BUPATI SUKABUMI
PROVINSI JAWA BARAT
PERATURAN BUPATI SUKABUMI
NOMOR 72 TAHUN 2022

TENTANG
PEDOMAN MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI SUKABUMI,

Menimbang :

a. bahwa dalam rangka untuk mencapai penerapan Sistem Pemerintahan Berbasis Elektronik yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas, diperlukan pedoman manajeman sistem pemerintahan berbasis elektronik di lingkunagn Pemerindah Daerah Kabupaten Sukabumi;
b. bahwa untuk menghasilkan kinerja teknologi informasi dan komunikasi yang baik dan berkelanjutan diperlukan penerapan tata kelola dan manajeman informasi dan komunikasi yang baik melalui audit teknolgi infomormasi dan komunikasi;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Pedoman Manajemen Sistem Pemerintahan Berbasis Elektronik dan Audit Teknologi Informasi dan Komunikasi;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-Daerah Kota Besar dalam Lingkungan Propinsi Djawa Timur, Djawa Tengah, Djawa Barat, dan dalam Daerah Istimewa Jogjakarta (Berita Negara Republik Indonesia Tahun 1950 Nomor 45) sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Pengubahan Undang-Undang Nomor 16 dan Nomor 17 Tahun 1950 (Republik Indonesia dahulu) tentang Pembentukan Kota-Kota Besar dan Kota-Kota Kecil di Jawa (Lembaran Negara Republik Indonesia Tahun 1954 Nomor 40, Tambahan Lembaran Negara Republik Indonesia Nomor 551);
3. 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)

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);

4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah Pusat dan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4. Lembaran Negara Republik Indonesia Nomor 6757);
5. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601) sebagaimana telah diubah dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
6. 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);
7. Peraturan Presiden Nomor 81 Tahun 2010 tentang Grand Design Reformasi Birokrasi 2010-2025;
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Menteri Pendayagunaan Aparatur Negara Reformasi Birokrasi Nomor 10 Tahun 2011 tentang Pedoman Pelaksanaan Program Manajemen Perubahan;
10. Peraturan Menteri Pendayagunaan Aparatur Negara Reformasi Birokrasi Nomor 14 Tahun 2011 tentang Pedoman Pelaksanaan Program Manajemen Pengetahuan (*Knowledge Management*);
11. 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);
12. 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);
13. 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);
14. Peraturan Daerah Kabupaten Sukabumi Nomor 7 Tahun

Lembaran Daerah Kabupaten Sukabumi Nomor 45) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Sukabumi Nomor 17 Tahun 2018 tentang Perubahan Atas Peraturan Daerah Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Pemerintah Kabupaten Sukabumi (Lembaran Daerah Kabupaten Sukabumi Tahun 2018 Nomor 17, Tambahan Lembaran Daerah Kabupaten Sukabumi Nomor 66);

15. Peraturan Daerah Kabupaten Sukabumi Nomor 3 Tahun 2019 tentang Penyelenggaraan Komunikasi, Informatika dan Persandian (Lembaran Daerah Kabupaten Sukabumi Tahun 2019 Nomor 3);
16. Peraturan Bupati Sukabumi Nomor 78 Tahun 2021 tentang Struktur Organisasi dan Tata Kerja Dinas Komunikasi, Informatika dan Persandian (Berita Daerah Kabupaten Sukabumi Tahun 2021 Nomor 78).

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PEDOMAN MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI.

BAB I
KETENTUAN UMUM
Pasal 1

Dalan Peraturan Bupati ini yang dimaksud dengan :

1. Daerah Kabupaten adalah Daerah Kabupaten Sukabumi.
2. Bupati adalah Bupati Sukabumi.
3. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Sukabumi.
4. Pemerintah Daerah Kabupaten yang selanjutnya disebut Pemerintah Daerah Kabupaten adalah Bupati sebagai unsur penyelenggara Pemerintah Kabupaten yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
5. Perangkat Daerah yang selanjutnya disebut PD adalah Unsur Pembantu Bupati dan DPRD dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
7. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas.
8. 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.

BAB II
PEDOMAN MANAJEMAN SPBE DAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

Pasal 2

Ruang lingkup pedoman Manajemen Sistem Pemerintahan Berbasis Elektronik dan Audit Teknologi Informasi dan Komunikasi meliputi:

a. manajemen risiko Sistem Pemerintahan Berbasis Elektronik;
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;
h. manajemen layanan Sistem Pemerintahan Berbasis Elektronik; dan
i. audit Teknologi Informasi dan Komunikasi.

Pasal 3

Pedoman mengenai penerapan Manajemen Sistem Pemerintahan Berbasis Elektronik dan Audit Teknologi Informasi dan Komunikasi sebagaimana tercantum dalam Lampiran sebagai bagian yang tidak terpisahkan dari Peraturan Bupati ini.

BAB III
KETENTUAN PENUTUP

Pasal 4

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Sukabumi.

Ditetapkan di Palabuhanratu
pada tanggal 30 Desember 2022

BUPATI SUKABUMI,

MARWAN HAMAMI

Diundangkan di Palabuhanratu
pada tanggal

SEKRETARIS DAERAH KABUPATEN SUKABUMI,

ADE SURYAMAN

BERITA DAERAH KABUPATEN SUKABUMI TAHUN 2022 NOMOR 72

LAMPIRAN
PERATURAN BUPATI SUKABUMI
NOMOR 72 TAHUN 2022
TENTANG
MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI PEDOMAN MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

BAB I
PENDAHULUAN

A. 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.

Kabupaten Sukabumi pada tahun 2019 memperoleh indeks SPBE sebesar 2,31 dengan predikat Cukup. Kemudian pada tahun 2020 menjadi 2,37 masih dengan predikat Cukup. Tahun 2021 indeks SPBE Kabupaten Sukabumi mengalami penurunan menjadi 1,56. Namun pada tahun 2022 indeks SPBE Kabupaten Sukabumi mengalami kenaikan menjadi 2,29. Indeks yang dihasilkan rata-rata dibawah indeks nasional. Hal tersebut menjadikan indeks yang dihasilkan masih terdapat banyak kekurangan yang perlu ditingkatkan mulai dari domain kebijakan, tata kelola, manajemen, dan layanan publik.

B. Maksud dan Tujuan

Pedoman ini dimaksudkan untuk memberikan panduan bagi Perangkat Daerah di Lingkungan Pemerintah Daerah Kabupaten Sukabumi dalam menerapkan Manajemen SPBE dan Audit TIK serta bertujuan untuk peningkatan penerapan SPBE di Lingkungan Pemerintah Daerah Kabupaten Sukabumi dan diharapkan bahwa pelayanan publik di Kabupaten Sukabumi dapat lebih efektif dan efisien, serta masyarakat dapat lebih mudah dalam mengakses informasi dan pelayanan publik yang tersedia.

C. Ruang Lingkup

Ruang Lingkup Pedoman ini meliputi:

a. manajemen risiko Sistem Pemerintahan Berbasis Elektronik;
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

manajemen layanan Sistem Pemerintahan Berbasis Elektronik i. Audit Teknologi Informasi dan Komunikasi.

BAB II
MANAJEMEN RISIKO SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK KABUPATEN SUKABUMI

A. PENDAHULUAN
1. Latar Belakang

Permasalahan dalam pengembangan SPBE secara nasional disebabkan oleh beberapa faktor diantaranya yaitu sebagai berikut: (1) Permasalahan pertama adalah belum adanya tata kelola SPBE yang terpadu di tingkat nasional maupun di tingkat Instansi Pusat dan Pemerintah Daerah; (2) 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; (3) 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: pertama, teknologi *mobile internet* dapat dimanfaatkan untuk kemudahan akses layanan pemerintah melalui gawai personal pengguna yang bebas bergerak tanpa batasan waktu dan lokasi; kedua, teknologi *cloud computing* memberikan efektivitas dan efisiensi yang tinggi untuk melakukan integrasi TIK; ketiga, 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; keempat, teknologi *big data analytics* mampu memberikan dukungan pengambilan keputusan dan penyusunan kebijakan bagi pemerintah; dan kelima, 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 Kabupaten Sukabumi sebagai penyelenggara SPBE. Untuk menjamin keberlangsungan penerapan SPBE, diperlukan manajemen risiko SPBE yang diterapkan Pemerintah Daerah Kabupaten Sukabumi 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 Kabupaten Sukabumi dalam melaksanakan Manajemen Risiko SPBE di lingkungannya.

Sedangkan tujuan dari Manajemen Risiko SPBE adalah:

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

3. Manfaat

Manfaat dari penerapan Manajemen Risiko SPBE dalam penerapan SPBE adalah:

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

4. Ruang Lingkup

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

1. Kerangka Kerja Manajemen Risiko SPBE;
2. Proses Manajemen Risiko SPBE;
3. Struktur Manajemen Risiko SPBE; dan
4. Budaya Sadar Risiko SPBE.

5. Pengertian Umum

1. Manajemen Risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE.
2. Risiko SPBE adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan penerapan SPBE.
3. Risiko SPBE Positif adalah peluang terjadinya suatu peristiwa yang akan meningkatkan keberhasilan terhadap pencapaian tujuan penerapan SPBE.
4. Risiko SPBE Negatif adalah peluang terjadinya suatu peristiwa yang akan menurunkan keberhasilan terhadap pencapaian tujuan penerapan SPBE
5. 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.

6. Area Dampak Risiko SPBE adalah pengelompokan area yang terkena dampak dari Risiko SPBE.
7. Kriteria Risiko SPBE adalah parameter atau ukuran secara kuantitatif atau kualitatif yang digunakan untuk menentukan Kriteria Kemungkinan Risiko SPBE dan Kriteria Dampak Risiko SPBE.
8. Kriteria Kemungkinan Risiko SPBE adalah besarnya peluang terjadinya suatu Risiko SPBE dalam periode tertentu.
9. Kriteria Dampak Risiko SPBE adalah besarnya akibat terjadinya suatu Risiko SPBE yang mempengaruhi sasaran SPBE.
10. Besaran Risiko SPBE adalah nilai Risiko SPBE yang dihasilkan dari proses analisis Risiko SPBE.
11. Level Risiko SPBE adalah pengelompokan Besaran Risiko SPBE yang mendeskripsikan tingkat Risiko SPBE.
12. 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 Kabupaten Sukabumi. Tujuan dari kerangka kerja Manajemen Risiko SPBE adalah untuk membantu Pemerintah Daerah 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.

Gambar 1. Kerangka Kerja Manajemen Risiko SPBE

I. Peningkatan Nilai dan Perlindungan

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

1. Terintegrasi, yaitu Manajemen Risiko SPBE merupakan serangkaian proses yang terintegrasi dengan proses pelaksanaan tugas dan fungsi Pemerintah Daerah Kabupaten;
2. 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;
3. Dapat disesuaikan, yaitu kerangka kerja dan proses Manajemen Risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal Pemerintah Daerah Kabupaten Sukabumi dalam penerapan SPBE;
4. Inklusif, yaitu Manajemen Risiko SPBE melibatkan semua pemangku kepentingan sesuai dengan pengetahuan, pandangan, dan persepsinya untuk membangun budaya sadar Risiko SPBE di Pemerintah Daerah Kabupaten Sukabumi;
5. Dinamis, yaitu Manajemen Risiko SPBE dapat dipergunakan untuk mengantisipasi dan merespon perubahan konteks Pemerintah Daerah Kabupaten Sukabumi dengan tepat dan sesuai waktu;
6. 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;
7. 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
8. Perbaikan berkelanjutan, yaitu Manajemen Risiko SPBE senantiasa dikembangkan melalui strategi perbaikan manajemen secara berkelanjutan dan peningkatan kematangan penerapan Manajemen Risiko SPBE.

II. Kepemimpinan dan Komitmen

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

1. Integrasi

Kerangka kerja Manajemen Risiko SPBE hendaknya diintegrasikan dengan proses pelaksanaan tugas dan fungsi Pemerintah Daerah Kabupaten Sukabumi. 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.

2. Desain

Perancangan kerangka kerja Manajemen Risiko SPBE dilakukan dengan cara:

a. Memahami struktur dan konteks organisasi termasuk tujuan, sasaran, dan kompleksitas organisasi;

b. Mengekspresikan komitmen pimpinan terhadap penerapan kerangka kerja Manajemen Risiko SPBE dalam bentuk kebijakan, pernyataan, atau bentuk dukungan lainnya;
c. Menetapkan kewenangan, tanggung jawab, dan akuntabilitas dari setiap peran di dalam kerangka kerja Manajemen Risiko SPBE;
d. Menyediakan sumber daya yang diperlukan seperti SDM dan kompetensi, anggaran, proses dan prosedur, informasi dan pengetahuan, dan pelatihan; dan
e. Membangun komunikasi dan konsultasi untuk efektivitas implementasi kerangka kerja Manajemen Risiko SPBE.

3. Implementasi

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

4. Pemantauan dan Evaluasi

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

5. 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.

III. 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 Kabupaten Sukabumi untuk pengambilan keputusan di tingkat strategis, operasional, dan pelaksanaan proyek. Proses Manajemen Risiko SPBE yang dilaksanakan oleh Pemerintah Daerah Kabupaten terdiri atas proses:

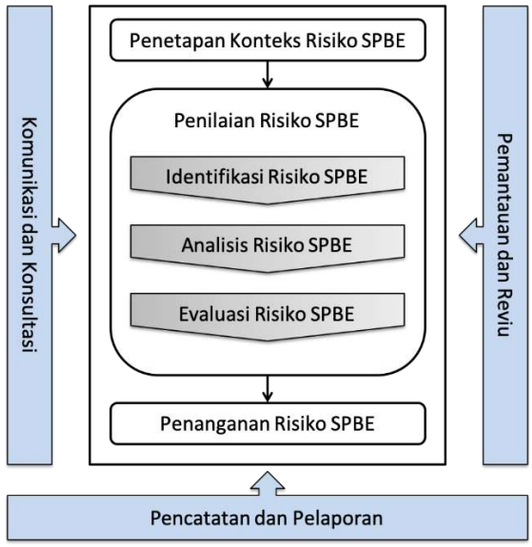
1. komunikasi dan konsultasi;
2. penetapan konteks Risiko SPBE;
3. penilaian Risiko SPBE, yang terdiri atas identifikasi Risiko SPBE, analisis Risiko SPBE, dan Evaluasi Risiko SPBE;
4. penanganan Risiko SPBE;
5. pemantauan dan reviu;
6. pencatatan dan pelaporan.

Sedangkan, tata kelola Manajemen Risiko SPBE merupakan mekanisme untuk mengatur kewenangan dan memastikan akuntabilitas pelaksanaan Manajemen Risiko SPBE Pemerintah Daerah Kabupaten. 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 Kabupaten 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.



Gambar 2. Proses Manajemen Risiko

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, Informatika dan Persandian Kabupaten Sukabumi.
Tugas UPR SPBE	Membantu Bupati dalam melaksanakan urusan pemerintahan yang menjadi kewenangan daerah dan tugas pembantuan di bidang Komunikasi dan Informatika, Persandian dan Statistik.
Fungsi UPR SPBE	Menetapkan kebijakan teknis tentang penyelenggaraan pelayanan komunikasi, informatika, persandian dan statistik.
Periode Waktu	1 Januari - 31 Desember 2023

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 Daerah Kabupaten Sukabumi	4,0

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	Kepala Dinas Komunikasi Informatika dan Persandian Kabupaten Sukabumi.
Koordinator Risiko SPBE	Sekretaris Dinas Komunikasi Informatika dan Persandian Kabupaten Sukabumi.
Pengelola Risiko SPBE	Kepala Bidang Aplikasi Informatika pada Dinas Komunikasi Informatika dan Persandian Kabupaten Sukabumi.

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	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 berikut 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 masing-masing 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 Sistem Pemerintahan Berbasis Elektronik	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	Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik	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 Kabupaten Sukabumi, merupakan Risiko SPBE yang berkaitan dengan penyusunan dan pelaksanaan perencanaan pembangunan SPBE Nasional dan Kabupaten/Kota;
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 Sukabumi;
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 Sukabumi; 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 Kabupaten Sukabumi. 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
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 berikut 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 berikut 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
	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 Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang-Kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

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

1) Identifikasi Risiko SPBE

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

a. Jenis Risiko SPBE

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

b. Kejadian

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

c. Penyebab

Penyebab dapat diidentifikasi dari akar masalah yang menjadi pemicu munculnya Risiko SPBE. Penyebab dapat berasal dari lingkungan internal maupun eksternal Instansi Pusat dan Pemerintah Daerah. Identifikasi penyebab akan membantu menemukan tindakan yang tepat untuk menangani Risiko SPBE.

d. Kategori

Penentuan Kategori Risiko SPBE didasarkan pada penyebab dari munculnya Risiko SPBE. Kategori Risko SPBE telah dijelaskan pada bagian angka 2 huruf f tentang Penetapan Kategori Risiko SPBE.

e. Dampak

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

f. Area Dampak

Penentuan Area Dampak Risiko SPBE didasarkan pada dampak yang telah teridentifikasi. Area Dampak Risiko telah dijelaskan pada bagian angka 2 huruf g 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 diEvaluasi	Kurangnya jumlah evaluator eksternal	SDM SPBE	Penurunan kinerja	Kinerja

2) Analisis Risiko SPBE

Analisis Risiko SPBE merupakan proses untuk melakukan penilaian atas Risiko SPBE yang telah diidentifikasi sebelumnya. Analisis Risiko SPBE dilakukan dengan cara menentukan sistem pengendalian, level

kemungkinan, dan level dampak terjadinya Risiko SPBE. Informasi yang dicantumkan pada analisis Risiko SPBE meliputi:

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

b. Level Kemungkinan

Penentuan level kemungkinan dilakukan dengan mengukur persentase probabilitas atau frekuensi peluang terjadinya Risiko SPBE dalam satu periode yang dicocokkan dengan Kriteria Kemungkinan Risiko SPBE sebagaimana telah dijelaskan pada bagian angka 2 huruf h. Penentuan level kemungkinan harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level kemungkinan tersebut.

c. Level Dampak

Penentuan level dampak dilakukan dengan mengukur besar dampak dari terjadinya Risiko SPBE yang dicocokan dengan Kriteria Dampak Risiko SPBE sebagaimana telah dijelaskan pada bagian angka 2 huruf h. Level dampak harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan level dampak tersebut.

d. Besaran Risiko SPBE dan Level Risiko SPBE

Penentuan Besaran Risiko SPBE dan Level Risiko SPBE didapat dari kombinasi Level Kemungkinan dan Level Dampak dengan menggunakan rumusan dalam Matriks Analisis Risiko SPBE sebagaimana telah dijelaskan pada bagian angka 2 huruf i.

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	Peningkatan 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

3) Evaluasi Risiko SPBE

Evaluasi Risiko SPBE dilakukan untuk mengambil keputusan mengenai perlu tidaknya dilakukan upaya penanganan Risiko SPBE lebih lanjut serta penentuan prioritas penanganannya. Pengambilan keputusan mengacu pada Selera Risiko SPBE yang telah ditentukan sebagaimana telah dijelaskan pada bagian angka 2 huruf j. 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:

a. Opsi Penanganan Risiko SPBE

Opsi penanganan Risiko SPBE, berisikan alternatif yang dipilih untuk menangani Risiko SPBE. Opsi penanganan Risiko SPBE dilakukan dengan mengidentifikasi berbagai opsi yang mungkin untuk diterapkan. Opsi penanganan Risiko SPBE terbagi menjadi dua, yaitu penanganan Risiko SPBE Positif dan penanganan Risiko SPBE Negatif. Adapun opsi yang ditentukan pada pedoman ini meliputi:

(1). Opsi Penanganan Risiko Positif

a) Eskalasi Risiko

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

b) Eksploitasi Risiko

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

c) Peningkatan Risiko

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

d) Pembagian Risiko

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

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

(2). Opsi Penanganan Risiko Negatif

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

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

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

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

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

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

c. Keluaran
Keluaran merupakan hasil dari rencana aksi penanganan Risiko SPBE.

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

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

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	Penagggung Jawab
Eksploitasi Risiko	o Pembinaan dan pengawasan lebih ditingkatkan; o Perbaikan dan penerapan SOP yang tegas; o Memasang sumber listrik yang tertutup; o Akses kunci masuk area lebih diperketat/ pemasangan kunci secara digital; o Menambah kapasitas BW; o Membuat peraturan tata tertib dengan sanksi yang tegas.	Kemungkinan terjadinya risiko akan dapat diminimalisir	Triwulan I dan II	Bidang Aplikasi Informatika
Mitigasi Risiko	Pengadaan Barang/jasa yaitu Pengadaan Sever serta sarana dan prasarana lainnya	Server sesuai kebutuhan	Triwulan II	Bidang Aplikasi 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:
   a) Formulir Konteks Risiko SPBE
      Formulir Konteks Risiko SPBE merupakan dokumen dari aktivitas penetapan konteks pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 2.0.
   b) Formulir Penilaian Risiko SPBE
      Formulir Penilaian Risiko SPBE merupakan dokumen dari aktivitas penilaian Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 3.0.
   c) Formulir Rencana Penanganan Risiko SPBE
      Formulir Rencana Penanganan Risiko SPBE merupakan dokumen dari aktivitas penanganan Risiko SPBE pada proses Manajemen Risiko SPBE. Formulir ini dapat dilihat pada Formulir 4.0.
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:
   a) Dokumen Kegiatan Komunikasi dan Konsultasi
      Dokumen Kegiatan Komunikasi dan Konsultasi merupakan dokumen dari aktivitas pelaksanaan kegiatan komunikasi dan konsultasi. Dokumen dapat berbentuk notulensi dan laporan atau dokumen lainnya yang dihasilkan dari pelaksanaan kegiatan komunikasi dan konsultasi.
   b) Dokumen Laporan Pemantauan
      Dokumen Laporan Pemantauan merupakan dokumen dari aktivitas pelaksanaan kegiatan pemantauan Risiko. Dalam pedoman ini menggunakan 2 format laporan yaitu laporan pemantauan triwulan dan laporan pemantauan tahunan.
      Laporan pemantauan triwulan menggambarkan kondisi pelaksanaan dalam waktu setiap tiga bulan terkait rencana aksi penanganan yang meliputi besaran/level Risiko SPBE saat ini dan proyeksi Risiko SPBE, penanganan yang telah dilakukan, rencana penanganan, penanggung jawab, dan waktu pelaksanaan.
      Laporan pemantauan tahunan merangkum laporan triwulan I sampai dengan triwulan IV dengan berfokus pada tendensi

besaran Risiko SPBE dan memberikan rekomendasi penanganan Risiko SPBE yang dapat digunakan sebagai masukan pelaksanaan proses Manajemen Risiko SPBE pada tahun selanjutnya. Format laporan pemantauan triwulan dan tahunan dapat dilihat pada formulir 5.0 di bawah ini.

Formulir 5.0

Laporan Pemantauan Risiko SPBE Triwulan I			
	Nama Unit	:	Dinas Komunikasi Informatika dan Persandian Kabupaten Sukabumi
	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.

Laporan Pemantauan Risiko SPBE Triwulan I

Laporan Pemantauan Risiko SPBE Triwulan I			
	Nama Unit	:	Dinas Komunikasi Informatika dan Persandian Kabupaten Sukabumi
	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 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 yang telah dilakukan
Pengadaan Barang/Jasa yaitu pengadaan server

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

Contoh Pengisian Formulir 5.0 Laporan Pemantauan Risiko SPBE Triwulan I

Laporan Pemantauan Risiko SPBE Tahunan

Laporan Pemantauan Risiko SPBE Triwulan I		
Nama Unit	:	Dinas Komunikasi Informatika dan Persandian Kabupaten Sukabumi
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 dan Proyeksi Risiko SPBE
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 SPBE 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

Contoh Pengisian Formulir 5.0 Laporan Pemantauan Risiko SPBE Tahunan

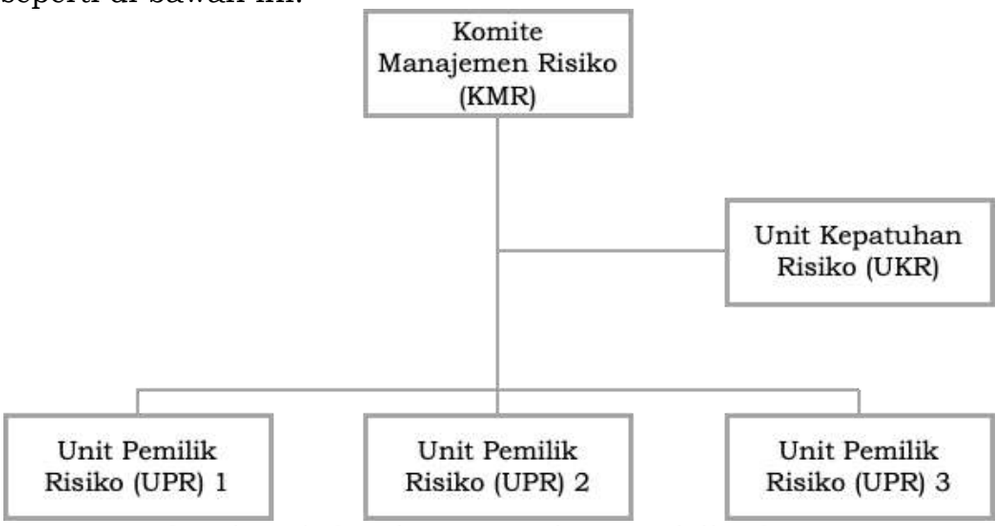
D. STRUKTUR MANAJEMEN DAN BUDAYA SADAR RISIKO SPBE

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.

I. Struktur Manajemen Risiko SPBE

Struktur Manajemen Risiko SPBE terdiri atas:

1. Komite Manajemen Risiko (KMR) SPBE yang memiliki fungsi penetapan kebijakan strategis terkait Manajemen Risiko SPBE.
2. Unit Pemilik Risiko (UPR) SPBE yang memiliki fungsi pelaksanaan Manajemen Risiko SPBE.
3. 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.

1. 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:

a. penyusunan dan penetapan kebijakan Manajemen Risiko SPBE;
b. penyusunan dan penetapan kerangka kerja dan pedoman pelaksanaan Manajemen Risiko SPBE;
c. penyusunan dan penetapan pakta integritas Manajemen Risiko SPBE;
d. penyusunan dan penetapan konteks Risiko SPBE;
e. pengendalian proses Risiko SPBE melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan Evaluasi terhadap penerapan Manajemen Risiko SPBE; dan
f. pelaksanaan komitmen pimpinan dan penerapan budaya sadar Risiko SPBE.

2. Unit Pemilik Risiko (UPR) SPBE

Unit Pemilik Risiko SPBE yang disingkat UPR SPBE merupakan unit kerja di Pemerintah Daerah Kota 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:

a. Pemilik Risiko SPBE merupakan pejabat yang bertanggung jawab atas pelaksanaan penerapan Manajemen Risiko SPBE di unit organisasi tersebut;
b. 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;
c. 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:

a. penyusunan dan penetapan penilaian Risiko SPBE dan rencana pelaksanaan Manajemen Risiko SPBE termasuk rencana kontinjensi penanganan Risiko SPBE;
b. pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan;
c. pelaksanaan operasional Manajemen Risiko SPBE yang efektif melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan Evaluasi; dan
d. pelaksanaan pembinaan budaya sadar Risiko SPBE melalui sosialisasi, bimbingan, pelatihan, dan supervisi penerapan Manajemen Risiko SPBE.

3. 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:

a. Penyusunan kebijakan pengawasan terhadap penerapan Manajemen Risiko SPBE;

b. pelaksanaan pengawasan intern terhadap penerapan Manajemen Risiko SPBE di semua UPR SPBE melalui audit, reviu, pemantauan, Evaluasi, dan kegiatan pengawasan lainnya;
c. pelaksanaan konsultasi dan asistensi kepada UPR SPBE dalam penerapan Manajemen Risiko SPBE;
d. penyusunan dan penyampaian rekomendasi terhadap efektivitas penerapan Manajemen Risiko SPBE kepada KMR SPBE dan UPR SPBE; dan
e. pelaksanaan konsultasi dan asistensi kepada UPR dalam pembinaan budaya sadar Risiko SPBE.

II. 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.

c. Pengukuran tingkat kesiapan budaya sadar Risiko SPBE.
   Pengukuran ini biasanya menggunakan kuesioner yang 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.
d. 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:
      a. 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.

b. 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.
c. 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.

E. FORMAT FORMULIR

FORMULIR 1.0

PAKTA INTEGRITAS MANAJEMEN RISIKO SPBE

<Logo Pemerintah Daerah Kabupaten Sukabumi>

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.	Sasaran SPBE	Indikator Kinerja	Identifikasi Risiko SPBE						Analisis Risiko SPBE							Evaluasi Risiko SPBE	
			Jenis Risiko SPBE	Kejadian	Penyebab	Kategori	Dampak	Area Dampak	Sistem pengendalian	Kemungkinan		Dampak		Besaran Risiko	Level Risiko	Keputusan Penanganan Risiko SPBE (Ya/Tidak)	Prioritas Risiko
										Level	Penjelasan	Level	Penjelasan				

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 SPBE

Penanganan Yang telah dilakukan

Rekomendasi	

BAB III
PEDOMAN TAHAPAN PENERAPAN MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH KABUPATEN SUKABUMI

A. PENDAHULUAN

Keamanan informasi menjadi hal yang sangat penting bagi yang menggunakan teknologi informasi, hal ini dikarenakan informasi merupakan aset yang harus dilindungi keamanannya. Penerapan Keamanan informasi bertujuan untuk menjamin keberlangsungan ketersediaan informasi dari risiko yang mungkin terjadi yang dapat menyebabkan pengelolaan proses menjadi terganggu. Untuk itu, Dinas Kominfo dan Persandian mempunyai tanggung jawab mengelola informasi agar terhindar dari risiko kerusakan, kehilangan atau terungkapnya informasi ke pihak luar. Proses perlindungan terhadap informasi tersebut harus dikelola dengan baik sehingga informasi yang dihasilkan dapat terjaga kerahasiannya, keakuratannya, dan ketersedian secara efektif. Semakin banyak informasi organisasi yang disimpan dan dikelola, maka semakin besar pula risiko terjadinya kerusakan, kehilangan atau terungkapnya informasi ke pihak luar yang tidak diinginkan. Proses perlindungan terhadap informasi tersebut harus dikelola dengan baik sehingga informasi yang dihasilkan dapat terjaga kerahasiannya (confidentiality), keakuratannya (integrity), dan ketersedian (availability) secara efektif.

B. Sasaran

Sejalan dengan pentingnya informasi, maka sasaran utama dari kebijakan keamanan informasi ini adalah memberikan arahan mengenai proses-proses keamanan informasi terkait dengan perlindungan terhadap aset teknologi informasi yang digunakan. Keamanan informasi dapat dicapai dengan penerapan secara menyeluruh dan konsisten terhadap kontrol keamanan informasi yang tertuang dalam kebijakan ini. Penggunaan, dan pengelolaan informasi melatarbelakangi disusunnya kebijakan keamanan informasi yang mengacu pada standar internasional sistem manajemen keamanan informasi sebagai panduan dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) di lingkungan Dinas Kominfo dan Persandian.

C. Tujuan

Dokumen ini bertujuan untuk menyediakan kerangka kerja dalam penerapan pengendalian pengamanan informasi dan untuk meningkatkan pengertian umum mengenai penerapan Sistem Manajemen Kemanan Informasi (SMKI) yang disesuaikan dengan standar yang berlaku mengenai Pengamanan Informasi.

Dengan adanya Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan di Dinas Kominfo dan Persandian diharapkan dapat meningkatkan perlindungan terhadap perangkat dan aplikasi dan mengurangi resiko penyalahgunaan informasi yang ada dalam rangka mengamankan data dan informasi milik Pemerintah Daerah Kabupaten Sukabumi.

D. Ruang Lingkup

Lingkup dalam kebijakan keamanan informasi di Dinas Kominfo dan Persandian ini mengacu kepada kontrol keamanan standard ISO 27001:2013.

E. KEBIJAKAN KEAMANAN INFORMASI

1. Arahan Manajemen Untuk Keamanan Informasi

Kebijakan Keamanan informasi bertujuan untuk melindungi aset organisasi yang dikelola dan digunakan agar terhindar dari berbagai ancaman internal maupun eksternal yang meliputi keamanan data, perangkat teknologi, infrastruktur dan sistem, seluruh aktivitas serta proses yang terkait dengan penyediaan informasi.

2. Kebijakan Keamanan Informasi

Aturan Kebijakan:

a) Dokumen kebijakan keamanan informasi harus disetujui oleh Kepala Dinas Kominfo dan Persandian untuk penerapan di lingkungan Pemerintah Daerah Kabupaten Sukabumi.
b) Dokumen Kebijakan Keamanan Informasi ini harus disosialisasikan kepada seluruh pegawai di lingkungan Pemerintah Daerah Kabupaten Sukabumi.

3. Peninjauan (review) Kebijakan Keamanan informasi

Aturan Kebijakan:

a) Dokumen kebijakan keamanan informasi harus dievaluasi setidaknya 1 kali dalam 1 tahun untuk menjaga kesesuaian efektifitas penerapannya.
b) Apabila dari hasil peninjauan terdapat perubahan maka harus dilakukan pengkinian terhadap dokumen kebijakan tersebut.

F. ORGANISASI KEAMANAN INFORMASI

1. Organisasi Internal

Dinas Kominfo dan Persandian harus secara jelas menetapkan tugas dan tanggung jawab serta proses koordinasi dalam proses keamanan informasi.

a) Tugas dan Tanggung Jawab keamanan informasi
   Aturan Kebijakan:
   1) Tugas dan tanggung jawab terkait keamanan informasi di lingkungan Pemerintah Daerah Kabupaten Sukabumi harus didefinisikan dan dialokasikan secara formal.
   2) Tugas dan tanggung jawab yang dimaksud dalam butir (1) diatas perlu mencakup:
      a. Tugas dan tanggung jawab pengamanan aset informasi dan pengelolaan informasi yang dimiliki dan/atau dikelola dalam lingkungan Dinas Kominfo dan Persandian.
      b. Tugas dan tanggung jawab untuk pengambilan keputusan terkait proses keamanan informasi.
   3) Setiap pegawai Dinas Kominfo dan Persandian harus memahami mengenai tugas dan tanggung jawab terkait proses operasional yang dilakukan dan kontrol keamanan informasi yang diterapkan dalam melindungi aset informasi dan aset pengolahan informasi yang dimiliki dan/atau dikelola dalam lingkungan Dinas Kominfo dan Persandian.
b) Pemisahan Tugas dan Tanggung Jawab
   Aturan Kebijakan:
   1) Tugas dan tanggung jawab dalam pekerjaan kritikal perlu dipisahkan untuk mengurangi risiko adanya penyalahgunaan aset informasi dan pengolahan informasi, baik disengaja maupun tidak disengaja.
   2) Pekerjaan kritikal yang dimaksud dalam butir (1) diatas mencakup namun tidak terbatas dalam:
      a. Pengembangan dan Operasional Sistem Informasi;

b. Operasional dan Keamanan Sistem Informasi;
c. Proses permohonan dan otorisasinya.

3) Apabila pemisahan tugas dan tanggung jawab tidak dapat diimplementasikan, kontrol tambahan perlu diimplementasikan.
4) Kontrol yang dimaksudkan dalam butir (3) diatas mencakup namun tidak terbatas pada:
   a. Pemantauan aktifitas pekerjaan;
   b. Mengaktifkan log / audit trail;
   c. Pengawasan manajemen;
   d. Rotasi tugas secara berkala

c) Hubungan dengan pihak berwenang
Aturan Kebijakan:
1) Daftar nomor telepon pihak berwenang seperti pihak ketiga Polisi, Pemadam Kebakaran, Pihak Keamanan Gedung, Pihak Penyedia Layanan Komunikasi dan lainnya perlu didata untuk melaporkan dan/atau menanggulangi insiden keamanan informasi.

d) Hubungan dengan Special Interest Group
Aturan Kebijakan:
1) Hubungan dengan pihak-pihak khusus seperti forum atau asosiasi profesional yang terkait dengan keamanan informasi harus dimiliki sebagai media untuk:
   a. Mendapat informasi terkini mengenai risiko atau ancaman terkait keamanan informasi;
   b. Mendapatkan informasi mengenai solusi terkini terkait kontrol keamanan informasi.
2) Implementasi dari butir (1) diatas mencakup namun tidak terbatas pada keanggotaan pada forum, asosiasi profesional maupun mailing list terkait keamanan informasi.

e) Keamanan Informasi Dalam Manajemen Proyek
Aturan Kebijakan:
1) Setiap pelaksanaan Proyek di lingkungan Pemda Kabupaten Sukabumi perlu memperhatikan aspek keamanan informasi.
2) Aspek keamanan informasi yang dimaksud mencakup proses risk assessment serta identifikasi dan implementasi kontrol keamanan informasi dalam pengelolaan setiap proyek.
3) Setiap proyek yang melibatkan pihak eksternal perlu memasukkan aspek kerahasiaan dalam perjanjian kerjasama.

2. Mobile Computing dan Teleworking

Proses ini bertujuan untuk memastikan keamanan informasi saat bekerja menggunakan perangkat mobile computing dan teleworking.

a. Kebijakan perangkat mobile
Aturan Kebijakan:
1) Pengguna fasilitas Notebook harus menjaga keamanan dari perangkat dan informasi yang disimpan pada perangkat pada saat digunakan di luar area organisasi.
2) Penggunaan fasilitas Notebook di luar area kantor harus dilengkapi dengan kontrol keamanan fisik untuk mencegah terjadinya pencurian/kehilangan perangkat.

3) Fasilitas Notebook milik Pemda Kab. Sukabumi tidak boleh ditinggalkan tanpa pengawasan atau tanpa pengamanan pada saat digunakan diluar area kantor.
4) Penggunaan fasilitas Notebook milik Pemda Kab. Sukabumi yang menyimpan informasi sensitif pada area publik, seperti restoran, stasiun, atau bandara harus sangat dibatasi.
5) Penggunaan fasilitas Wifi publik untuk mengirim informasi sensitif milik Dinas Kominfo dan Persandian harus sangat dibatasi.

b. Teleworking
Aturan Kebijakan:
1) Aktifitas teleworking tidak boleh dilakukan oleh personil Dinas Kominfo dan Persandian.

G. KEAMANAN SUMBER DAYA MANUSIA

1. Sebelum status kepegawaian dimulai (Prior to employment)

Proses keamanan sumber daya manusia dimulai sejak sebelum status kepegawaian dimulai. Status kepegawaian ini juga mencakup pihak ketiga yang memiliki aktivitas pekerjaan di lingkungan Dinas Kominfo dan Persandian.

a. Penyaringan (screening)
Aturan Kebijakan:
1) Pemeriksaan latar belakang harus dilakukan untuk setiap calon pegawai Dinas Kominfo dan Persandian yang memegang tugas pokok kritikal pada sistem.
2) Proses verifikasi latar belakang dapat dilakukan antara lain dengan:
a) Verifikasi terhadap referensi pengalamanpekerjaan;
b) Verifikasi terhadap kualifikasi akademik;
c) Verifikasi terhadap catatan kepolisian;
3) Verifikasi juga perlu dilakukan terhadap kompetensi calon pegawai dalam melaksanakan tugas dan tanggung jawab di lingkungan Dinas Kominfo dan Persandian.

b. Syarat dan Ketentuan Pegawai
Aturan Kebijakan:
1) Kewajiban pegawai untuk menjaga keamanan informasi perlu dicantumkan dalam kontrak kerja dan/atau tata tertib organisasi.
2) Setiap pegawai harus memahami kewajibannya untuk menjaga keamanan informasi yang terdapat dalam kontrak kerja dan/atau tata tertib organisasi.

2. Pada saat status kepegawaian berjalan

Proses ini bertujuan untuk menjamin bahwa personil Dinas Kominfo dan Persandian dan pihak ketiga yang bekerja di lingkungan Pemda Kabupaten Sukabumi memahami ancaman yang terkait dengan keamanan informasi termasuk tanggung jawabnya.

a. Tanggung Jawab Manajemen
Aturan Kebijakan:
1) Semua Kepala Bidang di Dinas Kominfo dan Persandian memahami dan menjalankan kebijakan dan prosedur kerja yang berlaku.

b. Kesadaran, Pendidikan dan Pelatihan Terkait Dengan Keamanan Informasi
Aturan Kebijakan:

1) Sosialisasi mengenai keamanan informasi kepada semua Pegawai Dinas Kominfo dan Persandian harus dilakukan secara berkala.
2) Materi sosialisasi pada butir (1) perlu disesuaikan dengan tugas dan tanggung jawab pekerjaan dari pegawai.

c. Proses Pendisiplinan

Aturan kebijakan:

1) Setiap pegawai dalam lingkungan Dinas Kominfo dan Persandian yang melakukan pelanggaran terkait keamanan informasi harus ditangani sesuai dengan proses pendisiplinan secara formal yang terdapat di dalam tata tertib organisasi.
2) Pemberian sanksi harus menimbang dan disesuaikan dengan tingkat pelanggaran yang dilakukan.

3. Pemberhentian atau pergantian status kepegawaian.

Untuk menjaga keamanan informasi organisasi pada saat proses pemberhentian dan penggantian status kepegawaian.

a. Pemberhentian atau Pergantian Status Kepegawaian.

Aturan Kebijakan:

1) Tanggung jawab keamanan informasi yang masih berlaku setelah pegawai sudah tidak bekerja lagi di lingkungan Dinas Kominfo dan Persandian atau setelah proses mutasi kerja, perlu diinformasikan kepada personil tersebut.
2) Hal ini mencakup namun tidak terbatas dari:
   a) Tidak menyebarkan informasi sensitif milik DKIP kepada pihak yang tidak berwenang.
   b) Tidak melakukan aktifitas yang dapat mengganggu keamanan informasi di lingkungan DKIP.

H. PENGELOLAAN ASET

1. Tanggung Jawab Terkait Aset

Untuk menjamin dan menjaga perlindungan terhadap aset Informasi dan pengolahan informasi milik Dinas Kominfo dan Persandian maka setiap aset harus diidentifikasi serta ditentukan kepemilikannya.

a. Inventarisasi Aset

Aturan Kebijakan:

1) Semua aset informasi dan pengolahan informasi yang dimiliki, digunakan dan/atau dikelola di lingkungan Dinas Kominfo dan Persandian harus diinventarisasi. Aset yang dimaksud meliputi:
   - Aset informasi, dalam bentuk *softcopy* maupun *hardcopy*.
   - Aset perangkat lunak dan aplikasi.
   - Aset fisik yang mengolah dan menyimpan informasi meliputi PC, Notebook, server, removable media, printer, dan scanner, dan untuk mesin fotokopi.
   - Aset jaringan, yang meliputi perangkat, layanan koneksi, dan keamanan jaringan.
   - Aset sarana maupun layanan pendukung seperti, Genset, UPS, serta AC.
   - Aset sumber daya manusia.
2) Daftar inventarisasi aset tersebut harus diperiksa kesesuaiannya dan dilakukan pengkinian secara berkala, minimal satu kali dalam satu tahun.
3) Setiap terdapat perubahan pada inventarisasi aset, sebagai contoh karena ada aset baru, perubahan peruntukan

maupun penghapusan aset, harus tercermin dalam daftar inventarisasi aset.

b. Kepemilikan Aset

Aturan Kebijakan:

1) Setiap aset dalam daftar inventarisasi aset harus dialokasikan kepemilikannya.
2) Kepemilikan aset dapat dialokasikan kepada individu atau unit kerja dalam lingkungan DKIP.
3) Pemilik dari aset tersebut akan bertanggung jawab dalam proses pengamanan aset tersebut.

c. Penggunaan Aset Yang Diterima

Aturan Kebijakan:

1) Aset informasi dan pengolahan informasi milik Dinas Kominfo dan Persandian hanya boleh digunakan untuk kebutuhan pekerjaan.
2) Penggunaan perangkat pribadi untuk mengakses informasi dan jaringan komunikasi DKIP harus melalui persetujuan Pejabat terkait di Dinas Kominfo dan Persandian.
3) Pada saat jam kerja, penggunaan jaringan komunikasi dan layanan jaringan, seperti fasilitas internet serta email, milik DKIP hanya untuk kebutuhan pekerjaan.
4) Penggunaan fasilitas internet DKIP untuk melakukan akses ke situs-situs yang mengandung materi pornografi, kekerasan, materi yang dapat mengundang kebencian terkait dengan suku, agama dan ras serta materi bajakan yang melanggar hak atas kekayaan intelektual, sangat dilarang.
5) Penggunaan modem data pada komputer milik DKIP dilarang dilakukan pada saat komputer tersebut terhubung ke jaringan komunikasi.

d. Pengembalian Aset

Aturan Kebijakan:

1) Setiap pegawai yang sudah tidak berkerja di lingkungan <unit> harus mengembalikan aset informasi dan pengolahan informasi milik DKIP yang sudah bukan menjadi kewenangannya.
2) Pengembalian aset dilakukan secara formal dan terdokumentasi sesuai dengan ketentuan yang berlaku.

2. Klasifikasi Informasi

Untuk menjaga dan menjamin keamanan informasi, klasifikasi terhadap informasi perlu dilakukan dengan mempertimbangkan kebutuhan, prioritas, sensitifitas, dan kritikalitas dalam proses bisnis Dinas Kominfo dan Persandian.

a. Klasifikasi Informasi

Aturan Kebijakan:

1) Klasifikasi jenis aset informasi di Dinas Kominfo dan Persandian disesuaikan dengan kebutuhan dan dampak bisnis. Klasifikasi tersebut meliputi:
   - Informasi Rahasia, yaitu informasi yang sangat sensitif dan hanya dapat diakses oleh individu / pihak tertentu.
   - Informasi Internal, yaitu data yang hanya dapat diakses secara internal dalam lingkungan Dinas Kominfo dan Persandian.
   - Informasi terbatas, yaitu informasi yang dapat diakses oleh pihak tertentu yang sudah diberikan otorisasi.

- Informasi publik, yaitu informasi yang dapat disebarkan ke publik.

2) Setiap Kepala Bidang di Dinas Kominfo dan Persandian dapat mengklasifikasikan informasi yang dianggap perlu sebagai informasi rahasia, di luar ketentuan perundang-undangan yang berlaku untuk mencegah gangguan terhadap proses bisnis organisasi.
3) Perlindungan terhadap aset informasi harus dilakukan secara memadai sesuai dengan klasifikasinya.
4) Tingkat perlindungan aset informasi dilakukan sesuai dengan aturan penanganan informasi yang diterapkan di lingkungan Dinas Kominfo dan Persandian.

b. Pelabelan dan Penanganan Informasi
Aturan Kebijakan:
1) Informasi harus diberi label / kode untuk memastikan penanganan informasi tersebut sesuai dengan tingkat klasifikasinya.
2) Pelabelan informasi dapat dilakukan melalui:
   a. Pelabelan secara fisik pada dokumen *hardcopy;*
   b. Pemberian *watermark* pada dokumen *softcopy;*
   c. Pemberian klasifikasi informasi pada *metadata* dari informasi *softcopy*.
3) Penanganan informasi harus dilakukan secara aman pada seluruh siklus hidup informasi yang mencakup proses pemrosesan, penyimpanan, distribusi, dan pemusnahan informasi.
4) Penanganan informasi perlu disesuaikan dengan klasifikasi dari informasi tersebut.

c. Penanganan Aset
Aturan Kebijakan:
1) Penanganan terhadap aset harus sesuai dengan klasifikasi dari aset informasi yang disimpan dan/atau diproses oleh aset tersebut untuk memastikan keamanan dari aset informasi.

3. Penanganan Media Penyimpanan Informasi

Pengelolaan ini diperlukan untuk mencegah pengungkapan (disclosure), modifikasi, removal atau penghancuran dari informasi sehingga harus dilindungi secara fisik.

a. Pengelolaan Removable Media
Aturan Kebijakan:
1) Penanganan *removable media* perlu disesuaikan dengan klasifikasi dari informasi yang disimpan didalamnya.
2) *Removable media* yang digunakan dalam lingkungan Dinas Kominfo dan Persandian perlu diinventarisasi.
3) Perangkat yang digunakan untuk mengakses *removable media* tersebut perlu mempunyai fitur keamanan yang memadai.
4) Informasi dalam *removable media* yang tidak akan digunakan kembali harus dihapus secara permanen.
5) Pegawai Dinas Kominfo dan Persandian harus selalu melakukan *scanning virus* terhadap *removable media* (*flash disk, external harddisk, tape backup*) untuk mencegah adanya kerusakan informasi akibat *malware*.
6) *Removable media* yang sensitif terhadap kondisi lingkungan (temperatur, kelembaban, debu) harus disimpan dalam

tempat yang sesuaidengan spesifikasi teknis yang disarankan.

b. Pemusnahan Media

Aturan Kebijakan:

1) Pemilik informasi atau pengelola media penyimpan informasi bertanggung jawab terhadap pemusnahan data/informasi.
2) Proses penghapusan informasi dari media penyimpanan perlu dilakukan sedemikian rupa sehingga dapat dipastikan bahwa informasi yang sudah dihapus, tidak dapat dibaca, digunakan dan diduplikasi kembali.
3) Proses pemusnahan informasi dalam bentuk *hardcopy* dapat dilakukan dengan menggunakan mesin *shredding*.
4) Penghapusan informasi dari media penyimpanan informasi elektronis dapat dilakukan dengan metode format ulang, penghancuran media, atau dengan metode *degaussing* (magnetisasi).
5) Dalam hal media penyimpan elektronis akan dialihkan peruntukkannya, maka data/informasi yang tersimpan dalam media tersebut yang dimaksud harus dihapus sebelum medianya dialihkan peruntukkannya.

I. PENGENDALIAN AKSES

1. Prasyarat Bisnis Dalam Pengendalian Akses

Proses ini bertujuan untuk mengendalikan akses kepada seluruh personil Dinas Kominfo dan Persandian dan pihak ketiga yang bekerja di lingkungan Dinas Kominfo dan Persandian untuk pengamanan informasi DKIP.

a. Kebijakan pengendalian hak akses

Aturan Kebijakan:

1) Pemberian hak akses terhadap Informasi dan sistem informasi harus disesuaikan dengan kewenangan yang dimiliki dari pihak yang akan mengakses dengan memperhatikan prinsip *need to know* dan *need to use*.
2) Pemetaan antara hak akses ke informasi dan sistem informasi, dengan tugas pekerjaan (*jobrole*) pegawai perlu didokumentasikan secara sebagai panduan dasar pemberian hak akses.
3) Akses ke sistem informasi wajib menggunakan *User ID* yang bersifat *unique* dan *password*.
4) Hak akses khusus (*privileged access rights*), seperti administrator sistem perlu teridentifikasi dan pemegang hak tersebut perlu terdokumentasikan.
5) Mekanisme untuk pengajuan, otorisasi, pengadministrasian, pemantauan dan peninjauan hak akses, perludidokumentasikan secara formal.
6) Peninjauan terhadap pemetaan hak akses dan alokasi hak akses perlu dilakukan secara berkala, paling sedikit satu kali dalam 3 (tiga) bulan.

b. Akses Ke Jaringan Dan Layanan Jaringan

Aturan Kebijakan:

1) Perangkat komputer yang terhubung ke jaringan dan layanan jaringan DKIP harus dilengkapi dengan mekanisme pengendalian akses pada sistem operasinya.
2) Akses ke segmentasi jaringan perlu dibatasi sesuai dengan tugas dan tanggung jawab operasional pengguna.

3) Pemetaan antara segmentasi jaringan dengan pengguna jaringan perlu ditetapkan dan didokumentasikan.
4) Akses ke segmentasi jaringan dimana terdapat perangkat sistem informasi kritikal (*server farm* atau *storage farm*) harus dikendalikan dan dibatasi sesuai dengan kebutuhan dari pengguna.
5) Akses ke jaringan nirkabel (Wifi) perlu diamankan dengan menggunakan *password* yang sesuai dengan kebijakan manajemen *password* yang berlaku.
6) Perangkat milik pribadi tidak diperkenankan untuk terhubung ke jaringan internal DKIP.
7) Semua akses ke perangkat jaringan DKIP hanya dapat dilakukan oleh administrator jaringan yang telah mendapatkan otorisasi dari Kepala Dinas Kominfo dan Persandian.
8) Akses ke jaringan internal secara *remote* harus dikontrol dan diamankan.
9) Akses ke jaringan internal secara *remote* harus mendapatkan persetujuan dari Kepala Dinas Kominfo dan Persandian.
10) Akses ke jaringan internal secara *remote* oleh pihak ketiga harus dibatasi jangka waktunya hanya pada saat munculnya kebutuhan akses secara *remote.*
11) Penggunaan jaringan dan layanan jaringan perlu dipantau dan ditinjau berkala melalui proses *review* dari *audit log*.
12) Jaringan dan layanan jaringan di Dinas Kominfo dan Persandian sedapat mungkin menerapkan teknologi pengamanan, seperti otentifikasi dan enkripsi jaringan.

2. Pengelolaan Akses Pengguna

Proses ini bertujuan untuk memastikan akses pengguna ke sistem informasi merupakan akses yang telah terotorisasi dan mencegah akses yang tanpa otorisasi ke dalam sistem informasi. Hal ini mencakup semua tahapan mulai registrasi *account* pengguna baru sampai dengan penghapusan *account* dari pengguna yang tidak memerlukan lagi akses ke dalam sistem informasi.

a. Pendaftaran dan penghapusan pengguna (*user*) sistem informasi
Aturan Kebijakan:
1) Proses registrasi dan deregistrasi pengguna ke sistem informasi DKIP harus ditetapkan secara formal dan diterapkan secara konsisten.
2) Hal ini mencakup proses permohonan, persetujuan dan pembuatan / penghapusan *user* ID.
3) *User ID* harus bersifat unik dan dapat dipetakan dengan identitas pengguna.
4) Penggunaan *user* ID secara *sharing* harus sangat dibatasi.
5) Penggunaan *user* ID secara *sharing* hanya dapat diizinkan apabila terdapat alasan operasional yang tidak dapat dihindari dan telah disetujui oleh kepala unit kerja yang membidangi keamanan sistem informasi di DKIP.
6) Segera mencabut atau menonaktifkan *user id* personil Dinas Kominfo dan Persandian yang telah berganti fungsi pekerjaan atau telah meninggalkan lingkungan DKIP.
7) Seluruh proses pendaftaran dan pencabutan pengguna harus didokumentasikan dengan baik.

b. Pemberian Hak Akses Pengguna
   Aturan Kebijakan:
   1) Permintaan untuk pemberian hak akses pengguna ke sistem informasi harus disetujui oleh atasan dari pengguna dan pemilik dari informasi atau sistem informasi.
   2) Persetujuan pemberian hak akses pengguna perlu menimbang kebutuhan operasional pekerjaan yang telah didokumentasikan dalam pemetaan hak akses.
   3) Pemberian hak akses hanya dapat dilakukan setelah persetujuan dalam butir (1) telah diberikan.
   4) Seluruh proses pemberian hak akses pengguna harus terdokumentasi dengan baik.

c. Pengelolaan Hak Akses Khusus (privileged access rights)
   Aturan Kebijakan:
   1) Hak akses khusus adalah hak akses ke informasi maupun sistem informasi dengan kemampuan (*privilege*) yang lebih tinggi dibandingkan hak akses lainnya. Sebagai contoh adalah hak akses dengan kemampuan (*privilege*) administrator atau *full access*.
   2) Pemberian dan penggunaan hak akses khusus harus dibatasi dan dikendalikan kepada personil dengan tugas dan tanggung jawab yang sesuai.
   3) Proses otorisasi dan catatan dari semua hak akses khusus yang diberikan harus didokumentasikan.
   4) Hak akses khusus perlu diberikan dalam format *user ID* yang berbeda dengan hak akses biasa dan bersifat sementara.
   5) Penggunaan hak akses khusus secara *sharing* harus sangat dibatasi.
   6) Penggunaan hak akses khusus secara *sharing* hanya dapat diizinkan apabila terdapat alasan operasional yang tidak dapat dihindari dan telah disetujui oleh kepala biro yang membidangi keamanan sistem informasi di DKIP.
   7) Penggunaan hak akses khusus secara *sharing* harus dikendalikan antara lain dengan kontrol-kontrol berikut:
      a. Penggantian *password* secara berkala;
      b. Penggantian *password* segera setelah salah satu pemegang hak tersebut tidak bekerja lagi atau mengalami mutasi kerja.
   8) Penggunaan hak akses khusus harus dimonitor untuk memastikan tidak adanya akses tanpa ijin.
   9) Hak akses khusus dengan tujuan untuk pelaksanaan audit terhadap sistem informasi harus diberikan dengan kemampuan (*privilege*) *read only*.

d. Pengelolaan Informasi Otentifikasi Rahasia Milik Pengguna
   Aturan Kebijakan:
   1) Informasi otentikasi rahasia adalah informasi rahasia yang digunakan untuk mengotentikasikan seorang pengguna. Contoh dari informasi ini adalah *password, smartcard, token,* atau PIN.
   2) Pengguna harus memahami kewajiban mereka untuk menjaga keamanan dari informasi otentikasi rahasia yang mereka miliki.
   3) Pengguna dilarang untuk memberikan informasi otentikasi rahasia miliknya kepada pihak lain.

4) Untuk informasi otentikasi dalam bentuk *password,* apabila pengguna terpaksa memberikan informasi tersebut kepada pihak lain, maka pengguna tersebut harus mengganti informasi tersebut pada kesempatan pertama.
5) Pemberian informasi otentikasi dalam bentuk *password* untuk pertama kali dapat menggunakan *password* sementara yang harus diganti oleh pengguna setelah proses *login* untuk pertama kalinya.
6) Informasi otentikasi yang bersifat *default* dari *vendor* perangkat atau aplikasi sistem informasi harus diganti pada saat instalasi perangkat atau aplikasi tersebut.

e. Peninjauan Terhadap Hak Akses Pengguna
Aturan Kebijakan:
1) Peninjauan hak akses dilakukan untuk memastikan kesesuaian hak akses yang dialokasikan dengan kondisi terkini dari pengguna, terkait kewenangan dan status kepegawaian, dari pengguna.
2) Pemilik atau administrator dari perangkat dan aplikasi sistem informasi harus melakukan peninjauan terhadap hak akses pengguna secara berkala minimal satu kali dalam 3 (tiga) bulan atau apabila terdapat perubahan pada:
   a. Status kepegawaian seperti mutasi atau terminasi.
   b. Proses bisnis organisasi.
   c. Proses sistem informasi.
3) Hak akses khusus (*privileged*) harus ditinjau secara *reguler* dengan jangka waktu setiap 1 (satu) bulan.

f. Perubahan atau Pencabutan Hak Akses
Aturan Kebijakan:
1) Pengguna yang mengalami perubahan fungsi pekerjaan/mutasi harus segera melaporkan perubahan tersebut dan mengajukan permintaan perubahan hak akses paling lambat 7 hari setelah perubahan/mutasi tersebut.
2) Perubahan hak akses hanya dapat dilakukan setelah persetujuan dari atasan pengguna dan pemilik informasi atau sistem informasi dengan memperhatikan pemetaan hak akses pengguna.
3) Pencabutan Hak akses pengguna dapat dilakukan:
   a. Atas permintaan dan persetujuan dari atasan pengguna dan pemilik sistem informasi;
   b. Secara otomatis, apabila pengguna sudah tidak bekerja lagi di lingkungan DKIP.
4) Hak akses untuk pengguna yang sudah tidak bekerja lagi di lingkungan DKIP harus dicabut atau di-*suspend* satu hari setelah hari terakhir pengguna tersebut.
5) Seluruh proses perubahan dan pencabutan hak akses pengguna harus terdokumentasi dengan baik.

3. Tanggung Jawab Pengguna (user)

Kontrol-kontrol ini bertujuan agar pengguna memiliki pemahaman mengenai penggunaan akses secara aman.

a. Penggunaan Informasi Otentifikasi Pengguna yang Bersifat Rahasia
Aturan Kebijakan:
1) Informasi otentikasi rahasia adalah informasi rahasia yang digunakan untuk mengotentikasikan seorang pengguna.

Contoh dari informasi ini adalah *password, smartcard, token,* atau PIN.

2) Setiap pengguna wajib menggunakan Informasi otentikasi rahasia dalam proses otentikasi ke perangkat dan aplikasi sistem informasi organisasi.
3) Setiap pengguna wajib menjaga kerahasiaan informasi otentikasi rahasia dan menghindari menyimpan informasi otentikasi rahasia di tempat terbuka atau tempat yang tidak memiliki pengamanan yang memadai.
4) Setiap Pegawai Dinas Kominfo dan Persandian wajib mengganti informasi otentikasi rahasia apabila ada indikasi adanya penyalahgunaan atau kebocoran.
5) Apabila password digunakan sebagai Informasi otentikasi rahasia, maka catatan yang berisi password tidak boleh disimpan pada tempat terbuka atau tanpa pengamanan yang memadai.
6) Apabila password digunakan sebagai Informasi otentikasi rahasia, maka password harus berkualitas dengan karakteristik sebagai berikut:
   - Panjang minimal karakter *password* pada perangkat dan aplikasi sistem informasi yang digunakan adalah 6 (enam) karakter;
   - Menggunakan kombinasi huruf dan angka dan sedapat mungkin menggunakan karakter khusus (*special character*), seperti: !$%#*, kecuali apabila perangkat atau aplikasi tidak memungkinkan.
   - Penggunaan perangkat atau aplikasi yang tidak dimungkinkan mengikuti kebijakan penggunaan *password* yang berkualitas harus mendapatkan persetujuan dari kepala unit kerja keamanan informasi dengan mempertimbangkan kebutuhan operasional, risiko dan kontrol kompensatif.
7) Password tidak boleh sama dengan User ID dan tidak berdasar pada sesuatu yang mudah ditebak misalnya: nama, nomor telepon, tanggal lahir, nama anggota keluarga, nama/identitas perusahaan.
8) Mengganti password secara berkala setiap 3 (tiga) bulan dengan menghindari menggunakan password yang sudah pernah digunakan.
9) Setiap pengguna wajib menjaga kerahasiaan password dan tidak diperkenankan memberikan password-nya kepada orang lain dan atau menggunakan *password* milik orang lain.

4. Pengendalian Akses Informasi dan Aplikasi

Proses ini bertujuan untuk mencegah akses tanpa wewenang ke sistem di Dinas Kominfo dan Persandian dengan membatasi akses ke sistem jaringan.

a. Pembatasan akses informasi
   Aturan Kebijakan:
   1) Akses ke informasi oleh pengguna harus dibatasi sesuai dengan tugas dan tanggung jawabnya.
b. Prosedur *log-on* secara aman
   Aturan Kebijakan:
   1) Akses ke sistem operasi harus dikontrol dengan menggunakan mekanisme *secure logon* meliputi:

- Tidak memberikan informasi bantuan yang dapat menyebabkan *log-on* tanpa ijin.
- Membatasi jumlah kesalahan dalam percobaan *log-on.*
- Tidak menampilkan karakter *password* pada saat *log-on.* Tampilan karakter *password* dapat diganti dengan simbol.

c. Sistem Pengelolaan Password
Aturan Kebijakan:
1) Sistem pengelolaan *password* harus dapat:
   a. Memastikan penggantian *password* secara *reguler* yaitu maksimal 3 (tiga) bulan sekali.
   b. Memastikan kualitas *password* sesuai dengan aturan dalam kebijakan ini.
   c. Memastikan penyimpanan dan pengiriman informasi *password* secara aman.

d. Penggunaan Program Utilisasi Khusus.
Aturan Kebijakan:
1) Penggunaan *system utility programs* yang berpotensi dapat mengambil alih pengendalian perangkat dan aplikasi sistem informasi harus dibatasi dan dikendalikan secara ketat.
2) *Administrator* harus melakukan proses identifikasi dan otorisasi untuk seluruh *system utilities* yang digunakan.

J. KRIPTOGRAFI

1. Pengendalian Kriptografi

Proses ini bertujuan untuk menjaga kerahasian, keaslian dan integritas informasi dengan menggunakan teknologi kriptografi.

a. Kebijakan penggunaan kriptografi
Aturan Kebijakan:
1) Penggunaan kriptografi perlu dipertimbangkan untuk menjaga kerahasiaan, keaslian dan integritas informasi;
2) Penggunaan kriptografi perlu mempertimbangkan kekuatan dari algoritma kriptografi.
3) Penggunaan kriptografi perlu dipertimbangkan untuk melindungi informasi pada perangkat *mobile* atau *removable* media.
4) Penggunaan teknologi kriptografi harus ditinjau terlebih dahulu oleh kepala biro yang membidangi keamanan informasi.
5) Penggunaan teknologi kriptografi harus disetujui terlebih dahulu oleh kepala biro yang membidangi teknologi informasi.

2. Manajemen dari key untuk kebutuhan kriptografi
Aturan Kebijakan:
1) Seluruh *key* kriptografi harus dilindungi dari modifikasi, kehilangan serta kerusakan.
2) Pengelolaan *key* kriptografi harus menggunakan prinsip *dual custody,* dimana *key* kriptografi tidak boleh diketahui oleh hanya satu personil saja.
3) Untuk *key* kriptografi dalam bentuk *cleartext,* maka pengiriman informasi dan *key* yang digunakan untuk mengenkripsi informasi tersebut harus dilakukan dalam media komunikasi yang berbeda. Sebagai contoh, pengiriman dokumen elektronik dilakukan melalui media email sedangkan pengiriman *password* yang digunakan untuk mengenkripsi dokumen tersebut dilakukan melalui SMS atau telepon.

K. KEAMANAN FISIK DAN LINGKUNGAN

1. Wilayah yang Aman

   Wilayah yang aman diperoleh melalui pembatasan wilayah dengan menggunakan pembatasan fisik untuk mencegah akses fisik tanpa ijin yang dapat menimbulkan gangguan, kehilangan atau kerusakan terhadap informasi milik DKIP.

   a. Perimeter Keamanan Fisik

      Aturan Kebijakan:

      1) Pembatasan wilayah dengan pembatas secara fisik harus digunakan untuk melindungi area yang berisi informasi dan atau fasilitas pengolahan informasi.
      2) Pengamanan fisik ruangan di Dinas Kominfo dan Persandian mengacu kepada klasifikasi wilayah masing-masing ruangan dengan menggunakan pembatas dan pengendalian akses fisik.

   b. Pengendalian Akses Fisik

      Aturan Kebijakan:

      1) Akses fisik wilayah aman harus dikendalikan untuk menjamin tidak adanya akses tanpa ijin.
      2) Tamu atau pihak ketiga yang datang ke area kerja di Dinas Kominfo dan Persandian harus tetap didampingi atau diawasi.
      3) Tamu atau pihak ketiga yang mengakses area kritikal di Dinas Kominfo dan Persandian hanya untuk pegawai yang mempunyai kewenangannya dan diotorisasi oleh Pejabat penanggung jawab di ruang tersebut dan harus diawasi dan didampingi oleh pegawai di ruangan tersebut.

   c. Pengamanan Ruang Kantor dan Fasilitasnya

      Aturan Kebijakan:

      1) Ruangan kerja dan fasilitas di Dinas Kominfo dan Persandian perlu diberikan pengamanan secara memadai dengan mempertimbangkan pemisahan dari wilayah akses umum.
      2) Untuk area kritikal di Dinas Kominfo dan Persandian tidak dipasang informasi / petunjuk lokasi yang jelas.
      3) Apabila memungkinkan, fasilitas yang digunakan untuk pemrosesan dan penyimpanan informasi sensitif sebaiknya terpisah dengan fasilitas yang digunakan untuk pekerjaan sehari-hari.

   d. Perlindungan Terhadap Ancaman Eksternal dan Lingkungan

      Aturan Kebijakan:

      1) Peralatan pemadam kebakaran yang memadai harus tersedia pada tempat yang sesuai.
      2) Khusus ruangan kritikal (*data center*) di Dinas Kominfo dan Persandian menggunakan peralatan pemadam kebakaran yang bersifat *non-liquid*.

   e. Bekerja di Area Aman

      Aturan Kebijakan:

      1) Pekerjaan yang dilakukan oleh pihak ketiga di area kritikal (*data center*) di lingkungan Dinas Kominfo dan Persandian harus selalu diawasi oleh personil penanggung jawab area tersebut untuk menghindari kegiatan yang tidak diinginkan.
      2) Setiap pegawai dan pihak ketiga dilarang membawa makanan, minuman, rokok, dan barang berbahaya ke dalam wilayah tertutup.
      3) Setiap pegawai dan pihak ketiga yang memasuki wilayah tertutup tidak diperkenankan membawa peralatan *visual*

recording (*camera, handphone* berkamera) tanpa otorisasi dari pejabat berwenang.

f. Area untuk delivery dan loading
   Aturan Kebijakan:
   1) Akses di wilayah *loading area* yang dapat memasuki wilayah Dinas Kominfo dan Persandian harus diamankan untuk menghindari akses tanpa ijin.

2. Perangkat

Pengamanan ini diperlukan untuk mencegah kehilangan, kerusakan, pencurian terhadap aset atau gangguan terhadap aktivitas.

a. Perlindungan dan penempatan peralatan
   Aturan Kebijakan:
   1) Perangkat pengolahan informasi yang dianggap kritikal perlu ditempatkan secara aman termasuk membatasi sudut pandang untuk mengurangi orang yang tidak berkepentingan yang dapat melihat informasi yang ditampilkan.

b. Sarana Pendukung
   Aturan Kebijakan:
   1) Semua sarana pendukung seperti *power supply*, *genset*, lampu darurat, dan *air conditioner* harus tersedia untuk mendukung kegiatan operasional Dinas Kominfo dan Persandian dan dipelihara secara berkala.

c. Pengamanan pengkabelan
   Aturan Kebijakan:
   1) Kabel listrik dan jaringan komunikasi harus terlindungi dan tidak diletakkan di area publik sehingga tidak mengalami kerusakan akibat ketidaksengajaan oleh personil maupun gigitan binatang pengerat.
   2) Penandaan kabel digunakan di Ruang *Server* Jaringan untuk mempermudah penanganan apabila terjadi masalah dan menghindari kesalahan dan didokumentasikan dengan baik.

d. Pemeliharaan peralatan
   Aturan Kebijakan:
   1) Peralatan sistem informasi seperti perangkat keras dan jaringan komunikasi, serta sarana pendukung harus dipelihara untuk menjamin ketersediaan dari peralatan tersebut secara terus menerus.

e. Pemindahan Peralatan Milik Dinas Kominfo dan Persandian
   Aturan Kebijakan:
   1) Peralatan, informasi, maupun perangkat lunak tidak boleh di bawa keluar wilayah Dinas Kominfo dan Persandian tanpa adanya ijin dari Pejabat terkait di Dinas Kominfo dan Persandian.

f. Pengamanan peralatan diluar wilayah DKIP
   Aturan Kebijakan:
   1) Penggunaan peralatan pengolahan informasi diluar wilayah Dinas Kominfo dan Persandian mempertimbangkan kebutuhan penggunaan aset tersebut.
   2) Aset TI yang bersifat *portable* seperti *notebook* yang dibawa ke luar area kantor tidak boleh ditinggalkan di area publik tanpa pengamanan yang memadai kabel pengunci (*cable lock*) serta *password*.

g. Pemusnahan atau Penggunaan Kembali Peralatan Secara Aman
Aturan Kebijakan:
1) Seluruh Aset TI yang akan dimusnahkan atau digunakan kembali harus diperiksa dan dipastikan bahwa tidak ada lagi data sensitif yang tersimpan dalam perangkat sehingga tidak dimungkinkan lagi untuk mengambil informasi yang sebelumnya terkandung di perangkat tersebut.

h. Perlindungan untuk perangkat yang tidak dalam pengawasannya
Aturan Kebijakan:
1) Pengguna harus memastikan aset yang sedang tidak digunakan telah terlindungi dengan baik dengan menghentikan (*terminate*) *session* aktif terhadap sistem setelah selesai digunakan.
2) Pengguna harus mengunci layar sistem operasi pada komputernya (*screen lock*) apabila meninggalkan komputernya.
3) Komputer perlu dilindungi dengan fitur penguncian layar secara otomatis (*screen saver lock*) apabila tidak aktifitas pada layar komputer selama 5 menit.

i. Clear desk dan clear screen
Aturan Kebijakan:
1) Seluruh personil Dinas Kominfo dan Persandian harus menerapkan *clear desk* dan *clear screen* terkait dengan keamanan informasi yang rahasia atau sensitif.
2) Semua informasi sensitif yang berbentuk *hardcopy* atau yang tersimpan dalam media penyimpanan dalam lemari yang terkunci.
3) Komputer harus di *log-off*/mengunci layar komputernya apabila sedang tidak digunakan.
4) Memindahkan dengan segera dokumen yang mengandung informasi sensitif dari mesin *printer.*

L. KEAMANAN OPERASIONAL

1. Tanggung Jawab dan Prosedur Operasional

Kendali sistem keamanan ini berfungsi untuk memastikan bahwa proses operasional fasilitas pengolahan informasi berjalan dengan benar dan aman.

a. Prosedur Operasional Yang Terdokumentasi
Aturan Kebijakan:
1) Setiap sistem yang dioperasikan di Dinas Kominfo dan Persandian harus dilengkapi dengan prosedur dan petunjuk pengoperasian.
2) Prosedur dan petunjuk ini harusdipelihara untuk menjaga kesesuaian dengan kondisi terkini.
3) Prosedur dan petunjuk ini harus tersedia bagi seluruh pengguna sistem informasi yang membutuhkannya.

b. Manajemen Perubahan
Aturan Kebijakan:
1) Seluruh perubahan dalam infrastruktur TI dan sistem aplikasi harus dikelola dan dikendalikan untuk menghindari terjadinya kegagalan dalam sistem informasi.
2) Pengendalian perubahan diterapkan pada infrastruktur dan sistem harus mengacu pada prosedur yang mempertimbangkan antara lain:
- Aspek risiko yang muncul terhadap kebutuhan bisnis.

- Dokumentasi atas *log* perubahan sesuai urutan waktu perubahan.
- Perencanaan dan pengujian perubahan.
- Tersedianya persetujuan formal untuk usulan perubahan
- *Review* dan pemantauan terhadap pelaksanaan perubahan.

c. Manajemen Kapasitas
Aturan Kebijakan:
1) Setiap penanggung jawab sistem di Dinas Kominfo dan Persandian harus melakukan mengelola kapasitas sistem informasi baik dalam pengembangan sistem aplikasi baru maupun bagi sistem yang sedang berjalan.
2) Proses pengelolaan kapasitas ini mempertimbangkan proyeksi kebutuhan operasional dan kebutuhan bisnis di masa datang.
3) Pengukuran kapasitas beserta pelaporannya dilakukan secara periodik minimal satu kali dalam satu tahun.

d. Pemisahan Lingkungan Pengembangan, Pengujian dan Operasional Sistem Informasi.
1) Lingkungan sistem informasi yang digunakan untuk proses pengembangan, pengujian dan operasional sistem informasi di DKIP harus dipisahkan.
2) Lingkungan sistem informasi yang dimaksud mencakup namun tidak terbatas pada *server,* hak akses pengguna dan/atau segmentasi jaringan.
3) Pemisahan yang dimaksud dapat dilakukan secara fisik maupun *logical.*

2. Perlindungan terhadap Malware

Pengguna sistem informasi di Dinas Kominfo dan Persandian perlu memahami bahaya dari *Malware* dan mengetahui bagaimana mencegah serta menangani adanya *Malware.*

a. Pengendalian Terhadap Malware
Aturan Kebijakan:
1) Kontrol terhadap *Malware* dapat dilakukan melalui pendeteksian dan pencegahan serangan *Malware* dan pemulihan setelah terjadi serangan dari *Malware*.
2) Pegawai Dinas Kominfo dan Persandian harus melindungi sistem informasi dari serangan *Malware* dengan tidak meng-*install* perangkat lunak bajakan, dan/atau perangkat lunak yang tidak sesuai dengan kebutuhan kerja.
3) Setiap perangkat seperti PC dan Notebook, dan server harus menggunakan antivirus untuk mencegah bahaya Malware (virus, worm, trojan).
4) Setiap personil Dinas Kominfo dan Persandian harus memastikan bahwa setiap file dokumen elektronis yang berasal dari media penyimpanan atau jaringan, termasuk e-mail dan internet, tidak mengandung virus dengan melakukan scanning terhadap file atau program tersebut sebelum mengakses atau menggunakan.
5) Update dan scanning rutin harus dilakukan secara otomatis untuk memastikan kemampuan program antivirus untuk mendeteksi dan menangani malware pada komputer dan mediapenyimpanan.

3. Backup

Proses *backup* diperlukan untuk menjamin integritas dan ketersediaan informasi serta fasilitas pengolahan informasi.

a. *Backup* Informasi

Aturan Kebijakan:

1) Informasi elektronis yang bersifat rahasia atau kritikal (memiliki tingkat integritas dan ketersediaan tinggi) harus memiliki *backup*, sehingga dalam hal data/informasi utama tidak dapat dibaca, rusak, dan lain sebagainya, masih dapat menggunakan data *backup*.
2) Frekuensi dan tingkat backup (penuh atau parsial) disesuaikan dengan kebutuhan kritikalitas bisnis.
3) Hasil backup harus disimpan pada tempat yang aman dan diusahakan ditempatkan diluar lokasi utama dan diberikan perlindungan secara fisik dan lingkungan yang memadai.
4) Media backup harus diuji secara berkala melalui uji restore untuk memastikan media tersebut dapat berfungsi dengan baik pada saat dibutuhkan.
5) Masa retensi dari backup informasi tergantung dari tingkat kritikalitas suatu informasi dan sistem yang dioperasikan di Dinas Kominfo dan Persandian.

4. Logging dan Pemantauan

Sistem informasi Dinas Kominfo dan Persandian perlu diawasi dan setiap kejadian keamanan informasi harus didokumentasikan dan dievaluasi berkala untuk memantau efektivitas dari kontrol keamanan informasi yang diterapkan.

a. Event Logging

Aturan kebijakan:

1) *Log* audit harus direkam dan disimpan pada sistem untuk memantau aktivitas pengguna dalam jangka waktu yang ditentukan.
2) *Log* audit yang perlu disimpan mencakup pada aspek berikut:
   - *User ID*
   - Tanggal dan waktu serta *detail* dari kejadian penting (*key events*) dalam sistem seperti *logon* dan *logoff.*
   - *Records* untuk percobaan akses baik yang berhasil maupun gagal.

b. Perlindungan terhadap informasi log

Aturan Kebijakan:

1) *Log system* harus dilindungi dari modifikasi dan akses tanpa ijin yaitu pembatasan terhadap perubahan atau penghapusan terhadap *log files.*
2) Administrator sistem harus memastikan kapasitas penyimpanan dari *log files* untuk menghindari penyimpanan yang penuh yang dapat menyebabkan kegagalan dalam untuk mencatat kejadian (*event*) atau *overwriting* kejadian (*event*) yang lama.
3) Penyimpanan audit *log* perlu mempertimbangkan masa retensi yang telah ditentukan dan kebutuhan untuk pengumpulan bukti audit.

c. *Log* bagi administrator dan operator sistem

Aturan Kebijakan:

1) Seluruh aktivitas administrator dan operator sistem informasi harus direkam dalam *log* dan ditinjau secara berkala yang mencakup:

- Waktu dari kejadian (*event*) baik yang sukses maupun gagal.
- Hak akses dan identitas dari administrator atau operator.

d. Sinkronisasi waktu

Aturan Kebijakan:

1) Waktu (*clock*) pada sistem pengolahan informasi harus disinkronisasikan dengan sebuah standar waktu yang akurat dan disepakati.
2) *Administrator server* harus memastikan waktu pada setiap sistem kritikal (*server*) telah disinkronisasi dengan standar waktu yang sesuai dengan butir (1) diatas dan melakukan pemantauan dan koreksi apabila terdapat deviasi.

5. Keamanan Operasional

Proses ini bertujuan untuk memastikan keamanan *system file* pada aplikasi. Pengolahan data dalam lingkungan pengujian perlu diperhatikan agar tidak terjadi pengungkapan dari data yang sensitif.

a. Instalasi perangkat lunak pada sistem operasional

Aturan Kebijakan:

1) Dinas Kominfo dan Persandian harus mengendalikan instalasi *software* pada sistem operasional (*production*) di Dinas Kominfo dan Persandian.
2) Pengendalian terhadap sistem operasional meliputi:
   - Sistem *production* hanya mengoperasikan *system* yang telah disetujui oleh Kepala Dinas Kominfo dan Persandian.
   - Konfigurasi sistem operasional harus didokumentasikan dan di-*update* setiap kali mengalami perubahan.

6. Pengelolaan technical vulnerability

Manajemen *technical vulnerabilities* harus diimplementasikan secara efektif, sistematik, dan secara rutin dengan disertai pengukuran efektivitasnya.

a. Pengendalian terhadap kelemahan teknis (*technical vulnerability*)

Aturan Kebijakan:

1) *Administrator* sistem informasi perlu mencari informasi terkini tentang *technical vulnerability* pada sistem informasi DKIP.
2) Informasi terkini tentang *technical vulnerability* dapat diperoleh dari proses *vulnerability assessment* atau dari forum terkait keamanan informasi.
3) Informasi mengenai *technical vulnerability* harus segera ditindaklanjuti untuk menghilangkan atau mengurangi dampaknya.

b. Pembatasan instalasi perangkat lunak

Aturan Kebijakan:

1) Instalasi atau modifikasi perangkat lunak harus dikendalikan untuk mengurangi risiko *downtime* pada sistem informasi.

7. Pertimbangan dalam audit sistem informasi

Proses ini bertujuan untuk memaksimalkan efektivitas dari proses audit dan meminimalkan adanya campur tangan pada proses audit.

a. Pengendalian terhadap audit sistem informasi

Aturan Kebijakan:

1) Auditor *system* informasi perlu merencanakan proses audit yang melibatkan pemeriksaan sistem operasional yang meliputi:
   - Ruang lingkup dari pemeriksaan audit harus disepakati dengan pihak manajemen terkait.

- Akses audit ke sistem informasi maupun informasi hanya dibatasi dengan hak akses *read only*.
- Pemantauan dan pencatatan seluruh akses ke sistem informasi untuk menghasilkan *reference trail*.
- Pelaksana audit harus memiliki independensi dari aktivitas yang diaudit.

M. KEAMANAN KOMUNIKASI

1. Manajemen Keamanan Jaringan

   Keamanan jaringan perlu dikelola dengan baik untuk menjamin perlindungan terhadap informasi yang dikirimkan melalui jaringan dan infrastruktur pendukung jaringan lainnya. Pengelolaan keamanan jaringan perlu mempertimbangkan perlindungan informasi sensitif melalui jaringan publik.

   a. Pengendalian jaringan

      Aturan Kebijakan:

      1) Akses ke perangkat jaringan dan sistem pendukungnya hanya dapat dilakukan oleh administrator jaringan atau pihak lainnya yang telah mendapat izin dari administrator jaringan.
      2) Jaringan dan perangkat jaringan DKIP perlu dipantau secara kontinu.
      3) Akses ke jaringan DKIP hanya diberikan kepada perangkat milik DKIP.
      4) Konfigurasi jaringan DKIP perlu dirancang sedemikian rupa sehingga kegagalan pada satu jalur komunikasi tidak akan membuat terhentinya layanan jaringan komunikasi DKIP.
      5) Akses dari jaringan eksternal DKIP ke jaringan internal DKIP harus melalui proses otentikasi.
      6) Akses dari jaringan eksternal DKIP ke jaringan internal DKIP perlu mempertimbangkan teknologi kriptografi pada jaringan, seperti teknologi VPN.

   b. Keamanan Layanan Jaringan

      Aturan Kebijakan:

      1) Layanan jaringan mencakup layanan sistem informasi yang menggunakan jaringan komunikasi DKIP. Hal ini mencakup namun tidak terbatas pada, email, internet, aplikasi berbasis *web.*
      2) Setiap akses ke layanan jaringan DKIP harus melalui proses otentikasi.
      3) Penggunaan layanan jaringan perlu dipantau secara kontinu.
      4) Setiap layanan jaringan perlu dilengkapi dengan fitur keamanan untuk menjaga aspek kerahasiaan dan integritas informasi.

   c. Pemisahan (segregation) dalam jaringan

      Aturan Kebijakan:

      1) Jaringan internal dan eksternal DKIP harus dipisahkan menggunakan *security gateway*. Hal ini mencakup namun tidak terbatas pada penggunaan *firewall, filtering router,* atau *server.*
      2) Jaringan internal DKIP perlu dipisahkan berdasarkan tingkat kritikalitas perangkat yang terdapat didalam jaringan tersebut dan/atau unit organisasi.
      3) *Server-server* yang digunakan oleh DKIP harus terdapat pada segmentasi jaringan tersendiri yang terpisah dari segmentasi jaringan pengguna.

4) *Server-server* yang digunakan untuk kegiatan operasional (*production*) harus dipisahkan dari *server-server* untuk kegiatan pengembangan dan/atau pengujian.
5) Pemisahan atau segmentasi dapat dilakukan secara fisik maupun *logical* berdasarkan risiko yang ada.

2. Pertukaran Informasi

Proses pertukaran informasi perlu diamankan untuk melindungi pertukaran informasi antara Dinas Kominfo dan Persandian dengan pihak eksternal dari ancaman.

a. Kebijakan dan Prosedur Pertukaran Informasi

Aturan Kebijakan:

1) Pertukaran Informasi dengan menggunakan fasilitas *e-mail* harus memperhatikan perlindungan terhadap informasi yang dipertukarkan (dalam bentuk *attachment*) dari salah pengiriman dan perusakan. Jika dimungkinkan menggunakan *password* untuk melindungi kerahasiaan, integritas dan keaslian Informasi yang dipertukarkan.

b. Perjanjian Pertukaran

Aturan Kebijakan:

1) Dinas Kominfo dan Persandian harus memastikan adanya perjanjian formal dalam melakukan pertukaran informasi dengan pihak lain untuk memastikan semua pihak yang terlibat melakukan pengamanan informasi dengan memuat hal-hal sebagai berikut:
   - Kesepakatan dalam kesepahaman yang sama terkait keamanan informasi sehingga informasi dapat dilindungi secara memadai.
   - Penyimpanan Informasi secara aman dan memadai.
   - Penggunaan sistem pelabelan yang telah disepakati untuk informasi yang sensitif.
   - Penggunaan teknologi password yang diperlukan.

c. Pesan Elektronik (*e-mail*)

Aturan Kebijakan:

1) Pengiriman informasi milik DKIP menggunakan *e-mail* harus dilindungi untuk menghindari kebocoran informasi secara tidak disengaja akibat kesalahan pengiriman dan tanpa ada pengamanan pada *file*.

d. Perjanjian Kerahasiaan

Aturan Kebijakan:

1) Setiap pegawai Dinas Kominfo dan Persandian maupun pihak ketiga yang bekerja di Dinas Kominfo dan Persandian harus menyetujui dan menandatangani pernyataan menjaga kerahasiaan informasi yang dituangkan dalam dokumen pernyataan kerahasiaan informasi atau kontrak kerja dan berlaku selama personil aktif di Dinas Kominfo dan Persandian.

N. AKUISISI DAN PEMELIHARAAN SISTEM

1. *Requirement* keamanan sistem informasi

Semua persyaratan keamanan pada sistem informasi harus diidentifikasi pada tahap analisa kebutuhan proyek untuk kemudian dipertimbangkan, disetujui, dan didokumentasikan sebagai bagian dari kebutuhan bisnis Dinas Kominfo dan Persandian.

a. Analisa dan penentuan spesifikasi dari kebutuhan keamanan dalam sistem informasi

Aturan Kebijakan:

1) Setiap perubahan terhadap sistem informasi DKIP, baik pengembangan baru maupun perbaikan terhadap sistem yang sudah ada, harus mempertimbangkan kebutuhan pengendalian keamanan informasi.
2) Untuk sistem yang disediakan melalui *vendor* penyedia, Dinas Kominfo dan Persandian perlu melakukan proses pengujian untuk menjamin terpenuhinya seluruh kebutuhan keamanan dalam sistem informasi.

b. Pengujian Penerimaan Sistem

Aturan Kebijakan:

1) Pengujian penerimaan sistem harus ditetapkan sesuai dengan kriteria sistem informasi baru, *upgrade* dan versi baru. Pengujian penerimaan sistem harus mencakup pengujian kebutuhan keamanan informasi dan kepatuhan untuk mengamankan pengembangan sistem.
2) Pengujian juga harus dilakukan pada komponen yang diterima dan sistem terpadu.

c. Pengamanan Lingkungan Pengembangan

1) Lingkungan Pengembangan harus diamankan untuk memastikan akses ke lingkungan tersebut hanya diberikan kepada pihak pengembang yang berwenang.
2) Jalur komunikasi ke lingkungan pengembangan hanya diberikan kepada pihak pengembang yang berwenang.
3) Pengamanan infrastruktur pengembangan yang mencakup namun tidak terbatas pada *server* dan jalur serta perangkat jaringan sedapat mungkin sama dengan pengamanan pada lingkungan *production.*

d. Pengujian Keamanan Sistem

1) Pengujian keamanan harus dilakukan pada sistem informasi yang baru dikembangkan sebelum sistem informasi tersebut dioperasionalkan.
2) Pengujian keamanan harus mencakup fitur keamanan pada infrastruktur dan/atau aplikasi yang baru dikembangkan.

O. HUBUNGAN DENGAN SUPPLIER

1. Pengamanan pada Proses Pengembangan dan Support

Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh *supplier*.

a. Kebijakan keamanan informasi untuk hubungan dengan *supplier*

Aturan Kebijakan:

1) Proses keamanan informasi dengan *supplier* harus disepakati dengan *supplier* terkait dengan akses pemasok untuk aset organisasi.

b. Menangani keamanan informasi dalam perjanjian dengan *supplier*

Aturan Kebijakan:

1) Perjanjian dengan *supplier* harus mencakup klausul kerahasiaan informasi yang disetujui oleh setiap *supplier*.
2) Setiap personil *supplier* yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau mengkonfigurasi komponen infrastruktur TI, dan informasi untuk organisasi harus menandatangani perjanjian kerahasiaan informasi.

c. *Supply Chain* dari teknologi informasi dan komunikasi

Aturan Kebijakan:

1) *Supply Chain* dari teknologi informasi dan komunikasi harus mencakup kebutuhan untuk mengatasi resiko terkait dengan keamanan informasi dan layanan teknologi dan produk *supply chain*.

2. Pengelolaan Pemberian Layanan (Service Delivery)

Pengelolaan pemberian layanan bertujuan untuk menjaga tingkat keamanan informasi dan tingkat layanan yang disetujui sesuai dengan perjanjian.

a. Pemantauan dan Peninjauan Layanan dari *Supplier*

Aturan Kebijakan:

1) Pemantauan terhadap layanan yang disediakan oleh Pihak Ketiga meliputi antara lain:
   - Memantau tingkat layanan yang diberikan sesuai dengan perjanjian kerja.
   - Mengkaji laporan yang disampaikan oleh Pihak Ketiga dengan melakukan pertemuan berkala yang dituangkan dalam risalah rapat atau laporan *progress* pelaksanaan pekerjaan pihak ketiga.

b. Mengelola perubahan kepada layanan dari *Supplier*

Aturan Kebijakan:

1) Seluruh perubahan terhadap layanan yang diberikan oleh pihak ketiga, termasuk operasional dan pemeliharaan harus dikelola dengan mempertimbangkan sistem yang dijalankan oleh Dinas Kominfo dan Persandian.

P. MANAJEMEN INSIDEN KEAMANAN INFORMASI

1. Manajemen insiden keamanan informasi dan perbaikan terhadap sistem

Proses ini bertujuan untuk memastikan bahwa manajemen insiden keamanan informasi telah dijalankan secara konsisten dan efektif yang mencakup pengalokasian tugas dan tanggung jawab terkait dengan penanganan insiden dan kelemahan keamanan informasi.

a. Tanggung jawab dan prosedur penanganan insiden keamanan informasi

Aturan Kebijakan:

1) Manajemen Dinas Kominfo dan Persandian mempunyai tanggung jawab untuk memastikan penanganan insiden informasi yang ditangani oleh pegawai Dinas Kominfo dan Persandian yang mempunyai kewenangan dalam mengkoordinasikan tindak lanjut insiden telah dijalankan dengan cepat dan efektif.

b. Pelaporan insiden dalam sistem keamanan informasi

Aturan Kebijakan:

1) Seluruh pegawai Dinas Kominfo dan Persandian harus melaporkan insiden keamanan informasi yang teridentifikasi secepat mungkin melalui mekanisme pelaporan insiden di Dinas Kominfo dan Persandian.

c. Proses pelaporan kelemahan dalam sistem keamanan informasi

Aturan Kebijakan:

1) Semua pegawai Dinas Kominfo dan Persandian yang menggunakan sistem wajib melaporkan kelemahan dalam sistem jaringan secepat mungkin untuk mencegah terjadinya insiden keamanan informasi.

d. Assessment dari dan Keputusan terhadap kejadian keamanan informasi
   Aturan Kebijakan:
   1) *Assessment* dari dan keputusan terhadap kejadian keamanan informasi harus diputuskan dan harus diklasifikasian sebagai insiden keamanan informasi.
   2) Klasifikasi prioritas insiden dapat membantu dampak dan tingkat insiden.
e. Response terhadap insiden keamanan informasi
   Aturan Kebijakan:
   1) Respon terhadap keamanan informasi harus ditanggapi sesuai dengan prosedur yang terdokumentasi.
   2) Insiden keamanan informasi harus ditanggapi oleh pihak yang terkait (manajemen, personil, pihak ketiga).
f. Proses pembelajaran dari insiden keamanan informasi
   Aturan Kebijakan:
   1) Setiap insiden keamanan informasi yang terjadi harus dievaluasi terkait dampak dan biaya dari insiden keamanan informasi dan digunakan sebagai bahan masukan untuk proses peninjauan dari kebijakan keamanan informasi.
g. Pengumpulan bukti (evidence)
   Aturan Kebijakan:
   1) Bukti dari tindak lanjut penanganan insiden harus dikumpulkan, disimpan, dan ditunjukkan terkait dengan proses audit dan atau *evidence trail* di kemudian hari.
   2) Bukti dalam bentuk kertas (*hardcopy*) perlu disimpan dengan catatan mengenai siapa yang melaporkan bukti tersebut, serta dimana dan kapan bukti itu ditemukan. Sedangkan bukti dalam bentuk *softcopy* perlu dijamin bahwa bukti tersebut dapat selalu diakses bila dibutuhkan dan bukti tersebut disimpan.

Q. KEAMANAN INFORMASI DALAM KELANGSUNGAN BISNIS

1. Keberlanjutan Keamanan Informasi

   Proses *business continuity management* harus diterapkan untuk meminimalkan dampak yang menghambat organisasi dan mencegah kehilangan aset informasi (disebabkan kejadian seperti bencana alam, kecelakaan, kerusakan peralatan, dan kesengajaan) pada *acceptable level* melalui kombinasi pengendalian pencegahan dan pemulihan (*recovery*).

   a. Penerapan proses *business continuity management*
      Aturan Kebijakan:
      1) Proses *business continuity management* harus dikembangkan dan dipelihara dengan mempertimbangkan kebutuhan keamanan informasi untuk keberlangsungan bisnis Dinas Kominfo dan Persandian dengan mempertimbangkan.
         - Pemahaman terhadap berbagai risiko yang dihadapi Dinas Kominfo dan Persandian terhadap insiden pada operasional atau keadaan darurat yang disebabkan oleh bencana alam yang mencakup prioritisasi dari proses bisnis kritikal.
         - Indentifikasi dari seluruh aset yang digunakan oleh proses bisnis kritikal.

- Pengembangan dan dokumentasi dari *business continuity plan* yang mencakup strategi *business continuity*.
- Pengalokasian tugas dan tanggung jawab proses *business continuity* dalam proses dan struktur Dinas Kominfo dan Persandian.

2) Manajemen Dinas Kominfo dan Persandian harus menetapkan tim penanggulangan dan pemulihan bencana dan menetapkan koordinasi pemulihan BCP dalam kerangka kerja *business continuity plan*.

b. Pengembangan dan implementasi *continuity plan* yang mencakup aspek keamanan informasi

Aturan Kebijakan:

1) Manajemen Dinas Kominfo dan Persandian harus menilai risiko yang berkaitan kritikalitas proses yang dijalankan terkait dengan *business continuity* sebagai kajian mengenai *Business Impact Analysis* (BIA) dengan mengidentifikasi dampak kegagalan maupun gangguan terhadap proses bisnis.

c. Pengujian *continuity plan* yang mencakup aspek keamanan informasi

Aturan Kebijakan:

1) Penanggung jawab *system* di Dinas Kominfo dan Persandian harus melakukan koordinasi terkait dengan perencanaan *business continuity* dalam rangka memelihara dan memastikan proses pemulihan operasi sistem informasi pada saat terjadi gangguan pada proses bisnis yang kritikal.
2) Proses perencanaan dan pengembangan *business continuity plan* meliputi:
   - Identifikasi dan kesepakatan untuk semua tanggung jawab pada tim BCP di Dinas Kominfo dan Persandian yang terlibat dalam pemulihan proses darurat.
   - Melengkapi prosedur operasional bisnis pada proses *recovery* dan *restoration.*
   - Rencana pelatihan untuk pegawai yang terlibat dalam proses-proses dalam *business continuity plan.*
   - Pengujian dari *business continuity plan.*
3) Manajemen Dinas Kominfo dan Persandian harus memastikan dokumen BCP yang disimpan dan selalu *up-to-date*.

2. Redundancies

Bertujuan untuk menjamin ketersedian dari fasilitas pemrosesan informasi.

a. Ketersediaan dari fasilitas pemrosesan informasi

Aturan Kebijakan:

1) Manajemen Dinas Kominfo dan Persandian harus memastikan infrastruktur sistem informasi DKIP mempunyai *redundancy* yang memadai untuk memenuhi kebutuhan ketersediaan sistem.
2) Kebutuhan ketersediaan sistem perlu dijabarkan secara formal berdasarkan kebutuhan penggunaan sistem informasi di DKIP.

R. KEPATUHAN (COMPLIENCE)

1. Kepatuhan Terhadap Prasyarat Hukum dan Kontraktual

   Proses ini bertujuan untuk mencegah terjadinya pelanggaran terhadap hukum, undang-undang, *contractual obligation,* dan kebutuhan keamanan lainnya.

   a. Identifikasi aturan hukum, regulasi maupun kontrak yang berlaku

      Aturan Kebijakan:

      1) Manajemen Dinas Kominfo dan Persandian harus mengidentifikasi semua persyaratan legal, regulasi, dan kontraktual secara terdokumentasikan untuk memastikan kesesuaiannya dengan peraturan / perundang-undangan yang berlaku secara nasional terhadap proses keamanan informasi yang diijalankan.

   b. Hak Atas Kekayaan Intelektual (HAKI)

      Aturan Kebijakan:

      1) Manajemen Dinas Kominfo dan Persandian harus memastikan penggunaan aset TI yang memiliki HAKI dan produk *software* berlisensi telah memenuhi kepatuhan terhadap peraturan, dan kebutuhan kontrak.
      2) Terkait dengan pengelolaan *software* di Dinas Kominfo dan Persandian, <unit> harus melaksanakan ketentuan sebagai berikut:
         - Perangkat lunak yang digunakan adalah perangkat lunak yang berlisensi.
         - Daftar Lisensi perangkat lunak ditatausahakan dengan baik, diperiksa status lisensi dan kesesuaiannya secara berkala.

   c. Perlindungan terhadap record Dinas Kominfo dan Persandian

      Aturan Kebijakan:

      1) *Record* perlu dikategorikan sesuai dengan tipenya seperti *record database*, *log* dari transaksi atau hasil audit yang perlu dilengkapi dengan keterangan mengenai masa simpan dan masa retensi.

2. Kepatuhan terhadap kebijakan, standar, dan technical complience

   Proses ini bertujuan untuk memastikan kepatuhan sistem terhadap kebijakan dan standar yang ditetapkan oleh Dinas Kominfo dan Persandian dengan melakukan peninjauan secara berkala.

   a. Kepatuhan terhadap kebijakan dan standard keamanan informasi

      Aturan Kebijakan:

      1) Manajemen Dinas Kominfo dan Persandian harus secara reguler melakukan tinjauan terhadap kepatuhan dari sistem informasi, termasuk penggunaan fasilitas pengolahan informasi, proses penanganan informasi dalam lingkup bagiannya sesuai dengan kebijakan, standar dan *requirement* keamanan informasi yang berlaku.

   b. Pemeriksaan technical compliance

      Aturan Kebijakan:

      1) Penanggung jawab *system* di Dinas Kominfo dan Persandian harus memeriksa sistem secara berkala untuk memastikan kesesuaian terhadap standar penerapan keamanan yang ditetapkan melalui pemeriksaan secara teknis dari sisi

perangkat lunak maupun perangkat keras sesuai dengan spesifikasi yang telah ditetapkan.

2) Apabila pemeriksaan *technical compliance* mencakup pelaksanaan *penetration test* atau *vulnerability assessment*, maka kegiatan *test* tersebut perlu direncanakan dan didokumentasikan dengan baik untuk mencegah risiko gangguan terhadap keamanan dari sistem informasi.

BAB IV
MANAJEMEN DATA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH DAERAH KABUPATEN SUKABUMI

A. Pendahuluan

Manajemen data dilaksanakan dengan tujuan untuk menjamin terwujudnya Data yang akurat, mutakhir, terintegrasi dan dapat diakses sebagai dasar perencanaan, pelaksanaan, Evaluasi dan pengendalian pembangunan nasional.

Sasaran dilaksanakannya manajemen data adalah agar Pemerintah Daerah:

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.

B. Ketentuan Umum

1. 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;
2. Data Statistik adalah Data berupa angka tentang karakteristik atau ciri khusus suatu populasi yang diperoleh dengan cara pengumpulan, pengolahan, penyajian, dan analisis;
3. Metadata adalah informasi dalam bentuk struktur dan format yang baku untuk menggambarkan Data, menjelaskan Data, serta memudahkan pencairan, penggunaan dan pengelolaan informasi Data;
4. Interoperabilitas Data adalah kemampuan data untuk dibagipakaikan antar sistem elektronik yang saling berinteraksi;
5. 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;
6. Kode Referensi adalah tanda berisi karakter yang mengandung atau menggambarkan makna, maksud atau norma tertentu sebagai rujukan identitas data yang bersifat unik;
7. Data Induk adalah Data yang mempresentasikan objek dalam proses bisnis pemerintah sesuai dengan Peraturan Bupati Sukabumi tentang Satu Data Indonesia Tingkat Kabupaten Sukabumi;
8. Satu Data Indonesia Tingkat Kabupaten Sukabumi adalah kebijakan tata kelola data pemerintah daerah untuk menghasilkan data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antar Perangkat Daerah, Badan Usaha Milik Daerah, Instansi Vertikal, Instansi Provinsi dan Instansi Pusat melalui pemenuhan Standar Data, Metadata, Interoperabilitas Data, dan menggunakan Kode Referensi dan Data Induk;
9. Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi adalah wadah komunikasi dan koordinasi Perangkat Daerah untuk penyelenggaraan Satu Data Indonesia Tingkat Kabupaten Sukabumi;
10. Produsen Data Tingkat Kabupaten Sukabumi adalah Perangkat Daerah dan Instansi Vertikal yang menghasilkan data berdasarkan

kewenangan sesuai dengan ketentuan peraturan perundang-undangan;

11. Pengguna Data adalah Instansi Pusat, Instansi Daerah, Perseorangan, Kelompok Orang, atau Badan Hukum yang menggunakan data;
12. 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;
13. Arsitektur Data adalah model yang mengatur dan menentukan jenis data yang dikumpulkan, disimpan, dikelola dan diintegrasikan dalam SPBE;
14. Manajemen Arsitektur Data adalah rangkaian proses untuk menetapkan dan menyebarluaskan komponen Arsitektur Data;
15. Manajemen Data Referensi adalah rangkaian proses perencanaan, pengumpulan, pemeriksaan dan penyebarluasan data referensi;
16. Manajemen Basis Data adalah proses pengelolaan kumpulan data yang disimpan di Satu Data Kabupaten Sukabumi;
17. Manajemen Kualitas Data adalah proses untuk memastikan data yang dihasilkan dan dikelola secara elektronik memenuhi prinsip Satu Data Indonesia;
18. Pembina Data adalah Instansi Pusat yang diberi kewenangan melakukan pembinaan terkait Data atau Instansi Daerah yang diberikan penugasan untuk melakukan pembinaan terkait data;
19. Pembina Data Statistik adalah instansi pusat yang melaksanakan tugas pemerintahan di bidang statistik di Provinsi atau Kabupaten/Kota;
20. Pembina data Geopasial adalah instansi Pemerintah Daerah Kabupaten Sukabumi yang diberikan penugasan sebagai pengelola simpul jaringan pemerintah daerah dalam jaringan informasi geospasial nasional;
21. Walidata adalah Perangkat Daerah Kota yang diberi kewenangan untuk melaksanakan urusan statistik yang bertugas melakukan kegiatan pengumpulan, pemeriksaan, dan pengelolaan data yang disampaikan oleh Produsen Data, serta menyebarluaskan data;
22. Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi adalah wadah komunikasi dan koordinasi untuk penyelenggaraan Satu Data Indonesia Tingkat Kabupaten Sukabumi;
23. Daftar Data adalah usulan data yang disampaikan oleh Walidata sebagai bahan penyusunan data prioritas dalam Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi;
24. Satu Data adalah suatu konsep tentang data yang tersedia secara bebas untuk diakses dan dimanfaatkan oleh masyarakat.

C. Ruang Lingkup

Manajemen data Pemerintah Daerah Kabupaten Sukabumi melalui serangkaian proses pengelolaan data yang terdiri dari:

1. Manajemen Arsitektur Data;
2. Manajemen Data Induk dan Referensi;
3. Manajemen Basis Data;
4. Manajemen Kualitas Data; dan
5. Manajemen Interoperabilitas Data.

D. Manajemen Arsitektur Data

Manajemen Arsitektur Data adalah rangkaian proses untuk menetapkan dan menyebarluaskan komponen Arsitektur Data. Manajemen Arsitektur data terdiri dari dua komponen utama yaitu :

1. Spesifikasi Data merupakan gambaran struktur Data fisik pada suatu sistem atau aplikasi yang umumnya berbentuk tabel, yang terdiri atas format dan struktur baku untuk Data Induk dan Data Referensi.
2. Ketentuan Data mencakup tata cara perencanaan, pengumpulan, pemeriksaan dan penyebarluasan spesifikasi Data.

Manajemen Arsitektur Data disusun untuk menyediakan data berkualitas tinggi, mengidentifikasi dan mendefinisikan kebutuhan Data; dan merancang struktur dan rencana untuk memenuhi kebutuhan Data saat ini dan kebutuhan Data jangka panjang.

Kegiatan Manajemen Arsitektur Data meliputi 3 (tiga) tahap yaitu:

1. Penyusunan dan Penetapan

   Pada tahap penyusunan dan penetapan Arsitektur Data SPBE ini Koordinator Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi bertanggung jawab mengoordinasikan pembahasan Arsitektur Data SPBE dalam Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi.

   Arsitektur Data SPBE disusun dengan mengacu pada Arsitektur SPBE Pemerintah Daerah serta memperhatikan:

   a. Rencana Induk SPBE Pemerintah Daerah;
   b. Rencana pembangunan jangka menengah Daerah;
   c. SIPD E-Database;
   d. Indikator tujuan pembangunan berkelanjutan;
   e. Indikator indeks daya saing Daerah;
   f. Kajian perencanaan pembangunan Daerah; dan
   g. Data dan informasi lainnya.
2. Penyebarluasan

   Penyebarluasan Arsitektur Data SPBE ini dilaksanakan melalui Satu Data Kabupaten Sukabumi. Pada tahap ini, Perangkat Daerah yang menyelenggarakan fungsi penunjang urusan pemerintahan di bidang perencanaan melalui Sekretariat Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi menyebarluaskan Arsitektur Data SPBE Kabupaten Sukabumi melalui Satu Data Kabupaten Sukabumi.
3. Reviu

   Reviu Arsitektur Data SPBE dilakukan sebagai bagian dari reviu terhadap Arsitektur SPBE Pemerintah Daerah. Koordinator Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi mengoordinasikan reviu terhadap Arsitektur Data SPBE dalam Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi. Reviu ini dilaksanakan pada paruh waktu pelaksanaan Arsitektur SPBE Pemerintah Daerah atau sewaktu-waktu sesuai dengan kebutuhan.

E. Manajemen Data Induk Dan Data Referansi

Manajemen Data Induk dan Data Referensi dilaksanakan untuk menyediakan Data yang sesuai struktur dan format baku yang ditentukan, dapat dijadikan acuan untuk menghasilkan Data yang akurat, mutakhir dan dapat dibagi pakaikan, dan menghindari duplikasi.

Kegiatan Manajemen Data Induk dan Data Referensi meliputi :

1. Perencanaan

   Perencanaan Data Induk dan Data Referensi dilaksanakan oleh Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi berdasarkan Daftar Data dan usulan Pembina Data.
2. Pengumpulan;

   Pengumpulan Data Induk dan Data Referensi dilakukan oleh Wali Data dalam Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi

3. Pemeriksaan;
   Pemeriksaan Data Induk dan Data Referensi dilakukan oleh Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi untuk memastikan kesesuaian dengan struktur dan format baku, kesesuaian dengan Daftar Data tahun berikutnya, dan tidak terjadi duplikasi. Data Induk dan Data Referensi disepakati dalam Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi. Kemudian disampaikan oleh Koordinator Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi kepada Bupati Sukabumi untuk ditetapkan.
4. Penyebarluasan;
   Penyebarluasan Data Induk dan Data Referensi dilakukan oleh Wali Data melalui Satu Data Kabupaten Sukabumi.
5. Pembaruan
   Pembaruan Data Induk dan Data Referensi diperbarui sesuai kebutuhan oleh Koordinator Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi melalui Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi.

Manajemen Data Induk dan Data Referensi dilaksanakan selaras dengan perumusan dan penyepakatan Kode Referensi yang telah diatur dalam Peraturan Bupati tentang Satu Data Indonesia Tingkat Kabupaten Sukabumi. Koordinator Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi merumuskan kebijakan teknis dalam rangka penyelarasan Manajemen Data Induk dan Data Referensi dengan Kode Referensi.

F. Manajemen Basis Data

Manajemen Basis Data adalah proses pengelolaan kumpulan Data yang disimpan di Satu Data Kabupaten Sukabumi. Manajemen Basis Data dilaksanakan untuk menyediakan basis Data yang menjamin penyimpanan Data yang akurat, mutakhir dan dapat dibagipakaikan pada Satu Data Kabupaten Sukabumi, menjamin ketersedian akses Data yang terus menerus, dan menjaga keamanan Data dari akses yang tidak sesuai ketentuan tata kelola Data atau peraturan perundangan terkait pengelolaan Data.

Kegiatan Manajemen Basis Data mencakup:

1. mendefinisikan kebutuhan Wali Data dan Produsen Data untuk Basis Data;
2. mengelola Basis Data di Satu Data Kabupaten Sukabumi, ketentuan penyimpanan Data ini diatur oleh Kepala Perangkat Daerah Kota yang menyelenggarakan urusan di bidang komunikasi dan informatika.
3. melakukan pemeriksaan Basis Data untuk kesesuaian dengan prinsip Satu Data Indonesia;
4. menyebarluaskan Basis Data melalui Satu Data Kabupaten Sukabumi;
5. membuat cadangan dan distribusi Basis Data; dan
6. merencanakan dan mengelola perbaruan Basis Data.

G. Manajemen Kualitas Data

Manajemen Kualitas Data adalah proses untuk memastikan Data yang dihasilkan dan dikelola secara elektronik memenuhi prinsip Satu Data Indonesia. Manajemen Kualitas Data dilaksanakan untuk menjamin Data yang dihasilkan Produsen Data yang memenuhi prinsip Satu Data Indonesia, dan diperbarui sesuai dengan jadwal pemutakhiran Data.

Kegiatan Manajemen Kualitas Data melingkupi kegiatan untuk:

1. mengembangkan dan mempromosikan kesadaran kualitas data;
2. menentukan persyaratan kualitas data;
3. menetapkan profil, analisis, dan nilai kualitas data;
4. menentukan matriks kualitas data;

5. menentukan aturan bisnis kualitas data;
6. menguji dan memvalidasi persyaratan kualitas data;
7. menetapkan dan mengevaluasi tingkat layanan kualitas data; dan
8. mengukur dan memantau kualitas data secara berkelanjutan.

Kegiatan Manajemen Kegiatan Manajemen Kualitas Data dilaksanakan melalui tahapan:

1. Perencanaan
   Perencanaan Kualitas Data dilaksanakan oleh Forum Satu Data Indonesia Tingkat Kabupaten Sukabumi dengan menyepakati Daftar Data, Data Prioritas dan jadwal pemutakhiran data.
2. Pemeriksaan
   Pemeriksaan Kualitas Data dilaksanakan dengan memeriksa kesesuaian data dengan prinsip Satu Data Indonesia, dan ketepatan jadwal pemutakhiran data. Pemeriksaan dilaksanakan oleh :
   a. Wali Data, termasuk wali Data pendukung, untuk Data yang termasuk dalam Daftar Data; dan
   b. Wali Data dan Pembina Data, untuk Data yang masuk dalam Data prioritas.
3. Penilaian
   Penilaian kualitas Data dilaksanakan oleh tim koordinasi SPBE di Kabupaten Sukabumi untuk menilai kinerja Produsen Data dan Wali Data dalam pengelolaan Data, sebagai bagian dari pemantauan dan Evaluasi terhadap SPBE.

H. Manajemen Interopabilitas Data

a. Manajemen Interopabilitas dilaksanakan untuk memenuhi kaidah Interoperabilitas Data dimana data harus:
   1. konsisten dalam sintak/bentuk, struktur/skema/ komposisi penyajian, dan semantik/ artikulasi keterbacaan; dan
   2. disimpan dalam format terbuka yang dapat dibaca Sistem Elektronik.

b. Interoperabilitas Data diselenggarakan dengan prinsip:
   1. aman dan andal;
   2. dapat digunakan kembali;
   3. dapat dibaca;
   4. dapat dikembangkan lebih lanjut secara mandiri;
   5. dapat diperiksa;
   6. dapat diukur kinerjanya;
   7. dapat diawasi dan dinilai tingkat pemanfaatannya; dan
   8. dapat dibagipakaikan antar Sistem Elektronik yang berbeda Karakteristik.

BAB V
MANAJEMEN ASET TEKNOLOGI INFORMASI DAN KOMUNIKASI KABUPATEN SUKABUMI

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 Kabupaten Sukabumi.
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 Kabupaten Sukabumi:

a. Sinkronisasi dan integrasi Rencana TIK Pemerintah Kabupaten Sukabumi;
b. Efisiensi belanja TIK Pemerintah Kabupaten Sukabumi;
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 Kabupaten Sukabumi
   2. Mendapatkan standar rujukan kualitas penyelenggaraan TIK di seluruh institusi pemerintahan
   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 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 akuisisi 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 manajemen 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 reviu 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 reviu 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:
         (1). Keselarasan tujuan organisasi dengan tujuan TIK, dimana setiap tujuan TIK harus mempunyai referensi tujuan organisasi.
         (2). Keselarasan arsitektur bisnis organisasi dengan arsitektur TIK (arsitektur informasi, arsitektur aplikasi, dan arsitektur infrastruktur).

(3). Keselarasan eksekusi inisiatif TIK dengan rencana strategis.

2) Manajemen Risiko
   a) Risiko-risiko prioritas dalam pengelolaan TIK oleh Pemerintah daerah Kabupaten mencakup:
      (1). 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.
      (2). 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.
      (3). 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:
      (1). Implementasi *Project Governance* untuk setiap proyek TIK yang diimplementasikan oleh seluruh Perangkat daerah Kabupaten.
      (2). 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:
      (1). Pemilihan sumber-sumber dana yang tidak memberatkan untuk pengadaan TIK.
      (2). Kelayakan belanja TIK secara finansial harus bisa diukur secara rasional dengan menggunakan metoda-metoda penganggaran modal (capital budgeting).
      (3). Dijalaninya prosedur pengadaan yang efisien dengan fokus tetap pada kualitas produk dan jasa TIK.
      (4). Prioritas anggaran diberikan untuk proyek TIK yang bermanfaat untuk banyak pihak, berbiaya rendah, dan cepat dirasakan manfaatnya.
      (5). Perhitungan manfaat dan biaya harus memasukkan unsur yang bersifat kasat mata (tangible) dan terukur maupun yang tidak tampak (intangible) dan relatif tidak mudah diukur.
      (6). 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.
      (7). 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:
   (1). Penyusunan arsitektur informasi yang mencerminkan kebutuhan informasi, struktur informasi dan pemetaan hak akses atas informasi oleh peran-peran yang ada dalam manajemen organisasi.
   (2). 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 antar institusi pemerintahan) yang meliputi:
   (1). Aplikasi, yaitu *software* aplikasi yang secara arsitektur teknis dapat di-*share* penggunaannya karena kesamaan kebutuhan fitur fungsionalitas.
   (2). Perbedaan hanya sebatas di aspek konten informasi Infrastruktur komunikasi.
   (3). 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:
   - Intensitas peninjauan indikator keberhasilan, paling sedikit 1 (satu) kali untuk setiap tahunnya.
   - Setiap siklus peninjauan indikator keberhasilan harus didokumentasikan dan tindak lanjut atas rekomendasi dimonitor secara reguler oleh manajemen.

- 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.
   - Inisiatif Evaluasi eksternal berasal dari pihak di Pemerintah Daerah Kabupaten.
   - Tujuan utama Evaluasi secara eksternal adalah mengetahui ketercapaian tujuan manajemen Aset TIK, dengan sudut pandang indikator keberhasilan yang relatif seragam.
   - 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.

c. Proses Perencanaan Sistem

1) 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.

2) Lingkup

   a) Sinkronisasi dan Integrasi.
      - Sinkronisasi dan integrasi perencanaan sistem dilakukan sejak di level Pemerintah daerah Kabupaten maupun hubungan dengan instansi pemerintah lain.
      - Tim Koordinasi SPBE memberikan persetujuan akhir atas Rencana Induk TIK lima tahunan Pemerintah daerah Kabupaten, yang kemudian akan disahkan oleh Bupati.
      - Dalam penyusunan Rencana Induk TIK lima tahunan Pemerintah daerah Kabupaten dapat meminta masukan kepada Dewan TIK Nasional.

   b) Siklus dan Lingkup Perencanaan.
      - 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.
      - 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.

o Tim Koordinasi SPBE dapat melakukan reviu kekinian dan kesesuaian Rencana Induk TIK Pemerintah Daerah Kabupaten secara reguler.

c) Perencanaan Arsitektur Informasi
   o 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.
   o Arsitektur informasi mencakup informasi terstruktur (data *mart*, *database*, *database* TABEL, pertukaran data) dan informasi tidak terstruktur (gambar, video, file dokumen, dsb).
   o Penetapan arsitektur informasi mencakup penetapan klasifikasi ke dalam kelas-kelas data, pemetaan kepemilikan data, dan pendefinisian data dictionary, dan syntax rules.
   o Arsitektur informasi juga menetapkan klasifikasi level keamanan data untuk setiap klasifikasi kelas data melalui penetapan kriteria yang tepat sesuai dengan kebutuhan organisasi.

d) Perencanaan Arsitektur Aplikasi
   o 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.
   o 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.

o 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 Kabupaten Sukabumi.

e) Perencanaan Arsitektur Infrastruktur Teknologi
   o Infrastruktur teknologi mencakup jaringan komunikasi, perangkat pemrosesan informasi (*server*, *workstation* dan *peripheral* pendukungnya), *software system* (sistem operasi, *database* RDBMS), dan media penyimpanan data.
   o 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.
   o Infrastruktur komunikasi: jaringan komputer/komunikasi, koneksi internet. Infrastruktur penyimpanan data (Data Center) dan/atau DRC (Disaster Recovery *Center).*
f) Perencanaan Manajemen dan Organisasi
   o Perencanaan organisasi mencakup identifikasi struktur organisasi pengelola yang akan melakukan operasional harian.
   o Perencanaan manajemen mencakup pendefinisian prosedur teknis dengan prioritas pada domain:
     - *Realisasi* Sistem
     - *Operasi Sistem*
     - *Pemeliharaan Sistem*
g) Perencanaan Pendekatan dan *Roadmap* Implementasi
   o 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.
   o Setiap inisiatif yang direncanakan selalu menyertakan proyeksi waktu, kapan benefit yang diharapkan dapat terealisasi (benefit realization schedule).

- Setiap perencanaan sistem mempunyai roadmap implementasi yang didasarkan pada analisa kesenjangan arsitektur (informasi, aplikasi dan infrastruktur teknologi) serta kesenjangan manajemen dan organisasi.
- 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.
- Penetapan peringkat prioritas portofolio proyek inisiatif TIK dilakukan setidaknya berdasarkan faktor level anggaran yang dibutuhkan, kompleksitas sistem, dan besar usaha yang diperlukan.

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

3) Mekanisme perencanaan
a) Perangkat Daerah Kabupaten mengusulkan kebutuhan aset TIK dalam Rencana Kebutuhan Barang Milik Daerah (pengadaan dan pemeliharaan).
b) Dalam menyusun kebutuhan aset TIK sebagaimana dimaksud pada huruf b memperhatikan standar barang dan standar kebutuhan serta dikonsultasikan kepada unit kerja Urusan Bidang Komunikasi dan Informatika.
c) 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 perundangan di bidang pengelolaan barang milik daerah.

d. Manajemen Belanja
1) 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

2) Lingkup
   a) 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.
   b) Sinkronisasi dan Integrasi
      - Pengelolaan belanja/investasi TIK dilakukan melalui mekanisme penyusunan Rencana Kegiatan dan Anggaran SKPD sesuai ketentuan peraturan perundang-undangan.
      - Tim Kooordinasi SPBE melakukan reviu dan persetujuan atas Rencana Kegiatan dan Anggaran TIK yang diajukan oleh Satuan Kerja Pengelola TIK atau Satuan Kerja Pemilik Proses Bisnis. reviu dan persetujuan ini ditujukan untuk memastikan tidak adanya redundansi proyek TIK di tiap Perangkat Daerah Kabupaten.
3) Pemilihan Mekanisme Penganggaran
   a) Tipe Mekanisme Penganggaran
      - 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.
      - 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.
   b) Kriteria Pemilihan Mekanisme Penganggaran
      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 faktor 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, CostBenefit 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.

4) Indikator Keberhasilan
   a) Digunakannya sumber-sumber pendanaan yang efisien.
   b) Kesesuaian realisasi penyerapan anggaran TIK dengan realisasi pekerjaan yang direncanakan.
   c) Diperolehnya sumber daya TIK yang berkualitas dengan melalui proses belanja/investasi TIK yang efisien, cepat, bersih dan transparan.

e. Proses Realisasi Sistem
   1) Definisi
      Realisasi sistem TIK merupakan proses yang ditujukan untuk mengimplementasikan perencanaan TIK, mulai dari pemilihan sistem TIK sampai dengan evaluasi pasca implementasi.
   2) Lingkup
      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:
- 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).
- Setiap software aplikasi yang direalisasikan harus disertai dengan training dan/atau transfer pengetahuan kepada pengguna dan administrator sistem.
- 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
- Teknologi infrastruktur mencakup perangkat keras pemrosesan informasi (server, workstation, dan peripheral), jaringan komunikasi dan software infrastruktur (sistem operasi, tool sistem).
- Pertimbangan kapasitas infrastruktur teknologi disesuaikan dengan kebutuhan, sehingga setiap realisasi infrastruktur teknologi selalu disertai sebelumnya dengan analisis kebutuhan kapasitas.
- 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.

3) 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) 6) Jumlah software aplikasi yang didukung dokumentasi memadai dari yang seharusnya.
   g) 7) Jumlah implementasi software aplikasi yang terlaksana tepat waktu.
   h) 8) Penurunan jumlah downtime infrastruktur.

f. Proses Pengadaan Aset TIK

Proses pengadaan Aset TIK dilaksanakan berdasarkan ketentuan peraturan perundang-undangan bidang pengadaan barang/jasa pemerintah.

g. Proses Pengoperasian Sistem

1) 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.

2) Lingkup
   a) Manajemen Tingkat Layanan
      - Manajemen TIK bertanggung jawab atas penyusunan dan *update* katalog layanan TIK, yang berisi sistem yang beroperasi dan layanan-layanan TIK yang menyusunnya.
      - Diprioritaskan bagi layanan-layanan TIK kritikal yang menyusun sebuah operasi sistem TIK harus memenuhi (SLA) yang ditetapkan sebagai sebuah requirement (persyaratan) oleh pemilik proses bisnis dan disetujui oleh manajemen Aset TIK.
      - Aspek minimal yang harus tercakup dalam setiap 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 direviu.

b) Keamanan dan Keberlangsungan Sistem
- Setiap operasi sistem TIK harus memperhatikan persyaratan minimal aspek keamanan sistem dan keberlangsungan sistem, terutama sistem TIK yang memfasilitasi layanan-layanan kritikal
- 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:
    (1). Untuk pengamanan dari sisi infrastruktur teknologi dapat diimplementasikan komponen standar.
    (2). 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.

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

d) 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).

e) Manajemen Data
(1). Data dari setiap software aplikasi secara kumulatif juga di *backup* secara terpusat dalam media penyimpanan data (*data storage*), terutama *software-software* aplikasi kritikal.
(2). Backup data dilakukan secara reguler, dengan frekuensi dan jenis backup disesuaikan dengan tingkat kritikal sistem.

(3). Dilakukan pengujian secara teratur mekanisme backup dan restore data, untuk memastikan integritas dan validitas prosedur.
(4). Implementasi mekanisme inventori atas media-media penyimpanan data, terutama media-media yang *off-line*.

f) Manajemen Layanan oleh Pihak Ketiga
(1). 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.

(2). Seluruh layanan TIK yang diselenggarakan oleh pihak ketiga harus mematuhi ketentuan-ketentuan operasi sistem yang telah dijelaskan sebelumnya.
(3). Secara reguler pihak ketiga penyelenggara layanan TIK harus memberikan laporan atas tingkat kepatuhan terhadap ketentuan- ketentuan operasi sistem di atas.
(4). 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.

3) Indikator Keberhasilan
a) Terkait dengan manajemen tingkat layananProsentase operasi sistem kritikal yang layanan-layanan TIK-nya disertai dengan SLA.
b) Terkait dengan keamanan dan keberlangsungan sistem Prosentase layanan TIK yang memenuhi SLA
c) Terkait dengan manajemen *software* aplikasi
(1). Tingkat kepatuhan sistem terhadap kriteria minimum yang telah ditetapkan
(2). Penurunan jumlah insiden yang terjadi terkait dengan permasalahan keamanan dan keberlangsungan sistem
(3). Penurunan jumlah insiden yang menyebabkan *downtime.*
(4). Penurunan jumlah waktu *downtime* total per durasi waktu.
d) Terkait dengan manajemen infrastruktur
(1). Tingkat kepatuhan pengguna terhadap prosedur-prosedur yang telah ditetapkan
(2). Penurunan jumlah kegagalan pengoperasian *software* aplikasi
e) Terkait dengan manajemen data
(1). Penurunan jumlah kegagalan *restore* data kritikal.
(2). Penurunan jumlah insiden terkait dengan permasalahan integritas data.

f) Terkait dengan manajemen layanan oleh pihak ketiga
   (1). Jumlah atau prosentase operasi sistem TIK yang memenuhi SLA.
   (2). Jumlah atau prosentase operasi sistem TIK yang memenuhi ketentuan minimum keamanan dan keberlangsungan sistem.
   (3). Jumlah atau prosentase operasi sistem TIK yang memenuhi ketentuan minimum manajemen data.
   (4). Penurunan jumlah insiden yang menyebabkan downtime.
   (5). Penurunan jumlah waktu downtime total per durasi waktu.
   (6). Penurunan jumlah kegagalan restore data kritikal.
   (7). Penurunan jumlah insiden terkait dengan permasalahan integritas data.

h. Pemeliharaan Sistem
   1) 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.
   2) Lingkup
      a) Pemeliharaan Software Aplikasi
         - Pemeliharaan software aplikasi
         - Manajemen Aset TIK menerapkan mekanisme patching software aplikasi atas software aplikasi yang dikembangkan secara mandiri atau kerjasama dengan pihak ketiga.
         - 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*.
      b) Pemeliharaan Infrastruktur Teknologi
         - 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*
         - 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.

c) Pemeliharaan Data
   - Keaslian, keutuhan, dan ketersediaan data harus menjadi perhatian. Semua pihak dalam institusi harus menaati prosedur pemeliharaan data yang telah ditetapkan
   - Data Center/Disaster Recovery Center (DC/DRC) dikelola sesuai dengan prosedur baku yang ada.
   - Data harus dilindungi dari pihak-pihak yang tidak memiliki hak akses serta pengubahan dan kesalahan alamat pengiriman data sensitif yang bernilai strategis.

d) Siklus Hidup dan Likuidasi Sumber Daya Infrastruktur Teknologi
   - 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.
   - Likuidasi sumber daya infrastruktur teknologi dapat dilakukan untuk teknologi lain yang lebih handal dan terjangkau pengadaannya.

e) Indikator Keberhasilan
   - Penurunan jumlah permasalahan yang terjadi di software aplikasi karena tidak optimalnya keberjalanan mekanisme patching.
   - Penurunan jumlah permasalahan yang terjadi di infrastruktur teknologi karena tidak optimalnya keberjalanan mekanisme patching.
   - Penurunan jumlah permasalahan yang terjadi karena aspek kapasitas infrastruktur teknologi.
   - 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.

i. Penghapusan Aset TIK

Penghapusan Aset TIK dilaksanakan berdasarkan ketentuan peraturan perundang-undangan di bidang pengelolaan barang milik daerah dan standar akuntansi pemerintahan.

BAB VI
MANAJEMEN SUMBER DAYA MANUSIA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAERAH KABUPATEN SUKABUMI

Manajemen sumber daya manusia bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE. Manajemen sumber daya manusia dilakukan melalui serangkaian proses perencanaan, pengembangan, pembinaan, dan pendayagunaan sumber daya manusia dalam SPBE.

Manajemen sumber daya manusia dilaksanakan unutk memastikan ketersediaan dan kompetensi sumber daya manusia untuk pelaksanaan Tata Kelola SPBE dan Manajemen SPBE.

Kompetensi Sumber Daya Manusia SPBE, meliputi:

1. Kompetensi di Bidang Proses Bisnis Pemerintahan;
2. Arsitektur SPBE;
3. Data dan Informasi;
4. Keamanan SPBE;
5. Aplikasi SPBE; dan
6. Infrastruktur SPBE

BAB VII
PEDOMAN MANAJEMEN PENGETAHUAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK KABUPATEN SUKABUMI

A. PENDAHULUAN

1. Latar belakang

Reformasi birokrasi pemerintah daerah antara lain bertujuan untuk memfasilitasi terwujudnya organisasi yang efektif dan efisien. Untuk mewujudkan organisasi tersebut, kementerian dan lembaga perlu secara aktif memanfaatkan kekayaan pengetahuannya sendiri, termasuk belajar dari pengalaman masa lalu. Umumnya, hal ini diwujudkan dalam bentuk aturan dan prosedur kerja dalam organisasi dan berbagai kegiatan perubahan dan perbaikan. Batu sandungan yang paling umum adalah kenyataan bahwa pengetahuan dan pengalaman dalam organisasi ini seringkali tersebar, tidak terdokumentasi, dan bahkan mungkin masih ada di benak setiap orang di dalamnya.

Manajemen pengetahuan atau *knowledge management* adalah upaya untuk meningkatkan kemampuan organisasi dalam mengelola kekayaan intelektualnya, yaitu pengetahuan dan pengalaman yang ada. Tujuannya tentu saja untuk menggunakan sumber daya tersebut untuk meningkatkan kinerja organisasi dan mempercepat pencapaian tujuan pelaksanaan reformasi birokrasi.

Pemerintah Kabupaten Sukabumi memiliki Knowledge Management Forum yang dapat digunakan untuk berbagi ilmu. Hal ini akan membantu merumuskan kebijakan reformasi birokrasi dan benchmark pemerintah daerah untuk Kabupaten Sukabumi. Pemda, sebaliknya, diharapkan untuk berpartisipasi aktif dalam berbagi pengetahuan tentang pengalaman mereka dalam melaksanakan reformasi birokrasi di forum manajemen pengetahuan. Oleh karena itu, panduan ini juga bertujuan untuk memberikan gambaran tentang penerapan manajemen pengetahuan. Hal ini akan sangat meningkatkan kesinambungan pelaksanaan reformasi birokrasi di pemerintah daerah.

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.

B. GAMBARAN UMUM

1. 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.

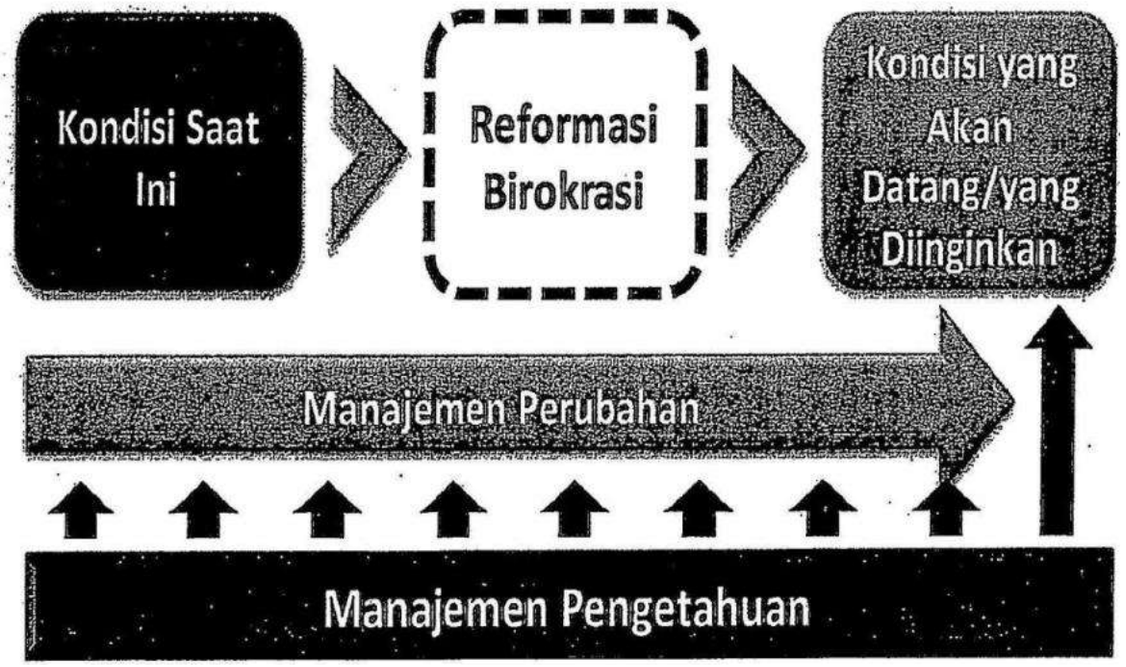
2. Prinsip

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. berbagi pengetahuan, yaitu proses menyebarkan dan membuat pengetahuan tersedia untuk berbagai kalangan yang membutuhkan di dalam organisasi penggunanya. Proses berbagi dapat terbentuk melalui proses sosial pada kultur organisasi yang menghargai aktivitas berbagi pengetahuan. Proses tersebut dapat berlangsung secara tradisional melalui diskusi dan kolokium, maupun melalui medium modern dengan berbasiskan teknologi.
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.

C. 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 jawabannya. 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 Sukabumi 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.

No	AREA PERUBAHAN	HASIL YANG DIHARAPKAN	KEBUTUHAN PENGETAHUAN
5	Penataan Sistem Manajemen Sumber Daya Manusia Aparatur	Dapat meningkatkan manajemen kinerja individu, menyempurnakan sistem informasi manajemen kepegawaian yang terintegrasi, dan meningkatkan profesionalisme pegawai.	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.
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 Kota, menyempurnakan integrasi perencanaan, penganggaran dan manajemen kinerja, serta keterlibatan pimpinan PD mulai dari perencanaan, penilaian kinerja dan pelaporan kinerja semakin meningkat, nilai Akuntabilitas Kinerja Instansi Pemerintah dari B menjadi BB bahkan 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

D. 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 Kabupaten dapat dijelaskan pada Gambar 2 berikut ini:

Gambar 2
Tahapan Implementasi Manajemen Pengetahuan

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

Langkah-langkah yang harus dilakukan pada tahap-2:

1) Pembentukan kebiasaan;
2) Penyediaan payung regulasi;
3) Pemanfaatan teknologi;
4) Penyelarasan dengan strategi manajemen perubahan.

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.

E. MERENCANAKAN IMPLEMENTASI MANAJEMEN PENGETAHUAN

Seperti yang telah disampaikan pada Bab IV, tahap Perencanaan Implementasi Manajemen Pengetahuan terdiri atas 6 (enam) kegiatan utama yang akan dijabarkan satu per satu di dalam bab ini. 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*:*

   a. 42 % di dalam pikiran (otak) pegawai;
   b. 26 % di dalam dokumen *hard copy* (kertas);
   c. 20 % di dalam dokumen elektronik; dan
   d. 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), penamaan 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, selanjutnya adalah 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 pengetahuan;
   2) Manajemen data;
   3) Penggunaan teknologi;
   4) Penggunaan dan evaluasi manajemen pengetahuan;

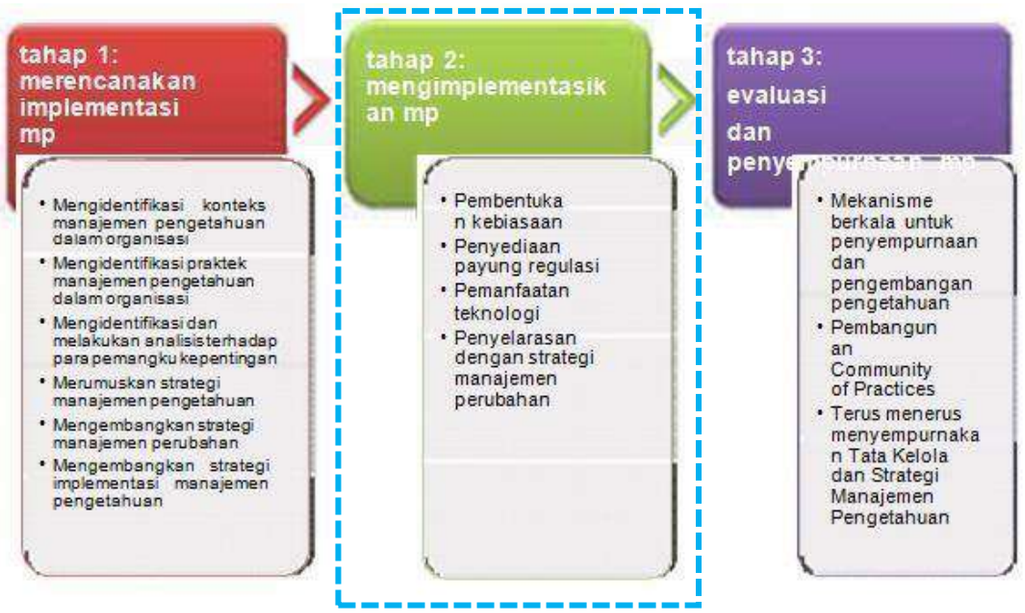
5) Dukungan budaya organisasi.

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.

F. 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 yang dijabarkan pada bab ini. 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 pengklasifkasian 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 integrasi 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.

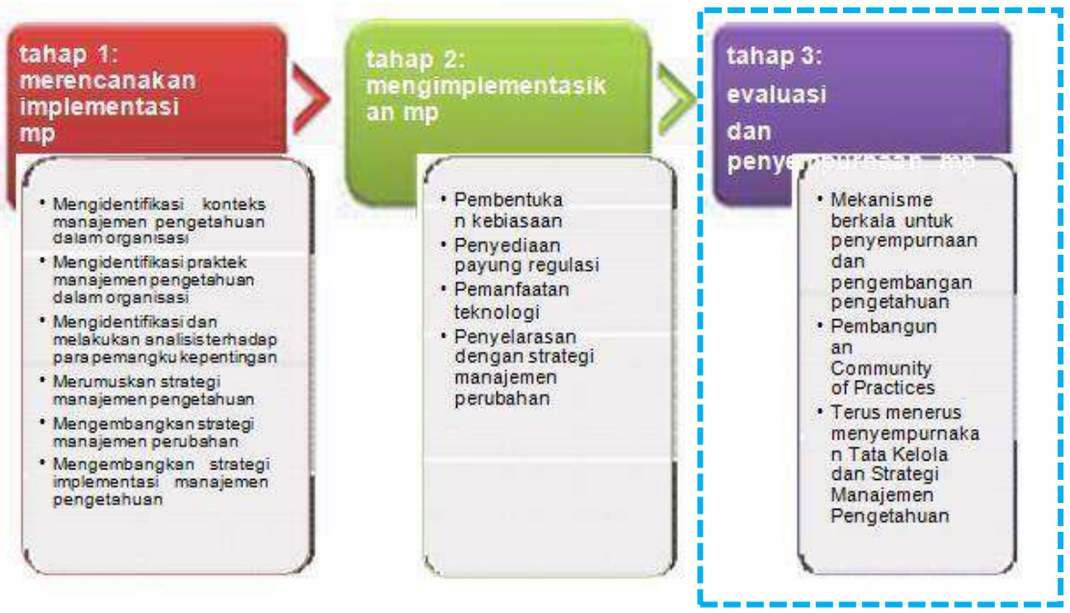
Keluaran pada Tahap Implementasi Manajemen Pengetahuan mencakup, antara lain:

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.

G. 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 Practice* (*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 dan Strategi Manajemen Pengetahuan

Hasil monitoring dan Evaluasi maupun berbagai pengalaman melalui 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:

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

BAB VIII
PEDOMAN MANAJEMEN PERUBAHAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH DAERAH KABUPATEN SUKABUMI

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.

B. GAMBARAN UMUM

1. 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.

2. 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.

C. 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:

a. Organisasi. Organisasi pemerintahan yang belum tepat fungsi dan tepat ukuran (*right sizing).*
b. 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.
c. 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.
d. Kewenangan. Masih adanya praktik penyimpangan dan penyalahgunaan wewenang dalam proses penyelenggaraan pemerintahan dan belum mantapnya akuntabilitas kinerja instansi pemerintah.
e. 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.

f. 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*).

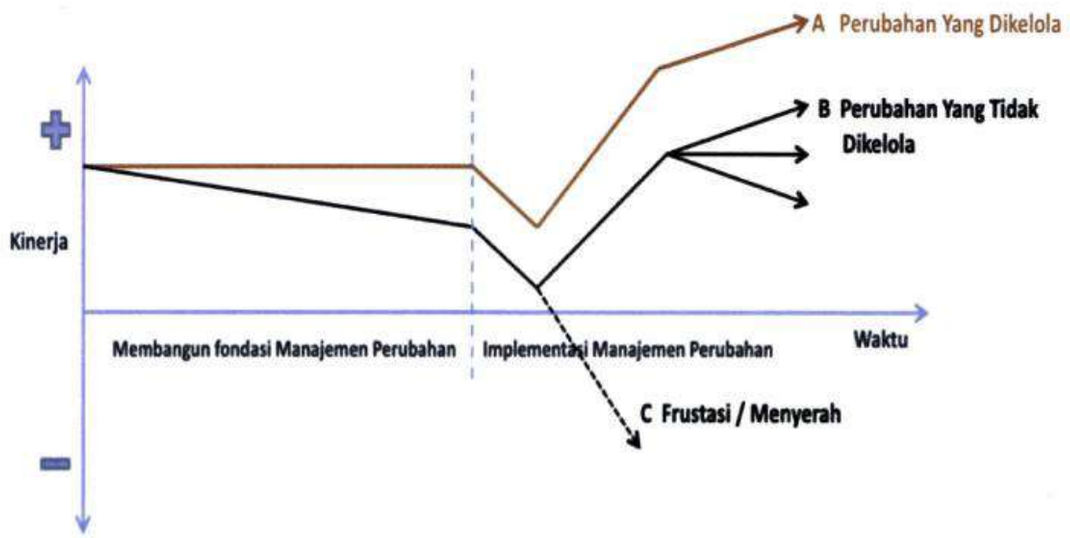
Reformasi birokrasi diharapkan akan menjadi pendorong perubahan untuk membawa Dinas/Badan dan Perangkat Daerah bergeser atau bergerak dari kondisi saat ini menuju ke kondisi yang diharapkan. Karena itu, perubahan yang dikelola secara holistik, terstruktur dan berorientasi hasil akan sangat membantu organisasi, 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:

a. Navigasi. Dimensi ini terkait dengan perencanaan dan pengelolaan perubahan atau transisi dari keadaan organisasi sekarang menuju kondisi organisasi yang diinginkan;
b. Kepemimpinan. Dimensi ini berupaya untuk membangun dan mengkomunikasikan visi perubahan di dalam kondisi yang diinginkan dan juga mengarahkan organisasi ke arah yang dituju;
c. Kepemilikan. Dimensi ini berupaya menciptakan kebutuhan untuk berubah melalui reformasi birokrasi;
d. 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

D. 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.

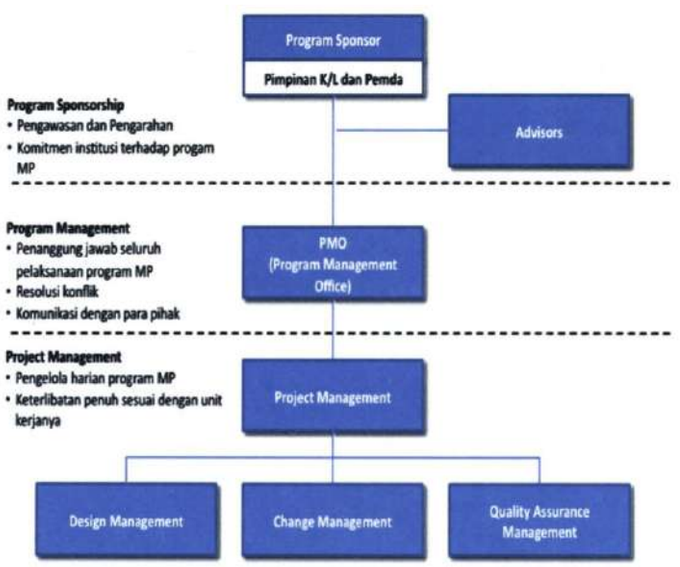
2) Membangun instrumen pengelolaan perubahan

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 instrumen 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.

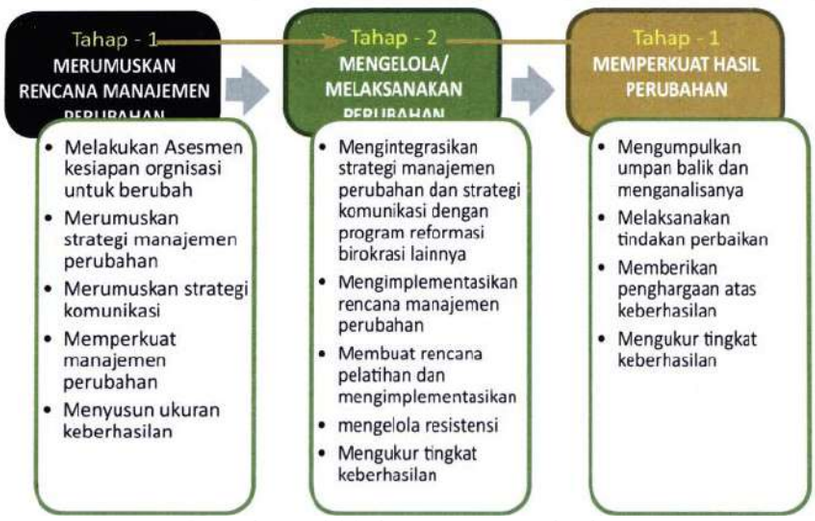
Sebagai ilustrasi pengorganisasian manajemen perubahan di Dinas/Badan dan Perangkat Daerah dapat dilihat pada TABEL 1.

TABEL 1
Ilustrasi Pengorganisasian Manajemen Perubahan

Tingkatan	Pemerintah Pusat	Pemerintah Daerah
Program Sponsorship	Pimpinan K/L	Gubernur/Wali Kota/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 Tahapan Perubahan

Secara komprehensif, langkah-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 standar dan Indikator Kinerja Utama (IKU).
    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.

E. PERUMUSAN RENCANA MANAJEMEN PERUBAHAN

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

a. Tahap Perumusan Rencana Manajemen Perubahan;
b. Tahap Pengelolaan / Pelaksanaan Perubahan; dan
c. Tahap Penguatan Hasil Perubahan.

Gambar 6. Perumusan rencana Manajemen Perubahan

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

- Asesmen terhadap para pemangku kepentingan dan tingkat partisipasi dan keterlibatan mereka terhadap perubahan;
- Asesmen terhadap organisasi yang mencakup kesiapan organisasi untuk berubah, peran, struktur, tugas dan fungsi organisasi untuk mendukung perubahan;
- Asesmen terhadap kemampuan dan kompetensi pegawai untuk mengelola perubahan;
- Pendesainan rencana manajemen perubahan, komunikasi dan pelatihan; dan
- 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/program/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	Resistensi berdasarkan sifatnya		Resistensi berdasarkan pelakunya	
		Aktif	Pasif	Individual	Kolektif
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).

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
2. NormativeReeducative	• 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 harmon is 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
3. Power-Coercive	• Pegawai pada dasarnya patuh dan melaksanakan apa yang diminta. • Perubahan akan berhasil didasarkan pada	• Dua faktor utama yang mempengaruhi pilihan ini adalah jangka waktu perubahan yang ada dan keseriusan

	pelaksanaan wewenang dan pemberlakuan sanksi. • Strategi ini pada dasarnya adalah memperkecil pilihan. • Berdasarkan pengalaman, banyak pegawai juga me rasa aman dan siap dengan strategi ini.	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 pimpinan.
4. Environmental-Adaptive	• Pegawai akan selalu menghindari kerugian & gangguan tetapi mereka mudah beradaptasi dengan keadaan baru. • Perubahan ini didasarkan pada kebutuhan membangun organisasi baru & 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 tra nsformatif. • 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
b. Besaran penolakan yang mungkin muncul. 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

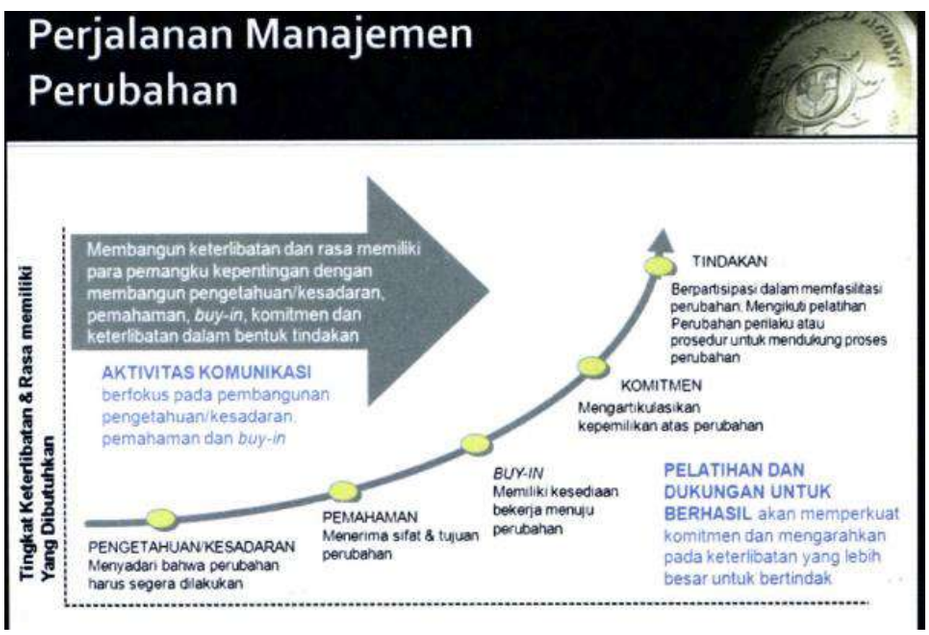
PROGRAM DAN KEGIATAN	**STRATEGI MANAJEMEN PERUBAHAN**			
	Empirical-Rational	Normative-Reeducative	Power-Coercive	Environmental-Adaptive
Penataan dan Penguatan Organisasi				
Redefinisi visi, misi dan strategi		Strategi- 2	Strategi- 1	
Restrukturisasi			Strategi- 1	Strategi- 3
Penguatan unit kerja pelaksana pelayanan publik		Strategi- 2		Strategi- 2

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 mengidentifikasi dan melakukan analisis terhadap para pemangku kepentingan dan hasil pada langkah 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 Saku	Rapat Pimpinan	Talkshow	Artikel Dimedia Massa	Newsletter	Konferensi Pers	Website	Memo	Rapat	Rapat Kerja Tahunan
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 kunci	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
c. Daerah untuk dapat mengelola manajemen perubahan;
d. Memastikan kepemilikan dari proses perubahan. Dalam kaitan reformasi birokrasi, maka pimpinan tertinggi Dinas/Badan dan Perangkat Daerah haruslah menjadi pemilik manajemen perubahan ini;
e. Mempersiapkan sumber daya yang dapat mendukung pelaksanaan manajemen perubahan;

f. Melakukan asesmen untuk mengetahui kondisi terkini organisasi dan kesiapannya untuk melakukan perubahan;
g. 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

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;

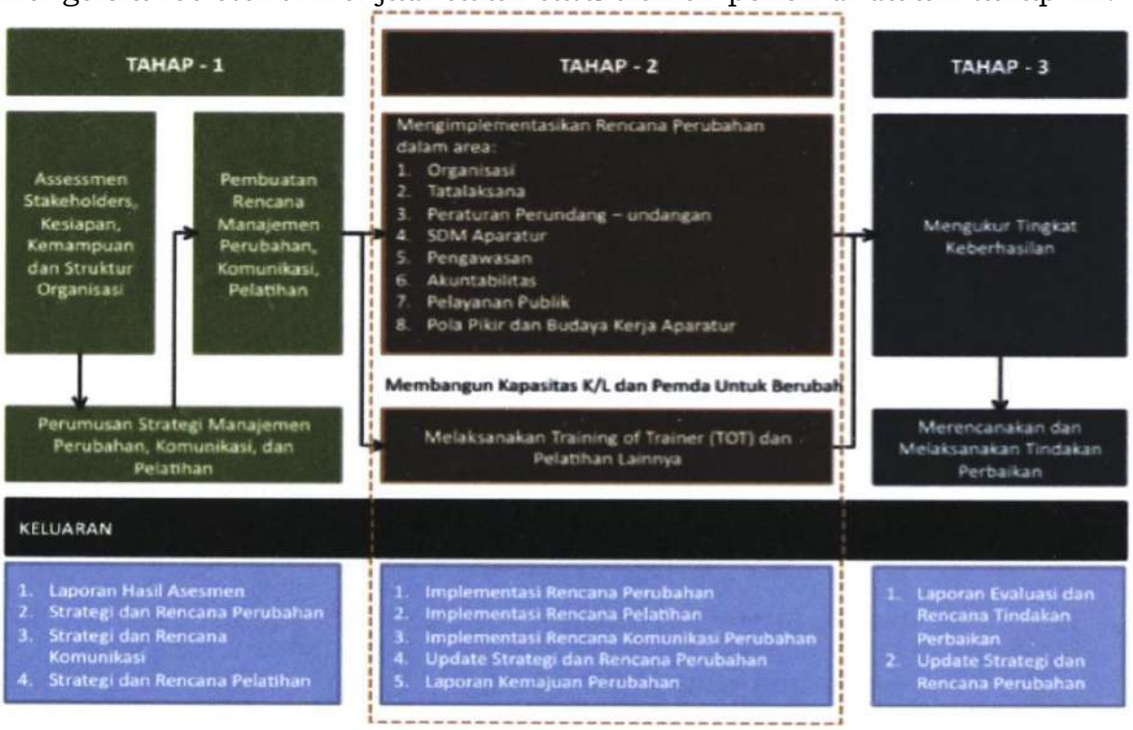
Keluaran utama (Major Output) pada Tahap 1 adalah sebagai berikut:

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.

F. PENGELOLAAN/PELAKSANAAN 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 Kabupaten Sukabumi Nomor 130 Tahun 2021 tentang Road Map Reformasi Birokrasi Pemerintah Daerah Kabupaten Sukabumi Tahun 2020 - 2023 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 75 (tujuh puluh lima) kegiatan reformasi birokrasi sebagaimana tertuang di dalam Peraturan Bupati Kabupaten Sukabumi Nomor 130 Tahun 2021 tentang *Road Map* Reformasi Birokrasi Pemerintah Daerah Kabupaten Sukabumi Tahun 2020-2023. Kegiatan- kegiatan tersebut harus didukung oleh strategi dan rencana perubahan dan komunikasi yang telah disusun pada tahap sebelumnya.

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 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.

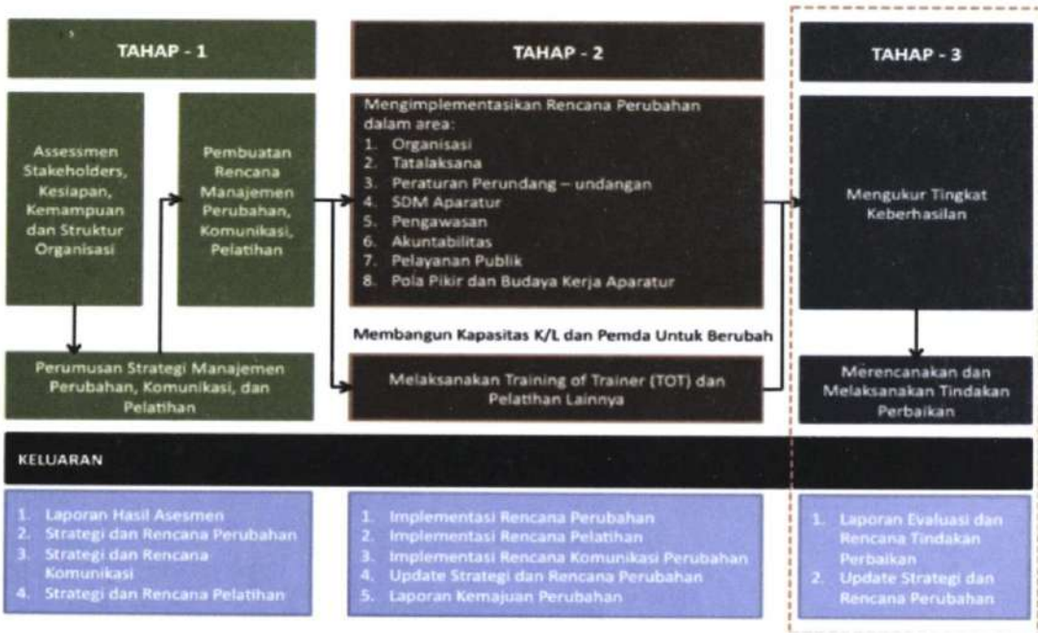
NO	TAKTIK	PENJELASAN
4	Fokus apa yang sudah dicapai saat ini	Sangat penting untuk memikirkan juga pada pencapaian yang sudah didapat, ketika persoalan dalam proses perubahan terjadi. Dengan melakukan ini biasanya orang akan menyadari bahwa lebih banyak hal yang telah berjalan baik daripada yang mereka 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.

G. PENGUATAN HASIL 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 Kabupaten Sukabumi Nomor 130 Tahun 2021 tentang *Road Map* Reformasi Birokrasi Pemerintah Daerah Kabupaten Sukabumi 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	• 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
Mendiagnosa kembali kesenjangan dan mengelola		

Mengimplementasikan tindakan perbaikan da 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.

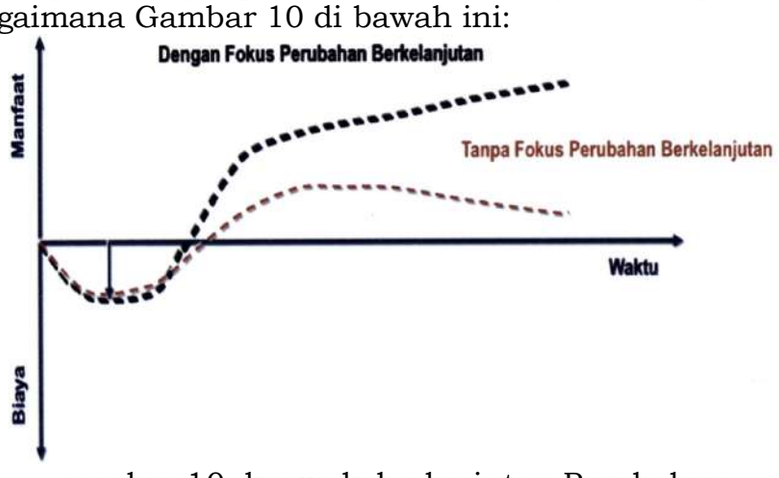
H. MEMBUAT PERUBAHAN BERKELANJUTAN

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 mekanisme 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

BAB IX
MANAJEMEN LAYANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PEMERINTAH KABUPATEN SUKABUMI

Manajemen Layanan SPBE bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE kepada Pengguna SPBE. Manajemen Layanan SPBE dilakukan melalui serangkaian proses pelayanan Pengguna SPBE, pengoperasian Layanan SPBE, dan pengelolaan Aplikasi SPBE.

Pelayanan Pengguna SPBE merupakan kegiatan pelayanan terhadap keluhan, gangguan, masalah, permintaan, dan perubahan Layanan SPBE dari Pengguna SPBE. Pengoperasian Layanan SPBE merupakan kegiatan pendayagunaan dan pemeliharaan Infrastruktur SPBE dan Aplikasi SPBE.

Pengelolaan Aplikasi SPBE sebagaimana dimaksud pada ayat (2) merupakan kegiatan pembangunan dan pengembangan aplikasi yang berpedoman pada metodologi pembangunan dan pengembangan Aplikasi SPBE.

BAB X
AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

A. AUDIT INFRASTRUKTUR SPBE

1. 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:

- Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Infrastruktur SPBE;
- Menyusun Kerangka Kerja regulasi Audit Infrastruktur SPBE dalam proses pendaftaran Auditor dan Lembaga Audit;
- Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Infrastruktur SPBE, guna menambah nilai kepada Unit yang diaudit melalui perbaikan proses dan operasionalnya; dan
- 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
   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 (*experience)* 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 audit memberikan 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 berbagai 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.

2. Tata Cara Pelaksanaan Audit Infrastruktur SPBE
   a. Tata Cara Pelaksanaan Audit

      Audit Infrastruktur 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:
      1) Penyiapan tim audit;
      2) Quick assessment;
      3) Penyiapan rencana audit;
      4) Penyepakatan rencana audit;
      5) Penyiapan protokol audit;
      6) Penetapan parameter acuan;
      7) Pertemuan pembukaan;
      8) Pelaksanaan lapangan;
      9) Pertemuan penutupan;
      10) Analisa data;
      11) Pengelolaan data;
      12) Penyusunan laporan;
      13) Proof-read laporan;
      14) Penyerahan laporan; dan
      15) 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: current issue, 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 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 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 SPBE. 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 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.

3. 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:
1) Evaluasi;
2) Pengarahan; dan
3) Pemantauan.

Ruang lingkup panduan audit manajemen infrastruktur SPBE terdiri atas tahapan:
1) Perencanaan;
2) Pengembangan;
3) Pengoperasian; dan
4) Pemantauan.

Audit manajemen infrastruktur mencakup aktivitas:
1) Manajemen sistem pengendalian internal;
2) Manajemen resiko;
3) Manajemen aset;
4) Manajemen pengetahuan;
5) Manajemen SDM;
6) Manajemen layanan;
7) Manajemen perubahan; dan
8) Manajemen data.

Ruang lingkup panduan fungsionalitas dan kinerja infrastruktur SPBE terdiri atas tahapan:
1) Perencanaan;
2) Pengembangan;
3) Pengoperasian; dan
4) 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:
1) Perencanaan Pusat Data Daerah;
2) Pengembangan Pusat Data Daerah;
3) Pengoperasian Pusat Data Daerah; dan
4) 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

1) Penggunaan perangkat Jaringan Intra Pemerintah antara lain: cara instalasi, akses terhadap perangkat, operasi terhadap perangkat;
2) Prosedur dan Tutorials; dan
3) 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 (*test report*).

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:

1) Lingkup pemeliharaan;
2) Alokasi sumber daya; dan
3) Pencatatan kinerja.

Kriteria penilaian audit infrastruktur SPBE yang terdiri atas Tata Kelola dan Manajemen, *Data Center*/Pusat Data, Jaringan Intra Pemerintah, dan Sistem Penghubung Layanan Pemerintah tercantum dalam Peraturan Bupati ini.

B. AUDIT APLIKASI SPBE

1. 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 nilaikepada 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
        a) 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;
        b) Pimpinan Unit TIK SPBE harus mengembangkan dan menjaga jaminan kualitas dan program peningkatan yang mencakup semua aspek pelaksanaan Audit Aplikasi SPBE;

c) 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:
   - memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*) dan pengalaman (*experience*) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;
   - menggunakan keahlian profesionalnya dengan cermat dan seksama (due professional care) serta berhati-hati (prudent) dalam setiap penugasan;
   - senantiasa mengasah dan melatih kecermatan profesionalnya;
   - meningkatkan pengetahuan, keahlian dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
   - mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
   - memiliki pengetahuan (knowledge), keterampilan (skill), sikap (attitude) dan pengalaman (experience) yang sesuai guna memenuhi tanggung jawabnya dalam pelaksanaan audit.

d) 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;

e) 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.

2) Standar Pelaksanaan

a) 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:
   - 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*);
   - Menyampaikan rencana audit (audit plan) kepada pimpinan Unit SPBE dan Auditee untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumber daya;
   - Mengelola sumberdaya audit yang tepat, memadai dan efektif untuk melaksanakan rencana audit yang telah disetujui;
   - Melakukan koordinasi dengan pimpinan Unit SPBE untuk menjamin bahwa pelaksanaan Audit Aplikasi SPBE berjalan efektif dan efisien; dan

- Memberi laporan yang memadai kepada pimpinan Unit SPBE dan unit mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.

b) Unit wajib melaksanakan Aktivitas audit Aplikasi SPBE jika memiliki tujuan sebagai berikut:
   - Peningkatan kinerja birokrasi dan pelayanan publik;
   - Penilaian kesesuaian dengan standar/prosedur/ pedoman, dan kesesuaian dengan rencana/kebutuhan/ kondisi;
   - Identifikasi status teknologi yang dimiliki, identifikasi daya saing/kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
   - Perencanaan pengembangan sistem/teknologi dan perencanaan perbaikan kelemahan; dan/atau
   - Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.

c) Pemeriksaan yang dilakukan mencakup:
   - Penerapan tata kelola dan manajemen Aplikasi SPBE;
   - Fungsionalitas dan Kinerja Aplikasi SPBE; dan
   - Tingkat kepatuhan terhadap regulasi

d) 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

e) Perencanaan tersebut yang dituangkan dalam Rencana Audit (*Audit Plan*) dengan mempertimbangkan berbagai hal, antara lain:
   - Sistem pengendalian internal dan kepatuhan Auditee terhadap acuan atau benchmark;
   - Penetapan tujuan audit aplikasi SPBE;
   - Penetapan kecukupan lingkup; dan
   - Penggunaan metodologi yang tepat

f) 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:
   - Memperoleh bukti-bukti audit yang cukup, handal dan relevan untuk mendukung penilaian dan kesimpulan;
   - Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
   - Menyiapkan, mengelola dan menyimpan data dan informasi yang diperoleh selama pelaksanaan audit; dan
   - Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.

g) 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

h) 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:
   - Kepatuhan terhadap Kode Etik dan Standar Audit;
   - bKesesuaian terhadap Piagam Audit;
   - Kesesuaian terhadap Rencana Audit; dan
   - Kesesuaian terhadap Protokol Audit

i) 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

j) 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

3) Standar Pelaporan
   a) Laporan hasil audit dibuat oleh Unit TIK SPBE dalam bentuk Dokumen Laporan Audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas;
   b) 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
4) Standar Tindak Lanjut
   a) Pemantauan terhadap legalitas, kompetensi dan kinerja Unit SPBE dilakukan melalui mekanisme registrasi dan laporan tahunan pelaksanaan audit;
   b) 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.

2. 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 (on site audit); dan
3) Tahap analisa data dan pelaporan (post audit).

Adapun tiga kelompok tersebut meliputi hal-hal sebagai berikut:

1) penyiapan tim audit;
2) quick assessment;
3) penyiapan rencana audit;
4) penyepakatan rencana audit
5) penyiapan protokol audit;
6) penetapan parameter acuan;

7) pertemuan pembukaan;
8) pelaksanaan lapangan;
9) pertemuan penutupan;
10) analisa data;
11) pengelolaan data;
12) penyusunan laporan;
13) proof-read laporan;
14) penyerahan laporan; dan
15) 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:

1) tujuan audit;
2) lingkup;
3) pendekatan;
4) kriteria;
5) parameter;
6) acuan;
7) metode pengumpulan data;
8) penentuan objek;
9) data primer dan sekunder;
10) metode analisa;
11) deliverable; dan
12) 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, 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 SPBE. 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 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 TIK SPBE kepada Unit SPBE dan lembaga lain sesuai kesepakatan dengan Auditee. Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh pimpinan Unit TIK SPBE kepada Unit SPBE 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.

3. Panduan Teknis 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:

a. Evaluasi Tata Kelola;
b. Pengarahan Tata Kelola; dan
c. 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 SPBE 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 penanganannya. (Troubleshooting); 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. Sumberdaya konfigurasi; dan
d. Penjadwalan manajemen konfigurasi.

Kriteria penilaian audit aplikasi SPBE berdasarkan ketentuan peraturan perundang-undangan.

BAB XI PENUTUP

Pedoman ini diharapkan dapat membantu Seluruh Perangkat Daerah dalam mengimplementasikan Manajemen Sistem Pemerintahan Berbasis Elektronik yang di dalamnya termasuk Manajemen Risiko SPBE, Manajemen Keamanan Informasi, Manajemen Aset Teknologi Informasi dan Komunikasi, Manajemen Pengetahuan dan Manajemen Perubahan. Pedoman ini juga diharapkan dapat menjadi acuan oleh Perangkat Daerah pengelola TIK dalam pelaksanaan Audit Infrastruktur dan Audit Aplikasi.

Penerapan Manajemen SPBE dan Audit TIK yang baik dan benar sesuai dengan pedoman yang ada dapat membantu meningkatkan kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah Kabupaten Sukabumi.

BUPATI SUKABUMI,

MARWAN HAMAMI