AUDIT TEKNOLOGI INFORMASI

PENERAPAN PADA *E-GOVERNMENT*

(*Best Practice e-government* Pemerintah Kota)

Buku ini merupakan luaran penelitian yang dibiayai oleh
Universitas Putra Indonesia YPTK Padang

Dr. Ir. Sumijan, M.Sc.
Pradani Ayu Widya Purnama, S.Kom., M.Kom.

AUDIT TEKNOLOGI INFORMASI

PENERAPAN PADA *E-GOVERNMENT*

(*Best Practice* e-*government* Pemerintah Kota)

UU No 28 tahun 2014 tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

i. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
ii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
iii. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

AUDIT TEKNOLOGI INFORMASI

PENERAPAN PADA *E-GOVERNMENT*

(*Best Practice* e-*government* Pemerintah Kota)

Dr. Ir. Sumijan, M.Sc.

Pradani Ayu Widya Purnama, S.Kom., M.Kom.

PENERBIT
INSAN CENDEKIA MANDIRI
Publisher of educational books

AUDIT TEKNOLOGI INFORMASI
PENERAPAN PADA *E-GOVERNMENT*
(*Best Practice e-government* Pemerintah Kota)
Dr. Ir. Sumijan, M.Sc.
Pradani Ayu Widya Purnama, S.Kom., M.Kom.

Editor:
Yahya Alhidayah

Desain Cover:
Mutia Anika

Sumber:
www.insancendekiamandiri.co.id

Tata Letak:
@Teamminang

Proofreader:
Tim Insan Cendekia

Ukuran:
xiv, 232 hlm, Uk: 14,8 x 21 cm

ISBN:
978-623-6719-98-5
Cetakan Pertama:
Oktober 2020

PENERBIT INSAN CENDEKIA MANDIRI
(Grup Penerbitan CV INSAN CENDEKIA MANDIRI)
Kapalo Koto No. 8, Selayo, Kecamatan Kubung, Kabupaten Solok
Sumatra Barat – Indonesia 27361
HP/WA: 0813-7272-5118
Website: www.insancendekiamandiri.co.id
www.insancendekiamandiri.com
E-mail: penerbitbic@gmail.com

KATA PENGANTAR

Audit Teknologi Informasi merupakan salah satu bidang kajian yang saat ini sedang berkembang secara pesat seiring dengan perkembangan dunia bisnis dan kemajuan teknologi informasi sebagai pendukung dari aktivitas dalam melakukan evaluasi dan pengukuran terhadap tingkat kematangan (*Maturity*) tata kelola teknologi informasi. Semakin kompleksnya sistem dan perannya di berbagai bidang kehidupan membutuhkan kajian Audit Teknologi Informasi melalui pendekatan yang nyata seperti pada Pemerintahan (*e-government*), bidang kesehatan, bidang pendidikan, dan lainnya.

Selama ini, pembahasan dan diskusi mengenai audit teknologi informasi masih banyak asumsi umum yang menggiring pemahaman bahwa audit teknologi informasi hanya berkaitan dengan pendekatan teknis dan konseptual saja. Multiperspektif atas audit teknologi informasi menunjukkan bahwa audit teknologi informasi merupakan suatu studi pada bidang multidisiplin seperti akuntansi, kesehatan, pemerintahan, kepolisian, psikologi, manajemen, dan lain sebagainya. Hal tersebut memperkuat posisi Audit Teknologi Informasi yang didukung oleh teknologi informasi dalam membentuk sistem *enterprise application*, memerankan fungsinya dalam mendongkrak rantai nilai suatu perusahaan untuk mengukur tingkat kematangan tata kelola penggunaan teknologi informasi.

Buku ini akan sangat berguna bagi manajemen tata kelola teknologi informasi khsususnya di pemerintahan atau pemakai aplikasi system informasi dan mahasiswa yang ingin memperoleh gambaran ringkas tetapi utuh tentang

implementasi dalam bentuk studi kasus dalam Audit Teknologi Informasi pada *e-government* terkait pendekatan, jenis audit teknologi informasi, dan peran audit teknologi informasi strategis dalam perusahaan untuk memprioritaskan pengembangan tata kelola teknologi informasi.

Penulisan Buku ini tidak akan terlaksana dengan baik tanpa bantuan dari berbagai pihak. Buku ini merupakan luaran penelitian yang dibiayai oleh Universitas Putra Indonesia YPTK Padang. Para penulis buku ini adalah lulusan Program Pacasarjana yang mendalami kajian Teknologi Informasi dan Komunikasi (dari aspek perilaku pengguna sistem dan pengelola Sistem), dan saat ini menjadi dosen tetap di Fakultas Ilmu Komputer, Univeristas Putra Indonesia "YPTK" Padang. Latar belakang salah satu penulis bergelar Doktor Teknologi Informasi (DTI) menjadi salah satu elemen yang memperkaya kajian dan paparan dalam buku ini.

Akhirnya saya ucapkan selamat kepada para penulis atas terbitnya buku ini, dan semoga buku ini bermanfaat bagi pembaca yang ingin belajar Audit Teknologi Informasi. Mudah-mudahan para penulis terus berkiprah dalam penulisan buku dan buku-buku yang lainnya serta pengembangan ilmu khususnya bidang Teknologi Informasi dan Komunikasi sesuai dengan perkembangan ilmu dan teknologi informasi saat ini berkembang pesat, akhirnya penulis memohon kepada pembaca buku ini jika ada masukan saran dan kritikan dalam buku ini silahkan di email: soe@upiyptk.org /sumijan@upiyptk.ac.id.

Padang, September 2020

Penulis

DAFTAR ISI

DAFTAR GAMBAR

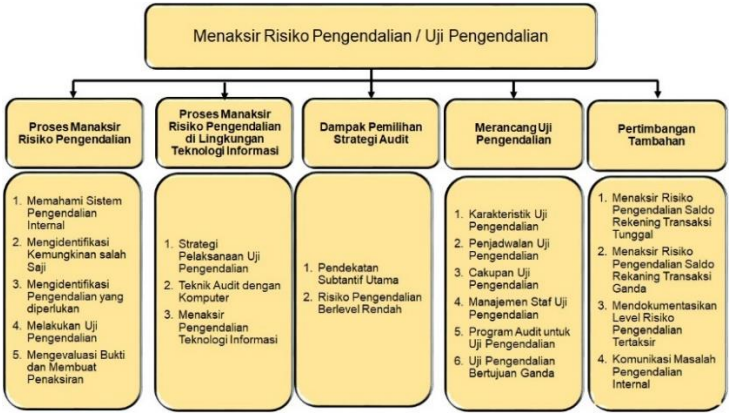
DAFTAR TABEL

BAB 1

KONSEP PENGENDALIAN INTERNAL

1.1. PENDAHULUAN

Pengendalian adalah proses audit fase II dan III, yaitu menaksir risiko salah saji yang material dan merespons risiko tertaksir tersebut. Auditor melakukan uji pengendalian untuk menentukan apakah pengendalian internal yang efektif telah diberlakukan untuk mencegah atau mendeteksi dan mengoreksi salah saji laporan keuangan. Auditor eksternal melakukan uji pengendalian atas seluruh asersi dalam laporan keuangan yang material untuk memberikan opini atas pengendalian internal. Auditor internal melakukan uji pengendalian untuk menindaklanjuti pendekatan risiko tertaksir berlevel rendah. Garis besar modul disajikan dalam diagram sebagai berikut:



Gambar 1.1. Resiko Pengendalian dan Uji Pengendalian

A. INTERNAL PENGENDALIAN DI PERUSAHAAN ENRON

Pada tanggal 23 Februari 2001, Arthur Andersen LLP menyatakan opini audit bahwa atas asersi manajemen sistem pengendalian internal di Enron Corp dan anak perusahaannya, per 31 Desember 2000, 1999, dan 1998 dapat memberikan kepastian yang wajar atas keandalan laporan keuangan dan perlindungan aset dari akuisisi, penggunaan, atau disposisi yang tidak sah, disajikan dengan wajar, di seluruh segi yang material, sesuai dengan standar pengendalian yang berlaku. Laporan ini sesuai dengan standar atestasi AICPA tentang pelaporan pengendalian internal dan sudah menggunakan komponen pengendalian internal COSO sebagai kriteria pelaporan pengendalian internal.

Arthur Andersen, LLP melakukan uji pengendalian untuk mendukung opini tersebut. Dengan menggunakan tinjauan ke belakang, apa yang dapat kita pelajari tentang pengendalian internal di Enron dan efektivitas uji pengendaliannya?

1. Direksi Enron, dengan mengabaikan konflik kepentingan mereka, mengizinkan Andrew Fastow, CFO, untuk bernegosiasi atas nama Enron dengan perusahaan-perusahaan yang CFO tersebut memiliki kepentingan kepemilikan. Pada akhirnya, Fastow mendapatkan sekitar $31 juta dolar untuk dirinya sendiri dari kesepakatan tersebut. Namun demikian, menurut Andersen, direksi menyetujui transaksi tersebut.
2. Enron memiliki sebuah kode etik perusahaan. Hal ini sudah benar. Tetapi apakah kode etik tersebut dipatuhi? Agar pengendalian internal bisa efektif, kode etik harus didesain dengan baik, didudukkan pada tempatnya di operasi, dan dilaksanakan secara efektif. Pada kasus ini, kode etik dirancang dengan baik tetapi sebagian besar diabaikan. Manajemen senior mengalami kegagalan untuk memberikan penekanan atas pentingnya masalah etika.
3. Pengendalian internal dimulai puncak organisasi. Selain masalah etika, manajemen senior sangat menekankan pencapaian target *earnings* kepada manajer yang lain. Para pejabat Enron menerima bonus berdasarkan pencapaian target mereka. Pada akhir tahun 1999 para eksekutif Enron mengatur transaksi dengan Merrill Lynch dan membayar fee $17 juta di akhir kuartal keempat yang memungkinkan Enron untuk mengakui $50 juta sebagai earnings dan mencapai target earnings mereka. (Kasus SEC Littigation No. 18515). Kasus tersebut oleh SAS 99 disebut sebagai insentif untuk melakukan kecurangan laporan keuangan.

4. Enron mendirikan Departemen Manajemen Risiko dan Pengendalian untuk mengevaluasi transaksi dan kesepakatan yang material dengan para rekanan. Namun demikian, para rekanan Enron diberi hak untuk memberi masukan tentang promosi dan bonus kepada para pejabat di departemen tersebut. Departemen Manajemen Risiko dan Pengendalian menjadi tidak independen, dan akibatnya sering memberikan kesimpulan yang tidak konsisten. Misalnya, manajemen senior tetap melakukan kesepakatan dengan rekanan untuk mencatat earnings meskipun menghadapi risiko yang tinggi. Kasus ini merupakan contoh pengendalian operasi yang tidak efektif.
5. Pertahanan utama perusahaan adalah para pekerjanya. Meskipun demikian, keprihatinan Sharon Watkins, Margaret Ceconi dan pekerja Enron lainnya diabaikan dan tidak ditangani secara serius. (sumber: Modern Auditing, William C, Boynton and Raymond N. Johnson).

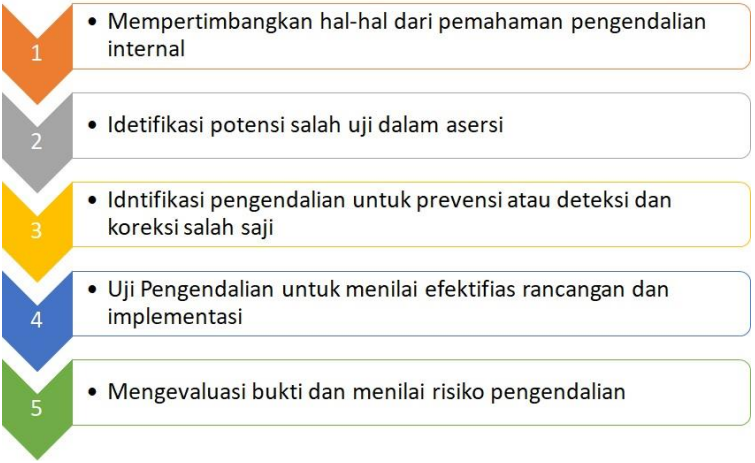
B. PROSES PENAKSIRAN RISIKO PENGENDALIAN

Tujuan penaksiran risiko pengendalian adalah untuk membantu auditor dalam membuat sebuah penilaian tentang risiko salah saji laporan keuangan yang material. Penaksiran risiko pengendalian meliputi evaluasi tentang efektivitas dari:

1. Rancangan pengendalian internal, dan
2. Implementasi pengendalian internal.

Penaksiran pengendalian risiko membantu auditor membuat penilaian tentang karakteristik, pemilihan, dan luasan prosedur audit. Pada akhirnya, uji pengendalian

memberikan bukti sebagai dasar opini auditor. Risiko pengendalian, seperti halnya model audit risiko atas komponen-komponen yang lain, ditaksir pada setiap asersi laporan keuangan. Banyak pengendalian mencegah salah saji dengan asersi pencatatan transaksi. Penaksiran risiko pengendalian dibuat atas masing-masing asersi, bukan atas pengendalian internal secara keseluruhan, setiap komponen pengendalian internal, atau setiap prosedur atau kebijakan. Dalam melakukan penaksiran risiko pengendalian untuk sebuah asersi, auditor mengikuti langkah-langkah yang digambarkan 1.2. Langkah keempat, yaitu melakukan uji pengendalian, tidak diharuskan bagi auditor internal apabila risiko pengendalian ditaksir pada level tinggi. Tiap langkah-langkah tersebut didiskusikan sebagai berikut.



Gambar 1.2. Langkah-langkah Penaksiran Risiko Pengendalian

1. **Mempertimbangkan Hal yang Diperoleh dari Prosedur**

Mendapatkan Pemahaman Auditor melakukan prosedur mendapatkan pemahaman pengendalian internal atas asersi laporan keuangan yang material. Auditor mendokumentasi pemahaman tersebut dalam bentuk kuesioner, bagan alir, dan/atau memoranda naratif tentang pengendalian internal. Analisis terhadap dokumen ini adalah titik awal penaksiran risiko pengendalian. Standar Audit, AU 319.25 (PSA No. 69 paragraf 19) menyatakan bahwa pemahaman yang digunakan oleh auditor untuk (1) mengidentifikasi jenis potensi salah saji, (2) mempertimbangkan faktor yang memengaruhi risiko salah saji yang material, dan (3) merancang uji pengendalian. Jadi, untuk kebijakan dan prosedur yang relevan dengan asersi tertentu, auditor menggunakan tipe jawaban Ya/Tidak dan komentar tertulis di dalam kuesioner, kelebihan dan kekurangan dicatat dalam bagan alir dan memoranda naratif.

Setelah mendapatkan pemahaman pengendalian internal, auditor melakukan penyelidikan, mengamati kinerja tugas dan pengendalian, dan menginspeksi dokumen-dokumen. Dalam proses ini auditor mungkin mendapatkan bukti tentang bagaimana pengendalian dalam implementasi aktual sehingga memungkinkan auditor untuk menaksir risiko pengendalian di bawah level tinggi. Umumnya bukti yang diperoleh tidak cukup luas untuk memungkinkan penaksiran risiko pengendalian pada level rendah, tetapi mungkin cukup untuk mendukung penaksiran risiko pengendalian pada level tinggi. Auditor mungkin mendasarkan

penaksiran risiko pengendalian pada bukti-bukti yang didapatkan ketika memahami pengendalian internal.

2. Identifikasi Potensi Salah Saji

Identifikasi potensi salah saji adalah proses yang digunakan auditor untuk mempertimbangkan titik-titik terjadinya kesalahan atau kecurangan untuk asersi yang terkait dengan kelas transaksi utama, saldo rekening, dan pengungkapan dalam laporan keuangan. Beberapa kantor audit menggunakan perangkat lunak komputer untuk menampilkan kuesioner dan sekaligus mengolah jawaban responden pada asersi tertentu. Oleh karena itu, semua auditor sangat perlu memahami logika komputer yang digunakan untuk mengevaluasi setiap asersi. Misalnya, potensi salah saji dalam asersi pengeluaran kas dan dua saldo rekening utama yang dipengaruhi oleh pengeluaran kas yaitu kas dan utang dagang. Contoh potensi salah saji untuk beberapa asersi terkait dengan transaksi pengeluaran kas diperlihatkan pada kolom pertama Gambar 1.2. Adalah pemahaman asersi yang menuntun auditor memahami potensi salah saji.

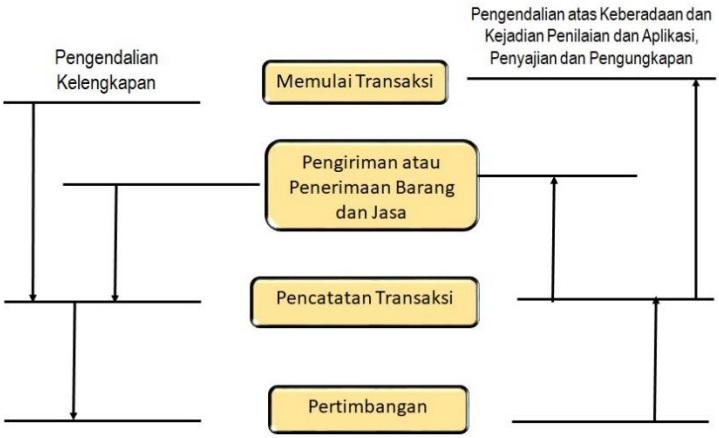
3. Identifikasi Pengendalian yang Diperlukan

Auditor mengidentifikasi pengendalian yang diperlukan untuk mencegah atau mendeteksi serta mengoreksi potensi salah saji untuk asersi. Identifikasi dilakukan dengan perangkat lunak yang memproses respons kuesioner atau secara manual dengan checklist. Pada saat identifikasi auditor harus memastikan:

a). Karakteristik pengendalian untuk mencegah atau mendeteksi dan mengoreksi salah saji;
b). Karakteristik pengendalian yang telah diimplementasikan oleh manajemen;
c). Efektivitas tiap pengendalian. Jika ditemukan beberapa pengendalian untuk sebuah asersi, auditor memilih pengendalian kunci, yaitu pengendalian yang diyakini paling efektif;
d). Risiko jika pengendalian tidak efektif.

Kolom kedua gambar 1.2. mengilustrasikan kemungkinan pengendalian untuk asersi laporan keuangan tertentu. Terdapat beberapa pengendalian yang dapat didesain untuk sebuah potensi salah saji. Sebaliknya, sebuah pengendalian dapat digunakan untuk mendeteksi lebih dari satu jenis potensi salah saji. Sebagai contoh, rekonsiliasi bank dapat digunakan untuk mendeteksi pencatatan cek pada jurnal pengeluaran kas dalam jumlah yang tidak semestinya (asersi penilaian dan alokasi), dan juga dapat mendeteksi cek yang belum di jurnal (asersi kelengkapan).

Banyak pengendalian internal memiliki sebuah desain umum. Tiap transaksi memiliki empat fungsi dasar; (1) memulai, (2) pengiriman atau penerimaan barang dan jasa, (3) pencatatan transaksi, dan (4) pertimbangan, seperti digambarkan dalam gambar 1.3.



Gambar 1.3. Fungsi Transaksi dan Desain Pengendalian Internal

Diskusi selanjutnya membicarakan bagaimana perusahaan mendesain pengendalian internal untuk mengendalikan asersi kelengkapan, keberadaan dan keterjadian, penilaian dan alokasi (keakuratan), dan penyajian dan pengungkapan (klasifikasi), tanpa memandang siklus transaksi.

Pengendalian internal atas asersi kelengkapan secara umum dimulai dengan mendapatkan informasi tentang transaksi ketika dimulai dan ikuti transaksinya melalui setiap fungsi. Biasanya digunakan dokumen yang sudah dinomori, catatan penomoran dokumen. Kemudian dikembangkan pelaporan dengan menandingkan setiap transaksi yang dimulai dengan pengiriman atau penerimaan barang atau jasa dan setiap transaksi yang dimulai dengan pencatatan transaksi tersebut. Misalnya, suatu sistem dapat menghasilkan laporan dari order penjualan yang

belum dikirimkan dan laporan pengiriman yang belum dibuatkan, dalam faktur penjualan. Perusahaan merekonsiliasi laporan penjualan dengan penerimaan kas atau membuat laporan jatuh tempo piutang untuk menentukan kas yang belum diterima.

Pengendalian internal atas asersi keberadaan dan keterjadian secara umum bekerja secara berkebalikan dengan asersi kelengkapan. Pengendalian atas keterjadian penjualan membandingkan informasi pencatatan transaksi dengan informasi tentang aliran barang atau jasa yang biasanya didapatkan pada saat pengiriman atau penerimaan barang atau jasa. Misalnya, membandingkan informasi dalam faktur penjualan dengan informasi tentang pengiriman dari barang atau penyelesaian jasa sebelumnya (informasi tentang kuantitas yang dicatat dalam bandingannya dengan kuantitas yang dikirimkan dan informasi tentang periode akuntansi ketika transaksi dicatat vs periode akuntansi ketika barang dikirimkan). Pengendalian atas keterjadian penerimaan atau pengeluaran kas dibandingkan dengan informasi tentang keberadaan piutang dan utang.

Pengendalian internal atas asersi penilaian dan alokasi menyerupai asersi keberadaan dan keterjadian. Pengendalian atas penilaian (keakuratan) membandingkan informasi tentang pencatatan transaksi dengan informasi tentang pengiriman atau penerimaan barang atau jasa dan informasi tentang memulai transaksi. Sebagai contoh, membandingkan informasi tantang faktur penjualan dengan informasi tentang pengiriman barang atau pengantaran jasa

sebelumnya dan juga dengan informasi tentang memulai transaksi. Pengendalian atas penilaian penerimaan atau pengeluaran kas dibandingkan dengan informasi piutang atau utang.

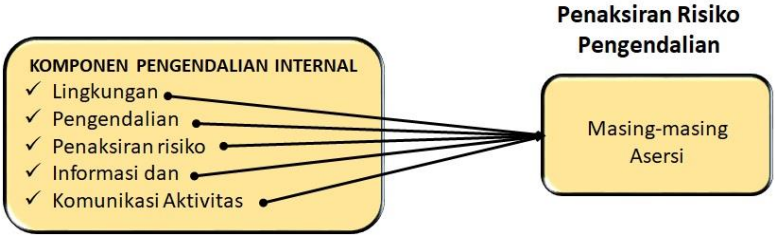
Pengendalian internal atas asersi penyajian dan pengungkapan (klasifikasi) membandingkan informasi tentang pencatatan transaksi dengan informasi ketika transaksi dimulai. Pengendalian tersebut membandingkan jumlah rekening buku besar yang berhubungan dengan pencatatan transaksi dengan jumlah akun yang ditetapkan saat transaksi dimulai. Misalnya, membandingkan masukan (input) informasi faktur penjualan dengan kode-kode akun dalam order penjualan.

Pemahaman pengendalian yang diperlukan juga membutuhkan pertimbangan kondisi dan penilaian. Misalnya, pada kasus transaksi dengan pengeluaran kas yang besar, diperlukan daftar cek terpisah yang sesuai dengan daftar ringkasan penerbitan cek dengan input jurnal pengeluaran kas untuk mendeteksi salah saji dengan cepat. Jika pengeluaran kas berjumlah sedikit dan waktu deteksi salah saji tidak esensial, rekonsiliasi bank periodik cukup memadai untuk mengompensasi kurangnya daftar cek harian. Dalam situasi tersebut, rekonsiliasi bank disebut pengendalian kompensasi.

Pengendalian yang diperlukan ditunjukkan pada Gambar 1.2, baik pengendalian aplikasi dalam perangkat lunak atau pengendalian manual dapat diklasifikasikan sebagai komponen pengendalian aktivitas dalam pengendalian internal. Auditor harus sadar bahwa beberapa komponen pengendalian

internal secara simultan dapat mempengaruhi risiko potensi salah saji dalam asersi terkait dengan beberapa kelas transaksi atau saldo rekening. Sebagai contoh, lingkungan pengendalian seperti kompetensi dan kepercayaan manajer dan pekerja yang terlibat dalam transaksi pengeluaran kas dapat mempengaruhi banyak asersi untuk kelas transaksi tersebut. Pada kenyataannya, kurangnya kompetensi dan kepercayaan manajer atau pekerja kunci dapat mengurangi efektivitas aktivitas pengendalian. Jadi, auditor harus mengasimilasikan informasi tentang tiap elemen sistem pengendalian internal ketika mempertimbangkan risiko potensi salah saji pada asersi tertentu. Konsep ini dapat digambarkan pada gambar di bawah ini.

Auditor dapat membuat penaksiran pendahuluan atas risiko pengendalian berdasarkan pemahaman menyeluruh tentang desain pengendalian dan bagaimana desain itu diimplementasikan. Dengan demikian, pengetahuan tersebut hanya memungkinkan auditor untuk menaksir risiko pengendalian pada level maksimal. Untuk menaksir risiko pengendalian di bawah level tinggi, harus diperoleh bukti efektivitas pengendalian yang diperlukan tersebut setelah diimplementasikan.



Gambar 1.4. Komponen Transaksi dan Desain Pengendalian Internal

4. Melakukan Uji Pengendalian

Kolom ketiga menampilkan uji pengendalian yang mungkin untuk tiap pengendalian yang ditampilkan pada kolom kedua. Uji pengendalian disajikan meliputi teknik audit berbantuan komputer, memeriksa dokumen, memeriksa personil, dan mengamati personil yang melakukan pengendalian. Uji pengendalian harus menghasilkan bukti efektivitas desain dan implementasi pengendalian yang dibutuhkan. Misalnya, menggunakan teknik audit berbantuan komputer untuk menguji bahwa komputer membandingkan jumlah cek yang diterbitkan dengan jurnal pengeluaran kas, diperoleh bukti efektivitas implementasi pengendalian atas pencatatan transaksi pengeluaran kas.

Dalam memilih pengujian yang harus dikerjakan, auditor mempertimbangkan jenis bukti yang diperlukan dan biaya pengujian. Setelah pengujian dipilih, auditor menyiapkan program pengauditan tertulis dan resmi untuk uji pengendalian yang direncanakan. Tambahan informasi tentang perencanaan dan pelaksanaan uji pengendalian

disediakan pada penjelasan lebih lanjut pada modul ini.

5. Evaluasi Bukti dan Membuat Penaksiran

Penaksiran akhir risiko pengendalian untuk asersi laporan keuangan didasarkan pada evaluasi bukti yang diperoleh dari (1) prosedur untuk memahami pengendalian internal dan (2) uji pengendalian terkait. Penentuan level risiko pengendalian tertaksir merupakan masalah penilaian profesional. Auditor harus mempertimbangkan karakteristik, pemilihan waktu, dan luasan uji pengendalian ketika membuat penilaian tersebut.

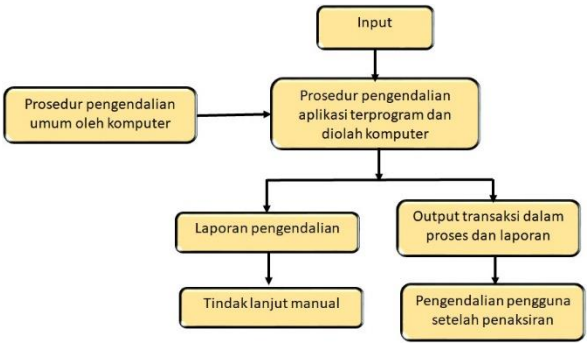
Jika mengidentifikasi kekuatan pengendalian internal, auditor harus menentukan apakah efektif dari segi kos jika menguji efektivitas implementasi pengendalian internal dan memodifikasi karakteristik, pemilihan waktu, atau luasan pengujian substantif. Jika menemukan kelemahan dalam pengendalian internal, auditor harus mempertimbangkan kemungkinan (frekuensi penyimpangan) dan besarnya potensi salah saji ketika menentukan apakah kelemahan pengendalian internal tersebut signifikan atau material.

Akhirnya, penaksiran risiko pengendalian dapat disajikan secara kuantitatif (misalnya terdapat 5% risiko bahwa pengendalian terkait tidak akan mencegah atau mendeteksi dan mengoreksi salah saji tertentu) atau secara kualitatif (misalnya terdapat risiko rendah bahwa pengendalian terkait tidak akan mencegah atau mendeteksi dan mengoreksi salah saji tertentu). Penaksiran risiko pengendalian untuk

sebuah asersi adalah faktor kritis dalam penentuan level deteksi risiko yang dapat diterima untuk asersi tersebut. Jika risiko pengendalian ditaksir terlalu rendah, deteksi risiko mungkin diatur terlalu tinggi dan auditor tidak dapat melakukan tes substantif yang memadai, akibatnya audit menjadi tidak efektif. Sebaliknya, jika risiko pengendalian diatur terlalu tinggi, tes substantif dilakukan secara berlebihan, akibatnya audit menjadi tidak efisien.

C. PENAKSIRAN RISIKO PENGENDALIAN DALAM LINGKUNGAN TEKNOLOGI INFORMASI

Pengendalian pemrosesan informasi meliputi prosedur pengendalian umum dan prosedur pengen-dalian aplikasi. Selain itu, auditor harus memahami prosedur tindak lanjut manual untuk transaksi yang diidentifikasi oleh pengendalian aplikasi dan kemungkinan pengendalian pengguna langsung yang terkait dengan asersi. Prosedur tersebut diringkas pada Gambar 1.5. Paparan ini sangat membantu pemahaman tiga strategi audit penting untuk melakukan uji pengendalian jika sistem akuntansi dan pengendalian memanfaatkan teknologi informasi (TI) secara ekstensif.



Gambar 1.5. *Overview* dari Komputer Pengendalian

1. Strategi Pelaksanaan Uji Pengendalian

Ketika menaksir risiko pengendalian, auditor harus memilih di antara ketiga strategi di bawah ini.

a. Penaksiran pengendalian risiko berdasarkan pengendalian pengguna.
b. Perencanaan penaksiran risiko pengendalian level rendah berdasarkan pengendalian aplikasi.
c. Perencanaan penaksiran risiko pengendalian level tinggi berdasarkan pada pengendalian umum dan tindak lanjut manual.

a. Pengendalian Pengguna

Pada banyak kasus, klien dapat mendesain prosedur manual untuk menguji kelengkapan dan akurasi proses transaksi dengan komputer. Misalnya, manajer yang biasa mengotorisasi transaksi dapat memeriksa daftar pembelian yang dibebankan padanya. Atau seorang pengguna dalam sebuah departemen dapat membandingkan output yang dihasilkan komputer dengan dokumen sumber. Meskipun kedua pengendalian tersebut mendeteksi dan mengoreksi salah saji, pembandingan output dari komputer dengan dokumen sumber dilaksanakan dengan lebih detail sehingga dapat memberikan kepastian yang lebih tinggi bahwa salah saji dapat dideteksi dan dikoreksi. Jika terdapat pengendalian pengguna, auditor dapat menguji pengendalian secara langsung, seperti menguji pengendalian manusia yang lain. Pengujian ini disebut sebagai pengauditan di sekitar komputer. Keuntungan dari strategi uji pengendalian ini adalah tidak

membutuhkan pengujian program komputer yang rumit.

b. Pengendalian Aplikasi

Banyak auditor mengambil keuntungan dari pengendalian otomatis dan merencanakan strategi penaksiran risiko pengendalian berlevel rendah berdasarkan pada pengendalian aplikasi komputer. Untuk mengeksekusi strategi ini auditor harus:

1) menguji pengendalian aplikasi komputer;
2) menguji pengendalian umum komputer;
3) menguji tindak lanjut manual untuk pengecualian yang ditemukan oleh pengendalian aplikasi.

Efektivitas ketiga level pengendalian tersebut penting untuk penaksiran risiko pengendalian berlevel rendah. Pertama, auditor menguji pengendalian aplikasi komputer menggunakan beberapa teknik audit berbantuan komputer. Tujuannya adalah untuk menentukan apakah pengendalian aplikasi dengan tepat mengidentifikasi pengecualian. Kedua, pengendalian umum komputer juga harus diuji. Pengendalian umum memberikan kepastian bahwa pengendalian aplikasi didesain dan diuji dengan benar, dan setiap perubahan mendapatkan pengesahan. Pada hakikatnya, pengendalian umum memberikan peningkatan kepastian bahwa pengendalian aplikasi berfungsi secara konsisten dari waktu ke waktu. Bukti adanya pengendalian umum yang kuat memungkinkan auditor untuk menguji aplikasi pada suatu titik pada suatu waktu dan meyakini bahwa pengendalian aplikasi berfungsi dengan cara yang sama pada waktu-waktu lain selama periode pengauditan.

AU319.96 (PSA No. 69 paragraf 84 seksi 9b.) menyatakan bahwa auditor dapat menguji program komputer pada bagian tertentu pada suatu waktu untuk mendapatkan bukti bahwa program mengeksekusi pengendalian secara efektif. Untuk memperbaiki ketepatan waktu perolehan bukti, auditor selanjutnya melakukan uji pengendalian yang terkait dengan modifikasi dan penggunaannya sehingga program pengendali proses tersebut beroperasi secara konsisten (disebut pengujian pengendalian umum).

Akhirnya, auditor juga harus menguji efektivitas prosedur tindak lanjut manual. Sebagai contoh, anggaplah pengendalian aplikasi komputer dengan benar mengidentifikasi transaksi yang dicatat dengan jumlah yang salah dan melaporkan transaksi tersebut laporan pengecualian untuk tindak lanjut dan koreksi. Jika tindak lanjut manual tidak efektif dalam mengoreksi item-item pada laporan pengecualian, maka pengendalian aplikasi tidak efektif dalam mendeteksi dan mengoreksi kesalahan.

c. Pengendalian Umum dan Prosedur Tindak Lanjut Manual

Untuk beberapa asersi, auditor merencanakan strategi audit yang menekankan pengujian detail, dan menggunakan rencana penaksiran risiko pengendalian berlevel tinggi. AICPA Internal Pengendalian Audit Guide menyajikan strategi audit yang memungkinkan auditor untuk menyelesaikan tugas tersebut berdasarkan pada bukti efektivitas pengendalian umum dan prosedur tindak lanjut

manual. Ketika menguji pengendalian umum, auditor mempelajari efektivitas desain dan pengujian pengendalian aplikasi. Selain itu, auditor dapat menyimpulkan efektivitas pengendalian aplikasi setelah meneliti tingkat pengetahuan personil yang mengerjakan prosedur tindak lanjut manual. Sebagai contoh, personil yang menindaklanjuti pengecualian memahami aliran transaksi dengan detail yang memadai sehingga dapat mengantisipasi transaksi yang muncul pada laporan pengecualian. Jika transaksi muncul di laporan pengecualian, auditor dapat mengambil kesimpulan tentang program pengendali proses. Bukti tersebut sudah memadai untuk menaksir risiko pengendalian pada level tinggi, tetapi pada level moderat atau rendah auditor harus menguji program secara langsung dengan teknik audit berbantuan komputer.

2. Teknik Audit Berbantuan Komputer

Teknik audit berbantuan komputer meliputi penggunaan komputer secara langsung untuk menguji pengendalian aplikasi, yang disebut audit menggunakan komputer. Pengujian tersebut digunakan secara ekstensif pada pengujian rutin (rutin berisi bahasa program, secara teknis pemrograman disebut *listing*) validasi input dan program pengendali proses. Penggunaan komputer dalam uji pengendalian bermanfaat jika:

a. program komputer menjalankan peran pengendalian internal yang signifikan;
b. terdapat kesenjangan jejak audit yang signifikan;
c. terdapat volume pencatatan yang besar untuk diuji.

Menggunakan teknik audit berbantuan komputer membutuhkan tim audit yang memiliki keahlian dan pengetahuan komputer, dan mungkin juga menimbulkan gangguan operasi Teknologi Informasi (TI) klien ketika auditor menggunakan peralatan, program, dan file-file TI-nya. Akhirnya, teknik audit berbantuan komputer merupakan cara yang efektif dalam uji pengendalian aplikasi komputer. Auditor juga harus menguji efektivitas implementatif dari prosedur tindak lanjut manual menyimpulkan efektivitas aktivitas pengendalian secara keseluruhan.

Teknik audit berbantuan komputer yang tersedia untuk menguji implementasi pengendalian aplikasi terprogram tertentu meliputi: (1) simulasi paralel, (2) pengujian data, (3) fasilitas pengujian yang terintegrasi, dan (4) pengawasan berkelanjutan sistem on-line real-time.

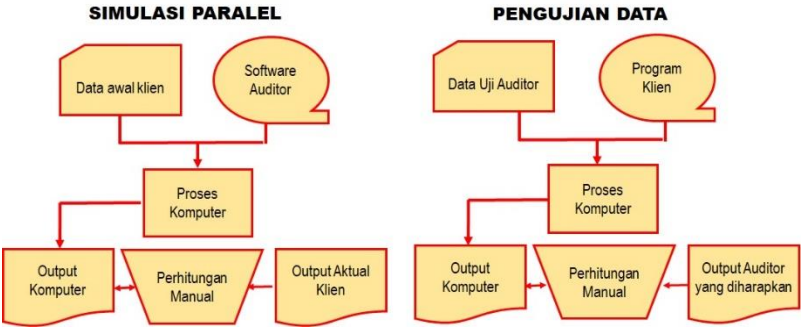
a. Simulasi paralel

Dalam simulasi paralel, data perusahaan aktual diproses ulang menggunakan program perangkat lunak milik auditor. Metode ini disebut demikian karena perangkat lunak didesain untuk mereproduksi atau meniru pemrosesan data klien yang aktual. Pendekatan ini diperlihatkan secara grafis pada bagian kiri Gambar 1.6.

Simulasi paralel dapat dikerjakan pada waktu yang berbeda sepanjang tahun dalam periode audit, dan dapat juga diterapkan pada proses ulang data historis. Pendekatan ini tidak mengontaminasi file klien, dan dapat dilakukan pada komputer yang terpisah.

Pendekatan ini memiliki keuntungan sebagai berikut.

1. Karena menggunakan data riil, auditor dapat memverifikasi transaksi dengan menelusuri transaksi tersebut ke dokumen sumber dan persetujuan.
2. Ukuran sampel dapat diperluas secara ekstensif dengan tambahan biaya yang relatif rendah.
3. Auditor dapat melakukan pengujian secara terpisah.



Gambar 1.6. Pendekatan Simulasi Paralel versus Pengujian Data

Jika auditor memutuskan untuk menggunakan simulasi paralel, data yang dipilih untuk simulasi haruslah representatif. Dimungkinkan juga sistem dari klien dapat melakukan operasi melebihi kapasitas perangkat lunak auditor.

b. Pengujian data

Dengan pendekatan pengujian data, transaksi buatan (*dummy*) disiapkan oleh auditor dan diproses

oleh program komputer klien dengan pengendalian oleh auditor. Pengujian data terdiri dari satu transaksi pada kondisi valid dan tidak valid. Pengujian data untuk penggajian termasuk juga kondisi pembayaran lembur yang valid dan tidak valid. Output proses pengujian data kemudian dibandingkan dengan output auditor yang diharapkan untuk menentukan pengendalian bekerja secara efektif. Pendekatan pengujian ini relatif sederhana, cepat, dan murah. Tabel keputusan yang digunakan untuk mendokumentasi pengendalian terprogram sangat bermanfaat dalam identifikasi kondisi yang diuji. Meskipun demikian, metode ini memiliki kekurangan sebagai berikut.

1) Program klien diuji hanya pada satu titik waktu tertentu, bukannya selama periode audit.
2) Metode ini hanya menguji keberadaan dan fungsi pengendalian pada program yang diuji.
3) Tidak ada dokumentasi pengujian yang diproses oleh sistem.
4) Operator komputer mengetahui adanya pengujian data, sehingga dapat menurunkan validitas output.
5) Luasan pengujian terbatas pada imajinasi auditor dan pengetahuan tentang pengendalian dalam aplikasi.

c. Fasilitas pengujian terintegrasi

Pendekatan fasilitas pengujian terintegrasi membutuhkan subsistem kecil (miniatur perusahaan) di dalam sistem TI reguler. Hal ini dapat dilakukan dengan membuat file-file master dummy

atau menambahkan master pencatatan dummy pada file-file klien. Data uji, khususnya yang di kode sesuai dengan file-file master dummy, dimasukkan ke dalam sistem bersama dengan transaksi aktual. Data uji harus meliputi semua jenis error/kesalahan dan pengecualian transaksi yang mungkin ditemukan. Dengan cara ini, data uji diperlakukan dengan pengendalian terprogram yang sama layaknya data aktual. Untuk subsistem, atau file-file dummy, dihasilkan sejumlah output terpisah yang kemudian dibandingkan dengan output auditor yang diharapkan.

Metode fasilitas pengujian yang terintegrasi memiliki kerugian karena risiko error pada data klien. Di samping itu, kemungkinan dibutuhkan modifikasi agar program klien dapat mengakomodasi data dummy. Proses pembalikan juga diperlukan untuk setiap transaksi uji yang dimasukkan ke dalam pencatatan akuntansi klien.

d. Pengawasan berkelanjutan pada sistem On-Line Real-Time (OLRT)

Pengujian data dapat digunakan untuk uji pengendalian dalam sistem entri on-line/proses on-line yang disebut sistem on-line real time (OLRT). Pendekatan ini tidak banyak digunakan oleh auditor karena masalah kontaminasi file data dan kesulitan pembalikan data hipotetis. Simulasi paralel dapat digunakan, akan tetapi ketersediaan perangkat lunak auditor yang dapat digunakan untuk meniru proses OLRT sangat terbatas. Sebagai pengganti pengujian tradisional, auditor menyusun untuk pengawasan

berkelanjutan pada sistem. Dengan teknik ini, rutin (rutin berisi kode bahasa program, secara teknis *programming* disebut *listing*) audit ditambahkan pada program pemrosesan klien. Transaksi yang masuk ke dalam sistem dengan di sampling dengan interval acak, dan output dari rutin tersebut digunakan untuk uji pengendalian. Untuk memungkinkan integrasi perangkat lunak audit ke dalam sistem proses OLRT, kemampuan pengait audit harus dibangun ke dalam program komputer client—baik sistem operasi maupun program aplikasi—pada saat sistem OLRT dibuat. Pengait audit merupakan titik pada program yang memungkinkan modul atau program audit untuk diintegrasikan ke dalam sistem operasi normal. Modul audit tersebut memberikan alat bagi auditor untuk memilih transaksi dengan karakteristik yang diinginkan, misalnya jenis transaksi tertentu atau sejumlah transaksi dengan nilai yang lebih besar atau lebih kecil dari nilai tertentu. Setelah transaksi tertentu diidentifikasi, data transaksi tersebut ditandai dengan beberapa metode. Dua dari metode tersebut adalah penandaan transaksi dan catatan audit.

1) Penandaan Transaksi

Metode penandaan transaksi meliputi penempatan indikator, atau tanda, pada transaksi tertentu. Penandaan transaksi tersebut memungkinkan penelusuran transaksi melalui sistem yang memprosesnya. Sistem harus diprogram untuk menyediakan cetakan hardcopy seluruh jalur yang diikuti transaksi. Pada jalur tertentu, dapat

diperoleh juga data yang berinteraksi dengan transaksi yang telah ditandai.

2) Catatan Audit

Catatan audit, kadang disebut sistem pengendalian audit review files (SCARF—file catatan audit pengendalian sistem) adalah catatan aktivitas pemrosesan tertentu. Catatan tersebut digunakan untuk mencatat semua keterjadian yang memenuhi kriteria yang dibuat oleh auditor yang terjadi pada titik tertentu dalam sistem. Transaksi atau keterjadian yang teridentifikasi ditulis ke dalam file yang hanya bisa diakses oleh auditor. Auditor kemudian dapat mencetak atau menggunakan teknik lain untuk menganalisis file tersebut dan melakukan pengujian lebih lanjut jika diperlukan.

3. Penaksiran Pengendalian Teknologi Informasi

Proses penaksiran risiko pengendalian adalah sama baik klien menggunakan pengendalian manual, maupun pengendalian yang memanfaatkan teknologi informasi, atau keduanya. Jadi, proses penaksiran risiko pengendalian meliputi (1) mempertimbangkan pengetahuan yang diperoleh dari prosedur untuk mendapatkan pemahaman, (2) mengidentifikasi potensi salah saji yang mungkin terjadi pada asersi, (3) mengidentifikasi pengendalian yang dibutuhkan untuk mencegah atau mendeteksi dan mengoreksi salah saji, (4) melakukan uji pengendalian, dan (5) mengevaluasi bukti dan menaksir risiko pengendalian.

Auditor harus mengidentifikasi potensi salah saji yang relevan terhadap asersi tertentu, kemudian

mengidentifikasi kemungkinan pengendalian (termasuk pengendalian aplikasi) yang ada, dan akhirnya merancang uji pengendalian yang tepat. Uji pengendalian dilakukan untuk mendapatkan bukti efektivitas dari desain atau implementasi pengendalian. Auditor melakukan pengujian demikian jika terdapat alasan bahwa bukti tersebut memungkinkan penurunan level risiko pengendalian tertaksir. Pengujian pengendalian aplikasi komputer meliputi beberapa teknik audit berbantuan komputer dan pengujian prosedur tindak lanjut manual.

Dalam sistem terkomputerisasi, pengendalian dapat atau tidak dapat menghasilkan bukti yang nyata. Jika komputer menghasilkan bukti nyata untuk memverifikasi bahwa prosedur diimplementasikan dan untuk mengevaluasi kepatutan kinerja, uji pengendalian TI dapat meliputi inspeksi dokumen. Namun demikian, jika bukti tersebut tidak dihasilkan oleh komputer, uji pengendalian harus meliputi teknik audit berbantuan komputer sebagaimana telah dibahas sebelumnya.

Tabel 1.1. Pertimbangan Penaksiran Risiko Pengendalian untuk Pengendalian Umum Komputer

Potensi Salah Saji	Pengendalian yang Diperlukan	Uji Pengendalian
Pengendalian Organisasional dan Operasional		
Operator komputer dapat mengubah program sehingga meloncati	Pemisahan tugas dalam TI atas pemrograman dan operasi komputer	Pengamatan pemisahan tugas dala TI

pengendalian tertrogram		
Personel TI dapat memulai dan memproses yang tidak sah	Pemisahan tugas antara departemen pengguna dan TI untuk memulai dan memproses transaksi	Pengamatan pemisahan tugas antara departemen pengguna dan pengolahan data elektronik
Pengendalian Pengembangan Sistem dan Dokumentasi		
Rancangan sistem tidak memenuhi kebutuhan departemen pengguna atau auditor. Perubahan system yang tidak terotorisasi mengakibatkan errors program yang tidak terantisipasi	Partisipasi personel dari departemen pengguna dan auditor internal dalam design dan persetujuan system baru. Verifikasi internal atas proses otorisasi, pengujian dan dokumentasi perubahan system sebelum implementasi.	Pemeriksaan pihak-pihak yang berpatisipasi dalam design system baru, pemeriksaan bukti persetujuan system baru. Pemeriksaan bukti verifikasi internal, penelusuran perubahan program tertentu dengan dokumen pendukung.
Pengendalian Perangkat Keras dan Sistem		
Malfungsi perlengkapan yang mengakibatkan pemrosesan	Pengendalian perangkat keras perangkat lunak di dalam sistem untuk mendeteksi perangkat lunak multifungsi	Pemeriksaan spesifikasi perangkat keras dan perangkat lunak
Perubahan sistem perangkat	Persetujuan dan dokumentasi semua	Pemeriksaan bukti

lunak yang tidak terotorisasi mengakibatkan eror perangkat lunak	perubahan perangkat lunak	persetujuan dan dokumentasi perubahan
Pengendalian Akses		
Pengguna yang tidak terotorisasi dapat mengakses perlengkapan TI	Pembangunan fasilitas fisik pengemanaan TI; laporan manajerial tentang pemakaian perlengkapan	Pemeriksaan pengaturan keamanan dan laporan pemakaian pemakaian perlengkapan
File data dan program dapat diproses atau diubah oleh pengguna yang tidak terotorisasi	Penggunaan *library*, *librarian* dan catatan untuk membatasi akses dan memonitor pemakaian	Pemeriksaan fasilitas dan catatan
Pengendalian Data dan Prosedural		
Eror terjadi pada saat *input atau pemrosesan data atau pendistribusian output*	Penggunaan kelompok pengendali data yang bertanggung jawab atas penjagaan pengendalian input, pemrosesan dan output data	Pengamatan terhadap kelompok pengendali data
Keberlanjutan operasi terganggu karena bencana alam, misalnya kebakaran atau banjir	Perencanaan kontingensi meliputi pembangunan fasilitas cadangan yang terpisah	Pemeriksaan perencanaan kontingensi

File data atau program rusak atau hilang	Penyimpanan *file* dan program cadangan yang terpisah, pembuatan rekontruksi file data	Pemeriksaan fasilitas penyimpanan, pemeriksaan kemampuan rekontruksi file

Tabel 1.2. Pertimbangan Penaksiran Risiko Pengendalian untuk Pengendalian Aplikasi Komputer

Potensi Salah Saji	**Pengendalian yang Diperlukan**	**Uji Pengendalian**
Pengendalian *Input*		
Data dari transaksi yang tidak terotorisasi dapat disbmisi untuk pemrosesan	Otorisasi dan persetujuan data di departemen pengguna, pengedalian aplikasi untuk membandingkan data dengan otorisasi	Pemeriksaan dokumen sumber dan batch transmisi untuk bukti persetujuan, uji pengendalian aplikasi dengan teknik audit berbantuan komputer dan uji tindak lanjut.
Data valid tidak menjadi bentuk yang dapat diakomodir oleh mesin dengan benar	Verifikasi (pengetikan ulang); penyuntingan rutin (kode bahasa program), kontrol total	Pengamatan prosedur verifikasi data; penggunaan teknik audit berbantuan komputer untuk dengan benar menguji rutin dan uji tindak lanjut manual, pemeriksaan

		rokonsilasi control total.
Error pada dokumen sumber tidak terkoreksi disubmisi kembali	Pembuatan catatan *error*; dikembalikan ke departemen pengguna untuk koreksi, tindak lanjut manual	Pemeriksaan catatan *error* dan bukti tindak lanjut
Pengendalian Pemrosesan		
File-file yang diproses dan di-update salah	Penggunaan label file eksternal dan internal	Pengamatan penggunaan label file, pemeriksaan dokumentasi label file internal
Data hilang, tertambahi, terduplikasi atau terubah selama pemrosesan	Penggunaan control total, pemeriksaan pembatasan dan kewajaran, dan uji urutan	Pemeriksaan bukti rekonsilisasi control total, penggunaan teknik audit berbantuan komputer untuk pemeriksaan komputer dan uji tindak lanjut manual
Pengendalian *Output*		
Output tidak benar	Rekonsilisasi total dengan control data atau departemen pengguna	Pemeriksaan bukti rekonsilisasi
Output terdistribusi kepada personel yang tidak terotisasi	Penggunaan lembaran control distribusi laporan, monitor kelompok data control	Pemeriksaan lembaran control distribusi laporan, pengamatan

		kelompok data kontrol

Tabel 1.3. Rangkuman Pengetahuan Auditor

No.	Pengetahuan Auditor	Rangkuman
1	Memahami langkah-langkah menaksir risiko pengendalian	Langkah-langkah penaksiran risiko pengendalian meliputi: 1) mempertimbangkan pengetahuan yang diperoleh dari prosedur untuk apakah pengendalian terkait dengan asersi telah dirancang dan diimplementasikan oleh manajemen, 2) mengidentifikasi kemungkinan salah saji yang mungkin terjadi pada asersi, 3) mengidentifikasi pengendalian yang diperlukan untuk mencegah atau mendeteksi dan mengoreksi salah saji tersebut, 4) melakukan uji pengendalian terhadap pengendalian yang diperlukan untuk menentukan efektivitas rancangan dan implementasinya, dan 5) mengevaluasi bukti dan menaksir risiko.
2	Memahami perbedaan penaksiran risiko pengendalian dengan dua strategi audit	Paparan 11-8 menggambarkan perbedaan antara dua strategi audit utama. Jika auditor merencanakan pendekatan substantif utama pada asersi, maka pengetahuan tentang efektivitas pengendalian internal harus diperoleh bersamaan dengan

	pendahuluan utama	pemahaman pengendalian internal, dan melanjutkan dengan uji substantif yang tepat yang mengurangi risiko deteksi pada level rendah. Jika auditor mengikuti pendekatan risiko pengendalian tertaksir berlevel rendah, maka harus digunakan uji pengendalian yang lebih ekstensif yang memungkinkan modifikasi karakteristik, pemilihan waktu, atau luasan rencana uji substantif.

1.2. PENGARUH STRATEGI AUDIT AWAL

Tanpa memandang strategi audit pendahuluan yang dipilih untuk bagian audit tertentu, auditor harus mengidentifikasi jenis potensi salah saji pada asersi. Namun demikian, cara bagaimana auditor mempertimbangkan faktor yang mempengaruhi risiko salah saji dan menaksir risiko dapat bervariasi sesuai dengan strategi audit yang dipilih. Tabel 1.1, Tabel 1.2 dan Tabel 1.3 menyoroti perbedaan dua pendekatan untuk memenuhi standar pekerjaan lapangan kedua.

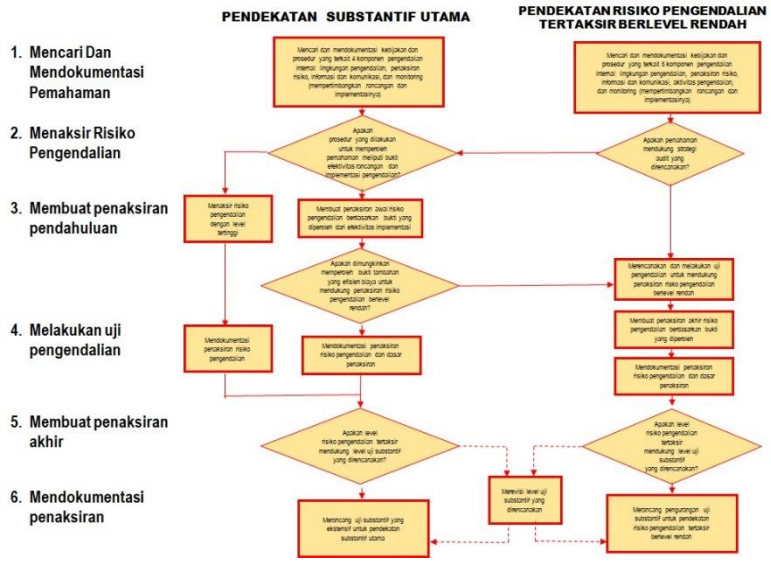
A. PENDEKATAN SUBSTANTIF UTAMA

Pemilihan pendekatan substantif utama memerlukan pengetahuan yang cukup tentang sistem pengendalian internal untuk memahami potensi penyebab salah saji dan bagaimana salah saji tersebut dapat dikontrol atau tidak. Selain itu, pada lingkungan TI yang intensif, auditor tidak perlu mengikuti pendekatan substantif utama karena uji substantif tidak mengurangi risiko audit ke level rendah.

Sejumlah perbedaan tercatat pada Paparan 1-8 yang berlabel Penaksiran Risiko Pengendalian. Pertama, salah satu komponen pendekatan substantif utama adalah level risiko pengendalian tertaksir pada level tinggi. Pernyataan ini didasarkan pada asumsi bahwa:

1. Tidak ada pengendalian internal yang signifikan terkait dengan asersi.
2. Pengendalian internal yang relevan kemungkinan tidak efektif.
3. Perolehan bukti efektivitas pengendalian internal yang relevan tidak efisien.

Jalur keputusan pada kolom Pendekatan Substantif Utama Gambar 1.7 memungkinkan untuk meneruskan, atau mengubah menjadi asumsi tersebut. Pada simbol keputusan pertama tertulis pertanyaan apakah bukti efektivitas desain dan implementasi pengendalian internal didapatkan ketika pemahaman pengendalian internal. Contoh uji pengendalian bersamaan adalah tinjauan ulang menyeluruh transaksi yang auditor menelusuri transaksi yang representatif dari kelas transaksi melalui seluruh langkah untuk mengonfirmasi pemahaman yang didapatkan dari kuesioner atau bagan alir. Jika bukti efektivitas desain dan implementasi pengendalian internal untuk asersi tidak diperoleh ketika pemahaman, auditor harus menaksir risiko pengendalian pada level maksimal dan mendokumentasikan kesimpulan tersebut pada kertas kerja. Jika didapatkan sedikit bukti, auditor dapat membuat penaksiran awal risiko pengendalian sedikit di bawah level maksimal atau tinggi. Pada kasus tersebut, auditor dianjurkan untuk mengubah strategi audit menjadi pendekatan risiko pengendalian tertaksir berlevel rendah.



Gambar 1.7. Pendekatan Simulasi Paralel versus Pengujian Data

Keputusan perubahan strategi audit harus mempertimbangkan kemungkinan mendapatkan bukti yang efisien secara kos untuk mendukung penaksiran risiko pengendalian dengan level yang lebih rendah. Agar kos efisien, kos gabungan untuk melakukan (1) uji pengendalian tambahan, (2) penurunan uji substantif dengan asumsi penaksiran risiko pengendalian berlevel lebih rendah terdukung harus lebih rendah ketimbang kos untuk mengerjakan level uji substantif yang lebih tinggi sesuai dengan pendekatan substantif utama. Hal ini digambarkan pada simbol keputusan kedua pada kolom Pendekatan Substantif Utama yang cabang Ya (garis putus-

putus ke kanan dari simbol tersebut) mewakili perubahan strategi ke pendekatan risiko pengendalian tertaksir berlevel rendah. Jika diputuskan tidak mengubah strategi, penaksiran risiko pengendalian sedikit di bawah level maksimal atau tinggi, dan dasar penaksiran tersebut, harus didokumentasi.

Simbol keputusan terakhir pada kolom Pendekatan Substantif Utama mensyaratkan auditor untuk mempertimbangkan apakah level risiko pengendalian tertaksir aktual mendukung level uji substantif yang direncanakan. Misalnya, auditor semula merencanakan risiko pengendalian pada level maksimal, sehingga direncanakan uji substantif pada level tertinggi. Tetapi jika didapatkan bukti ketika melakukan pemahaman yang mendukung penaksiran risiko pengendalian pada level tinggi, revisi perencanaan level uji substantif menjadi level yang lebih rendah sudah tepat. Auditor kemudian meneruskan dengan level uji substantif yang tepat.

B. RISIKO PENGENDALIAN TERTAKSIR BERLEVEL RENDAH

Pada beberapa kasus digunakan pendekatan risiko pengendalian tertaksir berlevel rendah karena klien memiliki pengendalian internal yang efektif dan auditor merencanakan untuk menguji pengendalian tersebut, mengurangi risiko pengendalian, dan mengubah karakteristik, pemilihan waktu, atau luasan uji substantif. Kasus tersebut sering terjadi pada perusahaan publik. Pendekatan risiko pengendalian tertaksir berlevel rendah dipilih karena uji substantif sendiri tidak cukup untuk mengurangi risiko audit ke level rendah.

Pemahaman dan dokumentasi pengendalian internal yang lebih luas, khususnya komponen aktivitas pengendalian, biasanya cukup untuk mendukung pendekatan risiko pengendalian tertaksir berlevel rendah. Jika menggunakan sistem tinjau ulang menyeluruh ditemukan bukti pengendalian yang tidak efektif, perlu dilakukan perubahan strategi menjadi pendekatan substantif utama. Pada Gambar 1.7, perubahan strategi tersebut ditunjukkan pada cabang Tidak dari bagian kiri simbol keputusan pertama pada kolom Pendekatan Risiko Pengendalian Terakhir Berlevel Rendah.

Jika pengalihan menjadi risiko pengendalian tertaksir berlevel rendah diteruskan, maka auditor merencanakan dan melakukan uji pengendalian tambahan. Bukti yang didapatkan dari uji tersebut dievaluasi untuk membuat penaksiran risiko pengendalian akhir atau aktual. Penaksiran akhir tersebut dan dasar penaksirannya didokumentasikan di kertas kerja. Simbol keputusan terakhir pada kolom Pendekatan Risiko Pengendalian Terakhir Berlevel Rendah di Gambar 1.7 mengharuskan auditor untuk mempertimbangkan apakah penaksiran risiko pengendalian aktual mendukung rencana level uji substantif, dan jika tidak, rencana uji substantif harus direvisi. Misalnya, auditor semula merencanakan risiko pengendalian tertaksir berlevel rendah sehingga menggunakan level uji substantif yang paling rendah. Tetapi jika uji pengendalian membuktikan pengendalian yang tidak efektif (risiko pengendalian ditaksir pada level tinggi atau maksimum), auditor harus merevisi level uji substantif yang direncanakan sesuai dengan perubahan menjadi pendekatan substantif utama. Keterjadian ini disajikan dengan garis putus-putus yang melengkung ke

arah bawah menuju bagian kiri kotak revisi level uji substantif di bagian dasar Gambar 1.7. Pada kedua kasus, Gambar 1.7 menggambarkan proses audit yang berkarakteristik berulang, dan langkah terakhirnya adalah mendesain uji substantif yang tepat untuk setiap situasi.

C. MENDESAIN UJI PENGENDALIAN

Tujuan penaksiran risiko pengendalian adalah untuk membantu auditor membuat keputusan tentang risiko salah saji yang material dalam asersi laporan keuangan. Untuk menyelesaikan tugas tersebut auditor harus mengevaluasi efektivitas desain dan implementasi pengendalian yang relevan.

Uji pengendalian yang didesain untuk mengevaluasi efektivitas implementasi pengendalian memperhatikan (1) bagaimana pengendalian diaplikasikan, (2) konsistensi aplikasi sepanjang periode, dan (3) diaplikasikan oleh siapa. Kepastian yang didapat dari uji pengendalian dipengaruhi oleh karakteristik, pemilihan waktu, dan luasan uji pengendalian.

1. Karakteristik Uji Pengendalian

Karakteristik uji pengendalian berkaitan dengan jenis bukti yang didapatkan. Uji pengendalian biasanya meliputi:

a. penyelidikan personel yang berwenang;
b. inspeksi dokumen, laporan, atau file elektronik, yang menunjukkan kinerja pengendalian;
c. pengamatan aplikasi pengendalian;
d. pengulangan aplikasi pengendalian oleh auditor, termasuk penggunaan teknik audit berbantuan komputer.

Semakin besar kepastian yang diinginkan dari uji pengendalian, semakin tinggi reliabilitas bukti yang dibutuhkan. Auditor sering menggabungkan jenis uji pengendalian tersebut di atas untuk mendapatkan bukti tentang desain dan implementasi pengendalian yang efektif.

Penyelidikan didesain untuk menilai (1) pemahaman pekerja tentang pengendalian komputer, (2) pemahaman pekerja tentang tugasnya, (3) kinerja setiap individu terhadap tugas tersebut, dan (4) frekuensi, penyebab, dan disposisi penyimpangan. Contohnya, pekerja-pekerja yang sering bekerja dengan transaksi dapat mengetahui transaksi yang seharusnya muncul di laporan pengecualian. Penyelidikan pekerja dapat membantu auditor memahami keahlian dan kemampuan pekerja dalam melaksanakan pengendalian, demikian juga dengan pengetahuan pekerja tentang pengendalian komputer dan tujuan tindak lanjut (follow-up) manual. Penyelidikan dapat juga mengungkap informasi tentang transaksi yang harus tampil di laporan pengecualian, misalnya laporan barang yang telah dipesan tetapi belum dikirimkan, dan transaksi yang seharusnya muncul di laporan tetapi tidak muncul. Auditor juga harus mempertimbangkan bahwa jawaban seorang pekerja yang tidak memuaskan mengindikasikan aplikasi pengendalian yang tidak tepat. Namun demikian, penyelidikan sendiri tidak menyediakan bukti yang memadai dan kuat untuk memungkinkan perkiraan risiko pengendalian di bawah maksimal. Penyelidikan harus dilengkapi dengan pengamatan, pemeriksaan dokumen, atau pengulangan pengendalian. Idealnya, pengamatan harus dikerjakan

tanpa sepengetahuan pekerja atau secara mendadak. Penyelidikan dan pengamatan sangat berguna untuk mendapatkan bukti tentang ketepatan pemisahan tugas. Kendala observasi terletak pada masalah waktu.

Pemeriksaan dokumen dan catatan dapat diterapkan jika terdapat jejak kinerja transaksi dalam bentuk catatan laporan pengecualian, tanda tangan, atau cap validasi yang mengindikasi bahwa pengendalian telah dilakukan dan pelakunya teridentifikasi. Misalnya, auditor dapat menginspeksi catatan pada laporan pengecualian atau catatan manajemen yang meninjau transaksi bisnis. Inspeksi catatan dapat memberikan bukti yang handal tentang tindakan pekerja atau manajemen. Namun demikian, tanda tangan pada dokumen yang menunjukkan persetujuan penanda tangan tidak selalu berarti bahwa penanda tangan telah memeriksa dokumen tersebut dengan seksama sebelum membubuhkan tanda tangan. Oleh karena itu, auditor biasanya meniru langkah pengendalian yang telah diimplementasikan untuk melakukan evaluasi secara seksama.

Dalam menirukan langkah pengendalian, auditor melakukan prosedur yang sama seperti yang telah diimplementasikan. Misalnya, jika manajer mereview transaksi penjualan mingguan untuk memastikan bahwa transaksi tersebut dibuat setelah analisis risiko kredit yang tepat, auditor harus mereview daftar yang ditandatangani oleh manajer dan mengevaluasi apakah tiap pelanggan memenuhi kriteria kredit perusahaan. Jika seorang pekerja melakukan prosedur tindak lanjut pada cek yang melebihi batas mesin penanda cek, auditor perlu mereview daftar pengecualian dan

memastikan disposisi selanjutnya atas item-item pada laporan pengecualian tersebut. Jika tindak lanjut manual tidak konsisten dengan kebijakan perusahaan, maka auditor harus menyimpulkan bahwa telah didapatkan bukti ketidakefektifan pengendalian. Auditor selanjutnya perlu mempertimbangkan kemungkinan salah saji yang material dalam insersi disebabkan kelemahan tersebut.

Karakteristik pengendalian mempengaruhi jenis prosedur audit yang dilakukan. Contohnya, ketika menguji prosedur tindak lanjut manual, auditor perlu mengevaluasi akurasi laporan (sering diuji baik dengan pengendalian umum komputer maupun pengendalian terprogram terhadap akurasi laporan) dan efektivitas prosedur tindak lanjut. Pengujian pengendalian atas sebuah estimasi akuntansi meliputi pengujian akurasi data yang digunakan untuk estimasi tersebut dan pengendalian manual atas reliabilitas dan konsistensi proses estimasi.

Akhirnya, tidak ditemukannya bukti salah saji membuktikan pengendalian yang efektif. Namun demikian, jika ditemukan salah saji selama audit, auditor harus mempertimbangkan salah saji tersebut ketika mengevaluasi efektivitas pengendalian internal.

2. Pemilihan Waktu Uji Pengendalian

Pemilihan waktu uji pengendalian menentukan periode yang tepat untuk uji pengendalian. Jika auditor menguji pengendalian hanya pada titik waktu tertentu, maka auditor hanya mendapatkan bukti pengendalian berlangsung efektif pada titik waktu tersebut. Jika auditor menguji pengendalian sepanjang periode, maka

auditor mendapatkan bukti efektivitas selama periode tersebut.

Sebagai contoh, observasi hanya memungkinkan pada titik waktu tertentu. Oleh karena itu, hal tersebut tidak cukup untuk mengevaluasi efektivitas untuk periode yang tidak diuji. Penggunaan teknik audit berbantuan komputer, seperti pengujian data, menyediakan kesimpulan tentang program komputer hanya pada satu titik waktu. Untuk meningkatkan ketepatan waktu perolehan bukti, auditor menggunakan pengujian pengendalian umum komputer melalui modifikasi dan penggunaan program komputer tersebut selama periode audit untuk mendapatkan bukti apakah pengendalian terprogram beroperasi secara konsisten selama periode audit. Kombinasi bukti tentang pengendalian umum komputer yang efektif memungkinkan auditor memperluas kesimpulan tentang pengendalian aplikasi bukan saja ketika aplikasi komputer diuji secara langsung.

Ketika mendapatkan bukti tentang rancangan atau implementasi pengendalian selama sebuah periode interim, auditor harus menentukan apakah bukti tambahan harus didapatkan selama periode yang tersisa. Auditor harus mempertimbangkan faktor-faktor berikut ketika mempertimbangkan bukti yang perlu didapat selama periode yang tersisa:

a. Signifikansi asersi yang diuji;
b. Pengendalian spesifik yang dievaluasi selama periode interim;
c. Derajat efektivitas desain dan implementasi pengendalian yang dievaluasi;

d. Hasil uji pengendalian yang digunakan untuk membuat evaluasi;
e. Panjang periode yang tersisa;
f. Bukti tentang desain dan implementasi dari pengujian pengendalian monitoring pihak klien dan uji substantif pada periode yang tersisa.

Selain itu, auditor harus mendapatkan bukti tentang karakteristik dan luas perubahan yang material dalam pengendalian internal, termasuk kebijakan, prosedur, dan personel yang terjadi setelah periode interim. Sebagai contoh, anggaplah auditor melakukan uji pengendalian tentang keberadaan dan keterjadian dan penilaian pencatatan penjualan (dan piutang), menaksir risiko pengendalian yang rendah, dan merencanakan mengerjakan uji substantif dengan mengirim konfirmasi beberapa bulan sebelum akhir tahun.

Sebelum mengirim konfirmasi, juga pada akhir tahun, auditor harus meng-update kesimpulan taksiran risiko pengendalian yang rendah. Jika prosedur pengendalian yang relevan adalah prosedur pengendalian terprogram, auditor menyelidiki perubahan program dan perubahan dalam prosedur tindak lanjut manual. Jika terdapat perubahan personel TI yang signifikan, auditor perlu melakukan pengujian tambahan atas pengendalian umum komputer dan mempertimbangkan perlunya pengujian tambahan pada aplikasi komputer. Jika terdapat perubahan pada personel yang melakukan prosedur tindak lanjut manual, auditor perlu melakukan pengujian tambahan atas aktivitas tindak lanjut manual pada item-item yang muncul pada laporan pengecualian.

Tujuannya adalah untuk menentukan apakah kesimpulan tentang uji pengendalian masih valid, sebelum melakukan uji substantif.

1.3. PEMILIHAN WAKTU UJI PENGENDALIAN

Periode waktu yang auditor melakukan uji pengendalian bervariasi sesuai dengan karakteristik pengendalian yang diuji dan frekuensi langkah pengendalian spesifik. Beberapa pengendalian berlangsung secara terus-menerus (contohnya pengendalian penjualan). Pengendalian yang lain dilakukan hanya pada waktu tertentu (misalnya pengendalian penghitungan fisik sediaan atau pengendalian pembuatan laporan keuangan).

Ketika melaporkan efektivitas pengendalian—per|| tanggal tertentu dan mendapatkan bukti efektivitas pengendalian yang berlaku pada tanggal interim, auditor harus menentukan apakah bukti tambahan harus didapatkan pada sisa periode. Untuk memutuskan hal tersebut, auditor harus mengevaluasi:

- uji pengendalian spesifik sebelum tanggal—per|| dan hasilnya;
- derajat bukti efektivitas pengendalian yang didapatkan;
- panjang sisa periode;
- kemungkinan perubahan yang signifikan pada pengendalian internal atas pelaporan keuangan setelah tanggal interim.

Terhadap pengendalian atas transaksi nonrutin yang material, pengendalian atas rekening atau proses dengan subjektivitas atau penilaian pengukuran yang

tinggi, atau pengendalian atas pencatatan penyesuaian akhir periode, auditor harus melakukan uji pengendalian pada saat yang lebih dekat dengan tanggal —per||, atau melakukan uji pengendalian pada tanggal —per||.

Perlunya auditor mempertimbangkan bukti selama periode audit sebelumnya dalam menaksir risiko pengendalian pada periode audit yang berjalan masih menjadi kontroversi. Jumlah aplikasi komputer bisa sangat besar sehingga auditor dapat merotasi uji pengendalian aplikasi tertentu. Standar audit memperbolehkan auditor merotasi uji pengendalian untuk perusahaan privat yang pengendaliannya diuji sedikitnya setiap tiga tahun.

Namun demikian, pengendalian terhadap risiko inheren yang material harus diuji selama periode audit berjalan. Selanjutnya rotasi uji pengendalian dari tahun ke tahun menjadi tidak tepat jika auditor menerbitkan opini atas pengendalian internal.

Penggunaan bukti yang diperoleh dari periode audit sebelumnya mengharuskan auditor mendapatkan bukti perubahan yang telah dilakukan sejak uji pengendalian terakhir. Auditor menggunakan kombinasi penyelidikan, observasi, dan inspeksi untuk memastikan pemahaman efektivitas desain pengendalian dan untuk memverifikasi bahwa pengendalian tersebut masih diimplementasikan. Misalnya, pada pengendalian otomatis, auditor perlu menyelidiki dan menginspeksi catatan perubahan pengendalian terprogram. Jika pengendalian telah berubah setelah diuji pada periode sebelumnya, bukti yang dikumpulkan sesudahnya menjadi tidak relevan lagi.

1. Luasan Uji Pengendalian

Secara umum, semakin rendah level taksiran risiko pengendalian, semakin luas luasan uji pengendalian. Pada kasus audit pengendalian internal atas pelaporan keuangan, auditor harus mendapatkan bukti efektivitas pengendalian atas asersi seluruh rekening dan pengungkapan dalam laporan keuangan yang material dan relevan.

Dalam penaksiran luasan uji pengendalian, auditor harus mempertimbangkan faktor-faktor di bawah ini.

a). Karakteristik pengendalian. Pengendalian manual memerlukan pengujian yang lebih ekstensif daripada pengendalian otomatis. Satu uji untuk setiap kondisi pengendalian terprogram sudah cukup untuk mendapatkan kepastian berlevel tinggi jika pengendalian umum berjalan efektif. Secara umum, semakin tinggi derajat kompleksitas dan level penilaian pada pengendalian aplikasi, diperlukan pengujian yang semakin luas. Semakin rendah level kompetensi pelaku pengendalian, maka semakin luas pengujian yang diperlukan.

b). Frekuensi langkah pengendalian. Secara umum, semakin sering langkah pengendalian manual, semakin banyak langkah pengendalian yang harus diuji. Semakin jarang langkah pengendalian, misalnya rekening rekonsiliasi bulanan, semakin sedikit pengujian yang diperlukan dari pada langkah pengendalian yang terjadi setiap hari atau setiap transaksi.

c). Pentingnya pengendalian. Pengendalian yang lebih penting harus diuji lebih ekstensif. Beberapa

pengendalian seperti lingkungan pengendalian atau pengendalian umum komputer memiliki imbas yang menyeluruh pada pengendalian lainnya. Semakin rendah level taksiran risiko pengendalian pada pengendalian tersebut, semakin ekstensif pengujian yang dibutuhkan.

Faktor-faktor yang mempengaruhi ukuran sampel uji pengendalian didiskusikan secara lebih mendalam di bab berikutnya.

2. Pemilihan Staf Uji Pengendalian

Keputusan final audit mempengaruhi pemilihan staf uji pengendalian, atau siapa yang harus mengerjakan uji pengendalian. Contohnya, tim audit biasanya memasukkan ahli audit komputer untuk mengevaluasi prosedur pengendalian umum komputer dan untuk mengerjakan teknik audit berbantuan komputer. Jika klien mendesain pengendalian untuk mengendalikan risiko bisnis tertentu, seperti risiko salah penagihan, auditor memerlukan staf yang memahami regulasi pemerintah untuk melakukan uji pengendalian tersebut. Pada banyak kasus, staf akuntan bagian jurnal dapat ditugaskan untuk mengerjakan uji pengendalian atas transaksi rutin seperti penjualan, pengeluaran, dan penggajian.

3. Program Audit untuk Tes Pengendalian

Keputusan auditor tentang karakteristik, luasan, dan pemilihan waktu uji pengendalian terus hingga manajemen staf harus di dokumentasi dalam program audit dan kertas kerja terkait. Sebuah contoh program audit untuk uji pengendalian transaksi pengeluaran

kas disajikan pada Paparan 1-9. Perhatikan bahwa program tersebut mencantumkan daftar prosedur yang digunakan untuk pengujian yang terkait dengan asersi tersebut dan mempunyai kolom yang mengindikasi (1) referensi silang untuk kertas kerja yang mendokumentasikan hasil pengujian, (2) pelaku pengujian, dan (3) tanggal penyelesaian pengujian. Rincian luasan dan pemilihan waktu pengujian dapat ditunjukkan dalam program audit tersebut atau pada referensi silang kertas kerja seperti yang diasumsikan pada contoh tersebut. Pembuatan kertas kerja yang menunjukkan sampel dan hasil pengujian dijelaskan pada bab selanjutnya, termasuk karakteristik penyampelan untuk uji pengendalian. Perlu dicatat bahwa daftar pengujian pada program audit formal pada tabel 1.6 diambil dari contoh uji pengendalian. Beberapa pengujian telah disusun ulang dan dikombinasi untuk kepentingan efisiensi.

Tabel 1.4. Contoh Sebagian Program Audit untuk Uji Pengendalian

Dibuat Oleh:_
Tanggal:
Diperiksa Oleh:_
Tanggal:

PT XXX
Rencana Uji Pengendalian-Transaksi Pengeluaran Kas
Untuk Periode yang Berakhir 31 Desember 20XX

Kertas Kerja Referensi	Asersi/Uji Pengendalian	Audit	Tanggal
	1. Mengatur penggunaan fasilitas komputer klien untuk menguji pengendalian aplikasi terprogram menggunakan pengujian data. Keterjadian 2. Meng-*input*-kan pengujian data untuk memastikan bahwa program secara tepat mengidentifikasi pengecualian untuk: a. Transaksi yang informasi *voucher* tidak sama dengan informasi pendukung yang. (Catatan: juga menguji pengendalian penilaian) b. Transaksi yang di-*input*-kan dua kali 3. Menginspeksi laporan pengecualian yang dihasilkan komputer di dalam siklus bisnis normal dan mengevaluasi efektivitas prosedur tindak lanjut manual 4. Mengobservasi bahwa hanya personel yang berwenang yang menangani cek setelah komputer menandatangani cek		

	5. Mengobservasi pemisahan tugas persetujuan *voucher* pembayaran dan penanganan cek yang sudah ditandatangani. 6. Ketidakcocokan antara jumlah cek yang diterbitkan dengan total *posting* untuk pengeluaran kas (Catatan: juga menguji pengendalian penilaian) 7. Mengobservasi penanganan dan penyimpanan cek yang tidak digunakan 8. Menyelidiki setiap pengeluaran kas yang dibuat dengan metode selain cek 9. Menginspeksi rekonsiliasi bank independen dan mengevaluasi efektivitas pengendaliannya (Catatan: Hal ini juga menguji pengendalian keberadaan & keterjadian & penilaian)		

4. Pengujian Dua Tujuan (Dual-Purpose Test)

Pada kebanyakan audit, uji pengendalian dikerjakan terutama selama pekerjaan interim, sementara uji substantif terhadap saldo dikerjakan terutama pada akhir tahun. Namun demikian, standar audit memperbolehkan uji substantif atas detail transaksi untuk mendeteksi kesalahan moneter di rekening selama pekerjaan interim. Pada kasus tersebut, auditor dapat melakukan uji pengendalian secara simultan pada transaksi yang sama. Misalnya, auditor memeriksa laporan pengecualian tentang pencatatan pengeluaran sekaligus mentabulasi kesalahan moneter pada voucher pembayaran.

Pengujian yang secara simultan melakukan uji pengendalian internal sekaligus menyediakan bukti substantif disebut pengujian dua tujuan. Selama melakukan pengujian ini, auditor harus berhati-hati agar baik bukti efektivitas pengendalian maupun kesalahan moneter dalam transaksi dapat diperoleh. Beberapa kantor audit menggunakan pengujian dua tujuan karena lebih efisien kos daripada pengujian terpisah.

1.4 PERTIMBANGAN TAMBAHAN

1. Penaksiran Risiko Pengendalian untuk Asersi Saldo Rekening yang Dipengaruhi Transaksi Tunggal

Proses penaksiran risiko pengendalian untuk asersi saldo rekening yang dipengaruhi transaksi tunggal bersifat langsung. Kasus ini banyak terjadi pada rekening laporan raba rugi. Contohnya, penjualan bertambah karena kredit transaksi penjualan dalam siklus pendapatan, dan banyak rekening biaya bertambah karena debit transaksi pembelian dalam siklus pengeluaran.

Pada kasus tersebut, penaksiran risiko pengendalian untuk tiap asersi saldo rekening adalah sama pada asersi kelas transaksi yang sama. Misalnya, penaksiran risiko pengendalian untuk asersi keberadaan dan keterjadian pada saldo rekening penjualan harus sama seperti asersi keberadaan dan keterjadian pada transaksi penjualan. Secara ekuivalen, penaksiran risiko pengendalian untuk asersi penilaian dan alokasi pada banyak biaya harus sama dengan asersi penilaian dan alokasi pada transaksi pembelian.

2. *Penaksiran Risiko Pengendalian Untuk Asersi Saldo Rekening yang Dipengaruhi Transaksi Multipel*

Banyak rekening neraca secara signifikan dipengaruhi lebih dari satu kelas transaksi. Misalnya, rekening piutang usaha bertambah karena transaksi penjualan pada siklus pendapatan dan berkurang karena penerimaan kas atau retur penjualan dan cadangan kerugian piutang. Dalam kasus tersebut, penaksiran risiko pengendalian untuk asersi saldo rekening harus mempertimbangkan penaksiran risiko pengendalian yang relevan untuk tiap kelas transaksi. Keberadaan dan keterjadian piutang usaha (yang mengakibatkan lebih saji piutang usaha) dipengaruhi oleh tiga transaksi (1) keberadaan dan keterjadian penjualan, (2) kelengkapan penerimaan kas, dan (3) kelengkapan retur penjualan dan cadangan kerugian piutang. Oleh karena itu, jika sebuah penjualan diakui, padahal seharusnya tidak, mengakibatkan masalah keberadaan piutang usaha. Demikian juga, masalah kelengkapan penerimaan kas atau retur penjualan juga mengakibatkan lebih saji piutang usaha (masalah keberadaan). Kegagalan pencatatan penerimaan kas dari pelanggan (masalah kelengkapan) mengakibatkan salah saji piutang usaha.

Kelengkapan piutang usaha (yang mengakibatkan kurang saji piutang usaha) juga dipengaruhi tiga transaksi (1) kelengkapan penjualan, (2) keberadaan dan keterjadian penerimaan kas, dan (3) keberadaan dan keterjadian retur penjualan cadangan kerugian piutang. Oleh karena itu, penjualan yang tidak tercatat mengakibatkan masalah kelengkapan rekening piutang usaha. Demikian juga, masalah keterjadian penerimaan kas atau retur penjualan akan mengakibatkan kurang saji

rekening piutang usaha (masalah kelengkapan). Tabel 1.5. menyajikan beberapa contoh dari jenis transaksi yang menambah atau mengurangi saldo rekening.

Tabel 1.5. Ringkasan Hubungan Antara Pernyataan Sald Akun & Pernyataan Kelas Transaksi

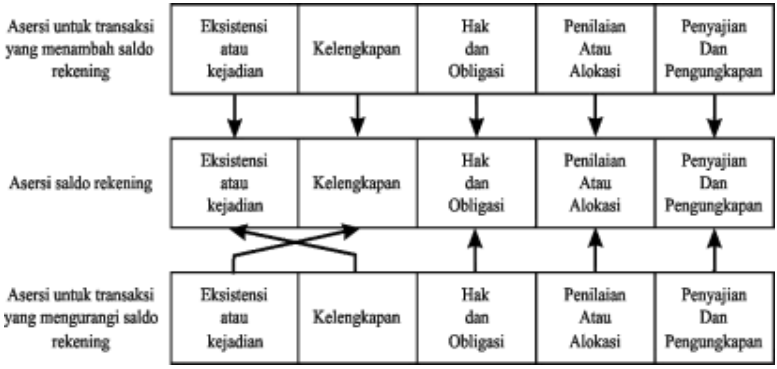
Asersi Saldo Rekening		**Asersi Kelas Transaksi yang Menambah Saldo Rekening**	**Asersi Kelas Transaksi yang Mengurangi Saldo Rekening**
Contoh 1	Keberadaan Piutang Usaha	Keberadaan dan keterjadian penjualan	Kelengkapan penerimaan Kelengkapan retur penjualan dan cadangan kerugian piutang
Contoh 2	Kelengkapan utang usaha	Kelengkapan pembelian	Keberadaan dan keterjadian pengeluaran kas Keberadaan dan keterjadian retur pembelian

Aturan umum di bawah ini menjelaskan hubungan antara asersi kelas transaksi dan asersi saldo rekening.

a. Penaksiran risiko pengendalian untuk asersi keberadaan dan keterjadian saldo rekening terkait dengan asersi keberadaan dan keterjadian untuk transaksi yang menambah saldo rekening dan juga asersi kelengkapan untuk transaksi yang mengurangi saldo akun.
b. Penaksiran risiko pengendalian untuk asersi kelengkapan saldo rekening terkait dengan asersi

kelengkapan transaksi yang menambah saldo rekening dan juga asersi keberadaan dan keterjadian untuk transaksi yang mengurangi saldo rekening.

c. Asersi hak dan obligasi saldo rekening terkait dengan asersi hak dan obligasi untuk transaksi baik yang mengurangi maupun yang menambah saldo rekening.
d. Asersi penilaian dan alokasi saldo rekening terkait dengan asersi penilaian dan alokasi untuk transaksi baik yang menambah maupun yang mengurangi saldo rekening.
e. Asersi penyajian dan pengungkapan saldo rekening terkait dengan asersi penyajian dan pengungkapan transaksi baik yang menambah dan mengurangi saldo rekening.



Gambar 1.8. Ringkasan Hubungan antara Asersi Saldo Rekening dan Asersi Kelas Transaksi

Merujuk gambar 1.8, anggaplah auditor mendapatkan penaksiran risiko pengendalian sebagai berikut dari kertas kerja yang didasarkan pada pemahaman tentang bagian pengendalian internal yang relevan berdasarkan uji pengendalian:

ASERSI TAKSIRAN RISIKO PENGENDALIAN

a. Keberadaan dan keterjadian penjualan rendah.
b. Kelengkapan penerimaan kas rendah.
c. Kelengkapan retur penjualan & cadangan kerugian piutang moderat.

Ketika penaksiran risiko pengendalian untuk asersi kelas transaksi yang relevan berbeda, auditor menilai materialitas tiap penaksiran ketika menggabungkan penaksiran. Alternatif lain, beberapa kantor audit memilih menggunakan penaksiran yang paling konservatif (paling tinggi). Oleh karena itu, penaksiran risiko pengendalian untuk keberadaan piutang usaha haruslah moderat jika retur penjualan dan cadangan kerugian piutang tidak material.

Setelah risiko pengendalian untuk asersi saldo rekening telah ditentukan, taksiran ini harus dibandingkan dengan rencana level penaksiran risiko pengendalian. Jika level yang direncanakan terdukung, auditor dapat melanjutkan mendesain uji substantif berdasarkan strategi audit pendahuluan. Sebaliknya, jika rencana level penaksiran risiko pengendalian tidak terdukung, rencana level uji substantif dan uji audit terkait harus direvisi untuk mendapatkan level risiko audit yang dikehendaki.

3. Dokumentasi Level Penaksiran Risiko Pengendalian

Kertas kerja auditor harus meliputi dokumentasi penaksiran risiko pengendalian. Hal-hal yang diharuskan adalah sebagai berikut.

a. Risiko pengendalian ditaksir pada level maksimal: hanya kesimpulan tersebut yang perlu didokumentasikan.

b. Risiko pengendalian ditaksir pada level di bawah maksimal. Dasar penaksiran harus didokumentasikan.

AU 319 tidak mengilustrasikan atau menyediakan petunjuk bentuk dokumentasi. Pada praktiknya, sebuah pendekatan yang umum digunakan adalah memoranda naratif yang disusun pada asersi laporan keuangan. Pendekatan ini diilustrasikan pada gambar 1.8, yang mendokumentasikan penaksiran risiko pengendalian untuk asersi transaksi penjualan yang tertentu. Perhatikan bahwa dasar penaksiran level di bawah maksimal untuk asersi kelengkapan sudah ditetapkan, sedangkan hanya kesimpulan dinyatakan karena penaksiran pada level maksimal, seperti diindikasikan untuk asersi ketepatan.

BAB 2

DASAR DAN KONSEP AUDIT TEKNOLOGI INFORMASI

2.1. Konsep Dasar Audit Teknologi Informasi

2.1.1. *Definisi Audit Teknologi Informasi*

Menurut (Arens dan Loebbecke, 2003), audit adalah suatu proses pengumpulan dan pengoperasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi yang dimaksud dengan kriteria-kriteria yang ditetapkan. *Auditing* seharusnya dilakukan oleh seseorang yang independen dan kompeten.

Menurut (Mulyadi, 2002), audit adalah suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pernyataan-pernyataan tentang kegiatan dana kejadian ekonomi, dengan tujuan untuk

menetapkan tingkat kesesuaian tentang pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan.

2.1.2. *Audit Sistem Teknologi Informasi*

Dalam Wikipedia, audit teknologi informasi (*information technology* (II) audit) atau audit sistem informasi (*information systems* (IS) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis.

Pada mulanya istilah ini dikenal dengan audit pemrosesan data elektronik, dan sekarang audit teknologi informasi secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu. Istilah lain dari audit teknologi informasi adalah audit komputer yang banyak dipakai untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam rnencapai target organisasinya. George H. Bodnar terjemahan Jusuf, berpendapat mengenai audit sistern informasi adalah bahwa sebagian besar perusahaan memperkerjakan auditor intern dan ekstern untuk mengaudit sistem informasi. Fokus audit arus pada sistem informasi itu sendiri dan pada validitas dan akurasi data yang diproses oleh sistem. Weber mengemukakan bahwa audit sistem informasi merupakan proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset dan

teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan pada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif dan efisien. Dengan demikian, Aktivitas audit perlu dilakukan untuk mengukur dan memastikan kesesuaian pengelolaan baik sistem maupun teknologi informasi dengan ketetapan dan standar yang berlaku pada suatu organisasi, sehingga perbaikan dapat dilakukan dengan lebih terarah dalam kerangka perbaikan berkelanjutan (Sarno, 2009: 27).

Berdasarkan pengertian yang telah diuraikan dan masih menurut Weber dapat disimpulkan bahwa tujuan dari audit sistem informasi adalah untuk mengetahui apakah pengelolaan sistem dan teknologi informasi telah mencapai tujuan strategisnya, yaitu:

1. Meningkatkan perlindungan terhadap asset-aset (*Asset safeguard*) Aset informasi perusahaan seperti perangkat keras (*hardware*), perangkat lunak (software, sumber daya manusia, file data harus dijaga oleh suatu system pengendalian intern yang baik agar tidak terjadi penyalahgunaan asset perusahaan.
2. Menjaga integritas data (*Data integrity*): Integritas adalah suatu konsep dasar sistem informasi, jika tidak terpelihara maka suatu perusahaan tidak akan memiliki lagi hasil atau laporan yang benar bahkan perusahaan dapat menderita kerugian.
3. Meningkatkan efektifitas sistem (*Effectivity*): Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila system infonnasi tersebut telah sesuai dengan kebutuhan user.

4. Meningkatkan efisiensi system (*Efficiency*).

2.1.3. *Definisi Monitoring*

Monitoring is a continuous assessment that aims at providing all stakeholders with early detailed information on the progress or delay of the ongoing assessed activities. It is em oversight of the activity's implementation stage. Its purpose is to detertnine if the outputs, deliveries and schedules planned have been reached so that action can be taken to correct the deficiencies as quickly as possible.

Dapat diartikan bahwa monitoring adalah pemantauan adalah penilaian yang berkesinambungan yang bertujuan untuk menyediakan semua informasi rinci kepada *stakeholder* dengan cepat pada kemajuan atau penundaan dinilai dari kegiatan yang sedang berlangsung itu adalah tahap pengawasan pelaksanaan kegiatan tersebut. Tujuannya adalah untuk menentukan jika output, pengirirnan, dan jadwal yang direncanakan telah dicapai sehingga tindakan dapat diambil untuk memperbaiki kekurangan secepat mungkin.

2.1.4. *Definisi Evaluation*

Evaluation is a systematic and objective examination concerning the relevance, effectiveness, efficiency and impact of activities in the light of specified objectives. The idea in evaluating projects is to isolate errors not to repeat them and to underline and promote the successful mechanismsfor current and future projects.

Dapat diartikan bahwa evaluation adalah pemeriksaan yang sistematis dan objektif tentang relevansi, efektivitas, efisiensi dan dampak dari kegiatan dalam tujuan tertentu. ide dalam mengevaluasi proyek

adalah untuk mengisolasi kesalahan tidak akan mengulangi dan untuk menggaris bawahi dan mempromosikan mekanisme sukses untuk proyek-proyek saat ini dan masa depan.

2.2 Model Standar Audit Sistem Informasi

Beberapa model standar Audit Sistem Informasi yang dapat dijadikan referensi pengelolaan TI, diantaranya ISO/lEe 17799, ITIL, COSO dan COBIT. Dalam hal ini yang akan dibahas dalam tugas akhir ini adalah model standar audit IT COBIT.

2.2.1 ISO/IEC17799 [13]

ISO/IEc 17799 dikembangkan oleh ISO (The International Organization for Standardizations pada tahun 2000 dan IEC (The International Electro technical), merupakan kode praktek untuk menyediakan suat:u kerangka sebagai standar keamanan informasi. JSOIIEC 17799:2005 Code of Practice for Irfonnation Security Management adalah standar internasional. Tujuan utama dari penyusunan standar ini adalah penerapan kearnanan inforrnasi dalam organisasi, Framework ini diarahkan untuk mengembangkan dan memelihara standar keamanan dan praktek manajemen dalam organisasi untuk meningkatkan ketahanan (*reliability*) bagi kearnanan informasi dalarn hubungan antar organisasi. Secara langsung tidak ada sertifikasi untuk ISO/IEC 17799:2005. Namun terdapat sertifikasi yang sesuai dengan ISO/IEC 27001 (BS 7799-2).

Diuraikan 10 bagian utama dan mengidentifikasi sasaran hasil dari hap kendali relatif untuk ditererapkan dalam standar ISO/IEC 17799:

1. Kebijakan keamanan (*security policy*);
2. Organisasi keamanan (*security organisation*);
3. Penggolongan asset dan kendali (*asset classification and control*);
4. Keamanan personil (*personnel security*);
5. Phisik dan keamanan lingkungan (*physical and environmental security*);
6. Komunikasi dan management operasi (*communnication and operations management*);
7. Kendali akses sistem (*system access control*);
8. Pengembangan system dan pemeliharaan (*system development and maintenance*);
9. Perencanaan kesinambungan bisnis (*business continuity planning*);
10. Pemenuhan (*compliance*);

2.2.2 ITIL

ITIL (*The IT Infrastructure Library*) dikembangkan oleh OGC (*The Office of Government Co771111 erce*) suatu badan di bawah pemerintahan Inggris, dengan bekerja sama dengan itSMF (*The IT Service Management Foruniy)* dan BSI (British Standard Institutes) ITIL merupakan suatu framework pengelolaan layanan TI (IT *Service Management* - ITSM) yang sudah diadopsi sebagai standar industri pengembangan industri perangkat lunak di dunia.

Pada 30 Juni 2007, OGC menerbitkan versi ketiga IIlL (IIlL v3) yang intinya terdiri dari lima bagian dan lebih mnenekankan pada pengelolaan siklus hidup layanan yang disediakan oleh teknologi informasi. Kelima bagian tersebut adalah:

1. *Service Strategy*
2. *Service Design*
3. *Service Transition*
4. *Service Operation*
5. *Continual Service Improvement*

ITSM memfokuskan diri pada 3 (tiga) tujuan utama, yaitu:

1. Menyelaraskan layanan II dengan kebutuhan sekarang dan akan datang dari bisnis dan pelanggannya.
2. Memperbaiki kualitas layanan-layanan TI.
3. Mengurangi biaya jangka panjang dari pengelolaan layanan-layanan tersebut.

Standar IilL berfokus kepada pelayanan customer, dan sama sekali tidak menyertakan proses penyelarasan strategi perusahaan terhadap strategi TI yang dikembangkan.

2.2.3 COSO

The Cotnitte of Sponsoring Organizations of the treadway commission's (COSO) dibentukpada tahun 1985 sebagai alinasi dari 5 (lima) organisasi professional. Organisasi tersebut terdiri dari American Accounting Association, American Instititue of Certified Public Accountants, Financial Executives International, Instititute of Management Accountants, dan The Institute of Inter nal Auditors. Koalisi 1111 didirikan untuk menyatukan pandangan dalam komunitas bisnis berkaitan dengan isu-isu seputar pelaporan keuangan yang mengandung unsur kecurigaan.

COSO *iComnnttee of Sponsoring Organization of the Treadway Connuissioni* merupakan sebuah organisasi di

Amerika yang berdedikasi dalam meningkatkan kualitas pelaporan finansial mencakup etika bisnis, kontrol internal dan *corporate governance*. COSO *framework* terdiri dari 3 dimensi yaitu:

1. Komponen Kontrol COSO: COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kontrol internal:
   a. *Control environment*
   b. *Risk assessment*
   c. *Control activities*
   d. *Information and communications*
   e. *Monitoring*
2. Sasaran kontrol dan internal: Sasaran kontrol internal dikategorikan menjadi beberapa area sebagai berikut:
   a. Efektifitas dan efisiensi operasional: Efisisensi dan efektifitas operasi dalam mencapai sasaran bisnis yang juga meliputi tujuan performansi dan keuntungan.
   b. Reliabilitas laporan keuangan/*Financial Reporting* Persiapan pelaporan anggaran finansial yang dapat dipercaya.
   c. Kepatuhan atas hukum dan peraturan yang berlaku Pemenuhan hukum dan aturan yang dapat dipercaya
3. Unit/Aktifitas Terhadap Organisasi: Dimensi ini mengidentifikasikan unit aktifitas pada organisasi yang menghubungkan kontrol internal. Kontrol internal menyangkut keseluruhan organisasi dan semua bagian-bagiannya, kontrol internal seharusnya diimplementasikan terhadap unit-unit dan aktifitas organisasi.

2.2.4 COBIT

Framework cOBIT (*Control Objectives for In/ormation and related Technology*) dikembangkan oleh IT Governance Institute, sebuah organisasi yang rnelakukan studi tentang model pengelolaan TI yang berbasis di Arnerika Serikat. COBIT *Framework* terdiri atas 4 domain utama:

1. *Planning & Organization*
2. *Acquisition & Itnpletuentasion*
3. *Delivery & Support*
4. *Monitoring*

2.3 Orientasi pada COBIT (*Control Objectives for Information and Realted Technology*)

COB IT merupakan suatu framework yang dikembangkan oleh IT Governance Institute, sebuah organisasi yang melakukan studi tentang model pengelolaan TI yang berbasis di Amerika Serikat.

COBIT mempertemukan kebutuhan beragam manajemen dengan menjembatani celah atau gap antara resiko bisnis, kebutuhan kontrol dan masalah-masalah teknis teknologi informasi. cOBIT menyediakan referensi best business practices yang mencakup keseluruhan proses bisnis perusahaan dan memaparkannya dalam struktur aktivitas-aktivitas logis yang dapat dikelola serta dikendalikan secara efektif. COBIT akan menolong manajemen dalam mengoptimumkan investasi TI nya melalui ukuran-ukuran dan pengukuran yang akan mernberikan sinyal bahaya bila suatu kesalahan atau risiko akan atau sedang terjadi. COB IT merupakan standar yang dinilai paling lengkap dan menyeluruh sebagai framework IT audit karena dikembangkan secara

berkelanjutan oleh lembaga swadaya profesional auditor yang tersebar di hampir seluruh negara. Dimana di setiap negara dibangun chapter yang dapat mengelola para profesional tersebut. Target pengguna dari framework COB IT adalah organisasi/perusahaan dari berbagai latar belakang dan para *profesional external assurance*. Secara manajerial target pengguna COBIT adalah manajer, pengguna dan profesional TI serta pengawas/pengendali profesional. Secara resmi tidak ada sertifikasi profesional resmi yang diterbitkan oleh ITOI atau organisasi manapun sebagai penyusun standar COBIT. Di Amerika Serikat standar COBIT sering digunakan dalam standar sertifikasi Certified Public Accountants (CPAs) dan Chartered Accountants (CAs) berdasarkan Statement 011 Auditing Standards (SAS) No. 70 Service Organisations reviel1i, Systrust certification or Sal' banes-Oxley c01l1pliance. Control Objectives for Information and related Technology atau disingkat dengan COB IT adalah suatu panduan standar praktek manajemen teknologi informasi dan sekumpulan dokumentasi *best practices* untuk tata kelola TI yang dapat membantu auditor, manajemen dan pengguna untuk menjembatani pemisah antara resiko bisnis, kebutuhan pengendalian, dan permasalahan-permasalahan teknis.

1. *Effectiveness*: Berkaitan dengan informasi yang relevan dan berkaitan dengan proses bisnis serta yang disampaikan benar, konsisten dan dapat digunakan tepat waktu.
2. *Efficiency*: Menyangkut penyediaan informasi melalui penggunaan sumber daya yang optimal (paling produktif dan ekonomis).

3. *Confidentiality*: Merupakan kerahasiaaan perusahaan dalam menjaga keamanan informasi dari ancaman dan gangguan pihak-pihak yang tidak bertanggungjawab.
4. Integrity: Berkaitan dengan keakuratan dan kelengkapan informasi serta validitas sesuai dengan nilai-nilai bisnis dan harapan.
5. *Availability*: Berkaitan dengan informasi yang tersedia ketika diperlukan oleh proses bisnis sekarang dan di masa depan. Hal ini juga menyangkut pengamanan sumber daya yang diperlukan dan kemampuan yang terkait.Co1l7pliance. Merupakan kepatuhan hukum, regulasi dan kesepakatan kontrak.
6. *Compliance*: Kepatuhan hukum, regulasi dan kesepakatan kontrak.
7. *Reliability*: Merupakan kehandalan informasi yang diperlukan manajemen dalarn mendukung kinerja.

Berikut merupakan 4 domain COBIT, yang terdiri dari:

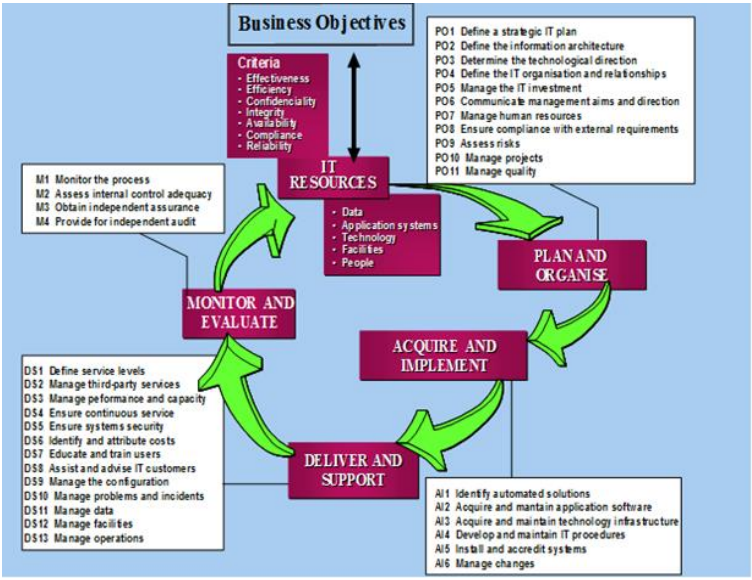
1. *Planning & Organisation*: Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi perusahaan, mencakup masalah strategi, taktik dan identifikasi cara terbaik IT untuk memberikan kontribusi rnaksimal terhadap pencapaian tujuan bisnis organisasi.
2. *Acquisition & Implementation*: Domain ini berkaitan dengan implementasi solusi IT dan integrasinya dalam proses bisnis organisasi, juga meliputi perubahan dan perawatan yang dibutuhkan sistern yang sedang berjalan untuk memastikan daur hidup sistem tersebut tetap terjaga.
3. *Delivery & Support*: Domain ini mencakup proses pemenuhan1ayanan IT, keamanan sistem,

kontinyuitas layanan, pelatihan dan pendidikan untuk pengguna, dan pemenuhan proses data yang sedang berjalan.

4. *Monitoring*: Domain ini berfokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan intern dan ekstern dan jaminan *independent* dari proses pemeriksaan yang dilakukan.

2.3.1 Kerangka Kerja COBIT

Secara jelas, COBIT membagi proses pengelolaan teknologi inforrnasi menjadi empat domain utama dengan total tiga puluh empat proses teknologi informasi, masing-masing domain dalam COB IT mempunyai beberapa rincian sebagai berikut (Sarno,2009: 31-42):



Gambar 2.1. Kerangka Kerja COBIT

1. *Planning & Organisation* (PO)

   Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi perusahaan, mencakup masalah strategi, taktik dan identifikasi cara terbaik IT untuk memberikan kontribusi maksimal terhadap pencapaian tujuan bisnis organisasi. Berikut ini *high*-level *control-objectives* dari domain ini sebagai berikut:

   1. POl Define a Strategic IT Plan.
   2. P02 Define the Information Architecture.
   3. P03 Determine Technological Direction.
   4. P04 Define the IT Organisation and Relationships.
   5. POS Manage the IT Investment.
   6. P06 Communicate Management Aims and Direction
   7. P07 Manage Human Resources.
   8. P08 Ensure Compliance with External Requirements.
   9. P09 Assess Risks POlO Manage Projects POll Manage Quality.

2. *Acquisition & Implementation*

   Domain ini berkaitan dengan implementasi solusi IT dan integrasinya dalam proses bisnis organisasi, juga meliputi perubahan dan perawatan yang dibutuhkan sistem yang sedang berjalan untuk memastikan daur hidup sistem tersebut tetap terjaga. Berikut ini *high-level control-objectives* dari domain ini sebagai berikut:

   1. All Identify Automated Solutions.
   2. AI2 Acquire and Maintain Application Software.
   3. AI3 Acquire and Maintain Technology Infrastructure.

4. AI4 Develop and Maintain Procedures.
5. AIS Install and Accredit Systems.
6. AI6 Manage Changes.

3. *Delivery and Support* (DS)

   Domain ini mencakup proses pemenuhan layanan IT, keamanan sistem, kontinyuitas layanan, pelatihan dan pendidikan untuk pengguna, dan pemenuhan proses data yang sedang berjalan. Berikut ini *high-level control-objectives* dari domain ini sebagai berikut:

   1. DSI Define and Manage Service Levels.
   2. DS2 Manage Third-Party Services.
   3. DS3 Manage Performance and Capacity.
   4. DS4 Ensure Continuous Service DS5 Ensure Systems Security DS6 Identify and Allocate Costs DS7 Educate and Train Users.
   5. DS8 Assist and Advise Customers.
   6. DS9 Manage the Configuration.
   7. DSIO Manage Problems and Incidents.
   8. DSll Manage Data DS12 Manage Facilities DS13 Manage Operations.

4. *Monitoring and Evaluation*

   Domain ini berfokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan intern dan ekstern dan jarninan independent dari proses pemeriksaan yang dilakukan. Berikut ini *high-level control-objectives* dari domain ini sebagai berikut:

   1. Ml Monitor the Processes
   2. M2 Assess Internal Control Adequacy
   3. M3 Obtain Independent Assurance
   4. M4 Provide for Independent Audit

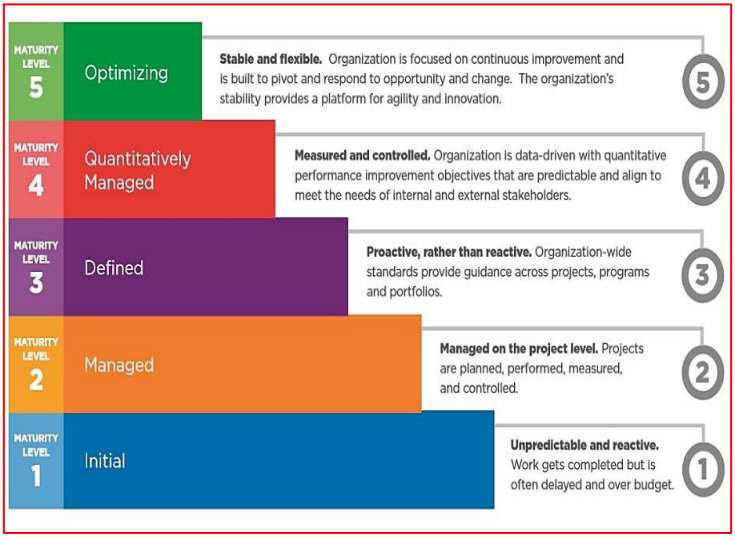
2.3.2 Management Guidelines COBIT [11]

COBIT mempunyai model kematangan (*maturity lJIodels*) untuk mengontrol proses-proses TI dengan menggunakan metode penilaian (*scoring*) sehingga suatu organisasi dapat menilai proses-proses TI yang dimilikinya dari skala *non-existent* sampai dengan optimised (dari 0 sampai 5). Selain itu, COB IT juga rnernpunyai ukuran-ukuran strategi lainnya sebagai berikut:

1. *Critical Success Factors* (CSF): Mendefinisikan hal-hal atau kegiatan penting yang dapat digunakan manajemen untuk dapat mengontrol proses-proses TI diorganisasinya.
2. *Key Goal Indicators* (KGI): Mendefinisikan ukuran-ukuran yang akan mernberikan gambaran kepada manajemen apakah proses-proses TI yang ada telah memenuhi kebutuhan proses bisnis yang ada. KGI biasanya berbentuk berbentuk informasi:
   a Ketersediaan informasi yang diperlukan dalam mendukung kebutuhan bisnis.
   b Efisiensi biaya dari proses dan operasi yang dilakukan.
   c Konfirmasi reliabilitas, efektifitas, dan compliance.
3. *Key Performance Indicators* (KPI): Mendefinisi kan ukuran-ukuran untuk menentukan kinerja proses-proses TI dilakukan untuk mewujudkan tujuan yang telah ditentukan, KPI biasanya berupa indikator kapabilitas, pelaksanaan, dan kemampuan sumber daya TI.

2.3.3 Maturity Model

Maturity model merupakan alat ukur untuk mengetahui kondisi proses IT yang digunakan pada saat sekarang oleh suatu organisasi. Kemudian dapat digunakan untuk mengendalikan dan memonitor proses IT untuk meyakinkan pencapaian tujuan-tujuan kinerja proses IT. Dalam pembuatan *Maturity* model ini digunakan kuisoner yang dibuat berdasarkan domain DS yang berasal dari COB IT untuk melakukan tahapan-tahapan analisis dengan objek yang terdapat pada *Control Objectives* yang telah ditentukan sebelumnya. Responden akan memilih tingkat pengelolaan yang sangat sesuai dengan kondisi saat ini.



Gambar 2.2. *Level Maturity* CMMI (CMMI Institute)

Model CMMI memiliki 5 tingkat tahapan kematangan (*Maturity Level*) yang dapat didefinisikan sebagai berikut:

1. Maturity level-1(ML-1) - Initial. Pada ML-1 ini proses biasanya berbentuk ad hoc. Sukses pada level ini didasarkan pada kerja keras dan kompetensi yang tinggi orang-orang yang ada di dalam organisasi tersebut
2. Maturity level-2 (ML-2) - Managed. Pada ML-2 ini sebuah organisasi telah mencapai seluruh specific dan generic goals pada Level 2. Dengan kata lain seluruh proses dalam organisasi telah direncanakan, dilaksanakan, diukur, dan dikontrol dengan baik
3. Maturity level-3 (ML-3) - Defined. Pada ML-3 ini sebuah organisasi telah mencapai seluruh specific dan generic goals pada Level 2 dan Level 3. Proses dicirikan dan dipaparkan dalam standar, prosedur, tool, dan metode
4. Maturity level-4 (ML-4) - Quantitatively Managed. Pada ML-4 ini, sebuah organisasi telah mencapai seluruh specific dan generic goals yang ada pada Level 2, 3, dan 4. Sebuah subproses dipilih yang secara signifikan terlibat dalam keseluruhan proses. Subproses yang terpilih ini kemudian dikontrol dengan menggunakan statistik atau teknik kuantitative lainnya
5. Maturity level-5 (ML-5) - Optimizing. Pada ML-5 ini suatu organisasi telah mencapai seluruh specific dan generic goals yang ada di Level 2, 3, 4, dan 5. ML-5 fokus kepada peningkatan proses secara berkesinambungan melalui inovasi teknologi.

BAB 3

KONSEP DASAR E-*GOVERNMENT*

3.1 Definisi E-*government*

Pengembangan e-*government* untuk sarana penyelenggaran fungsi pemerintahanan dan layanan publik artinya menyelenggarakan roda pemerintahan dengan bantuan (memanfaatkan) teknologi informasi dan komunikasi. Dalam arti melakukan transformasi sistem proses kerja secara manual ke sistem yang berbasis elektronik. Beberapa organisasi yang pada awalnya disusun untuk keperluan proses kerja secara manual pada akhirnya bisa jadi perlu diubah dan disesuaikan untuk memungkinkan berjalannya sistem elektronik secara efektif dan optimal. Tentu saja tidak semua proses kerja dapat ditransformasi ke dalam sistem elektronik. Ada beberapa yang masih harus mengunakan sistem manual, tetapi ada sebagian besar lainnya yang dapat dikerjakan dengan lebih cepat, efektif dan efisien melalui bantuan sistem elektronik.

Dalam pengembangan e-*government* diperlukan arsitektur dan kerangka pengembangan yang jelas agar hasilnya juga maksimal.

Penerapan teknologi informasi dan komunikasi di pemerintahan merupakan upaya untuk mengembangkan penyelenggaraan pemerintahan yang berbasiskan elektronik dalam rangka meningkatkan transparansi dan kualitas pelayanan publik secara efektif dan efisien.

Dalam pembangunan, pengembangan dan penerapan teknologi informasi di Pemerintah Kota didasarkan pada beberapa asas-asas berikut ini:

1. ***Asas Keterpaduan/Sinergi***

   Pembangunan dan penerapan teknologi informasi harus mampu mengintegrasikan semua informasi yang tersedia di pemerintahan daerah secara efektif untuk mendukung proses pengambilan keputusan. Pembakuan data dan informasi yang dibutuhkan antar instansi sangat diperlukan untuk dapat memenuhi asas keterpaduan ini.

2. ***Asas Peningkatan Kualitas SDM***

   Pembangunan dan penerapan teknologi informasi harus diupayakan untuk dapat memperkuat dan meningkatkan kualitas SDM lokal, baik secara internal yaitu dilingkungan pegawai pemerintah daerah ataupun secara eksternal dilingkungan masyarakat lokal.

3. ***Asas Manfaat/Dayaguna***

   Pembangunan dan penerapan teknologi informasi harus diupayakan untuk lebih efisien dan ekonomis serta berdayaguna tinggi. Sistem harus mampu untuk menyajikan informasi yang dibutuhkan secara cepat,

akurat dan tepat waktu sehingga dapat digunakan untuk mendukung pengambilan keputusan.

4. ***Asas Keamanan Dan Kehandalan***

   Pembangunan dan penerapan teknologi informasi harus dijamin kehandalannya sehingga mampu untuk selalu siap pakai sesuai dengan tingkat pelayanan yang dibutuhkan, serta terjamin tingkat keamanan dan kerahasiaan data sesuai dengan hukum dan perundang-undangan yang berlaku.

5. ***Asas Legalitas***

   Pembangunan dan penerapan teknologi informasi harus taat hukum, dalam hal ini harus menghormati hak-hak kekayaan intelektual (HaKI), copyright serta hak-hak lain yang diakui secara hukum dan perundang-undangan yang berlaku.

6. ***Asas Kesetaraan Hak Akses***

   Pembangunan dan penerapan teknologi informasi harus mampu menjamin dan menyediakan kesetaraan hak akses terhadap informasi pemerintahan yang bersifat terbuka untuk umum. Hal ini dimaksudkan untuk sedapat mungkin menghindarkan timbulnya kesenjangan digital pada daerah-daerah atau masyarakat tertentu.

7. ***Asas Fleksibilitas***

   Pembangunan dan penerapan teknologi informasi harus dilakukan secara modular dan berkelanjutan (*incremental development*) untuk menjamin tingkat fleksibilitas sistem terhadap perubahan-perubahan yang berlangsung baik di internal pemerintahan ataupun perubahan eksternal.

8. Asas Open System, Open Source dan Legal software

Pembangunan dan penerapan teknologi informasi dilakukan dengan menggunakan standard open system, sehingga memungkinkan untuk memadukan antar beberapa teknologi yang tersedia saat ini secara lebih efisien. Pemerintah daerah juga didorong untuk sedapat mungkin menggunakan aplikasi-aplikasi open source sehingga dapat meningkatkan tingkat efisiensi, nilai ekonomis pada investasi, dan menghindari ketergantungan absolute pada salah satu pihak serta mendukung gerakan IGOS (Indonesia, Go Open Source). Jika akan menggunakan aplikasi proprietary, maka harus mempertimbangkan aspek legalitasnya.

3.2 Kerangka Berpikir

Sesuai dengan yang telah digariskan dalam Inpres No. 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan e-*government* dalam paragraf tujuan Pengembangan e-*government* yang diarahkan untuk mencapai 4 tujuan utama, keempat tujuan tersebut areanya dipersempit hanya untuk wilayah kota saja yaitu:

1. Pembentukan jaringan informasi dan transaksi pelayanan publik yang memiliki kualitas dan lingkup yang dapat memuaskan masyarakat luas serta dapat terjangkau untuk setiap warga Kota pada setiap saat tidak dibatasi oleh sekat waktu dan dengan biaya yang terjangkau oleh masyarakat.
2. Pembentukan hubungan interaktif dengan dunia usaha untuk meningkatkan perkembangan perekonomian kota.

3. Pembentukan mekanisme dan saluran komunikasi untuk fasilitas dialog publik bagi masyarakat agar dapat berpartisipasi dalam perumusan kebijakan kota.
4. Pembentukan sistem manajemen dan proses kerja yang transparan dan efisien serta memperlancar transaksi dan layanan antar OPD/SKPD.

Dalam kerangka ini fungsi teknologi informasi tidak sekedar sebagai penunjang manajemen pemerintahan yang ada, tetapi justru merupakan sebagai hal yang justru menawarkan terjadinya perubahan-perubahan mendasar sehubungan dengan proses penyelenggaraan pemerintahan.

Pencapaian keseluruhan tujuan tersebut di atas adalah merupakan perwujudan dari kondisi ideal dimana pemerintah dengan dukungan teknologi informasi mampu memberikan pelayanan yang responsif dan berkualitas pada masyarakat umum, dunia usaha ataupun pelayanan antar OPD/SKPD.

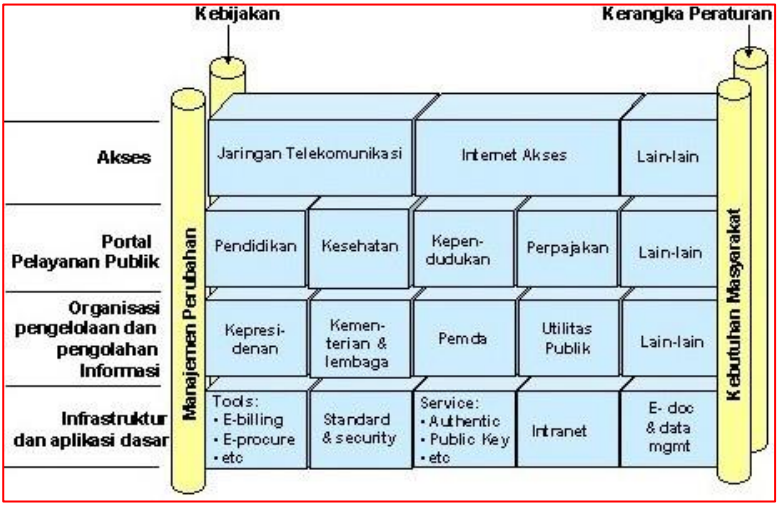
3.3 Aspek Legalitas

1. UU 32/2004 (Perubahan UU 22/1999) Tentang Pemerintah Daerah
2. Instruksi Presiden Republik Indonesia Nomor 6 tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia.
3. Kerangka kerja Teknologi Informasi Nasional (National IT Framework/NITF).
4. Keputusan Presiden Republik Indonesia Nomor 9 Tahun 2003 tentang Tim Koordinasi Telematika Indonesia.

5. Instruksi Presiden Republik Indonesia No. 3 Tahun 2003, tentang Strategi dan Kebijakan Nasional Pengembangan E-*government*.
6. Peraturan Presiden Republik Indonesia no 81 tahun 2010 tentang Grand Design Reformasi Birokrasi 2010 – 2025
7. KemenPANRB: Strategi Perceparan Reformasi Birokrasi

3.4. Konsep Penerapan

Untuk menjamin keterpaduan sistem pengelolaan dan pengolahan dokumen dan informasi elektronik dalam mengembangkan pelayanan publik yang transparan, pengembangan e-*government* pada setiap instansi harus berorientasi pada kerangka arsitektur di bawah ini.



Gambar 3.1. Kerangka e-*government*

Kerangka arsitektur itu terdiri dari empat lapis struktur, yakni:

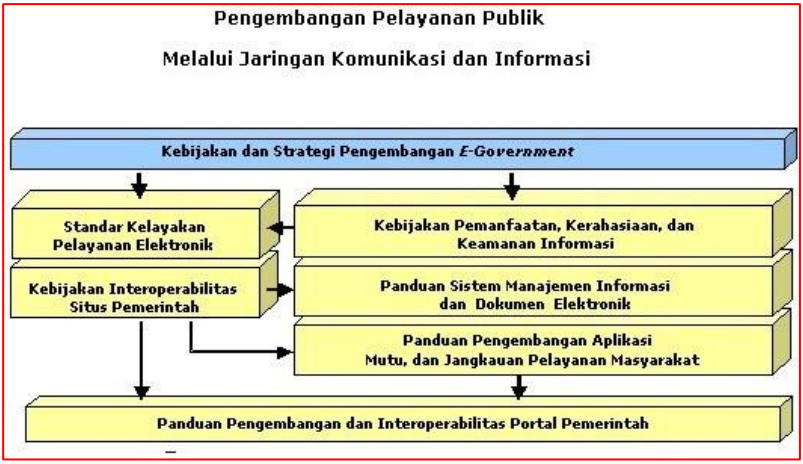
1. Akses: yaitu jaringan telekomunikasi, jaringan internet, dan media komunikasi lain yang dapat dipergunakan oleh masyarakat untuk mengakses portal pelayanan publik.
2. Portal Pelayanan Publik: yaitu situs-situs internet penyedia layanan publik tertentu yang mengintegrasikan proses pengolahan dan pengelolaan informasi dan dukumen elektronik di sejumlah instansi yang terkait.
3. Organisasi Pengelolaan & Pengolahan Informasi: yaitu organisasi pendukung (*back-office*) yang mengelola, menyediakan dan mengolah transaksi informasi dan dokumen elektronik.
4. Infrastruktur dan aplikasi dasar: yaitu semua prasarana baik berbentuk perangkat keras dan perangkat lunak yang diperlukan untuk mendukung pengelolaan, pengolahan, transaksi, dan penyaluran informasi. baik antar back-office, antar Portal Pelayanan Publik dengan back-office, maupun antara Portal Pelayanan Publik dengan jaringan internet, secara andal, aman, dan terpercaya.

Struktur tersebut ditunjang oleh 4 (empat) pilar, yakni penataan sistem manajemen dan proses kerja, pemahaman tentang kebutuhan publik, penguatan kerangka kebijakan, dan pemapanan peraturan dan perundang-undangan.

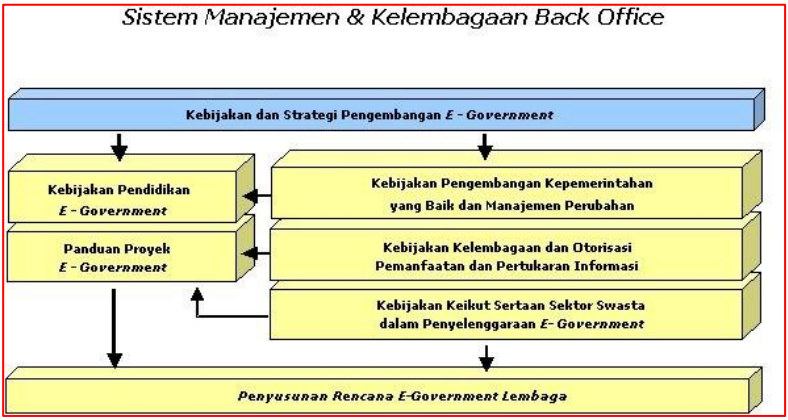
Agar pelaksanaan kebijakan pengembangan e-*government* dapat dilaksanakan secara sistematik dan terpadu, penyusunan kebijakan, peraturan dan perundang-

undangan, standardisasi, dan panduan yang diperlukan harus konsisten dan saling mendukung. Oleh karena itu perumusannya perlu mengacu pada kerangka yang utuh, serta diarahkan untuk memenuhi kebutuhan pembentukan pelayanan publik dan penguatan jaringan pengelolaan dan pengolahan informasi yang andal dan terpercaya.

Seperti digambarkan di bawah ini, kerangka tersebut mengkaitkan semua kebijakan, peraturan dan perundang-undangan, standardisasi, dan panduan sehingga terbentuk landasan untuk mendorong pembentukan *good governance.*



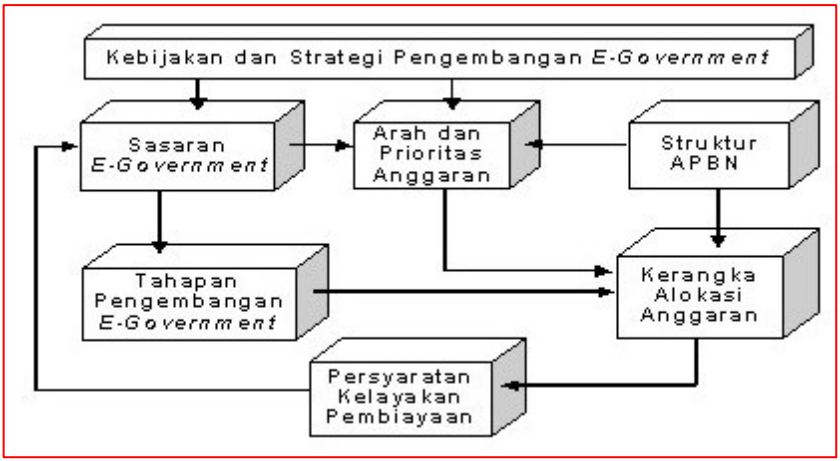
Gambar 3.2. Konsep Pelayanan Publik



Gambar 3.3. Kebijakan Pengembangan *E-goverment*

Pengembangan e-*government* memiliki lingkup kegiatan yang luas dan memerlukan investasi dan pembiayaan yang besar. Sementara itu ketersediaan anggaran pemerintah sangat terbatas dan masih harus dipergunakan untuk mengatasi berbagai permasalahan yang harus segera diselesaikan. Oleh karena itu pengalokasian anggaran untuk pengembangan e-*government* harus dilakukan secara hati-hati dan bertanggung jawab agar anggaran yang terbatas itu dapat dimanfaatkan secara efisien dan dapat menghasilkan daya ungkit yang kuat bagi pembentukan tata-pamong yang baik. Dengan demikian diperlukan siklus perencanaan, pengalokasian, pemanfaatan, dan pengevaluasian anggaran pengembangan e-*government* yang baik, sehingga pelaksanaan strategi untuk pencapaian tujuan strategis e-*government* dapat berjalan secara efektif.

Kesenjangan yang lebar antara besarnya kebutuhan anggaran dengan keterbatasan anggaran yang dapat disediakan akan menimbulkan pengalokasian anggaran yang buruk apabila arah dan prioritas penggunaan anggaran tidak terdefinisi dengan baik, proses pengalokasian anggaran tidak sistematik, dan praktek penganggaran yang tidak transparan karena lemahnya persyaratan kelayakan pembiayaan. Untuk menghindarkan pemborosan anggaran yang merupakan uang pembayar pajak, perlu dikembangkan kerangka perencanaan dan pengalokasian anggaran seperti tampak pada diagram di bawah.



Gambar 3.4. Kebijakan dan Strategi

E-*government* ini dapat diimplementasikan dalam berbagai cara. E-*government* pada prinsipnya harus:

1. Terbuka & Transparan. Terbuka dan Transparan, membuka akses informasi dan interaksi pada semua stakeholder yang berperan pada pemerintahan dan

pengambilan kebijakan. Infrastruktur jaringan komunikasi, internet, dan media website jika e-*government* menggunakan pilihan ini maka mendukung terciptanya interaksi terbuka dan transparan pada stakeholder kota tersebut. Komunikasi tersebut memungkinkan masukkan dari publik dapat ditampung dan ditindaklanjuti untuk mendapatkan solusi pembangunan kota.

2. Efisien & Efektif. Efisien dan efektif, mengembangkan sistem informasi administrasi yang lebih mudah, murah, cepat dan akurat tanpa menghilangan aspek legalitas administratifnya. Pada saat tertentu akan tercapai kepercayaan publik pada pelayanan administrasi pemerintah yang bersih dan akurat.
3. Jaringan Kerja. Jaringan kerja, memudahkan pertukaran data dan pengolahan informasi yang terdistribusi pada bagian-bagian dalam pemerintahan. Dengan cara ini dimungkinkan secara mudah dan cepat mendapatkan data dan informasi sesuai kebutuhan sehingga waktu dan hasil yang diperoleh menjadi lebih cepat dilakukan dengan jaringan kerja.
4. Integritas. Integritas, memelihara integritas sistem dan data yang ada dalam administrasi pemerintahan. Keterpaduan sistem menjadi tuntutan untuk memperoleh informasi yang akurat dalam mengambil kebijakan dan menyikapi situasi dan kondisi wilayahnya.

Mengingat pengembangan e-*government* merupakan sebuah proses transformasi dari manual ke elektronik, maka dibutuhkan upaya-upaya sistematis yang menyangkut subyek, obyek, dan metode yang terkait

dengan proses transformasi tersebut. Proses transformasi ini mengacu pada tiga hal, yaitu perundang-undangan di bidang teknologi informasi dan komunikasi, kondisi saat ini dan pengaruh lingkungan yang bersumber pada tuntutan layanan publik serta kemajuan teknologi informasi dan komunikasi.

3.5. Contoh Praktek Terbaik Implementasi

Mengembangkan sistem pelayanan yang handal dan terpercaya, serta terjangkau oleh masyarakat luas, menata sistem manajemen dan proses kerja pemerintahan, memanfaatkan teknologi informasi secara optimal, meningkatkan peran serta dunia usaha dan mengembangkan industri telekomunikasi dan teknologi informasi, mengembangkan kapasitas SDM di lingkungan pemerintahan dan meningkatkan e-*literacy* masyarakat, melaksanakan pengembangan secara sistematik melalui tahapan-tahapan yang realistik dan terukur.

Pemerintah Singapore telah membangun e-*government* pada tataran tertinggi di kawasan Asia dan bahkan mengalahkan Jepang. Singapura berhasil menunjukkan keunggulannya dalam promosi e-*Government*. Hal ini di indikasikan dari kegiatan-kegiatan yang mendukung implementasi e- *Government*. Salah satu implementasi e-*government* yang dilakukan pemerintah Singapura ialah *mobile government* (m-*goverment*). Di Singapura banyak layanan pemerintahan yang diberikan melalui SMS (*Short Message Service*) berupa pemberitahuan mengenai informasi yang penting bagi penduduk. Kini, semua pelaksanaan layanan publik di Singapura telah berlangsung secara elektronik.

Ke depan, Singapura selanjutnya akan memfasilitasi dan memampukan pergeseran besar pola pemikiran dari pola piker "Govt-To-You" (Pemerintah Untuk Anda) menjadi pola pikir "Govt-With-You" (Pemerintah Bersama dengan Anda), untuk mendorong inovasi dan mendorong proses 'co-*creation*' atau membangun bersama-sama (pemerintah dengan rakyatnya).

1. Regulasi dan kelembagaan

Dalam hal pengembangan regulasi dan kelembagaan maka Kota Padang bisa menjadi contoh yang baik, Pengelolaan e-government di Padang di laksanakan oleh Dinas Kominfo (eselon 2). Dalam pengembangan suprastruktur TIK, pada tahun 2010 saja, Pemerintah Kota Padang telah menetapkan, mengatur, dan mengundangkan sbb: (Pemko Padang).

2. Teknologi Informasi

Dalam hal pengembangan infrastruktur, maka Kota Padang bisa menjadi contoh yang sangat baik, Kota ini yang mempelopori pemanfaatan perangkat murah dan sistem yang murni di oprek sendiri akan tetapi availibilitynya sangat tinggi yang mampu melayani hingga tingkat desa, puskesmas dan sekolah negeri. Di Kota Padang pemanfaatan TIK terdiri dari:

1. LPSE Link: http://lpse.padang.go.id
2. Dishub ATCS: http://atcs.dishub.padang.go.id/
3. Sapo Link: http://saporancak.padang.go.id/perizinan/
4. E-Absensi Link: https://eabsensi.padang.go.id/
5. E-Musrembang Link: http://e-musrenbang.padang.go.id/

6. EVJAB Link: https://evjab.padang.go.id/
7. LAKIP Link: http://lakip.padang.go.id/portal/home
8. SIMDKP Link: https://simdkp.padang.go.id/
9. Sinjab Link: https://sinjab.padang.go.id/
10. New Simbangda Link: http://newsimbangda.padang.go.id
11. SIM Jabatan Link: http://sinjab.padang.go.id
12. BKD Link: http://simpeg.bkd.padang.go.id
13. KJKS Link: https://kjks.padang.go.id/auth
14. UMKM Link: http://umkm.padang.go.id
15. Silaras Link: http://silaras.padang.go.id/
16. Paten Link: http://paten-nanggalo.padang.go.id/home/
17. http://paten-padangbarat.padang.go.id/home/
18. PPID Link: http://ppid.padang.go.id/
19. http://padang.go.id/konten/e-*government*-kota-padang
20. Dan lain sebagainya.

3. Pengembangan Aplikasi

Dalam hal pengembangan aplikasi maka Kota Sragen sangat unggul dalam membangun aplikasi e-*Government*, melalui Bag. PDE telah dibangun aplikasi-aplikasi dasar yang sangat dibutuhkan dan langsung diterapkan melalui regulasi yang didukung langsung oleh kepala daerah (Wali Kota) sehingga tidak ada aplikasi yang tidak termanfaatkan. Aplikasi dibangun dengan platform opensource web base. Kunci suksesnya pemanfaatan aplikasi diantaranya selain dukungan pimpinan juga ketersediaan infrastruktur yang memadai. Jaringan internet telah tersedia hingga tingkat desa. Website terbaik di Indonesia tatakelola dan tampilannya

adalah kota. Sedangkan website pemko yang beda dari konsep pada umumnya adalah yang lebih menonjolkan pada layanan online. Sejak April 2003, Departemen Dalam Negeri (Depdagri) merintis penerapan Sistem Informasi Administrasi Kependudukan (SIAK). Di Kota Padang, Jawa Tengah, pemerintah Kabupaten/Kota di wilayah Provinsi Sumatera Barat sudah mampu menjalankan SIAK. Hanya butuh waktu dua menit untuk mengurus Kartu Tanda Penduduk (KTP) dengan biaya yang tidak mahal, sedangkan di Kota Padang Pemerintah Kabupaten/Kota lainnya telah meng-implementasikan beberapa aplikasi dengan database terintegrasi dengan beberapa aplikasinya diantaranya terintegrasi una menghindari duplikasi.

4. **Pengelolaan SDM**

   Pengelolaan SDM TIK yang bisa dicontoh adalah Pemko Padang dimana terdapat 7 orang master bidang TIK sesuai dengan kompetensi sesuai denggan bidang keahlian masing-masing bagian. Sehingga tidak diragukan lagi keunggulan produk inovasinya dalam bidang pengembangan aplikasi egovernment dan pengelolaan infrastruktur TIK-nya.

3.6. Tahapan Implementasi e-*government*

1. Tahap peletakan dasar e-*government* dengan membangun website informasi pembangunan kota serta pembangunan jaringan internet ke seluruh unsur pemerintah daerah.
2. Pengembangan aplikasi dasar untuk transaksi dan penyimpanan data, transaksi surat dan pengembangan

website interaktif. Pembangunan datacenter dengan *monitoring system.*

3. Pengembangan aplikasi untuk layanan internal kantor pemerintah, layanan sosial kemasyarakatan dan layanan bisnis. Pengembangan datacenter pada standar TIA 942 dan pembangunan data *recovery center.*
4. Pengembangan aplikasi terintegrasi, Sistem informasi eksekutif dan sistem informasi bantuan pengambilan keputusan. Pengembangan data *center* dan data *recovery* center serta pembangunan sistem pengamanan aset informasi pemerintah daerah.
5. Pengembangan dan pemanfaatan e-*government* sebagai motor penggerak sistem inovasi daerah.

Tabel 3.1. Pentahapan Implementasi sesuai *best practice* Pentahapan dari Kominfo:

Waktu	SDM	Infostruktur	Infrastruktur	Kebijakan
Jangka Pendek (tahun pertama)	Sosialisasi pengembangan e-gov Pembentukan tim tenaga ahli untuk pengembangan e- gov Pelatihan-pelatihan yang diaggap perlu untuk meningkatkan pemahaman SDM terhadap TIK	Identifikasi aplikasi yang ada di setiap instansi Identifikasi kebutuhan data dan informasi dalam e-gov Identifikasi kualitas informasi dan kuantitas informasi untuk semua pihak yang berkepentingan	Identifikasi jaringan disetiap instansi untuk memastikan infrastruktur jaringan	Pengesahan rencana induk pengembangan e- gorvernment Penetapan Dinas Pengelola TIK
Jangka Pendek	Pelatihan / sertifikasi Network Admin	Standarisasi database yang dibutuhkan	Perancangan jaringan dalam	Persiapan penetapan Struktur,

(tahun pertama)		untuk aplikasi-aplikasi e- gov Pembuatan Spesifikasi Kebutuhan Perangkat Lunak	instansi dan antar instansi Penambahan hardware workstation untuk kebutuhan e-government	tanggung jawab dan kompetensi pengelola TIK Penetapan interoperability antar SKPD Persiapan pembuatan perda SIN
Jangka Pendek (tahun pertama)	Pelatihan / Sertifikasi Database Admin Pelatihan penggunaan alikasi kritis	Pengembangan aplikasi dengan prioritas kritis	Implementasi jaringan hasil perancangan tahun sebelumnya Pengadaan Server yang memadai	Pembuatan perda tentang jabatan fungsional pengelola TIK Pembuatan Perda SIN
Jangka Menengah (s/d tahun kedua)	Pelatihan System Admin Pelatihan Penggunaan Aplikasi non kritis	Pengembangan aplikasi dengan prioritas non kritis	Migrasi dari server lama ke server baru Peningkatan Bandwidth Penambanhan workstation	Perancangan interoperability data antar SKPD
Jangka Panjang (s/d lima tahun)	Pelatihan penggunaan aplikasi secara keseluruhan Pelatihan perawatan aplikasi, jaringan	Pemeliharaan aplikasi dan data Pembangunan Data warehouse	Peningkatan Baddwidth Pemeliharaan jaringan	Sosialisasi dan Evaluasi pengembangan eGovernment

BAB 4

KONSEP DAN TATA KELOLA TIK & COBIT

4.1 Kebutuhan e-*government*

Implementasi e-*government* adalah suatu perubahan cara kerja seluruh jajaran pemerintahan yang tadinya menggunakan perangkat manual menjadi terotomatisasi dengan menggunakan perangkat teknologi informasi dan Komunikasi, e-*government* bukan hanya milik atau urusan Dinas Kominfo saja, akan tetapi merupakan urusan setiap komponen dalam pemerintahan. e-*government* dilaksanakan oleh seluruh jajaran pemerintah Kota yang terdiri dari:

a. Wali Kota/Wakil Wali Kota.
b. Dewan Perwakilan Rakyat Daerah beserta sekretariatnya.
c. Sekretariat Daerah.
d. Satuan Kerja Pelaksana Daerah.
e. Pemerintah Kecamatan dan Kelurahan-Desa

f. Perusahaan Daerah
g. Pengguna Layanan Pemerintah Daerah

Prinsip Pengembangan e-*government* adalah:

1. Pengembangan e-*government* yang sejalan dengan visi pembangunan Kota.
2. Penguatan kelembagaan dan kebijakan serta perencanaan e-*government*;
3. Penguatan infrastruktur TIK dengan membangun data center dan data *recovery center*; pemantapan jaringan internet milik pemerintah Kota serta pengelolaan keamanan informasi.
4. Pengembangan layanan TIK terintegrasi dengan pengelolaan data/informasi milik pemkab sebagai aset informasi yang bisa dikelola dan dimanfaatkan bersama seluruh SKPD dengan mekanisme dan dasar hukum yang jelas.
5. Pengembangan layanan internal birokrasi pemkab, layanan masyarakat, dan layanan dunia usaha serta koordinasi dan sinkronisasi dengan pemerintah vertikal dan horisontal
6. Pemanfaatan peran serta masyarakat dan pihak ketiga dalam mempercepat implementasi e-*government* serta memastikan benarnya arah pengembangannya berdasarkan kaidah ilmu dan standar pengembangan dan pemanfaatan TIK.

Kebutuhan Dasar e-government adalah:

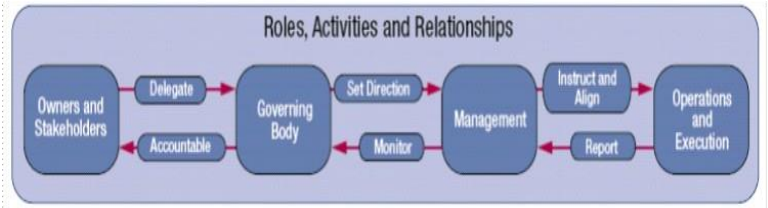
1. Kebijakan: Regulasi dan SOP
2. Kelembagaan:
   - ✓ e-*leadership* Pimpinan Daerah
   - ✓ SKPD Kominfo eselon 2

- ✓ CIO, Dewan TIK dan Relawan TIK
- ✓ SDM Pengelola dengan kualifikasi khusus
- ✓ Anggaran

3. Aplikasi e-*government*
   - ✓ Aset Data/Informasi Digital
   - ✓ Aplikasi dasar kesekretariatan, keuangan, kepegawaian, e-Mail, transfer data
   - ✓ Aplikasi pembangunan, monev dan Komunikasi vertikal
   - ✓ Aplikasi layanan masyarakat, layanan usaha
   - ✓ Aplikasi sistem pelaporan pimpinan
   - ✓ System Bantuan pengambilan keputusan
4. Sarana dan Prasarana TIK
   - ✓ Data *center*/*Data Recovery Center*
   - ✓ Bandwidth dan IP address
   - ✓ Jaringan WAN/MAN/LAN
   - ✓ Sistem Pengamanan
5. Perencanaan
   - ✓ Perencanaan induk, team dan mekanisme perencanaan
   - ✓ Kebutuhan dasar e-*government* di setiap SKPD selain Dinas Kominfo
6. Kebijakan: Regulasi dan SOP
7. Kelembagaan:
   - ✓ Pimpinan SKPD sebagai pengarah
   - ✓ Kelompok kerja pengelolaan sistem
   - ✓ Kelompok kerja pengelolaan sarana dan prasarana
   - ✓ Anggaran
8. Sarana dan Prasarana TIK
   - ✓ LAN dan switch
   - ✓ Server aplikasi
   - ✓ PC terminal

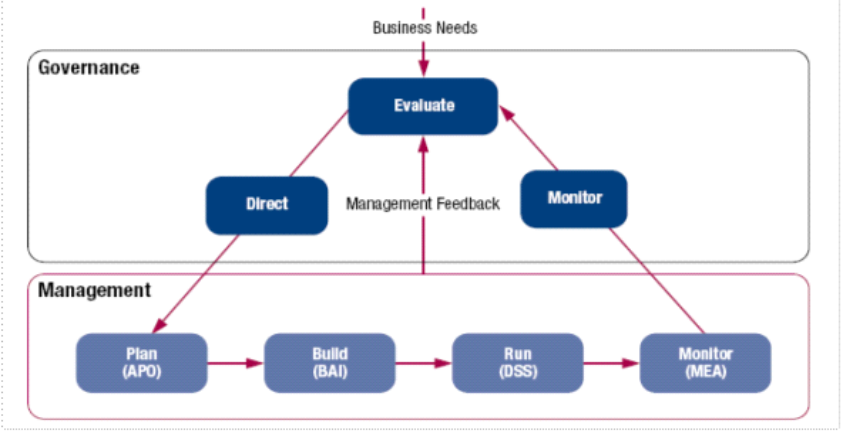
9. Aplikasi e-*government*
   - ✓ Aplikasi proses birokrasi dan pengolahan data SKPD
   - ✓ Aplikasi layanan masyarakat
   - ✓ Aplikasi sistem pelaporan pimpinan
   - ✓ Bantuan pengambilan keputusan
10. Perencanaan
11. Anggota perencana e-*government* Kota

4.2 Tata Kelola TIK Berbasis COBIT

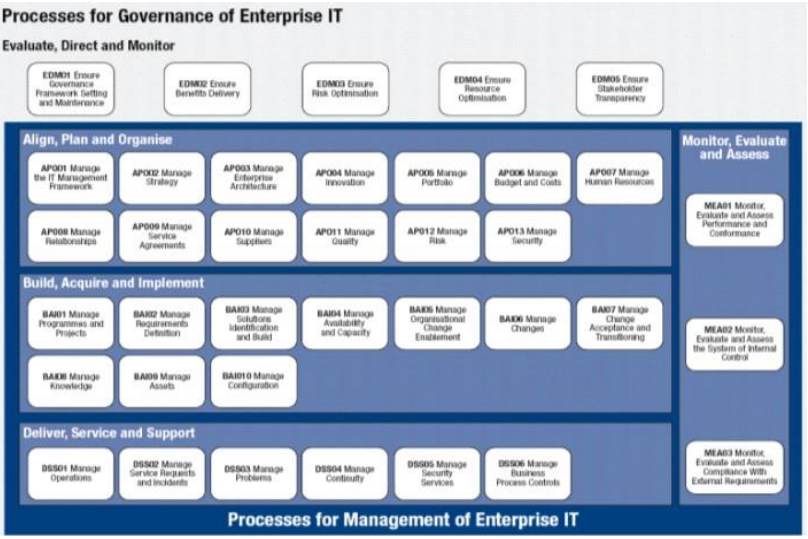
Pemangku Kepentingan	Instansi	Unit Kerja	Pelaksana
			
DPRD Masyarakat	Pemko	Kantor Kominfo	Manajemen Data Pengembangan Aplikasi
Menentukan regulasi Menentukan kebutuhan Menetapkan target Memberikan anggaran Kontrol dan monitoring	Melaksanakan program berdasarkan regulasi, dan target yg telah ditetapkan sesuai anggaran tersedia Menetapkan kegiatan berdasarkan program	Melaksanakan kegiatan berdasarkan pengarahan pimpinan Membagi pekerjaan sesuai komptensinya dan memberikan pengarahan teknis	Melaksanakan pekerjaan sesuai pembagian kerjanya Memberikan laporan dan hasil pelaksanaan pekerjaan

	Memberi pengarahan tujuan, sasaran dan target Kontrol dan monitoring Memberikan laporan program secara berkala	Menerima laporan dan hasil kegiatan Memberikan laporan kegiatan sesuai program yg telah didtetapkan	

Pembagian kerja bidang Teknologi Informasi



Gambar 4.1. Tata kelola TIK



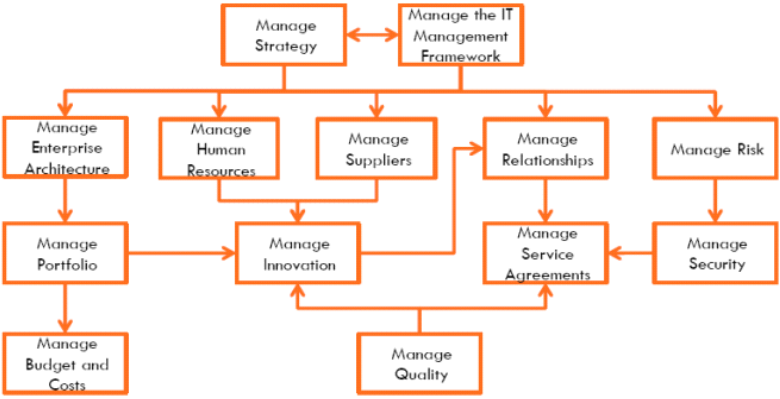
Gambar 4.2. Bisnis Proses pengelolaan TIK

IT Evaluate, Direct, Monitor (EDM)

1. Memastikan Pengaturan Kerangka Tata Kelola Dan Pemeliharaan
   - ✓ Melakukan evaluasi tata kelola sistem
   - ✓ Melakukan pengarahan tata kelola sistem
   - ✓ Melakukan monitoring tata kelola sistem
2. Memastikan Manfaat Hasil Kegiatan
   - ✓ Melakukan evaluasi nilai hasil kegiatan
   - ✓ Melakukan pengarahan nilai hasil kegiatan
   - ✓ Melakukan Monitoring nilai hasil kegiatan
3. Memastikan Optimasi Pengendalian Resiko
   - ✓ Melakukan evaluasi pengendalian resiko
   - ✓ Melakukan pengarahan pengendalian resiko
   - ✓ Melakukan monitoring pengendalian resiko
4. Memastikan Optimasi Pengendalian Sumber Daya
   - ✓ Melakukan evaluasi pengendalian sumber daya

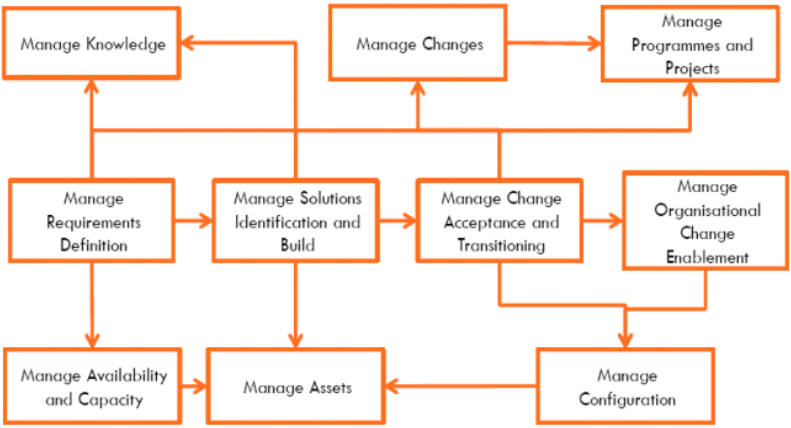
- ✓ Melakukan pengarahan pengendalian sumber daya
- ✓ Melakukan monitoring pengendalian sumber daya

5. Memastikan Sistem Pelaporan yang Transparan
   - ✓ Melakukan evaluasi sistem pelaporan pada pemangku kepentingan
   - ✓ Melakukan pengarahan sistem pelaporan dan koordinasi
   - ✓ Melakukan monitoring dan koordinasi
   - ✓ Keselarasan, perencanaan, dan pengaturan
6. Mengelola Kerangka Pikir Tata Kelola TIK
7. Mengelola Strategi
8. Mengelola *Enterprise Architecture*
9. Mengelola Inovasi
10. Mengelola Portofolio
11. Mengelola Anggaran dan Biaya
12. Mengelola Sumber Daya Manusia
13. Mengelola Hubungan/Koordinasi/Sinkronisasi
14. Mengelola Perjanjian Layanan
15. Mengelola Pemasok/Pihak Ketiga/Mitra/Vendor
16. Mengelola Kualitas
17. Mengelola Risiko
18. Mengelola Keamanan Sistem



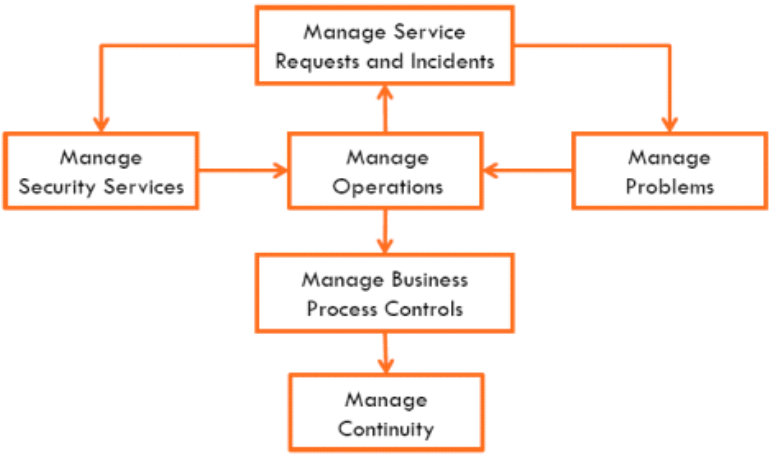
Gambar 4.3. Proses Bisnis TIK level 1

1. Pengembangan, Pengadaan, dan Pengoperasian
   - ✓ Mengelola Program dan Proyek
   - ✓ Mengelola Persyaratan Definition
   - ✓ Mengelola Solusi Identifikasi dan Pengembangan
   - ✓ Mengelola Ketersediaan dan Kapasitas
   - ✓ Mengelola Perubahan Organisasi Pemberdayaan
   - ✓ Mengelola Perubahan
   - ✓ Mengelola Perubahan Penerimaan dan Transisi
   - ✓ Mengelola Pengetahuan
   - ✓ Mengelola Aset
   - ✓ Mengelola Konfigurasi



Gambar 4.4. Proses Bisnis Pengembangan, Pengadaan, dan Pengoperasian

2. Memberikan hasil kegiatan, Pelayanan dan Dukungan
   - ✓ Mengelola Operasional.
   - ✓ Mengelola Permintaan Layanan dan penanganan Insiden.
   - ✓ Mengelola Permasalahan.
   - ✓ Mengelola Keberlanjutan Sistem.
   - ✓ Mengelola Keamanan Informasi.
   - ✓ Mengelola Proses Bisnis Kontrol.



Gambar 4.5. Proses Bisnis *Result Service and Support*

3. Memantau, Evaluasi dan Menilai
   - ✓ Memantau, Evaluasi dan Menilai Kinerja dan Kesesuaian.
   - ✓ Monitor, Evaluasi dan Menilai Sistem Pengendalian Intern.
   - ✓ Memantau, Evaluasi dan Menilai Kepatuhan dengan Persyaratan Eksternal.

4.3 Best Practice Implementasi TIK

Standar Umum Perencanaan Strategis TIK

1. Perencanaan strategis TI dibutuhkan untuk mengelola sumber daya IT yang selaras dengan prioritas dan kebijakan strategis.
2. Manajemen Nilai TIK (IT *Value Management*):
   a. Harus ada kerjasama antara TIK dan bisnis untuk memastikan bahwa portofolio terhadap investasi di bidang IT (IT-*enabled investments*) yang berisi program-program yang sesuai dengan arah dan tujuan pembangunan kota.
   b. Proses-proses TIK harus memberikan komponen-komponen TIK yang efektif dari program-program Pemkot dan peringatan dini dari penyimpangan-penyimpangan, termasuk mengenai biaya, jadwal atau fungsionalitas, yang dapat berdampak pada hasil/*outcome* yang diharapkan dari program.
   c. Layanan-layanan TIK harus dilaksanakan sesuai dengan SLA yang adil dan dapat dilaksanakan. Akuntabilitas untuk merealisasikan manfaat dan mengendalikan biaya harus dengan jelas dibebankan dan dimonitor.
   d. Harus ditetapkan evaluasi atas kasus-kasus bisnis secara adil, transparan, dapat diulang dan dapat dibandingkan, termasuk nilai keuangan (*financial worth*), resiko karena tidak diadakannya suatu kemampuan dan resiko karena tidak terealisasinya manfaat yang diharapkan.
3. Keselarasan TIK-Bisnis (*Business*-IT *Alignment*)
   a. Harus ada proses-proses pendidikan/*learning* dua arah dan keterlibatan timbal balik dalam

perencanaan strategis untuk mencapai integrasi dan keselarasan visi pembangunan dan pengembangan TIK.

b. Penilaian Kemampuan dan Kinerja Saat Ini (*Assessment of Current Capability and Performance*)
c. Harus dilakukan penilaian atas kemampuan dan kinerja dari solusi dan layanan saat ini untuk menetapkan suatu dasar terhadap kebutuhan mendatang mana yang dapat dibandingkan.
d. Harus didefinisikan kinerja berdasarkan kontribusi TIK pada, fungsionalitas, stabilitas, biaya, kekuatan, dan kelemahan.

4. Rencana Strategis TIK (IT *Strategic Plan*)
   a. Harus disusun suatu rencana strategis, dengan bekerjasama dengan *stakeholder* yang relevan, yang mendefinisikan bagaimana sasaran-sasaran TIK akan memberikan kontribusi pada tujuan-tujuan strategis Pemkot serta biaya-biaya dan resiko-resiko yang terkait.
   b. Rencana ini harus mencakup bagaimana TIK akan mendukung program-program investasi IT-enabled, layanan-layanan TIK, dan aset-aset TIK.
   c. TIK harus mendefinisikan bagaimana tujuan-tujuan akan dicapai, ukuran-ukuran yang digunakan dan prosedur-prosedur untuk mendapatkan sign-off dari stakeholder.
   d. Rencana strategis TIK harus mencakup anggaran investasi operasi, sumber pendanaan, strategi pengadaan (*sourcing*), strategi akuisisi, dan persyaratan-persyaratan dan regulasi.

e. Rencana strategis harus cukup detil sehingga memungkinkan disusunnya rencana taktis.

5. Rencana Taktis TIK (IT *Tactical Plan*)
   a. Harus dibuat suatu portofolio dari rencana-rencana taktis TIK yang diturunkan dari rencana stratejik TIK. Rencana-rencana taktis TIK tersebut harus membahas program investasi-investasi IT, layanan-layanan TIK, dan aset-aset TIK. Rencana-rencana taktis tersebut harus menjabarkan inisiatif-inisiatif TIK yang diperlukan, kebutuhan-kebutuhan sumber daya, dan bagaimana penggunaan sumber daya dan realisasi manfaatnya akan dikelola dan dimonitor.
   b. Rencana-rencana taktis tersebut harus cukup detil sehingga memungkinkan pendefinisian rencana-rencana proyek. Kumpulan rencana-rencana taktis dan inisiatif-inisiatif tersebut harus secara aktif dikelola dengan analisis portofolio layanan-layanan dan proyek-proyek.
   c. Manajemen Portofolio (IT *Portofolio Management*): Portofolio dari program-program untuk mencapai tujuan-tujuan bisnis tertentu harus dikelola secara aktif dengan mengenali, mendefinisikan, mengevaluasi, menentukan prioritas, memilih, menginisiasi, mengelola dan mengendalikan program-program. lni harus mencakup mengklarifikasikan hasil-hasil bisnis yang diinginkan, memastikan bahwa tujuan-tujuan program mendukung pencapaian hasil-hasil tersebut, memahami seluruh ruang lingkup upaya yang diperlukan untuk mencapai hasil-hasil

tersebut, menetapkan akuntabilitas secara jelas dengan ukuran-ukuran yang. mendukung, mendefinisikan proyek-proyek dalam program, mengalokasikan sumber daya dan pendanaan, mendelegasikan wewenang, dan mempersiapkan proyek-proyek yang diperlukan saat peluncuran program.

Standar Umum Identifikasi Solusi

1. Analisa kebutuhan atas aplikasi baru atau fungsi sebelum pembuatan dan pengembangan aplikasi harus dapat dijamin kebenarannya sesuai dengan tingkat dan pembangunan kota, eksekusi dengan memper-hitungkan tingkat resiko dan analisa efisiensi, dan kesimpulan dan keputusan final untuk membuat atau membeli.
2. Seluruh langkah ini digunakan untuk menjaga agar keputusan terhadap solusi atas kebutuhan IT dapat dioptimalkan pembiayaannya dan memungkinkan solusi yang dibuat dapat diimplementasikan.
3. Untuk mengidentifikasikan standar umum identifikasi solusi, maka pendefinisian dan pemeliharaan kebutuhan-kebutuhan fungsional dan teknis perlu pengenalan, penentuan prioritas, membuat spesifikasi dan menyepakati kebutuhan-kebutuhan fungsional dan teknis yang mencakup keseluruhan ruang lingkup dari semua inisiatif yang diperlukan untuk mencapai hasil/*outcome* yang diharapkan dari program investasi di bidang IT.
4. Harus didefinisikan dan diimplementasikan suatu prosedur pendefinisian dan pemeliharaan juga suatu

repository kebutuhan-kebutuhan yang sesuai dengan ukuran, kompleksitas, tujuan-tujuan, dan resiko-resiko dari inisiatif kegiatan yang sedang dipertimbangkan untuk dilaksanakan. Prosedur ini harus mempertimbangkan layanan Pemkot, arah strategis, rencana-rencana strategis dan taktis, proses-proses bisnis dan TI yang *inhouse* maupun di-*outsource*, persyaratan regulatori yang sedang muncul, keterampilan-keterampilan dan kompetensi-kompetensi orang, struktur, dan *enabling technology*. Harus dikonfirmasikan bahwa semua kebutuhan stakeholder, termasuk kriteria penerimaan yang relevan, diperhatikan, dimengerti, diprioritaskan dan dicatat sedemikian rupa sehingga mudah dipahami oleh stakeholder, sponsor-sponsor bisnis dan personil implementasi teknis.

5. Harus dikonfirmasikan bahwa kebutuhan-kebutuhan fungsional dan teknis diperhatikan, dimengerti dan ditentukan prioritasnya, mencakup aspek-aspek tentang:
   - ✓ Kontinuitas
   - ✓ Kepatuhan pada hukum dan peraturan
   - ✓ Kinerja
   - ✓ Keandalan
   - ✓ *Auditability*
   - ✓ Keamanan dan manajemen resiko
   - ✓ Ergonomika
   - ✓ *Operability* dan *usability*
   - ✓ *Safety*
   - ✓ Dokumentasi (*end user*, operasi, penggelaran, konfigurasi)

6. Analisis Resiko:
   a. Resiko-resiko terkait dengan pengembangan e-*government* dan rancangan solusi harus dikenali, didokumentasikan, dan dianalisa sebagai bagian dari proses penyusunan kebutuhan.
   b. Harus digunakan pendekatan holistik untuk analisis resiko, untuk memastikan bahwa teknologi dan proyek dikenali dengan semestinya, diperiksa, dinilai, dan dimengerti oleh semua stakeholders.
   c. Dampak dari proyek (pengembangan atau akuisisi, implementasi, operasi, pemberhentian, dan disposal) pada profit resiko Pemkot dan ancaman-ancaman pada integritas data, keamanan, ketersediaan, privasi, dan kepatuhan pada hukum dan peraturan, harus dipertimbangkan sebagai bagian dari analisis resiko.
   d. Aktivitas-aktivitas mitigasi resiko harus dipertimbangkan sebagai bagian dari definisi dari solusi-solusi yang mungkin.

7. Kajian Kelayakan dan Formulasi Langkah-Langkah Selanjutnya
   a. Kajian kelayakan dan formulasi langkah-langkah selanjutnya harus dapat dibuat suatu kajian kelayakan yang memeriksa kemungkinan meng-implementasikan kebutuhan.
   b. Manajemen e-*government*, dengan dukungan fungsi TIK, harus menilai kelayakan dan tindakan-tindakan alternatif dan membuat rekomendasi.
   c. Harus dilakukan kajian kelayakan yang dengan jelas dan ringkas menjabarkan alternatif- alternatif yang akan memenuhi kebutuhan bisnis dan kebutuhan

fungsional dengan suatu evaluasi kelayakan teknis dan ekonomis. Identifikasi tindakan yang diperlukan untuk mengadakan atau membangun, dan perhatikan keterbatasan-keterbatasan ruang lingkup dan atau waktu dan atau anggaran.

d. Langkah-langkah alternatif harus dikaji bersama semua stakeholder, dan dipilih satu yang paling sesuai berdasarkan kriteria kelayakan, termasuk resiko-resiko dan biaya.
e. Tindakan-tindakan yang dipilih harus diterjemahkan menjadi suatu rencana pengembangan atau akuisisi yang mengidentifikasi sumber daya yang akan digunakan dan tahapan-tahapan yang memerlukan keputusan dilaksanakan atau tidak dilaksanakan.

8. Kebutuhan-kebutuhan dan Keputusan Kelayakan dan Persetujuan
   a. Kebutuhan-kebutuhan dan keputusan kelayakan dan persetujuan harus diverifikasi bahwa prosesnya mensyaratkan persetujuan manajemen dan tanda tangannya pada laporan- laporan kebutuhan fungsional dan teknis dan kajian kelayakan, pada tahapan-tahapan yang ditentukan sebelumnya.
   b. Manajemen perlu membuat keputusan akhir tentang solusi yang dipilih dan pendekatan akuisisinya.
   c. Diperlukan penandatanganan (sign-off) dari manajemen dan otoritas teknis atas pendekatan-pendekatan yang diusulkan. Dapatkan juga umpan

balik yang memerlukan analisis kelayakan lebih lanjut.

d. Pada akhir setiap tahap yang penting dilakukan terhadap kualitas untuk menilai hasil-hasil pekerjaan dibanding kriteria penerimaan awal. Manajemen dan stakeholder lain harus menandatangani persetujuan setiap telaah kualitas yang berhasil.

Standar Umum Tentang Pengadaan dan Pemeliharaan Software

1. Rancangan Umum
   a. Kebutuhan-kebutuhan bisnis perlu diterjemahkan menjadi suatu rancangan umum (*high-level design*), dengan memperhatikan arah teknologi dan arsitektur informasi Pemkot.
   b. Spesifikasi rancangan harus mendapat persetujuan manajemen untuk memastikan bahwa rancangan umum tersebut menjawab kebutuhan-kebutuhannya. Jika timbal perbedaan teknis dan logis yang signifikan selama pengembangan atau pemeliharaan, maka harus dilakulan asesmen ulang.
2. Rancangan Detil:
   a. Harus dibuat/disusun rancangan detil dan kebutuhan-kebutuhan aplikasi software.
   b. Harus didefinisikan kriteria penerimaan dari kebutuhan-kebutuhan tersebut. Kebutuhan-kebutuhan tersebut perlu harus mendapat persetujuan untuk memastikan bahwa mereka terhubung dengan rancangan umum.

c. Harus dilakukan penilaian ulang jika terjadi perbedaan teknis dan logis selama pengembangan dan pemeliharaan.
d. Kendali Aplikasi dan Auditabiltas: Harus diterapkan kendali-kendali bisnis, bilamana sesuai, menjadi kendali-kendali aplikasi terotomasi sedemikian sehingga proses akurat, lengkap, tepat waktu, sah, dan dapat diaudit.
e. Keamanan dan Ketersediaan Aplikasi: Persyaratan-persyaratan keamanan dan ketersedian aplikasi harus ditangani sebagai jawaban atas resiko-resiko yang diketahul dan selaras dengan klasifikasi data, arsitektur informasi, arsitektur keamanan informasi, dan toleransi resiko Pemkot.
f. Konfigurasi dan Implementasi Aplikasi yang Diakuisisi: Aplikasi yang diakuisisi harus dikonfigurasikan dan diimplementasikan untuk memenuhi tujuan-tujuan bisnis.
g. Upgrade Besar pada Sistem *Existing*: Dalam hal perubahan-perubahan besar pada sistem existing yang mengakibatkan perubahan signifikan pada rancangan yang ada dan atau fungsionalitas, harus dilakukan proses serupa sebagaimana digunakan untuk pengembangan sistem baru.

3. Pengembangan Software Aplikasi:
   a. Harus dipastikan bahwa fungsionalitas yang diotomasikan dikembangkan sesuai dengan spesifikasi desain, standar-standar pengembangan dan dokumentasi, persyaratan-persyaratan *quality assurance* (QA), dan standar-standar persetujuan.

b. Harus dipastikan bahwa aspek-aspek hukum dan kontraktual diketahui dan ditangani untuk software aplikasi yang dikembangkan oleh pihak ketiga.
c. Penjaminan Mutu Software: Harus disusun, diberikan sumber daya dan dilaksanakan suatu rencana penjaminan mutu (*quality assurance*) untuk mendapatkan kualitas seperti dinyatakan dalam definisi kebutuhan dan kebijakan-kebijakan serta prosedur-prosedur kualitas Pemkot.
d. Manajemen kebutuhan-kebutuhan Aplikasi: Harus ada penelusuran atas setiap kebutuhan (termasuk semua kebutuhan yang ditolak) selama disain, pengembangan dan implementasi, dan perubahan-perubahan yang disetujui metafui suatu proses manajemen perubahan yang ditetapkan.
e. Pemeliharaan Software Aplikasi: Harus disusun suatu strategi dan rencana untuk pemeliharaan software aplikasi.

Standar Umum Pengelolaan Tingkat Layanan

1. Kerangka Kerja Manajemen Tingkat Layanan:
   a. Harus ada suatu kerangka kerja yang memberikan suatu proses manajemen tingkat layanan yang formal diantara SKPD TIK Pemkot dengan pengguna.
   b. Kerangka-kerja ini harus menjaga keselarasan dengan kebutuhan-kebutuhan dan prioritas-prioritas bisnis dan memfasilitasi pemahaman bersama di antara SKPD TIK Pemkot dan pengguna.
   c. Kerangka kerja harus mencakup proses-proses untuk mendefinisikan kebutuhan-kebutuhan

layanan, definisi-definisi layanan, SLA, OLA dan sumber-sumber pendanaan. Atribut-atribut ini harus diorganisir dalam suatu katalog layanan. Kerangka-kerja tersebut harus mendefinisikan struktur organisasional untuk manajemen tingkat layanan, mencakup peran-peran, tugas-tugas dan tanggung-jawab dari penyedia layanan internal dan eksternal dan pengguna.

2. Definisi Layanan-layanan:
   a. Harus disusun definisi dasar dari layanan-layanan TIK tentang karakteristik layanan dan kebutuhan-kebutuhan kinerja.
   b. Harus dipastikan bahwa definisi-definisi ini diorganisir dan disimpan dengan menerapkan pendekatan portofolio katalog layanan.

3. *Service Level Agreement*:
   a. Harus ada *Service Level Agreement* (SLA), yang didefinisikan dan disepakati oleh pengguna dan TIK, untuk semua layanan TIK yang penting, yang didasarkan pada kebutuhan-kebutuhan pengguna dan kemampuan TIK. Perjanjian ini harus mencakup
   b. Komitmen pengguna; kebutuhan dukungan layanan, metrik-metrik kualitatif dan kuantitatif untuk mengukur layanan yang disepakati para stakeholder, pendanaan dan pengaturan masalah komersial; dan peran dan tanggung jawab, termasuk pengawasan SLA.
   c. Perlu dipertimbangkan hal-hal seperti ketersediaan, keandalan, kinerja, kapasitas

pengembangan, tingkat dukungan, perencanaan kontinuitas, keamanan dan keterbatasan permintaan.

d. *Operating Level Agreement*: Harus ada *Operating Level Agreement* (OLA) yang menjabarkan bagaimana layanan-layanan akan diberikan untuk mendukung SLA secara optimal. OLA tersebut harus menetapkan proses-proses teknis dengan menggunakan kata-kata dan istilah-istilah yang mudah dimengerti oleh TIK dan dapat mendukung beberapa SLA.

4. Pemantauan dan Pelaporan SLA:
   a. Kriteria kinerja tingkat layanan harus dipantau secara terus menerus. Pencapalan tingkat layanan harus dilaporkan dalam bentuk yang mudah dimengerti oleh para stakeholder.
   b. Statistika pantauan harus dianalisa dan ditangani untuk mengenali kecenderungan-kecenderungan negatif maupun positif, untuk tiap layanan maupun secara keseluruhan.
   c. Review dari SLA dan Kontrak: SLA dan kontrak-kontrak pedukung (*underpinning contracts*) dengan penyedia layanan internal maupun eksternal harus ditelaah secara regular untuk memastikan bahwa kontrak-kontrak tersebut efektif, up-to-date, dan bahwa perubahan-perubahan kebutuhan telah diperhitungkan.

Standar Umum Rencana Kontinuitas Bisnis

1. Kerangka Kerja Kontinuitas:
   a. Harus dikembangkan suatu kerangka kerja kontinuitas TIK untuk mendukung manajemen kontinuitas bisnis bagi keseluruhan Pemkot, dengan menggunakan suatu proses yang konsisten.
   b. Kerangka-kerja ini bertujuan membantu penentuan kelenturan prasarana yang dibutuhkan dan mendorong pengembangan rencana-rencana kontinjensi TIK dan pemulihan bencana.
   c. Kerangka kerja tersebut harus menangani struktur organisasional untuk manajemen kontinuitas, yang mencakup peran-peran, tugas-tugas dan tanggung-jawab dari penyedia layanan internal maupun eksternal, manajemen dan penggunanya, dan proses-proses perencanaan untuk yang menyusun aturan-aturan dan struktur-struktur untuk mendokumentasikan, menguji dan melaksanakan rencana-rencana kontinjensi TIK dan pemulihan bencana.
   d. Rencana tersebut juga harus menangani hal-hal seperti identifikasi sumber daya kritis, mencatat ketergantungan pokok, pemantauan dan pelaporan ketersediaan sumber daya kritis, alternatif pemrosesan, dan prisnsip-prinsip dari *backup* dan *recovery.*

2. Rencana Kontinuitas TIK
   a. Harus dikembangkan rencana kontinuitas TIK berdasar pada kerangka-kerja tersebut dan dirancang untuk mengurangi dampak dari suatu

gangguan besar pada proses-proses dan fungsi-fungsi bisnis utama.

b. Rencana tersebut harus didasarkan pada pemahaman resiko kegiatan yang potensial dan membahas kebutuhan-kebutuhan akan kelenturan, pemrosesan alternatif dan kemampuan pemulihan dari semua layanan TIK.
c. Rencana tersebut juga harus mencakup pedomam penggunaan, peran dan tanggung-jawab, prosedur-prosedur, proses-proses komunikasi, dan pendekatan pengujian.

3. Sumber Daya TIK Kritis (Critical ICT Resources)
   a. Dalam rencana kontinuitas TIK, untuk membangun kelenturan dan menetapkan prioritas dalam situasi pemulihan, perhatian harus ditujukan pada hal-hal yang yang dinyatakan sebagai paling kritis. Harus dihindari pengalihan pada hal-hal yang tidak terlalu kritis dan harus dipastikan bahwa tanggapan dan pemulihan selaras dengan kebutuhan layanan pemkot yang diprioritaskan, dan memastikan bahwa biaya-biaya dijaga pada tingkat yang dapat diterima dan sesuai dengan persyaratan-persyaratan kontraktual dan regulasi.
   b. Harus diperhatikan kebutuhan-kebutuhan akan kelenturan, respond dan pemulihan untuk tingkat-tingkat berbeda, misalnya: satu sampai empat jam, empat sampai 24 jam, lebih dari 24 jam, dan periode-periode aktifitas pemkot yang kritis.

4. Pemeliharaan Rencana Kontinuitas TIK
    a. Manajemen TIK sebaiknya menyusun dan melaksanakan prosedur-prosedur pengendalian perubahan untuk memastikan bahwa rencana kontinuitas TI tetap up-to-date dan secara berlanjut mencerminkan kebutuhan layanan pemkot.
    b. Perubahan-perubahan prosedur dan tanggung jawab harus dikomunikasikan dengan jelas dan tepat waktu.

5. Pengujian Rencana Kontinuitas TIK
    a. Rencana kontinuitas TIK harus diuji secara reguler untuk memastikan bahwa sistem-sistem TI dapat dipulihkan secara efektif, kelemahan-kelemahan ditanggulangi dan recana tersebut tetap relevan. Pengujian ini memerlukan persiapan cermat, dokumentasi, pelaporan hasil-hasil pengujian, dan sesuai pelaksanaan rencana aksi sesuai hasil pengujian.
    b. Harus dipertimbangkan seberapa jauh pengujian dari pemulihan suatu aplikasi sampai skenario pengujian dari ujung ke ujung dan pengujian vendor terpadu/terintegrasi.

6. Pelatihan Rencana Kontuitas TIK
    a. Semua pihak berkepentingan harus diberikan sesi-sesi pelatihan regular tentang prosedur-prosedur dan peran-peran dan tanggung-jawab mereka jika terjadi suatu insiden atau bencana.
    b. Pelatihan harus diverifikasi dan diperbaiki sesuai dengan hasil pengujian kontijensi.

7. Distribusi Rencana Kontinuitas TIK
   a. Rencana kontinuitas TIK harus didistribusikan secara tepat dan aman dan tersedia bagi semua pihak yang diberi wewenang bilamana diperlukan.
   b. Harus diperhatikan bahwa rencana-rencana dapat diakses dalam semua skenario bencana.

8. Pemulihan dan Dimulai-Kembali Layanan TIK
   a. Harus ada rencana aksi untuk periode dimana layanan TIK sedang dipulihkan dan mulai memberikan layanan kembali. Ini dapat mencakup aktivasi dari situs backup, inisiasi pemrosesan alternatif, komunikasi *stakeholder* dan pengguna, dan prosedur-prosedur resumption.
   b. Harus dipastikan bahwa pengguna bisnis memahami waktu pemulihan layanan TIK dan investasi teknologi yang diperlukan untuk mendukung pemulihan bisnis dan kebutuhan-kebutuhan *resumption*.

9. *Off-Site Back-Up Storage*
   a. Semua backup media, dokumentasi dan sumber daya lain yang kritis untuk keperluan rencana-rencana pemulihan TI dan kontinuitas bisnis, harus disimpan di lokasi *offsite*. Isi dari backup storage harus ditentukan bersama oleh pemilik proses bisnis dan personil TIK.
   b. Manajemen dari *offsite storage* harus tanggap pada kebijakan klasifikasi data dan praktek-praktek media penyimpanan Pemkot.
   c. Manajemen TIK harus memastikan bahwa pengaturan offsite dinilai secara periodik, paling

kurang tiap tahun, diperiksa isinya, proteksi lingkungan dan keamanannya. Harus dipastikan kompatibilitas hardware dan software untuk menyimpan arsip data, dan secara periodik melakukan pengujian dan menyegarkan arsip data.

10. *Post-Resumption Review*

Harus ditentukan apakah manajemen TIK telah menetapkan prosedur untuk menilai kecukupan dari rencana dalam hubungannya dengan keberhasilan resumption dari fungsi TIK setelah bencana, dan mengupdate rencana tersebut sebagaimana mestinya.

Standar Umum Keamanan TIK

1. Pengelolaan Keamanan TIK: Keamanan TIK harus dikelola pada tingkat yang tepat setinggi-mungkin dalam organisasi, sehingga manajemen tindakan-tindakan keamanan sesuai dengan kebutuhan bisnis.
2. Rencana Keamanan TIK:
   a. Persyaratan-persyaratan bisnis, resiko, dan kepatuhan harus diterjemahkan kedalam rencana keamanan TIK secara keseluruhan, dengan memperhatikan prasarana TIK dan budaya keamanan.
   b. Harus dipastikan bahwa rencana tersebut diterapkan dalam kebijakan-kebijakan dan prosedur-prosedur keamanan bersama-sama dengan investasi yang tepat pada layanan-layanan, personil, software dan hardware.

c. Kebijakan-kebijakan dan prosedur-prosedur keamanan harus dikomunikasikan kepada *stakeholder* dan pengguna.

3. Manajemen Identitas
   a. Harus dipastikan bahwa semua pengguna (internal, eksternal, temporer) dan aktivitas mereka pada sistem-sistem TIK (aplikasi bisnis, lingkungan TIK, operasi sistem, pengembangan dan pemeliharaan) diidentifikasi secara unik. Identitas pengguna harus diaktifkan dengan mekanisme-mekanisme otentikasi.
   b. Harus dipastikan bahwa hak akses pengguna pada sistem dan data sesuai dengan kebutuhan bisnis yang didefinisikan dan didokumentasikan dan persyaratan jabatan dilampirkan pada identitas pengguna.
   c. Harus dipastikan bahwa hak akses pengguna diminta oleh *user management*, disetujui oleh pemilik sistem dan diimplementasikan oleh penanggung-jawab keamanan. ldentitas dan hak akses harus dipelihara dalam suatu central *repository*.
   d. Harus digelar aturan-aturan prosedural dan teknis, dan dijaga tetap up-to-date untuk menetapkan identifikasi pengguna, menerapkan otentikasi, dan meng-*enforce* hak akses.

4. Manajemen *User Account*
   a. Harus disusun suatu kumpulan prosedur manajemen akun pengguna (*user account management*) untuk menangani permintaan,

pembuatan, pengeluaran, penangguhan, modifikasi dan penutupan akun pengguna dan hak-hak terkaitnya. Masukkan suatu prosedur persetujuan menggambarkan pemilik data atau sistem memberikan hak akses.

b. Prosedur-prosedur ini harus berlaku untuk semua pengguna, termasuk administrator (pengguna dengan hak istimewa) dan pengguna internal maupun eksternal, untuk pemakaian normal atau kasus-kasus emergensi.
c. Hak-hak dan kewajiban-kewajiban atas akses pada sistem dan informasi Pemkot harus diatur secara kontraktual untuk semua jenis pengguna.
d. Harus dilakukan telaah manajemen atas semua akun dan hak-haknya.
e. Security Testing, Surveillance, and Monitoring
f. Harus dilakukan pengujian dan pemantauan atas implementasi keamanan TIK secara reguler.
g. Keamanan TIK harus diakreditasi ulang pada waktunya untuk memastikan bahwa baseline keamanan informasi Pemkot tetap terjaga.
h. Harus ada fungsi *logging* dan *monitoring* yang memungkinkan pencegahan dan atau deteksi dini dan pelaporan atas aktivitas-aktivitas tidak biasa dan atau abnormal, pada waktunya, yang mungkin perlu ditanggulangi.

5. Definisi Insiden Keamanan: Karakteristik-karakteristik insiden keamanan potensial harus didefinisikan dan dikomunikasikan dengan jelas sehingga dapat diklasifikasikan secara semestinya

dan ditangani oleh proses manajemen insiden dan problem.

6. Proteksi atas Teknologi Keamanan: Teknologi terkait keamanan harus dibuat tahan terhadap tampering, dan dokumentasi keamanan tidak boleh diungkap secara tak perlu.
7. Manajemen Kunci Kriptografi: Harus disusun kebijakan-kebijakan dan prosedur-prosedur untuk mengorganisir pembuatan, perubahan, pembatalan, destruksi, distribusi, sertifikasi, penyimpanan, pemasukan, penggunaan dan pengarsipan dari kunci-kunci kriptografi untuk memastikan perlindungan kunci dari modifikasi dan pengungkapan tidak sah.
8. Pencegahan, Deteksi, dan Koreksi Malicious Software: Harus disusun tindakan-tindakan pencegahan, detektif dan korektif (terutama *security patches* dan virus control yang up-to-date) diseluruh Pemkot untuk melindungi sistem informasi dan teknologi terhadap malware (misal virus, *worms*, *spyware*, *spam*).
9. Keamanan Jaringan: Harus digunakan teknik-teknik keamanan dan prosedur-prosedur manajemen terkait (misalnya: *firewall, security appliance*, segementasi jaringan, deteksi instruksi) untuk memberikan hak akses dan mengendalikan aliran informasi dari dan ke jaringan.
10. Pertukaran Data Sensitif: Pertukaran data transaksi yang sensitif harus dilakukan melalui suatu trusted path atau medium dengan kendali-kendali untuk memberikan otentisitas dari

konten: *proof of submission, proof of receipt*, dan non-*repudiation of origin.*

Standar Umum Pendidikan dan Pelatihan User

1. Identifikasi kebutuhan pendidikan dan pelatihan
2. Menetapkan dan secara reguler mengupdate suatu kurikulum untuk setiap kelompok pegawai target dengan memperhatikan:
   a. Kebutuhan dan strategi bisnis yang ada maupun yang akan datang
   b. Nilai dari informasi sebagai suatu aset
   c. Nilai-nilai korporat (nilai etikal, budaya pengendalian dan keamanan, dsb.)
   d. Implementasi dari prasarana TI dan software (misalnya: *package* dan aplikasi) baru
   e. Keterampilan-keterampilan sekarang dan yang akan datang, profil kompetensi, dan kebutuhan akan sertifikasi dan atau kredensial maupun reakreditasi yang diperlukan
   f. Metode penyampaian (misalnya: *classroom* dan *web-based*), ukuran target grup, aksesabilitas dan waktu.
3. Pelaksanaan pendidikan dan pelatihan
   a. Berdasarkan kebutuhan-kebutuhan pendidikan dan pelatihan yang diketahui, harus diidentifikasi kelompok-kelompok target beserta anggota-anggotanya, mekanisme penyampaian yang efisien, pengajar, instruktur, dan mentor.
   b. Harus ditunjuk pelatih-pelatih dan mengorganisasikan sesi-sesi training tepat waktu. Harus dicatat pendaftaran (termasuk *prerequisite*), kehadiran dan evaluasi kinerja sesi pelatihan.

4. Evaluasi pelatihan yang diterima
   a. Ketika selesai, harus dievaluasi penyampaian isi pendidikan dan pelatihan dalam hal relevansi, kualitas, efektivitas, retensi dari pengetahuan, biaya dan nilainya (*value*).
   b. Hasil-hasil dari evaluasi tersebut harus dijadikan masukan bagi penyusunan kurikulum yang akan datang dan pelaksanaan dari sesi-sesi *training*.

Standar Umum Pengelolaan Data

a. Kebutuhan Bisnis Akan Pengelolaan Data: Harus diverifikasi bahwa semua data yang diharapkan untuk pemrosesan diterima dan diproses dengan lengkap, akurat dan tepat waktu, dan semua keluaran diserahkan sesuai dengan kebutuhan bisnis. Harus mendukung kebutuhan untuk restart dan pemrosesan ulang.
b. Penyimpanan dan Pengaturan Retensi: Harus didefinisikan dan diterapkan prosedur-prosedur untuk menyimpan data secara efektif dan efisien, retensi dan pengarsipan memenuhi tujuan- tujuan bisnis, kebijakan keamanan Pemkot dan persyaratan regulatori.
c. Sistem Manajemen Pustaka Media: Harus didefinisikan dan diterapkan prosedur-prosedur untuk menjaga suatu persediaan media penyimpan dan pengarsip untuk memastikan integritas dan kegunaannya.
d. Disposal: Harus didefinisikan dan diimplementasikan prosedur-prosedur untuk memastikan bahwa kebutuhan-kebutuhan bisnis

akan perlindungan atas data yang sensitif serta software terpenuhi jika data dan hardware dibuang atau ditransfer.

e. Backup dan pengembalian backup (*restoration*): Harus didefinisikan dan diimplementasikan prosedur-prosedur untuk melakukan backup dan restorasi sistem, aplikasi-aplikasi, data dan dokumentasi, sesuai dengan kebutuhan-kebutuhan bisnis dan rencana kontinuitas.
f. Kebutuhan Keamananan untuk Manajemen Data: Harus didefinisikan dan diimplemetasikan kebijakan-kebijakan dan prosedur-prosedur untuk mengenali dan menerapkan persyaratan-persyaratan keamanan yang berlaku pada penerimaan, pemrosesan, penyimpanan, dan pengeluaran data untuk memenuhi tujuan-tujuan bisnis, kebijakan keamanan Pemkot, dan persyaratan regulatori.

Standar Umum Arsitektur Informasi

1. Model Arsitektur Informasi Enterprise
   a. Harus dibuat dan dipelihara suatu model informasi Pemkot untuk memungkinkan pengembangan aplikasi dan kegiatan-kegiatan pengambilan keputusan, konsisten dengan rencana-rencana TIK seperti dinyatakan dalam Standar Umum Rencana Stratejik TIK.
   b. Model tersebut harus memfasilitasi pembuatan, penggunaan dan sharing informasi oleh pengguna bisnis secara optimal, menjaga integritas dan

fleksibel, fungsional, cost-effective, tepat waktu, aman, dan lentur terhadap kegagalan.

c. Kamus Data dan Aturan Syntax Data: Harus dipelihara suatu kamus data yang mencakup aturan-aturan syntax data. Kamus ini harus memungkinkan penggunaan bersama elemen-elemen data di antara aplikasi-aplikasi dan sistem-sistem, mendorong suatu pemahaman bersama mengenai data di antara TIK dan pengguna bisnis, dan mencegah pembuatan elemen-elemen data yang tidak kompatibel.
d. Skema Klasifikasi Data: Harus ditetapkan suatu skema klasifikasi yang berlaku untuk seluruh Pemkot, berdasar pada sensitivitas dan kritikalitas (misalnya: public, confidential, top secret) dari data. Skema ini harus mencakup detil tentang kepemilikan data, definisi dari tingkat keamanan yang tepat dan kendali-kendali perlindungannya; dan suatu deskripsi ringkas dari kebutuhan retensi dan perusakan, kritikalitas dan sensitivitas. lni harus digunakan sebagai dasar bagi penerapan kendali seperti misalnya kendali akses, pengarsipan, dan enkripsi.
e. Manajemen Integritas: Harus didefinisikan dan diimplementasikan prosedur-prosedur untuk memastikan integritas dan konsistensi dari semua data yang disimpan dalam bentuk elektronik, seperti database, data warehouse, dan arsip data.

Standar Umum Penentuan Arah Teknologi

1. Perencanaan Arah Teknologi:
   a. Harus dianalisa teknologi-teknologi existing dan yang sedang muncul, dan direncanakan ke arah mana teknologi yang tepat untuk merealisasikan strategi TIK dan arsitektur sistem bisnis.
   b. Dalam rencana tersebut, harus diidentifikasi teknologi mana yang berpotensi menciptakan peluang-peluang bisnis.
   c. Rencana tersebut harus membahas arsitektur sistem, arah teknologi, strategi migrasi dan aspek kontijensi dari komponen-komponen infrastruktur.

2. Rencana Infrastruktur Teknologi
   a. Harus disusun dan diperlihara suatu rencana infrastruktur teknologi sesuai dengan rencana-rencana strategis dan taktis TIK.
   b. Rencana tersebut harus didasarkan pada arah teknologi dan mencakup pengaturan kontinjensi dan arahan untuk pengadaan sumber daya teknologi.
   c. Rencana tersebut harus memperhatikan perubahan-perubahan dalam lingkungan kompetitif, skala ekonomi untuk staffing dan investasi sistem informasi, dan peningkatan interoperabilitas dart platform-platform dan aplikasi-aplikasi.
   d. Pemantauan Kecenderungan dan ReguIasi Di Masa Mendatang: Harus ada suatu proses untuk memonitor kecenderungan-kecenderungan sektor bisnis, industri, teknologi, infrastruktur, legal dan lingkungan regulatori. Masukkan konsekuensi dari

kesenderungan-kecenderungan ini dalam penyusunan rencana infrastruktur teknologi TIK.

2. Standar-standar Teknologi
   a. Untuk memberikan solusi teknologi yang konsisten, efektif dan aman, harus ditetapkan suatu forum teknologi untuk memberikan pedoman-pedoman teknologi, advis tentang produk-produk infrastruktur dan pedoman dalam pemilihan teknologi, dan ukuran kepatuhan pada standar dan pedoman ini.
   b. Forum ini harus mengarahkan standar-standar dan praktek-praktek teknologi berdasarkan pada relevansi bisnis, resiko, dan kepatuhannya pada persyaratan eksternal.

3. Dewan Arsitektur TIK
   a. Harus ditetapkan suatu dewan arsitektur TIK untuk memberikan pedoman-pedoman arsitektur dan nasehat dalam aplikasinya, dan memeriksa kepatuhan.
   b. Dewan ini harus mengarahkan disain arsitektur TIK, memastikan bahwa arsitektur tersebut membisakan strategi bisnis dan memperhatikan kepatuhan regulatori dan persyaratan kontinuitas. lni terkait dengan standar umum pendefinisian arsitektur informasi.

Standar Umum Pengembangan Sumber Daya Manusia

1. Dalam proses manajemen sumber daya manusia TIK terdapat 8 area yang perlu diperhatikan, yaitu:

a. Perekrutan dan pemeliharaan personil
b. Matriks kompetensi personil
c. Penugasan personil
d. Pelatihan karyawan
e. Ketergantungan terhadap individu kunci
f. Prosedur pemeriksaan latar belakang personil
g. Evaluasi kinerja kerja karyawan
h. Penghentian atau pemindahan person!!

2. Perekrutan dan Pemeliharaan Personil: Proses rekrutmen personil TIK Pemkot harus selaras dengan kebijakan dan prosedur mengenai sumber daya manusia yang diterbitkan oleh Pemkot (contoh: perekrutan, orientasi, dan lainnya), dan mengacu kepada matriks kebutuhan kompetensi inti TIK.

3. Matrik Kompetensi Personil: Pemkot harus mendefinisikan matrik kebutuhan kompetensi inti TIK dan memastikan secara reguler bahwa matriks tersebut selalu dijaga. Dari matriks tersebut dapat dibuat program pemenuhan kebutuhan akan kompetensi inti TIK. Program-program tersebut dapat berupa pelatihan, pendidikan, dan sertifikasi.

4. Aturan Pengayakan (*Roles of Staffing*):
   a. Harus ada suatu kerangka-kerja sumber daya manusia yang mendefinisikan pembagian peran, tugas dan tanggung jawab, dan kompensasi.
   b. Pembuatan kerangka kerja sumber daya manusia ini harus memasukkan kebutuhan akan kebijakan dan prosedur dari manajemen, kode etik, dan praktek-praktek profesional.

c. Dalam kerangka kerja tersebut harus pula didefinisikan pengawasan yang diperlukan terhadap peran-peran yang telah didefiniskan. Tingkatan pengawasan sejalan dengan sensitivitas dari posisi dan tanggung jawab yang diberikan.

5. Pelatihan Karyawan
   a. Perlunya suatu orientasi/pengenalan terhadap lingkungan Pemkot dan ruang lingkup pekerjaan kepada pegawai baru agar pegawai baru tersebut dapat mulus masuk ke dalam pekerjaannya.
   b. Untuk selalu memelihara pengetahuan, kemampuan, dan keterampilan pegawai, maka pelatihan karyawan balk formal maupun informal harus selalu dirancang, dieksekusi, dan dimonitor tingkat keberhasilannya.
   c. Pelatihan mengenai *Internal Control* dan *Security Awareness* harus rutin diberikan kepada karyawan agar meminimalkan kejadian/masalah yang terkait dengan *security* yang dapat merugikan Pemkot.

6. Ketergantungan terhadap Individu Kunci
   a. Pemkot perlu melakukan usaha-usaha untuk meminimalkan ketergantungan pada suatu individu sehingga proses bisnis maupun sistem TIK Pemkot tetap dapat berjalan meskipun individu kunci tersebut mengundurkan diri ataupun dimutasikan.
   b. Aktivitas-aktivitas yang harus dilakukan guna mengurangi ketergantungan terhadap individu yang memegang peran kunci adalah sebagai berikut:

c. Memasangkan staf dengan staf lainnya dalam melakukan suatu pekerjaan. Dalam melakukan penugasan terhadap suatu pekerjaan harus dilakukan dengan mekanisme pairing (berpasangan) sehingga pengetahuan dalam melakukan pekerjaan tidak hanya dimiliki oleh sate individu tertentu.

7. Menangkap pengetahuan dari individu: Diperlukan suatu peraturan yang mewajibkan semua individu untuk membuat laporan tertulis mengenai aktivitas-aktivitas yang dilakukan sehari-harinya. Dalam laporan itu disebutkan:
   a. Bahan masukan yang diperlukan untuk melakukan aktivitasnya.
   b. Daftar langkah-langkah yang diperlukan dalam melakukan aktivitasnya.
   c. Keluaran yang dihasilkan dari aktivitasnya.
   d. Waktu yang dibutuhkan dalam melakukan aktivitasnya.

8. *Knowledge Sharing*
   a. Diperlukannya suatu database tempat menyimpan dokumentasi/laporan tertulis yang dihasilkan oleh individu-individu (pada point 2) dimana database tersebut dapat diakses oleh umum.
   b. Rencana suksesi/pelimpahan tugas. Diperlukannya suatu mekanisme suksesi/pelimpahan tugas dari suatu individu yang dimutasikan/dipromosikan/ pensiun kepada individu baru yang ditunjuk untuk menggantikan dirinya. Dalam mekanisme itu diatur:
   c. Waktu untuk transisi/pelimpahan tugas. Dalam waktu transisi ini, individu yang akan

dimutasikan/dipromosikan/pensiun diharuskan untuk menyelesaikan semua pekerjaan yang masih berjalan dan membimbing individu yang ditunjuk untuk menggantikan dirinya terhadap pekerjaan tersebut.

d. Daftar pekerjaan yang sudah selesai dikerjakan oleh individu yang akan dimutasikan/dipromosikan/ pensiun.
e. Daftar pekerjaan yang masih belum selesai dikerjakan.
f. Daftar pekerjaan yang masih belum dikerjakan.

9. Prosedur Pemeriksaan Latar Belakang Personil: Diperlukan prosedur pemeriksaan latar belakang personil dalam rekrutmen personil TI. Luasnya cakupan pemeriksaan latar belakang dan periode waktu pemeriksaan didasari atas sensitivitas dan kritikalitas suatu fungsi. Pemeriksaaan ini harus diaplikasikan kepada karyawan, kontraktor, dan vendor Pemkot.

10. Evaluasi Kinerja Kerja Karyawan
    a. Diperlukannya prosedur evaluasi kinerja kerja individu dimana evaluasi itu membandingkan pencapaian individu terhadap tujuan pekerjaan yang diturunkan dad tujuan organisasi, standar bake, dan uraian pekerjaan.
    b. Dari hasil evaluasi tersebut akan dihasilkan rencana pelatihan, konsultasi, penugasan yang dibutuhkan oleh pegawai guna meningkatkan kinerjanya.

11. Pemberhentian atau Pemindahan Personil: Adanya mekanisme yang mengatur aktivitas-aktivitas yang mesti dilakukan ketika adanya penghentian seorang pegawai (baik yang diajukan oleh pegawai itu sendiri maupun yang dilakukan oleh Pemkot) ataupun mutasi individu. Mekanisme tersebut harus mengatur hal-hal berikut ini:
    a. *Knowledge transfer*. Mewajibkan pegawai yang akan dimutasi/berhenti untuk memberikan semua dokumen-dokumen yang terkait dengan pekerjaan yang dilakukan kepada atasannya.
    b. Pengalihan tugas. Pemkot menugaskan individu lain guna mengambil alih tugas yang selama ini dilakukan oleh individu yang akan dimutasi/ berhenti.
    c. Penghapusan akses. Akses yang selama ini dimiliki oleh pegawai yang akan dimutasi/berhenti guna melakukan pekerjaannya sudah mulai dikurangi ketika surat mutasi/pemberhentian dikeluarkan. Akses harus sudah dihapus ketika pegawai itu sudah dimutasikan atau berhenti dari Pemkot.

Standar Umum Monitoring dan Evaluasi Kinerja TI

1. Pendekatan Monitoring: Tetapkan suatu pendekatan dan kerangka-kerja monitoring umum untuk mendefinisikan ruang lingkup, metodologi dan proses-proses yang harus diikuti untuk mengukur penyediaan solusi dan layanan TI, dan memantau kontribusi TI pada bisnis. Integrasikan kerangka kerja tersebut dengan sistem manajemen kinerja korporasi.

2. Definisi dan Pengumpulan Monitoring Data:
   a. Perlu bekerjasama dengan pengguna bisnis untuk mendefinisikan suatu target kinerja yang seimbang (*balanced*) dan mintakan persetujuan dari pengguna bisnis dan stakeholder lain yang relevan.
   b. Definisikan benchmark dengan mana target dibandingkan, dan identifikasi data yang tersedia untuk dikumpulkan untuk mengukur target-target. Tetapkan proses-proses untuk mengumpulkan data secara akurat dan tepat waktu untuk melaporkan kemajuan terhadap target.
   c. Metode Monitoring: Gelar suatu metode monitoring kinerja (misalnya *balance scorecard*) yang mencatat target; mencatat pengukuran-pengukuran; memberikan suatu pandangan yang tajam, menyeluruh, tentang kinerja TI; dan cocok dengan sistem monitoring enterprise.
   d. Penilaian Kinerja: Secara periodik lakukan penilaian periksa kinerja terhadap target, analisa penyebab setiap deviasi, dan inisiasi tindakan perbaikan untuk menanggulangi sebab-sebab yang mendasarinya. pada waktu-waktu yang tepat, lakukan analisis penyebab akar lintas deviasi-deviasi.

3. Pelaporan Kepada Pimpinan:
   a. Harus disusun laporan-laporan manajemen tentang kontribusi TI pada bisnis, terutama dalam hal kinerja dari portofolio enterprise, program-program investasi IT-enabled, dan solusi dan layanan kinerja yang diberikan oleh masing-masing program.

b. Masukkan dalam laporan-laporan status sejauh mana sasaran-sasaran yang direncanakan telah tercapai, sumber daya yang. dianggarkan telah terpakai, kumpulan target-target kinerja yang telah terpenuhi dan resiko-resiko yang dikenali telah dimitigasikan.
c. Harus diantisipasi review oleh manajemen senior dengan menyarankan tindakan-tindakan perbaikan untuk deviasi-deviasi yang besar. Berikan laporan tersebut kepada manajemen senior, dan mintalah umpan balik dari telaah manajemen.
d. Tindakan-Tindakan Perbaikan: Identifikasi dan inisiasi tindakan-tindakan perbaikan berdasarkan pemantauan kinerja, asesmen, dan pelaporan. Int termasuk tindak lanjut dari semua monitoring, pelaporan dan penilaian-penilaian melalui:
    1) Telaah, negosiasi, dan adanya tanggapan dari manajemen
    2) Penetapan tanggungjawab untuk perbaikan
    3) Penelusuran hasil-hasil dari tindakan-tindakan yang dijanjikan.

Standar Umum Pemantauan dan Evaluasi Pengendalian internal

1. Pemantauan Kerangka-Kerja Kontrol Intern: Terus menerus memantau, melakukan benchmark dan memperbaiki lingkungan kendali TI dan kerangka kendali untuk mencapai tujuan-tujuan organisasional.
2. Telaah Supervisori: Memantau dan mengevaluasi efektivitas dan efisiensi internal IT managerial review control.

3. *Control Exceptions*: Mengidentifikasi *control exception*, dan menganalisa dan mengidentifikasi akar penyebabnya. Eskalasikan *control exception* dan laporkan kepada pemangku kepentingan dengan semestinya. Lembagakan tindakan korektif yang diperlukan.
4. *Control Self Assessment*: Evaluasi kelengkapan dan efektivitas kendali manajemen atas proses-proses TI, kebijakan-kebijakan dan kontrak-kontrak melalui suatu program *self-assessment*.
5. *Assurance of Internal Control*: Dapatkan, sesuai dengan kebutuhan, kepastian lebih lanjut atas kelengkapan dan efektivitas dari kontrol intern melalui review oleh pihak ketiga.
6. Kontrol Intern pada Pihak Ketiga: Nilai status dari kontrol intern dari penyedia jasa eksternal.
7. Konfirmasikan bahwa penyedia jasa eksternal mematuhi persyaratan legal dan regulatori dan kewajiban-kewajiban kontraktual.
8. Tindakan Perbaikan: Kenali, inisiasikan, jejaki, dan implementasikan tindakan-tindakan remedial yang timbal dari control *assessment* dan pelaporan.

Standar Umum Kepatuhan pada Persyaratan Ekstern

1. Identifikasi dan Persyaratan-persyaratan Kepatuhan Legal Ekstern, Regulatori dan Kontraktual: Kenali, secara terus menerus, hukum-hukum lokal dan internasional, peraturan-peraturan, dan persyaratan eksternal lainnya yang harus dipatuhi dengan memasukkannya ke dalam kebijakan-kebijakan,

standar-standar, prosedur-prosedur dan metodologi-metodologi TI.

2. Optimisasi Tanggapan terhadap Persyaratan Ekstern: Review dan sesuaikan kebijakan-kebijakan, standar-standar, prosedur-prosedur dan metodologi-metodologi TI untuk memastikan bahwa persyaratan-persyaratan legal dan kontraktual diperhatikan dan dikomunikasikan.
3. Evaluasi Kepatuhan pada Persyaratan Ekstern: Konfirmasikan kepatuhan kebijakan kebijakan-kebijakan, standar-standar, prosedur-prosedur dan metodologi-metodologi TI dengan persyaratan-persyaratan legal dan regulatori.
4. *Positive Assurance of Compliance*: Dapatkan dan laporkan penjaminan kepatuhan pada semua kebijakan-kebijakan internal yang diturunkan dari arahan-arahan internal atau persyaratan-persyaratan legal, regulatori atau kontraktual ekstemal, memastikan bahwa setiap tindakan korektif untuk menutup kesenjangan kepatuhan telah dilaksanakan oleh pemilik proses yang bertanggung jawab pada waktunya.
5. Pelaporan Terpadu: Integrasikan pelaporan TI atas persyaratan-persyaratan legal, regulatori, dan kontraktual dengan keluaran yang serupa dengan fungsi bisnis lain.

Standar Umum Tata Kelola TI

1. Penetapan Kerangka Kerja Tata Kelola TI:
   a. Definisikan, tetapkan dan selarasan kerangka-kerja tata kelola TI dengan tata kelola dan Iingkungan

kendali keseluruhan organisasi. Dasarkan kerangka-kerja tersebut pada proses-proses TI dan model kendali yang sesual, dan sediakan akuntabilitas dan praktek- praktek yang jelas untuk menghindari kegagalan dalam kontrol intern dan pengawasan.

b. Konfirmasikan bahwa kerangka kerja tata kelola TI memastikan kepatuhan dengan hukum dan peraturan-peraturan dan selaras dengan strategi dan tujuan organisasi. Laporkan status tata-kelola dan masalah-masalah TI.

2. Keselarasan Strategis:
   a. Upayakan adanya pemahaman akan masalah-masalah strategis TI oleh eksekutif dan pengawas, seperti peran TI, kemampuan-kemampuan teknologi. Harus dipastikan bahwa ada pemahaman yang sama antara bisnis dan TI tentang kontribusi potensial TI pada strategi bisnis.
   b. Harus bekerjasama dengan pengawas dan badan-badan tata-kelola seperti komite strategi TIK untuk memberikan arahan stratejik pada manajemen TI, memastikan bahwa tujuan dan strategi tersebut dikaskadekan pada unit-unit bisnis dan fungsi-fungsi TI, dan bahwa di antara bisnis dan TI terbangun kepercayaan.
   c. Harus diupayakan keselarasan TI dengan bisnis dalam hal strategi dan operasi, mendorong tanggung jawab bersama di antara bisnis dan TI untuk pengambilan keputusan stratejik dan mendapatkan manfaat dari IT-*enabled investment*.

3. *Value Delivery*:
    a. Program-program IT-*enabled investment* dan aset-aset serta Iayanan-Iayanan lain harus dikelola untuk memastikan bahwa mereka memberikan manfaat sebesar mungkin dalam mendukung tujuan dan strategi bisnis.
    b. Harus dipastikan bahwa hasil bisnis yang diharapkan dari IT-*enabled investment* dan upaya penuh yang diperlukan untuk memperoleh hasil-hasil tersebut dipahami; bahwa kasus bisnis yang komprehensif dan konsisten dibuat dan disetujui oleh pemangku kepentingan; bahwa aset-aset dan investasi-investasi dikelola sepanjang sikius hidupnya; dan bahwa ada manajemen aktif untuk merealisasikan manfaat, seperti misalnya kontribusi pada layanan-layanan baru, peningkatan efisiensi dan tanggapan lebih balk pada permintaan pelanggan.
    c. Terapkan pendekatan berdisiplin atas pengelolaan portofolio, program dan proyek, mendesak agar bisnis mengambil kepemilikan semua 1T-enabled investment dan TI memastikan optimisasi biaya penyediaan kemampuan dan layanan TI.
    d. Manajemen Sumber Daya: Mengawasi investasi, penggunaan dan alokasi sumber daya TI melalui asesmen atas inisiatif-inisiatif dan operasi TI secara teratur untuk memastikan penyediaan sumber daya yang sesuai dan keselarasannya dengan tujuan-tujuan stratejik sekarang dan mendatang dan keharusan bisnis *(business imperative).*
    e. Manajemen Resiko: Harus bekerjasama dengan pengawas untuk mendefinisikan akan resiko TI

yang diinginkan/dapat ditoleransi oleh organisasi, dan mendapatkan penjaminan yang wajar bahwa resiko aktual TI tidak melampaui resiko yang diinginkan pengawas. Tanamkan tanggung jawab manajemen resiko dalam organisasi, memastikan bahwa bisnis dan TI menilai dan melaporkan secara regular resiko-resiko terkait TI dan dampaknya, dan bahwa posisi resiko TI organisasi adalah transparan pada semua pemangku kepentingan.

4. Manajemen Kinerja:
   a. Harus dipastikan bahwa tujuan-tujuan TI telah tercapai atau terlampaui, atau bahwa kemajuan ke arah sasaran-sasaran TI sesuai dengan harapan. Jika sasaran yang telah disepakati tidak tercapai atau kemajuan tak seperti diharapkan, review tindakan perbaikan manajemen.
   b. Harus dilaporkan kepada pengawas portofolio, program dan kinerja TI yang relevan, didukung laporan-laporan yang memungkinkan manajemen senior untuk menelaah kemajuan organisasi ke arah sasaran yang ditetapkan.

5. *Independent Assurance*: Hal-haI yang harus diperhatikan meliputi: Harus diperoleh asuran independen (intern atau ekstern) tentang kepatuhan TI pada hukum-hukum dan peraturan- peraturan yang relevan; kebijakan-kebijakan, standar-standar dan prosedur-prosedur organisasi; praktek-praktek yang diterima luas; dan kinerja TI yang efektif dan efisien.

Standar Umum Pendefinisian Proses, Organisasi, dan Hubungan TI

1. Kerangka-Kerja Proses TI: Harus didefinisikan kerangka kerja proses TI untuk melaksanakan rencana stratejik TI. Kerangka kerja ini harus mencakup suatu struktur proses TI dan hubungan-hubungan (misal: untuk mengelola *process gap* dan *process overlap,* kepemilikan, kematangan, pengukuran kinerja, perbaikan, kepatuhan, target kualitas, dan rencana untuk mencapainya).
2. Kerangka kerja tersebut harus memungkinkan integrasi proses-proses spesifik TI, manajemen portofolio TI, proses-proses bisnis dan proses-proses perubahan bisnis. Kerangka kerja TI tersebut harus dipadukan ke dalam suatu sistem manajemen kualitas (SMK) dan kerangka kerja kontrol intern.
3. Komite Strategi TI: Harus ditetapkan suatu komite strategi TI pada tingkat pengawas. Komite ini harus memastikan bahwa tata-kelola TI, sebagai bagian dari tata-kelola organisasi, ditangani secara memadai; memberikan advis tentang arah stratejik, dan menelaah investasi- investasi besar atas nama seluruh pengawas.
4. Komite Pengarah TI:
   a. Harus ditetapkan suatu komite pengarah TI (atau ekivalennya) terdiri dari eksekutif, manajemen bisnis dan TI.
   b. Menentukan prioritas program-program IT-enabled investment selaras dengan strategi dan prioritas organisasi.
   c. Menjejaki status proyek-proyek dan menyelesaikan konflik sumber daya.

5. Memantau Tingkat Layanan Dan Perbaikan Layanan
    a. Penempatan Fungsi TI dalam Organisasi: Fungsi TI harus ditetapkan dalam struktur seluruh oganisasi dengan suatu model bisnis tergantung pada pentingnya TI dalam organisasi, khususnya kritikalitasnya pada strategi bisnis dan tingkat ketergantungan operasional pada TI. Jalur peIaporan dari pemimpin TI harus sepadan dengan pentingnya TI dalam organisasi.
    b. Struktur Organisasi TI: Harus ditetapkan suatu struktur organisasi TI internal maupun eksternal yang mencerminkan kebutuhan bisnis. Di samping itu, harus disusun suatu proses untuk menelaah struktur organisasi TI secara periodik untuk menyesuaikan kebutuhan tenaga kerja dan strategi pengadaan tenaga kerja untuk memenuhi tujuan bisnis dan perubahan keadaan.
    c. Penetapan Peran dan Tanggung Jawab: Buat dan komunikasikan peran dan tanggung jawab untuk personil TI dan para pengguna akhir yang mendefinisikan antara otoritas, tanggung jawab dan akuntabilitas personil TI dan para pengguna akhir untuk memenuhi kebutuhan-kebutuhan organisasi.
    d. Tanggung Jawab Penjaminan Mutu TI: Alokasikan tanggung jawab atas kinerja dari fungsi quality assurance (QA) dan berikan kelompok QA sistem-sistem QA, pengendalian-pengendalian dan keahlian komunikasi yang sesuai. Pastikan bahwa penempatan organisasional, tanggung jawab dan ukuran kelompok QA memenuhi permintaan/ kebutuhan organisasi.

6. Tanggung Jawab atas Resiko, Keamanan, dan Kepatuhan:
    a. Tetapkan/letakkan kepemilikan, dan tanggung jawab atas resiko-resiko yang berhubungan dengan TI dalam bisnis pada tingkat senior yang sesuai. Definisikan dan alokasikan peran- peran yang kritis terhadap resiko-resiko TI, termasuk tanggung jawab spesifik atas keamanan informasi, keamanan fisik, dan kepatuhan/kesesuaian.
    b. Buatlah tanggung jawab manajemen keamanan pada tingkat perusahaan untuk menangani masalah-masalah tingkat organisasi. Beberapa tanggung jawab manajemen keamanan tambahan mungkin perlu dialokasikan pada sebuah tingkatan spesifik sistem (*system- specific*) untuk menangani masalah-masalah keamanan yang berhubungan dengannya. Dapatkan penjelasan dari manajemen senior mengenai resiko TI yang diiginkan dan persetujuannya atas setiap resiko TI selain itu.
    c. Kepemilikan Data dan Sistem: Berikan prosedur-prosedur dan alat-alat kepada bisnis
    d. yang memungkinkannya untuk dapat menangani tanggung jawabnya atas kepemilikan data dan sistem-sistem informasi. Para pemilik harus membuat berbagai keputusan dalam mengklasifikasikan informasi dan sistem, serta melindunginya (informasi dan sistem) sejalan dengan-pengklasifikasian ini.
    e. Supervisi: Implementasikan praktek-praktek pengawasan yang mencukupi dalam fungsi TI untuk memastikan bahwa peran dan tanggung jawab telah dilaksanakan dengan balk dan sesuai; untuk menilai

apakah semua personil memiliki otoritas dan sumber daya yang cukup untuk melaksanakan peran dan tanggung jawab mereka; serta untuk merevisi KP1 secara umum.

f. Pemisahan Tugas: Implementasikan sebuah pembagian peran dan tanggung jawab yang dapat mengurangi kemungkinan seorang individu mengkompromikan sebuah proses yang kritis. Pastikan bahwa para personil hanya melaksanakan tugas-tugas yang menjadi otoritasnya sesuai dengan pekerjaan dan posisi masing-masing personil.
g. IT Staffing: Evaluasi kebutuhan-kebutuhan staffing (tenaga kerja) secara reguler atau berdasarkan perubahan-perubahan besar pada bisnis, operasional atau lingkungan TI untuk memastikan bahwa fungsi TI memiliki sumber daya yang mencukupi untuk, dengan cukup dan sesuai, mendukung sasaran-sasaran dan tujuan-tujuan bisnis.
h. Personil TI Kunci: Definisikan dan identifikasikan personil kunci TI (misal personil pengganti/ cadangan), dan minimalisir ketergantungan pada hanya seorang individu yang meIakukan fungsi kerja yang kritis.
i. Kebijakan dan Prosedur Staf Kontrak: Pastikan bahwa para konsultan dan personil kontrak yang mendukung fungsi TI telah mengetahui dan patuh dengan kebijakan-kebijakan organisasi guna memberikan perlindungan bagi aset-aset organisasi, seperti apakah mereka memenuhi syarat-syarat kontrak yang telah disetujui.

j. Hubungan-Hubungan: Buat dan perliharalah sebuah koordinasi, komunikasi, dan struktur hubungan yang optimal antara fungsi TI dengan berbagal kepentingan lainnya balk di dalam maupun di luar fungsi TI, seperti dewan panel, para eksekutif, unit-unit bisnis, para pemakai perorangan, para supplier, para petugas keamanan, para manajer resiko, kelompok kepatuhan korporasi (*corporate compliance group*), sumber daya dan outsourcing dan manajemen offsite.

Standar Umum Manajemen Investasi TI

1. Kerangka-Kerja Manajemen Keuangan: Buat dan perliharalah sebuah kerangka kerja keuangan untuk mengatur investasi dan biaya atas aset-aset dan layanan-layanan TI melalui portofolio IT-*enabled investment*, kasus-kasus bisnis dan anggaran-anggaran TI.
2. Penentuan Prioritas dalam Anggaran TI: Implementasikan sebuah proses pengambilan keputusan untuk memprioritaskan pengalokasian sumber daya TI untuk berbagai operasi, proyek, dan pemeliharaan untuk memaksimalkan kontribusi TI dalam mengoptimalkan *return* dari portfolio program-program IT-enabled investment serta layanan-layanan dan aset-aset TI lainnya milik perusahaan.
3. Penganggaran TI:
   a. Buatlah dan implementasikan praktek-praktek untuk menyiapkan sebuah anggaran yang menggambarkan prioritas-prioritas yang telah dibuat oleh portofolio program-program IT-

enabled investment milik perusahaan, dan yang meliputi biaya-biaya yang berkelanjutan (*on going*) dari mengoperasikan dan memelihara infrastruktur yang telah ada.

b. Praktek-praktek ini harus mendukung baik pengembangan dari sebuah anggaran TI keseluruhan maupun pengembangan dari anggaran-anggaran untuk masing-masing program, dengan penekanan yang khusus pada komponen-komponen TI dari program- program tersebut.
c. Praktek-praktek tersebut juga harus memungkinkan iterbuka untuk revisi yang berkelanjutan (*on going*), perbaikan dan persetujuan atas anggaran keseluruhan dan anggaran-anggaran untuk masing-masing program.
d. Manajemen Biaya: Implementasikan sebuah proses manajemen biaya yang membandingkan biaya-biaya aktual dengan anggaran. Biaya harus dimonitor dan dilaporkan. Bila ada penyimpangan (deviasi), harus segera diidentifikasi dan dampak dari penyimpangan tersebut harus dinilai. Bersama dengan sponsor bisnis dari program-program tersebut, tindakan perbaikan yang sesuai harus dilakukan, dan jika perlu, kasus bisnis program tersebut harus diperbarui.

4. Manajemen Manfaat:
   a. Implementasikan sebuah proses untuk memonitor manfaat-manfaat dari pengadaan dan pemeliharaan fasilitas-fasilitas (*capabilities*) TI yang sesuai. Kontribusi TI terhadap bisnis, baik sebagai sebuah komponen dari program-program IT-enabled

investment maupun sebagai bagian dari pendukung operasional reguler, harus diidentifikasikan dan didokumentasikan dalam sebuah kasus bisnis, yang disetujui, dimonitor, dan dilaporkan.

b. Setiap laporan harus direvisi dan, bila terdapat kesempatan untuk meningkatkan kontribusi TI, maka tindakan-tindakan yang sesuai harus didefinisikan dan dilaksanakan. Bila perubahan-perubahan dalam kontribusi TI mempengaruhi sebuah program, atau bila perubahan-perubahan pada proyek-proyek berhubungan lainnya mempengaruhi sebuah program, maka kasus bisnis program tersebut harus diperbarui.

Standar Umum Komunikasi Arah dan Tujuan Manajemen

1. Lingkungan Kebijakan dan Pengendalian TI:
   a. Definisikan elemen-elemen dari sebuah lingkungan pengendalian untuk TI, sesuai dengan filosofi manajemen dan gaya operasi perusahaan. Elemen-elemen ini harus meliputi kebutuhan-kebutuhan yang diharapkan dalam hal penyampaian nilai (*delivery of value*) dari investasi-investasi TI, harapan akan resiko, integritas, nilai-nilai etis, kompetensi staf, akuntabilitas, dan tanggung jawab.
   b. Lingkungan pengendalian harus didasarkan pada sebuah budaya yang mendukung penyampaian nilai (*value delivery*) sejalan dengan pengelolaan resiko-resiko yang signifikan, mendukung kooperasi dan kerja tim antar divisi, mendukung kepatuhan dan kemajuan proses yang kontinyu, serta menangani

penyimpangan-penyimpangan (deviasi-deviasi) proyek (termasuk dengan kegagalan proyek) dengan baik.

c. Kerangka Kerja Kontrol Intern dan Resiko TI: Kembangkan dan pelihara sebuah kerangka kerja yang mendefinisikan pendekatan keseluruhan dari perusahaan pada resiko dan pengendalian TI, dan yang sesuai dengan kebijakan dan lingkungan pengendalian TI serta kerangka kerja resiko dan pengendalian perusahaan.
d. Manajemen Kebijakan TI: Kembangkan dan pelihara sebuah rangkaian kebijakan untuk mendukung strategi TI. Kebijakan-kebijakan ini harus meliputi maksud dan tujuan kebijakan; peran dan tanggung jawab; proses pengecualian (*exception*); pendekatan kepatuhan (*compliance approach*); dan pengacuannya pada prosedur-prosedur, standar-standar dan pedoman-pedoman. Relevansi kebijakan-kebijakan tersebut harus dikonfirmasi dan disetujui secara teratur.
e. Penerapan Kebijakan, Standar, dan Prosedur: Sebarkan dan implementasikan kebijakan-kebijakan TI kepada seluruh staf yang relevan, sehingga tertanam pada did mereka dan mereka menjadi bagian integral dari operasi-operasi perusahaan.
f. Komunikasi Sasaran dan Arah TI: Sebarkan dan implementasikan kebijakan-kebijakan TI pada seluruh staf yang relevan, sehingga tertanam pada diri mereka dan mereka menjadi bagian integral dari operasi-operasi perusahaan.

Standar Umum Manajemen Kualitas

1. Sistem Manajemen Kualitas:
   a. Buat dan peliharalah sebuah sistem manajemen kualitas *Quality Management System* (QMS) yang memberikan sebuah standar, pendekatan formal dan berkelanjutan dalam hal manajemen kualitas yang sesuai dengan kebutuhan-kebutuhan bisnis. QMS harus dapat mengidentifikasikan kebutuhan-kebutuhan dan kriteria kualitas; proses-proses kunci TI beserta urutan dan interaksinya; dan juga kebijakan-kebijakan, kriteria dan metode-metode untuk mendefinisikan, mendeteksi, mengkoreksi dan mencegah ketidak-normalan.
   b. QMS harus dapat mendefinisikan struktur organisasional untuk manajemen kualitas, yang mencakup peran-peran, tugas-tugas dan tanggung jawab dari manajemen kualitas. Semua area kunci harus mengembangkan rencana-rencana kualitas mereka sejalan dengan kriteria dan kebijakan, serta harus mencatat data kualitas. Awasi dan ukur efektivitas dan penerimaan QMS, serta tingkatkan (efektivitas dan penerimaan QMS) jika dibutuhkan.
   c. Standar-Standar TI dan Praktek-Praktek Kualitas: Identifikasi dan pertahankan standar-standar, prosedur-prosedur serta praktek-praktek untuk proses-proses kunci TI agar dapat mengarahkan organisasi dalam pencapaian maksud dan tujuan dari QMS. Gunakan praktek-praktek yang balk dalam industri sebagai acuan pada saat meningkatkan dan merancang praktek-praktek kualitas organisasi.

2. Pengembangan dan Akuisisi Standar:
   a. Terapkan dan pertahankan standar-standar untuk semua pengembangan dan akuisisi yang mengikuti daur hidup dari hasil/keluaran akhir (*ultimate deliverable*), dan sertakan *sign-off* pada *milestone-milestone* kunci berdasarkan kriteria *sign-off* yang telah disetujui.
   b. Pertimbangkan standar-standar pengkodean software; aturan-aturan pemberian nama; format-format file; standar-standar skema dan rancangan kamus data; standar-standar interface pemakai; interoperability; efisiensi kinerja sistem; skalabilitas; standar-standar untuk pengembangan dan pengujian; validasi atas kebutuhan-kebutuhan; rencana-rencana pengujian; serta pengujian unit, regresi dan integrasi.
   c. Fokus pada Pelanggan: Fokuskan manajemen kualitas pada para pelanggan dengan menentukan permintaan-permintaan mereka dan menyesuaikannya dengan standar-standar dan praktek-praktek TI. Definisikan peran dan tanggung jawab mengenai penyelesaian konflik antar pemakai/pelanggan dengan organisasi TI.
3. Perbaikan Berkelanjutan: Pertahankan dan komunikasikan secara teratur rencana kualitas keseluruhan yang mendorong adanya perbaikan yang berkelanjutan.
4. Pengukuran Kualitas, Pemantauan, dan Telaah: Definisikan, rencanakan dan implementasikan ukuran-ukuran untuk memonitor kepatuhan yang berlanjut terhadap QMS, seperti halnya nilai yang diberikan oleh QMS. Pengukuran, pengawasan dan pencatatan

informasi harus digunakan oleh pemakai proses untuk mengambil tindakan-tindakan perbaikan dan pencegahan yang sesuai.

Standar Umum Penilaian dan Manajemen Resiko

1. Kerangka-Kerja Manajemen Resiko TI: Buatlah sebuah kerangka kerja manajemen resiko TI yang sesuai dengan kerangka kerja manajemen resiko organisasi (perusahaan).
2. Penetapan Konteks Resiko: Buatlah sebuah konteks dimana kerangka kerja penilaian resiko diaplikasikan untuk memastikan keluaran-keluaran yang sesuai. Hal ini harus mencakup penentuan konteks internal dan eksternal untuk setiap penilaian resiko, sasaran dan tujuan dari penilaian, dan kriteria yang mendasari evaluasi resiko.
3. Penilaian Resiko: Nilailah secara berulang kemungkinan dan dampak dari semua resiko yang telah diidentifikasi, dengan memakai metode-metode kualitatif dan kuantitatif. Kemungkinan dan dampak yang berhubungan dengan resiko intrinsik dan resiko lainnya harus ditentukan secara individual, berdasarkan kategori dan sebuah basis portfolio.
4. Tanggapan Resiko: Kembangkan dan pelihara sebuah proses respon resiko yang dirancang untuk memastikan bahwa pengendalian-pengendalian cost-effective memitigasi pemaparan terhadap berbagai resiko secara berkelanjutan. Proses respon resiko harus dapat mengidentifikasi strategi-strategi resiko seperti penghindaran, pengurangan, pembagian atau penerimaan; menentukan tanggung jawab yang

terkait; dan mempertimbangkan tingkat-tingkat toleransi resiko.

5. Pemeliharaan dan Pemantauan Rencana Aksi Resiko:
   a. Buat prioritas dan rencanakan aktivitas-aktivitas pengendalian pada setiap tingkatan untuk mengimplementasikan respon-respon resiko yang diidentifikasi sesuai dengan yang dibutuhkan, termasuk dengan identifikasi biaya-biaya, manfaat-manfaat serta tanggung jawab atas pelaksanaannya.
   b. Dapatkan persetujuan untuk tindakan-tindakan yang direkomendasikan dan penerimaan atas setiap resiko-resiko yang lainnya (residual), dan pastikan bahwa tindakan-tindakan tersebut dimiliki oleh satu atau lebih pemilik proses yang terkena pengaruhnya.
   c. Awasi pelaksanaan dari rencana-rencana tersebut, dan laporkan setiap penyimpangan (deviasi) kepada manajemen senior.

Standar Umum Manajemen Proyek

1. Kerangka Kerja Manajemen Program:
   a. Peliharalah program dari proyek, yang berhubungan dengan portofolio program-program IT-*enabled investment*, dengan cara mengidentifikasikan, menentukan, mengevaluasi, membuat prioritas, menyeleksi, memulai, mengelola dan mengendalikan proyek. Pastikan bahwa proyek tersebut mendukung tujuan-tujuan dari program tersebut.
   b. Koordinasikan aktivitas-aktivitas dan sating ketergantungan antar beberapa proyek, aturlah

kontribusi dari semua proyek dalam program kepada keluaran-keluaran yang diharapkan, dan selesaikan kebutuhan-kebutuhan dan konflik-konflik sumber daya.

c. Kerangka Kerja Manajemen Proyek: Buatlah dan pelihara sebuah kerangka kerja manajemen proyek yang mendefinisikan ruang lingkup dan batasan-batasan dalam pengelolaan proyek, juga metode yang akan diterapkan dan diaplikasikan untuk setiap proyek yang disetujui. Kerangka kerja dan metode pendukung harus diintegrasikan ke dalam proses-proses manajemen program.

2. Pendekatan Manajemen Proyek:
   a. Buatlah sebuah pendekatan manajemen proyek yang sesuai dengan ukuran, kompleksitas, dan persyaratan regulatori dari setiap proyek. Struktur pengaturan proyek dapat mencakup peranan, tanggung jawab, akuntabilitas dan sponsor program, sponsor proyek, komite pengendali, kantor proyek dan manajer proyek, serta mekanisme-mekanisme yang melaluinya mereka dapat memenuhi berbagai tanggung jawab tersebut (seperti pelaporan dan revisi-revisi tahapan).
   b. Pastikan semua proyek TI memiliki sponsor dengan otoritas yang mencukupi untuk dapat memiliki pelaksanaan proyek dalam program strategis keseluruhan.

3. Komitmen Pemangku Kepentingan: Dapatkan komitmen dan partisipasi dari semua *stake holder* yang terkena pengaruh dalam pendefinisian dan

pelaksanaan proyek dalam konteks keseluruhan program IT-*enabled investment.*

4. Pernyataan Lingkup Proyek:
   a. Tentukan dan dokumentasikan sifat dan ruang lingkup proyek untuk mengkonfirmasikan dan mengembangkan sebuah pengertian bersama di antara para *stakeholder* mengenai ruang lingkup proyek dan bagaimana hubungannya dengan proyek-proyek lain dalam keseluruhan program IT-*enabled investment*.
   b. Definisi ini harus disetujui secara formal oleh para sponsor program dan proyek sebelum inisiasi proyek.

5. Inisiasi Tahapan Proyek:
   a. Setujui inisiasi setiap tahap proyek utama dan komunikasikan dengan seluruh *stakeholder*. Dasari persetujuan dari tahap inisiasi ini dengan keputusan-keputusan pengaturan program. Persetujuan atas tahap-tahap setelahnya harus didasari dengan revisi dan penerimaan hasil dari tahap sebelumnya serta persetujuan atas sebuah kasus bisnis yang diperbaharui pada revisi utama berikutnya dari progam tersebut.
   b. Dalam kejadian tahapan-tahapan proyek yang saling tumpang tindih (*overlap*), para sponsor program dan proyek harus membuat sebuah titik persetujuan untuk mengotorisasi kelanjutan proyek.

6. Rencana Proyek Terpadu:
    a. Buatlah sebuah rencana proyek terintegrasi formal dan disetujui (yang meliputi sumber daya bisnis dan sistem-sistem informasi) untuk memandu pelaksanaan proyek dan mengendalikannya selama hidup proyek tersebut. Aktivitas-aktivitas dan saling ketergantungan antar beberapa proyek dalam suatu program harus dapat dimengerti dan didokumentasikan.
    b. Rencana proyek harus terus dipelihara selama hidup proyek tersebut. Rencana proyek, dan perubahan-perubahannya, harus disetujui sesuai dengan kerangka kerja pengaturan progam dan proyek tersebut.

7. Sumber Daya Proyek: Tentukan tanggung jawab, hubungan, otoritas dan kriteria kinerja dari setiap anggota tim proyek, dan tentukan dasar untuk memperoleh dan menugasi anggota staf dan/atau kontraktor yang kompeten untuk proyek tersebut. Pengadaan produk-produk dan jasa-jasa yang dibutuhkan untuk setiap proyek harus direncanakan dan diatur untuk dapat mencapai tujuan-tujuan proyek dengan menggunakan praktek-praktek pengadaan milik organisasi.
8. Manajemen Resiko Proyek: Hilangkan atau minimalisir resiko-resiko spesifik yang berhubungan dengan proyek-proyek individual melalui sebuah proses yang sistematis yang meliputi perencanaan, pengidentifikasian, analisa, pengambilan tindakan, pengawasan dan pengendalian area-area' atau kejadian-kejadian yang mempunyai potensial

menyebabkan perubahan yang tidak diinginkan. Resiko-resiko yang dihadapi oleh proses manajemen proyek dan hasil proyek harus diketahui dan dicatat secara terpusat.

9. Rencana Kualitas Proyek: Buat sebuah rencana manajemen kualitas yang menjabarkan sistem kualitas proyek dan bagaimana implementasinya. Rencana tersebut harus direvisi secara formal dan disetujui oleh seluruh pihak yang berkepentingan dan kemudian dimasukkan ke dalam rencana proyek yang terintegrasi.
10. Rencana Penjaminan Mutu Proyek: Identifikasi tugas-tugas penjaminan untuk mendukung akreditasi sistem baru atau sistem yang dimodifikasi selama perencanaan proyek, dan masukkan ke dalam rencana proyek yang terintegrasi. Tugas-tugas tersebut harus memberikan penjaminan bahwa pengendalian-pengendalian internal dan fitur-fitur keamanan telah memenuhi persyaratan-persyaratan yang telah ditentukan sebelumnya.
11. Pengukuran, Pelaporan dan Pemantauan Kinerja Proyek: Ukurlah kinerja proyek berdasarkan ruang lingkup, jadwal, kualitas, biaya, dan kriteria resiko dari kinerja proyek kunci. Identifikasi setiap penyimpangan (deviasi) dari proyek dan program secara keseluruhan, dan laporkan hasilnya kepada para stakeholder kunci. Rekomendasikan, implementasikan dan awasi tindakan perbaikan, jika dibutuhkan, sesuai dengan kerangka kerja pengaturan program dan proyek.

12. Penutupan Proyek:
    a. Buatlah syarat dimana, pada akhir dari setiap proyek, para stakeholder proyek harus memastikan apakah proyek tersebut telah menghasilkan hasil-hasil dan manfaat-manfaat yang telah direncanakan.
    b. Identifikasikan dan komunikasikan setiap aktivitas-aktivitas outstanding yang dibutuhkan untuk mencapai hasil-hasil yang telah direncanakan dari proyek dan manfaat-manfaat dari program, serta identifikasi dan dokumentasikan pelajaran-pelajaran yang dipelajari (*lessons learned*) untuk dapat dipakai pada proyek-proyek dan program-program yang akan datang.

Standar Umum Pengadaan dan Pemeliharaan Infrastruktur Teknologi

1. Rencana Pengadaan Infrastruktur Teknologi: Harus disusun suatu rencana untuk pengadaan, implementasi dan pemeliharaan infrastruktur teknologi yang memenuhi kebutuhan-kebutuhan teknis dan fungsional dari birokrasi Pemkot.

2. Ketersediaan dan Proteksi Sumber Daya Infrastruktur:
    a. Harus diterapkan tindakan-tindakan pengendalian internal, pengamanan, dan *auditability* selama konfigurasi, integrasi, dan pemeliharaan hardware dan perangkat lunak infrastruktur untuk memproteksi sumber daya dan menjamin ketersediaan dan integritas.

b. Tanggung jawab untuk penggunaan komponen-komponen infrastruktur yang sensitif harus didefinisikan dengan jelas dan dipahami oleh pihak yang mengembangkan dan memadukan komponen-komponen infrastruktur tersebut. Penggunaannya harus dipantau dan dievaluasi.
c. Pemeliharaan Infrastruktur: Kembangkanlah sebuah strategi dan rencana untuk pemeliharaan infrastruktur, serta pastikan bahwa perubahan-perubahan telah dikendalikan sesuai dengan prosedur manajemen perubahan milik organisasi. Masukkan ke dalamnya revisi-revisi periodik terhadap kebutuhan-kebutuhan bisnis, manajemen tambahan (*patch*), strategi-strategi yang diperbarui, resiko-resiko, penilaian atas kelemahan-kelemahan dan kebutuhan-kebutuhan keamanan.
d. Lingkungan Pengujian Kelayakan: Buatlah lingkungan-lingkungan pengembangan dan pengujian untuk mendukung pengujian kelayakan dan integrasi yang efektif dan efisien atas komponen-komponen infrastruktur.

Standar Umum Enable Operation and Use

a. *Planning for Operational Solutions*: Kembangkan sebuah rencana untuk mengidentifikasikan dan mendokumentasikan semua aspek teknis, operasional, dan pemakaian seperti siapa-siapa saja yang akan mengoperasikan, memakai, dan memelihara solusi-solusi otomatis (*automated*

solutions) dapat melaksanakan tanggung jawab mereka.

b. Alih Pengetahuan ke Manajemen Bisnis: Alihkan pengetahuan kepada manajemen bisnis sehingga memungkinkan mereka untuk mengambil alih kepemilikan sistem dan data, serta melaksanakan tanggung jawab terhadap penyampaian dan kualitas layanan, pengendalian internal, serta administrasi aplikasi.
c. Alih Pengetahuan ke *End User*: Alihkan pengetahuan dan keterampilan kepada para pemakai akhir agar mereka dapat menggunakan sistem tersebut dengan efektif dan efisien dalam mendukung proses-proses bisnis.
d. Alih Pengetahuan ke Staf Operasi dan Support: Alihkan pengetahuan dan keterampilan kepada para pemakai akhir agar mereka dapat menggunakan sistem tersebut dengan efektif dan efisien dalam mendukung proses-proses bisnis.

Standar Umum Pengadaan Sumberdaya TI

1. Pengendalian Pengadaan: Kembangkan dan ikuti sebuah rangkaian prosedur dan standar yang konsisten dengan proses pengadaan dan strategi akuisisi organisasi secara keseluruhan untuk memperoleh infrastruktur, fasilitas-fasilitas, hardware, software dan jasa-jasa yang berhubungan dengan TI yang dibutuhkan oleh bisnis.
2. Manajemen Kontrak Supplier: Buatlah sebuah prosedur untuk membuat, memodifikasi dan mengakhiri kontrak untuk semua supplier. Prosedur

tersebut minimal harus meliputi tanggung jawab dan kewajiban (*liability*) hukum, keuangan, organisasional, dokumentasi, kinerja, keamanan, properti intelektual, dan pengakhiran (termasuk pasal-pasal penalti). Semua kontrak dan perubahannya harus direvisi oleh penasehat-penasehat hukum.

3. Pemilihan Supplier: Seleksi supplier sesuai dengan praktek yang adil dan formal untuk memastikan bahwa yang terbaik adalah yang sesuai dengan kebutuhan-kebutuhan yang telah ditentukan sebelumnya. Kebutuhan-kebutuhan tersebut harus dioptimalkan dengan masukan dari para supplier yang potensial.
4. Akuisisi Sumber Daya: Lindungi dan perkuat hak/kepentingan organisasi dalam semua persetujuan kontrak akuisisi, termasuk hak dan kewajiban semua pihak dalam syarat-syarat kontrak untuk akuisisi software, sumber daya pengembangan, infrastruktur dan jasa.

Standar Umum Pengelolaan Perubahan

1. Prosedur dan Standar Perubahan: Lindungi dan perkuat hak/kepentingan organisasi dalam semua persetujuan kontrak akuisisi, termasuk hak dan kewajiban semua pihak dalam syarat- syarat kontrak untuk akuisisi software, sumber daya pengembangan, infrastruktur dan jasa.
2. Penilaian Dampak, Penentuan Prioritas, dan Otorisasi: Nilai semua permintaan untuk perubahan dalam sebuah cara terstruktur untuk menentukan dampaknya pada sistem operasi beserta fungsinya.

Pastikan bahwa semua perubahan telah dikategorikan, dibuat prioritasnya, dan diotorisasi.

3. Perubahan Darurat: Buatlah sebuah proses untuk menentukan, mengangkat, menguji, mendokumentasikan, menilai, dan mengotorisasi perubahan-perubahan darurat yang tidak mengikuti proses perubahan yang telah ditetapkan
4. Penjejakan dan Pelaporan Status Perubahan:
   a. Buatlah sebuah sistem pencatatan dan pelaporan untuk mendokumentasikan perubahan- perubahan yang ditolak, mengkomunikasikan status dari perubahan-perubahan berjalan yang telah disetujui, dan melengkapi/menyelesaikan perubahan.
   b. Pastikan bahwa perubahan-perubahan yang telah disetujui telah diimplementasikan sesuai dengan yang telah direncanakan.
5. Penutupan dan Dokumentasi Perubahan: Kapanpun perubahan diimplementasikan, perbarui sistem yang terkait beserta dokumentasi dan prosedur pemakai sesuai dengan perubahannya.

Standar Umum Instalasi dan Akreditasi Solusi dan Perubahan

1. Pelatihan: Latih anggota staf dari departemen-departemen pemakai dan kelompok-kelompok operasi fungsi TI yang bersangkutan sesuai dengan rencana pelatihan dan implementasi yang telah ditentukan dan materi-materi yang bersangkutan, sebagai bagian dari setiap proyek pengembangan, implementasi, dan modifikasi sistem informasi.

2. Rencana Pengujian: Buatlah sebuah rencana pengujian yang didasarkan pada standar-standar yang menentukan peranan, tanggung-jawab, dan kriteria masuk dan keluar. Pastikan bahwa rencana tersebut disetujui oleh pihak-pihak yang relevan.
3. Rencana Implementasi: Buatlah sebuah rencana implementasi dan penghentian/mundur/penarikan (*fallback*).
4. Dapatkan persetujuan dari pihak-pihak yang relevan.
5. Lingkungan Pengujian: Tentukan dan buatlah sebuah representatif lingkungan pengujian yang aman sesuai dengan keamanan, pengendalian, praktek-praktek operasional, kebutuhan-kebutuhan kualitas dan privasi data, dan juga beban kerja.
6. Konversi Sistem dan Data: Rencanakan konversi data dan migrasi infrastruktur sebagai bagian dari metode-metode pengembangan organisasi, termasuk di dalamnya audit trail, *rollback* dan *fallback*.
7. Pengujian Perubahan: Ujilah perubahan yang ada secara independen dalam hubungannya dengan rencana pengujian yang telah ditentukan sebelum migrasi ke lingkungan operasional. Pastikan bahwa rencana tersebut mempertimbangkan keamanan dan kinerja.
8. Uji Penerimaan Final
    a. Pastikan bahwa para pemilik proses bisnis dan para *stakeholder* TI mengevaluasi keluaran dari proses pengujian seperti yang telah ditentukan oleh rencana pengujian.
    b. Perbaiki eror-eror signifikan yang teridentifikasi dalam proses pengujian, setelah menyelesaikan rangkaian pengujian yang telah ditentukan dalam

rencana pengujian berikut semua pengujian-pengujian kegagalan (regresi) yang diperlukan.

9. Promosi ke Produksi
   a. Setelah pengujian, kendalikan penyerahan sistem yang telah berubah kepada operasi, sesuai dengan rencana implementasi. Dapatkan persetujuan dari stakeholder kunci, seperti para pemakai, pemilik sistem dan manajemen operasional.
   b. Jika memungkinkan, jalankan sistem baru tersebut paralel dengan sistem yang lama untuk sementara waktu, dan bandingkan perilaku dan hasil-hasilnya.

10. Kajian Pasca-Implementasi: Buatlah prosedur-prosedur yang sesuai dengan standar-standar manajemen perubahan organisasi untuk mendapatkan sebuah revisi pasca-implementasi seperti yang ditetapkan dalam rencana implementasi

Standar Umum Pengelolaan Layanan Pihak Ketiga

1. Identifikasi Semua Hubungan Supplier: Identifikasi semua jasa supplier dan kategorikan meraka berdasarkan tipe, signifikansi dan pentingnya supplier. Peliharalah dokumentasi mengenai hubungan-hubungan teknis dan organisasional yang meliputi peran dan tanggung jawab, tujuan dan sasaran, hasil-hasil yang diharapkan, dan kualifikasi (kredensi) dari perwakilan supplier-supplier ini.
2. Manajemen Hubungan Supplier: Formalisasikan proses manajemen hubungan supplier untuk setiap supplier. Para pemilik hubungan harus menjadi

penghubung pada masalah-masalah pelanggan dan supplier dan memastikan kualitas dari hubungan tersebut didasari dengan kepercayaan dan transparansi (misal, melalui SLA).

3. Manajemen Resiko Supplier:
   a. Identifikasi dan mitigasi resiko-resiko yang berhubungan dengan kemampuan para supplier untuk terus memberikan jasa secara efektif dengan aman dan efisien secara terus menerus/ berkelanjutan.
   b. Pastikan bahwa kontrak-kontrak yang ada telah memenuhi standar-standar bisnis universal sesuai dengan syarat-syarat hukum dan pengaturan.
   c. Manajemen resiko selanjutnya harus mempertimbangkan perjanjian-perjanjian non-disclosure (non-*disclosure agreements* (NDA's)), kontrak-kontrak escrow, kelayakan supplier yang berlanjut/terus dipakai, kesesuaian dengan syarat-syarat keamanan, supplier-supplier alternatif, penalti-penalti dan penghargaan-penghargaan, dll.
   d. Pemantauan Kinerja Supplier: Buatlah sebuah proses untuk rrrengawasi penyampaian jasa untuk memastikan bahwa supplier tersebut telah memenuhi kebutuhan-kebutuhan bisnis yang ada dan terus menepati perjanjian-perjanjian kontrak dan SLA, dan juga bahwa kinerjanya kompetitif/bersaina dengan supplier-supplier alternatif dan kondisi pasar.

Standar Umum Pengelolaan Kinerja dan Kapasitas

1. Perencanaan Kinerja dan Kapasitas:
   a. Buatlah sebuah proses perencanaan untuk merevisi kinerja dan kapasitas sumber daya TI untuk memastikan bahwa kapasitas dan kinerja yang cost-justifiable (memadai dalam hal biaya) telah tersedia untuk memproses beban-beban kerja yang telah disetujui seperti yang telah ditentukan oleh SLA.
   b. Rencana-rencana kapasitas dan kinerja harus mengangkatimengatur teknik-teknik model yang sesuai untuk menghasilkan sebuah model dari kinerja, kapasitas dan throughput yang ada dan kinerja yang diperkirakan dari sumber daya TI.
2. Kinerja dan Kapasitas Sekarang: Nilailah kinerja dan kapasitas sumber daya TI sekarang untuk menentukan apakah kapasitas dan kinerjanya sudah mencukupi untuk menghasilkan tingkat-tingkat layanan yang telah disetujui sebelumnya.
3. Kinerja dan Kapasitas Mendatang
   a. Adakan perkiraan kinerja dan kapasitas sumber daya TI dengan jarak waktu yang teratur untuk meminimalisir resiko terputusnya layanan karena kapasitasnya tidak mencukupi atau buruknya kinerja, serta identifikasi kelebihan kapasitas untuk kemungkinan relokasi (*redeployment*).
   b. Identifikasi kecenderungan-kecenderungan beban kerja dan tentukan perkiraan-perkiraan untuk dimasukkan ke dalam rencana-rencana kinerja dan kapasitas.

4. Ketersediaan Sumber Daya TI
    a. Sediakan kapasitas dan kinerja yang dibutuhkan, dengan mempertimbangkan aspek-aspek seperti beban kerja normal, kontinjensi, kebutuhan-kebutuhan penyimpanan (*storage*) dan daur hidup sumber daya TI. Provisi-provisi seperti penentuan prioritas tugas, mekanisme- mekanisme toleransi kesalahan dan praktek-praktek alokasi sumber daya harus dibuat.
    b. Manajemen harus memastikan apakah rencana-rencana kontinjensi telah dengan benar memperhatikan ketersediaan, kapasitas, dan kinerja masing-masing sumber daya TI.

5. Pemantauan dan Pelaporan, pantau secara terus-menerus kinerja dan kapasitas dari sumber daya TI. Data yang dikumpulkan harus memenuhi dua maksud berikut:
    a. Untuk menjaga dan menyesuaikan kinerja sekarang dalam TI dan menangani masalah-masalah seperti kekenduran (*resilience*), kontinjensi, beban-beban kerja sekarang. dan yang diproyeksikan, rencana-rencana penyimpanan, dan akuisisi sumber daya.
    b. Untuk melaparkan ketersediaan jasa yang diserahkan kepada bisnis, seperti yang diminta dalam SLA.
    c. Sertakan semua laporan pengecualian (eksepsi) dengan rekomendasi-rekomendasi.

Standar Umum Identifikasi dan Alokasi Biaya

1. Definisi Layanan: Identifikasi semua biaya, dan petakan biaya-biaya tersebut dalam layanan- layanan TI untuk mendukung suatu model biaya yang transparan. Layanan-layanan TI harus dihubungkan dengan proses-proses bisnis seperti bagaimana bisnis tersebut dapat mengidentifikasikan tingkatan-tingkatan penagihan (*billing*) layanan yang terkait.
2. Akunting: Catat (*capture*) dan alokasikan biaya-biaya aktual sesuai dengan model biaya perusahaan. Varian-varian antara biaya perkiraan dengan biaya aktual harus dianalisa dan dilaporkan, sesuai dengan sistem-sistem pengukuran keuangan milik perusahaan.
3. Pemodelan Biaya dan Pembebanan
   a. Buatlah dan gunakan sebuah model pembiayaan TI berdasarkan definisi-definisi layanan yang mendukung penghitungan tingkat charge-back untuk tiap layanan.
   b. Model biaya TI tersebut harus memastikan bahwa permintaan pembayaran (*charge*) layanan dapat diidentifikasi, diukur dan diperkirakan oleh para pemakai untuk mendorong terciptanya pemakaian sumber daya dengan balk.
4. Pemeliharaan Model Biaya: Revisi dan buat target (*benchmark*) kesesuaian model recharge biaya (*cost-recharge*) untuk mempertahankan relevansi dan kesesuaiannya dengan aktivitas- aktivitas bisnis dan TI yang terus berevolusi.

Standar Umum Pengelolaan Service Desk dan Insiden

1. *Service Desk*
   a. Buatlah sebuah fungsi meja layanan (*service desk*), dimana para pengguna bertemu dengan TI, untuk mendaftar, mengkomunikasikan, melakukan dan menganalisa semua panggilan, kejadian-kejadian yang dilaporkan, permintaan-permintaan akan layanan dan permintaan-permintaan akan informasi.
   b. Harus terdapat prosedur-prosedur pemantauan dan pengangkatan (eskalasi) berdasarkan tingkatan-tingkatan layanan yang telah disetujui yang berhubungan (relatif) dengan SLA yang sesuai agar memungkinkan pengklasifikasian dan penentuan prioritas untuk setiap masalah yang dilaporkan, seperti sebuah masalah, permintaan akan layanan atau permintaan akan informasi.
   c. Ukurlah kepuasan para pemakai akhir terhadap kualitas meja layanan dan layanan-layanan TI.

2. Registrasi *Customer Query*
   a. Buatlah sebuah fungsi dan sistem yang memungkinkan penyortiran (*logging*) dan pencatatan/perunutan semua panggiIan, kejadian, permintaan akan layanan dan kebutuhan informasi.
   b. Fungsi dan sistem tersebut harus dapat bekerja tidak jauh dari proses-proses seperti manajemen kejadian, manajemen masalah, manajemen perubahan, manajemen kapasitas dan manajemen ketersediaan.
   c. Semua kejadian harus diklasifikasikan sesuai dengan prioritas layanan dan diserahkan kepada

tim manajemen masalah yang sesuai, jika diperlukan.

d. Para pelanggan harus terus diinformasikan mengenai status keluhan/permintaan mereka (*query*).

3. Eskalasi Insiden:
   a. Buatlah prosedur-prosedur meja layanan, sehingga kejadian-keadian yang tidak dapat diselesaikan dengan segera dapat diangkat (dieskalasi) sesuai dengan batasan-batasan yang didefinisikan di dalam SLA dan, jika memungkinkan, sediakan workarounds.
   b. Pastikan bahwa kepemilikan kejadian dan pemantauan daur hidup tetap berada pada meja layanan karena kejadian-kejadian ini adalah kejadian-kejadian berbasis pemakai (*user-based*), tanpa melihat kelompok TI mana yang sedang mengerjakan tindakan-tindakan perbaikannya.

4. Penutupan Insiden:
   a. Buatlah prosedur-prosedur untuk pemantauan yang sesuai atas penyelesaian keluhan/permintaan pelanggan. Jika suatu kejadian telah diselesaikan, pastikan bahwa meja layanan mencatat langkah-langkah penyelesaiannya, dan memastikan bahwa tindakan yang diambil telah disetujui oleh pelanggan.
   b. Catat dan laporkan juga kejadian-kejadian yang tidak terselesaikan (eror-eror dan *workaround* yang diketahui) untuk menyediakan informasi kepada manajemen masalah yang sesuai.

5. Pelaporan dan Trend Analysis: Buatlah laporan-laporan atas aktivitas meja layanan agar manajemen dapat mengukur kinerja layanan dan waktu respon layanan serta dapat mengidentifikasi kecenderungan-kecenderungan atau masalah-masalah yang berulang, sehingga pelayanan dapat terus ditingkatkan.

Standar Umum Pengelolaan Konfigurasi

1. Repositori Konfigurasi dan Baseline:
   a. Buatlah sebuah perangkat pendukung dan sebuah penyimpanan sentral (*central repository*) untuk menyimpan seluruh informasi yang relevan pada item-item konfigurasi. Pantau dan catat semua aset dan perubahan pada aset.
   b. Pertahankan sebuah garis dasar dari item-item konfigurasi untuk setiap sistem dan layanan sebagai sebuah titik (*checkpoint*) kemana harus kembali setelah mengalami perubahan-perubahan.

2. ldentifikasi dan Pemeliharaan Configuration Item:
   a. Buatlah prosedur-prosedur konfigurasi untuk mendukung manajemen dan penyortiran semua perubahan pada penyimpanan konfigurasi.
   b. Integrasikan prosedur-prosedur ini dengan proses-proses manajemen perubahan, manajemen kejadian dan manajemen masalah.
   c. Telaah Integritas Konfigurasi: Revisi secara periodik data konfigurasi untuk memastikan dan mengkonfirmasi integritas dari konfigurasi sekarang dan yang lalu. Revisi secara periodik

terhadap software yang diinstal berdasarkan kebijakan pemakaian software untuk mengidentifikasi software personal atau tidak berlisensi atau setiap instance sebagai akibat dari persetujuan-persetujuan lisensi yang ada. Laporkan, tindaki, dan perbaiki eror dan penyimpangan yang ada.

Standar Umum Pengelolaan Problem

1. Identifikasi dan Klasifikasi Problem:
   a. Implementasikan proses-proses untuk melaporkan dan mengklasifikasikan masalah-masalah yang telah teridentifikasi sebagai bagian dari manajemen kejadian. Langkah- Iangkah yang termasuk di dalam klasifikasi masalah serupa dengan langkah-langkah dalam klasifikasi kejadian; langkah-langkah tersebut adalah menentukan kategori, dampak, kepentingan dan prioritas.
   b. Kategorikan masalah-masalah dengan benar ke dalam kelompok-kelompok atau area-area (domain) yang berhubungan (misal, hardware, software, software pendukung).
   c. Kelompok-kelompok ini mungkin sesuai dengan tanggung jawab organisasional berbasis pemakai dan pelanggan, dan harus merupakan dasar untuk pengalokasian masalah-masalah kepada staf pendukung.

2. Problem Tracking dan Resolusi, pastikan bahwa sistem manajemen masalah menyediakan fasilitas-fasilitas penelusuran audit (*audit trail*) yang memadai yang

memungkinkan perunutan (*tracking*), analisa dan penentuan akar penyebab dari semua masalah yang dilaporkan dengan mempertimbangkan:

a. Semua item-item konfigurasi yang terkait
b. Masalah-masalah dan kejadian-kejadian yang belum diselesaikan (masih *outstanding*)
c. Eror-eror yang diketahui dan diduga
d. Perunutan (*tracking*) kecenderungan-kecenderungan masalah
e. Identifikasi dan mulailah solusi-solusi yang dapat dilanjutkan yang menangani peyebab akar, mengangkat permintaan-permintaan akan perubahan melalui proses manajemen perubahan yang telah dibuat.
f. Selama proses resolusi, manajemen masalah seharusnya mendapatkan laporan-laporan regular dari manajemen perubahan mengenal kemajuan dalam penyelesaian masalah dan eror.
g. Manajemen masalah harus memantau dampak yang berlanjut dari masalah-masalah dan eror-eror yang telah diketahui pada layanan pemakai. Dalam kejadian ketika dampak menjadi besar, manajemen masalah harus mengangkat masalah ini, kemudian mengacu masalah ini kepada dewan yang sesuai untuk meningkatkan prioritas dari RFC atau untuk mengimplementasikan perubahan darurat yang sesuai.
h. Pantau kemajuan dari penyelesaian masalah tersebut terhadap SLA.

3. Penutupan Problem: Buatlah sebuah prosedur untuk menutup catatan-catatan masalah baik setelah

konfirmasi kesuksesan eliminasi eror yang diketahui maupun setelah persetujuan dengan bisnis mengenai alternatif lain bagaimana menangani masalah tersebut

4. Integrasi Manajemen Konfigurasi, Insiden dan Problem: Integrasikan proses-proses manajemen konfigurasi, kejadian dan masalah yang terkait untuk memastikan efektifitas manajemen masalah dan memungkingkan terciptanya peningkatan-peningkatan.

Standar Umum Pengelolaan Lingkungan Fisik

1. Pemilihan dan Layout Lokasi:
   a. Tentukan dan seleksi situs-situs fisik untuk peralatan TI untuk mendukung strategi teknologi yang berhubungan dengan strategi bisnis.
   b. Penyeleksian dan rancangan dari tampilan (layout) sebuah situs selain harus memperhitungkan resiko yang berhubungan dengan bencana alam dan bencana buatan manusia, juga harus mempertimbangkan hukum-hukum dan peraturan-peraturan yang relevan, seperti peraturan kesehatan dan keamanan pekerjaan.

2. Tindakan Pengamanan Fisik:
   a. Tentukan dan implementasikan ukuran-ukuran keamanan fisik sesuai dengan kebutuhan-kebutuhan bisnis untuk mengamankan fokasi dan aset-aset fisik.
   b. Ukuran-ukuran keamanan fisik harus mampu secara efektif mencegah, mendeteksi dan memitigasi resiko yang berhubungan dengan

pencurian, suhu, kebakaran, asap, air, getaran, teror, pengrusakan, mati listrik (*power outage*), bahan-bahan kimia atau bahan- bahan peledak.

3. Akses Fisik:
   a. Tentukan dan implementasikan prosedur-prosedur untuk memberikan, membatasi dan membatalkan akses ke dalam lokasi-lokasi, gedung-gedung dan area-area sesuai dengan kebutuhan bisnis, termasuk pada saat darurat.
   b. Akses ke dalam lokasi, gedung dan area harus disesuaikan, diotorasi, disortir dan dimonitor.
   c. Hal ini harus diaplikasikan kepada semua orang yang memasuki lokasi-lokasi tersebut, termasuk staf, staf sementara, para klien, supplier, pengunjung atau pihak ketiga lainnya.
   d. Proteksi terhadap faktor-faktor lingkungan: Rancang dan implementasikan ukuran-ukuran untuk memberikan perlindungan dari faktor-faktor lingkungan. Pasanglah peralatan dan perangkat khusus untuk memantau dan mengendalikan lingkungan.

4. Manajemen Fasilitas Fisik: Aturlah fasilitas-fasilitas, termasuk peralatan listrik (power) dan komunikasi, sesuai dengan hukum dan peraturan yang berlaku, kebutuhan-kebutuhan teknis dan bisnis, spesifikasi-spesifikasi supplier, serta pedoman-pedoman kesehatan dan keamanan.

Standar Umum Pengelolaan Operasi

1. Prosedur dan Instruksi Operasi:
   a. Tentukan, implementasikan dan pertahankan prosedur-prosedur untuk operasi-operasi TI, dengan memastikan bahwa para anggota staf operasi telah mengenali dengan baik seluruh tugas-tugas pengoperasian yang relevan dengan mereka.
   b. Prosedur-prosedur operasional harus meliputi pertukaran shift kerja (penyerahan formal atas aktivitas, update status, masalah-masalah operasional, prosedur-prosedur pengangkatan dan laporan-laporan mengenai tanggung jawab yang berjalan) untuk mendukung tingkatan-tingkatan layanan yang telah disetujui dan untuk memastikan kelangsungan operasi.
2. *Job Scheduling*: Aturlah penjadwalan pekerjaan, proses dan tugas ke dalam urutan yang paling efisien dengan memaksimalkan throughput dan kegunaannya (utilisasi) untuk memenuhi kebutuhan-kebutuhan bisnis.
3. Pemantauan Sumber Daya TI:
   a. Tentukan dan implementasikan prosedur-prosedur untuk memantau infrastruktur TI dan kejadian-kejadian yang berhubungan.
   b. Pastikan bahwa informasi kronologis yang cukup telah disimpan dalam jurnal-jurnal (log) pengoperasian agar dapat dilakukan rekonstruksi, revisi dan pengujian (eksaminasi) atas urutan waktu dari berbagai operasi dan aktivitas-aktivitas lainnya yang ada di sekitar atau mendukung operasi-operasi tersebut.

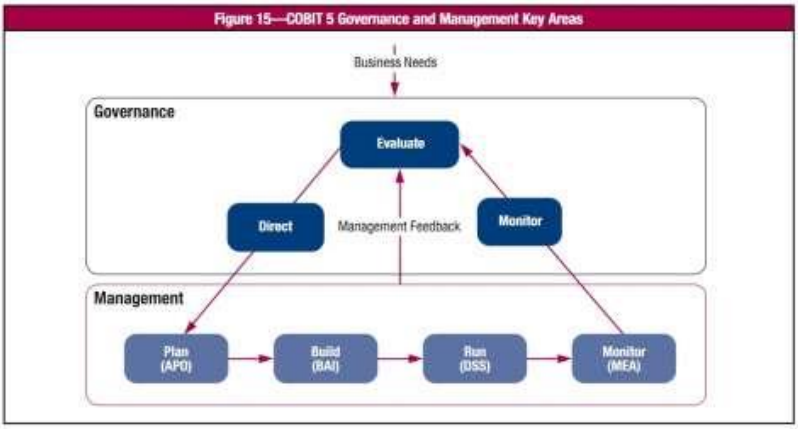
4. Peralatan Output dan Dokumen Sensitif: Buatlah pengamanan-pengamanan fisik, praktek-praktek akuntansi dan manajemen persediaan untuk aset-aset TI yang efektif, seperti formulir-formulir khusus, instrumen-instrumen yang dapat dinegosiasikan, printer-printer khusus atau kartu-kartu (token) keamanan.
5. *Preventive Maintenance* untuk *Hardware*: Tentukan dan implementasikan prosedur-prosedur untuk memastikan pemeliharaan infrastruktur dengan sesuai untuk mengurangi frekuensi dan dampak dari kegagalan-kegagalan atau buruknya kinerja.

4.4 Model Referensi dan Domain Framework COBIT 5

COBIT (*Control Objective for Information and related Technology)* merupakan panduan dari ISACA yang membahas tentang tata kelola dan manajemen teknologi informasi.

1. Tata Kelola, memuat lima proses tata kelola, dimana akan ditentukan praktik-praktik dalam setiap proses *Evaluate, Direct, dan Monitor* (EDM).
2. Manajemen, memuat empat domain, sejajar dengan area tanggung jawab dari *Plan, Build, Run, and Monitor* (PBRM), dan menyediakan ruang lingkup TI yang menyeluruh dari ujung ke ujung. Domain ini merupakan evolusi dari domain dan struktur proses dalam COBIT 4.1, yaitu:
   a. *Align, Plan, and Organize* (APO) – Penyelarasan, Perencanaan, dan Pengaturan.
   b. *Build, Acquare, and Implement* (BAI) – Membangun, Memperoleh, dan Mengimplementasikan.

c. *Deliver, Service and Support* (DSS) – Mengirimkan, Layanan, dan Dukungan.
d. *Monitor, Evaluate, and Assess* (MEA) – Pengawasan, Evaluasi, dan Penilaian.



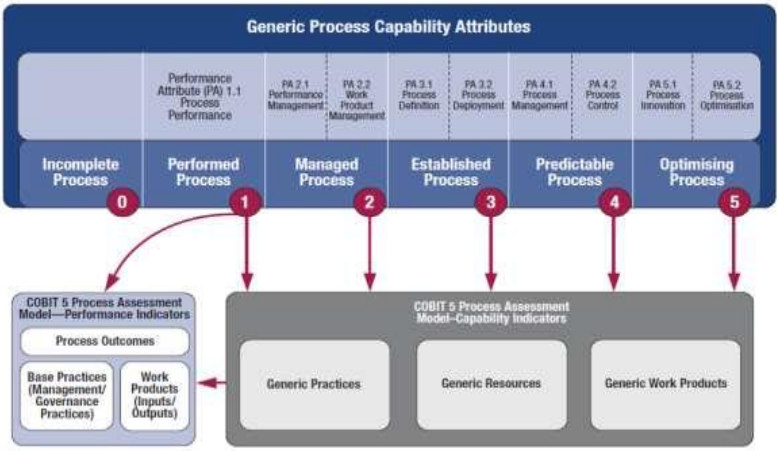
Gambar 4.6. Model Referensi Proses dalam COBIT 5

Pada gambar 1. dan gambar 2. menunjukkan enam tingkatan kapabilitas yang dapat dicapai oleh masing-masing proses, yaitu:

0. *Incomplete Process* – Proses tidak lengkap.
1. *Performed Process* – Proses dijalankan (satu atribut); Proses yang diimplementasikan berhasil mencapai tujuannya.
2. *Managed Process* – Proses teratur (dua atribut); Proses yang telah dijalankan seperti di atas telah diimplementasikan dalam cara yang lebih teratur (direncanakan, dipantau, dan disesuaikan).
3. *Established Process* – Proses tetap (dua atribut); Proses di atas telah diimplementasikan menggunakan proses

tertentu yang telah ditetapkan, yang mampu mencapai outcome yang diharapkan.

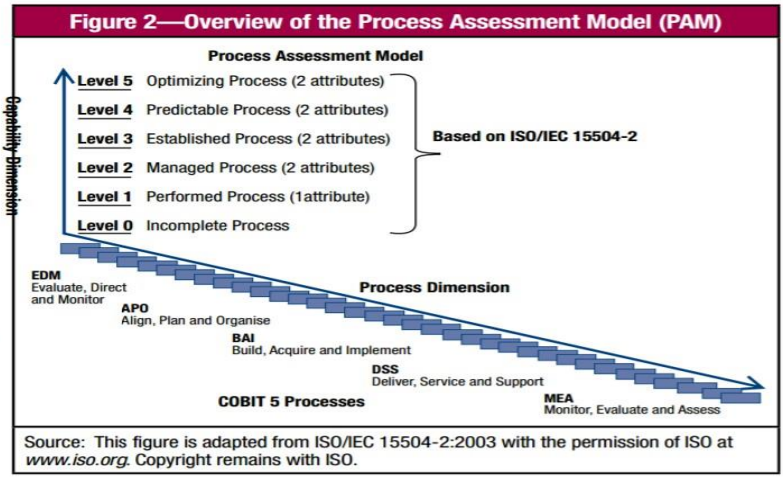
4. *Predictable Process* – Proses yang dapat diprediksi (dua atribut); Proses di atas telah dijalankan dalam batasan yang ditentukan untuk mencapai outcome proses yang diharapkan.
5. *Optimising Process* – Proses Optimasi (dua atribut); Proses di atas terus ditingkatkan secara berkelanjutan untuk memenuhi tujuan bisnis saat ini dan masa depan.



Gambar 4.7. Model Kematangan Proses dalam COBIT 5

4.5 COBIT 5 *Process Assessment* Model (PAM)

Proses *assessment* model merupakan model pengukuran yang digunakan dalam COBIT 5, di COBIT version 4.1 dikenal dengan COBIT maturity model. PAM di cobit 5 terbagi menjadi dua bagian, yang pertama adalah teknik pengukuran skala bertingkat (*scale rating*) yang digunakan untuk menilai bagian yang kedua yaitu dimensi proses yang terdiri dari 5 dimensi proses EDM, APO, BAI, DSS dan MEA [5]. Penilaian didasarkan berupa bukti untuk memastikan bahwa proses penilaian dapat diandalkan, konsisten, dan dapat dilakukan secara rutin di area tata kelola dan manajemen TI.



Gambar 4.8. COBIT 5 *Process Assessment* Model (PAM)

Pada Gambar 3, menjelaskan process assessment model terbagi menjadi 2 dimensi yaitu dimensi proses dan dimensi kapabilitas. Pada dimensi proses

menggambarkan proses menguraikan COBIT 5, sedangkan dimensi kapabilitas menjelaskan tingkat kematangan proses mulai dari level 0 sampai level 5.

4.6 Indikator Proses Kapabilitas

Indikator proses kapabilitas adalah kemampuan proses dalam meraih tingkat kapabilitas yang ditentukan oleh atribut proses. Dimensi kapabilitas mencakup enam tingkat kapabilitas, terdapat sembilan atribut proses

Tabel 4.1. Proses Kapabilitas Model Skala Kematangan Level Kapabilitas Value

No.	Skala Kematangan	Level Kapabilitas	Value
1.	0,00 – 0,50	Level 0	*Incomplete Process*
2.	0,51 – 1,50	Level 1	*Performed Process*
3.	1,51 – 2,50	Level 2	*Managed Process*
4.	2,51 – 3,50	Level 3	*Established Process*
5.	3,51 – 4,50	Level 4	*Predictable Process*
6.	4,51 – 5,00	Level 5	*Optimizing Process*

Tabel 1. menunjukkan indikator proses kapabilitas assessment model dibagi menjadi beberapa tingkatan yaitu:

1) Level 0 – *Incomplete Process:* Proses yang belum atau gagal diimplementasikan.

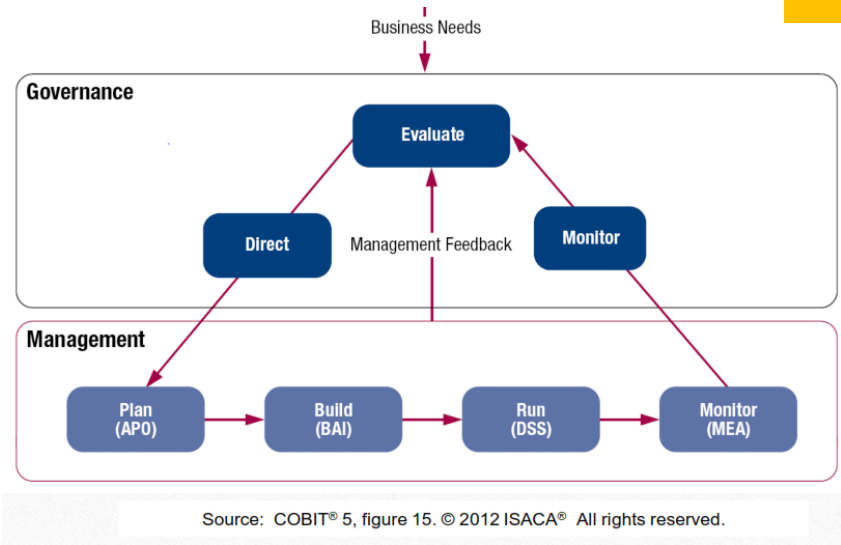
2) Level 1 – *Performed Process:* Proses yang menentukan tercapainya tujuan.
3) Level 2 – *Managed Process:* Proses yang mencakup perencanaan, monitor, dan penyesuaian.
4) Level 3 – *Established Process:* Proses yang sudah dibangun kemudian diimplementasikan untuk mencapai hasil dari proses.
5) Level 4 – *Predictable Process:* Proses yang sudah dibangun kemudian dioperasikan dengan batasan-batasan yang mampu meraih harapan dari proses.
6) Level 5 – *Optimizing Process:* Proses yang diprediksi secara terus-menerus ditingkatkan untuk memenuhi tujuan bisnis dan tujuan perusahaan.

BAB 5

PENERAPAN AUDIT SISTEM INFORMASI PADA *E-GOVERNMENT*

5.1 Kondisi Saat Ini

Kondisi saat ini dilakukan untuk mengetahui kendala-kendala dan memetakan capaian tingkat kematangan penerapan e-*government* pada Pemerintah Kota Padang. Analisa sistem bertujuan untuk memperoleh tingkat kematangan saat ini yang digunakan sebagai data diuji dan metode COBIT 5.0 yang diterapkan. Penelitian ini akan menganalisis dan mengevaluasi tingkat kematangan penerapan e-*government* di Kota Padang untuk membantu pihak Dinas Komunikasi dan Informasi Kota Padang dalam menentukan prioritas domain/aspek/indikator dalam mengambil kebijakan dan strategi dalam mengambil keputusan pengembangan e-*government* untuk menuju Sistem Pemerintahan Berbasis Elektronik (SPBE) yang berkualitas dengan capaian sangat baik.



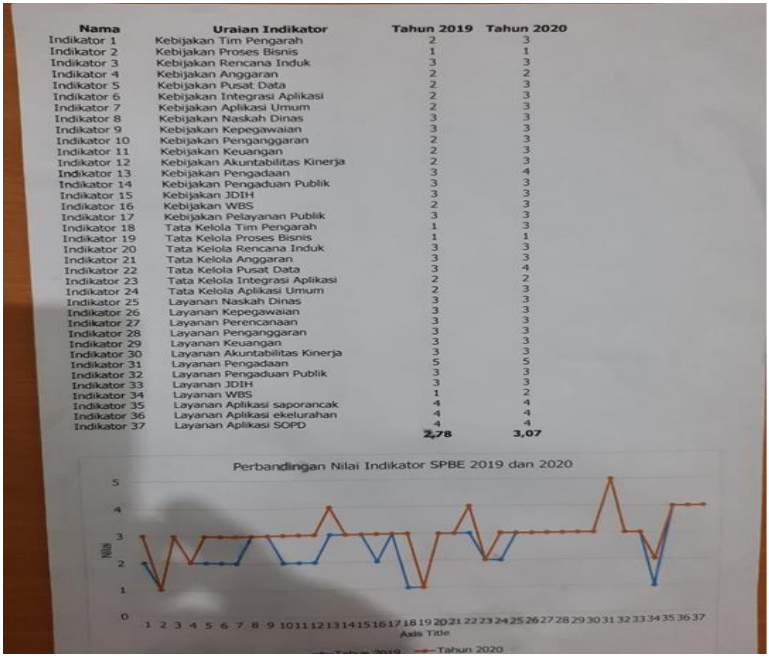
Source: COBIT® 5, figure 15. © 2012 ISACA® All rights reserved.

Gambar 5.1 Model Referensi Proses *dalam COBIT 5*

Bab ini membahasan tentang penerapan audit teknologi informasi pada e-government menggunakan model referensi proses dalam COBIT 5 seperti yang ditujukkan pada gambar 5.1, bahwa tahapan kerja terdiri dari mengidentifikasi masalah, menentukan tujuan, mempelajari literatur, memberikan rekomendasi untuk perbaikan selanjutnya. Pada penelitian ini yang menjadi *Capability Model* merupakan alat ukur untuk mengetahui kondisi proses IT pada e-Goverment di Pemerintah Kota Padang. Kegiatan analisis dan evaluasi serta pengukuran ini akan menghasilkan penilaian tentang kondisi sekarang dari proses domain sebagai berikut (1). APO (*Align, Plan and Organize*) untuk mengetahui tingkat kematangan perencanaan e-*government* di Pemerintah Kota Padang, (2). Evaluate, Direct, and Monitor (EDM), (3). *Build, Acquire, and*

Implement (BAI), (4). *Deliver, Service and Support* (DSS). COBIT 5 Model Referensi Proses (PRM) akan digunakan terutama untuk mendefinisikan domain dan ruang lingkup, tujuan proses dan hasil proses. Kerangka Pengukuran (MF) ISO / IEC 15504 akan memandu dalam menentukan tingkat kemampuan, atribut proses, dan skala peringkat. Process Assessment Model (PAM) harus mendefinisikan ruang lingkup, indikator, pemetaan dan terjemahan COBIT 5 PRM dan ISO/IEC 15504 MF ke dalam proses penilaian. Masukan awal untuk proses asesmen adalah informasi tentang proses, yaitu: tujuan, ruang lingkup, kendala, pengidentifikasi, pendekatan, domain, indikator, dan informasi tambahan lainnya. Proses penilaian membutuhkan peran dan tanggung jawab responden. Output dari proses penilaian dari input untuk mengidentifikasi bukti, proses penilaian yang digunakan, profil proses, dan informasi tambahan lainnya seperti diperlihatkan pada gambar 5.2.

5.2 Kondisi Data Saat ini dan Domain COBIT 5.0



Nama	Uraian Indikator	Tahun 2019	Tahun 2020
Indikator 1	Kebijakan Tim Pengarah	2	3
Indikator 2	Kebijakan Proses Bisnis	1	1
Indikator 3	Kebijakan Rencana Induk	3	3
Indikator 4	Kebijakan Anggaran	2	2
Indikator 5	Kebijakan Pusat Data	2	3
Indikator 6	Kebijakan Integrasi Aplikasi	2	3
Indikator 7	Kebijakan Aplikasi Umum	2	3
Indikator 8	Kebijakan Naskah Dinas	3	3
Indikator 9	Kebijakan Kepegawaian	3	3
Indikator 10	Kebijakan Penganggaran	2	3
Indikator 11	Kebijakan Keuangan	2	3
Indikator 12	Kebijakan Akuntabilitas Kinerja	2	3
Indikator 13	Kebijakan Pengadaan	3	4
Indikator 14	Kebijakan Pengaduan Publik	3	3
Indikator 15	Kebijakan JDIH	3	3
Indikator 16	Kebijakan WBS	2	3
Indikator 17	Kebijakan Pelayanan Publik	3	3
Indikator 18	Tata Kelola Tim Pengarah	1	3
Indikator 19	Tata Kelola Proses Bisnis	1	1
Indikator 20	Tata Kelola Rencana Induk	3	3
Indikator 21	Tata Kelola Anggaran	3	3
Indikator 22	Tata Kelola Pusat Data	3	4
Indikator 23	Tata Kelola Integrasi Aplikasi	2	2
Indikator 24	Tata Kelola Aplikasi Umum	2	3
Indikator 25	Layanan Naskah Dinas	3	3
Indikator 26	Layanan Kepegawaian	3	3
Indikator 27	Layanan Perencanaan	3	3
Indikator 28	Layanan Penganggaran	3	3
Indikator 29	Layanan Keuangan	3	3
Indikator 30	Layanan Akuntabilitas Kinerja	3	3
Indikator 31	Layanan Pengadaan	5	5
Indikator 32	Layanan Pengaduan Publik	3	3
Indikator 33	Layanan JDIH	3	3
Indikator 34	Layanan WBS	1	2
Indikator 35	Layanan Aplikasi saporancak	4	4
Indikator 36	Layanan Aplikasi ekelurahan	4	4
Indikator 37	Layanan Aplikasi SOPD	4	4
		2,78	3,07

(Sumber: Pemko Padang, 19 Agustus 2020)
Gambar 5.2 Hasil pemetaan SPBE 2018 dan 2019

Gambar 4.1 menunjukkan hasil Pengukuran capaian indeks SPBE Kota Padang Tahun 2018 dan 2019, terlihat bahwa ada kenaikan yang segnifikan, untuk mempercepat pengembangan penerapan SPBE terbut diperlukan cara untuk mengetahui skala prioritas agar dapat mengetahui dengan tepat dan akurat aspek/domain mana yang akan dikemabangkan speerti yang diperlihatkan pada Gambar 5.3.

DOMAIN/ASPEK/ INDIKATOR	URAIAN	JUMLAH INDIKATOR	TINGKAT KEMATANGAN (MATURITAS)	NILAI	
				INDEKS	PREDIKAT
DOMAIN-1	KEBIJAKAN INTERNAL SPBE	17	-	2.88	(Baik)
Aspek-1	Kebijakan Internal Tata Kelola SPBE	7	-	2.57	(Cukup)
Indikator-1	Kebijakan Internal Tim Pengarah SPBE Instansi Pemerintah	1	3	0.43	
Indikator-2	Kebijakan Internal Inovasi Proses Bisnis Terintegrasi	1	1	0.14	
Indikator-3	Kebijakan Internal Rencana Induk SPBE Instansi Pemerintah	1	3	0.43	
Indikator-4	Kebijakan Internal Anggaran dan Belanja TIK	1	2	0.29	
Indikator-5	Kebijakan Internal Pengoperasian Pusat Data	1	3	0.43	
Indikator-6	Kebijakan Internal Integrasi Sistem Aplikasi	1	3	0.43	
Indikator-7	Kebijakan Internal Penggunaan Aplikasi Umum Berbagi Pakai	1	3	0.43	
Aspek-2	Kebijakan Internal Layanan SPBE	10	-	3.10	(Baik)
Indikator-8	Kebijakan Internal Layanan Naskah Dinas	1	3	0.30	
Indikator-9	Kebijakan Internal Layanan Manajemen Kepegawaian	1	3	0.30	
Indikator-10	Kebijakan Internal Layanan Manajemen Perencanaan dan Penganggaran	1	3	0.30	
Indikator-11	Kebijakan Internal Layanan Manajemen Keuangan	1	3	0.30	
Indikator-12	Kebijakan Internal Layanan Manajemen Kinerja	1	3	0.30	
Indikator-13	Kebijakan Internal Layanan Pengadaan	1	4	0.40	
Indikator-14	Kebijakan Internal Layanan Pengaduan Publik	1	3	0.30	
Indikator-15	Kebijakan Internal Layanan Dokumentasi dan Informasi Hukum	1	3	0.30	
Indikator-16	Kebijakan Internal Layanan *Whistle Blowing System*	1	3	0.30	
Indikator-17	Kebijakan Internal Layanan Publik Instansi Pemerintah	1	3	0.30	
DOMAIN-2	TATA KELOLA SPBE	7	-	3.00	(Baik)
Aspek-3	Kelembagaan	2	-	3.00	(Baik)
Indikator-18	Tim Pengarah SPBE Instansi Pemerintah	1	3	1.50	
Indikator-19	Inovasi Proses Bisnis Terintegrasi	1	3	1.50	
Aspek-4	Strategi dan Perencanaan	2	-	3.00	(Baik)
Indikator-20	Rencana Induk SPBE Instansi Pemerintah	1	4	2.00	
Indikator-21	Anggaran dan Belanja TIK	1	2	1.00	
Aspek-5	Teknologi Informasi dan Komunikasi	3	-	3.00	(Baik)
Indikator-22	Pengoperasian Pusat Data	1	3	1.00	
Indikator-23	Integrasi Sistem Aplikasi	1	3	1.00	
Indikator-24	Penggunaan Aplikasi Umum Berbagi Pakai	1	3	1.00	
DOMAIN-3	LAYANAN SPBE	11	-	3.36	(Baik)
Aspek-6	Layanan Administrasi Pemerintahan Berbasis Elektronik	7	-	3.29	(Baik)
Indikator-25	Layanan Naskah Dinas	1	3	0.43	
Indikator-26	Layanan Manajemen Kepegawaian	1	3	0.43	
Indikator-27	Layanan Manajemen Perencanaan	1	3	0.43	
Indikator-28	Layanan Manajemen Penganggaran	1	3	0.43	
Indikator-29	Layanan Manajemen Keuangan	1	5	0.71	
Indikator-30	Layanan Manajemen Kinerja	1	3	0.43	
Indikator-31	Layanan Pengadaan	1	3	0.43	
Aspek-7	Layanan Publik Berbasis Elektronik	4	-	3.50	(Sangat Baik)
Indikator-32	Layanan Pengaduan Publik	1	2	0.50	
Indikator-33	Layanan Dokumentasi dan Informasi Hukum	1	4	1.00	
Indikator-34	Layanan *Whistle Blowing System*	1	4	1.00	
Indikator-35	Layanan Publik Instansi Pemerintah	1	4	1.00	

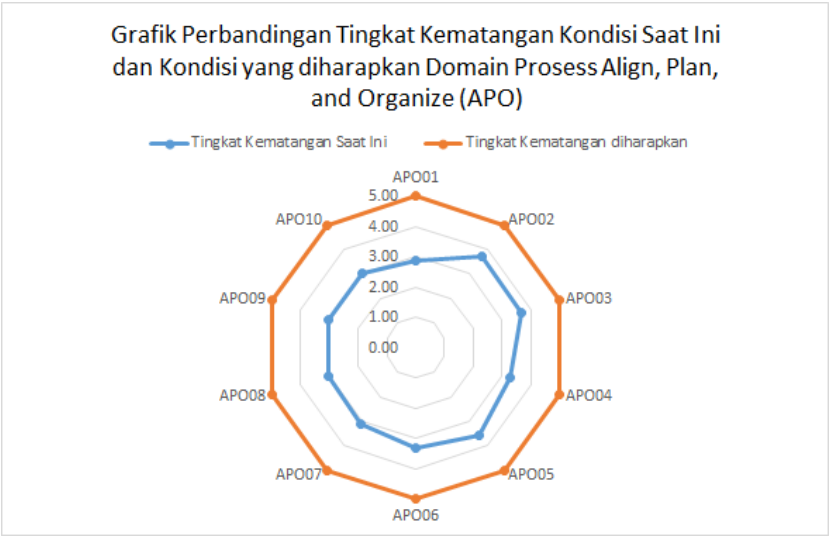
Gambar 5.3. Hasil Pemetaan SPBE 2019 dengan COBIT 5.0

5.3. Verifikasi dan Validasi Hasil dan Strategi Perbaikan

Tabel 5.1. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Align, Plan, and Organize* (APO)

No.	Deskripsi Aktifitas	Tingkat Kematangan Saat Ini	GAP	Tingkat Kematangan diharapkan
1	Mengoptimalkan penempatan fungsi TI	2.85	2.15	5.00
2	Mengelola perbaikan terus-menerus dari proses	3.70	1.30	5.00
3	Back-up dan Restore data terjadwal	3.65	1.35	5.00
4	Dapat menampung pertumbuhan data yang besar	3.25	1.75	5.00
5	Menjaga kepatuhan terhadap kebijakan dan prosedur	3.55	1.45	5.00
6	Mengelola perbaikan terus-menerus dari proses	3.31	1.69	5.00
7	Menggunakan enkripsi dalam pengiriman data	3.09	1.91	5.00
8	Menggunakan User ID dan Password	3.05	1.95	5.00
9	Pengamanan sistem Menggunakan User dan Password	3.01	1.99	5.00
10	Terdapat leveling hak akses data dan application	3.03	1.97	5.00

Tabel 5.1. dan gambar 5.4. Menunjukkan GAP analisis antara tingkat kematangan kondisi saat ini dan tingkat kematangan yang diharapkan, dari hasil analisa GAP menunujukkan bahwa tingkat kematangan untuk domain Align, Plan, and Organize (APO) masuk dalam ***level Established Process.***

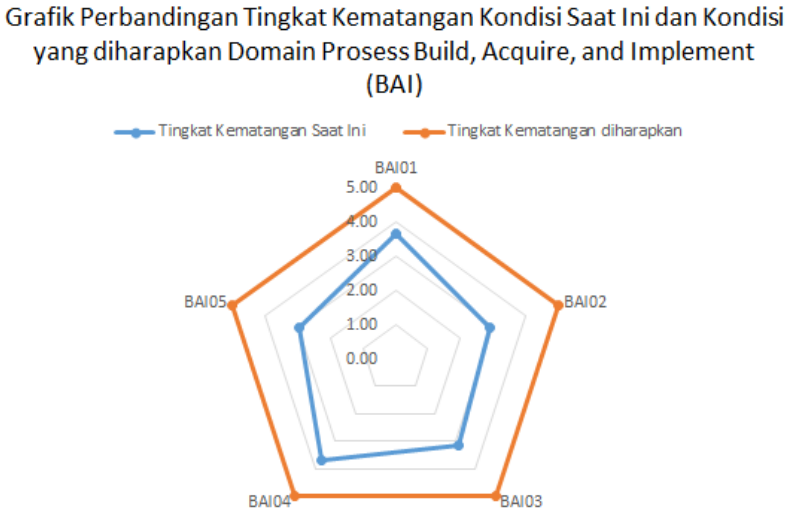


Gambar 5.4. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Align, Plan, and Organize* (APO)

Tabel 5.2. dan gambar 5.5. Menunjukkan GAP analisis antara tingkat kematangan kondisi saat ini dan tingkat kematangan yang diharapkan, dari hasil analisa GAP menunujukkan bahwa tingkat kematangan untuk domain Proses Build, Acquire, and Implement (BAI) masuk dalam ***level Established Process.***

Tabel 5.2. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Build, Acquire, and Implement* (BAI)

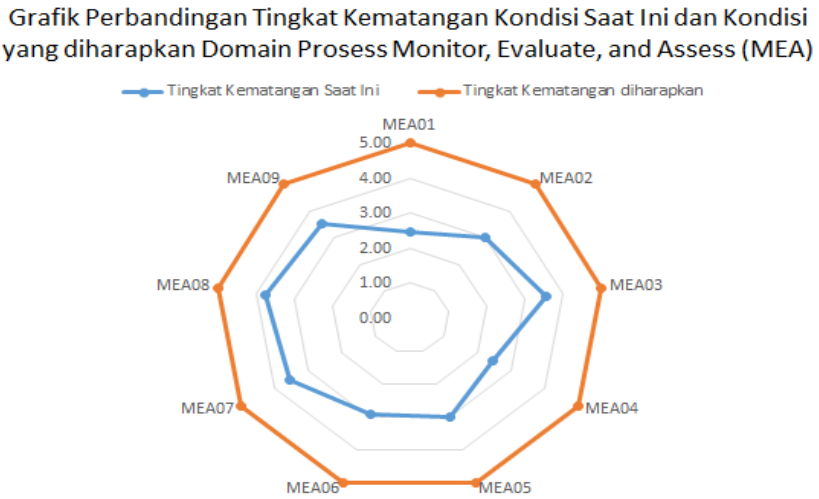
No.	Deskripsi Aktifitas	**Tingkat Kematangan Saat Ini**	**GAP**	Tingkat Kematangan diharapkan
1	Memiliki media penyimpanan backup data eksternal	3.65	1.35	5.00
2	Memiliki mekanisme restore akibat kerusakan data	2.92	2.08	5.00
3	Mengumpulkan, kinerja proses, dan kesesuaian data	3.15	1.85	5.00
4	Mengumpulkan, kinerja proses, dan kesesuaian data	3.66	1.34	5.00
5	Memastikan pelaksanaan tindakan perbaikan	2.95	2.05	5.00



Gambar 5.5. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Build, Acquire, and Implement* (BAI)

Tabel 5.3. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Monitor, Evaluate, and Assess* (MEA)

No.	Deskripsi Aktifitas	**Tingkat Kematangan Saat Ini**	**GAP**	Tingkat Kematangan diharapkan
1	Menggunakan audit trail dalam Server	2.45	2.55	5.00
2	Memiliki Mirror System dalam pengolaan Storage	3.01	1.99	5.00
3	Management dan Administrasi mudah	3.55	1.45	5.00
4	Menggunakan mekanisme security saat akses data	2.45	2.55	5.00
5	Memiliki Alur kerja secara otomatis (*Workflow*)	3.00	2.00	5.00
6	Bila bersifat transaksi, perlu adanya workflow	2.94	2.06	5.00
7	Memiliki Dokumentasi Aplikasi	3.55	1.45	5.00
8	Memiliki Dokumentasi hardware	3.75	1.25	5.00
9	Memiliki Dokumentasi Sistem	3.51	1.49	5.00

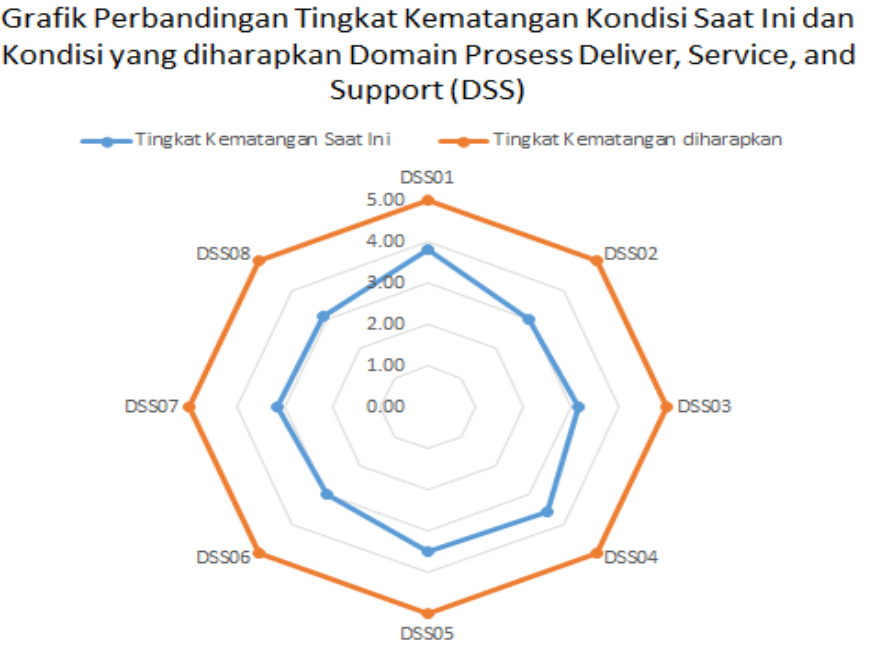


Gambar 5.6. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Monitor, Evaluate, and Assess* (MEA)

Tabel 5.3. dan gambar 5.6. Menunjukkan GAP analisis antara tingkat kematangan kondisi saat ini dan tingkat kematangan yang diharapkan, dari hasil analisa GAP menunujukkan bahwa tingkat kematangan untuk domain Proses Monitor, Evaluate, and Assess (MEA) masuk dalam ***level Established Process.***

Tabel 5.4. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Deliver, Service, and Support* (DSS)

No.	Deskripsi Aktifitas	**Tingkat Kematangan Saat Ini**	**GAP**	Tingkat Kematangan diharapkan
1	Aplikasi e-Layanan Berbasis web / Mobile	3.80	1.20	5.00
2	Dapat diakses oleh berbagai macam web browser	3.01	1.99	5.00
3	Dapat menggunakan attachment File	3.15	1.85	5.00
4	Dokumentasi jaringan dan pengelolaan	3.55	1.45	5.00
5	Jaringan komunikasi yang digunakan stabil	3.50	1.50	5.00
6	Jaringan yang digunakan lebih dari satu ISP	2.99	2.01	5.00
7	Memiliki Ruang Server khusus	3.15	1.85	5.00
8	Memiliki UPS dan Stabilizer	3.12	1.88	5.00

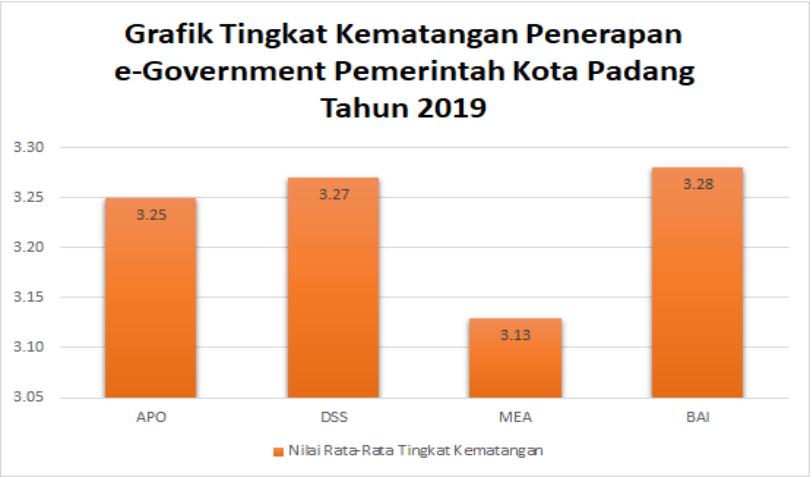


Gambar 5.7. Perbandingan Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan *Domain Proses Deliver, Service, and Support* (DSS)

Tabel 5.4. dan gambar 5.7. Menunjukkan GAP analisis antara tingkat kematangan kondisi saat ini dan tingkat kematangan yang diharapkan, dari hasil analisa GAP menunujukkan bahwa tingkat kematangan untuk domain Proses Deliver, Service, and Support (DSS) masuk dalam ***level Established Process.***

Tabel 5.5. Perbandingan Rata-rata Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses APO, DSS, MEA, dan BAI

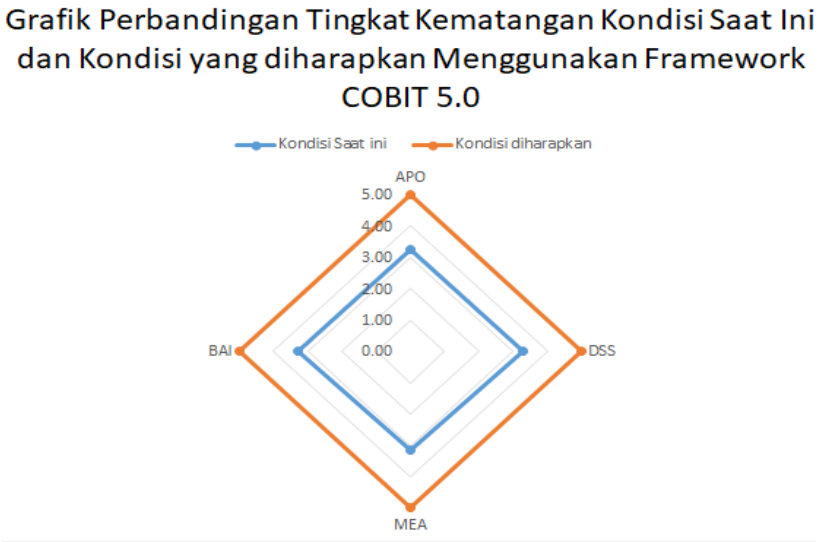
No.	Katogori	Nilai Rata-Rata Tingkat Kematangan
1	Align, Plan, and Organize (APO)	3.25
2	Build, Acquire, and Implement (BAI)	3.27
3	Monitor, Evaluate, and Assess (MEA)	3.13
4	Deliver, Service, and Support (DSS)	3.28
Rata-rata Tingkat Kematangan		3.23



Gambar 5.8. Perbandingan Rata-rata Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses APO, DSS, MEA, dan BAI

Tabel 5.6. Perbandingan Rata-rata Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses APO, DSS, MEA, dan BAI dengan Analisis GAP (kesenjangan)

Deskripsi Aktifitas	Nilai Rata-Rata Timgkat Kematangan		
	Saat ini	Diharapkan	GAP = Kondisi diharapkan - Kondisi Saat ini
APO	3.25	5.00	1.75 = 5 - 3.25
DSS	3.27	5.00	1.73 = 5 - 3.27
MEA	3.13	5.00	1.87 = 5 - 3.13
BAI	3.28	5.00	1.72 = 5 - 3.28



Gambar 5.9. Perbandingan Rata-rata Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses APO, DSS, MEA, dan BAI dengan Analisis GAP (kesenjangan)

5.4. Rekomendasi Perbaikan Selanjutnya

Tabel 5.7. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses APO dengan Analisis GAP (kesenjangan)

Deskripsi Aktifitas	Index Capability	Level / Target
APO01 : Mengoptimalkan penempatan fungsi TI	2.85	Level 3 Established Process / Level 5 Optimizing Process
APO02 : Mengelola perbaikan terus-menerus dari proses	3.7	Level 4 Predictable Process / Level 5 Optimizing Process
APO03 : Back-up dan Restore data terjadwal	3.65	Level 4 Predictable Process / Level 5 Optimizing Process
APO04 : Dapat menampung pertumbuhan data yang besar	3.25	Level 3 Established Process / Level 5 Optimizing Process
APO05 : Menjaga kepatuhan terhadap kebijakan dan prosedur	3.55	Level 4 Predictable Process / Level 5 Optimizing Process
APO06 : Mengelola Pemeliharaan terus-menerus dari proses	3.31	Level 3 Established Process / Level 5 Optimizing Process
APO07 : Menggunakan enkripsi dalam pengiriman data	3.09	Level 3 Established Process / Level 5 Optimizing Process
APO08 : Menggunakan User ID dan Password	3.05	Level 3 Established Process / Level 5 Optimizing Process

APO09 : Pengamanan sistem Menggunakan User ID dan Password	3.01	Level 3 Established Process / Level 5 Optimizing Process
APO10 : Terdapat leveling hak akses data dan application	3.03	Level 3 Established Process / Level 5 Optimizing Process

Tabel 5.8. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses BAI dengan Analisis GAP (kesenjangan)

Deskripsi Aktifitas	Index Capability	Level / Target
BAI01 : Memiliki media penyimpanan backup data eksternal	3.65	Level 4 Predictable Process / Level 5 Optimizing Process
BAI02 : Memiliki mekanisme restore akibat kerusakan data	2.92	Level 3 Established Process / Level 5 Optimizing Process
BAI03 : Mengelola, kinerja proses, dan kesesuaian data	3.15	Level 3 Established Process / Level 5 Optimizing Process
BAI04 : Menghimpun kinerja proses, dan kesesuaian data	3.66	Level 4 Predictable Process / Level 5 Optimizing Process
BAI05 : Memastikan pelaksanaan tindakan perbaikan	2.95	Level 3 Established Process / Level 5 Optimizing Process

Tabel 5.9. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses MEA dengan Analisis GAP (kesenjangan)

Deskripsi Aktifitas	Index Capability	Level / Target
MEA01 : Menggunakan audit trail dalam Server	2.45	Level 2 Managed Process / Level 5 Optimizing Process
MEA02 : Memiliki Mirror System dalam pengolaan Storage	3.01	Level 3 Established Process / Level 5 Optimizing Process
MEA03 : Management dan Administrasi mudah	3.55	Level 4 Predictable Process / Level 5 Optimizing Process
MEA04 : Menggunakan mekanisme security saat akses data	2.45	Level 2 Managed Process / Level 5 Optimizing Process
MEA05 : Memiliki Alur kerja secara otomatis (Workflow)	3	Level 3 Established Process / Level 5 Optimizing Process
MEA06 : Bila bersifat transaksi, perlu adanya workflow	2.94	Level 3 Established Process / Level 5 Optimizing Process
MEA07 : Memiliki Dokumentasi Aplikasi	3.55	Level 4 Predictable Process / Level 5 Optimizing Process
MEA08 : Memiliki Dokumentasi hardware	3.75	Level 4 Predictable Process / Level 5 Optimizing Process
MEA09 : Memiliki Dokumentasi Sistem	3.51	Level 4 Predictable Process / Level 5 Optimizing Process

Tabel 5.10. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses DSS dengan Analisis GAP (kesenjangan)

Deskripsi Aktifitas	Index Capability	Level / Target
DSS01 : Aplikasi e-Layanan Berbasis web/ Mobile	3.8	Level 4 Predictable Process / Level 5 Optimizing Process
DSS02 : Dapat diakses oleh berbagai macam web browser	3.01	Level 3 Established Process / Level 5 Optimizing Process
DSS03 : Dapat menggunakan attachment File	3.15	Level 3 Established Process / Level 5 Optimizing Process
DSS04 : Dokumentasi jaringan dan pengelolaan	3.55	Level 4 Predictable Process / Level 5 Optimizing Process
DSS05 : Jaringan komunikasi yang digunakan stabil	3.5	Level 3 Established Process / Level 5 Optimizing Process
DSS06 : Jaringan yang digunakan lebih dari satu ISP	2.99	Level 3 Established Process / Level 5 Optimizing Process
DSS07 : Memiliki Ruang Server khusus	3.15	Level 3 Established Process / Level 5 Optimizing Process
DSS08 : Memiliki UPS dan Stabilizer	3.12	Level 3 Established Process / Level 5 Optimizing Process

Tabel 5.11. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses APO

Deskripsi Aktifitas	Rekomendasi Perbaikan Selanjutnya
APO01	1. Melaksanakan TOT terhadap SDM bidang TI 2. menambah SDM dengan Kompetensi yang dibutuhkan.
APO02	1. Perlu melakukan upgrade Aplikasi Tools untuk Monitoring baik aplikasi, database dan Jaringan internet 2. Pengecekan versi / release software system yang digunakan.
APO03	1. Menambah Storage untuk mengantipasi pertunbuhan data yang besar. 2. Menambah kapasitas dan jumlah Coud storage.
APO04	1. Menambah Storage untuk mengantipasi pertunbuhan data yang besar. 2. Menambah kapasitas dan jumlah Coud storage.
APO05	1. Melaksanakan sosialisasi terkait SOP dan aturan serta kebijakan baik ke pengguna atau pengelola e-*government*.
APO06	1. Perlu melakukan upgrade Aplikasi Tools untuk Monitoring baik aplikasi, database dan Jaringan internet 2. Pengecekan versi / release software system yang digunakan.
APO07	1. Menerapkan Peraturan Daerah Provinsi Sumatera Barat No. 10 Tahun 2019, tentang Penyelenggaraan Persandian untuk pengamanan Informasi 2. Menggunakan metode Enkripsi yang telah teruji dan menurut penelitian dari perguruan tinggi.

APO08	1. Menerapkan Peraturan Daerah Provinsi Sumatera Barat No. 10 Tahun 2019, tentang Penyelenggaraan Persandian untuk pengamanan Informasi 2. Menggunakan metode Enkripsi yang telah teruji dan menurut penelitian dari perguruan tinggi. 3. Mengganti password secara berkala dan memberikan kombinasi antara karakter dan numerik serta special karakter.
APO09	1. Menerapkan Peraturan Daerah Provinsi Sumatera Barat No. 10 Tahun 2019, tentang Penyelenggaraan Persandian untuk pengamanan Informasi 2. Menggunakan metode Enkripsi yang telah teruji dan menurut penelitian dari perguruan tinggi. 3. Mengganti password secara berkala dan memberikan kombinasi antara karakter dan numerik serta special karakter.
APO10	1. Meningkatkan keamanan terkait hak akses baik ke database maupun ke aplikasi 2. Merekam Log File pada server untuk mendapatkan informasi pengguna illegal pada database maupun aplikasi.

Tabel 5.12. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses BAI

Deskripsi Aktifitas	Rekomendasi Perbaikan Selanjutnya
BAI01	1. Menambah Storage untuk mengantipasi pertunbuhan data yang besar. 2. Menambah kapasitas dan jumlah Coud storage. 3. Mengevaluasi storage yang digunakan agar proses transfer data dari/ke CPU kecepatannya stabil, bisa menggunakan Storage Area Network (SAN) atau RAPID (*Redundant Array of Independent Disks*) terbaru
BAI02	1. Membuat jadwal secara berkala untuk mengantisipasi terjadinya kerusakan akibat restore yang gagal 2. Menyusun rencana mekanisme restore yang baik untuk mengantisipasi terjadinya kerusakan akibat restore yang gagal
BAI03	1. Membuat roadmap pengelolaan kinerja proses dan pemutakhiran data secara otomatis dalam system aplikasi 2. Menyusin timeline secara otomatis dari Sistem Operasi yang digunakan. 3. Sebaiknya menggunakan Sistem Operasi yang mempunya lisensi resmi bukan opersource.
BAI04	1. Perlu membuat jadwal secara berkala dalam menghimpun kinerja proses dan pemutakhiran data secara otomatis dalam system aplikasi
BAI05	1. Perlu melakukan monitoring dan evaluasi terhadap setiap perbaikan dengan menggunakan instrument yang jelas. 2. Perlu mengukur tingkat prioritas terhadap setiap perbaikan yang urgensi untuk dilaksanakan, jika tidak dilaksanakan segera akan menimbulkan kerugian yang sangat besar.

Tabel 5.13. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses MEA

Deskripsi Aktifitas	Rekomendasi Perbaikan Selanjutnya
MEA01	1. Perlu membuat system auditing embedded di Server Database, Web Server, Application Server, Mail Server dan Domain Server.
MEA02	1. Perlu menggunakan Model Penyimpanan SSD dengan model RAID (*Redundant Array of Independent Disks)* untuk mengatipasi jika ada kerurakan storage.
MEA03	1. Perlu menggunakan system customation dalam mengendalikan Administrator baik Database dan Aplikasi.
MEA04	1. Perlu meningkatkan keamanan dan menggunakan software tools security yang lisensi.
MEA05	1. Perlu adanya otomasisasi Workflow yang menyatu dengan aplikasi
MEA06	1. Perlu adanya workflow untuk memudahkan pemeliharaan dan monitoring system, jika terjadi kendala-kendala pada saat terjadi tranksaksi baik offline maupun online.
MEA07	1. Perlu dilakukan revisi / release setiap ada perubahan dan pengembangan aplikasi dan modifikasi database.
MEA08	1. Perlu dilakukan revisi / release setiap terjadi upgrade dan penambahan hardware.
MEA09	1. Perlu dilakukan revisi / release setiap ada perubahan dan pengembangan sistem. 2. Perlu crosscheck roadmap TI dan roadmap e-*government* agar sesuai dengan dokumentasi system.

Tabel 5.14. Rekomendasi Perbaikan Selanjutnya Tingkat Kematangan antara Kondisi Saat ini dengan Kondisi yang diharapkan untuk Semua Domain Proses DSS

Deskripsi Aktifitas	Rekomendasi Perbaikan Selanjutnya
DSS01	1. Perlu menyediakan fasilitas customize dalam disain graphical user interface (GUI).
DSS02	1. Aplikasi yang akan dikembangkan dapat menggunakan berbagai media baik berbasis web maupun berbasis mobile.
DSS03	1. Membatasi format file yang diupload serta ukurannya agar tidak mengganggu stabilitas storage internal dan eksternal. 2. Melakukan Filterisasi terhadap File yang diupload agar tidak masuk file yang menyimpan Virus atau sejenisnya.
DSS04	1. Mengaktifkan Log File pada Server Database dan Aplikasi secara otomatis pada system Operasi, untuk mencatat aktifitas secara online dan real time.
DSS05	1. Menggunakan ISP Leased Line yang menggunakan unlimited bandwidth
DSS06	2. Memastikan ISP yang dilanggan menjamin kestabilan jaringan, tidak terganggu. 3. Melakukan MoU & MoA untuk mendapatkan jaminan jaringan yang digunakan lancer dan kalua ada gangguan secepatnya diantisipasi dengan cepat.
DSS07	1. Melakukan pengecekan terhadap suhu di runagan Server setiap saat. 2. Menggunakan alat otomatis untuk menentukan tingkat suhu agar stabil.

	3. Menggunakan lebih dari satu AC, sehingga bisa secara otomatis bergantian aktifnya dengan sensor.
DSS08	1. Melakukan pengecekan setiap saat terhadap pemakaian daya listrik. 2. Mengontrol aktifitas UPS apakah masih dapat menyimpan dengan baik untuk beberapa Jam. 3. Mengadakan battery kering UPS agar dapat bertahan lama selama PLN mati lampu.

BAB 6

STUDI KASUS AUDIT TEKNOLOGI INFORMASI

6.1. Audit Teknologi Informasi Pemerintahan Kota

Sebuah Pemerintahan Kota menunjuk tim audit TI UPI YPTK Padang untuk melakukan review atas penerapan sistem e-*government* di Pemerintahan Kota yang terintegrasi. Pemeriksaan ini terbagi dalam dua fase. Pada fase pertama mencakup kegiatan, sebagai berikut:

1. *Manajemen Proyek Apikasi yang telah dikembangkan*

   Melakukan review atas manajemen proyek aplikasi yang telah dikembangkan untuk memastikan bahwa semua outcome yang diharapkan tertuang dalam rencana roadmap TIK dan e-*government*. Pada tahapan ini, auditor TI melakukan review atas project aplikasi yang dikembangkan charter, sumber daya (*resource*)

yang digunakan, alokasi penugasan dan analisa tahapan pekerjaan proyek pengembangan aplikasi.

2. *Desain Proses dan Pengendalian Kontrol Aplikasi*

   Review mengenai desain pengendalian dalam modul-modul e-*government* tersebut, yaitu perencanaan sampai dengan Monitoring kegiatan. Untuk itu dilakukan review atas desain proses dimana auditor mengevaluasi proses, risiko dan pengendalian mulai dari tahapan input, proses maupun output.

6.2. *Check List* Audit Teknologi Informasi

Tabel 6.1. *Check List* Audit Teknologi Informasi

CHECK LIST AUDIT TEKNOLOGI INFORMASI				
NO	ITEM	Y	T	Keterangan
REVIEW PENGENDALIAN UMUM				
A. ORGANISASI				
I. Struktur Organisasi				
1	Terdapat Struktur Organisasi formal atas fungsi SISFO yang didukung oleh Top Manajemen			
2	Kedudukan SISFO cukup tinggi dalam struktur organisasi untuk dapat bersikap independent terhadap bagian lain.			
3	Terdapat pemisahan yang jelas antara fungsi pengolah data pada SISFO dengan pemakai data (user)			
II. Pemisahan Fungsi				
1	Terdapat uraian tugas dan tanggung jawab yang jelas dan tertulis mengenai fungsi-fungsi yang ada di Unit SISFO.			

2	Terdapat pemisahan fungsi antara programmer dan operator			
3	Terdapat pemisahan fungsi antara system manajer dan programmer			
4	Terdapat pemisahan fungsi antara system manajer dengan operator			
5	Fungsi Database Administrator yang terpisah dari Data/Program Librarian maupun dari Programer			
III. Kepegawaian				
1	Terdapat ketetapan tertulis tentang persyaratan keterampilan bagi setiap posisi yang ada di Unit Pengolah Data			
2	Latar belakang pendidikan/pengalaman setiap pegawai telah mendukung pekerjaannya			
3	Terdapat program pelatihan untuk meningkatkan kemampuan personel Unit Pengolah Data			
4	Terdapat evaluasi periodik berdasarkan criteria yang ada terhadap kinerja para personil			
B. PENGENDALIAN OPERASI				
I. Operasi Komputer				
1	Terdapat seluruh operasi computer telah dilakukan penjadualan sehingga dapat diselesaikan secara tepat waktu dan efisien			
2	Terdapat Staff yang bertanggungjawab untuk mengelola seluruh media computer (magnetic tape, disket, dll)			
3	Terdapat prosedur pengelolaan media computer dalam rangka melindungi data dari penyalahgunaan atau kerusakan			

4	Terdapat prosedur dan standard penggunaan identification terhadap seluruh media magnetis yang diperlukan			
II. Physical access, Logical access dan physical security				
1	Terdapat personil yang bertanggungjawab mengenai masalah physical access dan logical access			
2	Lokasi ruang server telah terpisah dari bagian lain			
3	Keberadaan ruang server tidak mencolok			
4	Terdapat pemisahan antara ruang programmer dengan ruang operasi			
5	Ruang server selalu terkunci setiap saat			
6	Terdapat pembatasan akses terhadap ruang server			
7	Terhadap instalasi computer yang kritis, terdapat metode pengawasan yang lebih ketat mengenai physical access			
8	Terminal-terminal yang berada di luar lokasi Unit Pengolah Data telah ditempatkan di lokasi yang aman			
9	Terhadap individu yang bukan Staff Unit Pengolah Data selalu didampingi bilamana mereka masuk ke ruang computer/storage /library.			
10	Kepada setiap pegawai yang berkepentingan memasuki system/aplikasi computer telah diberikan sebuah user-id yang unik			
11	Untuk setiap user login perlu dialokasikan akses provelage yang sesuai dengan tugas dan tanggung jawabnya			
12	Pada seluruh prosedur login, setiap pegawai diharuskan memberikan user-id dan password			

13	Terdapat pembatasan kesalahan dalam prosedur login sebelum terjadi penolakan			
14	Terdapat fasilitas automatic log-off bila pada jangka waktu tertentu tidak terdapat aktivitas pada terminal			
15	Adanya fungsi yang mengelola pemberian user-id dan password, serta akses provelage yang tidak dirangkap oleh programmer atau operator			
16	Password table tidak terdapat dalam bentuk hard-copy dan hanya dalam bentuk file computer yang telah di-enkripsi			
17	Peraturan pemakaian password dapat menjamin bahwa tidak terdapat kemungkinan suatu password diketahui oleh pihak lain			
18	Terdapat keharusan untuk mengubah password apabila telah melewati batas umur tertentu			
19	Terdapat system-log yang secara otomatis dapat mencatat seluruh kegiatan komputer			
20	Adanya prosedur yang secara periodic mengharuskan dilakukan evaluasi dalam rangka mengidentifikasi dan mengatasi adanya aktivitas yang tidak diotorisasi			
III. Enviromental Control				
1	Ruang computer telah dilengkapi dengan alat pendeteksi dan pencegah kebakaran			
2	Terhadap alat pemadam kebakaran yang terdapat di ruang server/back up data telah dilakukan pemeliharaan secara berkala			
3	Terdapat prosedur tertulis mengenai tata cara penanganan kebakaran untuk lingkungan system informasi			
4	Terdapat pelatihan dalam menghadapi bahaya kebakaran			

5	Ruang computer telah dilengkapi dengan alat pendingin serta alat pengatur kelembaban			
6	Tersedia fasilitas UPS (Uninteruptable Power Suplay) untuk computer utama yang dipakai perusahaan.			
IV. Pemulihan Masalah				
1	Terdapat prosedur back up yang memadai terhadap aplikasi dan data vital yang dimiliki			
2	Terdapat cadangan perangkat keras yang memadai untuk menjalankan aplikasi yang kritis apabila perangkat yang ada tidak dapat dipergunakan secara tiba-tiba.			
3	Tersedia off site storage untuk menyimpan back up data, aplikasi maupun dokumen penting			
4	Terdapat proteksi terhadap adanya gangguan listrik dengan menyediakan battery back up dan pemakaian UPS			
5	Terdapat proteksi terhadap kemungkinan system terinfeksi virus			
V. Pengembangan Sistem				
1	Terdapat prosedur tertulis dan baku yang dipakai untuk melakukan pengembangan dan pemeliharaan sistem			
2	Terdapat keterlibatan user dalam pengembangan sistem			
3	Setiap pengembangan dan pemeliharaan system berdasarkan permintaan dari user atau komite pengembangan			
4	Untuk setiap perubahan program telah terdapat otorisasi tertulis dari pejabat yang berwenang			
5	Internal auditor telah dilibatkan dalam setiap pengembangan sistem			

6	Pengembangan system telah berdasarkan metodologi yang efisien dan efektif			
7	Proses desain unuk memodifikasi program tidak dilakukan terhadap system produksi yang sedang berjalan tetapi dilakukan terhadap salinannya			
8	Seluruh kegiatan pengembangan system didokumentasikan dengan baik dan lengkap			
9	Untuk menghindari tuntutan hukum, perlu dilakukan pengendalian yang memadai guna mencegah kemungkinan pemakaian program bajakan			
VI. Dokumentasi Sistem				
1	Terdapat dokumentasi yang cukup untuk setiap aplikasi yang ada			
2	Terdapat standarisasi dalam perubahan : flow chart, decision table, daftar kata, dan singkatan serta dokumentasi			
3	Terdapat pemisahan antara dokumentasi system, dokumentasi program, serta dokumentasi operasi serta keterbatasan akses atas dokumentasi tersebut.			
4	Terdapat dokumentasi berupa alasan pengembangan system yang mencakup latas belakang, tujuan, dan ruang lingkup system, spesifikasi system yang menjelaskan operasi system serta Bukti Pengesahan atas pengembangan system			
5	Terdapat dokumentasi system yang meliputi bagan arus keterkaitan input, proses dan output serta penjelasan atas input, otput, proses yang diterapkan dalam sistem			
6	Terdapat dokumentasi program yang meliputi penjelasan atas fungsi setiap sub program, program listing dari source code, daftar			

	pengendalian aplikasi, dan catatan atas seluruh perubahan kode program			
7	Terdapat dokumentasi operasi yang meliputi penjelasan atas formulir-formulir input, output dan distribusi output, daftar instruksi pengoperasian program computer dan penjelasan rinci mengenai penanganan kerusakan dan gangguan			
8	Terdapat dokumentasi pemakai			
VII. Pengendalian Perangkat Keras dan *Operating System*				
1	Terdapat jaminan vendor atas hardware atau software yang baru dibeli			
2	Terdapat jaminan asuransi			
REVIEW PENGENDALIAN APLIKASI				
A. INPUT				
Kelengkapan, keakurasian, dan keabsahan data				
1	Terdapat prosedur penyiapan data yang harus ditaati oleh user, termasuk perubahan permanent maupun koreksi data untuk menjamin seluruh transaksi telah terekam			
2	Terdapat prosedur untuk menjamin bahwa seluruh transaksi yang masuk dan terekam dalam computer hanya transaksi yang telah terotorisasi secara sah			
3	Terdapat prosesur untuk menjamin bahwa seluruh transaksi yang telah terotorisasi telah direkam secara akurat ke dalam media komputer			
4	Terdapat pengendalian masukan (input) yang dapat meyakinkan bahwa data yang diterima oleh unit pengolah data tidak rusak/ditambahkan/diduplikasi/dimodifikasi			
5	Terdapat error listing			
6	Pengujian field checks			
7	Pengujian Financial Total			

8	Pengujian Limit Check			
9	Pengujian Range Check			
10	Pengujian Preformatting			
11	Pengujian Reasonableness Test			
12	Pengujian Record Count			
13	Pengujian Self Checking Digit			
14	Pengujian Sequence Check			
15	Pengujian Sign Check			
16	Pengujian Validity Check			
17	Pengujian Key verification			
18	Pengujian Redundancy Check			
19	Pengujian Echo Check			
20	Pengujian Completeness Check			
21	Pengujian Internal Header dan Trailer Label			
B. PROSES				
1	Terdapat prosedur yang dapat menjamin bahwa seluruh transaksi yang telah terotorisasi telah diproses			
2	Terdapat prosedur yang dapat menjamin bahwa seluruh transaksi yang telah terotorisasi telah diproses secara akurat			
3	Pengujian Limit, Reasonableness dan Sign Test			
4	Pengujian Positing, Crossfooting, dan Zero Balance Check			
5	Pengujian Run to Run Total			
6	Pengujian End of File Procedure			
7	Pengujian Audit Trail			
C. OUTPUT				
1	Terdapat prosedur yang menjamin bahwa output dari system informasi selalu direvie oleh user manajemen untuk menentukan kelengkapan, akurasi, dan konsistensinya			

2	Terdapat suatu metode dalam meyakinkan bahwa prosedur pengendalian yang mencakup kelengkapan, akurasi, dan keabsahan selalu dapat dijalankan.			
3	Terdapat kebijakan dan prosedur yang mengatur lamanya suatu data/dokumen dimusnahkan			
4	Terdapat error listing			
5	Terdapat Console Log atas terjadinya interupsi dan intervensi system yang tidak biasa			
6	Terdapat pengendalian distribusi laporan dan retensi atas laporan yang sudah tidak dibutuhkan lagi			
7	Terdapat User Review atas laporan-laporan yang dihasilkan			

6.3. Rencana Audit Teknologi Informasi

1. Tujuan Audit Teknologi Informasi:

a. Menilai Efektifitas Aplikasi Perencanaan sampai dengan Monitoring kegiatan di Pemerintahan Kota.
b. Menilai Efisiensi Sumber Daya dalam penggunaan Aplikasi Perencanaan sampai dengan Monitoring kegiatan di Pemerintahan Kota.

2. Ruang Lingkup Audit Teknologi Informasi:

a. Objek Audit:
   1) Pemerintahan Daerah Kota
   2) Ruang Kepala Daerah
   3) Ruang Ka. Dinas
   4) Ruang Ka. Bagian
   5) Ruang OPD/SKPD

b. Yang di Audit:
   1) Kepala Daerah
   2) Kepala Dinas
   3) Kepala Bagian
   4) Pengelola E-*government*
   5) Pengguna E-*government*
   6) OPD/SKPD
c. Periode Tahunan

3. Metode:

Audit Teknologi Informasi ini dilaksanakan dengan metode sebagai berikut:

a. Survei (dengan bantuan Kuisioner)
b. Interview
c. Observasi
d. Review dokumentasi

4. Susunan Anggota Tim (eksternal)

Tabel 6.2. Susunan Anggota Tim (eksternal)

No.	Nama	NIDN	Peran Dalam Tim	Jabatan
1.	Nama 1	XXXXX	Penanggung Jawab	-
2.	Nama 2	XXXXX	Pengawas	-
3.	Nama 3	XXXXX	Ketua Tim	-
4.	Nama 4	XXXXX	Reviewer	-
5.	Nama 5	XXXXX	Auditor 1	-
6.	Nama 6	XXXXX	Auditor 2	-
7.	Nama 7	XXXXX	Auditor 3	-

5. Jadwal Pelaksanaan:

Tabel 6.3. Jadwal Pelaksanaan

No	Kegiatan	Perencanaan
	Persiapan:	
1	Melakukan Koordinasi dengan pihak terkait untuk membahas rencana audit yang akan dilakukan	05 November 2020
2	Menyiapkan dokumentasi yang berkaitan dengan audit (Lembar kerja, survey, wawancara, dll)	06 – 07 November 2020
	Pendahuluan:	
3	Melakukan Sosialisasi dengan Pihak Terkait untuk kegiatan Audit yang akan dilakukan	08 November 2020
4	Mengumpulkan dokumentasi berkaitan dengan audit yang akan dilakukan seperti a Rencana Strategis (Renstra) b Rencana Kerja (Renja) c Struktur Organisasi dan Tata Kerja (SOTK) d Standar Operasional Prosedur (SOP) e Pengadaan Aplikasi f Manual Pengguna Aplikasi g dll	08 November 2020
5	Melakukan review terhadap dokumentasi yang berkaitan	09-10 November 2020
	Pelaksanaan:	

No	Kegiatan	Perencanaan
6	Melakukan Wawancara (interview) dengan Kepala Daerah, Kepala Dinas, Kepala Bagian, pengelola E-*government*, Pengguna E-*government*, OPD/SKPD	12 November 2020
7	Melakukan observasi langsung ke Dinas/OPD/SKPD untuk melihat proses Perencanaan sampai Monitoring	12 November 2020
8	Mengunpulkan data melalui survey yang dibuat untuk diisi oleh Kepala Daerah, Kepala Dinas, Kepala Bagian, pengelola E-*government*, Pengguna E-*government*, OPD/SKPD	13 – 14 November 2020
9	Melakukan penilaian tingkat kedewasaan (maturity level) untuk layanan aplikasi yang digunakan	13 – 14 November 2020
10	Melakukan Klarifikasi hasil Audit	14 November 2020
	Pelaporan:	
11	Mebuat Laporan yang berisi: a Perencanaan dan persiapan Audit SI/TI yg mencakup ruang lingkup dan tujuan audit (*scope* dan *objective*), b Kondisi sistem informasi/Aplikasi c Program Audit SI/TI yg dilakukan d Langkah Audit SI/TI yg dilakukan dan bukti (*evidence*) Audit SI/TI yg dikumpulkan,	15-16 November 2020

No	Kegiatan	Perencanaan
	e Temuan audit (*findings*) dan tingkat maturity Proses TI f Kesimpulan dari hasil temuan, g Laporan-laporan lain terkait sebagai hasil dr pekerjaan Audit SI/TI, h Rekomendasi untuk perbaikan berkelanjutan.	

6. Biaya:

Biaya yang ditimbulkan terkait dengan kegiatan Audit Teknologi Informasi ini, menggunakan beban biaya dari Universitas Putra Indonesia YPTK Padang.

7. Lain-lain:

Apabila diperlukan, pengawas dan atau penanggungjawab tim dapat menambah/ mengurangi anggota tim dan narasumber.

6.4. Program Pengujian Audit Teknologi Informasi Efektifitas Aplikasi Perencanaan sampai dengan Monitoring

Tabel 6.4. Program Pengujian Audit Teknologi Informasi

No.	Komponen (*Objective*)	Risiko (*Risk*)	Langkah-langkah Pengujian	Pelaksana Pengujian
1				

6.5. *Check List* Audit Teknologi Informasi

Tabel 6.5. Check List Audit Teknologi Informasi

CHECK LIST AUDIT TEKNOLOGI INFORMASI				
NO	**ITEM**	**Y**	**T**	**Keterangan**
1	Terdapat Struktur Organisasi formal di Pemerintah Kota.			
2	Terdapat SOP / Tupoksi Pemerintahan Daerah Kota			
3	Terdapat dokumen manual penggunaan aplikasi.			
4	Terdapat gap antara dokumen SOP dengan aplikasi berdasarkan hasil observasi atau berdasarkan dokumen manual penggunaan aplikasi.			
5	Terdapat uraian tugas dan tanggung jawab yang jelas dan tertulis mengenai fungsi-fungsi yang ada di Pemerintahan Daerah Kota.			
6	Terdapat bukti Registrasi untuk transaksi kegiatan mulai dari Perencanaan s.d Monitoring			

7	Terdapat Bukti validasi dan verifikasi terkait dengan transaksi kegiatan yang dilakukan oleh OPD/SKPD.			
8	Terdapat bukti maintenence aplikasi secara berkala			
9	Terdapat prosedur tetap jika aplikasi mengalami gangguan			
10	Kepada setiap pegawai yang berkepentingan memasuki system/aplikasi telah diberikan sebuah user-id yang unik			

DAFTAR PUSTAKA

Agoes, Sukrisno. 2014. *Auditing*. Jakarta: Salemba Empat.

Arens, A. Alvin., Elder, J. Randal., and Beasley, S. Mark. 2006. *Auditing and Assurance Service, 12th*. Prentice Hall, Pearson Education.

Boynton, C. William., Johnson, N. Raymond., and Kell, G. Walter, 2001. Modern Auditing., 7th, John Wiley & Sons, Inc.

CISA, Reza Aminy, M.TI. 2017. *Audit Sistem Infomasi: Lima Aspek Audit Sistem Informasi*. Yogyakarta: CV Mega Indo Komunika.

FASB. 1989. *Codification of Statements on Auditing Standard*. New York: AICPA.

Henry Hendarti. 2007. *Audit Sistem Informasi Lanjutan/Sanyoto Gondodiyoto, Edisi Pertama*. Jakarta: Mitra Wacana Media.

Ikatan Akuntan Indonesia. 2011. *Standar Profesional Akuntan Publik*. Salemba Empat. Jakarta: Pustaka Pendukung.

Mulyadi, 2002. Auditing, Edisi ke-6. Jakarta: Penerbit Salemba Empat.

Mulyadi. 2013. *Auditing Buku 1 edisi 6*. Jakarta: Salemba Empat.

Aichholzer, Georg. 2004. "*Scenarios of E-government in 2010 and Implications for Strategy Design*." *Electronic Jounal of E-government* 2 (1): 1–10.

Azkiya, H. (2017). *Penerapan e-government dalam peningkatan pelayanan publik*. *0714111330*.

Cockburn, *A. Using Both Incremental and Iterative Development*. CrossTalk: The Journal of Defense Software Engineering. 2008; 21(5): 27–30.

Djaelani, A. R. 2013. *Teknik Pengumpulan Data Dalam Penelitian Kualitatif.* Semarang- FPTK IKIP Semarang.

Gregory Curtin. 2007. *A Comparative Analysis of E-government in Latin America*: Applied Findings from United Nations E-*government* Readiness Reports, IGI Global Disseminator of Knowledge USA.

Hardjaloka, L. (2014). *Studi Penerapan E-government Di* Indonesia *Dan Negara Lainnya Sebagai Solusi Pemberantasan Korupsi Di Sektor Publik*. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *3*(3), 435–452. Retrieved from http://rechtsvinding.bphn.go.id/ejournal/index

Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003 tentang *Kebijakan dan Strategi Nasional Pengembangan e-government.*

Instruksi Presiden Republik Indonesia Nomor 6 tahun 2001 tentang *Telekomunikasi, Media dan Informatika (Telematika).*

Indrajit, R.E. 2006. *Evolusi Strategi Integrasi Sistem Informasi Ragam Institusi*. Jakarta.

Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003 tentang *Kebijakan & Strategi Nasional Pengembangan E-Gov*, Panduan Penyusunan Rencana Induk Pengembangan E-Gov Lembaga, 2003, Jakarta.

Instruksi Presiden Republik Indonesia Nomor 6 Tahun 2001 tentang *Telematika (Telekomunikasi, Media & Informatika)*, 2001, Jakarta.

Istiyanto, J.E., Sutanta, E. 2012. Model Interoperabilitas Antar Aplikasi e-government. *Jurnal Technoscientia, Volume V, Nomor 1, Edisi Februari* 2012, IST AKPRIND, Yogyakarta.

Layne, K., & Lee, J. (2001). *Developing Fully Functional e-government: A Four Stage Model. Government Information Quarterly*, 18 (2), 122-136.

Miftahuddin. (2018). *Terhadap Pengelolaan Dana Desa (Studi Kasus : Desa Panggungharjo Kecamatan Sewon Kabupaten Bantul*) Tesis Oleh : Nama : Miftahuddin Fakultas Ekonomi Universitas Islam Indonesia Yogyakarta.

Makoza, Frank. (2013). *The level of e-government Implementation: Case of Malawi. Electronic Journal of e-government*, Volume 11, Issue 2, (pp268-279)

Nugroho, L.N. 2008. *Persepsi-Persepsi tentang E-government*, diakses dari http://mti.ugm.ac.id/~lukito/3-project/substansi-content-buku/persepsi-persepsitentang-e-*government*/, 01-01-2012.

Pascual, P.J. 2003. *e-government, e-Asean Task Force UNDP-APDIP*. May 2003.

Peraturan Presiden (Perpres) Nomor 95 Tahun 2018 tentang *Sistem Pemerintahan Berbasis Elektronik (SPBE)*

Raharjo, B. 2001. *Membangun e-government*. ITB: Bandung.

Schwab, Klaus. 2016. *The Fourth Industrial Revolution 4.0*. Geneva, Switzerland: World economic Forum. World Economic Forum 91–93 route de la Capite CH-1223 Cologny/Geneva Switzerland www.weforum.org.

Sutanta, E., & Mustofa, K.s. 2012. *Identifying The Needs of Web Service to Data Synchronization Between Information Systems as E-government Ecosystem at Bantul*-Yogyakarta. Bandung: Teknik Informatika STMIK Bandung.

Sudibyo, D. 2011. *Menyimak e-KTP*, diakses dari http://deru.blogspot.com/2011/10 /menyimak-e-ktp.html#!/2011/10/ menyimak-e-ktp.html, 14-11-2011.

Sukyadi, D. 2009. *Model Interoperabilitas Sistem Informasi Layanan Publik Studi Kasus: e-government*. Karya Akhir, Prodi Magister Teknologi Informasi, Fasilkom, UI, Jakarta.

Supangkat, S.H. 2006. *Framework Strategi Implementasi E-government*. Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia, ITB, Bandung, 3-4 Mei 2006.

Supangkat, S.H., Sembiring, J., Rahmad, B., 2007*, IT Governance Nasional: Urgensi dan Kerangka Konstruksi,* Makalah dipresentasikan dalam Pertemuan Dewan TIK Nasional, Jakarta. 8 Januari 2007.

Sutanta, E., Ashari, A. 2012. *Pemanfaatan Database Kependudukan Terdistribusi pada Ragam Aplikasi Sistem Informasi di Pemerintah Kabupaten/Kota*, Jurnal Sistem Informasi & Teknologi Informasi (SISFOTENIKA), Volume 2, Nomor 1, Edisi Januari 2012, STMIK Pontianak, Kalimantan Barat.

UU Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Informasi dan Transaksi Elektronik atau Undang Undang nomor 11 tahun 2008 atau UU ITE adalah *UU yang mengatur tentang informasi serta transaksi elektronik,* atau teknologi informasi secara umum.

Williams, James G, and Toni Carbo. 2004. "*Models and Metrics for Evaluating Local Electronic Government Systems and Services*." *Electronic Journal of E-government* 2 (2). EJEG is published by Academic Conferences and Publishing

International Limited%0A33 Wood Lane, Sonning Common, Nr Reading, RG4 9SJ, UK.

Richardus Eko Indrajit. (2005). *E-government In Action*. Yogyakarta: Andi.

ISACA. 2012. COBIT 5 : *A Business Framework for the Governance and Management of Enterprise IT*. USA: ISACA.

ISACA. 2012. COBIT 5 : *Enabling Processes*. USA: ISACA.

ISACA. (2013). *COBIT Process Assessment Model (PAM): Using COBIT 5*. USA: ISACA.

Amalia, E., & Adietya, A. 2019. *Analisis dan Evaluasi Tingkat Kematangan E-government pada Information Architecture dengan Menggunakan United Nations Model*. JUMANJI (Jurnal Masyarakat Informatika Unjani), 3(01), 35-52.

Bouty, A. A., Koniyo, M. H., & Novian, D. (2019). *Evaluasi Sistem Pemerintahan Berbasis Elektronik Menggunakan E-government Maturity Model (Kasus Di Pemerintah Kota Gorontalo) The Evaluation Of Electronic Based Government System Using E-government Maturity Mode*L. Jurnal Penelitian Komunikasi dan Opini Publik Vol, 23(1), 16-24.

Damanik, M. P., & Purwaningsih, E. H. (2017). *E-government dan Aplikasinya di Lingkungan Pemerintah Daerah (Studi Kasus Kualitas Informasi Website Kabupaten Bengkalis Propinsi Riau).* Jurnal Studi Komunikasi dan Media, 21(2), 223355.

Saputra, M. R. Y., Winarno, W. W., & Henderi, H. 2020. *Evaluasi Tingkat Kematangan Spbe Di Disperindag Kabupaten Banjar*. Indonesian Journal of Business Intelligence (IJUBI), 3(1), 7-13.

Darmawan, A. K., & Dwiharto, A. 2019. Pengukuran Capability Level Kualitas Layanan E-*government* Kabupaten Pamekasan Menggunakan Framework COBIT 5.0. INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, 3(2), 93-103.

Primadewi, A., Yudatama, U., & Nugroho, S. 2017. *Pengukuran Tingkat Kematangan Pengembangan Business Intelligence Teknologi Informasi dan Komunikasi (TIK) pada Perguruan Tinggi.* Jurnal Rekayasa Sistem dan Teknologi Informasi, 1(1), 240111.

Wulansari, A., & Inayati, I. 2019. *Faktor-faktor kematangan implementasi e-government yang berorientasi kepada masyarakat*. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 5(1), 24-36.

Rahayuda, I. G. S. (2017). *Implementasi Teknologi Informasi Untuk Mengembangkan E-government Menggunakan Framework Laravel*. SEMNASTEKNOMEDIA ONLINE, 5(1), 2-4.

A CMMI Case Study: Process Engineering vs. Culture and Leadership. Jeffrey L. Dutton, Technical Director, Engineering Performance Improvement Centre, Jacobs Sverdrup

Function Point Pilot Results in IBG and RMG. Internal BMO Report, Alfred Allik, Director of Quality, BMO, September 2005.

Ottawa Software Quality Association &ASQ 0407 Software Focus Group November 2003 Process Improvement Experience: CMM Level 3 Best Practices, Gordana Kis, CSQA Sr. QA Specialist BMO.

Capability Maturity Model® Integration (CMMI®) Overview 2005 by Carnegie Mellon University.

CMU/SEI 01 Members of the Assessment Method Integrated Team Standard CMMISM Appraisal Method for Process Improvement (SCAMPISM), Version 1.1: Method Definition Document (CMU/SEI-2001-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001.
http://www.sei.cmu.edu/publications/documents/01.reports/01hb001.html.

Organizations. April 25, 2010.
http://www.scribd.com/doc/12596450/Software-Process-Models-and-Metricsfor-Small-Software-Organizations.

CMMI Product Team. CMMI for Development Version 1.2. CMU/SEI- 2006-TR-008, ESC-TR-2006-008. USA: Software Engineering Institute, Carnegie Mellon University. 2006.

Kneuper, R. CMMI–Improving Software and Systems Development Processes Using Capability Maturity Model Integration (CMMI-DEV). 2009.

CMMI Product Team. 2010. *CMMI for Development version 1.3*. Pittsburgh: Carnegie Mellon University.

TENTANG PENULIS

Dr. Ir. Sumijan, M.Sc. adalah Dosen Tetap Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang sejak 1991. Pendidikan Sarjana (S1) di Kampus Universitas Putra Indonesia "YPTK" Padang Tamat 1991, bidang Manajemen Informatika. Maraih Gelar Master dalam bidang Information Technology di University Technology Malaysia (UTM) tahun 1998. Meraih Gelar Doktor bidang Teknologi Informasi di Universitas Gunadarma Jakarta 2015. Bidang Penelitiannya adalah (1). Data Mining, (2). Artificial Intelligence, (3). Digital Image Processing.

Pradani Ayu Widya Purnama, S.Kom., M.Kom. adalah Dosen Tetap Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang sejak 2016. Pendidikan Sarjana (S1) di Kampus Universitas Putra Indonesia "YPTK" Padang Tamat 2014, bidang Teknik Informatika. Maraih Gelar Master dalam bidang Information Technology di Universitas Putra Indonesia "YPTK" Padang ditamatkan tahun 2016.

AUDIT TEKNOLOGI INFORMASI
PENERAPAN PADA *E-GOVERNMENT*
(*Best Practice e-government* Pemerintah Kota)

Auditing adalah suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan. Sedangkan audit IT adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal.

Tahapan audit teknologi sistem informasi dibagi menjadi 5 perencanaan (menentukan penugasan, menentukan staf dan jadwal audit, mengumpulkan informasi umum, melakukan *review* analitis), *review* pendahuluan (menentukan risiko audit yang diinginkan (*desired* audit risk), memperoleh pemahaman mengenai pengendalian manajemen, mendokumentasikan pengendalian aplikasi, menilai risiko pengendalian), pengujian pengendalian (pengujian pengendalian manajemen), pelaporan (menyusun dan mengkonfirmasi temuan, menganalisa temuan, menyusun simpulan/opini, menyusun konsep *management report/management letter*, menyampaikan dan menyajikan laporan), tindak lanjut (memantau rekomendasi).

Kasus penggunaan e-*government* (*best practice* pemerintah kota). Tingkat kematangan penerapan e-*government* di pemerintahan kota perlu diukur untuk mengetahui tata kelola konerja penerapan e-*government*, dalam hal ini ada beberapa domain, namun perlu memperhatikan rekomendasi dalam mengambil keputusan dan kebijakan dalam pengembangan dan penerapkan e-government di pemerintah kota agar dapat menentukan skala prioritas pengembangan dari tingkat kematangan (*maturity*) tata kelola teknologi informasi.

Penerbit Insan Cendekia Mandiri
Kapalo Koto No. 8, Selayo, Kec. Kubung, Solok
Email : penerbitbic@gmail.com
Website : www.insancendekiamandiri.co.id

IKAPI
IKATAN PENERBIT INDONESIA

IT
ISBN 978-623-6719-98-5
9 786236 719985