelolaan risiko terkait dengannya, diperlukan *Good Governance* terkait dengan TIK, yang dalam dokumen ini disebut sebagai Manajemen Aset TIK.

Berikut ini adalah analisis atas kondisi sekarang yang menjadi latar belakang perlunya Manajemen Aset TIK Pemerintah Daerah Kabupaten:

a. Perlunya Rencana TIK Pemerintah Daerah Kabupaten yang lebih harmonis, hampir semua Perangkat Daerah memiliki Rencana TIK, tetapi integrasi dan sinkronisasi di level Kabupaten masih lemah.
b. Perlunya pengelolaan yang lebih baik untuk merealisasikan *flagship* Pemerintah Daerah Kabupaten. *Flagship* Pemerintah Daerah Kabupaten yang merupakan inisiatif TIK strategis memerlukan pendekatan yang lebih baik, khususnya dalam hubungan antar lembaga dan hubungan dengan penyedia layanan.
c. Perlunya peningkatan efisiensi dan efektivitas belanja/investasi TIK Diperlukan mekanisme yang memungkinkan menghindari kemungkinan terjadinya redundansi inisiatif TIK, sehingga meningkatkan efisiensi dan efektivitas belanja/investasi TIK Pemerintah Daerah.
d. Perlunya pendekatan yang meningkatkan pencapaian *value* dari implementasi TIK nasional *Value* yang dapat diciptakan dengan implementasi TIK, khususnya yang dapat dirasakan langsung oleh publik.

2. Peruntukan

Panduan Manajemen Aset TIK Pemerintah Daerah Kabupaten diperuntukkan bagi seluruh instansi pemerintah di semua level Kabupaten Panduan Manajemen Aset TIK dalam dokumen ini tidak mengatur pengelolaan TIK di badan usaha milik daerah.

3. Lingkup

Panduan Umum Manajemen Aset TIK Pemerintah Daerah Kabupaten akan digunakan sebagai prinsip dan panduan bagi setiap Perangkat Daerah dalam penggunaan sumber daya TIK di Perangkat Daerah masing-masing, sehingga memenuhi asas: efektivitas, efisiensi, dan akseptabilitas.

4. Tujuan

Tujuan Panduan Umum Manajemen Aset TIK Pemerintah Daerah Kabupaten adalah memberikan batasan dan panduan bagi Perangkat Daerah dan entitas pengambil keputusan di dalamnya dalam pengelolaan sumber daya TIK.

Panduan Umum Manajemen Aset TIK yang dikembangkan ini juga akan menjadi rujukan bagi pihak-pihak di luar Pemerintah Daerah Kabupaten berikut, untuk memberikan pendapat, penilaian maupun Evaluasi atas penyelenggaraan TIK di institusi pemerintahan:

a. Internal Auditor pemerintahan;
b. Komunitas bisnis;
c. Publik.

Aspek-aspek berikut ini diharapkan akan mengalami peningkatan secara signifikan dengan implementasi Panduan Umum Manajemen Aset TIK Pemerintah Daerah:

a. Sinkronisasi dan integrasi Rencana TIK Pemerintah Daerah;
b. Efisiensi belanja TIK Pemerintah Daerah;
c. Realisasi solusi TIK yang sesuai kebutuhan secara efisien;
d. Operasi sistem TIK yang memberikan nilai tambah secara signifikan kepada publik dan internal manajemen pemerintahan.

5. Manfaat

Manfaat penerapan Manajemen Aset TIK di institusi pemerintahan dapat dilihat dalam 3 perspektif: nasional, Pemerintah Daerah Kabupaten, dan publik.

a. Nasional

Untuk level nasional, berikut ini adalah manfaat yang akan dapat dirasakan:

1) Koordinasi dan integrasi Rencana TIK Pemerintah Daerah;
2) Mendapatkan standar rujukan kualitas penyelenggaraan TIK di seluruh institusi pemerintahan; dan
3) Memudahkan monitoring dan Evaluasi penyelenggaraan TIK di seluruh institusi pemerintahan.

b. Pemerintah Daerah Kabupaten

Setiap Perangkat Daerah Kabupaten akan:

1) Mendapatkan batasan dan panduan sesuai *best practice* dalam penyelenggaraan TIK-nya di lingkungan masing-masing;
2) Mengoptimalkan ketercapaian value dari penyelenggaraan TIK di lingkungan kerjanya masing-masing: internal manajemen dan pelayanan publik.

c. Publik

Masyarakat diharapkan mendapat manfaat:

1) Kualitas pelayanan publik yang lebih baik;
2) Transparansi kriteria batasan penyelenggaraan TIK oleh institusi pemerintah, sehingga dapat melakukan fungsi *social control*.

6. Referensi

Dalam penyusunan Panduan Manajemen Aset TIK Pemerintah Daerah Kabupaten ini, tim penyusun menggunakan referensi dari berbagai sumber berikut ini:

a. *COBIT* (*Control Objective for Information and Related Technology*) yang dikeluarkan oleh *ISACA* (*Information System Audit & Control association*) versi 4.1;
b. *ITIL* (*Information Technology Infrastructure Library*);
c. ISO 27000 (*Information Security Management System*);
d. AS 8015-2005 (*Australian Standard on Corporate Governance of Information & Communication Technology*);
e. Riset *CISR MIT* (*Center for Information System Research* – MIT) tentang *IT Governance.*
f. Peraturan Menteri Dalam Negeri Nomor 19 Tahun 2016 Tentang Pedoman Pengelolaan Barang Milik Daerah.

B. Prinsip dan Model

1. Prinsip Dasar

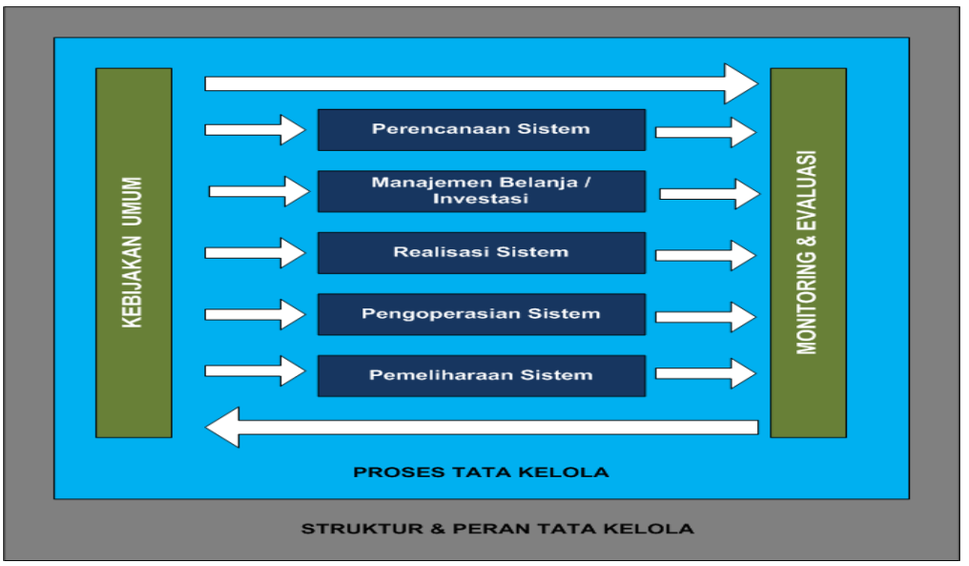
Bagian ini menjelaskan lima prinsip dasar yang menjadi pondasi bangunan Manajemen Aset TIK Pemerintah Daerah Kabupaten. Prinsip ini mendasari model dan tingkat kedalaman implementasi model.

a. Prinsip 1, Perencanaan TIK yang sinergis dan konvergen di level internal Pemerintah Daerah Kabupaten memastikan bahwa setiap inisiatif selalu didasarkan pada rencana yang telah disusun sebelumnya; dan memastikan bahwa rencana-rencana institusi di semua Perangkat Daerah, sinergis dan konvergen dengan rencana nasional.
b. Prinsip 2, Penetapan kepemimpinan dan tanggung jawab TIK yang jelas di level internal Pemerintah Daerah Kabupaten memastikan bahwa setiap Perangkat Daerah memahami dan menerima posisi dan tanggung jawabnya dalam peta TIK Pemerintah Daerah Kabupaten secara umum, dan memastikan bahwa seluruh entitas fungsional di setiap institusi memahami dan menerima perannya dalam pengelolaan TIK di institusinya masing-masing.
c. Prinsip 3, Pengembangan dan/atau akuisi TIK secara valid Memastikan bahwa setiap pengembangan dan/atau akuisisi TIK didasarkan pada alasan yang tepat dan dilakukan dengan cara yang tepat, berdasarkan analisis yang tepat dan terus-menerus. Memastikan bahwa dalam setiap pengembangan dan/atau akuisisi TIK selalu ada pertimbangan keseimbangan yang tepat atas manfaat jangka pendek dan jangka panjang, biaya dan risiko-risiko.
d. Prinsip 4, Memastikan operasi TIK berjalan dengan baik, kapan pun dibutuhkan memastikan kesesuaian TIK dalam mendukung institusi, responsif atas perubahan kebutuhan kegiatan institusi, dan memberikan dukungan kepada kegiatan institusi di semua waktu yang dibutuhkan institusi.
e. Prinsip 5, Memastikan terjadinya perbaikan berkesinambungan (*continuous improvement)* dengan memperhatikan faktor manajem Memastikan bahwa penetapan: tanggung jawab, perencanaan, pengembangan dan/ atau akuisisi, dan operasi TIK selalu dimonitor dan dievaluasi kinerjanya dalam rangka perbaikan

berkesinambugan (*continuous improvement).* Memastikan bahwa siklus perbaikan berkesinambungan (*continuous improvement)* dilakukan dengan memperhatikan manajemen perubahan organisasi dan sumber daya manusia perubahan organisasi dan sumber daya manusia.

2. Model

Model Manajemen Aset TIK Pemerintah Daerah Kabupaten difokuskan pada pengelolaan proses-proses TIK melalui mekanime pengarahan dan monitoring dan Evaluasi. Model keseluruhan Manajemen Aset TIK Pemerintah Daerah Kabupaten adalah sebagai berikut:



a. Struktur dan Peran Manajemen, yaitu entitas apa saja yang berperan dalam pengelolaan proses-proses TIK dan bagaimana pemetaan perannya dalam pengelolaan proses-proses TIK tersebut. Struktur dan peran manajemen ini mendasari seluruh proses manajemen Aset TIK.

b. Proses Manajemen, yaitu proses yang ditujukan untuk memastikan bahwa tujuan utama manajemen dapat tercapai, terkait dengan pencapaian tujuan organisasi, pengelolaan sumber daya, dan Manajemen Risiko.

1) Lingkup Proses Manajemen:

a) Perencanaan Sistem–Proses ini menangani identifikasi kebutuhan organisasi dan formulasi inisiatif-inisiatif TIK apa saja yang dapat memenuhi kebutuhan organisasi tersebut.

b) Manajemen Belanja/Investasi–Proses ini menangani pengelolaan investasi/belanja TIK.

c) Realisasi Sistem–Proses ini menangani pemilihan, penetapan, pengembangan/akuisisi sistem TIK, serta manajemen proyek TIK.

d) Pengoperasian Sistem–Proses ini menangani operasi TIK yang memberikan jaminan tingkat layanan dan keamanan sistem TIK yang dioperasikan.

e) Pemeliharaan Sistem–Proses ini menangani pemeliharaan aset-aset TIK untuk mendukung pengoperasian sistem yang optimal.

2) Mekanisme Proses Manajemen:

a) Kebijakan Umum, Kebijakan umum ditetapkan untuk memberikan tujuan dan batasan atas proses TIK bagaimana sebuah proses TIK dilakukan untuk memenuhi kebijakan yang ditetapkan.

b) Monitoring dan Evaluasi, Monitoring dam Evaluasi ditetapkan untuk memastikan adanya umpan balik atas pengelolaan TIK, yaitu berupa ketercapaian kinerja yang diharapkan. Untuk mendapatkan deskripsi kinerja setiap proses TIK digunakan indikator keberhasilan. Indikator keberhasilan inilah yang akan dapat digunakan oleh manajemen atau Auditor, untuk mengetahui apakah proses TIK telah dilakukan dengan baik.

C. Panduan Umum Struktur Dan Peran Manajemen

1. Struktur Manajemen

Penetapan entitas struktur manajemen ini dimaksudkan untuk memastikan kapasitas kepemimpinan yang memadai, dan hubungan antar Perangkat Daerah yang sinergis dalam perencanaan, penganggaran, realisasi sistem TIK, operasi sistem TIK, dan Evaluasi secara umum implementasi TIK di pemerintah Daerah kabupaten.Entitas struktur manajemen TIK:

a. Bupati.
b. Tim pengarah SPBE;
c. Tim Koordinasi SPBE;
d. Satuan Kerja Pengelola TIK Pemerintah Daerah Kabupaten yaitu Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang komunikasi dan informatika.
e. Satuan Pemilik Proses Bisnis yaitu satuan kerja Perangkat Daerah di luar satuan kerja pengelola TIK Pemerintah Daerah Kabupaten sebagai pemilik Proses Bisnis *(Business Process Owner).*

2. Deskripsi Peran

Deskripsi peran yang diuraikan di sini adalah peran yang mempunyai kaitan langsung dengan mekanisme manajemen Aset TIK Pemerintah Daerah Kabupaten.

a. Bupati:
   1) bertanggung jawab atas seluruh implementasi TIK Pemerintah Daerah Kabupaten; dan
   2) bertanggung jawab atas arahan strategis dan Evaluasi keseluruhan dari inisiatif TIK Pemerintah Daerah Kabupaten.
b. Tim Pengarah SPBE:
   1) mengoordinasikan perencanaan dan pelaksanaan inisiatif dan portofolio TIK Pemerintah Daerah Kabupaten; dan
   2) melakukan *review* berkala atas pelaksanaan implementasi TIK Pemerintah Daerah Kabupaten.

c. Tim Koordinasi SPBE:
   1) mensinergiskan dan mengintegrasikan Rencana TIK Pemerintah Daerah Kabupaten yang mengakomodir kepentingan seluruh Perangkat daerah Kabupaten;
   2) mensinergiskan rencana belanja/investasi Perangkat daerah Kabupaten untuk memastikan tidak adanya tumpang tindih (*redundancy*) inisiatif TIK; dan
   3) melakukan *review* atas Evaluasi berkala implementasi TIK yang dilakukan oleh Tim Pengarah SPBE, untuk memastikan keselarasan dengan rencana semula.

d. Satuan Kerja Pengelola TIK Pemerintah Daerah Kabupaten:
   1) bertanggung jawab atas implementasi sistem TIK, sesuai dengan spesifikasi kebutuhan yang diberikan oleh Satuan Kerja Pemilik Proses Bisnis; dan
   2) bertanggung jawab atas keberlangsungan dan kualitas aspek teknis sistem TIK dalam tahap operasional;
   3) bertanggung jawab atas pemeliharaan aset TIK Pemerintah Daerah Kabupaten.

e. Satuan Kerja Pemilik Proses Bisnis Institusi
   1) bertanggung jawab atas pendefinisian kebutuhan (*requirements*) dalam implementasi inisiatif TIK; dan
   2) memberikan masukan atas implementasi TIK, khususnya kualitas operasional sistem TIK.

D. Panduan Umum Proses Manajemen
   1. Kebijakan Umum
      a. Definisi

         Kebijakan umum merupakan pernyataan yang akan menjadi arahan dan batasan bagi setiap proses manajemen. Kebijakan ini berlaku untuk seluruh proses manajemen.

      b. Lingkup
         1) Keselarasan Strategis: Organisasi – TIK
            a) Arsitektur dan inisiatif TIK harus selaras dengan visi dan tujuan organisasi.
            b) Keselarasan strategis antara organisasi TIK dicapai melalui mekanisme berikut:
               - Keselarasan tujuan organisasi dengan tujuan TIK, dimana setiap tujuan TIK harus mempunyai referensi tujuan organisasi.
               - Keselarasan arsitektur bisnis organisasi dengan arsitektur TIK (arsitektur informasi, arsitektur aplikasi, dan arsitektur infrastruktur).
               - Keselarasan eksekusi inisiatif TIK dengan rencana strategis.
         2) Manajemen Risiko
            a) Risiko-risiko prioritas dalam pengelolaan TIK oleh Pemerintah daerah Kabupaten mencakup:
               - Risiko atas proyek mencakup kemungkinan tertundanya penyelesaian proyek TIK, biaya yang melebihi dari perkiraan atau hasil akhir

(*deliverables)* proyek tidak sesuai dengan spesifikasi yang telah ditentukan di awal.
- Risiko atas informasi mencakup akses yang tidak berhak atas Aset Informasi, pengubahan informasi oleh pihak yang tidak berhak dan penggunaan informasi oleh pihak yang tidak punya hak untuk keperluan yang tidak sebagaimana mestinya.
- Risiko atas keberlangsungan layanan mencakup kemungkinan terganggunya ketersediaan (*availabilitas)* layanan TIK atau layanan TIK.

b) Kontrol atas risiko proyek, risiko atas informasi, dan risiko atas keberlangsungan layanan secara umum mencakup:
- Implementasi *Project Governance* untuk setiap proyek TIK yang diimplementasikan oleh seluruh Perangkat daerah Kabupaten.
- Implementasi *Security Governance* di manajemen Aset TIK dan seluruh sistem TIK yang berjalan, khususnya untuk meminimalkan risiko atas informasi dan keberlangsungan layanan.

3) Manajemen Sumber daya

a) Manajemen sumber daya dalam Manajemen Aset TIK ditujukan untuk mencapai efisiensi dan efektivitas penggunaan sumber daya TIK, yang melingkupi sumber daya: finansial, informasi, teknologi, dan SDM.

b) Ketercapaian efisiensi finansial dicapai melalui:
- Pemilihan sumber-sumber dana yang tidak memberatkan untuk pengadaan TIK.
- Kelayakan belanja TIK secara finansial harus bisa diukur secara rasional dengan menggunakan metoda-metoda penganggaran modal (*capital budgeting*).
- Dijalaninya prosedur pengadaan yang efisien dengan fokus tetapnpada kualitas produk dan jasa TIK.
- Prioritas anggaran diberikan untuk proyek TIK yang bermanfaat untuk banyak pihak, berbiaya rendah, dan cepat dirasakan manfaatnya.
- Perhitungan manfaat dan biaya harus memasukkan unsur yang bersifat kasat mata (*tangible*) dan terukur maupun yang tidak tampak (*intangible*) dan relatif tidak mudah diukur.
- Efisiensi finansial harus mempertimbangkan biaya kepemilikan total (*Total Cost of Ownership* – TCO) yang bisa meliputi harga barang/jasa yang dibeli, biaya pelatihan karyawan, biaya perawatan (*maintenance cost*), biaya langganan (*subscription/license fee*), dan biaya-biaya yang terkait dengan pemerolehan barang/jasa yang dibeli.
- Efisiensi finansial bisa mempertimbangkan antara keputusan membeli atau membuat sendiri sumber daya TIK. Selain itu juga bisa mempertimbangkan antara sewa/*outsourcing*

dengan memiliki sumber daya TIK baik dengan membuat sendiri maupun membeli.

c) Ketercapaian efisiensi dan efektivitas sumber daya informasi di Pemerintah Daerah Kabupaten dicapai melalui:
   - Penyusunan arsitektur informasi yang mencerminkan kebutuhan informasi, struktur informasi dan pemetaan hak akses atas informasi oleh peran-peran yang ada dalam manajemen organisasi.
   - Identifikasi kebutuhan perangkat lunak aplikasi yang sesuai dengan spesifikasi arsitektur informasi, yang memungkinkan informasi diolah dan disampaikan kepada peran yang tepat secara efisien.

d) Efisiensi penggunaan teknologi (mencakup: platform aplikasi, *software* sistem, infrastruktur pemrosesan informasi, dan infrastruktur jaringan komunikasi) dicapai melalui konsep "mekanisme *shared service"* (baik di internal institusi pemerintahan atau antarinstitusi pemerintahan) yang meliputi:
   - Aplikasi, yaitu *software* aplikasi yang secara arsitektur teknis dapat di-*share* penggunaannya karena kesamaan kebutuhan fitur fungsionalitas.
   - Perbedaan hanya sebatas di aspek konten informasi Infrastruktur komunikasi.
   - Jaringan komputer/komunikasi, koneksi internet Data, yaitu keseluruhan Data yang menjadi konten informasi. Pengelolaan Data dilakukan dengan sistem *Data Center/Disaster Recovery Center* (DC/DRC).

2. Monitoring Dan Evaluasi

a. Definisi

Untuk memastikan adanya perbaikan berkesinambungan (*continuous improvement*), mekanisme monitoring dan Evaluasi akan memberikan umpan balik atas seluruh proses manajemen. Panduan umum monitoring dan Evaluasi memberikan arahan tentang objek dan mekanisme monitoring dan Evaluasi.

b. Lingkup

1) Objek Monitoring dan Evaluasi

Ketercapaian indikator keberhasilan untuk setiap proses tata kelola merupakan objek utama dari aktivitas monitoring dan Evaluasi. Indikator keberhasilan mencerminkan sejauh mana tujuan akhir dari setiap proses tata kelola telah tercapai. Indikator kinerja proses dapat digunakan untuk melakukan penelusuran balik atas ketercapaian sebuah indikator keberhasilan.

2) Mekanisme Monitoring dan Evaluasi

Secara internal, Pemerintah Daerah Kabupaten melakukan Evaluasi berupa peninjauan secara reguler atas ketercapaian indikator keberhasilan untuk setiap proses manajemen:

a) Intensitas peninjauan indikator keberhasilan, paling sedikit (satu) kali untuk setiap tahunnya.

b) Setiap siklus peninjauan indikator keberhasilan harus didokumentasikan dan tindak lanjut atas rekomendasi dimonitor secara reguler oleh manajemen.
c) Kerjasama dengan pihak ketiga dimungkinkan untuk pelaksanaan Evaluasi secara internal, karena keterbatasan keahlian dan SDM, dengan spesifikasi kebutuhan detail tetap berasal dari institusi pemerintahan terkait.

3) Secara eksternal, dimungkinkan diadakannya Evaluasi atas ketercapaian indikator keberhasilan sebuah institusi pemerintahan.
a) Inisiatif Evaluasi eksternal berasal dari pihak di Pemerintah Daerah Kabupaten.
b) Tujuan utama Evaluasi secara eksternal adalah mengetahui ketercapaian tujuan manajemen Aset TIK, dengan sudut pandang indikator keberhasilan yang relatif seragam.
c) Kerjasama dengan pihak ketiga dimungkinkan untuk pelaksanaan Evaluasi secara eksternal, karena keterbatasan keahlian dan SDM, dengan spesifikasi kebutuhan detail tetap berasal dari institusi pemerintahan terkait.

3. Proses Perencanaan Sistem
a. Definisi
Perencanaan Sistem merupakan proses yang ditujukan untuk menetapkan visi, arsitektur TIK dalam hubungannya dengan kebutuhan organisasi dan rencana realisasi atas implementasi visi dan arsitektur TIK tersebut. Rencana TIK yang telah disusun akan menjadi referensi bersama bagi seluruh satuan kerja dalam sebuah institusi atau referensi bersama beberapa institusi yang ingin mensinergiskan inisiatif TIK-nya.
b. Lingkup
1) Sinkronisasi dan Integrasi.
a) Sinkronisasi dan integrasi perencanaan sistem dilakukan sejak di level Pemerintah daerah Kabupaten maupun hubungan dengan instansi pemerintah lain.
b) Tim Koordinasi SPBE memberikan persetujuan akhir atas Rencana Induk TIK lima tahunan Pemerintah daerah Kabupaten, yang kemudian akan disahkan oleh Bupati.
c) Dalam penyusunan Rencana Induk TIK lima tahunan Pemerintah daerah Kabupaten dapat meminta masukan kepada Dewan TIK Nasional.
2) Siklus dan Lingkup Perencanaan.
a) Pemerintah Daerah Kabupaten memiliki Rencana Induk TIK lima tahunan yang akan menjadi dasar dalam pelaksanaan inisiatif TIK tahunan, dengan memperhatikan keselarasan dengan Rencana *Flagship* TIK Nasional.
b) Pemerintah Daerah Kabupaten minimal memiliki perencanaan atas komponen berikut ini:

- Arsitektur Informasi, yaitu model informasi organisasi yang mendefinisikan lingkup kebutuhan informasi yang dipetakan ke dalam Proses Bisnis organisasi terkait.
- Arsitektur Aplikasi, yaitu model aplikasi organisasi yang mendefinisikan lingkup aplikasi beserta persyaratan dan spesifikasi desain apa saja yang dibutuhkan oleh organisasi untuk mengakomodasi seluruh level Proses Bisnis organisasi seperti: transaksional, operasional, pelaporan, analisa, monitoring dan perencanaan.
- Arsitektur Infrastruktur Teknologi, yaitu: topologi, konfigurasi, dan spesifikasi infrastruktur teknologi beserta pendekatan siklus hidupnya untuk memastikan infrastruktur teknologi yang digunakan organisasi selalu sesuai dengan kebutuhan.
- Organisasi dan Manajemen, yaitu struktur organisasi dan deskripsi peran, serta kebijakan dan prosedur untuk menjalankan seluruh proses dalam manajemen Aset TIK.
- Pendekatan dan *Roadmap* Implementasi, yaitu pola pendekatan yang digunakan untuk memastikan implementasi seluruh arsitektur beserta organisasi dan manajemen, didukung oleh *roadmap* implementasi yang mendeskripsikan tahapan-tahapan target implementasi dalam sebuah durasi waktu tertentu.

c) Tim Koordinasi SPBE dapat melakukan *review* kekinian dan kesesuaian Rencana Induk TIK Pemerintah Daerah Kabupaten secara reguler.

3) Perencanaan Arsitektur Informasi

a) Tujuan yang ingin dicapai dengan perencanaan arsitektur informasi adalah tersedianya satu referensi model informasi organisasi, yang akan menjadi rujukan seluruh desain *software* aplikasi di tahap selanjutnya, dalam rangka mengurangi tingkat redundansi informasi.

b) Arsitektur informasi mencakup informasi terstruktur (data mart, database, database tabel, pertukaran Data) dan informasi tidak terstruktur (gambar, video, file dokumen, dsb).

c) Penetapan arsitektur informasi mencakup penetapan klasifikasi ke dalam kelas-kelas Data, pemetaan kepemilikan Data, dan pendefinisian data dictionary, dan syntax rules.

d) Arsitektur informasi juga menetapkan klasifikasi level keamanan Data untuk setiap klasifikasi kelas Data melalui penetapan kriteria yang tepat sesuai dengan kebutuhan organisasi.

4) Perencanaan Arsitektur Aplikasi
   a) Tujuan yang ingin dicapai dengan perencanaan arsitektur aplikasi adalah terealisasinya dukungan atas Proses Bisnis dimana setiap aplikasi selalu akan berkorelasi terhadap sebuah proses bisnis tertentu yang didukungnya.
   b) Arsitektur aplikasi memberikan peta tentang aplikasi apa saja yang dibutuhkan sesuai dengan karakteristik konteks organisasi dan manajemen. Secara umum kategorisasi dapat dilakukan atas:
      - Pelayanan Publik, merupakan aplikasi yang dikhususkan untuk memberikan pelayanan kepada warga dan komunitas bisnis, baik layanan informasi, komunikasi maupun transaksi.
      - Manajemen Internal, merupakan aplikasi yang dikhususkan untuk mengelola Proses Bisnis standar manajemen seperti keuangan, kepegawaian, pengelolaan aset, pengelolaan program kerja, monitoring kinerja, dan sejenisnya.
      - Pendukung Manajemen, merupakan aplikasi yang sifatnya mendukung operasional manajemen sehingga proses- Proses Bisnis standar manajemen dan pelayanan kepada publik dapat optimal, mencakup di antaranya fungsional informasi, komunikasi dan kolaborasi.
      - *Datawarehouse* & *Business Intelligence*, merupakan aplikasi yang digunakan untuk mengelola laporan dan fasilitas analisa Data multidimensional.
   c) Efisiensi arsitektur teknis aplikasi ditempuh melalui pendekatan *"One Stop Window"* untuk setiap tipe pelanggan institusi pemerintah, terutama publik dan bisnis. Melalui pendekatan ini, publik hanya perlu mengakses satu sistem (menggunakan beragam *delivery channel)* untuk mendapatkan layanan TIK. Pendekatan ini terutama diimplementasikan untuk implementasi *e-government* di Daerah.
5) Perencanaan Arsitektur Infrastruktur Teknologi
   a) Infrastruktur teknologi mencakup jaringan komunikasi, perangkat pemrosesan informasi (*server*, *workstation* dan *peripheral* pendukungnya), *software system* (sistem operasi, *database* RDBMS), dan media penyimpanan Data.
   b) Perencanaan arsitektur infrastruktur teknologi diharapkan dapat mengutamakan mekanisme *shared-services*, fokus ini ditujukan untuk meningkatkan efisiensi belanja TIK. Mekanisme *Shared-Services* arsitektur teknis diimplementasikan atas aspek-aspek sumberdaya.

c) Infrastruktur komunikasi: jaringan komputer/komunikasi, koneksi internet.Infrastruktur penyimpanan Data *(Data Center)* dan/atau DRC *(Disaster Recovery Center).*

6) Perencanaan Manajemen dan Organisasi
   a) Perencanaan organisasi mencakup identifikasi struktur organisasi pengelola yang akan melakukan operasional harian.
   b) Perencanaan manajemen mencakup pendefinisian prosedur teknis dengan prioritas pada domain:
      - Realisasi Sistem
      - Operasi Sistem
      - Pemeliharaan Sistem
7) Perencanaan Pendekatan dan *Roadmap* Implementasi
   a) Setiap perencanaan sistem menyertakan skenario *Project Governance* untuk setiap proyek inisiatif TIK yang direncanakan, untuk memastikan proyek-proyek inisiatif TIK dapat diselesaikan tepat waktu, tepat sasaran, dan tepat anggaran.
   b) Setiap inisiatif yang direncanakan selalu menyertakan proyeksi waktu, kapan benefit yang diharapkan dapat terealisasi (benefit realization schedule).
   c) Setiap perencanaan sistem mempunyai roadmap implementasi yang didasarkan pada analisa kesenjangan arsitektur (informasi, aplikasi dan infrastruktur teknologi) serta kesenjangan manajemen dan organisasi.
   d) Roadmap implementasi terdiri dari portofolio program implementasi (yang dapat terdiri dari beberapa portofolio proyek untuk setiap programnya), penetapan peringkat prioritas portofolio proyek, dan pemetaan dalam domain waktu sesuai dengan durasi waktu yang ditargetkan.
   e) Penetapan peringkat prioritas portofolio proyek inisiatif TIK dilakukan setidaknya berdasarkan faktor level anggaran yang dibutuhkan, kompleksitas sistem, dan besar usaha yang diperlukan.
8) Indikator Keberhasilan
   a) Keselarasan Strategis
      - Tingkat konsistensi dengan Rencana TIK Nasional.
      - Tingkat kontribusi tujuan TIK dalam mendukung tujuan organisasi secara umum, dalam perspektif desain.
      - Tingkat kepuasan *stakeholders* atas Rencana TIK yang sudah disusun, dalam perspektif akomodasi kepentingan.
      - Tingkat kesesuaian proyek-proyek TIK yang sudah/sedang berjalan dibandingkan dengan yang direncanakan, kesahihan dasar pengambilan keputusan jika terjadi deviasi khususnya untuk proyek-proyek TIK yang kritikal/strategis.

b) Efisiensi Arsitektur Teknis
Penurunan tingkat redundansi sistem akibat kurang optimalnya implementasi mekanisme *shared-services* arsitektur teknis.

c. Mekanisme perencanaan
1) Perangkat Daerah Kabupaten mengusulkan kebutuhan aset TIK dalam Rencana Kebutuhan Barang Milik Daerah (pengadaan dan pemeliharaan).
2) Dalam menyusun kebutuhan aset TIK sebagaimana dimaksud pada huruf a memperhatikan standar barang dan standar kebutuhan serta dikonsultasikan kepada unit kerja Urusan Bidang Komunikasi dan Informatika.
3) Perangkat daerah Kabupaten yang menyelenggarakan fungsi penunjang urusan pemerintahan menyusun kebutuhan aset TIK dalam Rencana Kebutuhan Barang Milik Daerah (pengadaan dan pemeliharaan) berdasarkan ketentuan Peraturan Perundang-undagan di bidang pengelolaan barang milik daerah.

4. Manajemen Belanja
a. Definisi
Manajemen Belanja/Investasi TIK merupakan proses pengelolaan anggaran untuk keperluan belanja/investasi TIK, sesuai dengan mekanisme proyek inisiatif TIK yang telah ditetapkan sebelumnya dalam Portotolio Proyek Inisiatif TIK dan Roadmap Implementasi. Realisasi belanja/investasi ini dilakukan melalui mekanisme penganggaran tahunan.

b. Lingkup
1) Cakupan Tipe Belanja/Investasi
Seluruh tipe belanja/investasi TIK yang mempunyai hubungan konsekuensi langsung dengan anggaran (termasuk juga pinjaman atau hibah, jika mempunyai konsekuensi langsung dengan anggaran), menggunakan referensi panduan umum dalam dokumen ini.
2) Sinkronisasi dan Integrasi
a) Pengelolaan belanja/investasi TIK dilakukan melalui mekanisme penyusunan Rencana Kegiatan dan Anggaran SKPD sesuai ketentuan Peraturan Perundang-undangan.
b) Tim Kooordinasi SPBE melakukan *review* dan persetujuan atas Rencana Kegiatan dan Anggaran TIK yang diajukan oleh Satuan Kerja Pengelola TIK atau Satuan Kerja Pemilik Proses Bisnis. *Review* dan persetujuan ini ditujukan untuk memastikan tidak adanya redundansi proyek TIK di tiap Perangkat Daerah kabupaten.

c. Pemilihan Mekanisme Penganggaran
1) Tipe Mekanisme Penganggaran
a) Pengeluaran Operasi (*Operational Expenditure* = *OpEx*).
Pengeluaran Operasi (*OpEx*) TIK adalah pengeluaran TIK dalam rangka menjaga tingkat dan kualitas layanan. Yang bisa dimasukkan dalam kriteria OpEx adalah

antara lain biaya gaji & lembur, biaya sewa alat, biaya overhead, ATK dan lain-lain.

b) Pengeluaran Modal (*Capital Expenditure* = *CapEx*).
Pengeluaran modal (*CapEx*) TIK adalah investasi dalam bentuk aset/ infrastruktur TIK yang diperlukan untuk memberikan, memperluas dan/atau meningkatkan kualitas layanan publik. Nilai buku aset akan disusut (depresiasi) selama umur ekonomisnya yang wajar (kecuali tanah). Yang termasuk *CapEx* antara lain: pembangunan/pembelian jaringan, *server* & PC, perangkat lunak, bangunan, dan tanah.

2) Kriteria Pemilihan Mekanisme Penganggaran

a) Beberapa faktor yang bisa dipertimbangkan dalam pemilihan pola penganggaran CapEx dan OpEx dijelaskan di bawah. Perlu diperhatikan bahwa tidak ada rumus tunggal (*one size fit all*) dalam penentuan pola tersebut sehingga diharapkan institusi mempertimbangkan semua factor secara komprehensif.

- Umur ekonomis sumber daya TIK
  Pengeluaran TIK yang mempunyai umur ekonomis lebih dari satu tahun bisa dipertimbangkan untuk menggunakan CapEx.
- Ketersediaan anggaran
  Jika institusi mempunyai anggaran TIK yang terbatas sebaiknya menggunakan pola OpEx (misal sewa atau *outsourcing*) karena cenderung lebih murah dibanding beli atau buat sendiri.
- Tingkat kecepatan keusangan (*obsoleteness*)
  Untuk teknologi yang cepat usang dengan tingkat kembalian yang yang tidak jelas atau berjangka panjang maka sebaiknya menggunakan pola OpEx.
- Nilai strategis TIK
  Sumber daya TIK yang bernilai strategis tinggi (kerahasiaan, nilai ekonomi, kedaulatan negara, dan hal lain yang sejenis) sebaiknya menggunakan pola CapEx.
- Karakteristik Proyek (skala, risiko, dll)
  Proyek TIK dengan skala (*magnitude*) besar biasanya juga punya risiko besar Risiko yang besar bisa diminimalkan dengan menggunakan pola OpEx. Dengan OpEx, biaya dan risiko menjadi lebih terukur (bulanan atau tahunan).
- Urgensi
  Sumber daya TIK yang dibutuhkan ketersediaannya dalam waktu singkat bisa menggunakan OpEx, misal dengan cara sewa atau *outsourcing*.
- Ketersediaan Pemasok
  Keberadaan pemasok (*vendor*) menjadi hal yang harus dipertimbangkan karena CapEx atau OpEx bisa tergantung dari ada tidaknya pemasok (*vendor*).
- Ketersediaan Sumber Daya

Sumber daya manusia TIK yang ada di dalam institusi bisa menentukan pola yang akan digunakan. Jika institusi tidak memiliki SDM TIK yang memadai maka OpEx (sewa atau *outsourcing*) bisa jadi pilihan.

- *Capital Budgeting*
  Pembuatan keputusan belanja/investasi TIK sebaiknya menggunakan perhitungan *capital budgeting* antara lain, *Internal Rate of Return* (IRR), *Net Present Value* (NPV), *Payback Period, Cost-Benefit Ratio*, dan *Return on Investment* (RoI).
- Visi dan Misi Pemerintah Daerah Kabupaten.
  Keputusan belanja/investasi TIK bisa sangat dipengaruhi oleh visi dan misi Pemerintah Daerah Kabupaten. Sebelum membuat keputusan belanja/investasi TIK sebaiknya merujuk ke visi dan misi Pemerintah Daerah Kabupaten untuk mengevaluasi relevansinya.

d. Indikator Keberhasilan
   1) Digunakannya sumber-sumber pendanaan yang efisien.
   2) Kesesuaian realisasi penyerapan anggaran TIK dengan realisasi pekerjaan yang direncanakan.
   3) Diperolehnya sumber daya TIK yang berkualitas dengan melalui proses belanja/investasi TIK yang efisien, cepat, bersih dan transparan.

5. Proses Realisasi Sistem
   a. Definisi

Realisasi sistem TIK merupakan proses yang ditujukan untuk mengimplementasikan perencanaan TIK, mulai dari pemilihan sistem TIK sampai dengan Evaluasi pasca implementasi.

   b. Lingkup
      1) Identifikasi dan Pemilihan Alternatif Sistem
         a) Identifikasi dan Pemilihan Alternatif Sistem
            - Pemilihan alternatif sistem atau proses pemilihan sistem dari alternatif sistem yang telah ada, dilakukan menggunakan referensi hasil studi kelayakan.
            - Manajemen Aset TIK melakukan studi kelayakan yang setidaknya terdiri dari aktivitas.
            - Untuk sistem TIK berskala besar, strategis, dan berpotensi mempengaruhi sistem-sistem TIK sebelumnya, pemilihan alternatif sistem TIK dapat dilakukan melalui mekanisme *Proof of Concept* (POC).
            - Pelaksanaan pemilihan sistem dari alternatif yang ada berdasarkan Peraturan Perundang-undangan tentang Pengadaan Barang dan Jasa.
         b) Realisasi *software* Aplikasi
            - Pengembangan dan/atau pengadaan (akuisisi) *software* aplikasi dilakukan berdasarkan metodologi *System Development Life Cycle (*SDLC*)*

yang dipergunakan secara luas oleh industri *software*, yang minimal mencakup kebutuhan akan:

- Penerjemahan kebutuhan/persyaratan bisnis ke dalam spesifikasi desain
- Penyusunan desain detail dan teknikal perangkat lunak aplikasi, termasuk juga di sini pengendalian aplikasi (*application control*) (yang memungkinkan setiap pemrosesan dalam perangkat lunak apliasi akurat, lengkap, tepat waktu, terotorisasi dan dapat diaudit) dan pengendalian keamanan aplikasi (*application security control*) (yang memungkinkan terpenuhinya aspek: kerahasiaan (*confidentiality*), ketersediaan (*availability*), dan integritas (*integrity*).
- Implementasi desain detail dan teknikal ke dalam kode program (*coding*).
- Manajemen perubahan persyaratan/kebutuhan.
- Pelaksanaan penjaminan mutu (*quality assurance*).
- Uji coba (*testing*): *unit testing, system testing, integration testing, user acceptance test* (UAT).
- Instalasi dan akreditasi.

o Metoda *SDLC* juga diimplementasikan atas upgrade atas *software* aplikasi yang ada (*eksisting*) bersifat utama (*mayor),* yang menghasilkan perubahan signifikan atas desain dan fungsionalitas yang ada (*eksisting*).

o Setiap *software* aplikasi yang direalisasikan harus disertai dengan *training* dan/atau transfer pengetahuan kepada pengguna dan administrator sistem.

o Setiap *software* aplikasi yang direalisasikan harus disertai oleh dokumentasi berikut ini:

- Dokumentasi hasil aktivitas tahapan-tahapan dalam SDLC.
- Manual Pengguna, Operasi, Dukungan Teknis dan Administrasi.
- Materi transfer pengetahuan & Materi *Training*.

c) Realisasi Infrastruktur Teknologi

o Teknologi infrastruktur mencakup perangkat keras pemrosesan informasi (*server, workstation,* dan *peripheral*), jaringan komunikasi dan *software* infrastruktur (sistem operasi, *tool* sistem).

o Pertimbangan kapasitas infrastruktur teknologi disesuaikan dengan kebutuhan, sehingga setiap realisasi infrastruktur teknologi selalu disertai sebelumnya dengan analisis kebutuhan kapasitas.

o Setiap realisasi infrastruktur teknologi selalu memperhatikan kontrol terkait dengan faktor keamanan dan *auditability* (memungkinkan audit atas kinerja dan

sejarah transaksi yang dilakukan), dengan tingkat kedalaman spesifikasi disesuaikan dengan kebutuhan manajemen.
- Tahapan *testing* selalu dilakukan sebelum masuk tahapan operasional, yang dilakukan di lingkungan terpisah *(environment test)* jika memungkinkan.

d) Realisasi Pengelolaan Data
- Setiap langkah pengelolaan Data harus memperhatikan tahapan: *input*, proses, dan *output* Data.
- Pada tahapan *input*, prosedur yang harus dijalankan adalah: prosedur akses Data, prosedur transaksi Data untuk memeriksa akurasi, kelengkapan, dan validitasnya, serta prosedur pencegahan kesalahan *input* Data.
- Pada tahapan proses, prosedur yang harus dijalankan adalah: prosedur pengolahan Data, prosedur validasi dan *editing*, serta prosedur penanganan kesalahan.
- Pada tahapan *output*, prosedur yang harus dijalankan adalah: Prosedur distribusi, penanganan kesalahan, dan keamanan Data.

c. Indikator Keberhasilan
a. Peningkatan jumlah realisasi sistem yang tidak mengalami *backlog* (tertunda dan mendesak untuk segera diselesaikan).
b. Persentase realisasi sistem yang disetujui oleh pemilik Proses Bisnis dan manajemen Aset TIK
c. Jumlah realisasi *software* aplikasi yang diselesaikan tepat waktu, sesuai spesifikasi dan selaras dengan arsitektur TIK.
d. Jumlah realisasi *software* aplikasi tanpa permasalahan integrasi selama implementasi.
e. Jumlah realisasi *software* aplikasi yang konsisten dengan perencanaan TIK yang telah disetujui.
f. Jumlah *software* aplikasi yang didukung dokumentasi memadai dari yang seharusnya.
g. Jumlah implementasi *software* aplikasi yang terlaksana tepat waktu.
h. Penurunan jumlah *downtime* infrastruktur.

6. Proses Pengadaan Aset TIK

Proses pengadaan Aset TIK dilaksanakan berdasarkan ketentuan Peraturan Perundang-undangan tentang Pengadaan Barang/Jasa Pemerintah.

7. Proses Pengoperasian Sistem
a. Definisi

Operasi sistem merupakan proses penyampaian layanan TIK, sebagai bagian dari dukungannya kepada Proses Bisnis manajemen, kepada pihak-pihak yang membutuhkan sesuai spesifikasi minimal yang telah ditentukan sebelumnya.

b. Lingkup

1) Manajemen Tingkat Layanan

a) Manajemen TIK bertanggung jawab atas penyusunan dan update katalog layanan TIK, yang berisi sistem yang beroperasi dan layanan-layanan TIK yang menyusunnya.

b) Diprioritaskan bagi layanan-layanan TIK kritikal yang menyusun sebuah operasi sistem TIK harus memenuhi *Service Level Agreement (SLA*) yang ditetapkan sebagai sebuah *requirement* (persyaratan) oleh pemilik Proses Bisnis dan disetujui oleh manajemen Aset TIK

c) Aspek minimal yang harus tercakup dalam setiap *Service Level Agreement* (*SLA*) layanan TIK kritikal tersebut mencakup:

- Waktu yang diperlukan untuk setiap layanan TIK yang diterima oleh konsumen.
- Prosentase tingkat ketersediaan (*availability*) sistem TIK.
- Waktu yang diperlukan untuk penyelesaian pengaduan insiden atau permasalahan dengan beberapa tingkatan kritikal sesuai dengan kebutuhan.
- Pencapaian SLA-SLA tersebut dilaporkan secara reguler oleh manajemen Aset TIK kepada Komite TIK untuk di-*review*.

2) Keamanan dan Keberlangsungan Sistem

a) Setiap operasi sistem TIK harus memperhatikan persyaratan minimal aspek keamanan sistem dan keberlangsungan sistem, terutama sistem TIK yang memfasilitasi layanan-layanan kritikal

b) Aspek keamanan dan keberlangsungan sistem minimal yang harus terpenuhi mencakup hal-hal berikut ini:

- Untuk pengamanan dari sisi *software* aplikasi dapat diimplementasikan komponen standar sebagai berikut:
- Untuk pengamanan dari sisi infrastruktur teknologi dapat diimplementasikan komponen standar.
- Untuk sistem kritikal dengan SLA yang ketat, dapat ditempuh melalui penyediaan sistem cadangan yang dapat secara cepat mengambil alih sistem utama jika terjadi gangguan *ketersediaan (availability)* pada sistem utama.
- *Assessment* kerentanan keamanan sistem *(security vulnerability system)* secara teratur sesuai dengan kebutuhan.
- Penyusunan *IT Contingency Plan* khususnya yang terkait dengan proses- Proses Bisnis kritikal, yang diuji validitasnya secara teratur sesuai dengan kebutuhan.

3) Manajemen *software* Aplikasi
   a) Setiap *software* aplikasi harus selalu menyertakan prosedur *backup* dan *restore*, dan juga mengimplementasikan fungsionalitasnya di dalam *software* aplikasi.
   b) Setiap pengoperasian *software* aplikasi harus disertai oleh dokumentasi berikut ini:
      - Dokumentasi hasil aktivitas tahapan-tahapan dalam *System Development Life Cycle (SDLC)*
      - Manual Pengguna, Operasi, Dukungan Teknis dan Administrasi
      - Materi transfer pengetahuan & Materi *Training*.

4) Manajemen Infrastruktur
   Setiap pengoperasian infrastruktur teknologi selalu memperhatikan kontrol yang terkait dengan faktor keamanan dan *auditability* (memungkinkan audit atas kinerja dan sejarah transaksi yang dilakukan).

5) Manajemen Data
   a) Data dari setiap *software* aplikasi secara kumulatif juga di *backup* secara terpusat dalam media penyimpanan Data (*data storage*), terutama *software- software* aplikasi kritikal.
   b) *Backup* Data dilakukan secara reguler, dengan frekuensi dan jenis *backup* disesuaikan dengan tingkat kritikal sistem.
   c) Dilakukan pengujian secara teratur mekanisme *backup* dan *restore* Data, untuk memastikan integritas dan validitas prosedur.
   d) Implementasi mekanisme inventori atas media-media penyimpanan Data, terutama media-media yang *off-line*.

6) Manajemen Layanan oleh Pihak Ketiga
   a) Layanan TIK dapat diselenggarakan sebagian atau seluruhnya oleh pihak ketiga, dengan mempertimbangkan faktor-faktor berikut ini:
      - Sumber daya internal yang dimiliki oleh institusi pemerintah terkait kurang memungkinkan, untuk mencapai tingkat layanan minimal yang diberikan kepada konsumen (publik atau bisnis).
      - Seluruh Data yang diolah melalui layanan pihak ketiga adalah Data milik institusi pemerintahan terkait, dan pihak ketiga harus menjaga.
   b) Seluruh layanan TIK yang diselenggarakan oleh pihak ketiga harus mematuhi ketentuan-ketentuan operasi sistem yang telah dijelaskan sebelumnya.
   c) Secara reguler pihak ketiga penyelenggara layanan TIK harus memberikan laporan atas tingkat kepatuhan terhadap ketentuan- ketentuan operasi sistem di atas.

d) Pihak institusi pemerintahan yang layanannya diselenggarakan oleh pihak ketiga terkait secara reguler dan insidental dapat melakukan audit atas laporan yang disampaikan oleh pihak ketiga untuk memastikan validitasnya, baik dilakukan secara internal atau menggunakan jasa pihak ketiga lain yang independen.

c. Indikator Keberhasilan

1) Terkait dengan manajemen tingkat layanan
Prosentase operasi sistem kritikal yang layanan-layanan TIK-nya disertai dengan SLA.
2) Terkait dengan keamanan dan keberlangsungan sistem
Prosentase layanan TIK yang memenuhi SLA.
3) Terkait dengan manajemen *software* aplikasi
   a) Tingkat kepatuhan sistem terhadap kriteria minimum yang telah ditetapkan
   b) Penurunan jumlah insiden yang terjadi terkait dengan permasalahan keamanan dan keberlangsungan sistem
   c) Penurunan jumlah insiden yang menyebabkan *downtime*
   d) Penurunan jumlah waktu *downtime* total per durasi waktu
4) Terkait dengan manajemen infrastruktur
   a) Tingkat kepatuhan pengguna terhadap prosedur-prosedur yang telah ditetapkan
   b) Penurunan jumlah kegagalan pengoperasian *software* aplikasi
5) Terkait dengan Manajemen Data
   a) Penurunan jumlah kegagalan *restore data* kritikal
   b) Penurunan jumlah insiden terkait dengan permasalahan integritas Data
6) Terkait dengan manajemen layanan oleh pihak ketiga
   a) Jumlah atau prosentase operasi sistem TIK yang memenuhi *SLA*.
   b) Jumlah atau prosentase operasi sistem TIK yang memenuhi ketentuan minimum keamanan dan keberlangsungan sistem.
   c) Jumlah atau prosentase operasi sistem TIK yang memenuhi ketentuan minimum Manajemen Data.
   d) Penurunan jumlah insiden yang menyebabkan *downtime.*
   e) Penurunan jumlah waktu *downtime* total per durasi waktu.
   f) Penurunan jumlah kegagalan *restore data* kritikal.
   g) Penurunan jumlah insiden terkait dengan permasalahan integritas Data.

8. Pemeliharaan Sistem

a. Definisi
Pemeliharaan sistem merupakan proses untuk memastikan bahwa seluruh sumber daya TIK dapat berfungsi sebagaimana mestinya dalam durasi waktu siklus hidup yang seharusnya, dalam rangka mendukung operasi sistem secara optimal.

b. Lingkup

1) Pemeliharaan *software* Aplikasi
   a) Pemeliharaan *software* aplikasi
   b) Manajemen Aset TIK menerapkan mekanisme patching *software* aplikasi atas *software* aplikasi yang dikembangkan secara mandiri atau kerjasama dengan pihak ketiga.
   c) Upgrade yang bersifat kecil (minor) atas *software* aplikasi minimal harus melalui *regression test* dan harus disertai dengan *update* dokumentasi yang terkait langsung dengan modul yang di*upgrade*.
2) Pemeliharaan Infrastruktur Teknologi
   a) Manajemen Aset TIK menerapkan mekanisme *patching* infrastruktur teknologi (yaitu *update patch* atas infrastruktur teknologi untuk menutup lobang kerentanan) atas seluruh infrastruktur teknologinya. Mekanisme *patching* ini jika memungkinkan dapat difasilitasi secara otomatis dengan *software tool*, sehingga meningkatkan efisiensi di sisi administrator dan pengguna akhir. Mekanisme *patching* ini minimal dilakukan atas:
      - *System software* Perangkat-perangkat jaringan
      - *System software* di server dan *workstation*
      - *Database server*
   b) Secara reguler manajemen Aset TIK melakukan penilaian pertumbuhan kapasitas dan membandingkannya dengan estimasi pertumbuhan. Berdasarkan analisis perbandingan tersebut, manajemen Aset TIK menyusun langkah untuk pengelolaan kapasitas dalam jangka menengah dan pendek.
3) Pemeliharaan Data
   a) Keaslian, keutuhan, dan ketersediaan Data harus menjadi perhatian. Semua pihak dalam institusi harus menaati prosedur pemeliharaan Data yang telah ditetapkan.
   b) *Data Center/Disaster Recovery Center* (DC/DRC) dikelola sesuai dengan prosedur baku yang ada.
   c) Data harus dilindungi dari pihak-pihak yang tidak memiliki hak akses serta pengubahan dan kesalahan alamat pengiriman Data sensitif yang bernilai strategis.
4) Siklus Hidup dan Likuidasi Sumber Daya Infrastruktur Teknologi
   a) Siklus hidup infrastruktur teknologi yang diimplementasikan terdiri dari fase-fase berikut:
      - Sudah tidak adanya *technical support.*
      - Keberadaannya sudah dapat digantikan dengan kehadiran infrastruktur teknologi lain yang lebih handal dan terjangkau pengadaannya.
   b) *Likuidasi* sumber daya infrastruktur teknologi dapat dilakukan untuk teknologi lain yang lebih handal dan terjangkau pengadaannya.

5) Indikator Keberhasilan
   a) Penurunan jumlah permasalahan yang terjadi di *software* aplikasi karena tidak optimalnya keberjalanan mekanisme *patching*.
   b) Penurunan jumlah permasalahan yang terjadi di infrastruktur teknologi karena tidak optimalnya keberjalanan mekanisme *patching*.
   c) Penurunan jumlah permasalahan yang terjadi karena aspek kapasitas infrastruktur teknologi.
   d) Penurunan jumlah permasalahan yang terjadi karena aspek keutuhan (integrity), kerahasiaan (*confidentiality*), dan ketersediaan (*availability*) Data Penurunan jumlah sumber daya infrastruktur teknologi di fase *sunset* yang masih belum dilikuidasi.

9. Penghapusan Aset TIK

Penghapusan Aset TIK dilaksanakan berdasarkan ketentuan Peraturan Perundang-undangan di bidang Pengelolaan Barang Milik Daerah dan Standar Akuntansi Pemerintahan.

BAB IV
MANAJEMEN PENGETAHUAN

A. Pendahuluan

1. Latar belakang

Reformasi birokrasi bagi Pemerintah Daerah Kabupaten dimaksudkan antara lain untuk mendorong terwujudnya organisasi yang efektif dan efisien. Untuk mewujudkan organisasi seperti itu, setiap instansi pemerintah harus siap untuk memanfaatkan kekayaan pengetahuan yang dimilikinya, termasuk belajar dari pengalaman-pengalaman di masa lampau. Secara umum hal itu diwujudkan dalam bentuk peraturan dan prosedur kerja dalam organisasi tersebut, serta rangkaian kegiatan untuk perubahan dan penyempurnaanya. Kendala yang sering dihadapi adalah kenyataan bahwa pengetahuan dan pengalaman dalam organisasi tersebut sering kali tersebar, tidak terdokumentasi dan bahkan mungkin masih ada di dalam kepala masing-masing individu dalam organisasi.

Manajemen Pengetahuan atau *knowledge management* merupakan upaya untuk meningkatkan kemampuan organisasi dalam mengelola aset intelektualnya: pengetahuan dan pengalaman yang ada. Tujuannya tentu saja adalah memanfaatkan aset tersebut untuk mencapai kinerja organisasi yang lebih baik untuk mempercepat pencapaian tujuan pelaksanaan reformasi birokrasi.

Pemerintah Daerah mengelola forum *knowledge management* yang dapat dimanfaatkan sebagai *knowledge sharing* yang berguna baik dalam perumusan kebijakan reformasi birokrasi dan juga sebagai *benchmarking* bagi Pemerintah Daerah. Sedangkan Perangkat Daerah diharapkan dapat berpatisipasi aktif dalam memberikan *knowledge sharing* pengalaman pelaksanaan reformasi birokrasi dalam forum *knowledge* management. Oleh karena itu pedoman ini juga dimaksudkan untuk memberikan gambaran mengenai penerapan manajemen pengetahuan (*knowledge management).* Hal ini akan sangat membantu keberlanjutan pelaksanaan reformasi birokrasi di Pemerintah Daerah Kabupaten.

2. Tujuan

a. Membantu mengelola forum manajemen pengetahuan;
b. Memberikan pemahaman kepada Perangkat Daerah mengenai knowledge management;
c. Mendorong Perangkat Daerah untuk berpartisipasi aktif dalam knowledge sharing yang dapat dimanfaatkan dalam perumusan kebijakan dan benchmarking pelaksanaan reformasi birokrasi.

3. Pengertian

a. Manajemen pengetahuan adalah upaya terstruktur dan sistematis dalam mengembangkan dan menggunakan pengetahuan yang dimiliki untuk membantu proses pengambilan keputusan bagi peningkatan kinerja organisasi. Aktivitas dalam manajemen pengetahuan meliputi upaya perolehan, penyimpanan, pengolahan dan pengambilan kembali, penggunaan dan penyebaran, serta Evaluasi dan penyempurnaan terhadap pengetahuan sebagai aset intelektual organisasi.

b. Pengetahuan adalah pemahaman tentang sesuatu hal berdasarkan interpretasi atas sebuah konteks permasalahan tertentu.

Kategori pengetahuan dalam organisasi adalah:

1) pengetahuan implisit (*tacit*), yaitu pengetahuan yang masih berada dalam pikiran individu yang memiliki pengetahuan tersebut. Pengetahuan implisit terdiri komponen kognitif dan komponen teknis. Komponen kognitif merupakan kerangka berpikir yang tidak dapat begitu saja diutarakan dalam sebuah representasi Data yang terstruktur, sehingga kerap kali disebut pengetahuan tak terstruktur. Sementara komponen teknis adalah konsep konkrit yang bisa diutarakan secara eksplisit, sehingga sering kali disebut pengetahuan terstruktur.
2) pengetahuan eksplisit, yaitu pengetahuan yang sudah secara eksplisit diutarakan dan tersedia dalam organisasi. Umumnya pengetahuan eksplisit bersifat terstruktur dan tercermin dalam berbagai rujukan peraturan dan standar kerja dalam organisasi. Pengetahuan akan dapat memberikan manfaat terbesar bagi organisasi mana kala bisa disebarkan kepada segenap pihak yang berkepentingan dalam organisasi tersebut.

c. Sistem manajemen pengetahuan (*knowledge Management System*) adalah sistem (umumnya berbasis teknologi informasi) yang digunakan untuk melakukan pengelolaan atas pengetahuan pada tiap tahapan, baik saat perolehan, penyimpanan, pengambilan kembali, pemanfaatan maupun penyempurnaannya.

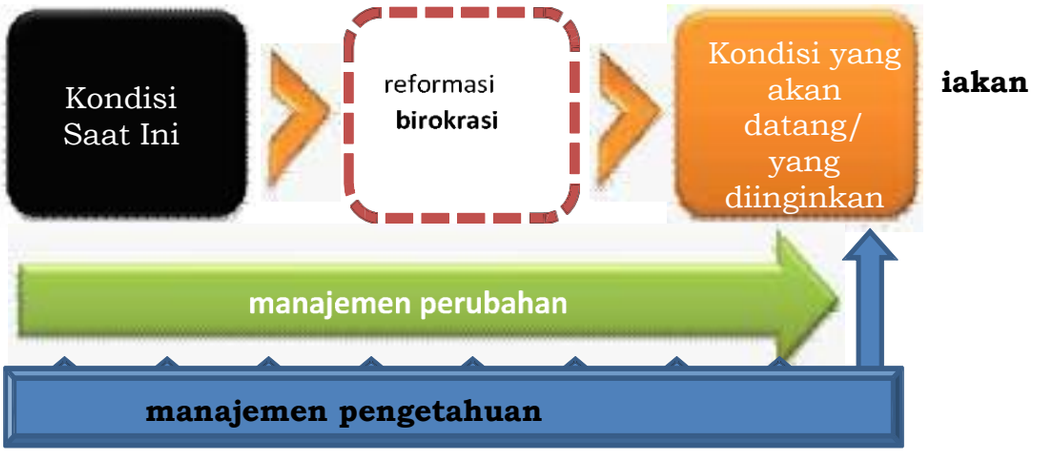
4. Prinsip

Pada prinsipnya ada tiga proses dasar dalam Manajemen Pengetahuan: perolehan/akuisisi pengetahuan, berbagi pengetahuan, dan pemanfaatan pengetahuan:

a. perolehan/akuisisi pengetahuan, yaitu proses perolehan ataupun pengembangan aset intelektual, termasuk pemahaman personal, keahlian, pengalaman dan relasi antar Data. Dalam proses ini terjadi perekaman Data dan penyimpanannya ke dalam *database* pengetahuan organisasi atau *knowledge repository*.
b. perolehan/akuisisi pengetahuan, yaitu proses perolehan ataupun pengembangan aset intelektual, termasuk pemahaman personal, keahlian, pengalaman dan relasi antar Data. Dalam proses ini terjadi perekaman Data dan penyimpanannya ke dalam database pengetahuan organisasi atau knowledge repository.
c. memanfaatkan pengetahuan, yaitu proses penggunaan-pengetahuan di dalam organisasi. Termasuk di dalamnya adalah penerapannya dalam pembentukan panduan-panduan kerja berdasarkan pengalaman dan pengetahuan di masa lampau. Dalam proses ini juga terjadi aktivitas pengembangan dan penyempurnaan lebih lanjut dari pengetahuan yang telah didapatkan.

B. Manajemen Pengetahuan Dalam Pelaksanaan Reformasi Birokrasi

Manajemen Pengetahuan berperan penting dalam membantu meningkatkan kinerja organisasi. Hal ini sejalan dengan salah satu tujuan pelaksanaan reformasi birokrasi. Manajemen Pengetahuan meningkatkan efektivitas organisasi karena dapat mendorong penggunaan pengetahuan yang sudah dimiliki (*knowledge reuse*) untuk meningkatkan kualitas proses pengambilan keputusan. Selain itu, Manajemen Pengetahuan juga dapat berperan sebagai alat bantu dalam proses perubahan atau pun transformasi organisasi, karena Manajemen Pengetahuan dapat membantu pembentukan budaya pembelajaran dalam suatu organisasi.



gambar 1
Kerangka Kerja Manajemen Pengetahuan Dalam Reformasi Birokrasi

Salah satu hasil reformasi birokrasi akan tercermin dari seberapa baik dan efektif sebuah organisasi melakukan aktivitas yang menjadi tanggung jawabnnya. Dengan adanya Manajemen Pengetahuan, organisasi dapat belajar untuk melaksanakan aktivitas yang semakin baik dari waktu ke waktu. Kemampuan individu dalam organisasi akan memanfaatkan pengetahuan kolektif yang mereka miliki sekaligus menghindari terjadinya pengulangan proses, termasuk di dalamnya kemampuan untuk belajar dan mengevaluasi tindakan yang telah dilakukan, yang pada gilirannya akan mempengaruhi kinerja organisasi itu sendiri.

Grand Design Reformasi Birokrasi 2010-2025 dan *Road Map* Reformasi Birokrasi Pemerintah Daerah Kabupaten Natuna Tahun 2020-2024 memuat 8 (delapan) area perubahan dan kondisi yang diinginkan. Penerapan Manajemen Pengetahuan akan membantu Pemerintah Daerah dalam upaya mewujudkan 8 area perubahan dan kondisi yang diinginkan tersebut. Tabel 1 menjelaskan kebutuhan pengetahuan dalam setiap area perubahan.

Tabel 1
Kebutuhan pengetahuan dalam proses perubahan

No	AREA PERUBAHAN	HASIL YANG DIHARAPKAN	KEBUTUHAN PENGETAHUAN
1	Manajemen Perubahan	Terwujudnya budaya pemerintahan yang bersih dan bebas dari Korupsi, Kolusi dan Nepotisme serta meningkatnya integritas, profesionalisme, dan citra aparatur sebagai pelayanan masyarakat.	Pengembangan dan penguatan Reformasi Birokrasi, Penguatan nilai integritas dan kepemimpinan, pengembangan dan implementasi budaya kerja
2	Penataan Peraturan Perundang-Undangan	Meningkatnya kualitas penyusunan dan penerapan regulasi daerah yang efektif, efisien, harmonis dan tidak tumpang tindih, serta terlaksananya perlindungan hukum bagi Aparatur Sipil Negara dan masyarakat miskin secara profesional.	Peta perundangan yang relevan, yang menghambat, jenis hambatan, kondisi-kondisi tertentu yang membuat regulasi sulit diterapkan, faktor penyimpangan yang bisa ditoleransi/deviasi.
3	Penataan dan Penguatan Organisasi	Terwujudnya Organisasi kelembagaan yang tepat fungsi dan tepat ukuran	Fungsi yang merupakan jabaran dari tugas dalam rangka mencapai tujuan organisasi dan perlu dikembangkan kapabilitasnya. Pengetahuan ini perlu dipadukan dan disempurnakan terus menerus sejalan dengan dinamika perubahan dan dengan perkembangan/ tuntutan kebutuhan jaman.
4	Penataan Tatalaksana	Penerapan sistem, proses dan prosedur kerja yang jelas, efektif, dan efisien, serta berbasis e-government	Pemahaman tentang SPBE, Manajemen kearsipan modern dan handal, Pengelolaan Keuangan secara tepat dan Pengelolaan Barang Milik Daerah secara tepat dan sesuai aturan

5	Penataan Sistem Manajemen Sumber Daya Manusia Aparatur	Dapat meningkatkan manajemen kinerja individu, Menyempurnakan Manajemen kepegawaian yang terintegrasi, dan Meningkatkan Profesionalisme pegawai.	Prinsip-prinsip manajemen ASN secara professional, Manajemen ASN berbasis Merit *System*, Pengembangan potensi dan karir ASN, Manajemen talenta
6	Penguatan Pengawasan	Dapat meningkatkan kapasitas Aparat Pengawasan Intern Pemerintah, meningkatkan penerapan penyelenggaraan pemerintahan yang bersih dan bebas Korupsi, Kolusi dan Nepotisme, dan mempertahankan opini Wajar Tanpa Pengecualian dari Badan Pemeriksa Keuangan.	Kompetensi APIP, Benturan Kepentingan, Sistem Pengendalian Internal Pemerintah, Zona Integritas dan Reformasi Birokrasi
7	Penguatan Akuntabilitas Kinerja	Penerapan Sistem Akuntabilitas Kinerja Instansi Pemerintah dan akuntabilitas aparatur semakin meningkat disemua Perangkat Daerah Kabupaten, menyempurnakan integrasi perencanaan, penganggaran dan manajemen kinerja, serta keterlibatan pimpinan SKPD mulai dari perencanaan, penilaian kinerja dan pelaporan kinerja semakin meningkat, sehingga dapat mempertahankan nilai Akuntabilitas Kinerja Instansi Pemerintah bahkan meningkatkan nilai Akuntabilitas Kinerja Instansi Pemerintah dari B menjadi A	Indikator akuntabilitas, cara mengukur dan Evaluasinya
8	Peningkatan Kualitas Pelayanan Publik	Dapat meningkatkan kualitas pelayanan publik sesuai kebutuhan dan harapan masyarakat,	Kebijakan Bidang Pelayanan Publik, Standar Pelayanan, Inovasi Proses Bisnis

C. Elemen Dan Tahapan Implementasi Manajemen Pengetahuan

1. Elemen Penerapan Manajemen Pengetahuan

Terdapat dua elemen pokok di dalam penerapan Manajemen Pengetahuan, yaitu kejelasan posisi Data dalam organisasi dan kejelasan Manajemen Data dan pengetahuan dalam organisasi. Kejelasan akan dua hal tersebut harus tertuang secara eksplisit dalam rencana dan strategi penerapan manajemen pengetahuan dalam Pemerintah Daerah Kabupaten.

a. Kejelasan posisi Data

Pemerintah Daerah Kabupaten harus secara tegas menyatakan bahwa ke depan akan menjadi organisasi pembelajaran yang mendasarkan segenap aktivitas dan proses pengambilan keputusan pada Data dan informasi yang valid, termasuk dalam penyusunan mekanisme, prosedur, tata laksana maupun pengelolaan mobilitas personel di dalamnya. Pemerintah Daerah Kabupaten perlu secara tegas menyatakan bahwa semua Data dan informasi adalah milik institusi. Setiap unit kerja bisa saja menjadi produsen, pengelola atau pun penanggung jawab validitas Data, tetapi bukan berarti memiliki hak untuk memiliki dan membatasi kepemilikan dan akses akan Data.

b. Kejelasan manajemen

Setelah posisi Data dan informasi sebagai sumber pengetahuan jelas, maka Pemerintah Daerah Kabupaten selanjutnya perlu menetapkan Manajemen Data dan informasi tersebut. Prinsip manajemen pada Manajemen Pengetahuan bersumber pada kejelasan posisi Data dan informasi. Walaupun semua Data dan informasi adalah milik institusi, tidak berarti tidak ada kejelasan otoritas yang dapat mengakses, mengubah, dan menyebarkan Data dan informasi tersebut. Penanggung jawab terhadap validitas Data dan informasi juga harus ada. Karena sifatnya yang mencakup seluruh lini organisasi, maka aturan manajemen ini ditetapkan dalam Peraturan Bupati.

Untuk sebuah jenis informasi dan pengetahuan tertentu bisa saja bersumber dari jenis Data yang berasal dari unit kerja yang berbeda. Masing-masing unit kerja juga akan saling menggunakan Data dan informasi dari unit kerja lainnya. Karena itu kejelasan akan manajemen ini menjadi sangat penting. Jika nantinya ada unit kerja yang bertanggung jawab atas penyimpanan Data misalnya (umumnya unit pengolahan Data atau pun unit teknologi informasi), tidak berarti unit yang bersangkutan yang memiliki dan bertanggung jawab penuh atas Data. Manajemen Data dan pengetahuan dalam organisasi akan mengatur mekanisme yang transparan dan akuntabel dalam pengelolaannya di Pemerintah Daerah Kabupaten dalam semua proses manajemen pengetahuan: perolehan/akuisisi Data, penyebaran pengetahuan, dan pemanfaatan pengetahuan untuk kepentingan lembaga.

2. Tahapan Implementasi Manajemen Pengetahuan

Tahapan penerapan manajemen pengetahuan dalam rangka pelaksanaan reformasi birokrasi di Pemerintah Daerah dapat dijelaskan pada Gambar 2 berikut ini:

Gambar 2
Tahapan Implementasi Manajemen Pengetahuan

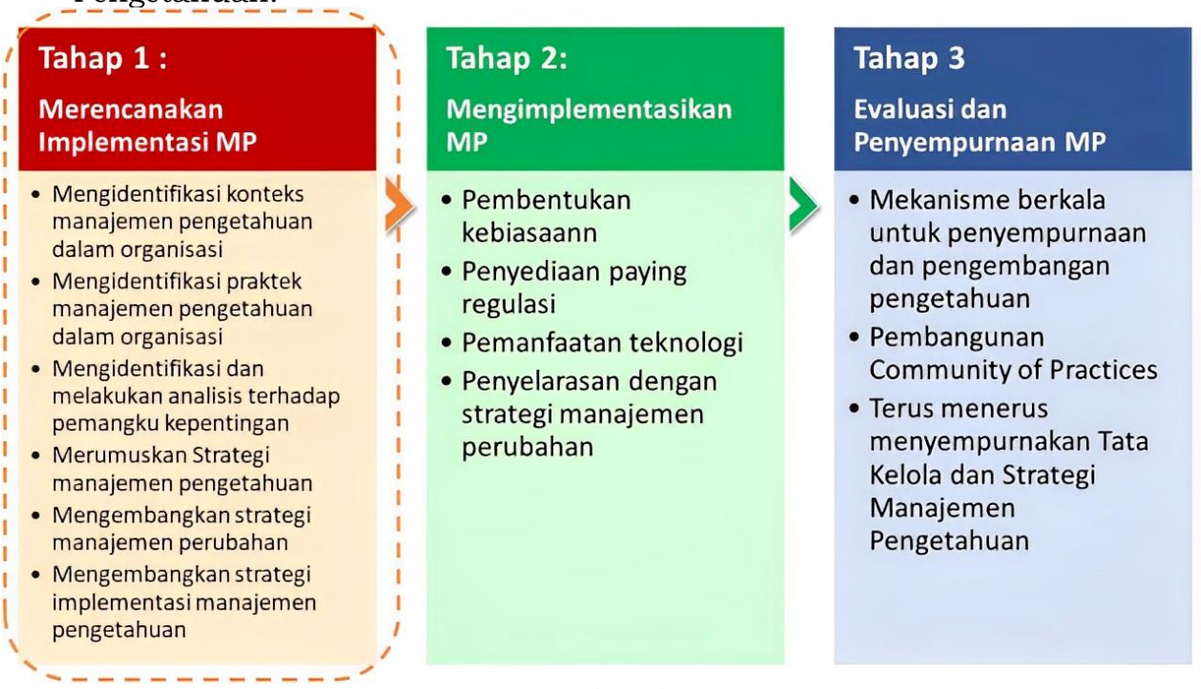
a. Langkah-langkah yang harus dilakukan pada tahap-1:
   1) Mengidentifikasi konteks manajemen pengetahuan dalam organisasi;
   2) Mengidentifikasi praktek manajemen pengetahuan dalam organisasi;
   3) Mengidentifikasi dan melakukan analisis terhadap para pemangku kepentingan;
   4) Merumuskan strategi manajemen pengetahuan;
   5) Mengembangkan strategi manajemen perubahan;
   6) Mengembangkan strategi implementasi manajemen pengetahuan.

b. Langkah-langkah yang harus dilakukan pada tahap-2:
   1) Pembentukan kebiasaan;
   2) Penyediaan payung regulasi;
   3) Pemanfaatan teknologi;
   4) Penyelarasan dengan strategi manajemen perubahan.

c. Langkah-langkah yang harus dilakukan pada tahap-3:
   1) Mekanisme berkala untuk penyempurnaan dan pengembangan pengetahuan;
   2) Pembangunan *Community of Practices;*
   3) Terus menerus menyempurnakan Manajemen dan Strategi Manajemen Pengetahuan.

D. Merencanakan Implementasi Manajemen Pengetahuan

Seperti yang telah disampaikan pada elemen dan tahapan implementasi manajemen pengetahuan, tahap Perencanaan Implementasi Manajemen Pengetahuan terdiri atas 6 (enam) kegiatan utama yang akan dijabarkan satu per satu di sini. Gambar 3 di bawah ini menjelaskan Tahap 1 dari kegiatan utama dalam perencanaan implementasi Manajemen Pengetahuan.



gambar 3
Merencanakan Implementasi Manajemen Pengetahuan

1. Mengidentifikasi Konteks Manajemen Pengetahuan Dalam Organisasi

Tahapan ini diawali dengan identifikasi bagaimana peran Data dan informasi sebagai sumber pengetahuan di dalam organisasi. Setiap Perangkat Daerah perlu memiliki semacam peta pengetahuan yang perlu dimiliki di dalam organisasi, ketersediaannya saat ini, cara memperolehnya, penggunaannya, hak akses dan distribusinya, dan sebagainya. Demikian pula rangkaian perubahan dari Data mentah menjadi informasi, dan dari informasi menjadi sebuah pengetahuan yang komprehensif. Tujuan dari tahapan ini adalah mengidentifikasi peran strategis pengetahuan dalam menentukan arah dan kebijakan organisasi.

2. Mengidentifikasi Praktek Manajemen Pengetahuan Dalam Organisasi

Kegiatan ini dilakukan untuk mengidentifikasikan bagaimana Data dan informasi dikelola di dalam organisasi. Di beberapa organisasi, penguasaan Data dan informasi sebagai basis dalam bekerja hanya terpusat pada sekelompok orang atau pada unit tertentu saja (eksklusif) sehingga pengambilan keputusan tidak tercipta dengan baik. Sebagai ilustrasi, riset dari Delphi Group (2007) menunjukkan bahwa secara persentase pengetahuan (*knowledge*) di dalam organisasi tersimpan dengan komposisi:

1. 42 % di dalam pikiran (otak) pegawai;
2. 26 % di dalam dokumen *hard copy* (kertas);
3. 20 % di dalam dokumen elektronik; dan
4. 12 % di dalam *electronic-based knowledge*.

Peran Data dan informasi di dalam organisasi pemerintah sangatlah signifikan, dan juga kepemilikan atas Data dan informasi tidak hanya berpengaruh pada posisi dan mobilitas vertikal, tetapi seringkali juga memiliki nilai material yang bisa diperjualbelikan.

Sebagai contoh, pengembangan dan pemanfaatan Manajemen Pengetahuan di salah satu instansi terkemuka dilakukan karena alasan berikut:

a. Menghindari terjadinya keluarnya pengetahuan yang dibawa oleh para pegawai yang sudah tidak bekerja lagi di Pemerintah Daerah Kabupaten;
b. Menghindari hilangnya pengetahuan yang berharga; dan
c. Menghindari terjadinya pengulangan proses.

Kondisi tersebut merupakan pintu pertama yang harus didobrak jika ingin mengimplementasikan manajemen pengetahuan. Segenap individu dalam organisasi harus disadarkan (dan dipaksa untuk sadar) bahwa semua aktivitas yang mereka lakukan adalah untuk kepentingan institusi.

3. Mengidentifikasi dan Melakukan analisis terhadap para pemangku kepentingan

Di dalam sebuah organisasi Pemerintah Daerah, akan banyak sekali unit dan satuan kerja yang terlibat dalam pengelolaan Data dan informasi. Segenap unit terkait tersebut perlu dipetakan dan diidentifikasi perannya. Ada unit yang berperan sebagai produsen dan/atau pengolah informasi dan ada yang sebagai konsumen dari informasi itu sendiri. Juga di dalam beberapa organisasi, sering kali terdapat beberapa unit kerja yang memiliki tanggung jawab akan jenis Data yang sama. Pemerintah Daerah Kabupaten perlu merumuskan dan menetapkan unit mana yang memiliki otoritas akhir terhadap validitas Data tersebut.

4. Merumuskan Strategi Manajemen Pengetahuan

Setelah rangkaian aktivitas di atas, sebuah peta awal akan mulai terbentuk sehingga bisa menjadi basis untuk menyusun sebuah strategi manajemen pengetahuan yang lebih komprehensif. Sesuai dengan elemen- elemen manajemen pengetahuan, strategi tersebut pada dasarnya akan menegaskan posisi Data dan manajemennya dalam organisasi. Selain itu juga akan dirumuskan faktor-faktor lain yang menunjang penerapan manajemen pengetahuan tersebut.

Isi dari sebuah Strategi Manajemen Pengetahuan setidaknya harus mencakup hal-hal sebagai berikut:

a. Posisi Data, informasi, dan pengetahuan dalam organisasi;
b. Manajemen, mencakup segenap aspek dalam manajemen pengetahuan sejak perolehan dan pengolahan, penyebaran maupun Evaluasi dan pengembangannya. Termasuk dalam hal ini adalah penetapan unit yang bertanggung jawab mengoordinasikan manajemen pengetahuan;
c. Pembentukan Budaya, berisi rumusan upaya untuk mendorong kemauan segenap individu dalam organisasi untuk berbagi Data dan pengetahuan, khususnya yang bersifat implisit. Bagian ini

harus diselaraskan dengan agenda manajemen perubahan dalam organisasi;

d. Manajemen Data, mengatur teknis pengelolaan Data, validasi, teknik transformasi (untuk pengolahan Data), penamanaan dan identitas Data, dan sejenisnya;
e. Penggunaan Teknologi, merumuskan jenis-jenis teknologi yang akan dimanfaatkan untuk melaksanakan manajemen pengetahuan dalam organisasi. Bagian ini harus diselaraskan dengan strategi manajemen teknologi informasi dalam organisasi;
f. Penggunaan Manajemen Pengetahuan, berisi rumusan pemanfaatan manajemen pengetahuan terkait dengan kepentingan strategis organisasi. Termasuk di dalamnya merumuskan mekanisme penggunaannya jika memerlukan interaksi dengan organisasi lainnya.

Sebagai contoh, salah satu strategi manajemen pengetahuan di salah satu instansi terkemuka untuk mengelola pengetahuan yang bersifat implicit adalah dengan melakukan *knowledge sharing forum* (forum untuk berbagi informasi, ilmu dan pengetahuan), dengan harapan bahwa *knowledge transfer* (transfer pengetahuan) dapat bergulir dengan lebih cepat. Sedangkan untuk yang bersifat eksplisit strateginya adalah dengan menyimpannya di dalam suatu *knowledge repository* berupa *knowledge management portal*. Melalui portal ini karyawan dapat mempelajari pengetahuan yang ada dan menyebarkannya kepada rekan-rekannya yang lain.

5. Mengembangkan Strategi Manajemen Perubahan

Dalam strategi manajemen pengetahuan, terdapat hal-hal yang menyangkut pembentukan budaya dan pembangunan manajemen dalam organisasi. Kedua hal ini sangat terkait dengan proses manajemen perubahan dalam organisasi. Karena itu, dalam setiap implementasi manajemen pengetahuan perlu dilakukan sinkronisasi dengan strategi manajemen perubahan (dikarenakan faktor manusia dan budaya sangat menentukan), dan jika strategi semacam itu belum ada maka perlu diikuti dengan pengembangan dan penyusunan strategi manajemen perubahan tersebut.

6. Mengembangkan Strategi Implementasi Manajemen Pengetahuan

Setelah Perangkat Daerah memiliki strategi tersebut, selanjutnyaadalah menyusun tahapan perubahan sesuai dengan kondisi dan batasan yang dimiliki. Ada beberapa faktor yang akan mempengaruhi penyusunan strategi dan tahapan implementasi tersebut, yaitu kondisi SDM dan kultur yang ada, perubahan regulasi, dan ketersediaan pendanaan. Kondisi tersebut bersifat unik untuk setiap organisasi dan memerlukan rumusan yang sesuai dengan fakta lapangan yang dihadapi.

Keluaran pada Tahap Perencanaan Implementasi Manajemen Pengetahuan mencakup:

a. Analisis Situasi, yang meliputi antara lain:
    1) Identifikasi peran strategis pengetahuan di dalam organisasi;

2) Inventori sumber – sumber pengetahuan, kategori pengetahuan di dalam organisasi dan kebutuhan informasi;
3) Analisis budaya organisasi yang ada saat ini.

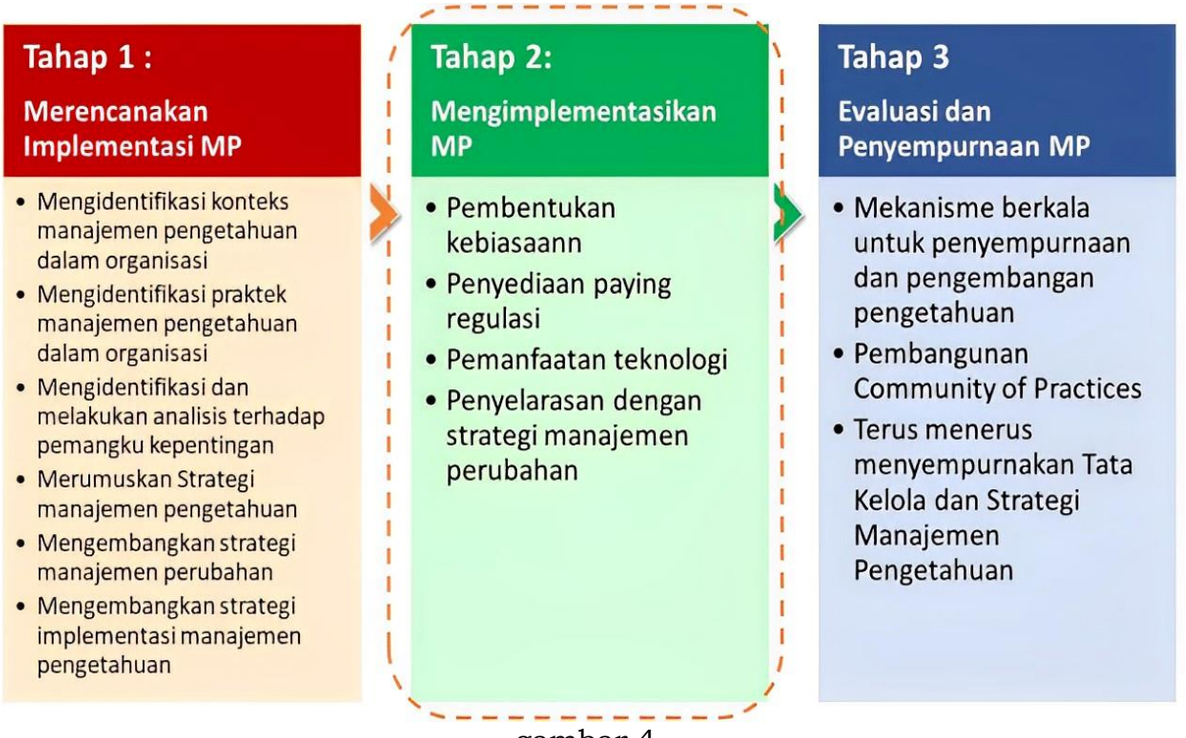
b. Strategi Manajemen Pengetahuan, yang meliputi antara lain:
1) Manajemen manajemen pengetahuan;
2) Manajemen Data;
3) Penggunaan teknologi;
4) Penggunaan dan valuasi manajemen pengetahuan;
5) Dukungan budaya organisasi.

c. Rencana Implementasi Manajemen Pengetahuan, yang meliputi antara lain:
1) Tahapan dan aktivitas yang akan dilakukan, termasuk waktu pekerjaan dan penyelesaian;
2) Indikator kinerja utama.

E. Mengimplementasikan Manajemen Pengetahuan

Terdapat tiga hal yang akan mempengaruhi implementasi manajemen pengetahuan, yaitu aspek SDM dan budaya organisasi, aspek regulasi, dan aspek pendanaan. Dengan mengesampingkan aspek pendanaan, maka ada dua faktor kunci yang perlu diperhatikan dalam implementasi Manajemen Pengetahuan, yaitu aspek SDM dan budaya serta aspek regulasi. Kedua aspek tersebut sering kali berkaitan satu sama lainnya. Selain itu, karena manajemen pengetahuan modern sangat tergantung pada pemanfaatan teknologi, maka aspek pemanfaatan teknologi juga perlu mendapat perhatian tersendiri.

Tahap pengimplementasian manajemen pengetahuan pada dasarnya mencakup 4 (empat) kegiatan utama. Gambar 4 di bawah ini menjelaskan kegiatan utama dalam implementasi manajemen pengetahuan.



gambar 4
mengimplementasikan manajemen Pengetahuan

1. Pembentukan Kebiasaan

   Salah satu upaya yang dapat dilakukan untuk mempersiapkan SDM dan membangun iklim yang kondusif adalah dengan membangun kebiasaan untuk berbagi Data dan pengetahuan. Kebiasaan ini akan menuntut pula adanya kebiasaan menggunakan Data yang akurat dan menyimpan Data yang dimiliki dengan rapi. Syarat pokok dalam pembentukan kebiasaan ini adalah dengan penetapan posisi Data sebagai milik organisasi, sebagaimana disebutkan di awal dokumen ini. Pada aktivitas ini mungkin akan masih ada benturan-benturan kewenangan, benturan regulasi maupun pertanyaan soal akurasi Data. Hal ini bisa diatasi dengan kesepakatan antar unit kerja yang terlibat.

2. Penyediaan Payung Regulasi

   Manajemen tidak akan efektif bilamana tidak memiliki payung regulasi yang cukup atau bahkan berbenturan dengan aturan formal yang ada. Rumusan manajemen pengetahuan dalam strategi manajemen pengetahuan perlu diikuti dengan penetapan kerangka regulasi yang menunjang. Sebagai contoh, keberhasilan implementasi manajemen pengetahuan di salah satu Badan Usaha Milik Negara (BUMN) terkemuka di bidang telekomunikasi adalah adanya kebijakan/regulasi yang mengatur manajemen pengetahuan selain adanya perencanaan strategis perusahaan yang mendukung strategi manajemen pengetahuan.

3. Pemanfaatan teknologi

   Dengan semakin besar volume Data dan kompleksnya kebutuhan Data, hampir mustahil untuk mengelola pengetahuan di dalam organiasi secara manual. Peran teknologi informasi akan sangat dominan dalam hal ini dan setidaknya akan mencakup kebutuhan-kebutuhan sebagai berikut:

   a. Perolehan dan pengolahan Data

      Antara lain sistem untuk merekam Data elektronik, baik Data terstruktur (dalam *database*) atau pun tidak terstruktur (dalam bentuk uraian teks, gambar, video, audio, dan sebagainya), sistem untuk mengolah Data (termasuk menyusun indeks, katalog, dan sebagainya), dan pengklasifikasian pengetahuan

   b. Penyebaran pengetahuan

      1) Fasilitas untuk penyebaran informasi serta melakukan komunikasi dan kolaborasi, seperti teknologi portal Internet dan Intranet, forum diskusi elektronik, sistem katalog elektronik, serta sistem pencarian dan temu kembali (*retrieval*) informasi – baik sistem pencarian manual maupun sistem deteksi dini akan kebutuhan Data dan informasi;
      2) Sistem yang mengatur hak akses untuk menggunakan pengetahuan dan menjaga kerahasiaannya.

   c. Evaluasi, pengembangan dan penyempurnaan pengetahuan

      Pada tahap awal bisa berupa forum diskusi elektronis dan sistem Katalog pengetahuan. Dalam jangka panjang, jika telah dilakukan integrase terhadap sistem informasi yang digunakan dalam proses kerja dalam organisasi, fasilitas ini bisa berkembang untuk mendeteksi pemanfaatan pengetahuan yang ada dalam pengambilan keputusan di segenap lini organisasi.

4. Penyelarasan Strategi Manajemen Pengetahuan Dengan Strategi

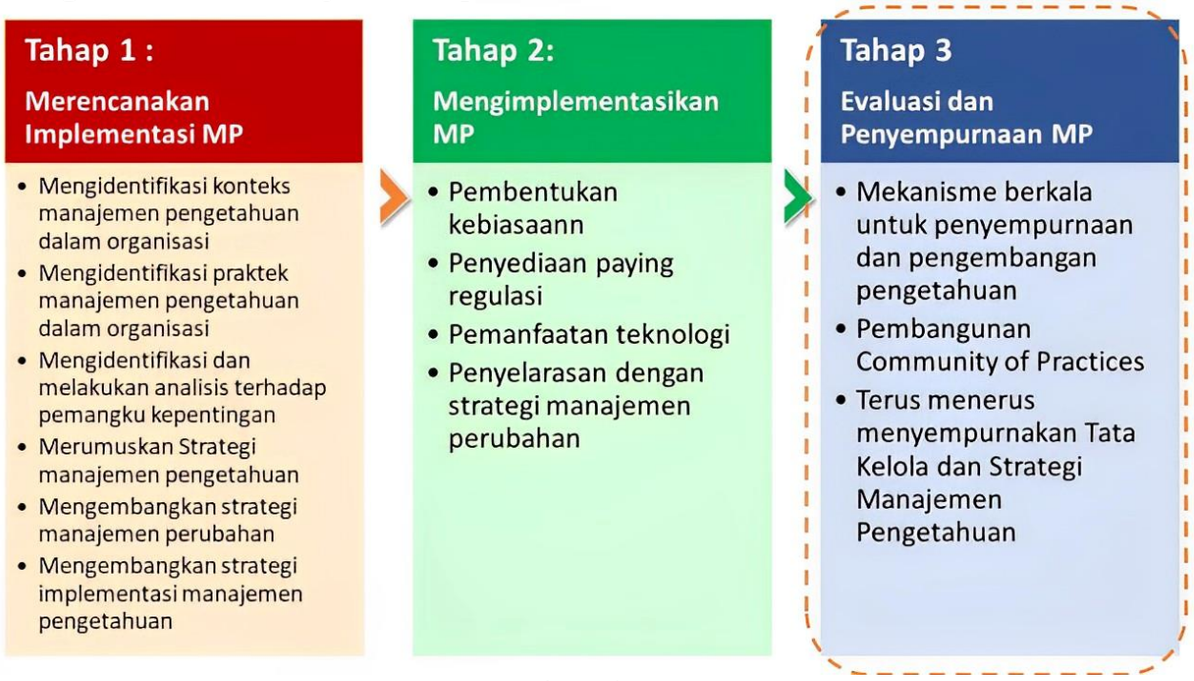
Manajemen Perubahan Implementasi manajemen pengetahuan ini juga terkait dengan proses transformasi budaya kerja dalam organisasi. Oleh karena itu, penyelarasan terus menerus dengan strategi manajemen perubahan perlu dilakukan. Setiap dinamika yang terjadi akan sangat potensial untuk saling mempengaruhi keduanya.

Keluaran pada Tahap Implementasi Manajemen Pengetahuan mencakup, antara lain:

a. Implementasi strategi dan rencana kerja manajemen pengetahuan;
b. Pembangunan payung hukum untuk menunjang implementasi manajemen pengetahuan secara berkesinambungan;
c. Laporan kemajuan perkembangan implementasi manajemen pengetahuan dan sinkronisasinya dengan implementasi manajemen perubahan.

F. Evaluasi Pelaksanaan Manajemen Pengetahuan

Kegiatan pada tahap ini pada dasarnya merupakan aktivitas monitoring dan Evaluasi, diikuti dengan serangkaian tindak lanjut untuk meningkatkan dan menyempurnakan kualitas pengetahuan yang dimiliki. Kegiatan tersebut dijelaskan pada Gambar 5 di bawah ini.



gambar 5
Evaluasi dan penyempurnaan manajemen pengetahuan

1. Mekanisme Berkala Penyempurnaan dan Pengembangan Pengetahuan

Setiap Perangkat Daerah secara berkala harus mengukur tingkat keberhasilan dari penerapan manajemen pengetahuan. Cara mengumpulkan dan menganalisis umpan balik, misalnya dengan melakukan kunjungan lapangan dan mengevaluasi penerapannya. Hasil Evaluasi tersebut digunakan untuk mendiagnosa kesenjangan antara pengetahuan yang dimiliki dengan kebutuhan maupun kekurangan- kekurangan lainnya yang mungkin masih ada. Selanjutnya organisasi perlu melaksanakan kegiatan untuk menyempurnakan katalog pengetahuan yang dimilikinya.

2. Pembangunan *Community of Practices (COP)*

Community of Practices adalah sekelompok individu yang memiliki kesamaan minat dan pengetahuan akan suatu hal atau bidang tertentu dan mereka secara reguler maupun insidentil bertemu untuk bertukar pikiran dan mendiskusikan hal-hal terkait dengan bidang yang mereka minati. Hasilnya kemudian mereka rumuskan menjadi sebuah panduan atau pengetahuan tertentu. Peran fasilitas diskusi elektronik sangat penting dalam pembentukan *COP*, walau tidak menghilangkan peran sesi pertemuan dan berbagi pengetahuan secara fisik.

Untuk memperkaya pengetahuan, pembentukan *COP* ini bisa melintasi batas organisasi bekerja sama dengan lembaga lain atau unit kerja di lembaga lain yang memiliki tugas pokok dan fungsi yang sejenis.

3. Perbaikan Terus-Menerus Manajemen di Strategi Manajemen Pengetahuan

Hasil monitoring dan Evaluasi maupun berbagai pengalaman melalui *Community of Practices* (COP) sering kali memicu perlunya penyempurnaan manajemen dan bahkan strategi manajemen pengetahuan yang dimiliki. Pemerintah Daerah Kabupaten harus memiliki fleksibilitas yang memadai dalam bentuk mekanisme perubahan manajemen dan strategi manajemen pengetahuan tersebut.

Keluaran pada Tahap Evaluasi dan Penyempurnaan Manajemen Pengetahuan mencakup:

a. Hasil monitoring dan Evaluasi implementasi manajemen pengetahuan;
b. Rekomendasi perbaikan untuk meningkatkan implementasi dan pengelolaan manajemen pengetahuan;
c. Pembentukan *Community of Practices* untuk menunjang keberlanjutan dan pemanfaatan manajemen perubahan di dalam organisasi.

Pedoman ini diharapkan dapat membantu Perangkat Daerah dalam mengimplementasikan Program Manajemen Pengetahuan. Program ini merupakan faktor kunci untuk membentuk proses pembelajaran terus menerus dalam organisasi, sehingga tidak saja membentuk perilaku yang konsisten bagi setiap aparatur negara maupun dalam memberikan pelayanan publik berkualitas yang konsisten, tetapi juga membantu Pemerintah Daerah Kabupaten dalam mengembangkan kualitas kerja organisasi yang bersangkutan. Kemampuan tersebut akan turut menjadi indikator suksesnya pelaksanaan reformasi birokrasi.

BAB V
PEDOMAN MANAJEMEN PERUBAHAN

A. Pendahuluan

1. Latar belakang

Manajemen Perubahan atau *change management* merupakan pengelolaan sumber daya dalam rangka mencapai tujuan organisasi dengan kinerja yang lebih baik. Perubahan merupakan pergeseran organisasi dari keadaan sekarang menuju keadaan yang diinginkan. Dalam organisasi, perubahan tersebut meliputi struktur, proses, orang, pola pikir dan budaya kerja. Perubahan sebagaimana yang diinginkan reformasi birokrasi bukanlah proses sederhana. Disamping itu, perubahan berpeluang memunculkan resistensi pada individu di dalam organisasi. Transparansi proses, komunikasi dan keterlibatan semua pihak dalam proses perubahan akan dapat mengurangi resistensi.

Mengingat besarnya cakupan kegiatan dan hasil perubahan yang diinginkan oleh reformasi birokrasi, maka mengelola perubahan untuk mencapai tujuan dan sasaran reformasi birokrasi menjadi sangat penting. Dalam rangka itu, disusun pedoman pelaksanaan manajemen perubahan, agar Dinas/Badan dan Perangkat Daerah memiliki kesamaan pemahaman dan dapat melaksanakannya dengan baik.

2. Tujuan

a. Membantu Perangkat Daerah dalam memahami manajemen perubahan sehubungan dengan pelaksanaan reformasi birokrasi;
b. Memberikan panduan kepada Perangkat Daerah dalam merencanakan, memantau, dan mengevaluasi pelaksanaan manajemen perubahan;
c. Memudahkan Dinas/Badan dan Perangkat Daerah melaksanakan manajemen perubahan.

3. Pengertian

a. Manajemen perubahan adalah suatu proses yang sistematis dengan menerapkan pengetahuan, sarana dan sumber daya yang diperlukan organisasi untuk bergeser dari kondisi sekarang menuju kondisi yang diinginkan, yaitu menuju ke arah kinerja yang lebih baik dan untuk mengelola individu yang akan terkena dampak dari proses perubahan tersebut.
b. Agen perubahan atau *agent of change* adalah individu/kelompok yang terlibat dalam merencanakan perubahan dan mengimplementasikannya. Dalam sebuah proses perubahan, para agen perubahan ini berperan sebagai *role model.* Biasanya agen perubahan adalah mereka yang “dapat” dijadikan contoh, baik dalam prestasi kerjanya dan dalam perilakunya. Agen perubahan terdiri dari pimpinan organisasi (sebuah keharusan) dan pegawai-pegawai yang “dipilih” berdasarkan kriteria tertentu, sesuai dengan tuntutan peran agen perubahan. Adapun peran agen perubahan adalah sebagai berikut:

1) katalis adalah peran untuk meyakinkan pegawai yang ada di masing- masing Dinas/Badan dan Perangkat Daerah tentang pentingnya perubahan menuju kondisi yang lebih baik (tujuan yang direncanakan).
2) Pemberi solusi adalah peran sebagai pemberi alternatif solusi kepada pegawai Dinas/Badan dan Perangkat Daerah yang mengalami kendala dalam proses berjalannya perubahan menuju tujuan akhir.
3) Mediator adalah peran untuk membantu melancarkan proses perubahan, terutama menyelesaikan masalah yang muncul di dalam pelaksanaan reformasi birokrasi dan membina hubungan antara pihak-pihak yang ada di dalam dan pihak di luar Dinas/Badan dan Perangkat Daerah terkait dalam proses perubahan.
4) Penghubung sumber Daya adalah peran untuk menghubungkan pegawai yang ada di dalam Dinas/Badan dan Perangkat Daerah kepada pemilik sumber daya atau pembuat kebijakan.

c. Role model adalah individu yang bisa dijadikan contoh dalam prestasi kerjanya, pola fikirnya (mind set) dan budaya kerjanya (cultur set) dalam proses perubahan.
d. Pemangku kepentingan adalah kelompok atau individu yang memiliki kepentingan serta dapat mempengaruhi dan atau dipengaruhi oleh suatu pencapaian tujuan tertentu.
e. strategi komunikasi adalah cara yang digunakan untuk menyampaikan informasi perubahan (baik program maupun kebijakan) dari satu pihak (agen perubahan dan tim manajemen perubahan Perangkat Daerah) kepada pihak internal Perangkat Daerah dan pihak eksternal. Dalam proses tersebut ditumbuhkan suatu proses pembelajaran dua arah tentang cara berpikir, merasakan, dan bertindak, untuk menghasilkan perubahan.

4. Prinsip
a. Kejelasan tujuan, adanya kejelasan tujuan atau hasil yang ingin dicapai dari proses perubahan.
b. Kesadaran akan proses, bahwa perubahan merupakan proses menuju kondisi yang lebih baik.
c. Membangun kepercayaan. Role model adalah kunci dalam membangun kepercayaan. Model positif dari seluruh pimpinan adalah sebuah keharusan untuk membangun kepercayaan.
d. Dimulai dari tingkatan paling atas. Perubahan tidak akan berhasil tanpa keterlibatan pimpinan tertinggi. Komitmen dan partisipasi aktif dari pimpinan tertinggi adalah sebuah keharusan untuk mencapai tujuan perubahan.
e. Besarnya partisipasi. Perubahan membutuhkan partisipasi aktif dari seluruh komponen yang terlibat dalam proses perubahan.
f. Tumbuhnya rasa memiliki. Menumbuhkan rasa kepemilikan dapat mendorong terjadinya perubahan dan mempertahankan momentum perubahan tetap terpelihara.
g. Ketersediaan sumber daya. Untuk melaksanakan perubahan dibutuhkan investasi sumber daya yang besar, baik dana, personil, waktu serta sarana dan prasarana.

h. Keteraturan salah satu kunci keberhasilan dalam pelaksanaan perubahan adalah adanya keteraturan atau kesetiaan pada rencana yang terstruktur.
i. Keberlanjutan komunikasi. Memberikan informasi berulang kali, melalui jalur media yang berbeda-beda dan dengan tingkat kedalaman yang semakin meningkat untuk membangun pengetahuan, pemahaman, keterampilan dan keyakinan dalam rangka membangun kepemilikan bersama proses perubahan.

B. Manajemen Perubahan Dalam Pelaksanaan Reformasi Birokrasi

Sesuai dengan pengertian manajemen perubahan di atas, maka dalam kerangka reformasi birokrasi, pemahaman manajemen perubahan dapat digambarkan sebagai berikut:

gambar 1
Kerangka Pikir Manajemen Perubahan Dalam reformasi birokrasi

Dalam peraturan Presiden Nomor 81 Tahun 2010 tentang *Grand Design* Reformasi Birokrasi 2010-2025 telah diidentifikasi kondisi yang dihadapi saat ini oleh birokrasi, yaitu:

1. Organisasi. Organisasi pemerintahan yang belum tepat fungsi dan tepat ukuran (*right sizing).*
2. Peraturan Perundang-undangan. Beberapa Peraturan Perundang-undangan di bidang Aparatur Negara masih ada yang tumpang tindih, inkonsisten, tidak jelas dan multi tafsir. Selain itu, masih ada pertentangan antara Peraturan Perundang-undangan yang satu dengan yang lainnya, baik yang sederajat maupun antara peraturan yang lebih tinggi dengan peraturan di bawahnya atau antara peraturan pusat dengan peraturan daerah. Disamping itu, banyak Peraturan Perundang-undangan yang belum disesuaikan dengan dinamika perubahan penyelenggaraan pemerintahan dan tuntutan masyarakat.
3. SDM Aparatur. SDM aparatur negara Indonesia (PNS) saat ini berjumlah 4,732,472 orang (Data BKN per Mei 2010). Masalah SDM aparatur negara adalah alokasi dalam hal kuantitas, kualitas, dan distribusi PNS menurut teritorial (daerah) tidak seimbang, serta tingkat produktivitas PNS masih rendah. Manajemen sumber daya manusia aparatur belum dilaksanakan secara optimal untuk meningkatkan profesionalisme, kinerja pegawai dan organisasi. Selain itu, sistem penggajian pegawai negeri belum didasarkan pada bobot pekerjaan/jabatan yang diperoleh dari Evaluasi jabatan. Gaji pokok yang ditetapkan berdasarkan golongan/pangkat tidak sepenuhnya mencerminkan beban tugas dan tanggung jawab. Tunjangan kinerja

belum sepenuhnya dikaitkan dengan prestasi kerja dan tunjangan pensiun belum menjamin kesejahteraan.

4. Kewenangan. Masih adanya praktik penyimpangan dan penyalahgunaan wewenang dalam proses penyelenggaraan pemerintahan dan belum mantapnya akuntabilitas kinerja instansi pemerintah.
5. Pelayanan publik. Pelayanan publik belum dapat mengakomodasi kepentingan seluruh lapisan masyarakat, dan belum memenuhi hak-hak dasar warga negara/penduduk. Penyelenggaraan pelayanan publik belum sesuai dengan harapan bangsa berpendapatan menengah yang semakin maju dan persaingan global yang semakin ketat.
6. Pola pikir (*mind-set*) dan budaya kerja (*culture-set*). Pola pikir (*mind-set*) dan budaya kerja (*culture-set*) birokrat belum sepenuhnya mendukung birokrasi yang efisien, efektif dan produktif, dan profesional. Selain itu birokrat belum benar-benar memiliki pola pikir yang melayani masyarakat, belum mencapai kinerja yang baik dan belum berorientasi pada hasil (*outcomes*).

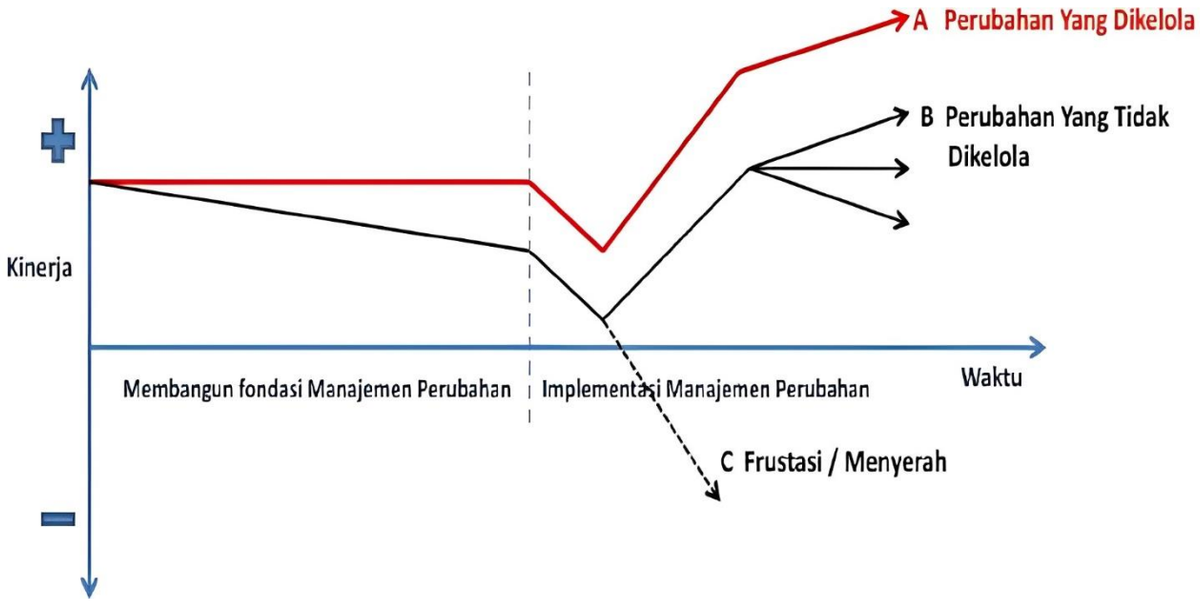
Reformasi birokrasi diharapkan akan menjadi pendorong perubahan untuk membawa Dinas/Badan dan Perangkat Daerah bergeser atau bergerak dari kondisi saat ini menuju ke kondisi yang diharapkan. Karena itu, perubahan yang dikelola secara holistik, terstruktur dan berorientasi hasil akan sangat membantu organisasi, tim kerja dan individu/staf di dalamnya dalam menjalani "masa transisi" menuju kondisi birokrasi yang diinginkan, seperti Gambar 2 di bawah ini:

gambar 2
Kondisi birokrasi yang Diinginkan

Terdapat 4 (empat) dimensi dasar yang penting dan patut untuk diperhatikan dan dikelola dengan baik selama jalannya masa transisi atau perubahan, yaitu:

1. Navigasi. Dimensi ini terkait dengan perencanaan dan pengelolaan perubahan atau transisi dari keadaan organisasi sekarang menuju kondisi organisasi yang diinginkan
2. kepemimpinan. Dimensi ini berupaya untuk membangun dan mengkomunikasikan visi perubahan di dalam kondisi yang diinginkan dan juga mengarahkan organisasi ke arah yang dituju;
3. kepemilikan. Dimensi ini berupaya menciptakan kebutuhan untuk berubah melalui reformasi birokrasi;
4. Penggerak. Dimensi ini terkait dengan penyediaan kompetensi atau keahlian, struktur dan lingkungan pendukung serta sumber daya lain untuk mendukung perubahan dan memastikan manfaat (benefit) yang diharapkan dapat terealisasi.

Sebagai ilustrasi, perubahan yang dikelola dengan baik akan mengikuti kurva A, sedangkan yang tidak dikelola dengan baik atau tidak dikelola sama sekali akan mengikuti kurva B, dengan risiko menuju lembah "keputusasaan" (*valley of despair*), yaitu kurva C, seperti terlihat gambar Gambar 3.



gambar 3
kurva kinerja – Dengan dan tanpa Manajemen Perubahan

C. Elemen Dan Tahapan Manajemen Perubahan

1. Elemen Perubahan

Proses perubahan terdiri dari 3 (tiga) elemen yang saling berhubungan, yaitu:

a. Tujuan perubahan

Adalah untuk mengubah secara sistematis dan konsisten dari sistem dan mekanisme kerja organisasi serta pola pikir dan budaya kerja individu atau unit kerja di dalamnya menjadi lebih baik sesuai dengan tujuan dan sasaran reformasi birokrasi.

b. Perencanaan perubahan

Apabila kebutuhan dan tujuan perubahan sudah jelas, maka perlu menyusun rencana perubahan untuk selanjutnya diimplementasikan. Untuk dapat mencapai 8 (delapan) area perubahan yang diinginkan dalam pelaksanaan reformasi

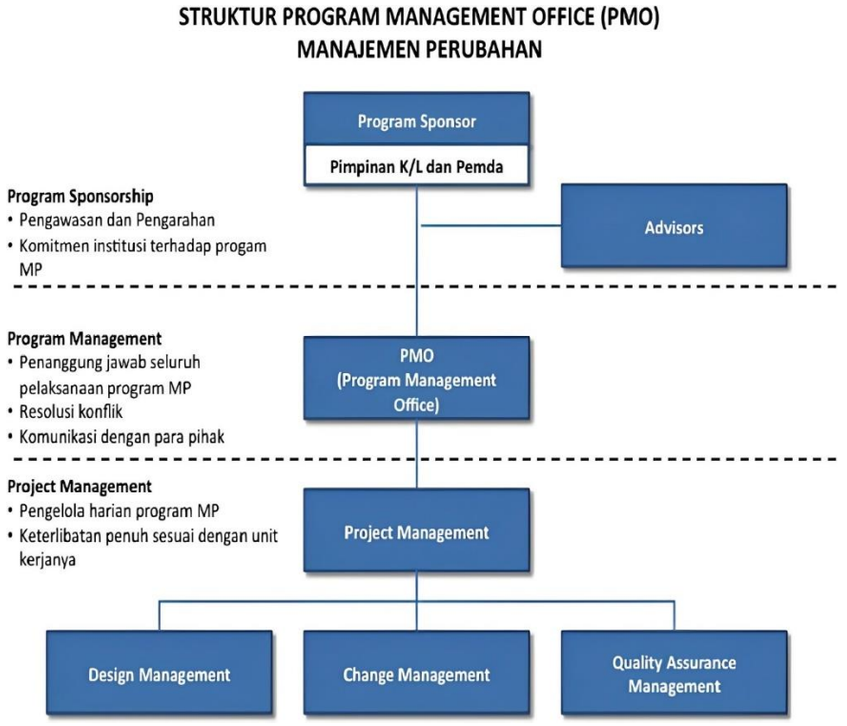
birokrasi, maka diperlukan perencanaan perubahan sebagai berikut:

1) Merencanakan strategi manajemen perubahan dan implementasi manajemen perubahan
   Dalam hal ini Dinas/Badan dan Perangkat Daerah harus menyusun rencana strategi perubahan dan implementasi manajemen perubahan. Rencana strategi perubahan disusun berdasarkan tujuan perubahan itu sendiri dan hasil perubahan yang diinginkan, seperti yang tertuang dalam *Grand Design* Reformasi Birokrasi 2010-2025. Rencana strategi juga harus mencakup area perubahan yang diinginkan, tim pengelola perubahan, waktu yang dibutuhkan, serta rencana anggarannya. Sedangkan implementasi manajemen perubahan adalah tahap melaksanakan rencana strategi perubahan yang sudah disusun oleh masing-masing Dinas/Badan dan Perangkat Daerah.
2) Membangun instrumen pengelolaan perubahan
   Mengingat besarnya agenda reformasi birokrasi dan proses perubahan yang akan dilakukan, maka penting untuk mengatur sistem pelaksanaan, sistem komunikasi, sistem monitor dan Evaluasi serta sistem pelaporan. Hal ini untuk memastikan proses perubahan berjalan sesuai dengan yang diharapkan.
3) Meningkatkan kapabilitas pengelola perubahan
   Meningkatkan kapabilitas pengelola perubahan merupakan salah satu kunci dalam melaksanakan perubahan. Ada berbagai macam cara untuk meningkatkan kapabilitas, misalnya melalui pelatihan ketrampilan berkomunikasi, menjadi fasilitator, menjadi motivator, menjadi mediator sampai dengan pelatihan membuat instrument sosialisasi dan internalisasi perubahan.

c. Tim pengelola perubahan
   Ada 3 (tiga) hal yang perlu dilakukan oleh tim pengelola perubahan, yaitu:
   1) Mendorong keinginan untuk berubah. Ada banyak hal yang bisa dilakukan untuk menciptakan keinginan berubah, antara lain:
      a) menciptakan *sense of urgency* dan kepedulian terhadap perubahan.
      b) memahami kepentingan dan ketakutan orang akan perubahan serta menyuarakan keberhasilan perubahan.
   2) Mengajak lebih banyak orang. Ada dua cara yang efektif untuk mengajak lebih banyak orang terlibat dalam proses perubahan, yaitu membangun strategi dan melaksanakannya secara reguler dan efektif memberikan tanggungjawab pada mereka yang terlibat, sehingga mereka merasa berkontribusi terhadap perubahan yang terjadi.
   3) Memelihara momentum. Proses perubahan dalam rangka reformasi birokrasi memerlukan waktu yang cukup lama. Oleh karena itu, bukan tidak mungkin antusiasme dan komitmen terhadap reformasi birokrasi menyusut atau menurun dan orang kembali pada cara kerja serta pola pikir

yang lama. Untuk itulah Perangkat Daerah perlu terus menumbuhkan dan memelihara momentum perubahan. Dua cara yang biasanya digunakan adalah mengembangkan kompetensi dan ketrampilan baru yang diperlukan dalam perubahan; memperkuat komitmen pegawai di masing-masing Perangkat Daerah secara berkala dan berkelanjutan.

Sedangkan model struktur tim pengelola perubahan atau biasa disebut *Program Management Office* (PMO) dapat digambarkan sebagai berikut



gambar 4
Struktur PMO Manajemen Perubahan

Program Management Office (PMO) dibentuk dalam rangka membantu tim reformasi birokrasi Dinas/Badan dan Perangkat Daerah. Oleh karena itu, diperlukan kerjasama dan kolaborasi yang erat antara tim PMO dengan tim reformasi birokrasi dan pejabat / pegawai lainnya.

Mengingat besarnya cakupan aktivitas dan pentingnya manajemen perubahan, maka struktur dan susunan tim PMO dalam melaksanakan program manajemen perubahan harus dapat mencerminkan kebutuhan tersebut. Melihat struktur di atas, maka dalam struktur tim pelaksana (*project management*) perlu ditambahkan 3 (tiga) sub tim, yaitu sub tim *Design Management*, sub tim *Change Management*, dan sub tim *Quality Assurance* (QA) *Management*. Setiap sub tim memiliki peran dan tanggung jawab masing- masing dalam pelaksanaan perubahan.

Sebagai contoh, sub tim *Design Management* memiliki peran dalam hal desain teknis program reformasi birokrasi. Sub tim *Change Management* berperan dalam hal persiapan teknis, pengembangan dan pelaksanan program manajemen perubahan, sedangkan sub tim QA Management berperan dalam memastikan kualitas perencanaan dan pelaksanaan program manajemen perubahan termasuk pemeriksaan kepatuhan akan realisasi dari perencanaan program. Oleh karena itu, orang yang masuk di

dalam sub tim harus sesuai dengan kriteria dan kompetensi pekerjaan yang dibutuhkan.

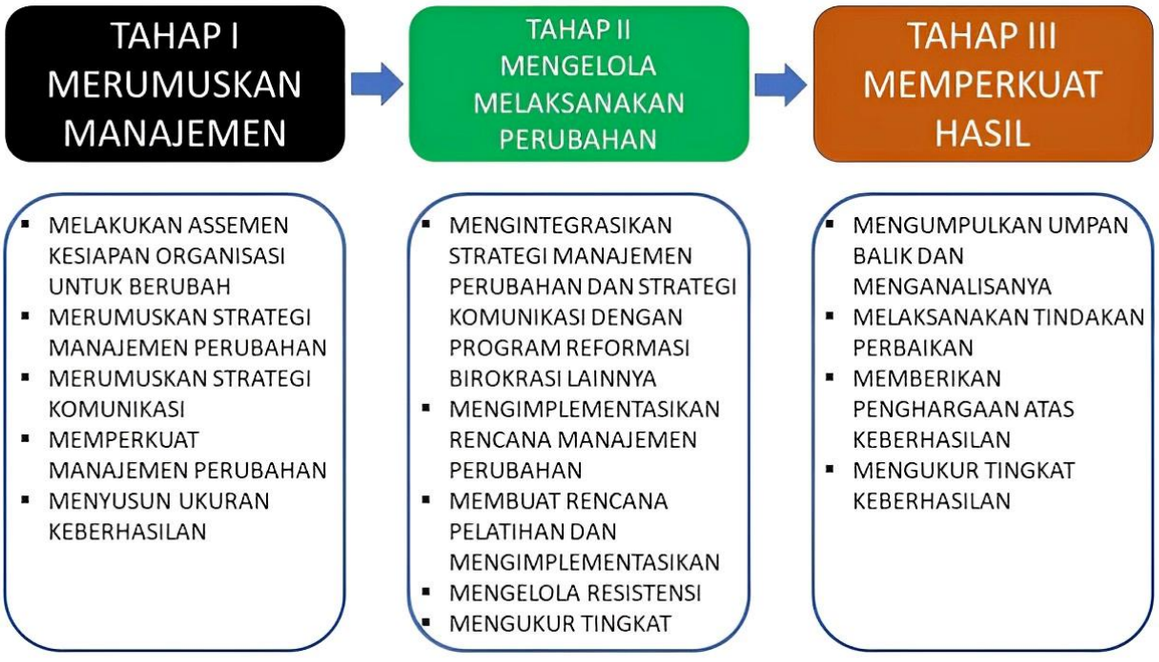
Sebagai ilustrasi pengorganisasian manajemen perubahan di Dinas/Badan dan Perangkat Daerah dapat dilihat pada Tabel 1.

Tabel 1
Ilustrasi Pengorganisasian Manajemen Perubahan

Tingkatan	Pemerintah Pusat	Pemerintah Daerah
Program Sponsorship	Pimpinan K/L	Gubernur/Bupati/ Walikota
Advisor	Sekjen /Sesma/Irjen	Sekda/Inspektur Prov/ Kab/Kota
Program Management	Dirjen/Deputi/ Ka Badan	Kepala SKPD
Project Manajement	Direktur/Ka Pusat/ Ka Kanwil/Ka Perwakilan	Ka Kantor/Kabid
Design Management, Change Management, dan *Quality Assurance Management*	Kasubdit/kabid	Kepala Seksi

2. Tahapan Perubahan

Tahapan perubahan dalam rangka pelaksanaan reformasi birokrasi di Dinas/Badan dan Perangkat Daerah dapat digambarkan sebagai berikut:



Gambar 5 Perubahan Tahapan

Secara komprehensif, langkaph-langkah penting yang harus dilaksanakan pada setiap tahap adalah sebagai berikut:

a. langkah-langkah yang harus dilakukan pada tahap-1:
   1) Melakukan pemetaan (*mapping*) terhadap para pemangku kepentingan dan melakukan asesmen atas pengaruh perubahan terhadap masing – masing pemangku kepentingan;
   2) Melakukan asesmen kesiapan perubahan, termasuk di dalamnya identifikasi penolakan terhadap perubahan;
   3) Melakukan asesmen terhadap tingkat partisipasi/dukungan para pemangku kepentingan dan kebutuhan akan komunikasi untuk manajemen perubahan, termasuk mengindentifikasikan penolakan terhadap perubahan;
   4) Melakukan asesmen terhadap organisasi, termasuk struktur, peran (*roles*) dan tanggung jawabnya (*responsibilities*);
   5) Melakukan asesmen terhadap kemampuan/kapabilitas dan *skills* organisasi untuk melaksanakan perubahan;
   6) Mengembangkan strategi manajemen perubahan, rencana dan aktivitas manajemen perubahan;
   7) Mengembangkan strategi dan rencana komunikasi;
   8) Mengembangkan strategi dan recana pelatihan, termasuk penetapan standard dan Indikator Kinerja Utama (IKU) Selain itu, langkah–langkah di bawah ini juga penting untuk dilakukan:
   9) Merumuskan manfaat (*benefit*) yang diperoleh dari hasil perubahan yang akan dilaksanakan;
   10) Memperkuat tim reformasi birokrasi Dinas/Badan dan Perangkat Daerah untuk lebih memahami manajemen perubahan, dan meningkatkan koordinasi dengan PMO; dan
   11) Merumuskan mekanisme internal pelaksanaan reformasi birokrasi pada masing-masing Dinas/Badan dan Perangkat Daerah termasuk sistem pelaksanaan, monitoring dan Evaluasi reformasi birokrasi serta pelaporan dan instrumen-instrumen yang diperlukan.

b. Langkah-langkah yang harus dilakukan pada tahap-2:
   1) Mengimplementasikan strategi, rencana dan aktivitas manajemen perubahan, termasuk tetap melakukan asesmen secara berkelanjutan terhadap pengarah perubahan pada masing-masing kelompok pemangku kepentingan;
   2) Mengimplementasikan strategi, rencana dan aktivitas komunikasi agar para pemangku kepentingan secara aktif terlibat (*engaged*), merasa memiliki proses perubahan dan mendorong perilaku dan pola pikir baru yang diharapkan dari proses perubahan serta mengurangi penolakan terhadap perubahan;
   3) Mengimplementasikan struktur organisasi yang baru, termasuk peran dan tanggung jawabnya yang baru untuk mendukung perubahan; dan
   4) Mengimplementasikan strategi, rencana dan aktivitas pelatihan untuk membekali para staf menjalani periode transisi dengan baik dan mengurangi penolakan.

Selain itu, langkah-langkah di bawah ini juga perlu untuk dilakukan:

1) Mengintegrasikan strategi manajemen perubahan dan strategi komunikasi dengan program dan kegiatan reformasi birokrasi sesuai *roadmap* reformasi birokrasi Dinas/Badan dan Perangkat Daerah;
2) Memberikan pengetahuan dan ketrampilan melalui asistensi dan fasilitasi yang diperlukan untuk membentuk ketrampilan, nilai-nilai, perilaku dan pola pikir baru (termasuk budaya kerja atau budaya organisasi yang baru) yang diharapkan dalam proses perubahan;
3) Mengimplementasikan manfaat yang telah dirumuskan agar perubahan dapat dirasakan secara positif oleh pemangku kepentingan;
4) Melakukan monitoring dan Evaluasi serta pelaporan atas pelaksanaan pengelolaan perubahan.

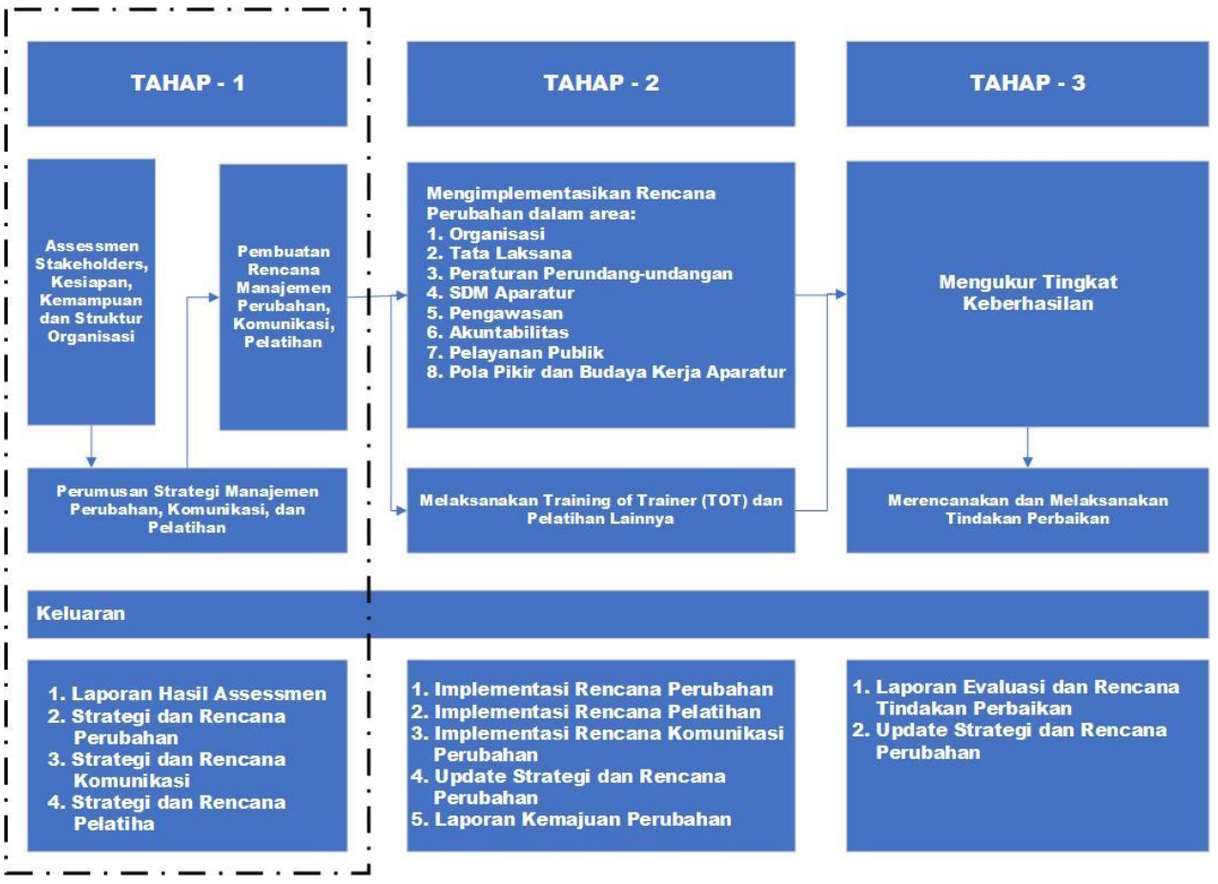
c. langkah-langkah yang harus dilakukan pada tahap-3:

1) Mengambil hikmah/pelajaran (*lesson learnt*) dari pelaksanaan keseluruhan strategi, rencana dan aktivitas manajemen perubahan, termasuk merumuskan dan melakukan koreksi atas perbaikan yang diperlukan, yang diperoleh dari:
   a) Pelaksanaan survei kepada para pemangku kepentingan yang terkena perubahan dan pengukuran tingkat keberhasilan;
   b) Kunjungan dan pengamatan ke unit-unit kerja yang melaksanakan proses perubahan; dan
   c) Umpan balik (*feedback*) secara langsung maupun tidak langsung yang diperoleh dari para pemangku kepentingan.
2) Melakukan Evaluasi terhadap efektivitas pelaksanaan strategi dan rencana komunikasi;
3) Melakukan Evaluasi terhadap strategi dan rencana pelatihan untuk mendukung perubahan;
4) Melakukan pemutakhiran atas Strategi dan Rencana Manajemen Perubahan berdasarkan Evaluasi di atas dan hikmah/pelajaran (*lesson learnt*) yang didapat;
5) Mengidentifikasi dan menyampaikan setiap keberhasilan kepada seluruh pejabat dan pegawai, melalui website/situs intranet; email blast; surat edaran; pidato dalam rapat; bulletin, dsb;
6) Memberikan penghargaan-penghargaan khusus kepada pegawai atau kelompok pegawai yang telah berhasil mengimplementasikan perubahan.

D. Perumusan Rencana Manajemen Perubahan

Pada bagian ini akan menguraikan secara lebih rinci tahapan dan juga kegiatan pokok yang menyertai tiap tahapan manajemen perubahan, meliputi:

1. Tahap Perumusan Rencana Manajemen Perubahan;
2. Tahap Pengelolaan/Pelaksanaan Perubahan; dan
3. Tahap Penguatan Hasil Perubahan.



Gambar 6
Perumusan rencana Manajemen Perubahan

Seperti yang sudah dijelaskan sebelumnya, tahap Perumusan Rencana Manajemen Perubahan akan difokuskan pada:

a. Asesmen terhadap para pemangku kepentingan dan tingkat partisipasi dan keterlibatan mereka terhadap perubahan;
b. Asesmen terhadap organisasi yang mencakup kesiapan organisasi untuk berubah, peran, struktur, tugas dan fungsi organisasi untuk mendukung perubahan;
c. Asesmen terhadap kemampuan dan kompetensi pegawai untuk mengelola perubahan;
d. Pendesainan rencana manajemen perubahan, komunikasi dan pelatihan; dan
e. Perumusan Manfaat (*Benefit*) yang akan diperoleh para pemangku kepentingan terhadap perubahan yang akan dilakukan.

1. Melakukan Pemetaan terhadap stakeholders (Pemangku Kepentingan)

Perangkat Daerah adalah organisasi publik yang memiliki banyak pemangku kepentingan. Pemangku kepentingan memiliki kekuatan, posisi penting, dan pengaruh terhadap isu yang berkaitan dengan perubahan. Oleh karena itu, di dalam Reformasi Birokrasi yang mengusung sejumlah perubahan yang signifikan, sangat penting bagi Perangkat Daerah mengenali para pemangku kepentingan berikut kebutuhannya. Pemangku kepentingan dapat dibagi menjadi:

a. Pemangku kepentingan utama

Pemangku kepentingan utama adalah pihak yang memiliki kaitan kepentingan secara langsung dengan suatu kebijakan, program, dan proyek. Mereka harus ditempatkan sebagai penentu utama dalam proses pengambilan keputusan;

b. Pemangku kepentingan pendukung

Pemangku kepentingan pendukung adalah pihak yang tidak memiliki kaitan kepentingan secara langsung terhadap suatu kebijakan, program, dan proyek, tetapi memiliki kepedulian dan keprihatinan sehingga mereka turut bersuara dan berpengaruh terhadap sikap masyarakat dan keputusan pemerintah.

c. Pemangku kepentingan kunci

Pemangku kepentingan kunci adalah pihak yang memiliki kewenangan secara resmi dalam hal pengambilan keputusan. Pemangku kepentingan kunci yang dimaksud adalah pengambil keputusan di Perangkat Daerah.

Format yang dapat digunakan untuk identifikasi pemangku kepentingan dapat dilihat pada Tabel 2:

Tabel 2
Identifikasi Awal Pemangku Kepentingan

No	Pemangku Kepentingan	Kaitan Kepentingan dengan kebijakan/progam/proyek		Memiliki Kewenangan	
		Langsung	Tidak Langsung	Resmi	Tidak Resmi
1					
2					
3					
4					
5					

Untuk melakukan pemetaan pemangku kepentingan berikut adalah antara lain beberapa pertanyaan yang harus dijawab:

- Siapa yang dapat atau mempunyai wewenang dalam pengambilan keputusan?
- Siapa yang mengendalikan perubahan?
- Siapa yang menjadi pendorong di belakang perubahan di masa lalu?
- Siapa yang akan mendapat manfaat secara langsung dari perubahan yang terjadi?
- Siapa yang tidak akan mendapat manfaat dari perubahan yang terjadi?
- Siapa yang akan mengontrol sumber daya yang dibutuhkan dalam perubahan?
- Siapa yang akan mempengaruhi para pemangku kepentingan lainnya?
- Siapa yang akan membantu suksesnya perubahan?

Jawaban atas pertanyaan-pertanyaan di atas akan berbeda-beda (meskipun akan ada yang sama) untuk setiap program reformasi birokrasi bahkan setiap kegiatan reformasi birokrasi.

Setelah melakukan identifikasi awal pemangku kepentingan seperti di atas, kemudian perlu dipetakan lebih lanjut bagaimana perubahan yang akan dilakukan akan memberikan dampak (*impact*) kepada para pemangku kepentingan dan bagaimana tingkat pengaruh atau kewenangan (*influence*) para pemangku kepentingan tersebut atas sukses atau mulusnya jalannya perubahan.

Tujuan dari pemetaan pemangku kepentingan adalah untuk melakukan asesmen dan memetakan para pemangku kepentingan terkait dengan peran dan kapasitas mereka dalam mempengaruhi keberhasilan jalannya perubahan agar berbagai kepentingan (*interests*) dari masing-masing pemangku kepentingan dapat teridentifikasi dengan baik. Selain itu, kegiatan ini juga berguna untuk melakukan prioritisasi para pemangku kepentingan berdasarkan tingkat kewenangan dan derajat dampak yang dimiliki sehingga strategi perubahan yang akan dibuat akan lebih efektif diimplementasikan.

Hasil yang diperoleh menjadi masukan penting bagi kegiatan asesmen terhadap kesiapan organisasi untuk berubah dan selanjutnya merupakan basis bagi pengembangan strategi perubahan dan strategi komunikasi.

2. Mengidentifikasi Resistensi atau Penolakan

Mengenali adanya resistensi atau penolakan dari pemangku kepentingan adalah hal yang penting untuk mengelola perubahan secara efektif. Secara umum resistensi atau penolakan terhadap perubahan berdasarkan sifatnya dapat digolongkan menjadi dua, yaitu:

a. Penolakan secara aktif atau terbuka.

   Penolakan secara terbuka biasanya lebih mudah ditangani. Biasanya orang akan menyatakan secara terbuka mengenai keberatan atau ketidak setujuan terhadap perubahan.

b. Penolakan secara pasif

   Penolakan ini biasanya muncul dalam bentuk simptom-simptom tertentu, seperti sering tidak hadir dalam rapat, tidak berpartisipasi dalam rapat, tidak memenuhi komitmen, produktivitas kerja menurun.

Resistensi atau penolakan terhadap perubahan berdasarkan pelakunya dapat digolongkan menjadi dua, yaitu:

a. Individual.

   Dalam sebuah proses perubahan resistensi individu tidak akan berpengaruh terlalu besar, kecuali individu tersebut adalah pejabat atau pimpinan tertinggi Dinas/Badan dan Perangkat Daerah.

b. Kolektif.

   Resistensi atau penolakan secara kolektif, akan sangat besar pengaruhnya terhadap proses perubahan.

Format yang dapat digunakan untuk mengidentifikasi resistensi atau penolakan dapat dilihat pada Tabel 3:

Tabel 3
Identifikasi Awal Resistensi Berdasarkan Sifat Dan Pelakunya

No	Pemangku Kepentingan	Kaitan Kepentingan dengan kebijakan/progam/proyek		Memiliki Kewenangan	
		Langsung	Tidak Langsung	Resmi	Tidak Resmi
1					
2					
3					
4					
5					

Setelah dilakukan identifikasi awal resistansi berdasarkan sifat dan pelakunya seperti di atas, kemudian tingkat resistensi para pemangku kepentingan dipetakan lebih lanjut ke dalam 3 (tiga) kategori, yaitu:

1. *Champion* (sangat mendukung perubahan dan tingkat resistansi perubahan yang sangat rendah);
2. *Floating Voter* (tingkat mendukung perubahan dan tingkat resistansi sama tinggi, tidak konsisten dan sewaktu – waktu dukungan perubahan atau resistansi dapat berubah); dan
3. *Blocker* (tidak mendukung perubahan sama sekali dan berpotensi melakukan sabotase terhadap perubahan yang akan dilakukan).

3. Mengenali besaran Perubahan yang Diinginkan

Untuk mengetahui seberapa besar upaya yang harus dilakukan oleh tim manajemen perubahan dalam mengelola perubahan, maka perlu dikenali dan diukur seberapa besar perubahan yang diinginkan.

Beberapa faktor yang perlu dipertimbangkan dalam mengukur besaran perubahan:

a. Seberapa kompleks perubahan yang akan dilakukan;
b. Jumlah kantor dan unit organisasi yang terlibat;
c. Jumlah pegawai yang terkena dampak perubahan dan hingga pada level apa tugas dan tanggung jawab mereka akan berubah;
d. Seberapa besar risiko yang harus dikelola.
e. Seberapa mudah diprediksi solusi perubahan yang akan diberikan;
f. Seberapa jelas dan konsisten pemahaman akan kondisi birokrasi yang diinginkan;
g. Apakah perubahan yang dilakukan bergantung pada pihak eksternal yang lain;
h. Seberapa besar tingkat resistansi terhadap perubahan.
i. Seberapa mampu Perangkat Daerah untuk melaksanakan perubahan;
j. Apakah kepemimpinan yang ada mendukung perubahan;
k. Apakah kepemimpinan yang ada memiliki kapabilitas dan kompetensi untuk mengelola perubahan;
l. Apakah Perangkat Daerah berpengalaman mengelola perubahan dengan sukses.
m. Seberapa mendesak (urgent) perubahan yang diinginkan

n. Apakah ada batas waktu yang dipersyaratkan untuk melaksanakan perubahan;
o. Kapan manfaat dari perubahan yang diharapkan dapat direalisasikan.
p. Cara menilai besaran perubahan dapat dilakukan melalui beberapa metode, antara lain:
   1) Studi dokumen, bila pernah terjadi perubahan sebelumnya; dan
   2) *Focused group discussion.*

4. Melakukan Asesmen kesiapan Organisasi untuk berubah

Reformasi Birokrasi dilaksanakan sebagai cara untuk mendorong perubahan ke arah yang lebih baik di Perangkat Daerah. Oleh karena itu perlu diukur seberapa besar kesiapan organisasi untuk melaksanakan dan menerima perubahan. Untuk mengukur kesiapan organisasi, biasanya digunakan kuesioner kesiapan organisasi menghadapi perubahan (*organization change readiness assessment*). Responden bisa diambil dari seluruh populasi atau diambil dengan cara sampel (bila cara sampel, maka semua posisi tunggal harus menjadi responden). Contoh kuesioner dimaksud disertakan dalam Standar dan Mekanisme Manajemen Sistem Pemerintahan Berbasis Elektronik.

Asesmen akan difokuskan pada beberapa elemen kunci di bawah ini:

a. Pemahaman terhadap visi, sasaran dan manfaat dari perubahan dalam kerangka reformasi birokrasi serta manfaat spesifik yang akan diperoleh oleh masing-masing kelompok pemangku kepentingan atas perubahan dimaksud;
b. Kepemimpinan, komitmen dan strategi untuk keseluruhan pengelolaan dan implementasi perubahan;
c. Apresiasi terhadap kebutuhan reformasi birokrasi yang difasilitasi oleh manajemen perubahan;
d. Persepsi para pemangku kepentingan terhadap *critical success factors* dan penghalang jalannya perubahan;
e. Kemauan para pemangku kepentingan untuk beradaptasi terhadap lingkungan atau kondisi yang baru serta potensi hambatan (*impediments*) yang dapat terjadi atas jalannya perubahan;
f. Pemahaman dan kesadaran terhadap dampak dari implementasi perubahan;
g. Tingkat partisipasi dari masing-masing pemangku kepentingan dan pengertian atas kebutuhan akan partisipasi lebih dalam terhadap implementasi keseluruhan perubahan;
h. Keefektifan dari pendekatan dan metode komunikasi yang ada saat ini.

Berdasarkan hasil asesmen maka potensi hambatan atas jalannya perubahan serta tingkat risikonya dapat teridentifikasi dengan baik. Risiko ini dapat mencakup:

a. Kurangnya kepemimpinan dan kurangnya partisipasi dan keterlibatan dari pemangku kepentingan kunci dan utama;

b. Adanya kebutuhan untuk peningkatan yang cukup signifikan atas kapabilitas atau *skill* untuk mengelola perubahan;
c. Pemahaman yang ada atas bagaimana masing-masing pemangku kepentingan merespon atau bereaksi atas perubahan yang akan dilakukan.

5. Mengembangkan strategi Perubahan

Fokus strategi perubahan adalah:

a. Memahami bagaimana perubahan akan berpengaruh ke manajemen organisasi, pegawai dan pemangku kepentingan yang lebih luas;
b. Memahami bagaimana perubahan akan berpengaruh ke budaya organisasi;
c. Mendefinisikan peran bahwa pimpinan dan pemangku kepentingan kunci seharusnya yang pertama berubah;
d. Membangun interaksi yang dapat membangkitkan komitmen perubahan dan perubahan benar-benar terjadi secara organisasional.

Secara umum ada 4 (empat) strategi dalam mengelola dan melaksanakan perubahan yang bisa dipilih sesuai dengan kondisi Perangkat Daerah. Keempat strategi dimaksud dapat dilihat pada Tabel 4 di bawah ini:

Tabel 4 Strategi Perubahan

STRATEGI MANAJEMEN PERUBAHAN	ASUMSI	FAKTOR YANG MEMPENGARUHI
1. Empirical-Rational	➢ Pegawai tergolong rasional dan selalu bergerak mengikuti kepentingan mereka. Oleh karenanya mereka dapat dibujuk ➢ Perubahan akan berhasil dengan komunikasi yang jelas dan insentif yang signifikan ➢ Bila insentif tidak sebanding dengan perubahannya, maka biasanya akan ada penolakan	➢ Strategi ini sangat dipengaruhi oleh besaran insentif ➢ Sulit diterapkan bila Insentif tidak signifikan

STRATEGI MANAJEMEN PERUBAHAN	ASUMSI	FAKTOR YANG MEMPENGARUHI
2. Normative-Reeducative	➢ Pegawai adalah makhluk sosial dan akan mematuhi norma-norma budaya dan nilai-nilai ➢ Perubahan akan berhasil bila didasarkan pendefinisian dan penafsiran kembali dari norma-norma dan nilai-nilai yang ada, untuk mengembangkan komitmen yang baru ➢ Sebagian besar pegawai ingin menyesuaikan diri dan mengikuti arus perubahan secara bersama-sama ➢ Hal terpenting dalam strategi ini, tim manajemen perubahan harus membangun dan menentukan arus perubahan yang diinginkan.	➢ Fokus perubahan pada strategi ini adalah perubahan budaya ➢ Budaya tidak akan berubah dalam waktu singkat. Oleh karena itu strategi ini bukan pilihan bila menginginkan dalam waktu cepat ➢ Akan berhasil bila hubungan dengan organisasi non-formal sebagai salah satu komponen pemangku kepentingan cukup harmonis
3. Power Coercive	➢ Pegawai pada dasarnya patuh dan melaksanakan apa yang diminta. ➢ Perubahan akan berhasi didasarkan pada pelaksanaan wewenang dan pemberlakuan sanksi. ➢ Strategi ini pada dasarnya adalah memperkecil pilihan. ➢ Berdasarkan pengalaman banyak pegawai juga merasa aman dan siap dengan strategi ini.	➢ Dua faktor utama yang mempengaruhi pilihan ini adalah jangka waktu perubahan yang ada dan keseriusan ancaman dampak perubahan. ➢ Biasanya *sense of urgency* terhadap perubahan sangat tinggi karena dihadapkan dengan waktu untuk berubah yang sangat sempit. ➢ Biasanya bila yang terancam adalah birokrasi organisasi, maka biasanya mereka akan segera menyesuaikan diri dengan perubahan ➢ Dalam strategi ini pemimpin harus memiliki kepemimpinan yang kuat, dan konsisten serta tepat dalam menghitung resiko, baik terhadap organisasi, pegawai maupun kepada sesama pemimpin.

STRATEGI MANAJEMEN PERUBAHAN	ASUMSI	FAKTOR YANG MEMPENGARUHI
4. Environmental Adaptive	➢ Pegawai akan selalu menghindari kerugian & gangguan tetapi mereka mudah beradaptasi dengan keadaan baru. ➢ Perubahan ini didasarkan pada kebutuhan membangun organisasi baru dan secara bertahap memindahkan orang dari yang lama ke yang baru ➢ Orang lebih cepat beradaptasi pada lingkungan baru dibandingkan dengan mengubah apa yang ada/apa yang sudah dijalani	➢ Pertimbangan utama adalah pada seberapa besar dan seberapa mendasar perubahan yang diinginkan. ➢ Sangat cocok untuk perubahan yang transformatif. ➢ Strategi ini dapat bekerja baik dalam waktu singkat maupun jangka waktu yang panjang ➢ Penting untuk dipertimbangkan adalah ketersediaan orang-orang yang kapabel dalam organisasi untuk membentuk organisasi dengan budaya baru

Beberapa faktor yang perlu dipertimbangkan dalam pemilihan strategi ini adalah:

a. Besaran perubahan yang akan terjadi atau yang diinginkan (merupakan hasil dari langkah pada sub-bagian B: Mengukur besaran perubahan yang diinginkan)
b. Besaran penolakan yang mungkin muncul (bisa dipahami dari hasil pada langkah sub-bagian C: asesmen kesiapan organisasi untuk berubah). Bila penolakan atau resistensi sangat tinggi, kombinasi strategi *power-coercive* dan *environmental adaptive* akan berhasil mendorong terjadinya perubahan. Sebaliknya bila resisten dan lemah, kombinasi strategi *rationale - empirical* dan *normative - educative* akan membawa perubahan yang diinginkan.
c. Jumlah atau populasi pegawai. Bila jumlah pegawai sangat besar, sangat beragam dan sebaran (demografi) yang sangat luas, memastikan pentingnya penerapan kombinasi keempat strategi yang ada.
d. Jangka waktu yang diperlukan dalam perubahan. Jangka waktu yang pendek dengan tingkat *urgency* yang tinggi, mendorong diterapkannya strategi power – *coercive.* Jangka waktu perubahan yang lebih lama penerapan kombinasi *rational-empirical*, *normative-reeducative*, dan *environmental- adaptive.*
e. Tenaga ahli. Bila organisasi memiliki tenaga ahli yang memadai dalam organisasi, maka kombinasi keempat strategi tersebut bisa diterapkan. Tetapi bila tidak ada tenaga ahli yang mendampingi dalam proses perubahan, maka biasanya strategi yang diterapkan adalah *power – coercive.*

Secara umum, tidak ada strategi manajemen perubahan tunggal, akan selalu ada kombinasi strategi manajemen perubahan. Bila melihat pada program dan kegiatan reformasi birokrasi, maka satu kegiatan dengan kegiatan lainnya akan memiliki strategi perubahan

yang berbeda. Oleh karena itu, dengan memahami strategi perubahan di atas, maka Perangkat Daerah akan dapat membuat pemetaan strategi manajemen perubahan, seperti contoh pada Tabel 5 sebagai berikut:

Tabel 5
Contoh Pemilihan strategi Perubahan

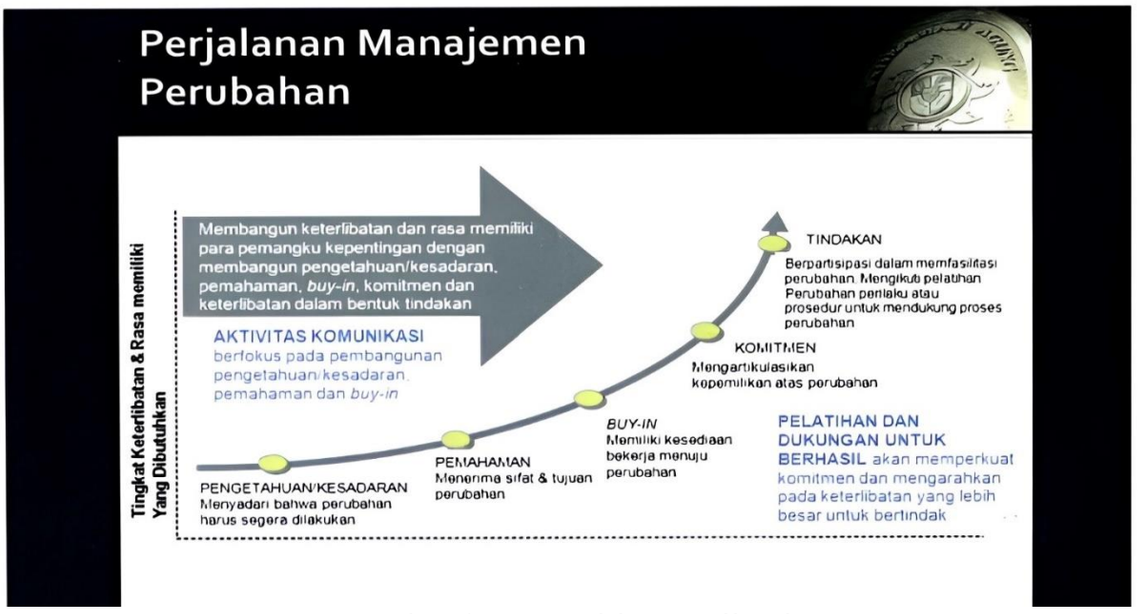
PROGRAM & KEGIATAN	STRATEGI MANAJEMEN			
	RATIONAL EMPIRICAL	NORMATIVE REDUCTATIVE	POWER - COERCIVE	ENVIROMENTAL-ADAPTIVE
Penataan Dan Penguatan Organisasi				
Redefinisi visi, misi dan strategi		Strategi - 2	Strategi - 1	
Restrukturisasi		Strategi - 2	Strategi - 1	Strategi - 3
Penguatan unit kerja pelaksana publik pelayanan		Strategi - 1		Strategi - 1

Strategi manajemen perubahan yang dipilih akan mempengaruhi strategi komunikasi yang akan dilaksanakan.

6. Mengembangkan strategi komunikasi

Tujuan utama pengembangan strategi komunikasi dalam manajemen perubahan adalah memfasilitasi terjadinya perubahan dalam perilaku. Strategi ini dikembangkan berdasarkan hasil pada sub-bagian A: mengidentifikasi dan melakukan analisis terhadap para pemangku kepentingan dan hasil pada langkah sub-bagian C: asesmen kesiapan organisasi untuk berubah.

Strategi komunikasi yang tepat akan membangun keterlibatan dan rasa memiliki dari seluruh pegawai dan juga para pemangku kepentingan lainnya terhadap perubahan yang dilaksanakan untuk mencapai hasil yang diinginkan. Berikut adalah gambaran perkembangan keterlibatan yang ditumbuhkan melalui proses komunikasi dalam manajemen perubahan.



gambar 7 strategi komunikasi

Perkembangan di atas akan tercapai bila prinsip pengembangan komunikasi dalam proses perubahan dipenuhi. Prinsip tersebut adalah:

a. Tentukan sumber tunggal untuk menetapkan dan menyetujui program komunikasi terkait tanggung jawab.
b. Pahami harapan para pemangku kepentingan dengan mengkomunikasikan tujuan program dengan jelas dan terus-menerus sepanjang proses pelaksanaan perubahan.“Selalu lakukan komunikasi”, untuk mengurangi kecemasan dan rasa ketidakpastian selama proses transformasi berlangsung.
c. Menjaga frekuensi komunikasi sepanjang durasi seluruh program.
d. Mengembangkan pesan yang tepat pada para pemangku kepentingan tertentu.
e. Mengkoordinasikan dan memaksimalkan media komunikasi yang sudah tersedia.

Faktor-faktor yang harus diperhatikan dalam pengembangan strategi komunikasi, adalah:

a. Kegiatan, jenis kegiatan apa yang akan dikomunikasikan?
b. Sumber daya (*resources*), berapa banyak anggaran yang dibutuhkan untuk mensosialisasikan kegiatan reformasi birokrasi ini? Sarana dan prasarana komunikasi apa yang diperlukan? Ketrampilan apa yang harus dimiliki untuk mengkomunikasikan kegiatan reformasi birokrasi ini?
c. *Timing*,berapa lama jangka waktu yang diperlukan untuk mengkomunikasikan? *Event* atau kesempatan khusus apa yang bisa digunakan sebagai media komunikasi?
d. Pesan kunci, pesan apa yang akan disampaikan pada *audience* – terkait problem yang dihadapi dan solusi yang ditawarkan dari reformasi birokrasi ini.
e. Evaluasi, bagaimana mengukur keberhasilan strategi komunikasi, termasuk bentuk perilaku apa yang diubah?
f. Sasaran, siapa yang menjadi sasaran komunikasi?
g. Komunikator, siapa yang akan menyampaikan pesan dalam komunikasi?
h. Media komunikasi, bagaimana kegiatan dan hasil reformasi birokrasi akan dipromosikan dan disosialisasikan? media komunikasi apa yang paling tepat untuk menjangkau audience?

Contoh format yang dapat digunakan untuk mengembangkan strategi komunikasi dapat dilihat pada Tabel 6 dan Tabel 7:

Tabel 6
Contoh Pengembangan strategi komunikasi

Kegiatan	*Kick-off* reformasi birokrasi
Anggaran yang dibutuhkan	Rp .....
Waktu yang dibutuhkan	3 bulan
Pesan yang disampaikan	➢ Bahwa Kementerian/Lembaga dan Pemerintah Daerah mengikuti proses reformasi birokrasi ➢ Latar belakang dan tujuan yang ingin dicapai melalui reformasi birokrasi ➢ Dukungan apa yang dibutuhkan dari pejabat, pegawai dan pemangku kepentingan lain dalam proses reformasi birokrasi ➢ Ukuran keberhasilan reformasi birokrasi ➢ Kementerian/Lembaga atau Pemerintah Daerah ➢ Jangka waktu proses pelaksanaan reformasi birokrasi ➢ Tim reformasi birokrasi Kementerian/Lembaga atau Pemerintah Daerah

Selanjutnya pemilihan media komunikasi untuk disampaikan oleh komunikator sesuai sasaran masing-masing dapat dilihat pada Tabel 7 di bawah ini:

Tabel 7
Contoh strategi komunikasi

SASARAN	KOMUNIKATOR	MEDIA KOMUNIKASI									
		Buku	Rapat	talkshow	Artikel di	Newsletter	Konferensi	Website	Memo	Rapat	Rapat Kerja
Pimpinan/Pejabat Kementerian/ Lembaga atau Pemerintah Daerah	Pimpinan tertinggi	✔	✔			✔		✔			
Seluruh pejabat dan pegawai		✔				✔		✔	✔	✔	✔
Pers/media	Pimpinan tertinggi; tim Reformasi birokrasi	✔					✔	✔			
Pemangku kepentingan Utama	Pimpinan tertinggi; Tim reformasi birokrasi	✔		✔	✔			✔			
Pemangku kepentingan pendukung	Tim reformasi birokrasi	✔		✔	✔			✔			
Pemangku kepentingan	Pimpinan tertinggi	✔		✔	✔			✔			
Target jumlah Sesi/jumlah buku Jumlah penayangan/ jumlah *newsletter*		....	....	....	....	....	....	....	....	....	....

Hal terpenting dalam tahap merumuskan rencana manajemen perubahan adalah :

a. Memahami reformasi birokrasi dan tujuan yang ingin dicapai;
b. Mempersiapkan tim reformasi birokrasi Dinas/Badan dan Perangkat Daerah untuk dapat mengelola manajemen perubahan;
c. Memastikan kepemilikan dari proses perubahan. Dalam kaitan reformasi birokrasi, maka pimpinan tertinggi Dinas/Badan dan Perangkat Daerah haruslah menjadi pemilik manajemen perubahan ini;
d. Mempersiapkan sumberdaya yang dapat mendukung pelaksanaan manajemen perubahan;
e. Melakukan asesmen untuk mengetahui kondisi terkini organisasi dan kesiapannya untuk melakukan perubahan;
f. Mencari referensi pada Dinas/Badan dan Perangkat Daerah atau organisasi lain yang sudah berhasil melakukan pengelolaan perubahan.

7. Merumuskan dan Mendefinisikan Struktur Yang Baru

Struktur di dalam organisasi termasuk fungsi, peran dan tanggung jawabnya perlu diselaraskan dengan perubahan menuju kondisi yang diinginkan. Dalam melakukan perubahan struktur juga diperlukan pemahaman atas Peraturan Perundang–undangan atau regulasi yang menaunginya agar desain organisasi yang baru untuk mendukung perubahan tetap di dalam koridor hukum yang diizinkan.

Dalam mendefinisikan struktur yang baru, perlu dilakukan terlebih dahulu asesmen terhadap hal di bawah ini, antara lain:

a. Peraturan yang melingkupi perubahan struktur;
b. Lingkungan strategis yang melingkupi organisasi;
c. Rencana strategis organisasi;
d. Struktur organisasi yang ada saat ini;
e. Faktor sukses kritis (*critical success factor*) organisasi dalam mencapai tujuan dan sasaran organisasi;
f. Proses Bisnis organisasi; dan
g. Sumber daya manusia dan pengelolaannya di dalam organisasi
h. Setelah dilakukan asesmen terhadap organisasi, kemudian dirumuskan dan didefinsikan bentuk struktur organisasi yang baru beserta fungsi, peran, tugas dan tanggung jawabnya yang baru.

8. Mengembangkan Strategi Pelatihan

a. Ruang lingkup pelatihan;
b. Target peserta atau kelompok pemangku kepentingan, yang memiliki tingkatan, posisi, tugas dan tanggung jawab serta kemampuan (*skills*) yang berbeda – beda;
c. Nama dan jenis pelatihan. Jenis pelatihan harus mencakup sisi atau aspek *non-technical (soft skills)* yang mendukung tercapainya kesuksesan perubahan disamping aspek *technical skills* yang dibutuhkan oleh para staf untuk mampu bekerja dalam suatu lingkungan yang baru hasil dari perubahan struktur organisasi, Proses Bisnis dan sistem;

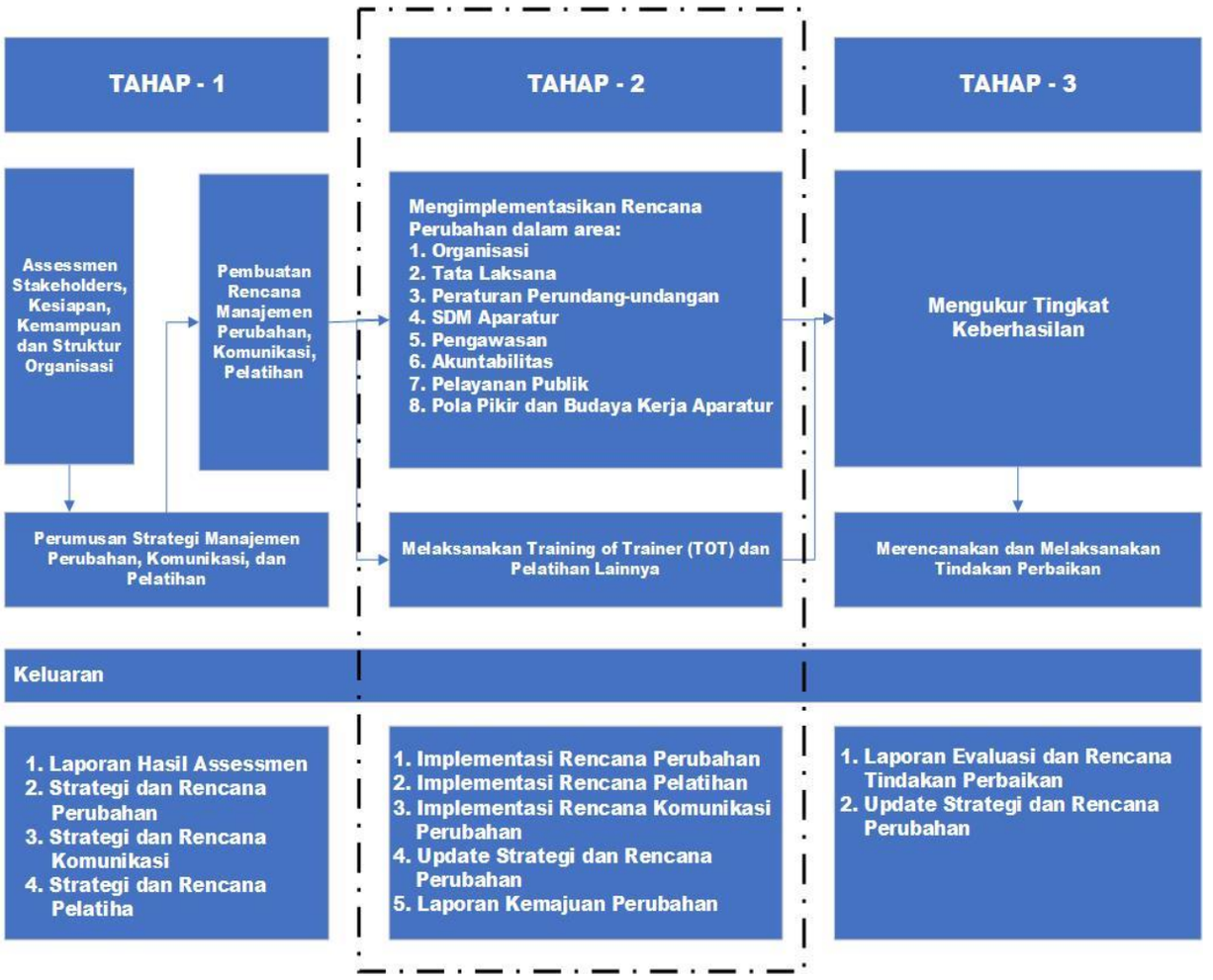
d. Sistematika pelatihan secara makro yang berisikan sasaran pelatihan (*key learning objectives*), lamanya waktu pelatihan, metoda pelatihan (antara lain, studi kasus, *exercise, role-play*) dan kriteria kesuksesan (*success criteria*) serta bagaimana mengukur kesuksesan tersebut;
e. Estimasi jumlah sesi yang dibutuhkan untuk tiap pelatihan beserta penentuan lokasi pelatihannya;
f. Estimasi jumlah peserta per pelatihan;
g. Estimasi biaya yang dibutuhkan.

Keluaran utama (*Major Output*) pada Tahap 1 adalah sebagai berikut:

a. Laporan Hasil Asesmen, seperti:
    1) Asesmen Kesiapan Perubahan;
    2) Pemetaan Pemangku Kepentingan dan Analisis Dampak Perubahan;
    3) Asesmen Keterlibatan Pemangku Kepentingan dan Kebutuhan Akan Komunikasi;
        a) Asesmen Kapabilitas Organisasi Saat Ini dan
        b) Assesmen Struktur Organisasi
b. Strategi dan Rencana Perubahan
c. Strategi dan Rencana Komunikasi Untuk Perubahan;
d. Strategi dan Rencana Pelatihan Untuk Perubahan.

E. Pengelolaan/Pelaksanaan Perubahan

Sebagaimana diuraikan dalam perumusan rencana manajemen perubahan, pengelolaan/pelaksanaan perubahan merupakan tahap kedua dalam penerapan manajemen perubahan. Tahap pengelolaan/pelaksanaan perubahan akan difokuskan pada pengimplementasian strategi dan rencana perubahan untuk mendukung pelaksanaan area perubahan yang terjadi pada reformasi birokrasi yang ditetapkan di dalam Peraturan Bupati Natuna Nomor 23 Tahun 2021 tentang *Road Map* Reformasi Birokrasi di Lingkungan Pemerintah Daerah Tahun 2020-2024 Implementasi rencana pelatihan, komunikasi untuk perubahan dan mengelola resistensi menjadi salah satu elemen pokok di dalam tahap ini.



gambar 8
Pengelolaan/Pelaksanaan Perubahan

1. Mengintegrasikan *Roadmap* Perangkat Daerah dengan strategi Perubahan dan strategi komunikasi

   Perangkat Daerah harus melaksanakan 56 (lima puluh enam) kegiatan reformasi birokrasi sebagaimana tertuang di dalam Peraturan Bupati Natuna Nomor 23 Tahun 2021 tentang *Road Map* Reformasi Birokrasi Di Lingkungan Pemerintah Daerah Tahun 2020-2024. Kelima puluh enam kegiatan ini harus didukung oleh strategi dan recana perubahan dan komunikasi yang telah disusun pada tahap sebelumnya.

   Pedoman manajemen pengetahuan memberikan contoh integrasi program pelaksanaan reformasi birokrasi dengan Strategi Perubahan dan Strategi Komunikasi. Dalam integrasi ini ada tiga tahapan proses komunikasi, yaitu sebelum pelaksanaan kegiatan; saat pelaksanaan kegiatan dan saat kegiatan selesai dilaksanakan.

2. Mengelola resistensi/Penolakan

   Berikut adalah beberapa cara untuk mengelola atau mengatasi resistensi/ penolakan:

   a. Mengkomunikasikan alasan-alasan rasional atas keputusan pimpinan melaksanakan reformasi birokrasi;
   b. Melibatkan pihak yang resisten dalam proses perubahan dan proses pengambilan keputusan;

c. Memfasilitasi dan memberikan dukungan melalui asistensi, pelatihan, dan sebagainya;
d. Memaksa pihak yang resisten atau menolak untuk menerima
e. perubahan, dan apabila diperlukan diberikan sanksi. Perlu diingat, bahwa cara ini adalah cara terakhir bila cara lain tidak berhasil.

Berikut adalah beberapa hal yang disarankan ketika berhadapan dengan resistensi atau penolakan:
a. Jangan berfokus pada resistensi atau penolakan ketika itu belum menjadi masalah;
b. Fokus untuk melihat bahwa perubahan ini bisa terus berjalan;
c. Berlakulah normal ketika resistensi dan penolakan terjadi;
d. Fokus apa yang sudah dicapai saat ini;
e. Lakukan terus apa yang telah berjalan dengan baik.

Cara untuk mengatasi resistensi dalam melaksanakan perubahan secara lebih lengkap dapat dilihat pada Tabel 8 di bawah ini:

Tabel 8
beberapa Cara Mengatasi resistensi Dalam Melaksanakan Perubahan

NO	TAKTIK	PENJELASAN
1	Jangan berfokus pada resistensi ketika itu belum menjadi masalah	Proses perubahan biasanya diawali dengan pesimisme. Banyak mendengar dan memikirkan pesimisme akan mempengaruhi sikap dan perilaku terhadap perubahan. Cara melawan pesimisme adalah dengan menumbuhkan optimisme. Tidak akan ada sebuah perubahan tanpa mencoba dan menjalani. Bila memang terjadi, maka seharusnya ini menjadi bagian dari resiko yang memang diperhitungkan, maka tindakan perbaikan baru perlu diambil.
2	Fokus untuk melihat bahwa perubahan ini bisa terus berjalan	Dengan memusatkan perhatian dan percaya bahwa perubahan akan terus berjalan, sering bekerja sangat baik karena memperkuat optimisme.
3	Berlakulah normal ketika penolakan terjadi	Ketika resistensi dan penolakan terjadi, berlakulah bahwa ini suatu kondisi yang memang sudah diperkirakan dan ini adalah sesuatu yang normal terjadi dalam sebuah proses perubahan. Sikap ini sangat penting untuk membantu mencegah orang menjadi patah semangat dan kehilangan kepercayaan terhadap perubahan.

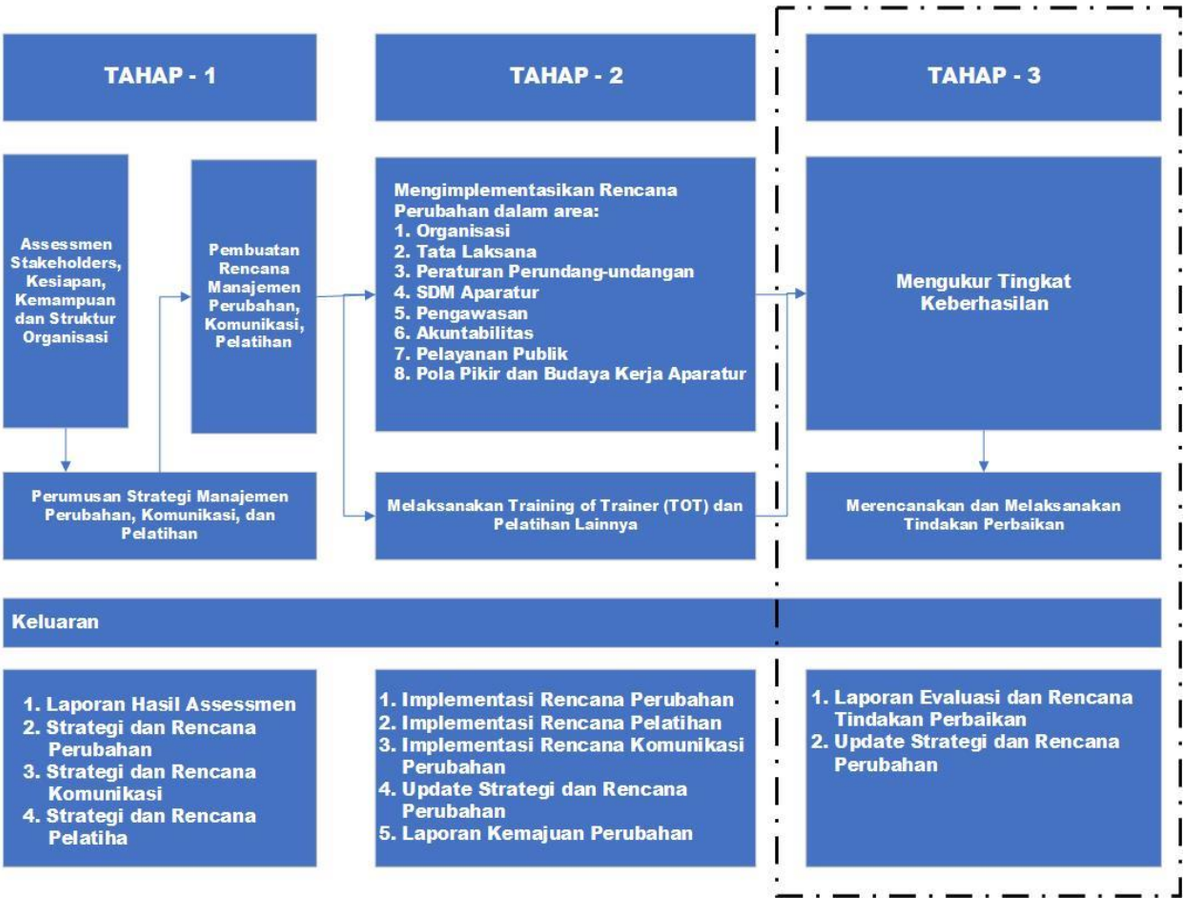
4	Fokus apa yang sudah dicapai saat ini	Sangat penting untuk memikirkan juga pada pencapaian yang sudah didapat, ketika persoalan dalam proses perubahan terjadi. Dengan melakukan ini biasanya orang akan menyadari bahwa lebih banyak hal yang telah berjalan baik daripada yang mereka pikir dan mereka biasanya menemukan keyakinan baru, optimisme dan fokus. Lebih jauh lagi, mereka menemukan ide-ide baru untuk mendapatkan perubahan dan mulai membuat kemajuan
5	Lakukan terus apa Yang telah berjalan dengan baik	Pikirkanlah apa-apa atau tindakan-tindakan yang telah berhasil dilakukan, sehingga ketika kesulitan datang – situasi dapat dengan cepat diatasi.

Keluaran utama Tahap 2 adalah sebagai berikut:

a. Implementasi Rencana Perubahan (*Change Plan*);
b. Pelaksanaan Pelatihan dan *Workshop* Manajemen Perubahan, termasuk Materi Pelatihan;
c. Pelaksanaan Program Pelatihan TOT (*Training of the Trainer*);
d. *Update* terhadap Strategi dan Rencana Perubahan;
e. Pelaksanaan Strategi dan Rencana Komunikasi Perubahan;
f. *Workshop* dan Program Pelatihan untuk Manajemen Komunikasi;
g. *Status Report* dan *update* yang berisikan antara lain:
    1) Keberhasilan dan hambatan;
    2) Rekomendasi perbaikan dan tindakan perbaikan.

F. Penguatan Hasil Perubahan

Sebagaimana diuraikan dalam perumusan rencana manajemen perubahan, Penguatan Hasil Perubahan merupakan tahap ketiga dalam penerapan manajemen perubahan. Tahap Penguatan Hasil Perubahan difokuskan pada pengukuran kemajuan atau tingkat keberhasilan perubahan yang dikaitkan area perubahan yang ditetapkan di dalam Peraturan Bupati Natuna Nomor 23 Tahun 2021 tentang *Road Map* Reformasi Birokrasi di Lingkungan Pemerintah Daerah Tahun 2020-2024, dan rencana serta tindak lanjut perbaikan atas hasil reviu dan Evaluasi pelaksanaan perubahan.



gambar 9
Penguatan hasil Perubahan

Beberapa kegiatan yang dilakukan dalam tahap ini merupakan bagian dari kegiatan monitoring dan Evaluasi. Kegiatan tersebut adalah:

a. Mengukur tingkat keberhasilan dari pelaksanaan rencana manajemen perubahan;
b. Mengumpulkan dan menganalisis umpan balik dengan cara melakukan kunjungan lapangan dan mengevaluasi pelaksanaan manajemen perubahan;
c. Mendiagnosa kembali kesenjangan dan mengelola penolakan yang terjadi dalam pelaksanaan manajemen perubahan;
d. Mengimplementasikan tindakan perbaikan dan membuat langkah tindak lanjut untuk keberlanjutan proses perubahan;
e. Memberikan penghargaan kepada pegawai yang berhasil mengimplementasikan perubahan dengan baik.

Tahap dan langkah penguatan hasil perubahan beserta keluarannya secara lebih lengkap dapat dilihat pada Tabel 9 di bawah ini:

Tabel 9
langkah Penguatan hasil Perubahan

TAHAP	LANGKAH	KELUARAN
Mengumpulkan dan menganalisis umpan balik Mendiagnosa kembali kesenjangan dan mengelola penolakan	Evaluasi pelaksanaan secara periodik Kunjungan ke unit kerja secara periodik untuk memastikan implementasi Survei implementasi secara periodik	Dokumen yang berisi, antara lain: Hasil Evaluasi Tingkat efektifitas
Mengimplementasikan tindakan perbaikan dan merayakan keberhasilan	Koreksi /aktivitas perbaikan bila Diperlukan Menyampaikan setiap keberhasilan kepada seluruh pejabat dan pegawai, melalui *website*/situs *intranet*, *email blast*; surat edaran; pidato dalam rapat; bulletin, dan sebagainya. Memberikan penghargaan khusus kepada pegawai atau kelompok pegawai yang telah berhasil mengimplementasikan perubahan	Dokumen yang berisi, antara lain: Rekomendasi perbaikan Daftar champions Penghargaan (*Rewards*)

Keluaran Utama Tahap 3 adalah sebagai berikut:

a. Pemutakhiran Strategi dan Rencana Perubahan;
b. Pemutakhiran Strategi dan Rencana Komunikasi untuk Perubahan;
c. Pemutakhiran Strategi dan Rencana Pelatihan;
d. Status *Report*, Evaluasi dan tindakan perbaikan berdasarkan hasil Evaluasi dan *feedback* yang diterima.

G. Membuat Perubahan Berkelanjutan

Membuat perubahan agar tetap berkelanjutan pada prinsipnya adalah mengakselerasi manfaat (*benefit*) yang telah didefinisikan sebelumnya, yang dapat dirasakan sepanjang atau selama mungkin walau kegiatan manajemen perubahan telah berakhir.

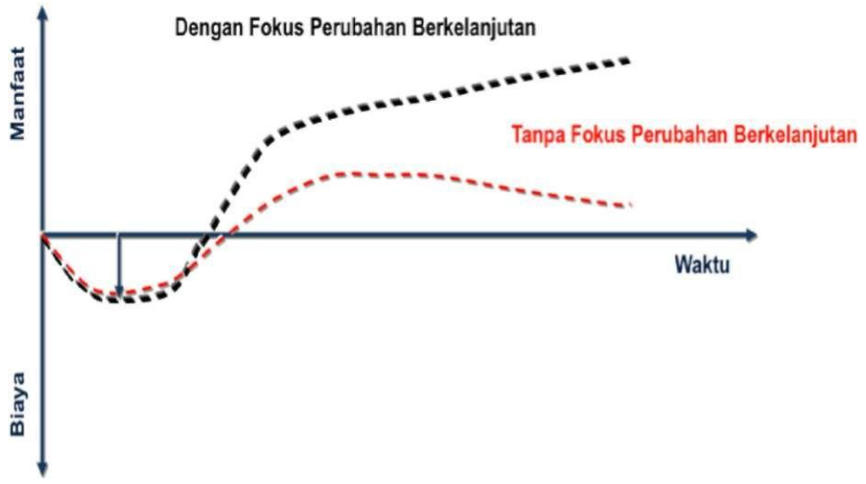
Untuk membuat hal ini terjadi, beberapa pendekatan di bawah ini dapat dilakukan oleh Kementerian/Lembaga dan Pemerintah Daerah:

a. Fokuskan pada manfaat yang didapat dari perubahan ini dan lakukan monitoring dan pengukuran untuk memantau proses realisasi manfaat ini
b. Mendorong partisipasi dan keterlibatan para pegawai yang terkena perubahan dan/atau yang melaksanakan perubahan dalam pekerjaan sehari – harinya dan memastikan terjadinya komunikasi yang efektif guna mendukung perubahan dan keseimbangan kegiatan

perubahan yang dikendalikan manajemen dengan ide atau usulan dari para pegawai

c. Membangun keberlanjutan (*sustainability*) dengan memantapkan dan memformalkan cara-cara atau mekasnisme baru ke dalam proses dan sistem manajemen kinerja dan pelatihan yang mendukung perubahan dan perolehan manfaat

Ilustrasi pentingnya perubahan keberlanjutan dapat dilihat pada kurva sebagaimana Gambar 10 di bawah ini:



gambar 10
kurva keberlanjutan Perubahan

Program manajemen perubahan menjadi salah satu faktor suksesnya pelaksanaan reformasi birokrasi, dan dimaksudkan untuk membantu meningkatkan capaian keberhasilan pelaksanaan reformasi birokrasi secara efektif dan efisien. Oleh karena itu, pedoman ini adalah untuk memandu Perangkat Daerah supaya dapat melaksanakan program manajemen perubahan secara baik dan benar.

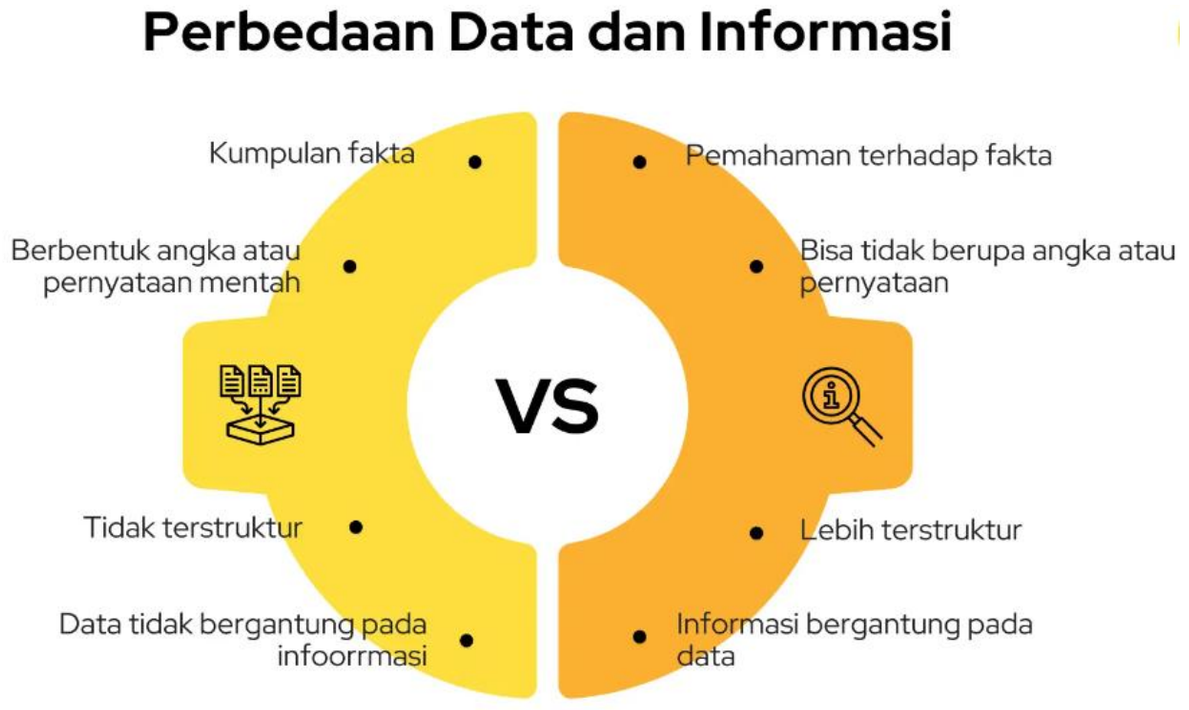
BAB VII
MANAJEMEN DATA

A. Pendahuluan

Manajemen Data SPBE Daerah disusun sebagai pedoman untuk menjamin terwujudnya Data yang akurat, mutakhir, terintegrasi dan dapat diakses sebagai dasar perencanaan, pelaksanaan, Evaluasi dan pengendalian pembangunan daerah. Manajemen Data SPBE Daerah dilaksanakan melalui serangkaian proses pengelolaan Arsitektur Data, Data Induk dan Data Referensi, Basis Data dan Kualitas Data. Manajemen Data SPBE Daerah dilaksanakan agar Pemerintah Daerah agar :

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

Penyelenggaraan Manajemen Data SPBE Daerah dilaksanakan oleh Penyelenggara Satu Data Daerah sesuai tugas dan fungsinya berdasarkan prinsip SDI. Penyelenggara Satu Data Daerah bertanggung jawab atas keakuratan Data dan Informasi yang disediakan serta keamanan Data dan Informasi yang bersifat strategis dan/atau rahasia. Penggunaan Data dan Informasi dilakukan dengan mengutamakan bagi pakai Data dan Informasi antar Perangkat Daerah, Instansi Pusat, dan/atau Pemerintah Daerah lain berdasarkan tujuan dan cakupan, penyediaan akses Data dan Informasi, dan pemenuhan standar Interoperabilitas Data dan Informasi.



Gambar 1 Perbedaan Data dan Informasi

Pemahaman dasar tentang Data, informasi dan pengetahuan adalah kunci bagaimana memahami Data. Kadang sering tertukar mana Data dan mana informasi. Yang pasti informasi adalah Data yang telah diolah sehingga memiliki makna. Mengolah Data adalah memberikan konteks atau melakukan agregasi seperti jumlah, rata rata, maksimum, minimum atau statistik lainnya.

Data dalam hal teknis dapat dimaknai sebagai tabel dengan single kolom, artinya tidak terdapat kolom bertingkat yang menjadi nama kolom atau header kolom. Kembali ke konsep awal, Data adalah fakta tentang sesuatu. Fakta tentang meja adalah warna, bentuk, tinggi, lebar, bahan, harga dan seterusnya. Sebuah fakta tentang meja yang dapat dilihat dan diperhatikan.

Kode Benda	Nama Benda	Bentuk	Tinggi	Berat	Warna	Harga

Dalam mengelola Data hal yang perlu diperhatikan adalah memahami tujuannya. Tujuan mengelola Data adalah menyediakan Data yang valid, akurat, akuntable, sehingga dapat diolah menjadi informasi atau pengetahuan yang membantu mengambil keputusan untuk bertindak.

Idenya sederhana, namun implementasinya tidak semudah ide yang ada. Permasalahan Data yang dihadapai oleh Indonesia adalah:

1. Jenis Data apa yang harus dipublish di portal?
2. Apa standar format Data yang akan dipublish?
3. Apa yang menjadi Metadata?
4. Siapa yang akan memanfaatkan Data tersebut ?
5. Siapa yang menghasilkan Data tersebut ?
6. Siapa yang memvalidasi dan memutakhirkan Data ?
7. Bagaimana menghilangkan ego sektoral sehingga tidak mau berbagi Data ?

Mungkin belum terwakili seluruh permasalahan Data di Indonesia, namun dari masalah yang ada, tentu saja dapat dicari suatu solusi akan Data. Maka lahirlah Peraturan Presiden Nomor 39 tahun 2019 tentang SDI. Setidaknya ada solusi secara makro untuk menyelesaikan masalah.

Tujuan dari Peraturan Presiden SDI adalah:

"**Mendorong pemanfaatan** Data **untuk pengambilan kebijakan dengan fondasi Data yang akurat, mutakhir, terpadu, terbuka dan Interoperasional**"

Jika didefinisikan dalam uraian singkat maka akan menjadi karakter Data pemerintah, sebagai berikut:

1. Data Pemerintah yang akurat dan mutakhir
2. Data Pemerintah yang Terpadu dan Terbuka
3. Data Pemerintah yang bisa berbagi pakai (interoperasional)

Wujud fisik yang dapat dilihat dari Peraturan Presiden SDI adalah Portal SDI, yaitu sebuah situs web yang mencoba untuk mempublish Data Indonesia.

Adapun indikator keberhasilan dari Peraturan Presiden SDI adalah:

1. Tingkat Pemenuhan Standar Data
2. Tingkat Pemenuhan Metadata
3. Tingkat Pemenuhan Kode Referensi Data Data Induk
4. Tingkat Aksesabilitas
5. Tingkat Ketersediaan
6. Tingkat Keterpaduan
7. Tingkat Interoperabilitas

Tujuan dan Indikator sudah jelas, maka langkah selanjutnya dalam Peraturan Presiden SDI adalah siapa yang melaksanakannya atau istilahnya orang-orang atau bidang yang terkait siapa saja. Terdapat pengelompokan stakeholder dalam Peraturan Presiden SDI, yaitu:

1. Pengarah Data
   Institusi yang bertugas mengarahkan tentang Data apa yang dipublish, Metadatanya, standar datanya. Yang masuk dalam lingkup ini adalah
   a. Bappenas (pusat) dan Bappeda dan Litbang Kabupaten Natuna, untuk Data Sektoral
   b. Badan Pusat Statistik, untuk Data Statistik
   c. Badan Infomasi Geospasial, untuk Data Geospasial
2. Produsen Data
   Institusi yang bertugas menghasilkan data, dan bertanggung jawab terhadap validitas dan ketersediaan Data. Yang masuk dalam lingkup ini adalah:
   a. Kementerian
   b. Perangkat Daerah
3. Wali Data
   Institusi yang bertugas menyebarluaskan Data, untuk dapat dimanfaatkan oleh sistem lain. Yang termasuk dalam lingkup ini adalah
   a. Kementerian Komunikasi dan Informatika
   b. Dinas Komunikasi dan Informatika

Maka jika tujuan, indikator dan stakeholder telah ditetapkan dalam Peraturan Presiden SDI, maka tinggal ditataran eksekusi yang akan menjadi kendala atau langkah berikutnya.

Dan jangan lupa, bahwa Portal SDI *Readable*, artinya Data yang terpublikasi disana akan dikonsumsi oleh mesin atau sistem, bukan oleh orang secara langsung.

Pemahaman ini menjadi kunci, sehingga dalam mempublish Data di portal Data, terdapat kesamaan persepsi terhadap format Data terbuka, seperti excel, txt, csv, atau API yang dapat dibaca langsung oleh mesin.

Jadi Portal Data ini akan menjadi sumber Data bagi pengolah Data yang akan memproduksi informasi. Perlu dipahami langkah menghasilkan informasi atau bahkan pengetahuan membutuhkan proses, yang antara lain adalah:

1. Menentukan Sumber Data
   Salah satu yang menjadi acuan dan memiliki sifat terbuka serta interoperabilitas adalah Portal Data.
2. Mengolah Data
   Sebuah mesin atau algoritma yang mampu melakukan agregasi atau penerapan *pattern* sehingga memunculkan Deskripsi, Diagnosa dan Prediksi.

3. Menampilkan Data
   Menyajikan hasil olahan Data ke dalam bentuk yang mudah dipahami dan dimengerti oleh siapapun. Bentuk ini biasanya kita kenal dengan grafik dan *dashboard*.

Jika melihat portal Data pemerintah khususnya di daerah, karena sekarang masing-masing memiliki portal Data sendiri-sendiri dan menjadi sebuah prestasi atau penilaian, banyak sekali ketidakseragaman dalam format Data, jenis Data, Metadata dan standar Data.

Hal ini terjadi karena interpretasi yang tidak sama terhadap Peraturan Presiden SDI, yang biasanya Pemerintah Daerah menunggu peraturan di level teknis.

Namun jika mampu memahami dengan baik apa itu esensi Data dan informasi, maka sebenarnya Pemerintah Daerah sudah dapat melakukan aksi dengan benar sebagai langkah awal.

B. Maksud dan Tujuan

Maksud pengaturan Pedoman Manajemen Data adalah memberikan ketersediaan Data yang handal untuk Kabupaten Natuna serta penerapan terhadap regulasi tentang Satu Data Indonesia. Hal ini memiliki dampak kepada penyusunan perencanaan pembangun.an yang berkualitas karena dapat mengandalkan Data yang berkualitas dan tersedia.

Adapun tujuan dari Pedoman Manajemen Data adalah:

1. memberikan pedoman korelasi dengan Arsitektur Data SPBE
2. membuat Standar kebutuhan Data Kabupaten Natuna
3. menentukan struktur *dataset* (basis data) untuk Perangkat Daerah
4. memastikan kualitas Data.

C. Pedoman Manajemen Data

Peraturan Menteri Perencanaan Pembangunan Nasional/ Kepala Badan Perencanaan Pembangunan Nasional Republik Indonesia Nomor 16 Tahun 2020 Tentang Manajemen Data Sistem Pemerintahan Berbasis Elektronik merupakan sebuah pijakan dalam pengelolaan Data di pemerintah daerah.

Manajemen Data SPBE bertujuan untuk menjamin terwujudnya Data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, Evaluasi, dan pengendalian pembangunan nasional. Sasaran utama dari Manajemen Data ini adalah:

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

Manajemen Data SPBE dilaksanakan melalui serangkaian proses pengelolaan, yang terdiri dari 4 proses pengelolaan.

1. Manajemen Arsitektur Data
   Rangkaian proses untuk menetapkan dan menyebarluaskan komponen Arsitektur Data, dimana proses tersebut adalah:
   a. menyediakan Data yang berkualitas tinggi
   b. mengidentifikasi dan mendefinisikan kebutuhan Data
   c. merancang struktur dan rencana untuk memenuhi kebutuhan Data saat ini dan kebutuhan Data jangka panjang.

2. Manajemen Data Induk dan Data Referensi
   Rangkaian proses perencanaan, pengumpulan, pemeriksaan dan penyebarluasan Data Referensi, dimana proses tersebut adalah:
   a. merencanakan Daftar Data Induk dan Data Referensi;
   b. mengumpulkan Data di walidata;
   c. memeriksa kesesuaian dengan struktur dan format baku, Daftar Data tahun berikutnya serta tidak terjadi duplikasi;
   d. menyebarluaskan Data Induk dan Data Referensi oleh walidata; dan
   e. memperbaharui Data Induk dan Data Referensi.
3. Manajemen Kualitas Data
   Rangkaian proses untuk memastikan Data yang dihasilkan dan dikelola secara elektronik memenuhi prinsip Satu Data Indonesia, dimana proses tersebut adalah:
   a. mengembangkan dan mempromosikan kesadaran kualitas Data;
   b. menentukan persyaratan kualitas Data;
   c. menetapkan profil, analisis, dan nilai kualitas Data;
   d. menentukan matriks kualitas Data;
   e. menentukan aturan bisnis kualitas Data;
   f. menguji dan memvalidasi persyaratan kualitas Data;
   g. menetapkan dan mengevaluasi tingkat layanan kualitas Data; dan
   h. mengukur dan memantau kualitas Data secara berkelanjutan.

BAB VII
MANAJEMEN LAYANAN

A. Pendahuluan

Manajemen layanan Sistem Pemerintahan Berbasis Elektronik (SPBE) dilakukan melalui serangkaian proses pelayanan Pengguna SPBE, pengoperasian Layanan SPBE, dan pengelolaan Aplikasi SPBE.

Pelayanan Pengguna SPBE, terdiri dari 1 (satu) fungsi *Service Desk* dan 5 (lima) proses meliputi:

1. Manajemen Gangguan Layanan SPBE,
2. Manajemen Masalah Layanan SPBE
3. Manajemen Konfigurasi Layanan SPBE;
4. Manajemen Perubahan Layanan SPBE; dan
5. Manajemen Rilis Layanan SPBE

Pengoperasian Layanan TIK, terdiri dari 2 (empat) proses meliputi:

1. Manajemen Tingkat Layanan;
2. Manajemen Kapasitas Layanan;
3. Manajemen Kelangsungan Layanan; dan
4. Manajemen Ketersediaan Layanan.

Pengelolaan Aplikasi SPBE, merupakan kegiatan pembangunan dan pengembangan aplikasi yang berpedoman pada metodologi pembangunan dan pengembangan Aplikasi SPBE.

B. Pelayanan Pengguna SPBE

1. Manajemen Gangguan Layanan
   a. Penanganan Gangguan Layanan
      1) Kepala Dinas Komunikasi dan Informatika bertanggung jawab dalam penerapan Manajemen Gangguan Layanan. Dalam penerapannya. Kepala Dinas menetapkan :
         a) Koordinator *Service Desk*, yang bertanggung jawab menerapkan efisiensi dan efektifitas manajemen *Service Desk*;
         b) Koordinator Manajemen Gangguan, yang bertanggung jawab menerapkan efisiensi dan efektifitas manajemen gangguan;
         c) Petugas *Service Desk*, yang bertugas melaksanakan registrasi gangguan, pelaporan gangguan, dan pemantauan status pemenuhan permintaan layanan, komunikasi dengan pengguna mengenai kemajuan penanganan gangguan dan penutupan gangguan;
         d) Pelaksana Teknis Manajemen Gangguan, yang bertugas melakukan investigasi dan diagnosa terhadap gangguan, solusi dan pemulihan gangguan, eskalasi gangguan, pemutakhiran catatan gangguan dan masukan mengenai solusi atas gangguan;
      2) Prosedur penanganan gangguan Layanan SPBE mencakup:
         a) Identifikasi dan pencatatan gangguan Layanan SPBE;
         b) Penentuan klasifikasi gangguan layanan TIK, dengan detil klasifikasi, prioritas, dan kode dampak;

c) Penugasan, pemantauan, dan komunikasi status kemajuan gangguan Layanan SPBE;
d) Eskalasi gangguan Layanan SPBE;
e) Koordinasi dengan proses manajemen Layanan SPBE lainnya; dan
f) Penutupan gangguan Layanan SPBE

b. Pengelolaan permintaan Layanan SPBE
Prosedur permintaan Layanan SPBE mencakup:
1) Identifikasi dan pencatatan permintaan Layanan SPBE;
2) Eskalasi permintaan Layanan SPBE;
3) Koordinasi dengan proses manajemen Layanan SPBE lainnya; dan
4) Penutupan permintaan Layanan SPBE.

2. Manajemen Masalah Layanan SPBE
a. Kepala Dinas bertanggung jawab dalam Manajemen Masalah Layanan. Dalam menjalankan tugasnya pada aspek manajemen masalah layanan, Kepala Dinas menetapkan:
1) Koordinator Manajemen Masalah, yang bertugas melakukan reviu efisiensi dan efektivitas proses pengendalian masalah layanan SPBE;
2) Pelaksana Teknis Manajemen Masalah, yang bertugas melaksanakan proses pengendalian masalah Layanan SPBE, melaksanakan proses pengendalian *error* Layanan SPBE, pengelolaan *known errors* sampai didapatkan solusi permanen, pemberian masukan kepada *Service Desk* mengenai solusi sementara terbaik yang dapat diterapkan untuk menangani gangguan terkait masalah Layanan SPBE yang belum terselesaikan atau *known error*.
b. Prosedur manajemen masalah Layanan SPBE, mencakup:
1) identifikasi dan pencatatan masalah Layanan SPBE;
2) klasifikasi masalah Layanan SPBE berdasarkan kategori, urgensi, dampak, dan prioritas terhadap kegiatan operasional;
3) investigasi dan diagnosa akar penyebab dari masalah layanan SPBE;
4) identifikasi dan pencatatan *error*;
5) pemantauan solusi *known error*/ masalah Layanan SPBE; dan
6) penutupan suatu masalah Layanan SPBE

3. Manajemen Konfigurasi Layanan SPBE
a. penyusunan rencana manajemen konfigurasi Layanan SPBE mencakup:
1) Pendefinisian tujuan, cakupan, dan objektif dari manajemen konfigurasi Layanan SPBE yang sesuai dengan kebutuhan operasional SPBE;
2) Penentuan rencana sumber daya manusia dalam pelaksanaan manajemen konfigurasi Layanan SPBE meliputi peran dan tanggung jawab serta beban kerja;
3) Perkiraan pertumbuhan Data komponen konfigurasi;
4) Kajian untuk membandingkan rencana pengelolaan komponen konfigurasi dengan kondisi yang sebenarnya; dan

5) Penentuan rencana pengawasan atas komponen konfigurasi milik pihak ketiga yang digunakan dalam operasional SPBE berdasarkan kesepakatan.

b. Pendefinisian dan identifikasi komponen konfigurasi Layanan SPBE, mencakup:
   1) Pendefinisian komponen konfigurasi dan memastikan tidak ada duplikasi komponen konfigurasi;
   2) Identifikasi relasi antara komponen konfigurasi;
   3) Penyusunan baseline konfigurasi;
   4) Penentuan standar penamaan untuk komponen konfigurasi; dan
   5) Pemberian label terhadap komponen konfigurasi.

c. Kontrol komponen konfigurasi, mencakup:
   1) Registrasi semua komponen konfigurasi beserta atribut dan relasinya;
   2) Pemuktahiran komponen konfigurasi;
   2) Pemeliharaan *Configuration Management Database* (CMDB);
   3) Penyusunan manajemen lisensi
   4) Penyusunan manajemen retensi dari setiap komponen konfigurasi

d. Status *accounting* komponen konfigurasi mencakup:
   1) Pengelolaan status konfigurasi selama masa aktifnya;
   2) Pengelolaan pencatatan, pengambilan, dan konsolidasi status konfigurasi saat ini dengan status sebelumnya untuk memastikan kebenaran dan keutuhan dari status konfigurasi;
   3) Pelaporan status semua komponen kofigurasi serta Data historikalnya kepada pihak-pihak yang membutuhkan.

e. Evaluasi untuk verifikasi komponen konfigurasu mencakup:
   1) Kajian dan Evaluasi untuk memverifikasi keberadaan fisik komponen konfigurasi yang ada di operasional terhadap Data komponen konfigurasi yang terekam di dalam CMDB;
   2) Pemeriksaan ketersediaan dan kelengkapan dokumen rilis Layanan SPBE dan konfigurasi sebelum suatu rilis diimplementasikan; dan
   3) Penetapan waktu untuk melakukan Evaluasi dengan mempertimbangkan beberapa kondisi seperti konfigurasi Layanan SPBE yang baru, sebelum dan setelah melakukan perubahan infrastruktrur SPBE, sebelum melakukan instalasi suatu rilis Layanan SPBE yang berdampak besar terhadap organisasi. setelah pemulihan dari bencana dan kembali ke kondisi yang normal; dan setelah terdeteksi adanya komponen konfigurasi. yang tidak sah.

4. Manajemen Perubahan Layanan SPBE

   Prosedur manajemen perubahan Layanan SPBE mencakup:
   a. Pengajuan permintaan perubahan Layanan SPBE;
   b. Pemeliharaan dan pemutakhiran informasi permintaan perubahan Layanan SPBE
   c. Pencatatan dan pengelolaan semua permintaan perubahan Layanan SPBE yang diajukan dalam suatu daftar rekaman permintaan perubahan termasuk pemutakhiran status dan informasinya;
   d. Pengkategorian untuk menentukan tingkat persetujuan yang diperlukan;

e. Penentuan kategori perubahan Layanan SPBE
f. Penetapan lamanya proses persetujuan perubahan Layanan SPBE
g. Pengkajian permintaan perubahan Layanan SPBE setidaknya mempertimbangkan informasi berikut:
   1) Dampak kepada pengguna;
   2) Dampak kepada komponen pendukung Layanan SPBE
   3) Kebutuhan sumber daya (termasuk kebutuhan komponen pendukung Layanan SPBE baru) dan biaya;
   4) Waktu yang diperlukan untuk melakukan implementasi perubahan Layanan SPBE;
   5) Manfaat permintaan perubahan Layanan SPBE;
   6) Dampak jika permintaan perubahan Layanan SPBE tidak diimplementasikan;
   7) Relasi atau keterkaitan dengan permintaan perubahan Layanan SPBE lainnya; dan
   8) Kemungkinan terjadinya gangguan layanan saat implementasi, misalnya *downtime*;
   9) Penunjukan personel atau kelompok kerja yang ditugaskan untuk melakukan kajian dampak dan menyusun rekomendasi sesuai kategori permintaan perubahan Layanan SPBE;
   10) Persetujuan permintaan perubahan Layanan SPBE (menyetujui atau menolak) berdasarkan hasil kajian, termasuk mencantumkan alasan untuk setiap permintaan perubahan yang ditolak atau tidak dapat diimplementasikan;
   11) Penjadwalan, penerbitan, dan pendistribusian jadwal implementasi permintaan perubahan Layanan SPBE secara berkala;
   12) Pemantauan status dan perkembangan implementasi atau rilis permintaan perubahan Layanan SPBE; dan
   13) Verifikasi, penerimaan, dan penutupan permintaan perubahan Layanan SPBE.

C. Pengoperasian Layanan SPBE
   1. Manajemen Tingkat Layanan SPBE mencakup:
      a. ldentifikasi dan pendefmisian kebutuhan Iayanan SPBE, yaitu: Koordinasi penyusunan Kebutuhan Tingkat Layanan, Koordinasi *penyusunan Service Specification Sheet*; dan Koordinasi penyusunan *Service Quality Plan*
      b. Penyusunan dan pemutakhiran dokumen manajemen tingkat Iayanan SPBE;
      c. Pemantauan dan pelaporan manajemen tingkat Iayanan SPBE terkait dengan pencapaian tingkat Layanan SPBE yang disepakati secara berkala;
      d. Pengkajian ulang Iayanan SPBE yaitu Koordinasi survei kepuasan pengguna dan koordinasi penyusunan *Service Improvement Program.*
   2. Manajemen Kapasitas Layanan SPBE. Mencakup:
      a. Manajemen kapasitas bisnis, yaitu analisis kapasitas komponen pendukung Layanan SPBE saat ini, prediksi kemampuan dan kapasitas komponen pendukung Layanan SPBE di masa mendatang, *application sizing* untuk menentukan sumber daya yang diperlukan dalam menjalankan Layanan SPBE barn atau perubahan Layanan SPBE, dan penyusunan rencana perubahan

kapasitas komponen pendukung Layanan SPBE di masa yang akan datang berdasarkan tingkat layanan yang disepakati dan biaya yang efektif dan efisien.

b. Manajemen kapasitas layanan dan sumber daya yaitu pemantauan penggunaan Layanan SPBE dan komponen pendukungnya secara berkelanjutan untuk memastikan penggunaan sumber daya perangkat lunak dan perangkat keras secara optimal, penentuan ambang batas dan acuan dari penggunaan komponen pendukung Layanan SPBE sebagai bagian dari proses pemantauan, analisis hasil pemantauan penggunaan Layanan SPBE dan komponen pendukungnya, pelaksanaan tuning/optimasi pada komponen pendukung Layanan SPBE berdasarkan hasil analisis, pelaksanaan Manejeman Permintaan berkoordinasi dengan proses Manajemen Tingkat Layanan, penyusunan dan pemutakhiran *Capacity Database*.

3. Manajemen Kelangsungan Layanan SPBE, mencakup:
   a. *Requirement and Strategy*, meliputi kegiatan: memastikan strategi pemulihan memenuhi kebutuhan bisnis, penyelarasan secara optimal opsi pengurangan risiko dan opsi pemulihan, analisis kelayakan dan perencanaan kapasitas untuk kebutuhan pembiayaan dengan merujuk pada proses manajemen kapasitas Layanan SPBE, penentuan prioritas pemulihan sementara untuk periode waktu tertentu, penentuan opsi pemulihan untuk komponen pendukung Layanan SPBE dan Data rekam kritikal, penentuan opsi potensial untuk pemulihan seperti prosedur manual, pemulihan gradual, pemulihan intermediasi, pemulihan cepat, dan pemulihan segera, penentuan dukungan strategi backup yang tepat; dan pelaporan strategi pemulihan.
   b. *Implementation*. Meliputi kegiatan : perencanaan implementasi dan organisasi, penyusunan rencana pemulihan keadaan darurat, prosedur inisiasi pengujian, yaitu: penyusunan rencana dan skenario pengujian, penyusunan format laporan dan Evaluasi pengujian rekomendasi penyempunaan rencana dan prosedur pemulihan, dan pengujian mendatang; dan umpan balik
   c. *Operational Management*, mencakup : pendidikan, pelatihan untuk meningkatkan kesadaran kepada semua pihak mengenai prosedur pemulihan Layanan SPBE, perencanaan, Evaluasi, dan pelaporan terhadap pemeliharaan rencana dan prosedur pemulihan Layanan SPBE, pelaksanaan pengujian berdasarkan prosedur inisiasi pengujian, pelaporan hasil pengujian, dan modifikasi rencana dan prosedur pemulihan berdasarkan hasil Evaluasi dan pengujian dengan mengacu pada proses manajemen perubahan Layanan SPBE
4. Manajemen Ketersediaan Layanan SPBE mencakup kegiatan:
   a. perencanaan ketersediaan Layanan SPBE yaitu penentuan persyaratan ketersediaan Layanan SPBE yang meliputi kegiatan:
      1) penentuan fungsi kerja vital terkait kegiatan kelangsungan Layanan SPBE;
      2) pendefmisian dan kesepakatan *downtime* Layanan SPBE;
      3) penentuan target dari ketersediaan, keterandalan, dan keterawatan dari komponen konfigurasi Layanan SPBE agar dapat didokumentasikan dan disetujui, perancangan ketersediaan Layanan SPBE agar target dari ketersediaan, keterandalan, dan keterawatan dapat terpenuhi, penentuan

kriteria rancangan pemulihan Layanan SPBE yang baru, penentuan dan pengaturan jadwal pemeliharaan komponen konfigurasi Layanan SPBE, penyusunan rencana ketersediaan Layanan SPBE secara berkala paling sedikit satu kali dalam setahun.

b. pemantauan ketersediaan Layanan SPBE, yaitu pemantauan, pengukuran, analisis tren, dan pelaporan dari ketersediaam keterandalan, dan keterawatan komponen konfigurasi, pemutakhiran rencana ketersediaan berdasarkan kebutuhan Layanan SPBE serta hasil pemantauan, pengukuran, analisis tren dan pelaporan dengan prioritas untuk peningkatan ketersediaan Layanan SPBE paling sedikit satu kali dalam setahun.

BAB VIII
MANAJEMEN SUMBER DAYA MANUSIA

Pemerintah Daerah mengelola aset sumber daya manusia untuk menjamin keberlangsungan dan peningkatan mutu layanan pemerintahan berbasis elektronik berdasarkan ketentuan Peraturan Perundang-undangan. Pengelolaan sumber daya manusia mencakup aparatur sipil negara dan masyarakat pengguna layanan pemerintahan berbasis elektronik.

Pengelolaan sumber daya manusia masyarakat pengguna layanan pemerintahan berbasis elektronik dilakukan melalui sosialisasi, diseminasi, bimbingan teknis, pelatihan penggunaan layanan pemerintahan berbasis elektronik. Dalam pelaksanaan manajemen sumber daya manusia, kepala Perangkat Daerah yang membidangi kepegawaian daerah dan kepala Perangkat Daerah yang menyelenggarakan urusan komunikasi dan informatika berkoordinasi dan dapat melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.

Pengembangan SDM SPBE dapat dicapai melalui peningkatan pengetahuan dan penerapan praktik terbaik SPBE, pembangunan budaya kerja berbasis SPBE, pengembangan jabatan fungsional PNS, dan pelaksanaan kemitraan dengan berbagai pihak.

A. Sumber Daya Manusia SPBE
   1. Pengembangan kepemimpinan SPBE di Pemerintah Daerah
      a. Kepemimpinan yang kuat, kolaboratif, dan inovatif sangat menentukan keberhasilan SPBE di Instansi Pusat dan Pemerintah Daerah melalui komitmen, keteladanan, dan arahan dari pimpinannya. Kepemimpinan SPBE tersebut juga diharapkan mampu mendorong terciptanya lingkungan kerja dan budaya kerja yang dapat mendukung kemajuan SPBE.
      b. Strategi untuk mencapai pengembangan kepemimpinan SPBE Pemerintah Daerah adalah:
         1) meningkatkan pengetahuan dan penerapan praktik terbaik SPBE bagi pimpinan di Pemerintah Daerah
         2) membangun budaya kerja berbasis SPBE bagi seluruh pegawai ASN
   2. Peningkatan kapasitas Sumber Daya Manusia SPBE
      a. Peningkatan kapasitas SDM SPBE mencakup upaya untuk menetapkan standar kompetensi teknis SPBE, mengembangkan kompetensi teknis SDM SPBE, mengembangkan pola karir dan remunerasi SDM SPBE agar pembangunan, pengembangan, pengoperasian, dan pemberian Layanan SPBE dapat berjalan dengan baik, berkesinambungan, dan memenuhi harapan/kebutuhan pengguna.

b. Strategi untuk mencapai peningkatan kapasitas SDM SPBE adalah:
   1) mengembangkan jabatan fungsional Pegawai Negeri Sipil (PNS) yang terkait dengan SPBE; dan
   2) membangun kemitraan dengan pihak non pemerintah dalam peningkatan kompetensi teknis ASN, penyediaan tenaga ahli, riset, serta pembangunan dan pengembangan SPBE.

BUPATI NATUNA,

ttd

WAN SISWANDI

LAMPIRAN III
PERATURAN BUPATI NATUNA
NOMOR 19 TAHUN 2024
TENTANG PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

STANDAR DAN TATA CARA PELAKSANAAN AUDIT INSFRASTRUKTUR DAN APLIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
STANDAR PELAKSANAAN AUDIT INFRASTRUKTUR SPBE

Standar Pelaksanaan Audit Infrastruktur SPBE adalah batasan minimal bagi Regulator dan Auditor untuk membantu pelaksanaan Audit serta prosedur yang harus dilaksanakan atau diterapkan dalam rangka pencapaian tujuan Audit.

Standar Pelaksanaan Audit Infrastruktur SPBE memiliki tujuan sebagai berikut:
a. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Infrastruktur SPBE;
b. Menyusun Kerangka Kerja regulasi Audit Infrastruktur SPBE dalam proses pendaftaran Auditor dan Lembaga Audit;
c. Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Infrastruktur SPBE, guna menambah nilai kepada Unit yang diaudit melalui perbaikan proses dan operasionalnya; dan
d. Menyusun dasar dalam melakukan Evaluasi terhadap regulasi dan pelaksanaan Audit Infrastruktur SPBE guna mendorong rencana perbaikan.

Standar Pelaksanaan Audit Infrastruktur SPBE mencakup hal-hal sebagai berikut:
a. Standar Umum;
b. Standar Pelaksanaan;
c. Standar Pelaporan; dan
d. Standar Tindak Lanjut

A. Standar Umum
   1. Standar Umum memberikan prinsip dasar untuk mengatur Auditor Infrastruktur SPBE dalam melaksanakan tugasnya dan memberikan layanan jasa Audit Infrastruktur SPBE sehingga pelaksanaan pekerjaan Audit Infrastruktur SPBE hingga pelaporannya dapat terlaksana dengan baik dan efektif.
   2. Pimpinan Unit SPBE harus mengembangkan dan menjaga jaminan kualitas dan program peningkatan yang mencakup semua aspek pelaksanaan Audit Infrastruktur SPBE
   3. Integritas Auditor Infrastruktur SPBE dan pelaksana pendaftaran diwujudkan melalui sikap independen, objektif, dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor Infrastruktur SPBE dituntut untuk menjalankan hal-hal sebagai berikut:
      a. Memiliki pengetahuan (*knowledge)* keterampilan (*skill),* sikap (*attitude*) dan pengalaman (*esperience)* yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;

b. Menggunakan keahlian profesionalnya dengan cermat dan seksama (*due profesional care*) serta berhati-hati (*prudent*) dalam setiap penugasan;
c. Senantiasa mengasah dan melatih kecermatan profesionalnya;
d. Meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
e. Mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
f. Memiliki pengetahuan (*knowledge*) keterampilan (*skill*), sikap (*attitude*) dan pengalaman (*experience*) yang sesuai guna memenuhi tanggung jawabnya dalam pelaksanaan audit.

4. Tujuan, wewenang dan tanggung jawab suatu aktivitas Audit Infrastruktur SPBE harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (*audit charter*), surat tugas, atau dokumen-dokumen yang setara. surat tugas atau piagam audit (*audit charter*) wajib menjelaskan tujuan audit, ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit.
5. Kepala Unit TIK SPBE atau pimpinan institusi pemberi tugas auditmemberikan tugas kepada tim audit dalam bentuk Surat Tugas atau dapat juga berupa piagam audit (*audit charter*) sebelum Audit Infrastruktur SPBE dilaksanakan

B. Standar Pelaksanaan

1. Ketua tim audit (*Lead Auditor)* harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit Infrastruktur SPBE tercapai.
2. Ketua tim audit (*Lead Auditor)* harus melakukan hal-hal sebagai berikut:
   a. Menyusun dan menetapkan rencana audit (*audit plan)* guna menentukan prioritas-prioritas dalam kegiatan Audit Infrastruktur SPBE yang konsisten dengan tujuan audit sesuai dengan piagam audit *(audit charter);*
   b. Menyampaikan rencana audit (*audit plan*) kepada pimpinan Unit SPBE dan *Auditee* untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumberdaya;
   c. Mengelola sumberdaya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit yang telah disetujui;
   d. Melakukan koordinasi dengan pimpinan Unit SPBE untuk menjamin bahwa pelaksanaan Audit Infrastruktur SPBE berjalan efektif dan efisien; dan
   e. Memberi laporan yang memadai kepada pimpinan Unit SPBE dan Unit mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
3. Unit mengajukan permintaan Audit Infrastruktur SPBE untuk satu atau lebih dari tujuan berikut:
   a. Peningkatan kinerja birokrasi dan pelayanan publik;
   b. Penilaian kesesuaian dengan standar/prosedur/pedoman dan kesesuaian dengan rencana/kebutuhan/kondisi;
   c. Identifikasi status teknologi yang dimiliki, identifikasi kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
   d. Perencanaan pengembangan sistem/teknologi dan perencanaan perbaikan kelemahan; dan/atau

e. Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.

4. Pemeriksaan yang dilakukan oleh *Auditee* mencakup:
   a. Penerapan tata kelola dan manajemen Infrastruktur SPBE;
   b. Fungsionalitas dan kinerja Infrastruktur SPBE; dan
   c. Tingkat kepatuhan terhadap regulasi.
5. Dalam hal merencanakan Audit Infrastruktur SPBE, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit Infrastruktur SPBE, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit. Perencanaan tersebut yang dituangkan dalam rencana audit (*audit plan*) dengan mempertimbangkan berbagahi hal, antara lain:
   a. Sistem pengendalian internal dan kepatuhan *Auditee* terhadap acuan atau *benchmark*;
   b. Penetapan tujuan Audit Infrastruktur SPBE;
   c. Penetapan kecukupan lingkup; dan
   d. Penggunaan metodologi yang tepat.
6. Dalam hal pelaksanaan Audit Infrastruktur SPBE, Auditor Infrastruktur SPBE harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit. Dalam melaksanakan audit tersebut, Auditor Infrastruktur SPBE harus:
   a. Memperoleh bukti-bukti audit yang cukup, handal, dan relevan untuk mendukung penilaian audit dan kesimpulan audit;
   b. Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
   c. Menyiapkan, mengelola dan menyimpan Data dan informasi yang diperoleh selama pelaksanaan audit; dan
   d. Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
7. Dalam hal komunikasi atas hasil Audit Infrastruktur SPBE, Auditor Infrastruktur SPBE harus mengkomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak. Jika komunikasi final berisi kesalahan atau penghilangan yang signifikan, ketua tim audit (Lead Auditor) harus mengkomunikasikan informasi yang telah diperbaiki kepada semua pihak yang menerima komunikasi.
8. Aspek monitoring dalam aktivitas Audit Infrastruktur SPBE meliputi:
   a. Kepatuhan terhadap Kode Etik dan Standar Audit;
   b. Kesesuaian terhadap Piagam Audit;
   c. Kesesuaian terhadap Rencana Audit; dan
   d. Kesesuaian terhadap Protokol Audit.
9. Tim pengawas mutu Unit SPBE menyampaikan hasil monitoring kepada pimpinan Unit SPBE secara berkala. Selanjutnya, Pimpinan Unit SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil monitoring
10. Evaluasi mencakup perencanaan, pelaksanaan, dan pelaporan Audit Infrastruktur SPBE. Lalu, Tim pengawas mutu audit Unit SPBE menyampaikan hasil Evaluasi audit kepada pimpinan Unit SPBE. Kemudian, Pimpinan Unit SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil Evaluasi audit

C. Standar Pelaporan
   1. Laporan hasil audit dibuat oleh Unit SPBE dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas.
   2. Laporan audit harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan audit. Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan, dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh *Auditee* secara tertulis dari pejabat *Auditee* yang bertanggung jawab.

D. Standar Tindak Lanjut
   1. Pemantauan terhadap legalitas, kompetensi, dan kinerja Unit SPBE dilakukan melalui mekanisme registrasi dan laporan tahunan pelaksanaan audit.
   2. Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan. Ketua tim audit (*Lead Auditor*) harus menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan dan rekomendasi audit oleh *Auditee*, mencakup cara berkomunikasi dengan *Auditee*, prosedur pemantauan, dan laporan status temuan.

BAB II
TATA CARA PELAKSANAAN AUDIT INFRASTRUKTUR SPBE

A. Tata Cara Pelaksanaan Audit

Audit Infrastrtuktur SPBE dilakukan Unit TIK SPBE berdasarkan permintaan Unit atau penugasan Unit TIK. Audit Infrastruktur SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar terbagi dalam tiga kelompok tahapan, yaitu:

1. Tahap perencanaan (*pre-audit*);
2. Tahap pelaksanaan lapangan (*on site audit*);dan
3. Tahap analisa Data dan pelaporan (*postaudit*).

Adapun tiga kelompok tersebut meliputi hal-hal sebagai berikut :

a. Penyiapan tim audit
b. *Quick assessment*
c. Penyiapan rencana audit
d. Penyepakatan rencana audit
e. Penyiapan protokol audit
f. Penetapan parameter acuan
g. Pertemuan pembukaan
h. Pelaksanaan lapangan
i. Pertemuan penutupan
j. Analisa Data
k. Pengelolaan Data
l. Penyusunan laporan
m. *Proof-read* laporan
n. Penyerahan laporan; dan
o. Evaluasi aktivitas.

Audit Infrastruktur SPBE dilakukan oleh sebuah tim audit yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:

1. Pengawas mutu, berperan melakukan monitoring dan Evaluasi aktivitas audit untuk menjamin pelaksanaan audit sesuai dengan standar audit. Pengawas mutu harus memiliki kualifikasi Auditor teknologi utama atau yang setara;
2. *Lead Auditor*, bertanggung jawab merencanakan audit teknologi, melaksanakan audit di lapangan, mengendalikan Data dan melaporkan hasil audit teknologi. Lead Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi madya;
3. Auditor, bertugas membantu Lead Auditor dalam aktivitas audit teknologi. Auditor harus mempunyai kualifikasi minimal setara dengan Auditor teknologi muda;
4. Asisten Auditor, bertugas membantu Auditor dalam aktivitas audit teknologi.
5. Teknisi, bertugas membantu Auditor dalam pengumpulan Data lapangan;
6. Narasumber, berperan memberi masukan yang berkaitan dengan isu, status teknologi, dan keilmuan yang relevan.

Quick Assessment dilakukan untuk mengenali obyek audit dengan mengidentifikasi: *currentissue*, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, Proses Bisnis dari organisasi, atau bagian yang diaudit

Tim Audit Infrastruktur SPBE harus merencanakan tindakan audit dengan mendefinisikan hal-hal berikut :

a. Tujuan audit;
b. Lingkup;
c. Pendekatan;
d. Kriteria;
e. Parameter;
f. Acuan;
g. Metode pengumpulan Data;
h. Penentuan objek;
i. Data primer dan sekunder;
j. Metode analisa;
k. *Deliverable*;dan
l. Perkiraan jadwal pelaksanaan.

Hal-hal tersebut harus dicantumkan dalam Rencana Audit (*Audit Plan*). Ketua tim audit dan *Auditee* harus menyepakati rencana audit sebelum tahap pelaksanaan audit. Dalam pelaksanaan kegiatan audit, tim Audit Infrastruktur SPBE harus:

1. Menyusun protokol audit yang berisi detail instrumen audit, antara lain:
    a. Daftar Data, pertanyaan dan pengujian
    b. Formulir untuk mencatat Data, jawaban, hasil observasi dan hasil pengujian
2. Menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan pembanding;
3. Melakukan pertemuan pembukaan dengan Auditee;
4. Melaksanakan audit lapangan, melalui:
    a. Penelaahan dokumen;
    b. Wawancara;
    c. Observasi lapangan;
    d. Pengujian; dan
    e. Verifikasi bukti.
5. Melakukan pertemuan penutupan dengan Auditee
6. Melakukan analisis bukti; dan
7. Mengelola Data.

Data status teknologi SPBE dikumpulkan secara objektif berdasarkan fakta yang ada pada *Auditee*; Deskripsi data dan informasi yang dikumpulkan mengikuti kriteria penilaian yang sudah dikeluarkan dalam proses Manajemen Risiko SPBE dari Standar dan Mekanisme Manajemen Sistem Pemerintahan Berbasis Elektronik dan ditetapkan tersendiri oleh Kepala Unit

Temuan Audit Infrastruktur SPBE merupakan keadaan dimana fakta status aset teknologi SPBE *Auditee*; tidak sesuai dengan persyaratan Infrastruktur SPBE. Auditor dapat mengurangi atau menambahkan lingkup Data sebagaimana tercantum proses Manajemen Risiko SPBE dari Standar

dan Mekanisme Manajemen Sistem Pemerintahan Berbasis Elektronik Peraturan Unit ini sepanjang relevan dengan objek dan rencana penggunaan hasil audit sesuai kebutuhan *Auditee*

Monitoring memberikan informasi untuk suatu kegiatan audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit. Monitoring dilakukan oleh tim pengawas mutu. Tim pengawas mutu harus menetapkan suatu proses tindak lanjut untuk memonitor dan meyakinkan bahwa tindak lanjut yang telah ditetapkan oleh pimpinan Unit TIK SPBE diimplementasikan secara efektif. Tim pengawas mutu dapat berasal dari pihak eksternal

Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya. Evaluasi dilakukan oleh tim pengawas mutu setelah aktivitas audit selesai. Tim Pengawas mutu menyampaikan hasil Evaluasi audit kepada pimpinan Unit TIK SPBE dan Unit. Pimpinan Unit TIK SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil Evaluasi audit.

B. Tata Cara Pelaporan Audit

Laporan audit disampaikan oleh ketua tim audit kepada pimpinan Unit SPBE. Laporan mencakup latar belakang, tujuan, lingkup, pendekatan audit, kriteria dan acuan, metoda pengumpulan Data, metode analisa, hasil analisis, temuan dan kesimpulan, dan rekomendasi. Pada setiap halaman dokumen laporan hasil audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurang- kurangnya: tahun pelaksanaan audit, nomor urut atau nomor seri dokumen, domain Aplikasi atau Infrastruktur SPBE, *Auditee*; dan kode pengendalian distribusi salinan dokumen.

Draft laporan direviu oleh ketua tim audit untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit. Laporan Audit disahkan oleh pimpinan Unit TIK SPBE

Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Laporan Audit didistribusikan kepada pimpinan Unit SPBE Laporan hasil audit disampaikan oleh pimpinan Unit SPBE kepada *Auditee* dan lembaga lain sesuai kesepakatan dengan *Auditee* Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh pimpinan Unit SPBE kepada Unit TIK SPBE satu kali dalam satu tahun dengan format sebagai berikut :

FORMAT LAPORAN PERIODIK AUDIT INFRASTRUKTUR SPBE

A. Identitas UNIT	
Nama UNIT	(isi nama Lembaga Pelaksana Audit)
Periode pelaporan	(isi periode pelaporan)
B. Penanggung Jawab Penyelenggaraan Audit	
Nama	(isi nama lengkap)
Jabatan	(isi jabatan resmi)
NIP	(isi Nomor induk pegawai)
Kontak	(isi nomor telepon dan surel ybs)
C. Penyelenggaraan Audit	
Judul Audit TIK	(isi judul)
Tanggal Laporan Audit	(isi tanggal)
Jenis Audit	(isi jenis audit)

Lingkup Audit	(isi lingkup audit)
Ringkasan Hasil Audit	
Ringkasan Temuan	Ringkasan Rekomendasi
(parameter)	(parameter)
(temuan 1) jenis dan narasi	(rekomendasi 1)
	narasi singkat dan tenggat waktu
(temuan 2)	(rekomendasi 2)

D. Tindak Lanjut Audit		
Informasi Tindak Lanjut Audit		
Rekomendasi #1	Tenggat waktu	Tindak Lanjut #1
Rekomendasi #2	Tenggat waktu	Tindak Lanjut #2
Rekomendasi #3	Tenggat waktu	Tindak Lanjut #3

Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh secara tertulis dari pejabat *Auditee* yang bertanggung jawab.

Laporan pelaksanaan audit dibuat oleh Unit TIK berdasarkan hasil pelaporan oleh Unit SPBE disampaikan kepada tim koordinasi SPBE nasional dan lembaga lain sesuai ketentuan perundangan.

C. Tata Cara Tindak Lanjut Audit

Kesepakatan proses pemantauan dilakukan dalam bentuk observasi pada pada waktu yang disepakati oleh Unit SPBE dan *Auditee* yang sekurang-kurangnya meliputi: lingkup, objek, jangka waktu, beban pembiayaan, dan penanggung jawab. Pemantauan dapat dilakukan oleh Unit SPBE atau Auditor lain yang disepakati. Konfirmasi terhadap hasil audit dilakukan paling banyak tiga kali.

Pemantauan dilakukan dalam bentuk observasi pada *Auditee* pada waktu yang disepakati oleh tim koordinasi SPBE nasional. Tindak lanjut perbaikan dari *Auditee* perlu dievaluasi oleh Auditor. Evaluasi dilakukan untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi *Auditee*.

D. Tata Cara Pembiayaan Audit

Pembiayaan untuk pelaksanaan Audit ditanggung oleh *Auditee*. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas Proses Bisnis. Pembiayaan dan mekanisme pelaksanaannya dapat dilakukan melalui kontrak atau swakelola sesuai ketentuan Peraturan Perundang-undangan.

BAB III
PANDUAN TEKNIS AUDIT INFRASTRUKTUR SPBE

A. Panduan Teknis Umum Audit Infrastruktur SPBE

Ruang lingkup Panduan Teknis Umum Audit Infrastruktur SPBE adalah sebagai berikut:

1. Tata kelola Infrastruktur SPBE;
2. Manajemen Infrastruktur SPBE; dan
3. Fungsionalitas dan kinerja Infrastruktur SPBE.

Ruang lingkup panduan audit tata kelola Infrastruktur SPBE mencakup aktivitas:

a. Evaluasi;
b. Pengarahan; dan
c. Pemantauan.

Ruang lingkup panduan audit manajemen Infrastruktur SPBE terdiri atas tahapan:

a. Perencanaan;
b. Pengembangan;
c. Pengoperasian; dan
d. Pemantauan.

Audit manajemen infrastruktur mencakup aktivitas:

a. Manajemen sistem pengendalian internal;
b. Manajemen resiko;
c. Manajemen *asset*;
d. Manajemen pengetahuan;
e. Manajemen SDM;
f. Manajemen layanan;
g. Manajemen perubahan; dan
h. Manajemen Data.

Ruang lingkup panduan fungsionalitas dan kinerja Infrastruktur SPBE terdiri atas tahapan:

a. Perencanaan
b. Pengembangan
c. Pengoperasian; dan
d. Pemeliharaan.

Hal teknis yang diaudit difokuskan pada Fungsionalitas dan Kinerja Infrastruktur SPBE

B. Panduan Teknis Pusat Data Daerah

Panduan teknis audit Pusat Data Daerah dimaksudkan sebagai panduan dalam pelaksanaan Audit Infrastruktur SPBE. Audit teknis Pusat Data Daerah mencakup fungsionalitas dan kinerja. Lingkup panduan teknis audit Pusat Data Daerah terdiri atas :

a. Perencanaan Pusat Data Daerah;
b. Pengembangan Pusat Data Daerah;
c. Pengoperasian Pusat Data Daerah; dan
d. Pemeliharaan Pusat Data Daerah.

Pusat Data Daerah direncanakan dengan mengacu kepada Arsitektur SPBE nasional, Arsitektur SPBE instansi pusat, atau Arsitektur SPBE Pemerintah Daerah, peta rencana SPBE nasional, peta rencana SPBE instansi pusat dan peta rencana SPBE pemerintah daerah. Perencanaan Pusat Data Daerah mencakup analisis kebutuhan, pengelolaan lokasi, bangunan, kebakaran, kelistrikan, suhu, pengkabelan, pembagian ruangan, sistem monitoring lingkungan, persediaan bahan bakar, sistem pendingin dan sistem jaringan data.

Pusat Data Daerah dapat dikembangkan oleh tim internal organisasi atau dari pihak ketiga dengan mengacu kepada deskripsi dalam rancangan. Pengembangan Pusat Data Daerah mencakup implementasi, instalasi dan pengujian. Uji coba terhadap Pusat Data Daerah harus terdokumentasi dalam suatu rencana pengujian (*test plan*), rancangan pengujian (*test design*), prosedur pengujian (*test procedures*), dan laporan pengujian (*test report*).

Pusat Data Daerah dilengkapi dengan dokumentasi penggunaan Pusat Data Nasional baik untuk operator maupun administrator. Dokumentasi tersebut mencakup organisasi, tata kerja, manajemen operasi, pusat pemulihan bencana, Infrastruktur, manajemen SDM Pusat Data, monitoring, pelaporan dan pengendalian, serta manajemen layanan Pusat Data.

Pemeliharaan terhadap Pusat Data Daerah didokumentasikan dalam suatu dokumen yang mencakup pemeliharaan, manajemen konfigurasi perangkat, dan pemantauan.

C. Panduan Teknis Jaringan Intra Pemerintah

Panduan teknis audit Jaringan Intra Pemerintah dimaksudkan sebagai panduan dalam pelaksanaan audit Jaringan Intra Pemerintah Daerah. Audit teknis Jaringan Intra Pemerintah mencakup fungsionalitas dan kinerja. Lingkup panduan teknis audit Jaringan Intra Pemerintah terdiri atas :

1. Perencanaan Jaringan Intra Pemerintah;
2. Pengembangan Jaringan Intra Pemerintah;
3. Pengoperasian Jaringan Intra Pemerintah; dan
4. Pemeliharaan Jaringan Intra Pemerintah.

Jaringan Intra Pemerintah direncanakan dengan mengacu kepada Arsitektur SPBE Nasional, Arsitektur SPBE Instansi Pusat, Peta Rencana SPBE Nasional. Perencanaan Jaringan Intra Pemerintah disusun berdasarkan persyaratan Jaringan Intra Pemerintah dengan mempertimbangkan kebutuhan dan Infrastruktur SPBE Daerah mencakup kebutuhan bisnis, kebutuhan jaringan dan rancangan jaringan.

Jaringan Intra Pemerintah dapat dikembangkan oleh tim internal organisasi atau dari pihak ketiga dengan mengacu kepada deskripsi dalam rancangan. Konfigurasi jaringan SPBE dapat dikustomisasi dan dilengkapi dengan dokumentasi yang memadai. Uji coba terhadap Jaringan Intra Pemerintah harus terdokumentasi dalam suatu rencana pengujian (*test plan*), rancangan pengujian (*test design*), prosedur pengujian (*test procedures*) dan laporan pengujian (*test report*).

Jaringan Intra Pemerintah dilengkapi dengan dokumentasi penggunaan Jaringan Intra Pemerintah baik untuk operator maupun administrator. Dokumentasi tersebut mencakup

a. Penggunaan perangkat Jaringan Intra Pemerintah antara lain: cara instalasi, akses terhadap perangkat, operasi terhadap perangkat;

b. Prosedur dan *Tutorials*; dan
c. Gangguan dan penangannya.

Pemeliharaan terhadap Jaringan Intra Pemerintah didokumentasikan dalam suatu dokumen yang mencakup pemeliharaan jaringan dan manajemen konfigurasi jaringan.

D. Panduan Teknis Audit Sistem Penghubung Layanan Pemerintah

Panduan teknis audit Sistem Penghubung Layanan Pemerintah dimaksudkan sebagai panduan dalam pelaksanaan Audit Infrastruktur SPBE. Audit teknis Sistem Penghubung Layanan Pemerintah mencakup fungsionalitas dan kinerja. Lingkup panduan teknis audit Sistem Penghubung Layanan Pemerintah terdiri atas:

1. Perencanaan Sistem Penghubung Layanan Pemerintah;
2. Pengembangan Sistem Penghubung Layanan Pemerintah;
3. Pengoperasian Sistem Penghubung Layanan Pemerintah; dan;
4. Pemeliharaan Sistem Penghubung Layanan Pemerintah.

Sistem Penghubung Layanan Pemerintah direncanakan dengan mengacu kepada Arsitektur SPBE nasional, Arsitektur SPBE instansi pusat, atau arsitektur SPBE pemerintah daerah, peta rencana SPBE nasional, Peta Rencana SPBE instansi pusat dan Peta Rencana SPBE pemerintah daerah. Perencanaan Sistem Penghubung Layanan Pemerintah mencakup prinsip, kebijakan, dan organisasi

Sistem Penghubung Layanan Pemerintah dapat dikembangkan oleh tim internal organisasi atau dari pihak ketiga dengan mengacu kepada deskripsi dalam rancangan. Pengembangan Sistem Penghubung Layanan Pemerintah mencakup implementasi, pengujian dan instalasi. Uji coba terhadap Sistem Penghubung Layanan Pemerintah harus terdokumentasi dalam suatu rencana pengujian (*test plan*), rancangan pengujian (*test design*), prosedur pengujian (*test procedures*) dan laporan pengujian (*testreport*)

Sistem Penghubung Layanan Pemerintah dilengkapi dengan dokumentasi penggunaan Sistem Penghubung Layanan Pemerintah baik untuk operator maupun administrator. Dokumentasi tersebut mencakup penyelenggaraan dan mekanisme kerja

Pemeliharaan terhadap Jaringan Intra Pemerintah didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:

a. Lingkup pemeliharaan
b. Alokasi sumber daya; dan
c. Pencatatan kinerja.

Kriteria penilaian Audit Infrastruktur SPBE yang terdiri atas Tata Kelola dan Manajemen, Pusat Data/Pusat Data, Jaringan Intra Pemerintah, dan Sistem Penghubung Layanan Pemerintah tercantum dalam Lampiran III Peraturan Bupati ini.

BAB IV
STANDAR PELAKSANAAN AUDIT APLIKASI SPBE

Standar Audit Aplikasi SPBE merupakan batasan minimal bagi Regulator dan Auditor guna membantu pelaksanaan Audit serta prosedur yang harus dilaksanakan atau diterapkan dalam rangka pencapaian tujuan Audit. Tujuan dari Standar Audit Aplikasi SPBE adalah sebagai berikut:

a. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Aplikasi SPBE;
b. Menyusun Kerangka Kerja regulasi Audit Aplikasi SPBE dalam proses pendaftaran Auditor dan Lembaga Audit Terakreditasi;
c. Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Aplikasi SPBE, guna menambah nilai kepada Auditee melalui perbaikan proses dan operasionalnya;
d. Menyusun dasar dalam melakukan Evaluasi terhadap regulasi dan pelaksanaan Audit Aplikasi SPBE guna mendorong rencana perbaikan.

Standar Audit Aplikasi SPBE mencakup hal-hal sebagai berikut

1. Standar Umum;
2. Standar Pelaksanaan;
3. Standar Pelaporan; dan
4. Standar Tindak Lanjut.

A. Standar Umum

1. Standar Umum memberikan prinsip dasar untuk mengatur Auditor Aplikasi SPBE dalam melaksanakan tugasnya, dan mengatur Audit Aplikasi SPBE hingga pelaporannya dapat terlaksana dengan baik dan efektif;
2. Pimpinan Unit TIK SPBE harus mengembangkan dan menjaga jaminan kualitas dan program peningkatan yang mencakup semua aspek pelaksanaan Audit Aplikasi SPBE;
3. Integritas Auditor aplikasi SPBE dan pelaksana pendaftaran diwujudkan melalui sikap independen, objektif dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor Aplikasi SPBE dituntut untuk menjalankan hal-hal sebagai berikut:
    a. memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*) dan pengalaman (*experience*) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;
    b. menggunakan keahlian profesionalnya dengan cermat dan seksama (due professional care) serta berhati-hati (prudent) dalam setiap penugasan;
    c. senantiasa mengasah dan melatih kecermatan profesionalnya;
    d. meningkatkan pengetahuan, keahlian dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
    e. mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
    f. memiliki pengetahuan (knowledge), keterampilan (skill), sikap (attitude) dan pengalaman (experience) yang sesuai guna memenuhi tanggung jawabnya dalam pelaksanaan audit.

4. Tujuan, wewenang dan tanggung jawab suatu aktivitas Audit Aplikasi SPBE harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (*audit charter*), surat tugas, atau dokumen-dokumen yang setara. Surat Tugas atau piagam audit (*audit charter*) wajib menjelaskan tujuan audit, ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit;
5. Pimpinan Unit SPBE atau pimpinan institusi pemberi tugas audit memberikan tugas kepada tim audit dalam bentuk Surat Tugas atau dapat juga berupa piagam audit (audit charter) sebelum Audit Aplikasi SPBE dilaksanakan.

B. Standar Pelaksanaan
1. Ketua tim audit (*Lead Auditor*) harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan audit Aplikasi SPBE tercapai. Ketua tim audit (*Lead Auditor*) harus melakukan hal- hal sebagai berikut :
   a. Menyusun dan menetapkan rencana audit *(audit plan*) guna menentukan prioritas-prioritas dalam kegiatan Audit Aplikasi SPBE, yang konsisten dengan tujuan audit sesuai dengan piagam audit (*audit charter*);
   b. Menyampaikan rencana audit (audit plan) kepada pimpinan Unit SPBE dan Auditee untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumberdaya;
   c. Mengelola sumber daya audit yang tepat, memadai dan efektif untuk melaksanakan rencana audit yang telah disetujui;
   d. Melakukan koordinasi dengan pimpinan Unit SPBE untuk menjamin bahwa pelaksanaan Audit Aplikasi SPBE berjalan efektif dan efisien; dan
   e. Memberi laporan yang memadai kepada pimpinan Unit SPBE dan unit mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
2. Unit wajib melaksanakan Aktivitas Audit Aplikasi SPBE jika memiliki tujuan sebagai berikut :
   a. Peningkatan kinerja birokrasi dan pelayanan publik;
   b. Penilaian kesesuaian dengan standar/prosedur/pedoman, dan kesesuaian dengan rencana/kebutuhan/kondisi;
   c. Identifikasi status teknologi yang dimiliki, identifikasi daya saing/kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
   d. Perencanaan pengembangan sistem/teknologi dan perencanaan perbaikan kelemahan; dan/atau
   e. Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.
3. Pemeriksaan yang dilakukan mencakup:
   a. Penerapan tata kelola dan manajemen Aplikasi SPBE;
   b. Fungsionalitas dan Kinerja Aplikasi SPBE; dan
   c. Tingkat kepatuhan terhadap regulasi
4. Dalam hal merencanakan audit Aplikasi SPBE, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit Aplikasi SPBE, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit

5. Perencanaan tersebut yang dituangkan dalam Rencana Audit (*Audit Plan*) dengan mempertimbangkan berbagahi hal, antara lain:
   a. Sistem pengendalian internal dan kepatuhan *Auditeeter* hadap acuan atau *benchmark*;
   b. Penetapan tujuan Audit Aplikasi SPBE;
   c. Penetapan kecukupan lingkup; dan
   d. Penggunaan metodologi yang tepat.
6. Dalam hal pelaksanaan Audit Aplikasi SPBE, Auditor Aplikasi SPBE harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit. Dalam melaksanakan audit tersebut, Auditor Aplikasi SPBE harus:
   a. Memperoleh bukti-bukti audit yang cukup, handal dan relevan untuk mendukung penilaian dan kesimpulan;
   b. Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
   c. Menyiapkan, mengelola dan menyimpan Data dan informasi yang diperoleh selama pelaksanaan audit; dan
   d. Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
7. Dalam hal komunikasi atas hasil Audit Aplikasi SPBE, Auditor Aplikasi SPBE harus mengkomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak
8. Jika komunikasi final berisi kesalahan atau penghilangan yang signifikan, ketua tim audit (*Lead Auditor*) harus mengkomunikasikan informasi yang telah diperbaiki kepada semua pihak yang menerima komunikasi Aspek monitoring dalam aktivitas Audit Aplikasi SPBE meliputi :
   a. Kepatuhan terhadap Kode Etik dan Standar Audit;
   b. Kesesuaian terhadap Piagam Audit;
   c. Kesesuaian terhadap Rencana Audit; dan
   d. Kesesuaian terhadap Protokol Audit.
9. Tim pengawas mutu Unit SPBE menyampaikan hasil monitoring kepada pimpinan Unit SPBE secara berkala. Selanjutnya, Pimpinan Unit SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil monitoring
10. Evaluasi mencakup perencanaan, pelaksanaan dan pelaporan Audit Aplikasi SPBE. Lalu, Tim pengawas mutu audit Unit SPBE menyampaikan hasil Evaluasi audit kepada pimpinan Unit SPBE Kemudian, Pimpinan Unit SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil Evaluasi audit

C. Standar Pelaporan
   1. Laporan hasil audit dibuat oleh Unit TIK SPBE dalam bentuk Dokumen Laporan Audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas;
   2. Laporan Audit harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan Audit. Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh *Auditee* secara tertulis dari pejabat *Auditee* yang bertanggung jawab

D. Standar Tindak Lanjut
   1. Pemantauan terhadap legalitas, kompetensi dan kinerja Unit SPBE dilakukan melalui mekanisme registrasi dan laporan tahunan pelaksanaan audit;
   2. Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan, ketua tim audit (*Lead Auditor*) harus menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan dan rekomendasi audit oleh *Auditee*, mencakup cara berkomunikasi dengan *Auditee*, prosedur pemantauan, dan laporan status temuan.

BAB V
TATA CARA PELAKSANAAN AUDIT APLIKASI SPBE

A. Tata Cara Pelaksanaan Audit

Audit Aplikasi SPBE dilakukan Unit TIK SPBE berdasarkan Permintaan *Auditee* atau penugasan Unit. Audit Aplikasi SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar terbagi dalam tiga kelompok tahapan, yaitu:

1. Tahap perencanaan (*pre-audit*);
2. Tahap pelaksanaan lapangan (onsite audit);dan
3. Tahap analisa Data dan pelaporan (*post audit*).

Adapun tiga kelompok tersebut meliputi hal-hal sebagai berikut:

a. penyiapan tim audit;
b. *quick assessment*;
c. penyiapan rencana audit;
d. penyepakatan rencana audit
e. penyiapan protokol audit;
f. penetapan parameter acuan;
g. pertemuan pembukaan;
h. pelaksanaan lapangan;
i. pertemuan penutupan;
j. analisa Data;
k. pengelolaan Data;
l. penyusunan laporan;
m. *proof-read* laporan;
n. penyerahan laporan; dan
o. Evaluasi aktivitas.

Audit Aplikasi SPBE dilakukan oleh sebuah tim audit yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:

1. Pengawas mutu, berperan melakukan monitoring dan Evaluasi aktivitas audit untuk menjamin pelaksanaan audit sesuai dengan standar audit. Pengawas Mutu harus memiliki kualifikasi Auditor Teknologi Utama atau yang setara;
2. *Lead Auditor*, bertanggung jawab merencanakan audit teknologi, melaksanakan audit di lapangan, mengendalikan Data dan melaporkan hasil audit teknologi. Lead Auditor harus mempunyai kualifikasi minimal setara dengan Auditor Teknologi Madya;
3. Auditor, bertugas membantu Lead Auditor dalam aktivitas audit teknologi. Auditor harus mempunyai kualifikasi minimal setara dengan Auditor Teknologi Muda;
4. Asisten Auditor, bertugas membantu Auditor dalam aktivitas audit teknologi;
5. Teknisi, bertugas membantu Auditor dalam pengumpulan Data lapangan;
6. Narasumber, berperan memberi masukan yang berkaitan dengan isu, status teknologi, dan keilmuan yang relevan.

Quick Assessment dilakukan untuk mengenali obyek audit dengan mengidentifikasi: *Current issue* , lokasi organisasi yang diaudit, struktur

organisasi dari organisasi yang diaudit, Proses Bisnis dari organisasi, atau bagian yang diaudit.

Tim Audit Aplikasi SPBE harus merencanakan tindakan audit dengan mendefinisikan hal-hal berikut :

a. tujuan audit;
b. lingkup;
c. pendekatan;
d. kriteria;
e. parameter;
f. acuan;
g. metode pengumpulan Data;
h. penentuan objek;
i. Data primer dan sekunder;
j. metode analisa;
k. deliverable; dan
l. perkiraan jadwal pelaksanaan.

Hal-hal tersebut harus dicantumkan dalam Rencana Audit (*Audit Plan*). Ketua tim audit dan *Audit Plan*. harus menyepakati rencana audit sebelum tahap pelaksanaan audit.

Dalam pelaksanaan kegiatan audit, Tim Audit Aplikasi SPBE harus:

1. menyusun protokol audit yang berisi detail instrumen audit, antara lain:
   a. Daftar Data, pertanyaan dan pengujian; dan
   b. formulir untuk mencatat Data, jawaban, hasil observasi dan hasil pengujian
2. menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan pembanding;
3. melakukan Pertemuan Pembukaan dengan Auditee;
4. melaksanakan audit lapangan, melalui:
   a. penelaahan dokumen;
   b. wawancara;
   c. observasi lapangan;
   d. pengujian; dan
   e. verifikasi bukti.
5. melakukan Pertemuan Penutupan dengan Auditee
6. melakukan analisis bukti; dan
7. mengelola Data

Data status teknologi SPBE dikumpulkan secara objektif berdasarkan fakta yang ada pada *Auditee*. Deskripsi Data dan informasi yang dikumpulkan mengikuti kriteria penilaian berdasarkan ketentuan Peraturan Perundang-undangan dan ditetapkan tersendiri oleh Kepala Unit TIK. Temuan Audit Aplikasi SPBE merupakan keadaan dimana fakta status aset teknologi SPBE *Auditee*; tidak sesuai dengan persyaratan teknis Aplikasi SPBE. Auditor dapat mengurangi atau menambahkan lingkup Data sebagaimana tercantum dalam panduan teknis Audit Infrastruktur SPBE, sepanjang relevan dengan objek dan rencana penggunaan hasil audit sesuai kebutuhan *Auditee*.

Monitoring memberikan informasi untuk suatu kegiatan audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit. Monitoring dilakukan oleh tim pengawas mutu. Tim

pengawas mutu harus menetapkan suatu proses tindak lanjut untuk memonitor dan meyakinkan bahwa tindak lanjut yang telah ditetapkan oleh pimpinan Unit SPBE diimplementasikan secara efektif. Tim pengawas mutu dapat berasal dari pihak eksternal.

Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya. Evaluasi dilakukan oleh tim pengawas mutu setelah aktivitas audit selesai. Tim pengawas mutu menyampaikan hasil Evaluasi audit kepada pimpinan Unit TIK SPBE dan Unit. Pimpinan Unit TIK SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil Evaluasi audit.

B. Tata Cara Pelaporan Audit

Laporan audit disampaikan oleh ketua tim audit kepada pimpinan Unit TIK SPBE. Laporan mencakup latar belakang, tujuan, lingkup, pendekatan audit, kriteria dan acuan, metoda pengumpulan Data, metoda analisa, hasil analisis, temuan dan kesimpulan, dan rekomendasi. Pada setiap halaman dokumen laporan hasil audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurang- kurangnya: tahun pelaksanaan audit, nomor urut atau nomor seri dokumen, domain Aplikasi atau Infrastruktur SPBE, *Auditee*, dan kode pengendalian distribusi salinan dokumen

Draft laporan diriviu oleh ketua tim audit untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit. Laporan Audit disahkan oleh pimpinan Unit TIK SPBE

Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Laporan Audit didistribusikan kepada pimpinan UNIT SPBE. Laporan hasil audit disampaikan oleh pimpinan Unit Tik SPBE kepada UNIT dan lembaga lain sesuai kesepakatan dengan *Auditee*. Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh pimpinan Unit TIK SPBE kepada Unit satu kali dalam satu tahun dengan format sebagai berikut :

FORMAT LAPORAN PERIODIK AUDIT APLIKASI SPBE

A. Identitas UNIT	
Nama Unit	(isi nama Lembaga Pelaksana Audit)
Periode pelaporan	(isi periode pelaporan)
B. Penanggung Jawab Penyelenggaraan Audit	
Nama	(isi nama lengkap)
Jabatan	(isi jabatan resmi)
NIP	(isi Nomor induk pegawai)
Kontak	(isi nomor telepon dan surel ybs)
C. Penyelenggaraan Audit	
Judul Audit TIK	(isi judul)
Tanggal Laporan Audit	(isi tanggal)
Jenis Audit	(isi jenis audit)
Lingkup Audit	(isi lingkup audit)
Ringkasan Hasil Audit	
Ringkasan Temuan (parameter)	Ringkasan Rekomendasi (parameter)
(temuan 1) jenis dan narasi	(rekomendasi 1)

	narasi singkat dan tenggat waktu	
(temuan 2)	(rekomendasi 2)	
D. Tindak Lanjut Audit		
Informasi Tindak Lanjut Audit		
Rekomendasi #1	Tenggat waktu	Tindak Lanjut #1
Rekomendasi #2	Tenggat waktu	Tindak Lanjut #2
Rekomendasi #3	Tenggat waktu	Tindak Lanjut #3

Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh *Auditee*. secara tertulis dari pejabat *Auditee* yang bertanggung jawab.

Laporan pelaksanaan audit dibuat oleh Unit TIK SPBE berdasarkan hasil pelaporan oleh Unit SPBE disampaikan kepada tim koordinasi SPBE nasional dan lembaga lain sesuai ketentuan perundangan.

C. Tata Cara Tindak Lanjut Audit

Kesepakatan proses pemantauan dilakukan dalam bentuk observasi pada *Auditee* pada waktu yang disepakati oleh Unit SPBE dan *Auditee* yang sekurang-kurangnya meliputi: lingkup, objek, jangka waktu, beban pembiayaan, dan penanggung-jawab. Pemantauan dapat dilakukan oleh Unit SPBE atau Auditor lain yang disepakati. Konfirmasi terhadap hasil audit dilakukan paling banyak tiga kali.

Pemantauan dilakukan dalam bentuk observasi pada *Auditee* pada waktu yang disepakati oleh tim koordinasi SPBE nasional. Tindak lanjut perbaikan dari *Auditee* perlu dievaluasi oleh Auditor. Evaluasi dilakukan untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi *Auditee*.

D. Tata Cara Pembiayaan Audit

Pembiayaan untuk pelaksanaan Audit ditanggung oleh *Auditee*. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas Proses Bisnis. Pembiayaan dan mekanisme pelaksanaannya dapat dilakukan melalui kontrak atau swakelola sesuai ketentuan Peraturan Perundang-undangan.

BAB VI
PANDUAN TEKNIS AUDIT APLIKASI SPBE

A. Panduan Teknis Umum Audit Aplikasi SPBE

Panduan teknis Audit Aplikasi SPBE dimaksudkan sebagai acuan dalam menetapkan lingkup area audit aplikasi, kriteria audit, dan penilaian status teknologi Aplikasi SPBE Ruang lingkup panduan audit tata kelola Aplikasi SPBE mencakup aktivitas:

1. Evaluasi Tata Kelola;
2. Pengarahan Tata Kelola; dan
3. Pemantauan Tata Kelola

Audit Manajemen Aplikasi Mencakup Aktivitas :

a. Manajemen Sistem Pengendalian Internal;
b. Manajemen Resiko;
c. Manajemen Aset;
d. Manajemen Pengetahuan;
e. Manajemen SDM;
f. Manajemen Layanan;
g. Manajemen Perubahan; dan
h. Manajemen Data.

Ruang Lingkup Panduan Fungsionalitas dan Kinerja Aplikasi SPB terdiri atas tahapan:

a. Perencanaan Aplikasi;
b. Pengembangan Aplikasi;
c. Pengoperasian Aplikasi; dan
d. Pemeliharaan Aplikasi

Perencanaan aplikasi disusun dalam suatu dokumen menggunakan basis spesifikasi yang mencakup unsur:

a. Kemampuan Aplikasi; dan
b. Persyaratan Proses Bisnis unit.

Kemampuan aplikasi mengacu kepada:

a. Arsitektur SPBE secara berjenjang; dan
b. Persyaratan bisnis organisasi.

Arsitektur SPBE terdiri atas arsitektur SPBE Nasional, Arsitektur SPBE instansi pusat atau Arsitektur SPBE Pemerintah Daerah. Persyaratan proses bisnis *Auditee*, dirumuskan dengan mempertimbangkan kebutuhan, peluang dan Proses Bisnis. Persyaratan tersebut diterjemahkan ke dalam persyaratan aplikasi yang mencakup kebutuhan fungsi, antarmuka, Data, kinerja dan batasan rancangan

Rancangan aplikasi disusun berdasarkan persyaratan aplikasi serta memperhatikan kesesuaiannya terhadap ketentuan perundangan dan integrasi Data. Rancangan tersebut beserta penjelasannya didokumentasikan sebagai Dokumen Deskripsi Rancangan Aplikasi

Aplikasi SPBE dikembangkan oleh tim internal *Auditee* dan/atau pihak ketiga dengan mengacu kepada dokumen Deskripsi Rancangan Aplikasi. Kode sumber (*Source Code*) aplikasi harus dilengkapi dengan dokumentasi yang memadai. Kode sumber (*source code*) aplikasi menggunakan *open source*, dapat dikustomisasi dan dilengkapi dengan dokumentasi yang

memadai. Pengembangan Aplikasi SPBE harus disertai dengan uji coba fungsionalitasnya Pembangunan aplikasi harus didokumentasikan dalam dokumen Prosedur Pembangunan Aplikasi (*System build procedures*) yang dilengkapi dengan panduan instalasi aplikasi untuk menerapkan aplikasi di lingkungan sistem yang ada.

Aplikasi yang dikembangkan mengacu pada ketentuan perundangan yang berlaku.

Pengembangan aplikasi harus dilengkapi dengan dokumentasi penggunaan aplikasi dan tanggungjawab Data pengguna. Penggunaan aplikasi mencakup pengguna dengan klasifikasi *end-users*, dan administrator. Dokumentasi penggunaan aplikasi mencakup:

a. Penggunaan aplikasi secara umum, antara lain: cara instalasi, akses terhadap aplikasi, operasi terhadap Data;
b. Tutorials;
c. Dokumen Teknis;
d. Pesan kesalahan dan penangannya. (*Trouble shooting*); dan
e. Kinerja pengoperasian aplikasi dapat dievaluasi dari fungsi komponen perangkat lunak Sistem Elektronik yang digunakan untuk menjalankan SPBE.

Kinerja sistem elektronik untuk mendukung fungsi *Auditee* dikelompokkan ke dalam 3 klasifikasi, yaitu:

a. Mampu mendukung semua fungsi Proses Bisnis *Auditee*;
b. Mampu mendukung Sebagian fungsi Proses Bisnis *Auditee*, dan
c. Belum mampu mendukung fungsi Proses Bisnis *Auditee*.

Pemeliharaan terhadap aplikasi didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:

a. Lingkup pemeliharaan;
b. Alokasi sumberdaya;
c. Pencatatan kinerja; dan
d. Urutan/rangkaian proses pemeliharaan.

Perubahan terhadap aplikasi didokumentasikan dalam suatu dokumen *Software Configuration Management* yang mencakup:

a. Lingkup konfigurasi;
b. Aktivitas dan manajemen konfigurasi;
c. Sumber daya konfigurasi; dan
d. Penjadwalan manajemen konfigurasi.

Kriteria penilaian audit aplikasi SPBE berdasarkan ketentuan Peraturan Perundang-undangan.

BUPATI NATUNA,

ttd

WAN SISWANDI