

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **2.1. Konsep Teoritis**

##### **2.1.1. Pengertian Sistem**

Ali dan Wangdra (2010: 8) menyebutkan bahwa Sistem (*system*) adalah kumpulan dari sub-sub sistem, elemen-elemen, prosedur-prosedur yang saling berintegrasi untuk mencapai tujuan tertentu, seperti informasi, target atau *goal*. Karakter suatu sistem terdiri dari Komponen (*Components*), Batas Sistem (*Boundary*), Lingkungan luar sistem (*Environments*), Penghubung (*Interface*), *Input Process* dan *Output*, Sasaran (*Objectives*), Tujuan (*Goal*).

Rochaety (2013: 3) menyimpulkan bahwa sistem dapat didefinisikan sebagai suatu kesatuan yang terdiri dari dua atau lebih komponen atau subsistem yang berinteraksi untuk mencapai suatu tujuan.

Nugroho (2008: 17) menyimpulkan bahwa sistem adalah sekelompok elemen yang terintegrasi dengan maksud yang sama untuk mencapai suatu tujuan. Hal pertama yang perlu diperhatikan dalam suatu sistem adalah elemen-elemennya. Tentunya setiap sistem memiliki elemen-elemen sendiri, yang kombinasinya berbeda antara sistem yang satu dengan sistem yang lain. Namun demikian, susunan dasarnya tetap sama.

### 2.1.2. Pengertian Informasi

Menurut Rochaety (2013: 6) menyimpulkan bahwa informasi merupakan kumpulan data yang telah diolah baik bersifat kualitatif maupun kuantitatif dan memiliki arti luas.

Zakiyudin (2012: 10) menyimpulkan bahwa informasi adalah data yang telah diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya. Informasi merupakan salah satu sumber daya yang sangat diperlukan dalam suatu organisasi.

Sedangkan Ali dan Wangdra (2010: 10) menyebutkan bahwa informasi adalah data yang diolah menjadi suatu bentuk yang penting bagi si penerima dan mempunyai nilai yang nyata atau dapat dirasakan manfaatnya dalam keputusan-keputusan yang akan datang.

Adapun kualitas informasi di tentukan oleh beberapa faktor, yaitu:

1. Keakuratan dan Teruji Kebenarannya

Artinya informasi harus bebas dari kesalahan-kesalahan, tidak bias dan tidak menyesatkan. Kesalahan-kesalahan itu dapat berupa kesalahan perhitungan maupun akibat gangguan (*noise*) yang dapat mengubah dan merusak informasi tersebut.

2. Kesempurnaan Informasi

Untuk mendukung faktor pertama tersebut diatas, maka kesempurnaan informasi menjadi faktor penting, dimana informasi disajikan lengkap tanpa pengurangan, penambahan atau perubahan.

3. Tepat Waktu

Informasi harus disajikan secara tepat waktu, mengingat informasi akan menjadi dasar dalam pengambilan keputusan. Keterlambatan informasi akan mengakibatkan kekeliruan dalam pengambilan keputusan.

#### 4. Relevansi

Informasi akan memiliki nilai manfaat yang tinggi, jika informasi tersebut diterima oleh mereka yang membutuhkan dan menjadi tidak berguna jika diberikan kepada mereka yang tidak membutuhkan.

#### 5. Mudah dan Murah

Kini, cara dan biaya untuk memperoleh informasi juga menjadi bahan pertimbangan tersendiri. Bilamana cara dan biaya untuk memperoleh informasi sulit dan mahal, maka orang tidak berminat untuk memperolehnya atau mencari alternatif substitusinya. Biaya mahal yang dimaksud disini, jika bobot informasi tidak sebanding dengan biaya yang harus dikeluarkan. Dan melalui teknologi internet, kini orang atau perusahaan dapat memperoleh informasi dengan mudah dan murah.

### **2.1.3. Pengertian Sistem Informasi**

Menurut Zakiyudin (2012: 13) sistem informasi adalah suatu sistem yang ada di dalam organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi yang bersifat manajerial dan kegiatan strategi dari suatu organisasi dan pihak luar tertentu dengan laporan yang diperlukan.

Ali dan Wangdra (2010: 13) menyimpulkan bahwa Sistem Informasi (*information system*) merupakan suatu kumpulan dari komponen-komponen dalam suatu perusahaan atau organisasi yang berhubungan dengan proses penciptaan dan pengaliran informasi. Dalam hal ini, TI hanya merupakan salah satu komponen dalam perusahaan. Komponen-komponen lainnya adalah prosedur, struktur organisasi, sumber daya manusia, produk, pelanggan, rekanan dan sebagainya. Keandalan suatu sistem informasi dalam organisasi terletak pada keterkaitan antar komponen yang ada, sehingga dapat dihasilkan dan dialirkan suatu informasi yang berguna (akurat, terpercaya detail, cepat, relevan dan sebagainya) untuk lembaga yang bersangkutan.

Sistem informasi dapat juga dikatakan sebagai suatu totalitas terpadu terdiri dari prosedur, tenaga pengolah (*brainware*), perangkat lunak (*software*), perangkat keras (*hardware*), pangkalan data (*database*), perangkat telekomunikasi (*telecommunication*) yang saling ketergantungan dan saling menentukan dalam rangka menyediakan informasi untuk mendukung proses pengambilan keputusan.

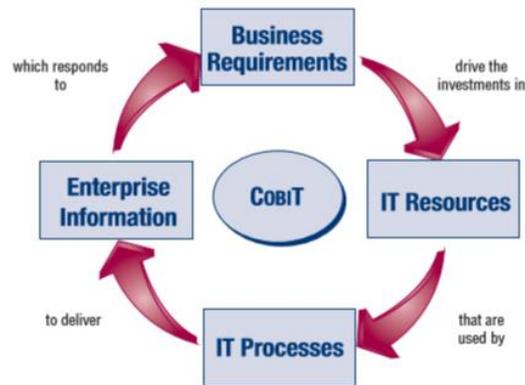
#### **2.1.4. Pengertian Sistem Pengadaan Secara Elektronik (SPSE)**

Sistem Pengadaan secara elektronik adalah Pengadaan Barang/Jasa yang dilaksanakan dengan menggunakan teknologi informasi dan transaksi elektronik sesuai dengan ketentuan peraturan perundang-undangan. Penyelenggaraan Pengadaan Barang/Jasa Pemerintah secara elektronik diatur dalam Peraturan Presiden nomor 54 Tahun 2010 tentang Pengadaan Barang/Jasa Pemerintah, dan sebagaimana ketentuan dalam pasal 131 ayat (1) bahwa pada tahun 2012 K/L/D/I

wajib melaksanakan Pengadaan Barang/Jasa secara elektronik untuk sebagian/seluruh paket-paket pekerjaan. Selain itu dalam Perpres 54 Tahun 2010 juga mengatur mengenai Layanan Pengadaan Secara Elektronik (LPSE) sebagai unit kerja K/L/D/I untuk menyelenggarakan sistem pelayanan Pengadaan Barang/Jasa secara elektronik yang ketentuan teknis operasionalnya diatur oleh Peraturan Kepala LKPP No. 2 Tahun 2010 tentang Layanan Pengadaan Secara Elektronik. LPSE dalam menyelenggarakan sistem pelayanan Pengadaan Barang/Jasa secara elektronik wajib memenuhi ketentuan sebagaimana yang ditentukan dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

#### **2.1.5. COBIT**

COBIT adalah singkatan dari *Control Objectives for Information and related Technology*. COBIT merupakan standar Tata Kelola TI yang dikembangkan oleh *IT Governance Institute (ITGI)*, yaitu sebuah organisasi yang melakukan studi tentang model Tata Kelola TI yang berbasis di Amerika Serikat. Berbeda dengan standar-standar Tata Kelola TI lainnya, COBIT mempunyai cakupan yang lebih luas, komprehensif dan mendalam dalam melihat proses pengelolaan TI, COBIT juga dapat digunakan sebagai *framework* untuk melakukan audit Teknologi Informasi. ITGI mengeluarkan versi COBIT secara bertahap. Dimulai dari COBIT 2.0, COBIT 3.0, COBIT 4.0, COBIT 4.1 dan terakhir yang baru dirilis pada pertengahan tahun 2012 adalah COBIT 5.0.



**Sumber:** IT Governance Institute 2007

**Gambar 2.1.** Prinsip Dasar COBIT

Manajemen sebuah organisasi akan berfungsi secara efektif apabila para pengambil keputusan selalu ditunjang dengan keberadaan informasi yang berkualitas. COBIT mendeskripsikan karakteristik informasi yang berkualitas menjadi tujuh (7) aspek utama, yaitu:

1. *Effectiveness*, dimana informasi yang dihasilkan haruslah relevan dan dapat memenuhi kebutuhan dari setiap proses bisnis terkait dan tersedia secara tepat waktu, akurat, konsisten dan dapat dengan mudah diakses.
2. *Efficiency*, dimana informasi dapat diperoleh dan disediakan melalui cara yang ekonomis, terutama terkait dengan konsumsi sumber daya yang dialokasikan.
3. *Confidentiality*, dimana informasi rahasia dan yang bersifat sensitif harus dapat dilindungi atau dipinjam keamanannya terutama dari pihak-pihak yang tidak berhak mengetahuinya.

4. *Availability*, dimana informasi haruslah tersedia bilamana dibutuhkan dengan kinerja waktu dan kapabilitas yang diharapkan.
5. *Compliance*, dimana informasi yang dimiliki harus dapat dipertanggungjawabkan kebenarannya dan mengacu pada hukum maupun regulasi yang berlaku termasuk di dalamnya mengikuti standar nasional atau internasional yang ada.
6. *Reliability*, dimana informasi yang dihasilkan haruslah berasal dari sumber yang dapat dipercaya sehingga tidak menyesatkan para pengambil keputusan yang menggunakan informasi tersebut.

Untuk memastikan hasil yang diperoleh dari proses TI sesuai kebutuhan bisnis, perlu diterapkan kendali-kendali yang tepat terhadap proses TI tersebut. Hasil yang diperoleh perlu diukur dan dibandingkan kesesuaiannya dengan kebutuhan bisnis organisasi secara berkala.

Keseluruhan informasi tersebut dihasilkan oleh sebuah TI yang dimiliki organisasi, dimana didalamnya terdapat sejumlah komponen sumber daya penting, yaitu:

1. Aplikasi, yang merupakan sekumpulan program untuk mengolah dan menampilkan data maupun informasi yang dimiliki oleh organisasi.
2. Informasi, yang merupakan hasil pengolahan dari data yang merupakan bahan mentah dari setiap informasi yang dihasilkan, dimana di dalamnya terkandung fakta dari aktivitas transaksi

dan interaksi sehari-hari masing-masing proses bisnis yang ada di organisasi.

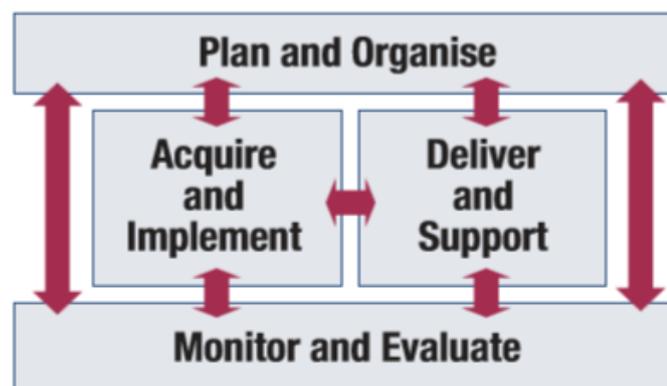
3. Infrastruktur, yang terdiri dari sejumlah perangkat keras, infrastruktur teknologi informasi sebagai teknologi pendukung untuk menjalankan portfolio aplikasi yang ada. Selain itu yang termasuk dalam infrastruktur dapat berupa sarana fisik seperti ruangan dan gedung dimana keseluruhan perangkat sistem dan teknologi informasi ditempatkan.
4. Manusia, yang merupakan pemakai dan pengelola dari sistem informasi yang dimiliki.

Kerangka kerja COBIT menyediakan model proses yang umumnya ditemukan dalam aktivitas TI dalam empat domain proses yang saling terkait yaitu: *Plan and Organize* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS) serta *Monitor and Evaluate* (ME). Adapun penjelasan masing-masing domain tersebut yaitu sebagai berikut:

1. *Plan and Organise* (PO), Domain ini mencakup masalah mengidentifikasi cara terbaik TI untuk memberikan kontribusi yang maksimal terhadap pencapaian tujuan bisnis organisasi. Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi organisasi.
2. *Acquire and Implement* (AI), Domain ini menitikberatkan pada proses pemilihan, pengadaan dan penerapan TI yang digunakan. Pelaksanaan strategi yang telah ditetapkan, harus disertai solusi-solusi TI yang sesuai

dan solusi TI tersebut diadakan, diimplementasikan dan diintegrasikan ke dalam proses bisnis organisasi.

3. *Deliver and Support* (DS), Domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan.
4. *Monitor and Evaluate* (ME), Domain ini menitikberatkan pada proses pengawasan pengelolaan TI pada organisasi seluruh kendali-kendali yang diterapkan setiap proses TI harus diawasi dan dinilai kelayakannya secara berkala. Domain ini fokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan internal dan eksternal.



Sumber: IT Governance Institute 2007

**Gambar 2.2. 4** (Empat) Domain dalam COBIT yang menggambarkan siklus hidup TI yang saling berhubungan

#### 2.1.6. *Control Objectives* Masing-masing Domain pada COBIT 4.0

### 2.1.6.1 *Plan and Organise*

#### 1. PO1 Mendefinisikan rencana strategis TI (*Define a Strategic IT Plan*)

##### PO1.1 Nilai Manajemen TI (*IT Value Management*)

Bekerja dengan bisnis untuk memastikan bahwa portofolio perusahaan dari investasi *TI-enabled* berisi program yang memiliki kasus bisnis yang kuat.

##### PO1.2 Penyelarasan bisnis TI (*Business-IT Alignment*)

Menetapkan proses pendidikan *bi-directional* dan keterlibatan timbal balik dalam perencanaan strategis untuk mencapai bisnis dan TI penyelarasan dan integrasi.

##### PO1.3 Penilaian Kemampuan dan kinerja Saat Ini (*Assessment of Current Capability and Performance*)

Menilai kemampuan saat ini dan kinerja solusi dan layanan pengiriman untuk membangun dasar terhadap yang kebutuhan masa depan dapat dibandingkan.

##### PO1.4 Rencana Strategis TI (*IT Strategic Plan*)

Membuat rencana strategis yang mendefinisikan, dalam kerjasama dengan *stakeholder* terkait, bagaimana tujuan IT akan memberikan kontribusi untuk tujuan strategis perusahaan dan biaya terkait dan risiko.

##### PO1.5 Rencana Taktis TI (*IT Tactical Plans*)

Membuat portofolio rencana IT taktis yang berasal dari rencana strategis TI. Rencana taktis harus membahas investasi Program *IT-enabled*, layanan TI dan aset TI.

#### PO1.6 Manajemen Portofolio TI (*IT Portfolio Management*)

Aktif mengelola dengan bisnis portofolio *IT-enabled* program investasi yang dibutuhkan untuk mencapai tujuan bisnis strategis yang spesifik dengan mengidentifikasi, mendefinisikan, mengevaluasi, memprioritaskan, memilih, memulai, mengelola dan mengendalikan program.

## 2. PO2 Mendefinisikan arsitektur informasi (*Define the Information Architecture*).

### PO2.1 Model Informasi Enterprise Architecture (*Enterprise Information Architecture Model*).

Membangun dan memelihara model informasi perusahaan untuk memungkinkan pengembangan aplikasi dan kegiatan pendukung keputusan, konsisten dengan IT berencana seperti yang dijelaskan dalam PO1.

### PO2.2 Perusahaan Kamus Data dan Data Aturan Syntax (*Enterprise Data Dictionary and Data Syntax Rules*).

Menjaga kamus data perusahaan yang menggabungkan aturan sintaks data organisasi.

### PO2.3 Skema Klasifikasi Data (*Data Classification Scheme*).

Membangun skema klasifikasi yang berlaku di seluruh perusahaan, berdasarkan kekritisian dan sensitivitas (misalnya, publik, rahasia, rahasia) dari data perusahaan.

#### PO2.4 Manajemen Integritas (*Integrity Management*)

Mendefinisikan dan menerapkan prosedur untuk memastikan integritas dan konsistensi dari semua data yang tersimpan dalam bentuk elektronik, seperti database, gudang data dan data arsip.

### 3. PO3 Menentukan arahan teknologi (*Determine Technological Direction*).

#### PO3.1 Perencanaan Tujuan Teknologi (*Technological Direction Planning*)

Analisis teknologi yang sudah ada dan muncul, dan rencana arah mana teknologi yang tepat untuk mewujudkan strategi TI dan arsitektur sistem bisnis.

#### PO3.2 Rencana Infrastruktur Teknologi (*Technology Infrastructure Plan*)

Menciptakan dan mempertahankan rencana infrastruktur teknologi yang sesuai dengan rencana strategis dan taktis IT.

#### PO3.3 Memantau Tren dan Peraturan Masa Depan (*Monitor Future Trends and Regulations*)

Menetapkan proses untuk memantau tren sektor bisnis, industri, teknologi, infrastruktur, lingkungan hukum dan peraturan. Menggabungkan konsekuensi dari tren ini ke dalam pengembangan rencana infrastruktur teknologi IT.

#### PO3.4 Standar Teknologi (*Technology Standards*)

Untuk memberikan konsisten, efektif dan aman solusi teknologi *enterprise wide*, membentuk forum teknologi untuk memberikan pedoman teknologi, saran pada produk infrastruktur dan bimbingan pada pemilihan teknologi, dan mengukur kepatuhan dengan standar dan pedoman.

#### PO3.5 Arsitektur Papan TI (*IT Architecture Board*)

Membangun arsitektur papan TI untuk memberikan pedoman arsitektur dan saran pada aplikasi mereka, dan untuk memverifikasi kepatuhan.

### 4. PO4 Mendefinisikan proses TI, organisasi dan keterhubungannya (*Define the IT Processes, Organisation and Relationships*).

#### PO4.1 Proses Kerangka TI (*IT Process Framework*)

Mendefinisikan kerangka proses TI untuk melaksanakan rencana strategis TI. Kerangka kerja ini harus mencakup struktur proses TI dan hubungan (misalnya, untuk mengelola kesenjangan proses dan tumpang tindih), kepemilikan, jatuh tempo, pengukuran kinerja, perbaikan, kepatuhan, target kualitas dan rencana untuk mencapainya.

#### PO4.2 Komite Strategi TI (*IT Strategy Committee*)

Membentuk komite strategi TI di tingkat dewan. Komite ini harus memastikan bahwa tata kelola TI, sebagai bagian dari tata kelola perusahaan, yang ditangani; nasihat tentang arah strategis; dan meninjau investasi besar atas nama full board.

#### PO4.3 Komite Pengarah TI (*IT Steering Committee*)

Membentuk komite pengarah IT (atau setara) yang terdiri dari eksekutif, bisnis dan manajemen TI untuk Menentukan prioritas *IT-enabled* program investasi sejalan dengan strategi bisnis perusahaan dan prioritas, Melacak status proyek dan menyelesaikan tingkat pelayanan konflik, Memantau sumber daya dan perbaikan layanan.

PO4.4 Penempatan Organisasi Fungsi TI (*Organisational Placement of the IT Function*).

Tempatkan fungsi IT dalam struktur organisasi secara keseluruhan dengan model bisnis bergantung pada pentingnya IT dalam perusahaan, khususnya kekritisannya untuk strategi bisnis dan tingkat ketergantungan operasional TI. Garis pelaporan dari CIO harus sepadan dengan pentingnya IT dalam perusahaan.

PO4.5 Struktur Organisasi TI (*IT Organisational Structure*)

Membentuk struktur organisasi TI internal dan eksternal yang mencerminkan kebutuhan bisnis. Selain itu, menempatkan proses di tempat untuk secara berkala meninjau struktur organisasi TI untuk menyesuaikan kebutuhan staf dan strategi sourcing untuk memenuhi diharapkan tujuan bisnis dan perubahan keadaan.

PO4.6 Pembentukan Peran dan Tanggung Jawab (*Establishment of Roles and Responsibilities*)

Membangun dan mengkomunikasikan peran dan tanggung jawab untuk personil IT dan pengguna akhir yang menggambarkan antara personil IT dan otoritas pengguna akhir, tanggung jawab dan akuntabilitas untuk memenuhi kebutuhan organisasi.

PO4.7 Tanggung Jawab Untuk Jaminan Kualitas TI (*Responsibility for IT Quality Assurance*)

Menetapkan tanggung jawab untuk kinerja jaminan kualitas (QA) fungsi dan memberikan kelompok QA dengan sistem QA sesuai, kontrol dan keahlian komunikasi. Pastikan bahwa penempatan organisasi dan tanggung jawab dan besarnya kelompok QA memenuhi persyaratan organisasi.

PO4.8 Tanggung jawab untuk Risiko, Keamanan dan Kepatuhan (*Responsibility for Risk, Security and Compliance*)

Menanamkan kepemilikan dan tanggung jawab untuk risiko dalam bisnis IT yang terkait pada tingkat senior yang sesuai. Mendefinisikan dan menetapkan peran penting untuk mengelola risiko TI, termasuk tanggung jawab khusus untuk keamanan informasi, keamanan fisik dan kepatuhan.

PO4.9 Data dan Kepemilikan Sistem (*Data and System Ownership*)

Menyediakan bisnis dengan prosedur dan alat-alat, memungkinkan untuk mengatasi tanggung jawabnya untuk kepemilikan data dan sistem informasi. Pemilik harus membuat keputusan tentang klasifikasi informasi dan sistem dan melindungi mereka sejalan dengan klasifikasi ini.

PO4.10 Pengawasasn (*Supervision*)

Menerapkan praktek pengawasan yang memadai dalam fungsi IT untuk memastikan bahwa peran dan tanggung jawab itu dilakukan dengan benar, untuk menilai apakah semua personel memiliki kewenangan yang cukup dan sumber daya untuk menjalankan peran dan tanggung jawab mereka, dan untuk umum meninjau KPI.

PO4.11 Pemisahan Tugas (*Segregation of Duties*)

Menerapkan pembagian peran dan tanggung jawab yang mengurangi kemungkinan untuk satu individu untuk kompromi proses kritis. Pastikan bahwa personil menjalankan tugas hanya berwenang yang relevan dengan pekerjaan masing-masing dan posisi.

PO4.12 Kepegawaian TI (*IT Staffing*)

Mengevaluasi kebutuhan kepegawaian secara teratur atau pada perubahan besar untuk bisnis, operasional atau lingkungan TI untuk memastikan bahwa fungsi IT memiliki sumber daya yang cukup untuk cukup dan tepat mendukung tujuan bisnis dan tujuan.

PO4.13 Personil TI Utama (*Key IT Personnel*)

Mendefinisikan dan mengidentifikasi personil IT kunci (misalnya, penggantian / personil cadangan), dan meminimalkan ketergantungan pada satu individu melakukan fungsi pekerjaan penting.

PO4.14 Kebijakan dan Prosedur Tenaga Kontrak (*Contracted Staff Policies and Procedures*).

Pastikan bahwa konsultan dan tenaga kontrak yang mendukung fungsi IT mengetahui dan mematuhi kebijakan organisasi untuk perlindungan aset

informasi organisasi sehingga mereka memenuhi disepakati persyaratan kontrak.

#### PO4.15 Hubungan (*Relationships*)

Membangun dan memelihara koordinasi, komunikasi dan penghubung struktur yang optimal antara fungsi TI dan berbagai kepentingan lain di dalam dan di luar fungsi IT, seperti papan, eksekutif, unit bisnis, pengguna individu, pemasok, petugas keamanan, manajer risiko, kelompok perusahaan kepatuhan, agen outsourcing dan manajemen *offsite*.

### 5. PO5 Mengelola investasi TI (*Manage the IT Investment*)

#### PO5.1 Kerangka Manajemen keuangan (*Financial Management Framework*)

Membangun dan mempertahankan kerangka kerja keuangan untuk mengelola investasi dan biaya aset dan layanan TI melalui portofolio investasi *IT-enabled*, kasus bisnis dan anggaran TI.

#### PO5.2 Prioritas Dalam Anggaran TI (*Prioritisation Within IT Budget*)

Melaksanakan proses pengambilan keputusan untuk memprioritaskan alokasi sumber daya TI untuk operasi, proyek dan pemeliharaan untuk memaksimalkan TI kontribusi untuk mengoptimalkan pengembalian portofolio perusahaan tentang *IT-enabled* program investasi dan layanan TI lainnya dan aset.

#### PO5.3 Penganggaran TI (*IT Budgeting*)

Menetapkan dan menerapkan praktik menyiapkan anggaran mencerminkan prioritas yang ditetapkan oleh portofolio perusahaan tentang program investasi *IT-enabled*, dan termasuk biaya berkelanjutan dari operasi dan pemeliharaan infrastruktur saat ini.

PO5.4 Manajemen Biaya (*Cost Management*)

Melaksanakan proses manajemen biaya membandingkan biaya aktual dengan anggaran. Biaya harus dipantau dan dilaporkan. Di mana ada penyimpangan, ini harus diidentifikasi secara tepat waktu dan dampak dari penyimpangan pada program harus dinilai.

PO5.5 Manajemen Manfaat (*Benefit Management*)

Menerapkan proses untuk memantau manfaat dari menyediakan dan memelihara kemampuan IT yang tepat.

6. PO6 Mengkomunikasikan tujuan dan arahan manajemen (*Communicate Management Aims and Direction*).

PO6.1 Kebijakan TI dan Pengendalian Lingkungan (*IT Policy and Control Environment*)

Tentukan unsur-unsur dari lingkungan pengendalian untuk TI, selaras dengan filosofi manajemen perusahaan dan gaya operasi.

PO6.2 Pengendalian Kerangka Kerja dan Resiko TI Perusahaan (*Enterprise IT Risk and Control Framework*)

Mengembangkan dan mempertahankan kerangka kerja yang mendefinisikan pendekatan perusahaan secara keseluruhan untuk IT risiko dan kontrol dan yang sejalan dengan kebijakan TI dan lingkungan kontrol dan kerangka risiko perusahaan dan kontrol.

PO6.3 Kebijakan Manajemen TI (*IT Policies Management*)

Mengembangkan dan mempertahankan serangkaian kebijakan untuk mendukung strategi TI.

PO6.4 Menyediakan Kebijakan, Standard dan Prosedur (*Policy, Standard and Procedures Rollout*)

Menyediakan dan menegakkan kebijakan untuk semua staf yang relevan TI, sehingga mereka dibangun ke dalam dan merupakan bagian integral dari operasi perusahaan.

PO6.5 Komunikasi Tujuan dan Arah TI (*Communication of IT Objectives and Direction*)

Mengkomunikasikan kesadaran dan pemahaman tentang bisnis dan tujuan TI dan arah kepada pemegang saham yang tepat dan pengguna di seluruh perusahaan.

7. PO7 Mengelola sumber daya TI (*Manage IT Human Resources*)

PO7.1 Perekrutan Personil dan Penyimpanan (*Personnel Recruitment and Retention*)

Menjaga proses perekrutan personel TI sesuai dengan kebijakan dan prosedur personel organisasi secara keseluruhan (misalnya, mempekerjakan, lingkungan kerja yang positif, yang berorientasi).

#### PO7.2 Keahlian Personil (*Personnel Competencies*)

Secara teratur memverifikasi bahwa personel memiliki kompetensi untuk memenuhi peran mereka atas dasar pendidikan, pelatihan dan / atau pengalaman.

#### PO7.3 Peran Karyawan (*Staffing of Roles*)

Tentukan, memantau dan mengawasi peran, tanggung jawab dan kerangka kerja kompensasi bagi, termasuk persyaratan untuk mematuhi kebijakan manajemen dan prosedur, kode etik, dan praktek profesional.

#### PO7.4 Pelatihan Personil (*Personnel Training*)

Menyediakan karyawan TI dengan orientasi yang tepat ketika menyewa dan pelatihan yang berkelanjutan untuk menjaga pengetahuan, keterampilan, kemampuan, kontrol internal mereka dan kesadaran keamanan pada tingkat yang diperlukan untuk mencapai tujuan organisasi.

#### PO7.5 Ketergantungan Pada Individu (*Dependence Upon Individuals*)

Meminimalkan paparan ketergantungan kritis pada individu utama melalui menangkap pengetahuan (dokumentasi), berbagi pengetahuan, perencanaan suksesi dan staf cadangan.

#### PO7.6 Prosedur Pemeriksaan Personil (*Personnel Clearance Procedures*)

Sertakan pemeriksaan latar belakang dalam proses rekrutmen TI. Tingkat dan frekuensi ulasan periodik pemeriksaan ini harus tergantung pada

kepekaan dan / atau kekritisannya dari fungsi dan harus diterapkan bagi karyawan, kontraktor dan vendor.

PO7.7 Evaluasi Prestasi Kerja Karyawan (*Employee Job Performance Evaluation*)

Membutuhkan evaluasi tepat waktu akan dilakukan secara teratur terhadap tujuan individu yang berasal dari tujuan organisasi, standar yang ditetapkan dan tanggung jawab pekerjaan yang spesifik. Karyawan harus menerima pelatihan pada kinerja dan melakukan kapanpun.

PO7.8 Perubahan Pekerjaan dan Pemutusan (*Job Change and Termination*)

Mengambil tindakan bijaksana mengenai perubahan pekerjaan, terutama penghentian pekerjaan. Transfer pengetahuan harus diatur, tanggung jawab ditugaskan kembali dan hak akses dihapus sehingga risiko diminimalkan dan kesinambungan fungsi dijamin

8. PO8 Mengelola kualitas (*Manage Quality*)

PO8.1 Sistem Manajemen Kualitas (*Quality Management System*)

Membangun dan memelihara SMM yang menyediakan standar, manajemen mutu pendekatan mengenai formal dan berkelanjutan yang selaras dengan kebutuhan bisnis.

PO8.2 Standar IT dan Praktek Kualitas (*IT Standards and Quality Practices*)

Mengidentifikasi dan mempertahankan standar, prosedur dan praktek untuk kunci proses TI untuk memandu organisasi dalam memenuhi

maksud dari QMS. Menggunakan praktik industri yang baik untuk referensi ketika meningkatkan dan menyesuaikan praktek mutu organisasi.

#### PO8.3 Pengembangan dan Standar Akuisisi (*Development and Acquisition Standards*)

Mengadopsi dan mempertahankan standar untuk semua pengembangan dan akuisisi yang mengikuti siklus hidup deliverable utama, dan termasuk tanda-off di tonggak kunci berdasarkan disepakati kriteria sign-off.

#### PO8.4 Fokus Pada Pelanggan (*Customer Focus*)

Manajemen mutu fokus pada pelanggan dengan menentukan kebutuhan mereka dan menyelaraskan mereka dengan standar dan praktik. Mendefinisikan peran dan tanggung jawab mengenai resolusi konflik antara pengguna / pelanggan dan organisasi TI.

#### PO8.5 Perbaikan Terus-Menerus (*Continuous Improvement*)

Memelihara dan teratur berkomunikasi rencana kualitas keseluruhan yang mempromosikan perbaikan terus-menerus.

#### PO8.6 Pengukuran Kualitas, Pemantauan dan Ulasan (*Quality Measurement, Monitoring and Review*)

Tentukan, merencanakan dan melaksanakan pengukuran untuk memantau terus kepatuhan terhadap SMM, serta nilai SMM menyediakan. Pengukuran, pemantauan dan pencatatan informasi harus digunakan oleh

pemilik proses untuk mengambil tindakan perbaikan dan pencegahan yang tepat.

9. PO9 Menaksir dan mengelola resiko TI (*Assess and Manage IT Risks*)

PO9.1 Kerangka Kerja Manajemen Risiko TI (*IT Risk Management Framework*)

Membentuk kerangka kerja manajemen risiko TI yang sejalan dengan kerangka kerja manajemen risiko (perusahaan itu) organisasi.

PO9.2 Pembentukan Konteks Risiko (*Establishment of Risk Context*)

Menetapkan konteks di mana kerangka penilaian risiko diterapkan untuk memastikan hasil yang tepat. Ini harus mencakup menentukan konteks internal dan eksternal masing-masing penilaian risiko, tujuan dari penilaian, dan kriteria yang risiko dievaluasi.

PO9.3 Identifikasi Peristiwa (*Event Identification*)

Identifikasi peristiwa (ancaman realistis penting yang mengeksploitasi kerentanan yang berlaku signifikan) dengan potensi dampak negatif pada tujuan atau operasi perusahaan, termasuk bisnis, peraturan, hukum, teknologi, mitra dagang, sumber daya manusia dan aspek operasional .

PO9.4 Penilaian Resiko (*Risk Assessment*)

Menilai secara berulang kemungkinan dan dampak dari semua risiko yang teridentifikasi, menggunakan metode kualitatif dan kuantitatif.

#### PO9.5 Respon Terhadap Resiko (*Risk Response*)

Mengembangkan dan memelihara proses respon risiko yang dirancang untuk memastikan bahwa kontrol biaya-efektif mengurangi eksposur risiko secara berkelanjutan.

#### PO9.6 Pemeliharaan dan Pemantauan Rencana Aksi Risiko (*Maintenance and Monitoring of a Risk Action Plan*)

Prioritaskan dan merencanakan kegiatan pengendalian di semua tingkatan untuk melaksanakan tanggapan risiko diidentifikasi sebagai diperlukan, termasuk identifikasi biaya, manfaat dan tanggung jawab untuk eksekusi.

### 10. PO10 Mengelola proyek (*Manage Projects*)

#### PO10.1 Kerangka Manajemen Program (*Programme Management Framework*)

Menjaga program proyek, terkait dengan portofolio *IT-enabled* program investasi, dengan mengidentifikasi, mendefinisikan, mengevaluasi, memprioritaskan, memilih, memulai, mengelola dan mengendalikan proyek.

#### PO10.2 Kerangka Manajemen Proyek (*Project Management Framework*)

Membangun dan mempertahankan kerangka kerja manajemen proyek yang mendefinisikan ruang lingkup dan batas-batas mengelola proyek, serta metode yang akan diadopsi dan diterapkan untuk setiap proyek yang dilakukan.

#### PO10.3 Pendekatan Manajemen Proyek (*Project Management Approach*)

Menetapkan pendekatan manajemen proyek sepadan dengan ukuran, kompleksitas dan persyaratan peraturan dari setiap proyek.

PO10.4 Komitmen Pemangku Kepentingan (*Stakeholder Commitment*)

Mendapatkan komitmen dan partisipasi dari pemangku kepentingan yang terkena dampak dalam definisi dan pelaksanaan proyek dalam konteks program investasi *IT-enabled* keseluruhan.

PO10.5 Pernyataan Lingkup proyek (*Project Scope Statement*)

Tentukan dan mendokumentasikan sifat dan lingkup proyek untuk mengkonfirmasi dan mengembangkan di antara para pemangku kepentingan pemahaman umum dari lingkup proyek dan bagaimana kaitannya dengan proyek lain dalam program investasi *IT-enabled* keseluruhan.

PO10.6 Inisiasi Tahap proyek (*Project Phase Initiation*)

Menyetujui inisiasi setiap fase proyek besar dan berkomunikasi kepada semua pemangku kepentingan. Mendasarkan persetujuan dari tahap awal pada keputusan tata kelola program.

PO10.7 Rencana Proyek Terpadu (*Integrated Project Plan*)

Membentuk formal, disetujui terintegrasi rencana proyek (meliputi bisnis dan sistem informasi sumber daya) untuk memandu pelaksanaan dan pengendalian proyek sepanjang hidup proyek.

PO10.8 Sumber Daya proyek (*Project Resources*)

Tentukan tanggung jawab, hubungan, wewenang dan kriteria kinerja anggota tim proyek, dan menentukan dasar untuk memperoleh dan

menugaskan anggota staf yang kompeten dan / atau kontraktor untuk proyek.

PO10.9 Manajemen Risiko Proyek (*Project Risk Management*)

Menghilangkan atau meminimalkan risiko spesifik yang terkait dengan proyek-proyek individu melalui proses yang sistematis perencanaan, mengidentifikasi, menganalisis, menanggapi, pemantauan dan pengendalian daerah atau peristiwa yang memiliki potensi untuk menyebabkan perubahan yang tidak diinginkan

PO10.10 Rencana Mutu Proyek (*Project Quality Plan*)

Siapkan rencana manajemen mutu yang menggambarkan sistem kualitas proyek dan bagaimana hal itu akan dilaksanakan. Rencana tersebut harus secara formal ditinjau dan disetujui oleh semua pihak yang terkait dan kemudian dimasukkan ke dalam rencana proyek terpadu.

PO10.11 Proyek Kontrol Perubahan (*Project Change Control*)

Membangun sistem kontrol perubahan untuk setiap proyek, sehingga semua perubahan baseline proyek (misalnya, biaya, jadwal, lingkup, kualitas) yang tepat, disetujui dan dimasukkan ke dalam rencana proyek terintegrasi sejalan dengan program dan kerangka tata kelola proyek.

PO10.12 Proyek Perencanaan Metode Jaminan (*Project Planning of Assurance Methods*)

Mengidentifikasi tugas jaminan yang dibutuhkan untuk mendukung akreditasi sistem baru atau diubah selama perencanaan proyek, dan memasukkan mereka dalam rencana proyek terpadu. Tugas harus

memberikan jaminan bahwa pengendalian internal dan fitur keamanan memenuhi persyaratan yang ditetapkan.

PO10.13 Proyek Pengukuran Kinerja, Pelaporan dan Pengawasan (*Project Performance Measurement, Reporting and Monitoring*)

Mengukur kinerja proyek terhadap kriteria lingkup kinerja proyek, jadwal, kualitas, biaya dan risiko utama. Mengidentifikasi penyimpangan apapun dari rencana tersebut.

PO10.14 Proyek Penutupan (*Project Closure*)

Mengharuskan, pada akhir setiap proyek, pemangku kepentingan proyek memastikan apakah proyek tersebut menyampaikan hasil yang direncanakan dan manfaat.

### **2.1.6.2 *Acquire and Implement***

1. AI1 Mengidentifikasi Solusi Otomatis (*Identify Automated Solutions*)

AI1.1 Definisi dan Pemeliharaan Bisnis Kebutuhan Fungsional dan Teknis (*Definition and Maintenance of Business Functional and Technical Requirements*)

Mengidentifikasi, memprioritaskan, tentukan dan menyepakati bisnis kebutuhan fungsional dan teknis meliputi ruang lingkup penuh dari semua inisiatif yang diperlukan untuk mencapai hasil yang diharapkan dari program investasi pengaktifan TI.

AI1.2 Analisis Laporan Risiko (*Risk Analysis Report*)

Mengidentifikasi, dokumen dan menganalisis risiko yang terkait dengan kebutuhan bisnis dan solusi desain sebagai bagian dari proses organisasi untuk pengembangan persyaratan.

#### AI1.3 Studi Kelayakan dan Penyusunan Program Alternatif Aksi (*Feasibility Study and Formulation of Alternative Courses of Action*)

Mengembangkan studi kelayakan yang mengkaji kemungkinan penerapan persyaratan. Manajemen bisnis, didukung oleh fungsi TI, harus menilai kelayakan dan tindakan alternatif dan membuat rekomendasi kepada sponsor bisnis.

#### AI1.4 Persyaratan dan Kelayakan Keputusan dan Persetujuan (*Requirements and Feasibility Decision and Approval*)

Memverifikasi bahwa proses ini membutuhkan sponsor bisnis untuk menyetujui dan menandatangani bisnis kebutuhan fungsional dan teknis dan laporan studi kelayakan pada tahap kunci yang telah ditentukan. Sponsor bisnis harus membuat keputusan akhir sehubungan dengan pilihan solusi dan akuisisi pendekatan.

## 2. AI2 Memperoleh dan Mempertahankan Aplikasi Software (*Acquire and Maintain Application Software*)

### AI2.1 Desain Tingkat Tinggi (*High-level Design*)

Terjemahkan kebutuhan bisnis ke dalam spesifikasi desain tingkat tinggi untuk perangkat lunak akuisisi, dengan mempertimbangkan teknologi arah dan informasi arsitektur organisasi.

### AI2.2 Desain yang Rinci (*Detailed Design*)

Siapkan desain rinci dan persyaratan aplikasi perangkat lunak teknis. Mendefinisikan kriteria untuk penerimaan persyaratan. Memiliki persyaratan yang disetujui untuk memastikan bahwa mereka sesuai dengan desain tingkat tinggi.

### AI2.3 Pengontrolan Aplikasi dan Audit (*Application Control and Auditability*)

Melaksanakan kontrol bisnis, dimana tepat, dalam pengendalian aplikasi otomatis sehingga pengolahan akurat, lengkap, tepat waktu, resmi dan auditable.

### AI2.4 Keamanan dan Ketersediaan aplikasi (*Application Security and Availability*)

Aplikasi alamat keamanan dan ketersediaan persyaratan dalam menanggapi risiko yang teridentifikasi dan sesuai dengan klasifikasi data organisasi, arsitektur informasi, arsitektur keamanan informasi dan toleransi risiko

### AI2.5 Konfigurasi dan Implementasi Software Aplikasi Yang Diperoleh (*Configuration and Implementation of Acquired Application Software*)

Mengkonfigurasi dan mengimplementasikan perangkat lunak aplikasi mengakuisisi untuk memenuhi tujuan bisnis.

### AI2.6 Upgrade besar untuk Sistem yang Ada (*Major Upgrades to Existing Systems*)

Dalam hal perubahan besar untuk sistem yang mengakibatkan perubahan signifikan dalam desain dan / atau fungsi saat ini sudah ada, mengikuti proses perkembangan yang sama seperti yang digunakan untuk pengembangan sistem baru.

#### AI2.7 Pengembangan Aplikasi Perangkat Lunak (*Development of Application Software*)

Memastikan bahwa fungsi otomatis dikembangkan sesuai dengan spesifikasi desain, standar pengembangan dan dokumentasi, persyaratan QA, dan standar persetujuan. Memastikan bahwa semua aspek hukum dan kontrak diidentifikasi dan ditangani untuk aplikasi perangkat lunak yang dikembangkan oleh pihak ketiga.

#### AI2.8 Jaminan Kualitas Perangkat Lunak (*Software Quality Assurance*)

Mengembangkan sumber daya dan melaksanakan rencana *software* QA untuk mendapatkan kualitas yang ditentukan dalam definisi persyaratan dan kebijakan dan prosedur mutu organisasi.

#### AI2.9 Manajemen Aplikasi Persyaratan (*Applications Requirements Management*)

Melacak status kebutuhan individu (termasuk semua persyaratan ditolak) selama desain, pengembangan dan implementasi, dan menyetujui perubahan persyaratan melalui proses perubahan manajemen didirikan.

#### AI2.10 Perbaikan Aplikasi Perangkat Lunak (*Application Software Maintenance*)

Mengembangkan strategi dan rencana untuk pemeliharaan aplikasi perangkat lunak.

3. AI3 Memperoleh dan Mempertahankan Teknologi Infrastruktur (*Acquire and Maintain Technology Infrastructure*)

AI3.1 Rencana Akuisisi Infrastruktur teknologi (*Technological Infrastructure Acquisition Plan*)

Menghasilkan rencana untuk akuisisi, implementasi dan pemeliharaan infrastruktur teknologi yang memenuhi bisnis yang didirikan persyaratan fungsional dan teknis dan sesuai dengan arah teknologi organisasi.

AI3.2 Perlindungan Sumber Daya Infrastruktur dan Ketersediaan (*Infrastructure Resource Protection and Availability*)

Melaksanakan pengendalian internal, langkah-langkah keamanan dan auditability selama konfigurasi, integrasi dan pemeliharaan perangkat keras dan perangkat lunak infrastruktur untuk melindungi sumber daya dan menjamin ketersediaan dan integritas.

AI3.3 Pemeliharaan infrastruktur (*Infrastructure Maintenance*)

Mengembangkan strategi dan rencana untuk pemeliharaan infrastruktur, dan memastikan bahwa perubahan dikendalikan sesuai dengan prosedur perubahan manajemen organisasi.

AI3.4 Kelayakan Uji Lingkungan (*Feasibility Test Environment*)

Membangun pengembangan dan pengujian lingkungan untuk mendukung efektif dan efisien kelayakan dan integrasi pengujian komponen infrastruktur.

4. AI4 Mengaktifkan Operasi dan Penggunaan (*Enable Operation and Use*)

AI4.1 Perencanaan untuk Solusi Operasional (*Planning for Operational Solutions*)

Mengembangkan rencana untuk mengidentifikasi dan mendokumentasikan semua teknis, operasional dan penggunaan aspek sehingga semua orang yang akan beroperasi, menggunakan dan memelihara solusi otomatis dapat melaksanakan tanggung jawab mereka.

AI4.2 Transfer Pengetahuan Manajemen Bisnis (*Knowledge Transfer to Business Management*)

Mentransfer pengetahuan untuk manajemen bisnis untuk memungkinkan orang-orang untuk mengambil kepemilikan sistem dan data, dan melaksanakan tanggung jawab untuk pengiriman layanan dan kualitas, pengendalian internal, dan administrasi aplikasi.

AI4.3 Transfer Pengetahuan untuk Pengguna Akhir (*Knowledge Transfer to End Users*)

Mentransfer pengetahuan dan keterampilan untuk memungkinkan pengguna akhir untuk secara efektif dan efisien menggunakan sistem dalam mendukung proses bisnis.

AI4.4 Transfer Pengetahuan untuk Operasi dan Dukungan Staf (*Knowledge Transfer to Operations and Support Staff*)

Mentransfer pengetahuan dan keterampilan yang memungkinkan operasi dan staf dukungan teknis untuk secara efektif dan efisien memberikan dukungan dan memelihara sistem dan infrastruktur terkait.

5. AI5 Pengadaan Sumber daya TI (*Procure IT Resource*)

AI5.1 Pengadaan Kontrol (*Procurement Control*)

Mengembangkan dan mengikuti serangkaian prosedur dan standar yang konsisten dengan proses pengadaan keseluruhan organisasi bisnis dan strategi akuisisi untuk memperoleh IT terkait infrastruktur, fasilitas, perangkat keras, perangkat lunak dan layanan yang dibutuhkan oleh bisnis.

AI5.2 Manajemen Kontrak Pemasok (*Supplier Contract Management*)

Menyiapkan prosedur untuk membangun, memodifikasi dan mengakhiri kontrak untuk semua pemasok. Prosedur harus mencakup, minimal, hukum, keuangan, organisasi, dokumenter, kinerja, keamanan, kekayaan intelektual, dan tanggung jawab terminasi dan kewajiban (termasuk klausul penalti). Semua kontrak dan perubahan kontrak harus ditinjau oleh penasehat hukum.

AI5.3 Seleksi Pemasok (*Supplier Selection*)

Pilih pemasok menurut praktek yang adil dan formal untuk memastikan terbaik fit layak berdasarkan persyaratan yang ditentukan. Persyaratan harus dioptimalkan dengan masukan dari calon pemasok.

AI5.4 Memperoleh Sumber Daya TI (*IT Resources Acquisition*)

Melindungi dan menegakkan kepentingan organisasi di semua perjanjian kontrak akuisisi, termasuk hak dan kewajiban semua pihak dalam hal kontrak untuk perolehan perangkat lunak, sumber daya pembangunan, infrastruktur dan jasa.

6. AI6 Mengelola Perubahan (*Manage Changes*)

AI6.1 Perubahan Standar dan Prosedur (*Change Standards and Procedures*)

Menyiapkan prosedur manajemen perubahan formal untuk menangani dengan cara yang standar semua permintaan (termasuk pemeliharaan dan patch) untuk perubahan aplikasi, prosedur, proses, sistem dan layanan parameter, dan platform yang mendasari.

AI6.2 Penilaian Dampak, Prioritas dan Otorisasi (*Impact Assessment, Prioritisation and Authorisation*)

Menilai semua permintaan untuk perubahan dalam cara yang terstruktur untuk menentukan dampak pada sistem operasional dan fungsionalitas. Memastikan bahwa perubahan dikategorikan, diprioritaskan dan berwenang.

AI6.3 Perubahan Darurat (*Emergency Changes*)

Menetapkan proses untuk mendefinisikan, mengangkat, pengujian, mendokumentasikan, menilai dan otorisasi perubahan darurat yang tidak mengikuti proses perubahan didirikan

#### AI6.4 Perubahan Pelacakan Status dan Pelaporan (*Change Status Tracking and Reporting*)

Membangun sistem pelacakan dan pelaporan untuk mendokumentasikan perubahan ditolak, mengkomunikasikan status disetujui dan dalam proses perubahan, dan perubahan lengkap. Pastikan bahwa menyetujui perubahan diimplementasikan seperti yang direncanakan.

#### AI6.5 Perubahan Penutupan dan Dokumentasi (*Change Closure and Documentation*)

Setiap kali perubahan diimplementasikan, memperbarui sistem yang terkait dan dokumentasi pengguna dan prosedur sesuai.

### 7. AI7 Menginstal dan Mengakreditasi Solusi dan Perubahan (*Install and Accredited Solutions and Changes*)

#### AI7.1 Pelatihan (*Training*)

Melatih anggota staf dari departemen pengguna yang terkena dampak dan kelompok operasi fungsi IT sesuai dengan rencana pelatihan dan implementasi pasti dan bahan terkait, sebagai bagian dari setiap pengembangan sistem informasi, implementasi atau proyek modifikasi.

#### AI7.2 Rencana Uji (*Test Plan*)

Menetapkan rencana uji berdasarkan standar *organisation wide* yang mendefinisikan peran, tanggung jawab, dan masuk dan keluar kriteria. Pastikan bahwa rencana itu disetujui oleh pihak-pihak terkait.

#### AI7.3 Rencana Implementasi (*Implementation Plan*)

Membentuk pelaksanaan dan rencana mundur / *backout*. Mendapatkan persetujuan dari pihak-pihak terkait.

#### AI7.4 Uji Lingkungan (*Test Environment*)

Menentukan dan menetapkan perwakilan lingkungan pengujian aman dari lingkungan operasi yang direncanakan relatif terhadap keamanan, pengendalian internal, praktek operasional, kualitas data dan persyaratan privasi, dan beban kerja.

#### AI7.5 Perubahan Sistem dan Data (*System and Data Conversion*)

Rencana konversi data dan migrasi infrastruktur sebagai bagian dari metode pengembangan organisasi, termasuk audit, *rollbacks* dan *fallbacks*.

#### AI7.6 Pengujian Perubahan (*Testing of Changes*)

Perubahan tes mandiri sesuai dengan rencana tes ditentukan sebelum migrasi ke lingkungan operasional. Memastikan bahwa rencana tersebut menganggap keamanan dan kinerja.

#### AI7.7 Pengujian Penerimaan Akhir (*Final Acceptance Test*)

Memastikan bahwa pemilik proses bisnis dan TI stakeholder mengevaluasi hasil dari proses pengujian yang ditentukan oleh rencana uji. Memulihkan kesalahan signifikan yang diidentifikasi dalam proses pengujian, setelah menyelesaikan suite tes diidentifikasi dalam rencana uji dan setiap tes regresi diperlukan.

#### AI7.8 Promosi ke Produksi (*Promotion to Production*)

Berikut pengujian, mengontrol serah terima sistem berubah ke operasi, menjaganya agar tetap sejalan dengan rencana implementasi. Memperoleh persetujuan dari *stakeholder* utama, seperti pengguna, pemilik sistem dan manajemen operasional.

#### AI7.9 Pasca-pelaksanaan Ulasan (*Post-implementation Review*)

Menetapkan prosedur sesuai dengan standar manajemen perubahan organisasi memerlukan *review* pasca-pelaksanaan sebagaimana diatur dalam rencana implementasi.

### **2.1.6.3 Deliver and Support**

1. DS1 Mendefinisikan dan Mengelola Tingkat Layanan (*Define and Manage Service Levels*)

#### DS1.1 Kerangka Service Level Manajemen (*Service Level Management Framework*)

Mendefinisikan kerangka kerja yang menyediakan proses manajemen tingkat layanan formal antara pelanggan dan penyedia layanan.

#### DS1.2 Definisi Layanan (*Definition of Services*)

Definisi dasar dari layanan TI pada karakteristik layanan dan kebutuhan bisnis. Pastikan bahwa mereka terorganisir dan disimpan secara terpusat melalui pelaksanaan pendekatan portofolio katalog layanan.

#### DS1.3 Tingkatan Jasa Persetujuan (*Service Level Agreements*)

Mendefinisikan dan menyetujui SLA untuk semua layanan TI penting berdasarkan kebutuhan pelanggan dan kemampuan IT.

#### DS1.4 Perjanjian Tingkat operasi (*Operating Level Agreements*)

Tentukan OLA yang menjelaskan bagaimana layanan akan secara teknis disampaikan untuk mendukung SLA secara optimal. The OLA harus menentukan proses teknis dalam hal berarti bagi penyedia dan dapat mendukung beberapa SLA.

#### DS1.5 Pemantauan dan Pelaporan Prestasi Tingkat Pelayanan (*Monitoring and Reporting of Service Level Achievements*)

Terus memantau kriteria kinerja *service level* tertentu. Laporan tentang pencapaian tingkat pelayanan harus disediakan dalam format yang berarti bagi para pemangku kepentingan.

#### DS1.6 Ulasan Layanan Perjanjian Tingkat dan Kontrak (*Review of Service Level Agreements and Contracts*)

Secara teratur meninjau SLA dan kontrak mendasari dengan penyedia layanan internal dan eksternal untuk memastikan bahwa mereka efektif dan up to date dan bahwa perubahan persyaratan telah diperhitungkan.

## 2. DS2 Mengelola Layanan pihak ketiga (*Manage Third-party Services*)

### DS2.1 Identifikasi Semua Hubungan Pemasok (*Identification of All Supplier Relationships*)

Mengidentifikasi semua layanan pemasok, dan mengkategorikan mereka sesuai dengan jenis pemasok, signifikansi dan kekritisan. Memelihara dokumentasi formal hubungan teknis dan organisasi yang meliputi peran dan tanggung jawab, tujuan, kiriman diharapkan, dan mandat perwakilan dari pemasok.

### DS2.2 Manajemen Hubungan Pemasok (*Supplier Relationship Management*)

Memformalkan proses manajemen hubungan pemasok untuk setiap pemasok. Pemilik hubungan harus bekerja sama dalam isu-isu pelanggan dan pemasok dan memastikan kualitas hubungan berdasarkan kepercayaan dan transparansi (misalnya, melalui SLA).

### DS2.3 Manajemen Risiko pemasok (*Supplier Risk Management*)

Mengidentifikasi dan mengurangi risiko yang berkaitan dengan *suppliers ability* untuk melanjutkan pelayanan yang efektif dengan cara yang aman dan efisien secara terus menerus.

### DS2.4 Pemantauan Kinerja pemasok (*Supplier Performance Monitoring*)

Menetapkan proses untuk memantau pelayanan untuk memastikan bahwa pemasok adalah memenuhi kebutuhan bisnis saat ini dan terus mematuhi perjanjian kontrak dan SLA, dan kinerja yang kompetitif dengan pemasok alternatif dan kondisi pasar.

3. DS3 Mengelola Kinerja dan Kapasitas (*Manage Performance and Capacity*)

DS3.1 Kinerja dan Kapasitas Perencanaan (*Performance and Capacity Planning*)

Menetapkan proses perencanaan untuk meninjau kinerja dan kapasitas sumber daya TI untuk memastikan bahwa kapasitas biaya-dibenarkan dan kinerja yang tersedia untuk memproses disepakati beban kerja sebagaimana ditentukan oleh SLA.

DS3.2 Kinerja saat ini dan Kapasitas (*Current Performance and Capacity*)

Menilai kinerja dan kapasitas sumber daya TI saat ini untuk menentukan apakah kapasitas dan kinerja yang cukup ada untuk memberikan terhadap tingkat layanan yang disepakati.

DS3.3 Kinerja masa depan dan Kapasitas (*Future Performance and Capacity*)

Melakukan kinerja dan kapasitas peramalan sumber daya TI secara berkala untuk meminimalkan risiko gangguan layanan karena kapasitas

yang tidak memadai atau penurunan kinerja, dan mengidentifikasi kelebihan kapasitas untuk kemungkinan pemindahan.

#### DS3.4 Ketersediaan Sumber Daya TI (*IT Resources Availability*)

Menyediakan kapasitas yang diperlukan dan kinerja, memperhitungkan aspek seperti beban kerja normal, kontinjensi, persyaratan penyimpanan dan sumber daya TI siklus hidup.

#### DS3.5 Pemantauan dan Pelaporan (*Monitoring and Reporting*)

Terus memantau kinerja dan kapasitas sumber daya TI. Data yang dikumpulkan harus melayani dua tujuan:

1. Untuk mempertahankan dan menyempurnakan kinerja saat ini dalam IT dan menangani masalah-masalah seperti ketahanan, kontinjensi, saat ini dan proyeksi beban kerja, rencana penyimpanan, dan akuisisi sumber daya
2. Untuk melaporkan ketersediaan layanan dikirim ke bisnis, seperti yang dipersyaratkan oleh SLA

#### 4. DS4 Pastikan Layanan Kontinyu (*Ensure Continuous Service*)

##### DS4.1 Kerangka Kontinyu TI (*IT Continuity Framework*)

Mengembangkan kerangka kerja untuk kelangsungan IT untuk mendukung manajemen kelangsungan bisnis perusahaan-menggunakan proses yang konsisten.

#### DS4.2 Rencana Kontinyu TI (*IT Continuity Plans*)

Mengembangkan IT rencana kesinambungan berdasarkan kerangka dan dirancang untuk mengurangi dampak dari gangguan besar pada fungsi bisnis utama dan proses.

#### DS4.3 Kritis Sumber Daya TI (*Critical IT Resources*)

Memusatkan perhatian pada item ditetapkan sebagai yang paling penting dalam rencana kesinambungan TI untuk membangun di ketahanan dan menetapkan prioritas dalam situasi pemulihan.

#### DS4.4 Pemeliharaan Rencana Kontinuitas TI (*Maintenance of the IT Continuity Plan*)

Mendorong manajemen TI untuk menentukan dan melaksanakan prosedur perubahan kontrol untuk memastikan bahwa rencana kesinambungan TI terus up to date dan terus mencerminkan kebutuhan bisnis yang sebenarnya.

#### DS4.5 Pengujian Rencana Kontinuitas TI (*Testing of the IT Continuity Plan*)

Menguji rencana kesinambungan TI secara teratur untuk memastikan bahwa sistem TI dapat secara efektif pulih, kekurangan ditangani dan rencana tetap relevan.

#### DS4.6 Pelatihan Rencana Kontinuitas TI (*IT Continuity Plan Training*)

Menyediakan semua pihak terkait dengan sesi pelatihan rutin mengenai prosedur dan peran mereka dan tanggung jawab dalam kasus insiden atau bencana. Verifikasi dan meningkatkan pelatihan sesuai dengan hasil tes kontingensi.

#### DS4.7 Distribusi Rencana Kontinuitas TI (*Distribution of the IT Continuity Plan*)

Menentukan bahwa strategi distribusi ditetapkan dan berhasil ada untuk memastikan bahwa rencana benar dan aman didistribusikan dan tersedia untuk berwenang, pihak yang berkepentingan kapan dan di mana diperlukan. Perhatian harus dibayar untuk membuat rencana diakses di bawah semua skenario bencana.

#### DS4.8 Pemulihan dan Kembalinya Pelayanan TI (*IT Services Recovery and Resumption*)

Rencana tindakan yang akan diambil untuk periode ketika TI sudah mulai pulih dan melanjutkan layanan. Ini mungkin termasuk aktivasi situs cadangan, inisiasi alternatif pengolahan, pelanggan dan pemangku kepentingan komunikasi, dan prosedur dimulainya kembali. Memastikan bahwa bisnis memahami IT kali pemulihan dan investasi teknologi yang

diperlukan untuk mendukung pemulihan bisnis dan kebutuhan dimulainya kembali.

#### DS4.9 Penyimpanan Cadangan Luar (*Offsite Backup Storage*)

Menyimpan media backup *offsite* semua penting, dokumentasi dan sumber daya TI lainnya yang diperlukan untuk pemulihan dan kesinambungan bisnis IT rencana.

#### DS4.10 Pasca kembalinya Ulasan (*Post-resumption Review*)

Menentukan apakah manajemen TI telah menetapkan prosedur untuk menilai kecukupan rencana sehubungan dengan dimulainya kembali sukses dari fungsi TI setelah bencana, dan memperbarui rencana yang sesuai.

### 5. DS5 Memastikan Sistem Keamanan (*Ensure Systems Security*)

#### DS5.1 Keamanan Manajemen TI (*Management of IT Security*)

Mengelola keamanan TI pada tingkat organisasi tertinggi yang tepat, sehingga pengelolaan tindakan keamanan ini sejalan dengan kebutuhan bisnis.

#### DS5.2 Rencana Keamanan TI (*IT Security Plan*)

Menerjemahkan bisnis, risiko dan persyaratan kepatuhan dalam rencana keamanan TI secara keseluruhan, dengan mempertimbangkan infrastruktur TI dan budaya keamanan. Memastikan bahwa rencana tersebut diimplementasikan dalam kebijakan dan prosedur keamanan bersama-sama dengan investasi yang tepat dalam layanan, personil,

perangkat lunak dan perangkat keras. Mengkomunikasikan kebijakan dan prosedur keamanan untuk *stakeholder* dan pengguna.

#### DS5.3 Manajemen Identitas (*Identity Management*)

Memastikan bahwa semua pengguna (*internal, eksternal* dan sementara) dan aktivitas mereka pada sistem IT (aplikasi bisnis, lingkungan TI, sistem operasi, pengembangan dan pemeliharaan) yang unik diidentifikasi.

#### DS5.4 Pengelolaan Pengguna Akun (*User Account Management*)

Permintaan alamat, membangun, menerbitkan, menanggukhan, memodifikasi dan menutup account pengguna dan hak pengguna terkait dengan serangkaian prosedur manajemen akun pengguna.

#### DS5.5 Pengujian Keamanan, Pengawasan dan Pemantauan (*Security Testing, Surveillance and Monitoring*)

Tes dan memonitor pelaksanaan keamanan IT dengan cara proaktif. keamanan TI harus reaccredited pada waktu yang tepat untuk memastikan bahwa dasar keamanan informasi perusahaan yang disetujui ini dipertahankan.

#### DS5.6 Definisi Insiden Keamanan (*Security Incident Definition*)

Jelas mendefinisikan dan mengkomunikasikan karakteristik insiden keamanan potensial sehingga mereka dapat benar diklasifikasikan dan diperlakukan dengan proses manajemen insiden dan masalah.

#### DS5.7 Perlindungan Keamanan Teknologi (*Protection of Security Technology*)

Membuat teknologi yang berhubungan dengan keamanan tahan terhadap gangguan, dan tidak mengungkapkan dokumentasi keamanan tidak perlu.

#### DS5.8 Pengelolaan Kunci Kriptografi (*Cryptographic Key Management*)

Menentukan bahwa kebijakan dan prosedur di tempat untuk mengatur generasi, perubahan, pencabutan, kehancuran, distribusi, sertifikasi, penyimpanan, entri, penggunaan dan pengarsipan kunci kriptografi untuk memastikan perlindungan kunci terhadap modifikasi dan pengungkapan yang tidak sah.

#### DS5.9 Pencegahan Perangkat Lunak Berbahaya, Deteksi dan Koreksi (*Malicious Software Prevention, Detection and Correction*)

Masukan preventif, detektif dan langkah-langkah perbaikan di tempat (terutama *up-to-date patch* keamanan dan kontrol virus) di seluruh organisasi untuk melindungi sistem informasi dan teknologi dari *malware* (misalnya, *virus*, *worm*, *spyware*, *spam*).

#### DS5.10 Keamanan Jaringan (*Network Security*)

Gunakan teknik dan prosedur keamanan manajemen terkait (mis, *firewall*, peralatan keamanan, segmentasi jaringan, deteksi intrusi) untuk mengotorisasi akses dan kontrol arus informasi dari dan ke jaringan.

#### DS5.11 Pertukaran Data Sensitif (*Exchange of Sensitive Data*)

Pertukaran data transaksi sensitif hanya melalui jalur dipercaya atau menengah dengan kontrol untuk menyediakan keaslian konten, bukti penyerahan, bukti penerimaan dan *non-repudiation* asal.

#### **2.1.6.4 Monitor and Evaluate**

1. ME1 Memantau dan Mengevaluasi Kinerja IT (*Monitor and Evaluate IT Performance*)

##### ME1.1 Pendekatan Pemantauan (*Monitoring Approach*)

Membangun kerangka pemantauan umum dan pendekatan untuk menentukan ruang lingkup, metodologi dan proses yang harus diikuti untuk mengukur TI solusi dan layanan pengiriman, dan memantau TI kontribusi untuk bisnis. Mengintegrasikan kerangka dengan sistem manajemen kinerja perusahaan.

##### ME1.2 Definisi dan Pengumpulan Data Pemantauan (*Definition and Collection of Monitoring Data*)

Bekerja dengan bisnis untuk menentukan yang seimbang target kinerja dan telah mereka disetujui oleh bisnis dan pemangku kepentingan terkait lainnya. Menentukan tolok ukur yang dapat digunakan untuk membandingkan target, dan mengidentifikasi data yang tersedia harus dikumpulkan untuk mengukur target. Menetapkan proses untuk mengumpulkan data yang tepat waktu dan akurat untuk melaporkan kemajuan terhadap sasaran.

##### ME1.3 Metode Pemantauan (*Monitoring Method*)

Menyebarkan metode pemantauan kinerja (misalnya, balanced scorecard) yang mencatat target; menangkap pengukuran; menyediakan ringkas, all-around lihat kinerja TI; dan cocok dalam sistem pemantauan perusahaan.

#### ME1.4 Penilaian Kinerja (*Performance Assessment*)

Berkala meninjau kinerja terhadap target, menganalisis penyebab penyimpangan, dan melakukan tindakan perbaikan untuk mengatasi penyebab utama. Pada waktu yang tepat, melakukan analisis akar penyebab seluruh penyimpangan.

#### ME1.5 Dewan dan Eksekutif Pelaporan (*Board and Executive Reporting*)

Mengembangkan laporan manajemen senior TI kontribusi bisnis, khususnya dalam hal kinerja portofolio perusahaan itu, *IT-enabled* program investasi, dan solusi dan layanan kinerja penyampaian program individu. Termasuk dalam status laporan sejauh mana tujuan yang direncanakan telah dicapai, sumber dianggarkan digunakan, target kinerja yang ditetapkan bertemu dan risiko yang teridentifikasi dimitigasi. Mengantisipasi tinjauan manajemen senior dengan menyarankan tindakan perbaikan untuk penyimpangan yang besar. Memberikan laporan kepada manajemen senior, dan mengumpulkan umpan balik dari tinjauan manajemen.

#### ME1.6 Tindakan Perbaikan (*Remedial Actions*)

Mengidentifikasi dan melakukan tindakan perbaikan berdasarkan pemantauan kinerja, penilaian dan pelaporan. Ini termasuk tindak lanjut dari semua pemantauan, pelaporan dan penilaian melalui:

1. Review, negosiasi dan pembentukan tanggapan manajemen
2. Penugasan tanggung jawab untuk remediasi
3. Pelacakan dari hasil tindakan yang dilakukan

2. ME2 Memantau dan Mengevaluasi Pengendalian Internal (*Monitor and Evaluate Internal Control*)

ME2.1 Pemantauan Kerangka Pengendalian Internal (*Monitoring of Internal Control Framework*)

Terus memantau, patokan dan meningkatkan lingkungan pengendalian TI dan kerangka kontrol untuk memenuhi tujuan organisasi.

ME2.2 Ulasan Pengawas (*Supervisory Review*)

Memantau dan mengevaluasi efisiensi dan efektivitas TI internal ulasan manajerial kontrol.

ME2.3 Kontrol Pengecualian (*Control Exceptions*)

Mengidentifikasi pengecualian kontrol, dan menganalisis dan mengidentifikasi akar penyebab yang mendasarinya. Meningkatkan pengecualian kontrol dan melaporkan kepada *stakeholders* tepat. Lembaga tindakan korektif yang diperlukan.

ME2.4 Pemantauan Penilaian Diri (*Control Self-assessment*)

Mengevaluasi kelengkapan dan efektivitas pengendalian manajemen atas proses TI, kebijakan dan kontrak melalui program berkelanjutan dari penilaian diri.

ME2.5 Jaminan Pengendalian Internal (*Assurance of Internal Control*)

Memperoleh, sesuai kebutuhan, jaminan lebih lanjut dari kelengkapan dan efektivitas pengendalian internal melalui ulasan pihak ketiga.

ME2.6 Pengendalian Internal di Pihak Ketiga (*Internal Control at Third Parties*)

Menilai status kontrol providers'internal layanan eksternal.

Mengkonfirmasi bahwa penyedia layanan eksternal mematuhi persyaratan hukum dan peraturan dan kewajiban kontraktual.

ME2.7 Tindakan Perbaikan (*Remedial Actions*)

Mengidentifikasi, memulai, melacak dan menerapkan tindakan perbaikan yang timbul dari penilaian kontrol dan pelaporan.

3. ME3 Memastikan Kepatuhan Dengan Persyaratan Eksternal (*Ensure Compliance With External Requirements*)

ME3.1 Identifikasi External Hukum, Peraturan dan Kontrak Kepatuhan (*Identification of External Legal, Regulatory and Contractual Compliance Requirements*)

Mengidentifikasi, secara terus menerus, hukum lokal dan internasional, peraturan, dan persyaratan eksternal lain yang harus dipenuhi untuk

dimasukkan ke dalam organisasi TI kebijakan, standar, prosedur dan metodologi.

ME3.2 Optimalisasi Respon untuk Persyaratan Eksternal (*Optimisation of Response to External Requirements*)

Meninjau dan menyesuaikan IT kebijakan, standar, prosedur dan metodologi untuk memastikan bahwa persyaratan hukum, peraturan dan kontrak yang ditangani dan dikomunikasikan.

ME3.3 Evaluasi Kepatuhan Dengan Persyaratan Eksternal (*Evaluation of Compliance With External Requirements*)

Konfirmasi kepatuhan kebijakan IT, standar, prosedur dan metodologi dengan persyaratan hukum dan peraturan.

ME3.4 Jaminan positif Kepatuhan (*Positive Assurance of Compliance*)

Memperoleh dan melaporkan jaminan kepatuhan dan ketaatan terhadap semua kebijakan internal yang berasal dari arahan internal maupun persyaratan hukum, peraturan atau kontrak eksternal.

ME3.5 Pelaporan terpadu (*Integrated Reporting*)

Mengintegrasikan IT melaporkan persyaratan hukum, peraturan dan kontrak dengan output yang sama dari fungsi bisnis lainnya.

4. ME4 Menyediakan IT Governance (*Provide IT Governance*)

ME4.1 Pembentukan Kerangka Kerja IT Governance (*Establishment of an IT Governance Framework*)

Mendefinisikan, membangun dan menyelaraskan kerangka tata kelola TI dengan tata kelola perusahaan dan pengendalian lingkungan secara keseluruhan.

#### ME4.2 Penyelarasan Strategis (*Strategic Alignment*)

Aktifkan papan dan pemahaman eksekutif isu strategis TI, seperti peran IT, wawasan teknologi dan kemampuan. Pastikan bahwa ada pemahaman bersama antara bisnis dan TI mengenai potensi kontribusi TI dengan strategi bisnis.

#### ME4.3 Nilai Pengiriman (*Value Delivery*)

Mengelola *IT-enabled* program investasi dan aset TI lainnya dan layanan untuk memastikan bahwa mereka memberikan nilai terbesar yang mungkin dalam mendukung strategi dan tujuan perusahaan.

#### ME4.4 Pengelolaan Sumber Daya (*Resource Management*)

Mengawasi investasi, penggunaan dan alokasi sumber daya TI melalui penilaian reguler inisiatif TI dan operasi untuk memastikan resourcing yang tepat dan sejalan dengan tujuan strategis saat ini dan masa depan dan imperatif bisnis.

#### ME4.5 Manajemen Resiko (*Risk Management*)

Bekerja dengan papan untuk menentukan selera perusahaan untuk risiko TI, dan memperoleh keyakinan memadai bahwa risiko TI praktik manajemen yang tepat untuk memastikan bahwa risiko TI yang sebenarnya tidak melebihi *risk appetite* dewan.

#### ME4.6 Pengukuran Kinerja (*Performance Measurement*)

Mengkonfirmasi bahwa telah disepakati tujuan TI telah memenuhi atau melampaui, atau bahwa kemajuan menuju tujuan IT memenuhi harapan. Di mana disepakati tujuan telah terjawab atau kemajuan tidak seperti yang diharapkan, tindakan perbaikan manajemen Ulasan ini.

#### ME4.7 Keyakinan Independen (*Independent Assurance*)

Memperoleh keyakinan independen (internal atau eksternal) tentang kesesuaian TI dengan hukum dan peraturan yang relevan; kebijakan organisasi, standar dan prosedur; yang berlaku umum; dan kinerja yang efektif dan efisien dari IT.

### **2.1.7. Tingkat Kematangan (*Maturity Level*)**

COBIT melihat bahwa menerapkan mekanisme *governance* secara efektif tidaklah mudah, namun harus melalui berbagai tahap *maturity* (kematangan) tertentu. Model *maturity* untuk mengontrol proses IT, sehingga manajemen dapat mengetahui dimana posisi organisasi sekarang dan diposisi mana organisasi ingin berada. Tingkat kematangan tersebut memiliki level pengelompokkan kapabilitas perusahaan dalam pengelolaan proses TI dari level nol atau *non-existent* (belum tersedia) hingga ke level lima atau *optimised* (teroptimasi).



Sumber: IT Governance Institute 2007

**Gambar 2.3.** Grafik Tingkat Kematangan

Dengan menggunakan model tingkat kematangan yang dikembangkan untuk masing-masing 34 proses TI cobit, manajemen perusahaan dapat mengidentifikasi:

1. Kinerja aktual perusahaan, dimana posisi perusahaan saat ini.
2. Status industri saat ini, sebagai perbandingan.
3. Target perusahaan untuk perbaikan, apa yang ingin dicapai perusahaan.
4. Jalur pertumbuhan yang diperlukan antara saat ini dan yang akan datang.

**Tabel 2.1.** Tingkat Kematangan (*Maturity Level*)

Level	Penjelasan
-------	------------

<p style="text-align: center;"><b>0</b></p> <p style="text-align: center;"><b>Non existent</b></p> <p style="text-align: center;"><b>(Tidak Ada)</b></p>	<p>Ini merupakan tingkatan paling kecil dimana Tidak terdapat proses terkait sama sekali.</p>
<p style="text-align: center;"><b>1</b></p> <p style="text-align: center;"><b>Initial</b></p> <p style="text-align: center;"><b>(Insialisasi)</b></p>	<p>Tahap dimana manajemen sadar akan pentingnya diperhatikan proses terkait, tetapi implementasi yang terjadi masih bersifat reaktif, sesuai dengan kebutuhan yang mendadak yang ada dan tidak terorganisir.</p>
<p style="text-align: center;"><b>2</b></p> <p style="text-align: center;"><b>Repeatable</b></p> <p style="text-align: center;"><b>(Dapat Diulang)</b></p>	<p>Tahap dimana manajemen telah memiliki pola untuk mengelola proses terkait berdasarkan pengalaman yang berulang yang pernah dilakukan sebelum-sebelumnya. Namun, pola tersebut belum terstandarisasi. Kurangnya prosedur yang tidak terstandarisasi dan tidak dikomunikasikan dan juga keterbatasan staf ahli menyebabkan masih terjadinya penyimpangan.</p>
<p style="text-align: center;"><b>3</b></p> <p style="text-align: center;"><b>Defined</b></p> <p style="text-align: center;"><b>(Ditetapkan)</b></p>	<p>Tahap dimana manajemen telah berhasil menciptakan dan mengkomunikasikan standar baku pengelolaan proses terkait walaupun belum dilakukan secara terintegrasi.</p>

<p style="text-align: center;"><b>4</b></p> <p style="text-align: center;"><b>Managed (Diatur)</b></p>	<p>Tahap dimana kegiatan dan standar yang ada telah diterapkan secara formal dan terintegrasi. Serta terdapat pula indikator sebagai pengukur kemajuan kinerja secara kuantitatif bagi pihak manajemen.</p>
<p style="text-align: center;"><b>5</b></p> <p style="text-align: center;"><b>Optimised (Dioptimalisasi)</b></p>	<p>Tahap dimana manajemen telah berkomitmen terhadap proses yang ada agar dapat menjadi sebuah <i>best practice</i> yang selalu dikembangkan.</p>

Sumber: Sarno 2009

## 2.2. Sejarah Singkat Perusahaan

### 2.2.1. Sejarah Singkat Badan Pengusahaan Batam

Otorita Batam merupakan cikal bakal dari Badan Pengusahaan Batam (BP Batam). Pada PP 46 disebutkan bahwa Otorita Pengembangan Daerah Industri Pulau Batam berubah menjadi Badan Pengusahaan Kawasan Batam dengan keberadaannya selama 70 tahun sejak PP 46 ditandatangani.

Hal ini memberikan kepastian hukum kepada para investor baik lokal maupun asing selama itu untuk berinvestasi di Batam. BP Batam mempunyai Visi dan Misi yang jelas untuk mengembangkan Batam kedepan.

Saat ini BP Batam mendapatkan kewenangan dari pemerintah pusat khususnya yang menjadi kewenangan Departemen Perdagangan untuk mengeluarkan perijinan lalu lintas keluar masuk barang. Perijinan tersebut diantaranya Perijinan IP Plastik dan Scrap Plastik, Perijinan IT-PT, Perijinan IT Cakram, Perijinan IT Alat Pertanian, Perijinan IT Garam Perijinan, Mesin Fotocopy dan printer berwarna, Perijinan Pemasukan Barang Modal Bukan Baru, Perijinan Bongkar Muat, Pelabuhan Khusus, Perijinan Pelepasan Kapal Laut



**Gambar 2.4.** Gedung Badan Pengusahaan Batam

Adapun perijinan yang sebelumnya berada di Otorita Batam diantaranya Perijinan Fatwa Planologi, Perijinan Alokasi Lahan, Perijinan titik-titik lokasi iklan, SK BKPM tentang registrasi perusahaan di Indonesia, Angka Pengenal Import Terbatas (APIT), serta Izin Usaha Tetap (IUT).

### **2.2.2. Visi dan Misi**

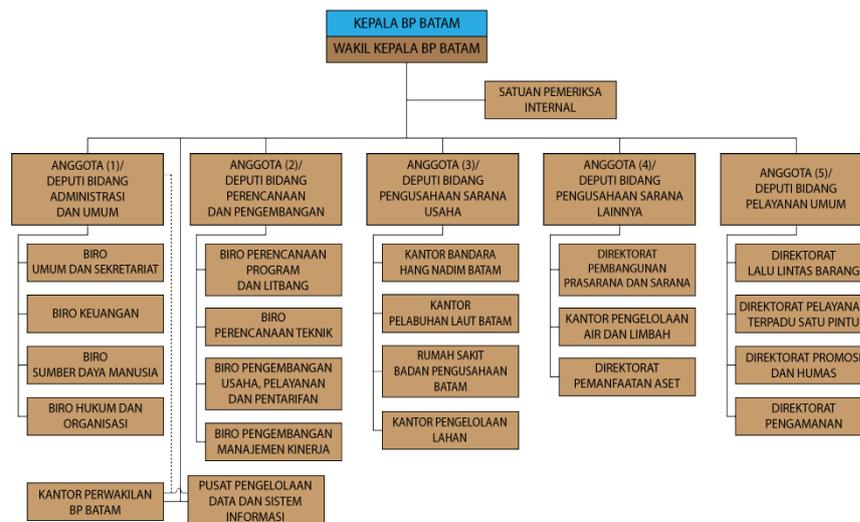
#### **Visi**

Menjadikan Kawasan Batam sebagai Kawasan Ekonomi terkemuka Asia Pasifik dan kontributor utama pembangunan Ekonomi Nasional.

## Misi

1. Mewujudkan Pulau Batam Sebagai Daerah Industri Hijau Berorientasi Ekspor.
2. Mewujudkan Pulau Batam Menjadi Kawasan Wisata Bahari Unggul dan Transshipment Perdagangan International.

### 2.2.3. Struktur Organisasi



Sesuai dengan:

- Peraturan Kepala Badan Pengusahaan Kawasan Perdagangan Bebas dan Pelabuhan Bebas Batam Nomor 5 Tahun 2015 tentang Susunan Organisasi dan Tata Kerja Unit Kerja di bawah Anggota/ Deputi di Lingkungan Badan Pengusahaan Kawasan Perdagangan Bebas dan Pelabuhan Bebas Batam
- Keputusan Kepala Badan Pengusahaan Kawasan Perdagangan Bebas dan Pelabuhan Bebas Batam Nomor 23 Tahun 2015 tanggal 5 Mei 2015
- Surat Perintah Kepala Badan Pengusahaan Kawasan Perdagangan Bebas dan Pelabuhan Bebas Batam Nomor 40/KA/5/2015 tanggal 5 Mei 2015

Sumber: *Website* Badan Pengusahaan Batam 2016

**Gambar 2.5.** Struktur Organisasi Badan Pengusahaan Batam

### **2.3. Penelitian Terdahulu**

Dalam penelitian ini penulis memaparkan beberapa penelitian terdahulu yang relevan dengan permasalahan yang akan diteliti diantaranya:

**Tabel 2.2.** Penelitian Terdahulu

No	Penulis	Judul	Metode	Hasil
1.	Agus Prasetyo Utomo dan Novita Mariana (2011).	Analisis Tata Kelola Teknologi Informasi ( <i>It Governance</i> ) Pada Bidang Akademik Dengan COBIT Frame Work Studi Kasus Pada Univeritas Stikubank Semarang.  (ISSN 0854-9524, Volume 16 Nomor 2)	COBIT  FrameWork  4.0	<p>1. Dari hasil penelitian didapatkan bahwa Lembaga UNISBANK memiliki pengelolaan TI dalam mendukung layanan akademik dan dirasakan perlu dilakukan perbaikan terhadap beberapa <i>control process</i> yang dirasakan sangat penting menurut lembaga yang terkait saat ini.</p> <p>2. Penentuan <i>control process</i> melatih dan mendidik <i>users</i>, mengelola data dari domain <i>delivery and support</i>, me-monitor dan evaluasi kinerja TI dari domain <i>monitor and evaluate</i> merupakan <i>control process</i> yang penting untuk diperbaiki.</p>

				3. Dalam pembuatan rekomendasi <i>IT Governance</i> dilakukan berdasarkan posisi <i>maturity</i> masing-masing <i>control process</i> tersebut.
2.	Ade Andri Hendriadi, M. Jajuli, Kun Siwi T (2012).	Pengukuran Kinerja Sistem Informasi Akademik Dengan Menggunakan Kerangka Kerja COBIT 4.1 Pada Domain <i>Plan And Organise</i> Di Universitas Singaperbangsa Karawang.  (ISSN 1412-86676, Volume 10 Nomor 22)	COBIT 4.1	1. Tata Kelola TI sistem informasi akademik pada Universitas Singaperbangsa Karawang sudah dilakukan walaupun masih belum berjalan secara optimal karena belum mencapai pada tingkat kematangan yang diharapkan.  2. Tingkat kematangan ( <i>maturity level</i> ) yang ada pada setiap proses TI yang terdapat dalam domain <i>Plan and Organise</i> (PO) rata-rata pada level 2,446 dan masih berada pada level 2 ( <i>repeatable but intuitive</i> ).  3. Proses tata kelola TI di UNSIKA telah memiliki

				<p>pola yang berulang kali dilakukan dalam melakukan manajemen aktivitas terkait dengan tata kelola TI, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidakkonsistenan.</p>
3.	<p>Indri Sudanawati Rozas, Danar Ayu Ristyantie Effendy (2012)</p>	<p>Mengukur Efektivitas Hasil Audit Teknologi Informasi COBIT 4.1 Berdasarkan Perspektif End User.  (ISSN 1858-4667, Volume 17 Nomor 2)</p>	COBIT 4.1	<ol style="list-style-type: none"> <li>1. Perspektif end user tidak mempengaruhi hasil pengukuran audit TI secara signifikan.</li> <li>2. Hasil audit I dengan jumlah responden yang hanya 2 orang (DSTI dan Wakil Rektor I) tidak berbeda nyata dengan hasil audit dengan jumlah responden 26 (end user).</li> <li>3. Penentuan responden berdasarkan pada RACI Chart yang ada didalam COBIT 4.1 telah dibuat sesuai dengan kebutuhan audit.</li> </ol>

				4. Keterlibatan end user dalam proses audit teknologi informasi tidak signifikan.
4.	Juliandarini dan Sri Handayaningsih (2013).	Audit Sistem Informasi Pada Digilib Universitas XYZ Menggunakan Kerangka Kerja COBIT 4.0.  (ISSN 2338-5197, Volume 1 Nomor 1)	COBIT 4.0	<p>1. Hasil audit pada proses pengelolaan kinerja dan kapasitas atau manage performance and capability (DS3) menunjukkan tingkat kematangan DIGILIB untuk saat ini (<i>as is</i>) berada pada tingkat dua (2) yakni berulang secara intuitif/repetable. Sedangkan tingkat kematangan pada masa depan (<i>to be</i>) DIGILIB untuk proses DS3 menunjukkan tingkat kematangan tiga (3) yakni proses terdefinisi/defined.</p> <p>2. Hasil audit pada proses pengelolaan data atau manage data (DS11) menunjukkan tingkat</p>

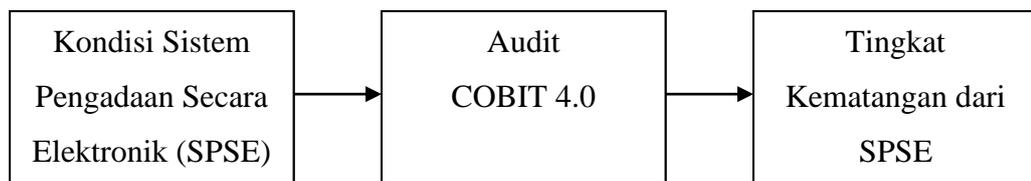
				<p>kematangan satu (1) yakni berada pada tingkat awal/initial untuk sistem informasi DIGILIB saat ini (<i>as is</i>). Sedangkan tingkat kematangan yang diharapkan untuk proses DS11 adalah tingkat tiga (3) yakni proses terdefinisi/<i>defined</i>.</p> <p>3. Rekomendasi berdasarkan laporan hasil audit, usulan perbaikan berdasarkan tingkat kematangan dan model tata kelola baru yang sudah teruji diharapkan mampu untuk memberikan solusi dalam penanganan pengelolaan kinerja dan kapabilitas serta penanganan masalah pengelolaan data pada sistem informasi DIGILIB milik perpustakaan Universitas XYZ.</p>
--	--	--	--	---

5.	Dewi Ciptaningrum, Eko Nugroho, Dani Adhipta (2015)	Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5. (ISSN 2089-9815)	COBIT 5	<ol style="list-style-type: none"> <li>1. Hasil dari lima (5) proses tingkat kapabilitas keamanan SI, semua proses berada pada tingkat kapabilitas 1 Performed Process.</li> <li>2. Hasil penilaian tingkat kapabilitas keamanan SI tidak dapat mencapai level yang ditargetkan dalam jangka pendek yaitu level 3.</li> <li>3. Untuk meningkatkan tingkat kapabilitas keamanan SI agar mencapai level yang ditargetkan, Bagian TIT Setda Kota Yogyakarta harus melakukan serangkaian praktik dasar perbaikan proses dan menghasilkan serangkaian produk kerja pada level 1 kinerja proses (performed process).</li> </ol>
----	--	--	---------	---

## 2.4. Kerangka Berpikir

Kerangka berfikir merupakan model konseptual tentang bagaimana teori berhubungan dengan berbagai faktor yang telah diidentifikasi sebagai masalah yang penting (Sugiyono, 2009:60).

Adapun kerangka berpikir pada penelitian ini adalah:



**Gambar 2.4.** Kerangka Berpikir

## 2.5. Hipotesis

Menurut Sugiyono (2009: 64) hipotesis merupakan jawaban sementara terhadap rumusan masalah penelitian, di mana rumusan masalah penelitian telah dinyatakan dalam bentuk kalimat pertanyaan. Dikatakan sementara, karena

jawaban yang diberikan baru didasarkan pada teori yang relevan, belum didasarkan pada fakta-fakta empiris yang diperoleh melalui pengumpulan data.

Adapun hipotesis dalam penelitian ini yaitu:

1. *Monitoring Approach* dipersepsikan sangat perlu pada Badan perusahaan Batam.
2. *Definition and Collection of Monitoring Data* dipersepsikan sangat perlu pada Badan perusahaan Batam.
3. *Monitoring Method* dipersepsikan sangat perlu pada Badan perusahaan Batam.
4. *Performance Assesment* dipersepsikan sangat perlu pada Badan perusahaan Batam.
5. *Board and Executive Reporting* dipersepsikan sangat perlu pada Badan perusahaan Batam.
6. *Remedial Actions* dipersepsikan sangat perlu pada Badan perusahaan Batam.