TATA KELOLA TEKNOLOGI INFORMASI

Berkembangnya teknologi dan bisnis membuktikan bahwa tata kelola teknologi informasi mempunyai peranan penting dalam mencapai tujuan organisasi. Tata kelola Teknologi Informasi (TI) merupakan dasar dalam membangun struktur yang dapat menyelaraskan proses TI dengan tujuan bisnis atau tujuan organisasi. Dengan adanya tata kelola TI, perusahaan dapat memastikan bahwa manajemen organisasi dapat terlaksana dan bahkan dapat dievaluasi ke arah yang lebih baik. Buku ini membahas konsep tata kelola TI secara mendalam yaitu bagaimana tata kelola TI pertama kali dikenal, mengapa ia penting hingga kepada proses tata kelola mulai dari perencanaan, pengelolaan dan pelaksanaan tata kelola TI di level organisasi atau korporat yang dapat membantu dalam menyelaraskan tujuan bisnis dengan strategi TI yang dibangun.

Rahmani

PT Cahaya Rahmat Rahmani
JL Kemuning Baru Komplek Ar Rahman
CahayaRahmatRahmani@gmail.com

ISBN 978-623-88417-8-3
9 786238 841783

ANINDA MULIANA, M.Kom TATA KELOLA TEKNOLOGI INFORMASI

TATA KELOLA TEKNOLOGI INFORMASI

Aninda Muliani, M.Kom

Tata Kelola Teknologi Informasi

Tata Kelola Teknologi Informasi

Aninda Muliani, M.Kom

PT. Cahaya Rahmat Rahmani

Tata Kelola Teknologi Informasi

Penulis :

Aninda Muliani, M.Kom

ISBN : 978-623-88417-8-3

IKAPI : 064/SUT/2022

Tata Letak dan Desain Sampul:
CRR

Redaksi :
Jl. Kemuning Baru, Blok B, No. 38
Percut Sei Tuan 20371
Tel +6282164198713
Email : cahayarahmatrahmani@gmail.com

Penerbit :
PT Cahaya Rahmat Rahmani
Jl. Kemuning Baru, Blok B, No. 38
Percut Sei Tuan 20371
Tel +6282164198713
Email : cahayarahmatrahmani@gmail.com
Web : https://www.cahayarahmatrahmani.store

Cetakan Pertama, Mei 2023

KATA PENGANTAR

Puji dan syukur kepada Allah SWT yang telah memberikan kekuatan akal dan fisik untuk dapat menuangkan ide dan pemikiran sehingga buku ini dapat terselesaikan. Kemudian shalawat dan salam juga kita haturkan kepada Nabi Muhammad SAW sebagai contoh tauladan terbaik yang membukakan jalan kebenaran bagi seluruh alam. Penulis mengucapkan terima kasih kepada suami, anak-anak, para pimpinan, dan teman sejawat atas perhatian dan dukungannya dalam penyelesaian buku ini,

Berkembangnya teknologi dan bisnis membuktikan bahwa tata kelola teknologi informasi mempunyai peranan penting dalam mencapai tujuan organisasi. Tata kelola TI merupakan dasar dalam membangun struktur yang dapat menyelaraskan proses TI dengan tujuan bisnis ataupun tujuan organisasi. Dengan adanya tata kelola TI, perusahaan dapat memastikan bahwa manajemen organisasi dapat terlaksana dan bahkan dapat dievaluasi ke arah yang lebih baik.

Buku ini membahas konsep tata kelola TI secara mendalam yaitu bagaimana tata kelola TI pertama kali dikenal, mengapa ia penting hingga kepada proses tata kelola dimulai dari perencanaan, pengelolaan dan pelaksanaan tata kelola TI di level organisasi atau korporat yang dapat membantu dalam menyelaraskan tujuan bisnis dengan strategi TI yang dibangun.

Penulis menyadari bahwa masih banyak kekurangan dan keterbatasan pada buku ini. Penulis sangat menerima masukan dan saran dari para pembaca untuk perbaikan buku ini pada edisi berikutnya. Semoga buku ini dapat membantu dalam memahami tentang tata kelola TI serta berkontribusi dalam mendukung tercapainya tujuan dari proses belajar mengajar pada mata kuliah tata kelola TI.

Wassalam.

Medan, Maret 2023

Aninda Muliani M.Kom

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
KONSEP TATA KELOLA TEKNOLOGI INFORMASI

1.1 Pentingnya Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi (TI) adalah konsep yang hampir tidak dikenal puluhan tahun lalu. Istilah tata kelola pada awalnya hanya merujuk pada tata kelola perusahaan atau lebih dikenal dengan istilah *corporate governance* yang dirancang agar pengelolaan perusahaan dapat berjalan secara profesional dan sesuai dengan dengan harapan para pemilik kepentingan perusahaan. Fungsi teknologi informasi di perusahaan dianggap hanya sebagai fungsi pendukung yang sangat penting tetapi bukan sebagai kegiatan bisnis yang utama.

Pemikiran tentang tata kelola perusahaan benar-benar berubah setelah terjadinya sebuah peristiwa yang sangat mengguncang perekonomian Amerika Serikat pada awal abad ke-20, tepatnya di tahun 2002. Adalah perusahaan Enron, salah satu perusahaan energi terbesar di Amerika Serikat, yang tiba-tiba saja mengalami kebangkrutan tidak terduga pada saat aktivitas bisnis perusahaan tampak berjalan normal. Hal ini tentu saja mengejutkan semua pihak, terutama di kalangan investor, serta menimbulkan pertanyaan mengapa hal tersebut dapat terjadi. Skandal serupa ternyata tidak hanya dialami oleh satu perusahaan, tetapi juga disusul oleh perusahaan besar lainnya seperti Tyco International yang bergerak di bidang keamanan dan WorldCom di bidang telekomunikasi, serta nama lain seperti Adelphia dan Pregerian Systems. Skandal-skandal tersebut menyebabkan kerugian trilyunan dolar bagi investor karena runtuhnya harga saham perusahaan dan mengguncang kepercayaan masyarakat terhadap pasar saham nasional. Hal ini memaksa pemerintah Amerika Serikat menyelidiki dan menemukan fakta bahwa banyak tata kelola perusahaan dan praktik keuangan yang curang. Sebagai tanggapan terhadap sejumlah skandal akuntansi perusahaan besar tersebut, dibentuklah dewan yang membahas masalah ini. Maka

pada tanggal 30 Juli 2002, dihasilkan sebuah hukum federal Amerika Serikat bernama **Sarbanes-Oxley Act** atau sering disingkat dengan **SOx** atau **Sarbox**. Akta ini diberi nama dua orang pencetusnya, yaitu Senator Paul Sarbanes dan Anggota Dewan Michael G. Oaxley dan kemudian disahkan oleh Presiden George W. Bush.

Undang-undang Sarbox menetapkan suatu standar baru dan lebih baik bagi semua dewan dan manajemen perusahaan serta akuntan publik. Akta ini terdiri dari 11 judul atau bagian yang menetapkan hal-hal seperti tanggung jawab tambahan dewan perusahaan hingga hukuman pidana serta menuntut Badan Sekuritas dan Bursa Amerika Serikat untuk menerapkan aturan persyaratan baru untuk menaati hukum ini.

Peraturan perundang-undangan ini telah memberikan dampak yang besar pada pelaporan keuangan dan praktik tata kelola perusahaan, awalnya di Amerika Serikat dan kemudian di seluruh dunia. Tata kelola perusahaan yang baik, menurut (Daniri Achmad, 2022), dapat meningkatkan legitimasi perusahaan yang dikelola dengan transparan, adil, dan dapat dipertanggungjawabkan. Transparansi dapat diterapkan dengan mawujudkan tata kelola TI karena tata kelola TI merupakan salah satu pilar utama dari tata kelola perusahaan yang baik (*good corporate governance*).

1.2 Perkembangan Tata Kelola Teknologi Informasi

Aplikasi komputer dan teknologi informasi pertama meledak ke dunia bisnis terutama di Amerika Serikat dan Eropa mulai pada awal 1960-an. Banyak perusahaan menawarkan produk perangkat keras dan perangkat lunak komputer. Semua perusahaan ingin mempercepat proses bisnisnya dengan memanfaatkan teknologi baru, kemudian investasi besar-besaran dilakukan dalam memasang sistem baru, mempekerjakan dan melatih pemrogram dan analis untuk membangun dan meluncurkannya. Meskipun beberapa kegagalan di sepanjang jalan, kita semua menggunakan

dan mendapat manfaat hari ini dari perkembangan produk perangkat keras dan perangkat lunak computer tersebut.

Saat ini, sistem TI yang didukung oleh teknologi yang terus berubah dan meningkat adalah komponen utama dari hampir semua kegiatan bisnis. Namun, aktivitas TI tampaknya belum didukung oleh beberapa standar dan prosedur yang sama di semua perusahaan. Misalnya, sistem akuntansi dan standar keuangan didukung oleh pengakuan prinsip akuntansi yang ditelaah oleh auditor independen dan diikuti aturan akuntansi keuangan pemerintah, seperti pada Bada Sekuritas dan Bursa Amerika Serikat. Terdapat aturan dan standar praktik terbaik hampir pada setiap bidang bisnis, seperti dalam banyak aspek pemasaran dan pengendalian mutu. Ini tidak berlaku untuk sistem dan proses TI. Terlepas dari kenyataan bahwa operasi TI menghadapi peningkatan persyaratan kepatuhan pemerintah dan profesional dan menghadapi berbagai risiko terkait sistem, ada kebutuhan akan praktik berkelanjutan untuk tata kelola TI yang lebih baik.

Pada sub-bab sebelumnya telah dijelaskan bahwa perundang-undangan Sarbox membawa dampak yang sangat besar terhadap praktek tata kelola perusahaan. Undang-undang ini dibuat untuk meningkatkan transparansi perusahaan seperti proses pelaporan dan audit keuangan. Meskipun aturan audit dan pengendalian internal SOx telah mengubah banyak auditor eksternal dan tata cara praktik keuangannya, Sox juga mempunyai dampak yang besar terhadap tata kelola TI perusahaan terutama pada Section 404. SOx memperkenalkan serangkaian proses yang benar-benar berubah untuk audit eksternal dan memberikan tanggung jawab tata kelola baru kepada eksekutif senior dan anggota dewan. SOx juga mendirikan Dewan Pengawas Akuntansi Perusahaan Publik (PCAOB), yaitu semacam badan pemeriksa keuangan, dan juga sebuah pengawas otoritas di bawah Badan Sekuritas dan Bursa (SEC) yang menerbitkan standard audit keuangan dan memantau tata kelola auditor eksternal. Aturan administratif telah dikembangkan oleh SEC berdasarkan undang-undang SOx.

1.3 Pengertian Tata Kelola TI

"Governance" merupakan turunan dari kata "government", yang artinya membuat kebijakan (*policies*) yang sejalan/selaras dengan keinginan/aspirasi masyarakat atau kontituen (Handler & Lobba, 2005). Sedangkan penggunaan pengertian "governance" terhadap Teknologi Informasi (IT Governance) maksudnya adalah, penerapan kebijakan TI di dalam organisasi agar pemakaian TI (berikut pengadaan dan pelayanannya) diarahkan sesuai dengan tujuan organisasi tersebut.

Menurut Sambamurthy and Zmud (1999), IT Governance dimaksudkan sebagai pola dari otoritas/kebijakan terhadap aktivitas TI (IT Process). Pola ini diantaranya adalah membangun kebijakan dan pengelolaan IT Infrastructure, penggunaan TI oleh end-user secara efisien, efektif dan aman, serta proses IT Project Management yang efektif.

Standar COBIT dari lembaga ISACA di Amerika Serikat mendefinisikan IT Governance "*as a structure of relationships and processes to direct and control the enterprise in order to achieve the entreprise's goals by value while balancing risk versus return over IT and its processes"*.

Sedangkan Oltsik (2003) mendefinisikan IT Governance sebagai kumpulan kebijakan, proses/aktivitas dan prosedur untuk mendukung pengoperasian TI agar hasilnya sejalan dengan strategi bisnis (strategi organisasi). Ruang lingkup IT Governance di perusahaan skala besar biasanya mencakup hal-hal yang berkaitan dengan Change Management, Problem Management, Release Management, Availability Management dan bahkan Service-Level Management.

Lebih lanjut Oltsik mengatakan bahwa IT Governance yang baik harus berkualitas, well-defined dan bersifat "*repeatable processes*" yang terukur (metric). IT Governance yang dikembangkan dalam suatu organisasi modern berfungsi pula mendefinisikan (outline) kebijakan-kebijakan TI, menetapkan prosedur penting IT Process, dokumentasi aktivitas TI, termasuk

membangun IT Plan yang efektif berdasarkan perubahan lingkungan perusahaan dan perkembangan TI.

Tata kelola TI merupakan bagian yang tidak terpisahkan dari tata kelola perusahaan, atau biasa kita sebut good governance. Teknologi informasi (TI) merupakan faktor kunci keberhasilan di era ekonomi informasi ini. TI sudah menjadi bagian sentral dari banyak proses bisnis, terutama di bidang manajemen keuangan. Artinya tata kelola perusahaan (*enterprise governance*) dan tata kelola TI (IT *governance*) tidak lagi dianggap sebagai dua hal yang terpisah.

Tata kelola TI menyediakan struktur dasar yang menghubungkan dan menyelaraskan proses TI, sumber daya TI, dan informasi yang dibutuhkan oleh bisnis untuk menjalankan strateginya guna mencapai tujuannya. Tata kelola TI mengintegrasikan dan mengoptimalkan metode perencanaan, pengorganisasian, penerapan akuisisi dan penyebaran, pengiriman dan dukungan, serta pemantauan dan evaluasi kinerja TI. Penting untuk diketahui bahwa tata kelola TI merupakan bagian integral dari penerapan tata kelola perusahaan yang berhasil dengan memastikan peningkatan yang terukur dalam kinerja dan efisiensi proses bisnis.

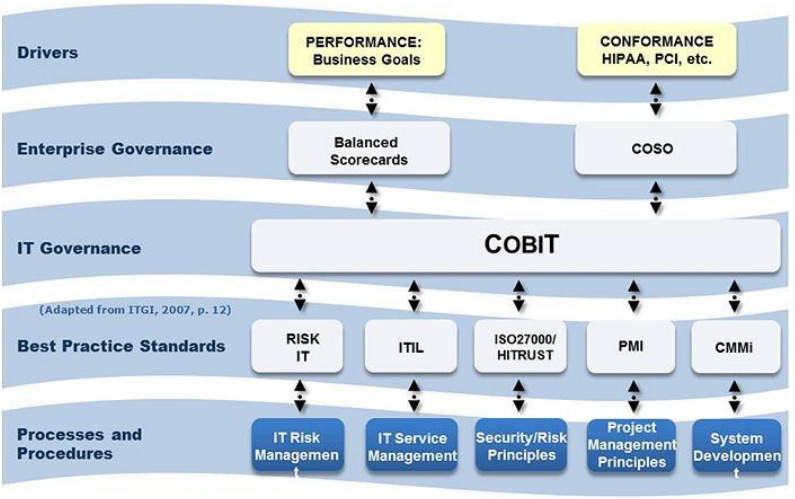
Adapun pengertian tata kelola TI yang dinyatakan oleh IT Goverment Insitute (2003) adalah sebagai berikut: *"IT Governance is the resposibility of the board of directors and executive management. IT is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."* Dari interpretasi pernyataan tersebut, dijelaskan bahwa tata kelola TI merupakan tanggung jawab manajemen senior dan manajemen senior suatu perusahaan. Tata kelola TI ini merupakan bagian dari tata kelola perusahaan yang mencakup kepemimpinan, struktur organisasi, dan proses untuk memastikan keberlanjutan organisasi TI serta mengembangkan strategi dan tujuan organisasi.

Dari beberapa definisi Tata Kelola TI tersebut, maka kita simpulkan bahwa tujuan dibangunnya IT Governance intinya adalah, menyelaraskan IT Resources yang sudah diinvestasikan jutaan dollar tersebut dengan strategi organisasi (agar menjadi *enabler*).

Konsep Information of Technology (IT) governance adalah cara mengelola penggunaan teknologi informasi di sebuah organisasi. IT Governance menggabungkan good practices dari perencanaan dan pengorganisasian, pembangunan dan pengimplementasian, delivery dan support, serta memonitor kinerja system informasi untuk memastikan kalua informasi dan teknologi yang berhubungan mendukung tujuan dan misi organisasi. Salah satu cara mengetahui hal tersebut adalah dengan melakukan proses audit terhadap sistem tersebut.

Audit dilakukan dengan tujuan untuk menetapkan kondisi saat ini, mencari kekurangan-kekurangan dan merekomendasikan perbaikan agar sistem informasi lebih berguna dalam mendukung organisasi. Audit Sistem Informasi dapat dilakukan perusahaan untuk mengevaluasi/audit sistem yang telah ada juka terdapat kekurangan terhadap sistem yang ada.

Oleh karena itu, dengan adanya IT Govenance (Tata Kelola TI yang baik) yang berjalan di dalam suatu organisasi perusahaan tersebut, maka puluhan IT *processes* (IT *activities*) yang dijalankan dapat berjalan secara sistematis, terkendali dan efektif. Bahkan pada menciptakan efisiensi dengan sendirinya mengurangi biaya operasional dan meningkatkan daya saing. Output dan outcome dari IT Governance yang baik tersebut hanya dapat dicapai jika tata kelola tersebut dikembangkan dengan menggunakan IT Framework berstandar internasional, misalnya dengan mengimplementasikan COBIT, IT-IL Management, COSO, ISO IT Security dan sebagainya.

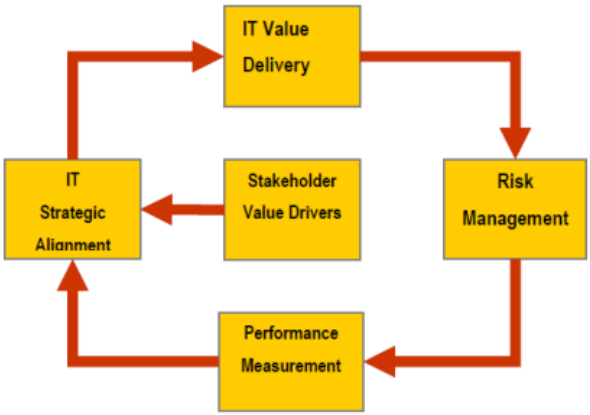


Gambar 1.1 Beberapa framework IT Governance

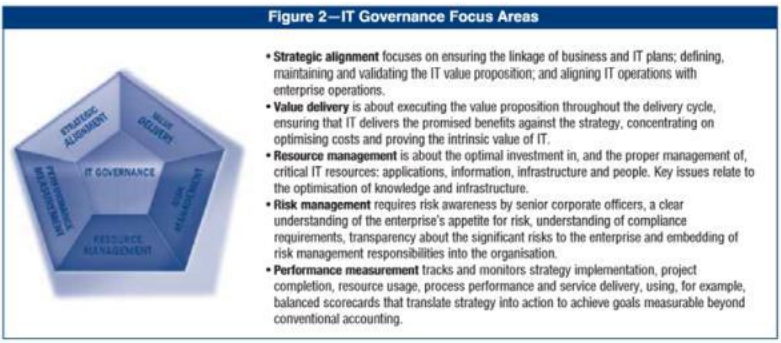
(Sumber: www.itgi.org)

1.4 Fokus Area Tata Kelola TI

Fokus area tata kelola TI adalah bagaimana menyelaraskan tujuan bisnis dengan menggunakan TI sehingga tujuan bisnis dapat dicapai dengan mudah dan investasi yang dikeluarkan dalam penggunaan TI secara konsisten dapat kembali menjadi modal bagi organisasi. Penggunaan IT tentunya harus dilakukan dalam suatu administrasi dimana penggunaan IT tidak akan sia-sia. Fokus area tata kelola teknologi informasi dibagi menjadi 5 bagian, yaitu *strategic alignment, value delivery, resource management, risk management, dan performance measurement.*



Gambar 1.2 Fokus Area Tata Kelola TI



Gambar 1.3 Fokus Area IT Governance menurut ITGI

(Sumber: www.itgi.org)

Menurut IT Governance Institute (ITGI) bahwa tata kelola TI terdapat lima area yang menjadi fokus perhatian, yaitu :

• Keselarasan strategi (*strategic alignment*)

Penerapan TI harus benar-benar mendukung pencapaian misi perusahaan dimana strategi TI harus selaras dengan strategi bisnis organisasi/perusahaan. Memastikan keterkaitan antara bisnis dengan ketentuan rencana teknologi informasi, pemeliharaan, serta validasi usulan nilai teknologi informasi, dan menyelaraskan tujuan

bisnis dan tujuan teknologi teknologi. Pada area ini organisasi dituntut untuk menyelaraskan tujuan dari organisasi dengan implementasi penggunaan TI. Secara tidak langsung penyelarasan antara tujuan organisasi dengan penggunaan TI harus sesuai dengan strategi yang akan diterapkan oleh manajemen eksekutif maupun direksi pada perusahaan.

• Penyampaian nilai (*value delivery*)

Penerapan TI harus dapat memberikan nilai tambah bagi pencapaian misi organisasi. Menjalankan proposisi nilai seluruh siklus delivery, memastikan bahwa teknologi informasi memberikan manfaat sesuai dengan tujuan bisnis yang dituangkan dalam strategi, berkonsentrasi pada biaya mengoptimalkan dan membuktikan nilai intrinsik dari teknologi informasi. Pada organisasi pengguna TI tidak lagi berfokus tentang bagaimana penggunaan TI dapat selaras dengan tujuan organisasi, melainkan bagaimana TI yang telah dipilih dan disesuaikan dengan tujuan organisasi dapat berjalan sealaras tujuan bisnis dan penggunaan TI.

• Manajemen resiko (*risk management*)

Penerapan TI harus disertai dengan identifikasi resiko-resiko TI, sehingga dampaknya dapat ditangani. Tentang kesadaran mengelola risiko oleh pejabat senior pada perusahaan, bagaimana memahami persyaratan kepatuhan, keterbukaan tentang risiko yang signifikan terhadap perusahaan dan menanamkan tanggung jawab manajemen risiko ke dalam organisasi. Risk management merupakan tahapan dimana perusahaan atau organisasi dapat memperhitungkan tingkatan dari sebuah resiko yang terjadi maupun akan terjadi dari penggunaan TI pada proses bisnis.

Risiko akan suatu kejadian tidak dapat dihilangkan melainkan dapat diminimalisir sehingga risiko yang semula dapat menjadi suatu ancaman dapat ditekan dampaknya bahkan dapat menjadi suatu manfaat bagi organisasi. Pada manajemen risiko penilaian awal terhadap risiko yang ada sangatlah penting. Penilaian ini dilakukan guna menentukan seberapa besar risiko yang ada sehingga pada tahapan selanjutnya dapat ditentukan

metode atau cara apa yang tepat untuk melakukan penanganan terhadap risiko yang terjadi atau akan terjadi. Selain itu manajemen risiko juga menjadi suatu acuan terhadap penanganan risiko yang lebih terstruktur sehingga ketika suatu organisasi mengalami suatu kejadian dapat ditangani dengan tahapan atau proses yang telah ditentukan sehingga pencarian terhadap solusi dapat mudah ditentukan serta diaplikasikan.

• Manajemen sumberdaya (*resource management*)

Penerapan TI harus didukung oleh sumberdaya yang memadai dan penggunaan sumberdaya sedapat mungkin dilakukan secara optimal. Tentang investasi yang optimal dalam pengelolaan sumber daya teknologi informasi (aplikasi, informasi, infrastruktur, SDM, dan pengoptimalisasian infrastruktur). Resource management menekankan bagaimana memanfaatkan sumber daya yang ada dapat bermanfaat dalam proses pelaksanaan bisnis dengan memanfaatkan TI mulai dari software, hardware, brainware (pengguna) sehingga seluruh aspek tersebut dapat berjalan sesuai dengan semestinya.

Selain itu perhitungan biaya dalam penggunaan TI masuk ke dalam aspek ini sehingga berapa biaya yang ditentukan, seberapa efektif (terkait biaya) hingga kapan investasi terhadap TI akan kembali menjadi modal dapat diperhitungkan.

• Pengukuran kinerja (*performance measurement*)

Penerapan TI harus diukur dan dievaluasi secara berkala untuk memastikan bahwa kinerja dan kapasitas TI sesuai dengan kebutuhan bisnis.

Pengukuran kinerja dan track implementasi strategi, penyelesaian proyek, penggunaan sumber daya, kinerja proses, dan pelayanan, misalnya balanced scorecard yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan yang terukur.

1.5 Proses Tata Kelola TI

Proses IT Governance dimulai dengan menentukan sasaran untuk IT perusahaan, menyediakan petunjuk awal. Setelah itu, perulangan secara berkelanjutan dibentuk; kinerja diukur dan dibandingkan dengan sasaran awal, menghasilkan arahan Kembali dari aktivitas yang diperlukan dan perubahan sasaran yang sesuai. Ketika sasaran menjadi tanggung jawab utama dan ukuran kinerja manajemen, itu jelas harus dikembangkan dengan perencanaan yang baik sehingga sasaran dapat terjangkau dan ukuran menggambarkan sasaran dengan tepat

Ketidakefetifan IT Governance memungkikan penyebab dari pengalaman negative perusahaan dalam pemanfaatan IT, antara lain :

a) Kerugian bisnis, kerusakan reputasi atau posisi kompetitif yang menurun/lemah.

b) Batas waktu tidak tercapai, biaya lebih tinggi dibandingkan harapan yang diinginkan

c) Efisiensi dan proses perusahaan memberi dampak negatif terhadap kualitas penggunaan IT.

d) Kegagalan inisiatif IT dapat membawa inovasi dan manfaat yang dijanjikan.

Menurut Fox dan Zonneveld, menyimpulkan dalam tatakelola yang baik, peranan IT Governance

merupakan hal yang sangat penting, dalam konteks organisasi bisnis yang berkembang kebutuhan akan IT bukan merupakan barang yang langka.

1.6 Tujuan Tata Kelola TI

IT Governance bertujuan untuk mengarahkan IT dan memastikan pencapaian kinerja sesuai dengan tujuan yang diinginkan, antara lain:

a) IT menjadi searah dengan perusahaan dan manfaat yang dijanjikan dapat terealisasi

b) IT memungkinkan perusahaan memanfaatkan peluang dan memaksimalkan keuntungan.

c) Sumber daya IT digunakan secara bertanggung jawab

d) IT berkaitan erat dengan resiko yang harus diatur dengan baik.

1.7 Tata Kelola yang Baik (*Good Governance*)

Kunci utama memahami good governance adalah pemahaman atas prinsip-prinsip di dalamnya. Bertolak dari prinsip-prinsip ini akan didapatkan tolak ukur kinerja suatu pemerintahan. Baik-buruknya pemerintahan bisa dinilai bila ia telah bersinggungan dengan semua unsur prinsip-prinsip good governance. Menyadari pentingnya masalah ini, prinsip-prinsip good governance diurai satu persatu sebagaimana tertera di bawah ini:

1) Partisipasi Masyarakat

Semua warga masyarakat mempunyai suara dalam pengambilan keputusan, baik secara langsung maupun melalui lembaga-lembaga perwakilan sah yang mewakili kepentingan mereka. Partisipasi menyeluruh tersebut dibangun berdasarkan kebebasan berkumpul dan mengungkapkan pendapat, serta kapasitas untuk berpartisipasi secara konstruktif.

2) Tegaknya Supremasi

Hukum Kerangka hukum harus adil dan diberlakukan tanpa pandang bulu, termasuk di dalamnya hukum-hukum yang menyangkut hak asasi manusia.

3) Transparansi

Tranparansi dibangun atas dasar arus informasi yang bebas. Seluruh proses pemerintahan, lembaga-lembaga dan informasi perlu dapat diakses oleh pihak-pihak yang berkepentingan, dan informasi yang tersedia harus memadai agar dapat dimengerti dan dipantau.

4) Peduli pada Stakeholder

Lembaga-lembaga dan seluruh proses pemerintahan harus berusaha melayani semua pihak yang berkepentingan.

5) Berorientasi pada Konsensus

Tata pemerintahan yang baik menjembatani kepentingan-kepentingan yang berbeda demi terbangunnya suatu konsensus menyeluruh dalam hal apa yang terbaik bagi kelompok-kelompok masyarakat, dan bila mungkin, konsensus dalam hal kebijakankebijakan dan prosedur-prosedur.

6) Kesetaraan

Semua warga masyarakat mempunyai kesempatan memperbaiki atau mempertahankan kesejahteraan mereka.

7) Efektifitas dan Efisiensi

Proses-proses pemerintahan dan lembaga-lembaga membuahkan hasil sesuai kebutuhan warga masyarakat dan dengan menggunakan sumber-sumber daya yang ada seoptimal mungkin.

8) Akuntabilitas

Para pengambil keputusan di pemerintah, sektor swasta dan organisasi-organisasi masyarakat bertanggung jawab baik kepada masyarakat maupun kepada lembaga-lembaga yang berkepentingan. Bentuk pertanggung jawaban tersebut berbeda

satu dengan lainnya tergantung dari jenis organisasi yang bersangkutan.

9) Visi Strategis

Para pemimpin dan masyarakat memiliki perspektif yang luas dan jauh ke depan atas tata pemerintahan yang baik dan pembangunan manusia, serta kepekaan akan apa saja yang dibutuhkan untuk mewujudkan perkembangan tersebut. Selain itu mereka juga harus memiliki pemahaman atas kompleksitas kesejarahan, budaya dan sosial yangmenjadi dasar bagi perspektif tersebut.

BAB 2
BUDAYA MANAJEMEN INFORMASI

2.1 Pengertian Budaya Informasi

Budaya informasi adalah kecenderungan seseorang dalam menggunakan informasi untuk menyelesaikan pekerjaannya. Informasi yang digunakan merupakan transformasi dari data-data yang dihasilkan berdasarkan fakta.

Pengertian budaya informasi menurut Marchand (dalam Suroso, 1996) adalah mencakup nilai-nilai, sikap dan perilaku yang mempengaruhi orang dalam perusahaan tersebut di dalam segenap cara pandang, mengumpulkan, mengorganisasi, memproses, menggunakan dan mengkomunikasikan informasi.

Informasi adalah fungsi penting yang membantu mengurangi kecemasan. Menurut Notoatmodjo (2003), semakin banyak informasi dapat mempengaruhi atau meningkatkan pengetahuan seseorang dan dengan pengetahuan menyadarkan manusia bahwa pada akhirnya seseorang akan berperilaku sesuai dengan pengetahuan yang dimilikinya. Seseorang dapat menemukan bahwa informasi sangat membantu dalam meningkatkan pengetahuan seseorang, yang nantinya akan membentuk pandangan dan wawasan seseorang.

Saat ini, semakin banyak perusahaan yang menyadari pentingnya melakukan transformasi perusahaan sesuai dengan perkembangan industri dan pasar. Akibatnya, banyak manajer setuju bahwa budaya informasi merupakan faktor penting dalam perumusan strategi dan implementasi perubahan (Suroso, 1998).

Akhirnya, tujuan literasi informasi pada hakekatnya berpengaruh positif terhadap perilaku, baik individu maupun organisasi. Terhubung dengan perusahaan, budaya informasi memungkinkan perusahaan untuk lebih maju dalam mendukung keputusan strategis.

2.2 Model Manajemen Informasi

Justin Keen dalam risetnya, telah menemukan bahwa terdapat 5 jenis model struktur manajemen informasi yang sangat dipengaruhi oleh budaya informasi perusahaan yang relevan. Kelima model dan karakteristiknya dijelaskan sebagai berikut (Indrajit, 2016):

• Utopianisme teknokratis adalah suatu sistem di mana suatu organisasi secara ketat, komprehensif, dan konsisten mengatur penciptaan, distribusi, dan distribusi, serta menggunakan setiap jenis informasi dalam perusahaan. Untuk kelancaran penyebaran informasi, setiap individu harus mengikuti prosedur dan standar tertentu ketika menggunakan perangkat teknologi informasi dan komunikasi yang berbeda. Dengan kata lain, setiap individu dalam organisasi ini harus "mengenal IT" karena teknologi dan informasi telah menjadi aset tak ternilai yang tidak terpisahkan bagi keberadaan bisnis. Dengan bentuk ini, biasanya ada unit TI yang bertanggung jawab untuk "menjamin" tercapainya lingkungan budaya informasi yang serius dan "benar" (sesuai aturan yang disepakati).

• Anarki adalah keadaan di mana perusahaan tidak memiliki kebijakan dan prosedur yang berkaitan dengan pengelolaan informasi. Setiap individu bebas dan kewajiban untuk mengurus kebutuhan informasi masing-masing, sesuai dengan peran, tugas dan tanggung jawabnya dalam organisasi. Perseroan hanya menyediakan teknologi dan titik akses ke berbagai sumber informasi terkait operasionalnya, baik internal maupun eksternal. Tentunya dalam kerangka ini tidak akan ada unit organisasi yang bertanggung jawab atas pengelolaan informasi, karena seringkali perusahaan mengalihkan hak penyediaan infrastruktur informasi dan komunikasi kepada pihak ketiga melalui outsourcing.

• Feodalisme terjadi ketika tata kelola informasi dan kebutuhan manajemen dimiliki atau "dimiliki" oleh satu atau lebih fungsi organisasi khusus. Unit organisasi inilah yang menentukan model informasi, kategori, dan standar yang harus dikelola oleh perusahaan, dan akan membuat informasi tersebut tersedia untuk

semua individu yang ada. Dalam format kerangka kerja ini, individu dan entitas lain umumnya akan sangat bergantung pada departemen atau departemen TI yang bersangkutan. • Rezim otoritarian menempatkan direksi perusahaan atau biasa disebut dewan direksi sebagai badan yang memutuskan dan mengontrol keberadaan informasi di perusahaan. Dewan inilah yang akan menentukan jenis dan jenis informasi yang dibutuhkan perusahaan, siapa yang dapat memperoleh dan mengaksesnya, serta struktur kontrol dan pelaporan manajemen yang terkait dengan informasi tersebut. Ada atau tidaknya departemen yang bertanggung jawab atas teknologi informasi sebagian besar ditentukan oleh dewan direksi.

• Federalisme dianggap sebagai sistem manajemen yang cukup "demokratis" karena pihak berkepentingan tertentu memiliki "konsensus" tentang pengelolaan informasi yang ada dan beredar di dalam perusahaan. Bentuk persetujuan yang dimaksud dapat bervariasi dari yang sangat formal, seperti kesepakatan untuk membentuk unit atau komunitas khusus dalam setiap fungsi, hingga informal, seperti; membentuk dewan yang mewakili pengguna.

2.3 Hubungan Organisasi dan Budaya Manajemen Informasi

Organisasi, dalam hal ini adalah perusahaan, sangat dipengaruhi oleh budaya manajemen informasi. Banyak perusahaan yang kurang memperhatikan tingkat kematangan budaya informasi di perusahaan, padahal budaya manajemen informasi ini sangat berpengaruh pada saat membentuk struktur unit teknologi informasi beserta mekanismenya. Tidak heran jika di negara maju dimana mayoritas individunya memiliki “information literacy” dan “technology literacy” yang tinggi, model anarchy kerap menjadi pilihan utama karena dinilai demokratis dan menjunjung tinggi hak individu untuk memilih dan menentukan informasi apa saja yang relevan baginya. Sementara itu untuk sebuah perusahaan yang sangat bergantung dengan informasi namun baru pimpinan saja yang mengerti nilai

strategisnya, penerapan model dictatorship akan lebih efektif hasilnya dibandingkan dengan model lainnya.

Faktanya tidak semua perusahaan mengerti dan memahami fungsi strategis dari informasi di era globalisasi saat ini. Sering dijumpai kasus dimana hanya segelintir individu yang paham betul makna informasi dan bagaimana pemanfaatannya dapat meningkatkan kinerja usaha secara signifikan. Sementara itu tidak jarang pula ditemui perusahaan dimana mayoritas manajemen dan karyawannya sangat berniat untuk mempelajari seluk beluk informasi beserta teknologinya, namun mereka yang telah memiliki pemahaman tidak mau membagikan ilmunya kepada mereka yang membutuhkan (Indrajit, 2016).

BAB 3
MANAJEMEN DAN TATA KELOLA TI

Manajemen dan tata kelola merupakan dua kata yang kerap digunakan dan tak jarang penggunaannya sering tertukar. Manajemen merupakan suatu usaha atau rangkaian proses dalam mengelola sejumlah sumber daya demi tercapainya tujuan tertentu. Proses yang dimaksud adalah perencanaan, pengorganisasian, pelaksanaan, pemantauan, pemantauan dan evaluasi yang sebelumnya dikenal dengan POAC yang merupakan singkatan dari perencanaan, pengorganisasian, pengoperasian dan pemantauan.

Berbeda dengan manajemen, *governance* yang sering dipadankan dengan istilah tata kelola memiliki dimensi yang berbeda dengan manajemen karena berada pada tataran yang lebih hakiki (filosofis) yaitu bagaimana agar suatu rangkaian aktivitas POAC pada menejemen dilakukan dengan mengacu pada prinsi-prinsip kebaikan. Oleh karena itu, manajemen lebih dekat dengan dimensi proses karena sifatnya mengelola sumber daya, sedangkan tata kelola berada pada dimensi struktur pertanggungjawaban dan pengambilan keputusan terhadap berbagai kegiatan yang strategis. Dimana tata kelola memiliki 5 prinsip yang berlaku secara umum, yaitu *transparency* (transparansi), *accountability* (akuntabilitas), *responsibility* (tanggung jawab), *independence* (bebas) dan *fairness* (adil).

3.1 Manajemen TI

Dalam dunia teknologi informasi, dikenal pula istilah Manajemen TI, karena pada dasarnya sebuah organisasi perlu mengelola berbagai asset teknologi yang dimilikinya untuk mendukung perusahaan dalam mencapai visi dan misinya. Sumber daya teknologi informasi didefinisikan sebagai hardware atau perangkat keras, infrastruktur jaringan, perangkat lunak atau software, basis data atau database, alat informasi atau infoware,

sarana dan prasarana pendukung teknologi (data center, ruang server, backup system, dan sebagainya) serta aset manusia berupa pengelola, pengguna, dan penyelenggara.

Manajemen TI mengacu pada perencanaan, pengelolaan, pengaturan, dan pengendalian sumber daya TI berdasarkan kebutuhan dan prioritas. Sumber daya dalam konteks ini adalah sumber daya TI yaitu perangkat keras atau hardware, infrastruktur jaringan, perangkat lunak atau perangkat lunak, basis data atau basis data, alat informasi atau infoware, sarana dan prasarana pendukung teknis (pusat data, ruang server). sistem keamanan, dll.) dan manajer operasional (pengguna, penyelenggara, implementasi/operator).

Tujuan utama manajemen TI adalah menggunakan teknologi untuk menciptakan nilai. Untuk mencapai tujuan ini, strategi bisnis dan strategi teknologi harus diselaraskan. Dunia pengelolaan TI teknologi informasi sangat dibutuhkan oleh organisasi untuk mengelola berbagai aset teknologi yang dimilikinya untuk membantu mewujudkan visi dan misinya.

Sebuah asosiasi pengaudit internasional ISACA (Information System Audit and Control Association) melalui entitas risetnya ITGI (Information Technology Governance Institute), yang menyusun COBIT versi 4.0, membagi domain manajemen teknologi informasi menjadi 4 (empat) bagian besar, yaitu masing-masing:

a. Domain Perencanaan dan Pengorganisasian (*Planning and Organisation*);
b. Domain Pengadaan dan Penerapan (*Acquisition and Implementation*);
c. Domain Pemanfaatan dan Pemeliharaan (*Delivery and Support*) ; dan
d. Domain Pengawasan dan Penilaian (*Monitoring and Evaluation*).

Masing-masing domain tersebut terdiri dari sejumlah proses terkait dengan pengelolaan sumber daya teknologi informasi dalam sebuah organisasi.

3.2 Governance TI

Kata governance berasal dari bahasa Latin yaitu *gubernare*. Banyak orang menggunakan istilah governance sebagai padanannya dalam bahasa Indonesia. Tata kelola sering dikaitkan dengan konteks/tingkat organisasi (misalnya perusahaan atau lembaga pemerintah). Dalam konteks perusahaan, tata kelola yang baik membantu mengamankan masa depan perusahaan dengan menyelaraskan strategi perusahaan dengan visi dan tujuan perusahaan. Oleh karena itu, tata kelola perusahaan pada hakekatnya adalah sistem pengendalian perusahaan.

Singkatnya, tata kelola terutama struktur dan mekanisme yang dirancang untuk memberikan administrator organisasi, atau administrator, kontrol yang memadai. Tata kelola dan manajemen memiliki fungsi strategis, dan manajemen juga memiliki fungsi operasional. Namun, ada kalanya Anda perlu memahami batasan tata kelola dan kontrol. Di dunia akademik, tata kelola, khususnya tata kelola TI, didominasi oleh perdebatan di tingkat organisasi (khususnya korporat/unit bisnis). Dalam konteks perusahaan, tata kelola TI merupakan bagian integral dari tata kelola perusahaan yang baik. Namun, seperti diketahui, topik tata kelola TI sebenarnya adalah topik manajemen bisnis, bukan topik teknologi informasi.

Dengan berfokus pada di mana dan bagaimana keputusan dibuat, oleh siapa, keputusan apa yang dibuat, dan mengapa, tata kelola TI menyediakan mekanisme untuk memberikan nilai, kinerja, dan mitigasi risiko. Oleh karena itu, tata kelola TI umumnya terkait dengan orang (SDM), proses dan budaya. Inti dari tata kelola dalam situasi apapun adalah bahwa tujuan utama pada dasarnya adalah sistem yang terorganisir untuk mencapai tujuan tersebut.

Dalam konteks governance, ISACA dan ITGI menggunakan terminologi yang diperkenalkan untuk pertama kalinya yaitu RACI, yang merupakan singkatan dari:

a. Responsible; merupakan pihak yang bertugas sebagai pelaksana utama sebuah aktivitas atau kegiatan tertentu;
b. Accountable; merupakan pihak yang paling bertanggung jawab terhadap keberadaan dan/atau kinerja sebuah aktivitas atau kegiatan tertentu;
c. Consulted; merupakan pihak yang harus diminta pendapatanya (dikonsultasikan) dalam konteks pelaksanaan sebuah aktivitas atau kegiatan tertentu; dan
d. Informed; merupakan pihak yang harus diinformasikan (diberitahukan) dalam konteks pelaksanaan sebuah aktivitas atau kegiatan tertentu.

Dengan berpegang pada prinsip-prinsip ini, maka sebuah perusahaan atau organisasi perlu memetakan proses atau aktivitas yang dimilikinya dengan struktur organisasi yang ada, sehingga dalam konteks pengambilan keputusan dan pertanggung jawaban terhadap berbagai kegiatan menjadi jelas bagi seluruh pemangku kepentingan yang terlibat. Kalau manajemen biasanya berada dalam tataran "line management" ke bawah, maka untuk governance prinsip atau struktur pengambilan keputusan disusun untuk mereka yang berada pada level "senior management" ke atas (tingkat direktur hingga komisaris selaku wakil dari pemegang saham).

BAB 4

PENGENDALIAN INTERNAL ORGANISASI

Kebutuhan akan pengendalian internal yang kuat dan efektif adalah adalah elemen kunci tata kelola TI perusahaan. Kebutuhan untuk membangun dan kemudian menilai pengendalian internal telah ada sejak hari-hari awal audit dan juga demikian menjadi perhatian penting akan kembali ke hari-hari awal teknologi informasi audit (TI).

Meskipun ada banyak definisi pengendalian internal dalam beberapa tahun terakhir, definisi umum yang baik untuk tata kelola TI adalah bahwa pengendalian internal adalah suatu proses, yang dilakukan oleh dewan direksi, manajemen, dan personel lain, yang dirancang untuk memberikan keyakinan memadai mengenai pencapaian tujuan dalam efektivitas dan efisiensi operasi, keandalan pelaporan keuangan perusahaan, dan sistem dan proses TI perusahaan, semuanya sesuai dengan hukum dan peraturan. Definisi ini mirip dengan definisi yang diakui dengan baik yang ditetapkan oleh sebuah komite bernama COSO (*Committee of Sponsoring Organizations*) yaitu panduan kontrol internal yang memiliki otoritas penting di Amerika Serikat.

Manajer perusahaan bertanggung jawab untuk menerapkan dan mengelola pengendalian proses internal, sementara auditor mereka bertindak sebagai pihak independen untuk meninjau dan melakukan pengujian pengendalian internal tersebut serta melaporkannya kepada manajemen dan pihak lain apakah mereka memadai. Peninjau pengendalian internal ini terdiri dari dua pihak yaitu auditor internal dan eksternal. Internal auditor umumnya mengikuti pedoman dari Institute of Internal Auditors (IIA) sedangkan auditor eksternal di Amerika Serikat harus mempunyai sertifikasi standar American Institute of Certified Public Accountants (AICPA). Kedua organisasi audit ini memiliki warisan yaitu kembali ke kertas dan pensil dan sebelum penggunaan dan ketergantungan yang meluas saat ini pada sistem

dan proses TI. Setelah bertahun-tahun, Asosiasi Audit dan Kontrol Sistem Informasi (ISACA) dan IT-nya profesional audit juga telah memenuhi sebagian besar kebutuhan akan pengendalian internal yang efektif.

4.1 Pentingnya Pengendalian Internal bagi Perusahaan

Pengendalian internal adalah salah satu konsep terpenting dan mendasar yang harus dipahami oleh manajer senior dan profesional bisnis di semua tingkatan. Profesional bisnis membangun dan menggunakan pengendalian internal, sementara auditor meninjau dan menguji operasional, IT, dan sistem dan proses keuangan dengan tujuan mengevaluasi internal mereka kontrol. Meskipun auditor internal dan eksternal memiliki tujuan yang berbeda, sebagian besar dari kami referensi dalam bab ini berlaku untuk manajer senior yang memiliki tanggung jawab utama untuk memahami masalah tata kelola TI dan menilai kontrol internal terkait TI.

Meskipun ada banyak definisi pengendalian internal yang sedikit berbeda di masa lalu, kerangka pengendalian internal COSO dibahas pada bagian berikut memberikan definisi yang tepat untuk manajer senior. Ia mengakui bahwa internal kontrol melampaui hanya masalah akuntansi dan keuangan dan mencakup semua perusahaan proses. Juga, karena TI begitu tertanam dalam semua proses bisnis, terkait TI pengendalian internal merupakan bagian utama dari keseluruhan pemahaman kita tentang pengendalian internal.

Suatu unit atau proses perusahaan memiliki pengendalian internal yang baik jika:

a. memenuhi apa yang telah ditetapkan misi secara etis,
b. menghasilkan data yang akurat dan dapat diandalkan,
c. sesuai dengan undang-undang dan kebijakan perusahaan yang berlaku,
d. menyediakan penggunaan yang ekonomis dan efisien sumber dayanya, dan

e. menyediakan pengamanan aset yang tepat. Semua anggota dari suatu perusahaan bertanggung jawab atas pengendalian internal di wilayah operasinya dan untuk mengoperasikannya secara efektif.

4.2 Tata Kelola TI dan Kontrol Internal COSO

Auditor TI melayani peran audit eksternal dan internal, meskipun mungkin sebagian besar profesional di sini berfungsi sebagai auditor internal untuk perusahaan mereka. Menindaklanjuti diskusi sebelumnya tentang Aturan Sarbanes-Oxley Act (SOx), bab ini memperkenalkan apa yang dikenal sebagai kerangka kerja pengendalian internal COSO dan juga menguraikan proses tata kelola TI terkait COSO dalam bisnis saat ini perusahaan. Kontrol internal COSO dan SOx, yang dibahas pada bab sebelumnya, dimulai dari Amerika Serikat, namun aturan panduan kontrol internal sekarang telah diterima di seluruh dunia. Keduanya memiliki asal-usul sebagai panduan tinjauan keuangan dan operasi umum dan sangat berlaku untuk lingkungan tata kelola TI juga.

Pemahaman dan penggunaan kerangka pengendalian internal COSO penting untuk membangun proses tata kelola TI yang efektif. Sementara aturan dan prosedur ini memiliki asal-usul dalam pelaporan dan audit keuangan, di dunia yang berpusat pada TI saat ini, internal COSO kontrol adalah alat tata kelola TI yang penting. Ini adalah aturan yang harus diikuti oleh perusahaan untuk menegaskan atau membuktikan kepada regulator bahwa organisasi mereka memiliki internal yang efektif kontrol di tempat dan bahwa mereka beroperasi sesuai dengan aturan-aturan baru.

Terlepas dari definisi internal yang luas, banyak profesional bisnis memiliki masalah dalam memahami sepenuhnya dan menerapkan konsep pengendalian internal. Melihat definisi kami sedikit berbeda, konsepnya pengendalian internal dan proses pengendalian pendukung kembali ke mekanik dasar dan prosedur dokumen yang dulu sering ada dalam bisnis sehari-hari operasi dan kehidupan. Proses kontrol diperlukan untuk aktivitas di dalam dan

di luar hari ini perusahaan, dan banyak konsep dan prinsip dasar yang sama di mana pun pengendalian dilaksanakan.

Mobil menyediakan beberapa contoh kontrol dasar. Ketika akselerator kontrol kecepatan ditekan, mobil melaju lebih cepat. Saat rem ditekan, mobil melambat atau berhenti. Saat setir berbelok, kendaraan berbelok. Pengemudi mengendalikan mobil, dan ketiganya mewakili sistem kontrol internal dasar mobil. Jika pengemudi tidak menggunakan atau tidak benar menggunakan pedal gas, rem, atau setir, mobil akan beroperasi di luar kendali. Memperluas konsep ini sedikit saja, rambu berhenti, rambu penunjuk arah lalu lintas, dan gerbang penyeberangan penghalang semuanya mewakili kontrol eksternal untuk mobil dan pengemudinya. Sopir adalah operator proses atau sistem pengendalian internal berbasis mobil, tetapi memiliki sedikit keputusan otoritas atas pesan yang disampaikan dari kontrol eksternal lampu lalu lintas.

Dari perspektif pengendalian internal, sebuah perusahaan dapat dibandingkan dengan mobil kita contoh. Ada banyak sistem dan proses perusahaan di tempat kerja, seperti operasi akuntansi, proses penjualan, dan sistem TI. Jika manajemen tidak beroperasi atau mengarahkan proses ini dengan benar, perusahaan dapat beroperasi di luar kendali. Semua anggota perusahaan harus mengembangkan pemahaman tentang pengendalian yang tepat sistem dan kemudian menentukan apakah mereka terhubung dengan benar untuk mengelola perusahaan. Ini disebut sebagai sistem pengendalian internal perusahaan.

BAB 5
FRAMEWORK TATA KELOLA TI

Profesional perusahaan dan manajer senior tertentu memerlukan penggunaan seperangkat standar atau kerangka kerja untuk mengatur praktik tata kelola TI dan prosedur pengendalian internal mereka secara umum. Kepatuhan terhadap kerangka kerja seperti itu memungkinkan manajer senior serta profesional perusahaan di bidang keahlian mereka diakui sebagai spesialis di bidangnya. Kerangka pengendalian internal, Komite Organisasi Sponsor (COSO), seperti yang diperkenalkan di Bab 4, telah menjadi alat tata kelola TI yang penting untuk mengevaluasi dan meningkatkan proses tata kelola TI untuk rentang yang luas dari sistem dan proses TI serta akuntansi internal mengontrol aturan di bawah Sarbanes-Oxley Act (SOx) yang diperkenalkan di Bab 1. Namun, beberapa manajer senior dan profesional teknologi informasi (TI), khususnya, telah menyatakan keprihatinannya dengan menggunakan kerangka pengendalian internal COSO dalam orientasi dunia TI saat ini. Kekhawatirannya adalah bahwa pedoman pengendalian internal COSO yang diterbitkan tidak hanya memberikan penekanan yang cukup pada alat dan proses TI. Misalnya yang asli, Materi panduan pengendalian internal COSO yang diterbitkan tahun 1992 terutama terlihat pada kontrol internal aplikasi TI pada tingkat yang sangat tinggi, meskipun masih banyak lagi kebutuhan untuk panduan pengendalian internal tambahan khusus TI di dunia saat ini.

5.1 Framework IT Infrastucture Library (ITIL)

ITIL dikembangkan sejak tahun 1980-an oleh The Office of Government Commerce (OGC) suatu badan dibawah pemerintah Inggris, dengan bekerja sama dengan The IT Service Management Forum (ITSMF) dan British Standard Institute (BSI) namun penggunaan ITIL baru meluas pada pertengahan 1990-an dengan spesifikasi versi keduanya (ITIL v2) yang paling dikenal dengan

dua set bukunya yang berhubungan dengan ITSM (IT Service Management), yaitu Service Delivery (Antar Layanan) dan Service Support (Dukungan Layanan). ITIL merupakan suatu framework pengelolaan layanan TI (IT Service Management - ITSM) yang sudah diadopsi sebagai standar industri pengembangan industri perangkat lunak di dunia. Kerangka kerja digunakan untuk mendefinisikan pengelolan layanan yang terintegrasi, berbasiskan proses dan praktik-praktik yang terbaik dalam organisasi. Pada awalnya ITIL adalah serangkaian lebih dari 40 buku pedoman tentang pengelolaan layanan IT yang terdiri dari 26 modul, dikarenakan adanya peningkatan pelayanan yang berkesinambungan dan adaptasi terhadap situasi saat ini dalam lingkungan (TI) modern ITIL 1.0 di rilis besar dan digabungkan menjadi delapan inti manual: ITIL 2.0. Pada awal musim panas 2007 ITIL 3.0 diterbitkan. Ini didirikan struktur yang sama sekali baru. Ini terdiri dari tiga bidang utama: ITIL Core Publikasi, ITIL Pelengkap Bimbingan, dan ITIL Web Support Services Pada 30 Juni 2007, OGC (Office of Government Commerce) menerbitkan versi ketiga ITIL (ITIL v3) yang intinya terdiri dari lima bagian dan lebih menekankan pada pengelolaan siklus hidup layanan yang disediakan oleh teknologi informasi yaitu Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement. Versi ini menekankan pada integrasi antara bisnis dengan IT dan menekankan pada pendekatan lifecycle untuk service management. ITIL adalah framework untuk IT Service Management. Proses-proses yang dijelaskan di ITIL bertujuan untuk meningkatkan efisiensi (decrease cost) dan keefektifan (increase quality) dari IT services. Tujuan dari ITIL antara lain yaitu:

• Mengurangi biaya-biaya

• Meningkatkan ketersediaan

• Meningkatkan kapasitas

• Meningkatkan throughput

• Mengoptimalkan pemanfaatan sumber daya

• Meningkatkan skalabilitas

Kelebihan dari ITIL antara lain:

• Netral

• Komprehensif

• Modular

• Pendekatan kualitas

• Efektifitas biaya

• Bisa diaplikasikan secara universal

• Tersedianya alat pendukung Standar ITIL berfokus kepada pelayanan customer, dan sama sekali tidak menyertakan proses penyelarasan strategi perusahaan terhadap strategi TI yang dikembangkan.

5.2 ISO/EIC 17799

ISO/IEC pertama kali diterbitkan pada desember tahun 2000 dikembangkan oleh The International Organization for Standardization (ISO) dan The International Electrotechnical Commission (IEC) yang awalnya adalah ISO/IEC 27001 tentang "Information Security Management System (ISMS) requirements" dan kemudian direvisi ISO/IEC 17799 pada tahun 2005 adalah merupakan tonggak utama dalam perjalanan perkembangan standarisasi information security management. ISO17799 memberikan secara komprehensif alat pengendalian information security management yang berisikan praktek terbaik dalam keamanan informasi. Standar ini sampai sekarang belum sempurna karena hanya meliputi seluruh area yang penting saja sehingga masih mengalami revisi yang seksama.

ISO/IEC 17799 bertujuan memperkuat 3 (tiga) elemen dasar keamanan informasi, yaitu :

• *Confidentiality*, memastikan bahwa informasi hanya dapat diakses oleh yang berhak.

• *Integrity*, menjaga akurasi dan selesainya informasi dan metode pemrosesan.

• *Availability*, memastikan bahwa user yang terotorisasi mendapatkan akses kepada informasi dan aset yang terhubung dengannya ketika memerlukannya.

Sedangkan tujuan pengendalian ISO 17799 adalah :

a. Memberikan rekomendasi manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggungjawab dalam inisiasi, implementasi, atau mengelola keamanan informasi pada organisasinya. ISO 17799 Merupakan standar keamanan internasional manajemen yang pertama kali diterapkan
b. Untuk meyakinkan kerahasiaan, integritas dan ketersediaan asset informasi untuk perusahaan tetapi lebih penting lagi, bagi para pelanggan. Jaminan dicapai melalui Kontrol / pengendalian bahwa manajemen diciptakan dan dipelihara di dalam organisasi. Untuk menjalankannya, ISO 17799 menggambarkan suatu proses atas penyelesaian dengan menyediakan basis untuk keseluruhan Sistem Manajemen Keamanan Informasi (ISMS).

Komponen-komponen dari ISO-17799, adapun 10 control clauses ISO-17799 terdiri dari :

- Kebijakan Pengamanan (Security Policy)

Mengarahkan visi dan misi manajemen agar kelangsungan organisasi dapat dipertahankan dengan mengamankan dan menjaga integritas/keutuhan data/informasi penting yang dimiliki oleh perusahaan. Kebijakan pengamanan sangat diperlukan mengingat banyaknya masalah-masalah non teknis seperti penggunaan password oleh lebih dari satu orang yang menunjukan tidak adanya kepatuhan dalam menjalankan sistem keamanan informasi. Kebijakan pengamanan ini meliputi aspek infratruktur dan regulasi keamanan informasi. Hal pertama dalam pembuatan kebijakan

keamanan adalah dengan melakukan inventarisasi data-data perusahaan. Selanjutnya dibuat regulasi yang melibatkan semua departemen, sehingga peraturan yang akan dibuat tersebut dapat diterima oleh semua pihak. Setelah itu rancangan peraturan tersebut diajukan ke pihak direksi untuk mendapatkan persetujuan dan dukungan agar dapat diterapkan dengan baik.

- Pengendalian Akses Sistem (System Access Control)

Mengendalikan akses user terhadap informasi-informasi dengan cara mengatur kewenangannya, termasuk pengendalian secara mobile-computing ataupun tele networking. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada yang meliputi berbagai aspek seperti :

a. Persyaratan bisnis untuk kendali akses;
b. Pengelolaan akses user (User Access Management);
c. Kesadaran keamanan informasi (User Responsibilities);
d. Kendali akses ke jaringan (Network Access Control);
e. Kendali akses terhadap sistem operasi (Operating System Access Control);
f. Pengelolaan akses terhadap aplikasi (Application Access Management);
g. Pengawasan dan penggunaan akses sistem (Monitoring System Access and Use);
h. Mobile Computing dan Telenetworking.

- Pengelolaan Komunikasi dan Kegiatan (Communication and Operations Management)

Menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan dikomunikasikan guna menghindari kesalahan operasional. Pengaturan tentang alur komunikasi dan operasi yang terjadi meliputi berbagai aspek, yaitu :

a. Prosedur dan tanggung jawab operasional;
b. Perencanaan dan penerimaan sistem;
c. Perlindungan terhadap software jahat (malicious software);
d. Housekeeping;
e. Pengelolaan Network;
f. Pengamanan dan Pemeliharaan Media;
g. Pertukaran informasi dan software.

- Pengembangan dan Pemeliharaan Sistem (System Development and Maintenance)

Memastikan bahwa sistem operasi maupun aplikasi yang baru diimplementasikan mampu bersinergi melalui verifikasi dan validasi. Penelitian untuk pengembangan dan pemeliharaan sistem meliputi berbagai aspek, seperti : Persyaratan pengamanan sistem; Pengamanan sistem aplikasi; Penerapan Kriptografi; Pengamanan file sistem; dan Pengamanan pengembangan dan proses pendukungnya.

- Pengamanan Fisik dan Lingkungan (Physical and Environmental Security)

Mencegah kehilangan dan/atau kerusakan data yang diakibatkan oleh lingkungan secara fisik, termasuk bencana alam dan pencurian data yang tersimpan dalam media penyimpanan atau dalam fasilitas penyimpan informasi yang lain. Pengamanan fisik dan lingkungan ini meliputi aspek : Pengamanan area tempat informasi disimpan; Pengamanan alat dan peralatan yang berhubungan dengan informasi yang akan dilindungi; dan Pengendalian secara umum terhadap lingkungan dan hardware informasi.

- Penyesuaian (Compliance)

Memastikan implementasi kebijakan-kebijakan keamanan selaras dengan peraturan dan perundangan yang berlaku, termasuk perjanjian kontrak melalui audit sistem secara berkala. Aspek-aspek yang diperlukan untuk membentuk prosedur dan peraturan, yaitu : Penyesuaian dengan persyaratan legal; Peninjauan kembali kebijakan pengamanan dan penyesuaian secara teknis; serta Pertimbangan dan audit sistem.

- Keamanan personel/sumber daya manusia (Personnel Security)

Upaya pengurangan resiko dari penyalahgunaan fungsi dan/atau wewenang akibat kesalahan manusia (human error), manipulasi data dalam pengoperasian sistem serta aplikasi oleh user. Kegiatan yang dilakukan diantaranya adalah pelatihan-pelatihan mengenai kesadaran informasi (security awareness) agar setiap user mampu menjaga keamanan data dan informasi dalam lingkup kerja masing-masing.

Personnel Security meliputi berbagai aspek, yaitu: Security in Job Definition and Resourcing; Pelatihan-pelatihan dan Responding to Security Incidens and Malfunction.

- Organisasi Keamanan (Security Organization)

Memelihara keamanan informasi secara global pada suatu organisasi atau instansi, memelihara dan menjaga keutuhan sistem informasi internal terhadap ancaman pihak eksternal, termasuk pengendalian terhadap pengolahan informasi yang dilakukan oleh pihak ketiga (outsourcing). Aspek yang terlingkupi, yaitu keamanan dan pengendalian akses pihak ketiga dan *outsourcing*.

- Klasifikasi dan pengendalian aset (Asset Classification and Control)

Memberikan perlindungan terhadap aset perusahaan yang berupa aset informasi berdasarkan tingkat perlindungan yang telah

ditentukan. Perlindungan aset ini meliputi accountability for Asset dan klasifikasi informasi.

- Pengelolaan Kelangsungan Usaha (Business Continuity Management)

Siaga terhadap resiko yang mungkin timbul didalam aktivitas lingkungan bisnis yang bisa mengakibatkan ”major failure” atau resiko kegagalan sistem utama ataupun ”disaster” atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan pengelolaan untuk kelangsungan proses bisnis, dengan mempertimbangkan semua aspek dari business continuity management.

Penggunaan ISO 17799

Penggunaan dari ISO 17799 masih merupakan alat bantu yang berguna baik itu pihak internal maupun pihak eksternal yaitu:

• Organisasi, untuk mempelajari serta melaksanakannya guna

mendapatkan sertifikasi tersebut

• Auditor TI, untuk membandingkan kesesuaian antara standar

dengan kenyataan yang ada di organisasi tersebut

• Auditor Keuangan, digunakan sebagai salah satu acuan untuk menentukan dalamnya pemeriksaan

• Pemerintah atau institusi lain yang berkepentingan.

Keuntungan utama dari BS7799/ISO17799 berhubungan dengan kepercayaan publik. Sama seperti ISO 9000 yang mencerminkan jaminan kualitas.

• Standar ini merupakan tanda kepercayaan dalam seluruh keamanan perusahaan.

• Manajemen kebijakan terpusat dan prosedur.

• Menjamin layanan informasi yang tepat guna.

• Mengurangi biaya manajemen,

• Dokumentasi yang lengkap atas segala perubahan/revisi.

• Suatu metoda untuk menentukan target dan mengusulkan peningkatan.

• Basis untuk standard keamanan informasi internal perusahaan

5.3 COSO

COSO merupakan singkatan dari Committee of Sponsoring Organization of the Treadway Commission, yang dibentuk pada tahun 1985 dengan tujuannya adalah untuk mengidentifikasi faktor-faktor yang menyebabkan kecurangan (fraund) seperti penggelapan laporan keuangan dan membuat rekomendasi untuk mengurangi kejadian tersebut. COSO telah menyusun suatu definisi umum untuk pengendalian, standar, dan kriteria internal yang dapat digunakan perusahaan untuk menilai sistem pengendalian yang berdedikasi dalam meningkatkan kualitas pelaporan finansial mencakup etika bisnis, kontrol internal dan corporate governance.

COSO mempunyai misi yaitu memberikan pemikiran kepemimpinan melalui pengembangan kerangka kerja dan pedoman yang komprehensif tentang manajemen risiko perusahaan , pengendalian internal dan pencegahan kecurangan yang dirancang untuk meningkatkan kinerja organisasi dan tata pemerintahan dan untuk mengurangi tingkat kecurangan dalam organisasi dan visinya adalah menjadi pemikiran pemimpin yang diakui di pasar global pada pengembangan di bidang risiko dan pengendalian yang memungkinkan tata kelola organisasi yang baik dan pengurangan kecurangan.

COSO framework terdiri dari 3 dimensi yaitu :

• Komponen kontrol COSO.

COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kontrol internal adalah

Monitoring, Information and communications, Control activities, Risk assessment, dan Control environment.

• Sasaran kontrol internal.

Sasaran kontrol internal dikategorikan menjadi beberapa area sebagai berikut :

- *Operations*. Efisisensi dan efektifitas operasi dalam mencapai sasaran bisnis yang juga meliputi tujuan performansi dan keuntungan.

- *Financial reporting*. Persiapan pelaporan anggaran finansial yang dapat dipercaya.

- *Compliance*. Pemenuhan hukum dan aturan yang dapat dipercaya.

• Unit/Aktifitas Terhadap Organisasi

Dimensi ini mengidentifikasikan unit/aktifitas pada organisasi yang menghubungkan kontrol internal. Kontrol internal menyangkut keseluruhan organisasi dan semua bagianbagiannya. Kontrol internal seharusnya diimplementasikan terhadap unit-unit dan aktifitas organisasi.

Kerangka Kerja COSO menetapkan definisi pengendalian internal, menjelaskan komponen-komponennya, dan menyediakan kriteria terhadap sistem pengendalian yang dapat dievaluasi. Termasuk juga disebutkan didalamnya adalah memberikan pedoman penyusunan pengendalian internal untuk tujuan pelporan kepada publik dan menyediakan bahan-bahan kepada manajemen, auditor, dan pengguna lainnya untuk mengevaluasi sistem pengendalian internal. Jadi, dua tujuan utama dari laporan tersebut adalah (1) untuk menetapkan definisi umum pengendalian internal

yang melayani berbagai pihak, dan (2) menyediakan standar terhadap organisasi yang dapat menilai sistem pengendalian dan menentukan cara untuk meningkatkan/memperbaiki sistem tersebut.

Definisi Pengendalian Internal COSO adalah "suatu proses, yang dipengaruhi oleh dewan komisaris, manajemen, dan personil lainnya dari sebuah entitas, yang dirancang untuk memberikan keyakinan/jaminan yang wajar berkaitan dengan pencapaian tujuan dalam kategori berikut : Efektivitas dan efisiensi operasi, Keandalan laporan keuangan, Kepatuhan terhadap hukum dan peraturan yang berlaku. Laporan ini menekankan bahwa sistem pengendalian internal adalah merupakan alat/perangkat dari manajemen dan bukan pengganti manajemen. Jadi manajemen dan sistem pengendalian seharusnya dibentuk didalam kegiatan operasi.

Pihak yang Terlibat

Dokumen COSO menyatakan bahwa pihak-pihak yang terlibat terkait Pengendalian Internal adalah dewan komisaris, manajemen, dan pihak-pihak lainnya yang mendukung pencapaian tujuan organisasi. Serta menyatakan bahwa tanggung jawab atas penetapan, penjagaan, dan pengawasan sistem

Pengendalian Internal adalah tanggung jawab manajemen. COSO mengidentifikasi Sistem Pengendalian Internal yang efektif meliputi lima komponen yang saling berhubungan untuk mendukung pencapaian tujuan entitas, yaitu :

• Penilaian Risiko (Risk Assessment)

Terdiri dari identifikasi risiko dan analisis risiko. Identifikasi risiko meliputi pengujian terhadap faktor-faktor eksternal seperti perkembangan teknologi, persaingan, dan perubahan ekonomi.

Factor internal diantaranya kompetensi karyawan, sifat dari aktivitas bisnis, dan karakteristik pengelolaan sistem informasi. Sedangkan Analisis Risiko meliputi mengestimasi signifikansi risiko, menilai kemungkinan terjadinya risik, dan bagaimana mengelola risiko.

• Lingkungan Pengendalian (Control Environment)

Merupakan pondasi dari komponen lainnya dan meliputi

beberapa faktor diantaranya :

- Integritas dan Etika

- Komitmen untuk meningkatkan kompetensi

- Dewan komisaris dan komite audit

- Filosofi manajemen dan jenis operasi

- Kebijakan dan praktek sumber daya manusia

COSO menyediakan pedoman untuk mengevaluasi tiap factor tersebut diatas. Misal, Filosofi manajemen dan jenis operasi dapat dinilai dengan cara menguji sifat dari penerimaan risiko bisnis, frekuensi interaksi dari tiap subordinat, dan pengaruhnya terhadap laporan keuangan.

• Aktivitas Pengendalian (Control Activities)

Aktivitas Pengendalian terdiri dari kebijakan dan prosedur yang menjamin karyawan melaksanakan arahan dari manajemen. Aktivitas Pengendalian meliputi review terhadap sistem pengendalian, pemisahan tugas, dan pengendalian terhadap sistem informasi.

Pengendalian terhadap sistem informasi meliputi dua cara :

- *General controls*, mencakup kontrol terhadap akses, perangkat lunak, dan system development.

- *Application controls,* mencakup pencegahan dan deteksin transaksi yang tidak terotorisasi. Berfungsi untuk menjamin

completeness, accuracy, authorization and validity dari proses transaksi

• Informasi dan komunikasi

COSO menyatakan perlunya untuk mengakses informasi dari dalam dan luar, mengembangkan strategi yang potensial dan sistem terintegrasi, serta perlunya data yang berkualitas. Sedangkan diskusi mengenai komunikasi berfokus kepada menyampaikan permasalahan Pengendalian Internal, dan mengumpulkan informasi pesaing.

• Pengawasan (*Monitoring*)

Karena Pengendalian Internal harus dilakukan sepanjang waktu, maka COSO menyatakan perlunya manajemen untuk terus melakukan pengawasan terhadap keseluruhan Sistem Pengendalian Internal melalui aktivitas yang berkelanjutan dan melalui evaluasi yang ditujukan terhadap aktivitas atau area yang khusus. Di tahun 2004, COSO mengeluarkan report 'Enterprise Risk Management Integrated Framework', sebagai pengembangan COSO framework di atas. Dijelaskan ada 8 komponen dalam

Enterprise Risk Management, yaitu :

• Lingkungan Internal (*Internal Environment*)

Sangat menentukan warna dari sebuah organisasi dan memberi dasar bagi cara pandang terhadap risiko dari setiap orang dalam organisasi tersebut. Didalam lingkungan internal ini termasuk, filosofi manajemen risikodan risk appetite, nilainilai etika dan integritas, dan lingkungan dimana kesemuanya tersebut berjalan.

• Penentuan Tujuan (*Objective Setting*)

Tujuan perusahaan harus ada terlebih dahulu sebelum manajemen dapat mengidentifikasi kejadian kejadian yang berpotensi mempengaruhi dalam pencapaian tujuan tersebut. ERM memastikan bahwa manajemen memiliki sebuah proses untuk

menetapkan tujuan dan tujuan tersebut terkait serta mendukung misi perusahaan dan konsisten dengan risk appetite-nya.

• Identifikasi Kejadian (*Event Identification*)

Kejadian internal dan eksternal yang mempengaruhi pencapaian tujuan perusahaan harus diidentifikasi, dan dibedakan antara risiko dan peluang yang dapat terjadi. Peluang dikembalikan kepada proses penetapan strategi atau tujuan manajemen.

• Penilaian Risiko (*Risk Assessment*)

Risiko dianalisis dengan memperhitungkan kemungkinan terjadi (likelihood) dan dampaknya (impact), sebagai dasar bagi penentuan pengelolaan risiko.

• Respons Risiko (*Risk Response*)

Manajemen memilih respons risiko, menghindar, menerima, mengurangi, mengalihkan, dan mengembangkan suatu kegiatan agar risiko yang terjadi masih sesuai dengan toleransi dan risk appetite.

• Kegiatan Pengendalian (*Control Activities*)

Kebijakan serta prosedur yang ditetapkan dan diimplementasikan untuk membantu memastikan respons risiko berjalan dengan efektif.

• Informasi dan Komunikasi (*Information and Communication*)

Informasi yang relevan diidentifikasi, ditangkap, dan dikomunikasikan dalam bentuk dan waktu yang memungkinkan setiap orang menjalankan tanggung jawabnya.

• Pengawasan (*Monitoring*),

Keseluruhan proses ERM dimonitor dan modifikasi dilakukan apabila perlu. Pengawasan dilakukan secara melekat pada kegiatan manajemen yang berjalan terus-menerus, melalui evaluasi secara khusus, atau dengan keduanya.

BAB 6

Control Objectives for IT and Related Technology (COBIT)

6. 1 Pengertian COBIT

Control Objectives for Information and Related Technology (COBIT) dapat definisikan sebagai alat pengendalian untuk informasi dan teknologi terkait dan merupakan standar terbuka untuk pengendalian terhadap teknologi informasi yang dikembangkan oleh Information *System Audit and Control Association* (ISACA) melalui lembaga yang dibentuknya yaitu *Information and Technology Governance Institute* (ITGI) pada tahun 1992.

Cobit yang pertama kali diluncurkan pada tahun 1996, mengalami perubahan berupa perhatian lebih kepada dokumen sumber,revisi pada tingkat lebih lanjut serta tujuan pengendalian rinci dan tambahan seperangkat alat implementasi *(implementation tool set)* pada edisi keduanya yang dipublikasikan pada tahun 1998. Cobit pada edisi ketiga ditandai dengan masuknya penerbit utama baru COBIT yaitu ITGI. COBIT edisi keempat merupakan versi terakhir dari tujuan pengendalian untuk informasi dan teknologi terkait.

Berikut adalah manfaat dari menerapkan COBIT sebagai kerangka tata kelola TI (ITGI, 2007) :

• Penyelarasan yang lebih baik, berdasarkan focus bisnis.

• Pandangan dipahami oleh manajemen TI.

• Kepemilikan dan tanggung jawab yang jelas, berdasarkan orientasi proses.

• Penerimanaan umum dengan pihak ketiga dan regulator.

• Pemahaman kepada semua pihak yang berkepentingan, menggunakan bahasa yang umum.

• Pemenuhan persyaratan COSO untuk lingkungan pengendalian TI.

6.2 Visi Misi COBIT

Adapun visi misi COBIT adalah :

• Visi COBIT adalah sebagai model untuk penguasaan TI.

• Misi COBIT adalah melakukan penelitian, pengembangan, publikasi, dan promosi terhadap control objectives yang diterima di lingkungan internasional dan digunakan sehari-hari oleh manajer dan auditor.

6.3 Fokus COBIT

Fokus COBIT lebih kepada control (pengendalian) dan berkurang pada fokus pelaksanaannya. Hal-hal yang dilakukan COBIT adalah :

• Meningkatkan efisiensi dan efektivitas TI,

• Membantu TI dalam memahami kebutuhan bisnis,

• Menempatkan praktik untuk kebutuhan bisnis seefisien mungkin,

• Memastikan keselarasan antara bisnis dengan TI,

• Membantu eksekutif dalam memahami dan mengelola investasi TI sepanjang masa hidupnya.

6.4 Manfaat Penerapan COBIT

Adapun manfaat penerapan implementasi COBIT adalah :

• Merupakan bahasa umum untuk eksekutif, manajemen, dan staf TI.

• Pandangan tentang apa yang dilakukan TI & dapat dipahami manajemen.

• Pemahaman tentang bagaimana bisnis dan TI dapat bekerja sama.

• Penyelarasan yang lebih baik yang berdasarkan pada fokus organisasi.

• Kualitas layanan TI yang lebih baik.

• Peningkatan efisiensi dan optimalisasi biaya.

• Mengurangi risiko operasional.

• Manajemen TI yang lebih efektif.

• Memperjelas pengembangan kebijakan.

• Memicu lebih banyaknya audit yang efisien dan berhasil.

• Memperjelas kepemilikan dan tanggung jawab, berdasarkan

orientasi proses.

6.5 Target User COBIT

Menurut ISACA, COBIT utamanya ditargetkan untuk kelompok berikut :

• Manajer

Manajer sebagai pihak yang memegang tanggung jawab eksekutif dalam operasi perusahaan membutuhkan informasi untuk mengendalikan operasi di lingkup internal dan mengarahkan proses bisnis. COBIT dapat membantu manajer bisnis dan manajer TI untuk menyeimbangkan risiko dan mengendalikan investasi di dalam lingkungan TI yang seringkali tidak dapat ditebak.

• User (Pengguna Akhir)

COBIT menawarkan sebuah framework untuk memperoleh keyakinan pada keamanan dan pengendalian layanan TI yang disediakan baik oleh pihak internal maupun eksternal organisasi.

• Auditor

COBIT membantu auditor untuk memberikan struktur dan memperkuat opini mereka dan menyediakan saran untuk manajemen bagaimana cara meningkatkan pengendalian internal.

• Konsultan Bisnis dan TI

Konsultan bisnis dan TI dapat memberikan pengetahuan mengenai framework dan metode dalam TI kepada sebuah organisasi, sekaligus menyediakan saran kepada manajemen bisnis dan TI dalam meningkatkan tata kelola TI.

• Profesional Manajemen Layanan TI (IT Service Management Professionals)

COBIT membantu untuk meningkatkan manajemen layanan TI dengan menyediakan sebuah framework yang mencakup siklus hidup yang komplit dari sistem dan layanan TI.

6.6 COBIT dan Tujuan Bisnis

Menurut Sarno (2009: 19) . COBIT mendefinisikan tujuan bisnis terkait dengan aktivitas teknologi informasi yang umumnya ada di perusahaan. Pada kerangka kerja COBIT hanya menjelaskan tujuan-tujuan bisnis yang berkaitan dengan proses teknologi informasi. Demi memudahkan proses kontrol, COBIT mengelompokkan tujuan tersebut ke dalam perspektif kinerja *Balanced Scorecard* seperti terlihat dalam tabel 6.1 (ITGI, COBIT 4.1, 2007). Perusahaan/organisasi mungkin tidak memiliki semua tujuan bisnis seperti yang dikelompokkan dalam tabel tersebut. Dalam penyusunan tujuan bisnis, perusahaan dapat memilih yang sesuai dengan karakteristik organisasinya masing-masing. Pemilihan tujuan bisnis dapat dilakukan dengan mendefinisikan proses bisnis utama maupun bisnis pendukung organisasi terlebih dahulu.

Tabel 6.1 Tujuan Bisnis dalam COBIT

Perspektif Kinerja	No.	Tujuan Bisnis
Perspektif Keuangan	1.	Penyediaan pengembalian investasi yang baik dari bisnis yang dibangkitkan teknologi informasi.
	2.	Pengelolaan resiko bisnis yang terkait dengan teknologi informasi.
	3.	Peningkatan transparansi dan tata kelola perusahaan.
Perspektif Pelanggan	4.	Peningkatan layanan dan orientasi terhadap pelanggan.
	5.	Penawaran produk dan jasa yang kompetitif.
	6.	Penentuan ketersediaan dan kelancaran layanan.
	7.	Penciptaan ketangkasan (*agility*) untuk menjawab permintaan bisnis yang berubah.
	8.	Pencapaian optimasi biaya dari penyampaian layanan.

	9.	Perolehan informasi yang bermanfaat dan handal untuk pembuatan keputusan strategis.
Perspektif Proses Bisnis/ Internal	10.	Peningkatan dan pemeliharaan fungsionalitas proses
	11.	Penurunan biaya proses.
	12.	Penyediaan kepatutan terhadap hukum eksternal, regulasi dan kontrak.
	13.	Penyediaan kepatutan terhadap kebijakan internal.
	14.	Pengelolaan perubahan bisnis.
	15.	Peningkatan dan pengelolaan produktivitas operasional dan staf.
Perspektif Pembelajaran & Pertumbuhan	16.	Pengelolaan inovasi produk dan bisnis.
	17.	Perolehan dan pemeliharaan karyawan yang cakap

6.7 Tujuan Teknologi Informasi

Tujuan diluncurkan COBIT adalah untuk mengembangkan, melakukan riset dan mempublikasikan suatu standar teknologi informasi yang diterima umum dan selalu *up to date* untuk digunakan dalam kegiatan bisnis sehari-hari.

Dengan bahasa lain, COBIT dapat pula dikatakan sebagai sekumpulan dokumentasi *best practices* untuk IT governance yang dapat membantu auditor, manajemen and pengguna *(user)* untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol dan permasalahan-permasalahan teknis melalui pengendalian terhadap masing-masing dari 34 proses IT, meningkatkan tingkatan kemapanan proses dalam IT dan memenuhi ekspektasi bisnis dari IT. COBIT mampu menyediakan bahasa yang umum sehingga dapat dipahami oleh semua pihak. Adopsi yang cepat dari COBIT di seluruh dunia dapat dikaitkan dengan semakin besarnya perhatian yang diberikan terhadap *corporate governance* dan kebutuhan perusahaan agar mampu berbuat lebih dengan sumber daya yang sedikit meskipun ketika terjadi kondisi ekonomi yang sulit.

Fokus utama COBIT adalah harapan bahwa melalui adopsi COBIT ini perusahaan akan mampu meningkatkan nilai tambah melalui penggunaan TI dan mengurangi resiko-resiko inheren yang teridentifikasi didalamnya.

Untuk mengetahui keterkaitan antara tujuan bisnis dengan tujuan teknologi informasi, maka perlu dipahami terlebih dahulu keseluruhan tujuan teknologi informasi yang telah didefinisikan dan diklasifikasikan pada kerangka kerja COBIT seperti yang terlihat pada tabel 6.2 (ITGI, COBIT 4.1, 2007). Pemetaan tujuan teknologi informasi tersebut dapat dijadikan acuan bagi perusahaan/ organisasi dalam menerjemahkan kebutuhan bisnis akan ketersediaan teknologi informasi. Perlu diketahui bahwa tujuan bisnis yang dipaparkan hanya merupakan tujuan yang terkait atau yang dapat membangkitkan bisnis.

Tabel 6.2 Tujuan Teknologi Informasi dalam COBIT

No.	Tujuan Teknologi Informasi
1.	Respon terhadap kebutuhan bisnis yang selaras dengan strategi bisnis.
2.	Respon terhadap kebutuhan tata kelola yang sesuai dengan arahan direksi.
3.	Kepastian akan kepuasan pengguna akhir dengan penawaran dan tingkatan layanan.
4.	Pengoptimasian dari penggunaan informasi.
5.	Penciptaan teknologi informasi yang tangkas (*IT Agility*).
6.	Pendefinisian bagaimana kebutuhan fungsional bisnis dan kontrol diterjemahkan dalam solusi otomatis yang efektif dan efisien.
7.	Perolehan dan pemeliharaan sistem aplikasi yang standar dan terintegrasi.
8.	Perolehan dan pemeliharaan infrastruktur teknologi informasi yang strandar dan terintegrasi.
9.	Perolehan dan pemeliharaan kemampuran teknologi informasi sebagai
10.	Jaminan akan kepuasan yang saling menguntungkan dengan pihak ketiga.

11.	Jaminan akan konsistensi terhadap integrasi aplikasi ke dalam proses bisnis.
12.	Jaminan transparansi dan pemahaman terhadap biaya teknologi informasi, keuntungan, strategi, kebijakan dan tingkatan layanan.
13.	Jaminan akan penggunaan dan kinerja dari aplikasi serta solusi teknologi yang sesuai.
14.	Kemampuan memberikan penjelasan dan perlindungan terhadap aset-aset teknologi informasi.
15.	Pengoptimasian infrastruktur, sumber daya dan kemampuan teknologi informasi.
16.	Pengurangan terhadap ketidaklengkapan dan pengolahan kembali dari solusi dan penyampaian layanan.
17.	Perlindungan terhadap pencapaian sasaran teknologi informasi.
18.	Penentuan kejelasan mengenai resiko dari dampak bisnis terhadap sasaran dan sumber daya teknologi informasi.
19.	Jaminan bahwa informasi yang kritis dan rahasia disembunyikan dari pihak-pihak yang tidak berkepentingan.
20.	Kepastian bahwa transaksi bisnis yang secara otomatis dan pertukaran informasi dapat dipercaya.
21.	Jaminan bahwa layanan dan infrastruktur teknologi informasi dapat sepatutnya mengatasi dan memulihkan kegagalan karena eror, serangan yang disengaja maupun bencana alam.
22.	Kepastian akan minimnya dampak bisnis dalam kejadian gangguan layanan atau perubahan teknologi informasi.

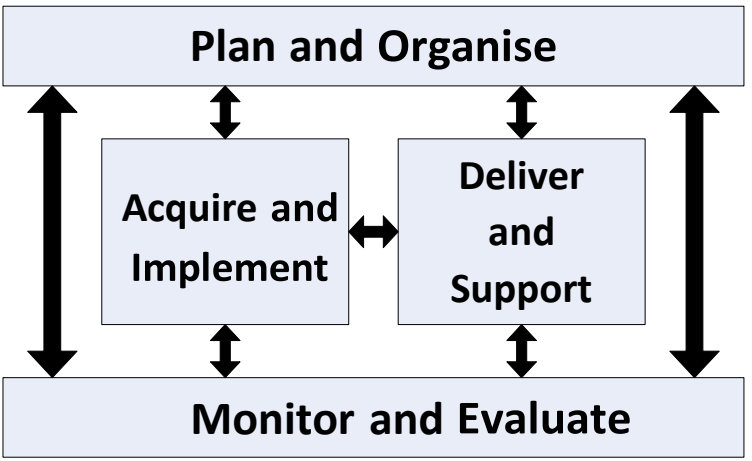
23.	Jaminan bahwa layanan teknologi informasi yang tersedia sesuai dengan yang dibutuhkan.
24.	Peningkatan terhadap efisiensi biaya teknologi informasi dan kontribusinya terhadap keuntungan bisnis.
25,	Penyampaian rencangan tepat waku dan sesuai dengan kualitas standar maupun anggaran biaya.
26.	Pemeliharaan terhadap integritas informasi dan pemrosesan infrastruktur.
27.	Kepastian bahwa teknologi informasi selaras degan regulasi dan hokum yang berlaku.
28.	Jaminan bahwa teknologi informasi dapat menunjukkan kualitas layanan yang efisien dalam hal biaya, perbaikan yang berkelanjutan dan kesiapan terhadap perubahan di masa mendatang

Menurut Alindita (2008), *IT Governance* adalah sistem yang mengatur dan mengendalikan seluruh proses teknologi informasi perusahaan/organisasi yang strukturnya akan menetapkan pendistribusian hak dan tanggung jawab antara pihak-pihak yang terlibat juga berisikan peraturan serta strategi yang ditetapkan perusahaan/ organisasi.

Menurut Indrajit (2004). *Information System Audit and Control Association* (ISACA) memperkenalkan sebuah kerangka untuk mengelola *IT Governance* di sebuah perusahaan yang dikenal dengan nama COBIT .

Menurut Putra (2009). Pada dasarnya COBIT dikembangkan untuk membantu memenuhi berbagai kebutuhan manajemen terhadap informasi dengan menjembatani kesenjangan antara resiko bisnis, kontrol dan masalah teknik.

Menurut Surendro (2004: 243) karakteristik utama kerangka kerja COBIT adalah pengelompokkan aktivitas teknologi informasi dalam empat *domain*, yaitu *Plan and Organise* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS) serta *Monitor and Evaluate* (ME). *Domain* PO menyediakan arahan untuk mewujudkan solusi penyampaian (AI) dan penyampaian jasa (DS). AI menyediakan solusi dan menyalurkannya untuk dapat diubah menjadi jasa. Sementara DS menerima solusi tersebut dan membuatnya lebih bermanfaat bagi pengguna akhir. Sedangkan ME memonitor seluruh proses untuk kepastian bahwa arahan yang diberikan telah diikuti. Keterkaitan keempat *domain* COBIT dapat dilihat dalam gambar 6.1 (ITGI, COBIT 4.1, 2007).



Gambar 6.1 Keterkaitan *Domain* dalam COBIT

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

1. *Plan and Oganise* (PO)

Membahas mengenai strategi, taktik, dan pengidentifikasian teknologi informasi dalam mendukung tercapainya tujuan bisnis. *Domain* PO ini terdiri dari 10 (sepuluh) proses teknologi informasi seperti terlihat pada tabel 6.3.

Tabel 6.3 Proses Teknologi Informasi dalam *Domain* PO

PO1	Mendefinisikan rencana strategis TI
PO2	Mendefinisikan arsitektur informasi
PO3	Menentukan arahan teknologi
PO4	Mendefinisikan proses TI, organisasi dan keterhubungannya
PO5	Mengelola investasi TI
PO6	Mengkomunikasikan tujuan dan arahan manajemen
PO7	Mengelola sumber daya TI
PO8	Mengelola kualitas
PO9	Menaksir dan mengelola resiko TI
PO10	Mengelola proyek

2. *Acquire and Implement* (AI)

Pada domain *Acquire and Implement* sebuah solusi teknologi informasi perlu diidentifikasikan, dikembangkan, diimplementasikan dan diintegrasikan ke dalam proses bisnis. *Domain* AI ini terdiri dari 7 (tujuh) proses teknologi informasi seperti terlihat pada tabel 6.4.

Tabel 6.4 Proses Teknologi Informasi dalam *Domain* AI

AI1	Mengidentifikasi solusi otomatis
AI2	Memperoleh dan memelihara software aplikasi
AI3	Memperoleh dan memelihara infrastruktur teknologi
AI4	Memungkinkan operasional dan penggunaan
AI5	Memenuhi sumber daya TI
AI6	Mengelola perubahan
AI7	Instalasi dan akreditasi solusi beserta perubahaannya

3. *Deliver and Support* (DS)

Domain ini fokus pada aspek penyampaian teknologi informasi terhadap dukungan dan layanan teknologi informasi mencakup dukungan dan layanan teknologi informasi pada bisnis, mulai dari penanganan keamanan dan kesinambungan, dukungan bagi pengguna serta manajemen data. *Domain* DS ini terdiri dari 13 (tiga belas) proses teknologi informasi seperti terlihat pada tabel 6.5.

Tabel 6.5 Proses Teknologi Informasi dalam *Domain* DS

DS1	Mendefinisikan dan mengelola tingkat layanan
DS2	Mengelola layanan pihak ketiga
DS3	Mengelola kinerja dan kapasitas
DS4	Memastikan layanan yang berkelanjutan
DS5	Memastikan keamanan system
DS6	Mengidentifikasikan dan mengalokasikan biaya
DS7	Mendidik dan melatih pengguna
DS8	Mengelola *service desk* dan insiden
DS9	Mengelola konfigurasi
DS10	Mengelola permasalahan
DS11	Mengelola data
DS12	Mengelola lingkungan fisik

DS13	Mengelola operasi

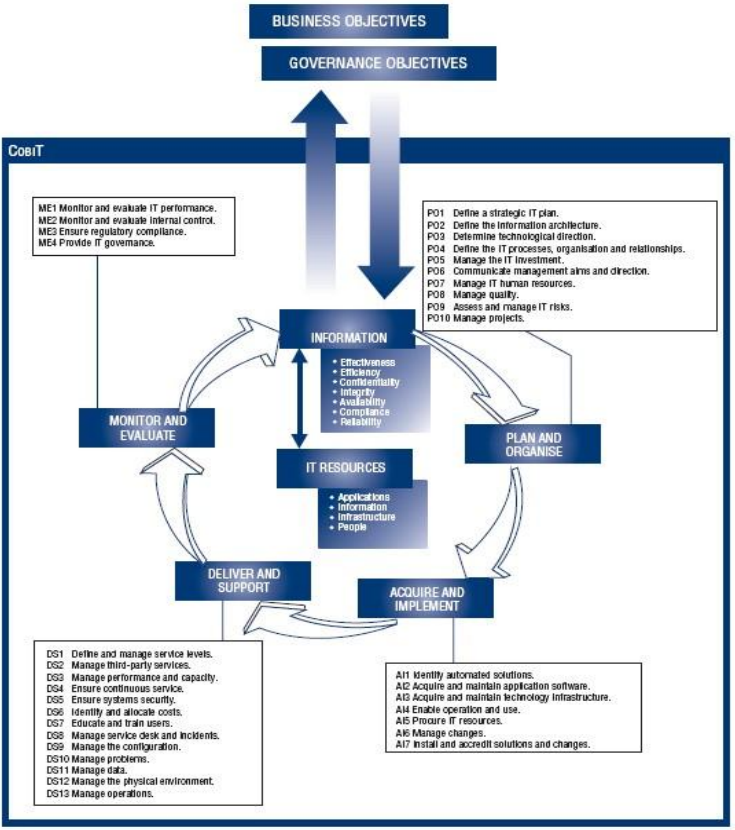
4. *Monitor and Evaluate* (ME)

Pada domain ini akan ditekankan kepada pentingnya semua proses teknologi informasi perlu diakses secara berkala untuk menjaga kualitas dan kesesuaian dengan standar yang telah ditetapkan. *Domain* ME ini terdiri dari 4 (empat) proses teknologi informasi seperti terlihat pada tabel 6.6.

Tabel 6.6 Proses Teknologi Informasi dalam *Domain* ME

ME1	Mengawasi dan mengevaluasi kinerja TI
ME2	Mengawasi dan mengevaluasi kontrol internal
ME3	Memastikan pemenuhan terhadap kebutuhan eksternal
ME4	Menyediakan tata kelola TI

COBIT memberikan satu langkah praktis melalui *domain* dan *framework* yang menggambarkan aktivitas teknologi informasi dalam suatu struktur dan proses yang disesuaikan. Gambaran kerangka kerja (*framework*) COBIT secara keseluruhan dapat dilihat pada gambar berikut :



Gambar 6.2 Kerangka Kerja COBIT 4.1

(Sumber: *Information Technology Governace Institute*, 2007)

ITGI (*Information Technology Governance Institue*, 2007) memberikan pemetaan tujuan teknologi informasi dan tujuan bisnis berdasarkan standar COBIT menjadi 28 tujuan teknologi informasi dan 17 tujuan bisnis.

Gambar 6.3 Pemetaan Tujuan Bisnis dan Tujuan Teknologi Informasi berdasarkan COBIT

No.	Tujuan Bisnis	Tujuan Teknologi Informasi						
1.	Penyediaan pengembalian investasi yang baik dari bisnis yang dibangkitkan teknologi informasi.	24						
2.	Pengelolaan resiko bisnis yang terkait dengan teknologi informasi.	2	14	17	18	19	21	22
3.	Peningkatan transparansi dan tata kelola perusahaan.	2	18					
4.	Peningkatan layanan dan orientasi terhadap pelanggan.	3	23					
5.	Penawaran produk dan jasa yang kompetitif.	5	24					
6.	Penentuan ketersediaan dan kelancaran layanan.	10	16	22	23			

7.	Penciptaan ketangkasan (*agility*) untuk menjawab permintaan bisnis yang berubah.	1	5	25				
8.	Pencapaian optimasi biaya dari penyampaian layanan.	7	8	10	24			
9.	Perolehan informasi yang bermanfaat dan handal untuk pembuatan keputusan strategis.	2	4	12	20	26		
10.	Peningkatan dan pemeliharaan fungsionalitas proses bisnis.	6	7	11				
11.	Penurunan biaya proses.	7	8	13	15	24		
12.	Penyediaan kepatutan terhadap hokum eksternal, regulasi dan kontrak.	2	19	20	21	22	26	27
13.	Penyediaan kepatutan terhadap kebijakan internal.	2	13					
14.	Pengelolaan perubahan bisnis.	1	5	6	11	28		

15.	Peningkatan dan pengelolaan produktivitas operasional dan staf.	7	8	11	13			
16.	Pengelolaan inovasi produk dan bisnis.	5	25	28				
17.	Perolehan dan pemeliharaan karyawan yang cakap dan termotivasi.	9						

Sumber: Sarno, 2009: 57-59

Menurut (Gondodiyoto, 2007). Suatu organisasi dapat dianggap sukses membangun teknologi informasi dalam suatu kerangka sistem informasi yang lengkap apabila telah memenuhi kriteria ukuran informasi Kriteria ukuran informasi berdasarkan kerangka kerja COBIT dapat dilihat pada tabel 6.8:

Gambar 6.4 Kriteria Ukuran Informasi berdasarkan COBIT

Efektif	Jika sistem informasi sesuai dengan kebutuhan pemakai.
Efisien	Jika penggunaan sumberdaya optimal.
Kerahasiaan	Memfokuskan proteksi terhadap informasi yang penting dari orang yang tidak memiliki hak otoritas.

Integritas	Berhubungan dengan akurasi dan kelengkapan informasi.
Ketersediaan	Berkaitan dengan informasi yang tersedia pada saat yang diperlukan dalam proses bisnis.
Pemenuhan	Sesuai kebijakan organisasi, aturan hokum dan peraturan yang berlaku.
Keandalan	Terkait dengan ketentuan kecocokan informasi untuk mengoperasikan perusahaan, pelaporan dan pertanggungjawaban.

Menurut Sarno (2009: 147-163). Pengukuran informasi melalui audit teknologi informasi dengan mengacu pada contoh yang baik (*best prastice*) berdasarkan kerangka kerja COBIT.

6.8 Stakeholder

COBIT dirancang untuk digunakan oleh tiga pengguna berbeda yaitu :

a. Manajemen

Dengan penerapan COBIT ,manajemen dapat terbantu dalam proses penyeimbangan resiko dan pengendalian investasi dalam lingkungan IT yang tidak dapat diprediksi.

b. User

Pengguna dapat menggunakan COBIT untuk memperoleh keyakinan atas layanan keamanan dan pengendalian IT yang disediakan oleh pihak internal atau pihak ketiga.

c. Auditor

Dengan penerapan COBIT, auditor dapat memeproleh dukungan dalam opini yang dihasilkan dan/atau untuk memberikan saran kepda manajemen atas pengendalian internal yang ada.

6.9 Overview COBIT

Secara singkat dapat COBIT memiliki kerangka kerja yang terdiri atas beberapa arahan *(guindelines*), yakni :

6.9.1 Control Objectives

COBIT terdiri atas 4 tujuan pengendalian tingkat-tinggi *(high-level control objectives)*, yaitu :

1. Planning and Organization

Mencakup strategi, taktik dan perhatian atas identifikasi bagaimana IT secara maksimal dapat berkontribusi dalam pencapaian tujuan bisnis.Selain itu, realisasi dari visi strategis perlu direncanakan, dikomunikasikan, dan dikelola untuk berbagi perspektif ynag berbeda.Terakhir, sebuah pengorganisasian yang baik serta infrastruktur teknologi harus ditempatkan di tempat yang semestinya.Proses dalam domain ini adalah:

1. Menetapkan rencana strategi IT
2. Menetapkan susunan informasi

3. Menetapkan kebijakan teknologi

4. Menetapkan hubungan dan organisasi IT

5. Mengelola investasi IT

6. Mengkomunikasikan arah dan tujuan manajemen

7. Mengelola sumberdaya manusia

8. Memastikan pemenuhan keperluan pihak eksternal

9. Menaksir risiko

10. Mengelola proyek

11. Mengelola kualitas

2. Acqusition and Implementation

Untuk merealisasikan stategi IT, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan, dan terintegrasi ke dalam proses bisnis. Selain itu, perubahan serta pemeliharaan sistem yang ada harus di cakup dalam domain ini untuk memastikan bahwa siklus hidup akan terus berlangsung untuk sistem-sistem ini.Langkah-langkah domain ini adalah :

1. Mengidentifikasi solusi terotomatisasi

2. Mendapatkan dan memelihara software aplikasi

3. Mengembangkan dan memelihara prosedur

4. Memasang dan mengakui sistem

5. Mengelola perubahan

3. Delivery and Support

Domain ini berfokus utama pada aspek penyampaian/pengiriman dari IT.Domain ini mencakup area-area seperti pengoperasian aplikasi-aplikasi dalam sistem IT dan hasilnya, dan juga proses dukungan yang memungkinkan pengoperasian sistem IT tersebut dengan efektif dan efisien. Proses dukungan ini termasuk isu/masalah keamanan dan juga pelatihan. Proses dalam domain ini adalah :

a. Menetapkan dan mengelola tingkat pelayaran

b. Mengelola pelayanan kepada pihak lain

c. Mengelola kinerja dan kapasitas

d. Memastikan pelayanan yang kontinyu

e. Memastikan keamanan sistem

f. Melakukan identifikasi terhadap atribut biaya

g. Memberi pelatihan kepada user

h. Melayani konsumen IT

i. Mengelola konfigurasi/susunan

j. Mengelola masalah dan kecelakaan k. Mengelola data

l. Mengelola fasilitas

m. Mengelola operasi

4. Monitoring and Evaluating

Semua proses IT perlu dinilai secara teratur sepanjang waktu untuk menjaga kualitas dan pemenuhan atas syarat pendendalian. Domain ini menunjuk pada perlunya pengawasan manajemen atas proses pengendalian dalam organisasi serta penilaian independen yang dilakukan baik auditor internal maupun eksternal atau diperoleh dari sumber-sumber alternatif lainnya. Proses dalam domain ini sebagai berikut :

1. Memonitor proses

2. Menaksir kecukupan pengendalian internal

3. Mendapatkan kepastian yang independen

6.9.2 Auditor Guidelines COBIT

Berisi sebanyak 318 tujuan – tujuan pengendalian yang bersifat rinci *(detailed control objectives*) untuk membantu para auditor dalam memberikan management assurance dan/atau saran perbaikan.

6.9.3 Management Guidelines COBIT

Berisi arahan, baik secara umum maupun spesifik , mengenai apa saja yang mesti dilakukan.

Kerangka kerja COBIT juga memasukkan hal-hal-berikut ini :

1. Maturity Models : untuk memetakan *status maturity* proses-proses TI (dalam 0-5) dibandingkan dengan “the best in the class in the industry”dan juga international besr practices.

2. Critical Success Factors (CSFs) : arahan implementasi bagi manajemen agar dapat melakukan kontrol atas proses Ti.

3. Key Goal Indicators (KGIs) : kinerja proses-proses TI sehubungan dengan *business requirements.*

4. Key Performance Indicators (KPIs) : kinerja proses-proses TI sehubungan dengan *process goal*.

6.9.4 Konsep Pengendalian

COBIT mengadopsi definisi pengendalian dari COSO yaitu : ‘kebijakan, prosedur, dan praktik, dan struktur organisasi yang dirancang untuk memberikan keyakinan yang wajar bahwa tujuan organisasi dapat dicapai dan hal-hal yang tidak diinginkan dapat dicegah atau dideteksi dan diperbaiki”. Sedangkan dalam tujuan pengendalian, COBIT mendefinisikannya sebagai : “Suatu pernyataan atas hasil yang diinginkan atau tujuan yang ingin dicapai dengan mengimplementasikan prosedur pengendalian dalam aktivitas TI tertentu”.

COBIT melihat pengendalian dala tiga dimensi berbeda yaitu sumber IT, proses IT, dan kriteria informasi IT. Dimensi pertama mencakup semua asset IT suatu perusahaan, yang dapat diidentifikasikan sebagai berikut :

a. Data

b. Sistem aplikasi

c. Teknologi

d. Fasilitas

e. Manusia

Proses IT sebagai dimensi kedua dari COBIT terdiri dari tiga segmen, yaitu : domains, proses, dan aktivitas. Sedangkan dalam dimensi ketiganya COBIT menetapkan kriteria informasi yang berguna dalam mendukung tercapainya tujuan organisasi dengan merujuk pada kebutuhan informasi di organisasi atau perusahaan. COBIT mengkombinasikan beberapa prinsip penyusunan informasi berdasarkan model-model yang sudah ada, dan merumuskan kedalam tiga kategori utama, yaitu : *quality, fiduciary responsibility dan security*. Tiga kategori ini kemudian diuraikan lebih lanjut dalam kriteria-kriteria sebagai berikut :

a. Efektifitas

b. Efisiensi

c. Kerahasiaan

d. Integritas

e. Ketersediaan

f. Kepatuhan

g. Keandalan

6.10 Maturity Models

Maturity model adalah suatu cara untuk mengukur bagaimana suatu proses manajemen telah dilakukan. Secara umum, maturity model berguna untuk memampukan perusahaan melakukan *branch marking* dan identifikasi pembaharuan yang dilakukan. Keuntungan dari pendekatan *maturity model* ini adalah kemudahan bagi manajemen untuk menempatkan dirinya pada skala tertentu dan menghargai apa yang perlu diikutsertakan jika peningkatan performa diperlukan.

Model akan membantu para profesional untuk menjelaskan kepada para manajer dimana manajemen proses TI muncul dan menetapkan target dimana perusahaan harus ada. *Maturity* yang dapat dipengaruhi oleh *business objective* perusahaan, lingkungan operasional, dan praktik industri. Setiap proses pada CobIT terdapat skala penilaian berdasarkan deskripsi *maturity model* secara umum dibawah ini :

1) Level 0 – *Non Existent*

Benar-benar kurang proses yang sepenuhnya diketahui perusahaan. Perusahaan bahkan belum mengenali isu yang harus dihadapi.

2) Level 1 – *Initial*

Ada bukti bahwa perusahaan telah menganalisa isu-isu yang ada dan harus diselesaikan. Namun tidak ada proses yang terstandarisasi dan ada beberapa pendekatan yang bersifat *ad-hoc* yang cenderung diaplikasikan pada kasus individual atau kasus per kasus.

3) Level 2 – *Repeatable*

Proses telah dikembangkan pada tahap dimana prosedur yang sama diikuti oleh beberapa orang yang berbeda pada saat melakukan tugas yang sama. Tidak ada pelatihan formal atau komunikasi setiap individu. Ada kecenderungan untuk bertumpu pada pengetahuan individu sehingga kesalahan cenderung terjadi.

4) Level 3 – *Defined Process*

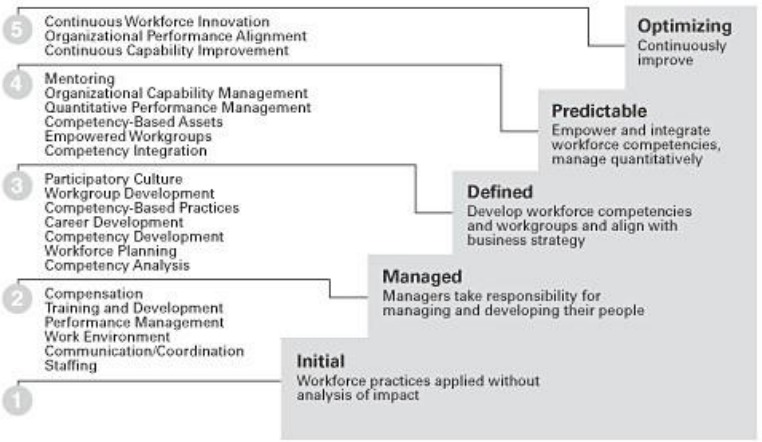
Prosedur telah distandarisasi dan didokumentasi serta dikomunikasikan melalui pelatihan. Namun hal ini diserahkan pelaksanaannya kepada masing-masing individu untuk mengikutinya atau tidak, dan penyimpangan sulit untuk dideteksi.

5) Level 4 – *Managed*

Adalah mungkin untuk memonitor dan mengukur kepatuhan terhadap prosedur- prosedur dan melakukan suatu tindakan ketika suatu proses tidak sesuai.

6) Level 5 – *Optimised*

Proses telah diperbaiki pada tingkat *best practice* berdasarkan pada hasil dari peningkatan yang berkelanjutan dan maturity modelling dengan perusahaan lain. TI digunakan pada cara yang terintegrasi ke arus kerja yang telah terotomatisasi, menyediakan perangkat untuk meningkatkan kualitas dan efektivitas sehingga membuat perusahaan cepat beradaptasi.



Gambar 6.5 Skala Penilaian proses pada CobIT

BAB 7

Control Ojective for Information and Related Technology (COBIT) versi 4.1

Framework COBIT 4.1 merupakan teknik yang dapat membantu dalam identifikasi TI *control issue* bagi auditor, sedangkan untuk TI users untuk memperoleh keyakinan atas sistem aplikasi yang dipergunakan, dan manajer untuk mengambil keputusan investasi di bidang TI serta infrastrukturnya. Secara garis besar audit menggunakan COBIT 4.1 memiliki prinsip dasar *Business Requirement*, *IT resources*, dan *IT Process*. Dengan dilakukannya audit TI diharapkan dapat memberikan dampak positif bagi TI organisasi dalam memperbaiki mekanisme, integritas, efektivitas dan efisiensi sistem (ITGI, 2017).

Berikut adalah manfaat dari menerapkan COBIT 4.1 sebagai kerangka tata kelola TI (ITGI, 2007) :

- Pengelarasan yang lebih baik, berdasarkan focus bisnis.
- Pandanangan dipahami oleh manajemen TI.
- Kepemilikan dan tanggung jawab yang jelas, berdasarkan orientasi proses.
- Penerimanaan umum dengan pihak ketiga dan regulator.
- Pemahaman kepada semua pihak yang berkepentingan, menggunakan bahasa yang umum.
- Pemenuhan persyaratan COSO untuk lingkungan pengendalian TI.

7.1. Visi Misi COBIT

Adapun visi misi COBIT adalah :

- Visi COBIT adalah sebagai model untuk penguasaan TI.
- Misi COBIT adalah melakukan penelitian, pengembangan, publikasi, dan promosi terhadap control objectives yang diterima di lingkungan internasional dan digunakan sehari-hari oleh manajer dan auditor.

7.2. Fokus CoBIT

Fokus COBIT lebih kepada *control* (pengendalian) dan berkurang pada fokus pelaksanaannya.

Hal-hal yang dilakukan COBIT adalah :

- Meningkatkan efisiensi dan efektivitas TI,
- Membantu TI dalam memahami kebutuhan bisnis,
- Menempatkan praktik untuk kebutuhan bisnis seefisien mungkin,
- Memastikan keselarasan antara bisnis dengan TI,
- Membantu eksekutif dalam memahami dan mengelola investasi TI sepanjang masa hidupnya.

7.3. Manfaat Penerapan COBIT

Adapun manfaat penerapan implementasi COBIT adalah :

- Merupakan bahasa umum untuk eksekutif, manajemen, dan staf TI.
- Pandangan tentang apa yang dilakukan TI & dapat dipahami manajemen.
- Pemahaman tentang bagaimana bisnis dan TI dapat bekerja sama.
- Penyelarasan yang lebih baik yang berdasarkan pada fokus organisasi.

- Kualitas layanan TI yang lebih baik.
- Peningkatan efisiensi dan optimalisasi biaya.
- Mengurangi risiko operasional.
- Manajemen TI yang lebih efektif.
- Memperjelas pengembangan kebijakan.
- Memicu lebih banyaknya audit yang efisien dan berhasil.
- Memperjelas kepemilikan dan tanggung jawab, berdasarkan orientasi proses.

7.4. Target User COBIT

Menurut ISACA, COBIT utamanya ditargetkan untuk kelompok berikut :

- Manajer

  Manajer sebagai pihak yang memegang tanggung jawab eksekutif dalam operasi perusahaan membutuhkan informasi untuk mengendalikan operasi di lingkup internal dan mengarahkan proses bisnis. COBIT dapat membantu manajer bisnis dan manajer TI untuk menyeimbangkan risiko dan mengendalikan investasi di dalam lingkungan TI yang seringkali tidak dapat ditebak.

- *User* (Pengguna Akhir)

  COBIT menawarkan sebuah *framework* untuk memperoleh keyakinan pada keamanan dan pengendalian layanan TI yang disediakan baik oleh pihak internal maupun eksternal organisasi.

- Auditor

  COBIT membantu auditor untuk memberikan struktur dan memperkuat opini mereka dan menyediakan saran untuk

manajemen bagaimana cara meningkatkan pengendalian internal.

- Konsultan Bisnis dan TI

  Konsultan bisnis dan TI dapat memberikan pengetahuan mengenai *framework* dan metode dalam TI kepada sebuah organisasi, sekaligus menyediakan saran kepada manajemen bisnis dan TI dalam meningkatkan tata kelola TI.

- Profesional Manajemen Layanan TI (*IT Service Management Professional*)

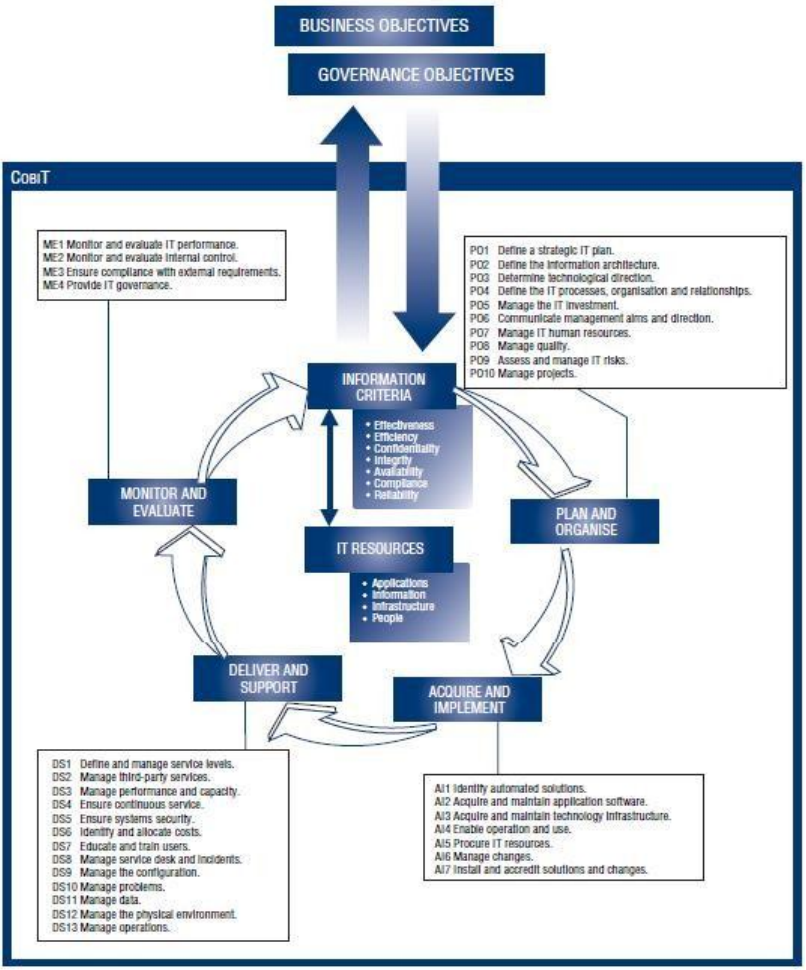
  COBIT membantu untuk meningkatkan manajemen layanan TI dengan menyediakan sebuah *framework* yang mencakup siklus hidup yang komplit dari sistem dan layanan TI.

7.5. Kerangka Kerja COBIT 4.1

Kerangka kerja pengendalian COBIT terdiri dari empat hal, yakni :

- Mengaitkannya dengan tujuan organisasi,
- Mengorganisasikan aktivitas TI ke dalam model proses,
- Mengidentifikasi sumber daya utama TI untuk melakukan percepatan,

Mendefinisikan tujuan pengendalian manajemen untuk dipertimbangkan.



Gambar 7.1 Framework COBIT 4.1

Kerangka kerja COBIT yang terdiri dari 34 proses TI yang terbagi ke dalam 4 domain pengelolaan, yaitu (Surendro, 2009) :

- Plan and Organise (PO)

Domain ini mencakup strategi dan taktik, dan perhatian pada identifikasi cara TI dapat berkontribusi terbaik pada pencapaian objektif bisnis. Menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi organisasi.

- *Acquire and Implement* (AI)

  Domain ini menitikberatkan pada proses pemilihan, pengadaaan dan penerapan TI yang digunakan. Pelaksanaan strategi yang telah ditetapkan, harus disertai solusi-solusi TI, diimplementasikan dan diintegrasikan ke dalam proses bisnis organisasi.

- *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.

- *Monitor and Evaluate* (ME)

  Domain ini menitikberatkan pada proses pengawasan pengelolaan TI pada organisasi di setiap kendali-kendali yang diterapkan pada proses TI. Domain ini fokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan internal dan eksternal.

Kriteria kontrol untuk informasi sebagaimana dikemukakan COBIT adalah (ITGI, 2007) :

- *Effectiveness* (efektivitas), terkait dengan informasi yang relevan dan berhubungan pada proses bisnis serta disampaikan juga secara tepat waktu, benar, konsisten, dan mudah.

- *Efficiency* (efisiensi), terkait dengan ketentuan informasi melalui penggunaan sumber daya secara optimal.

- *Confidentiality* (kerahasiaan), terkait dengan pengamanan terhadap informasi yang sensitif dari pihak yang tidak berhak.
- *Integrity* (integritas), terkait dengan keakuratan dan kelengkapan informasi serta validitasnya sesuai dengan nilai dan harapan bisnis.
- *Availbility* (ketersediaan), terkait dengan ketersediaan informasi pada saat kapanpun diperlukan oleh proses bisnis.
- *Compliance* (kepatuhan) terkait dengan kepatuhan pada hukum, regulasi, maupun perjanjian kontrak.
- *Reliability* (keandalan), terkait dengan penyediaan informasi yang tepat bagi manajemen untuk mendukung operasional suatu entitas dan menjalankan tanggungjawab tata kelolanya.

Untuk menganalisa dengan menggunakan COBIT 4.1 ada 4 domain yang perlu diperhatikan yaitu :

Domain PO (*Plan and Organize*)

Pada domain PO memfokuskan pada proses perencanaan dan penyelarasan TI (Teknologi Informasi) dengan strategi perusahaan, termasuk strategi, taktik dan identifikasi peran TI memberikan peran maksimal untuk mecapai tujuan bisnis suatu organisasi sehingga tercipta organisasi dengan infrastruktur TI dengan baik. Domain PO terdiri dari 10 sub proses dan 66 sub- sub proses pada tabel 7.1.

Tabel 7.1 Domain PO (Plan and Organize)

No	Domain	Sub-Domain
1	*PO1 Define a Strategic IT*	*PO1.1 IT Value Management* *PO1.2 Business IT Aligment* *PO1.3 Assement of Current Capability and Performance* *PO1.4 IT Strategic Plan* *PO1.5 IT Tactical Plans* *PO1.6 IT Portfolio Management*
2	*PO2 Define the Information Architecture*	*PO2.1 Enterprise Information Architecture Model* *PO2.2 Enterprise Data Dictionary and Syntax Rules* *PO2.3 Data Classification Scheme* *PO2.4 Integrity Management*
3	*PO3 Determine Technological Direction*	*PO3.1 Technological Direction Planning* *PO3.2 Technology Infrastructure Plan* *PO3.3 Monitor Future Trends and Regulations* *PO3.4 Technology Standart* *PO3.5 IT Architecture Board*
4	*PO4 Define the It Processes Organization and Relstionships*	*PO4.1 IT Proses Framework* *PO4.2 IT Strategy Committee* *PO4.3 IT Steering Committee* *PO4.4 Organisational Placement of the IT Function* *PO4.5 IT Organisational Structure* *PO4.6 Establisthment of Roles and Responsibilities* *PO4.7 Responsibilities for IT Quality Assurance*

No	Domain	Sub-Domain	
		PO4.8	*Responsibilities for Risk, Security and Compliance*
		PO4.9	*Data and System Ownership*
		PO4.10	*Supervision*
		PO4.11	*Segregation of Duties*
5	*PO5 Manage the IT Investment*	*PO5.1*	*Financial Management Framework*
		PO5.2	*Prioritisation Within It Budget*
		PO5.3	*IT Budgeting*
		PO5.4	*Cost Management*
		PO5.5	*Benefit Management*
6	*PO6 Communicate Management Aims and Direction*	*PO6.1*	*IT Policy and Control Environment*
		PO6.2	*Enterprise IT Risk and Control Framewor*
		PO6.3	*IT Policies Management*
		PO6.4	*Policy, Standard and Procedure Rollout*
		PO6.5	*Communication of IT Objectives and Direction*
7	*PO7 Manage It Human Resources*	*PO7.1*	*Personnel Recruitment and Retention*
		PO7.2	*Personnel Competencies*
		PO7.3	*Staffing og Roles*
		PO7.4	*Personnel Training*
		PO7.5	*Dependence Upon Individuals*
		PO7.6	*Personnel Clearance Procedures*
		PO7.7	*Employee Job Performance Evaluation*
		PO7.8	*Job Change and Termination*

No	Domain	Sub-Domain	
8	*PO8 Manage Quality*	*PO8.1*	*Quality Management System*
		PO8.2	*IT Standards and Quality Practices*
		PO8.3	*Development and Acquisition Standards*
		PO8.4	*Customer Focus*
		PO8.5	*Continuous Improvement*
		PO8.6	*Quality Measurement, Monitoring and Review*
9	*PO9 Assess and Manage IT Risk*	*PO9.1*	*IT Risk Management Framework*
		PO9.2	*Establishment of Risk Context*
		PO9.3	*Event Identification*
		PO9.4	*Risk Assessment*
		PO9.5	*Risk Response*
		PO9.6	*Maintenance and Monitoring of a Risk Action*
10	*PO10 Manage Projects*	*PO10.1*	*Programme Management Framework*
		PO10.2	*Project Management Framework*
		PO10.3	*Project Management Approach*
		PO10.4	*Stakeholder Commitment*
		PO10.5	*Project Scope Statement*
		PO10.6	*Project Phase Initiation*
		PO10.7	*Integrated Project Plan*
		PO10.8	*Project Resources*
		PO10.9	*Project Risk Management*
		PO10.10	*Project Quality Plan*
		PO10.11	*Project Change Control*

No	Domain	Sub-Domain
		PO10.12 *Project Planning of Assurance Methods* *PO10.13* *Project Performance Meansurement, Reporting and Monitoring* *PO10.14* *Project Closure*

Domain AI (Aquire and Implement)

Domain ini memfokuskan kepada kegiatan yang berkaitan dengan implementasi solusi teknologi informasi (TI) dan integritas terhadap proses bisnis dalam organisasi guna mewujudkan strategi TI, meliputi; perubahan-perubahan dan pemeliharaan yang diperlukan untuk sistem yang berjalan untuk memastikan *life cycle system* (alur hidup sistem) tetap terjaga. Domain AI terdiri dari 7 sub proses dan 40 sub-sub proses pada tabel 7.2.

Tabel 7.2 Domain AI (Aquire and Implement)

No	Domain	Sub-Domain
1	*AI1 identify Automated Solutions*	*AI1.1* *Definition and Maintenance of Business Functional and Technical Requitment* *AI1.2* *Risk Analysis Report* *AI1.3* *Feasibility Study and Formulation of Alternative Courses of Action* *AI1.4* *Requitments and Feasibility Decision and Approval*

No	Domain	Sub-Domain	
2	*AI2 Acquire and Maintain Application Software*	*AI2.1*	*High Level Design*
		AI2.2	*Detailed Design*
		AI2.3	*Application Control and Auditability*
		AI2.4	*Application Security and Availability*
		AI2.5	*Configuration and Implementation of Acquired Application Software*
		AI2.6	*Major Upgrades to Existing Systems*
		AI2.7	*Development of Appliction Software*
		AI2.8	*Software Quality Assurance*
		AI2.9	*Application Requirements Management*
3	*AI3 Acquire and Maintain Technology Infrastructure*	*AI3.1*	*Technology Infrastructure Acquisition Plan*
		AI3.2	*Infrastructure Resource Protection and Availability*
		AI3.3	*Infrastructure Maintenance*
		AI3.4	*Feasibility Test Environment*

No	Domain	Sub-Domain
4	*AI4 Enable Operation and Use*	*AI4.1 Planning for Operational Solution* *AI4.2 Knowledge Transfer to Business Management* *AI4.3 Knowledge Transfer to End Users* *AI4.4 Knowledge Transfer to Operations and Support Staff*
5	*AI5 Procure IT Resources*	*AI5.1 Procurement Control* *AI5.2 Supplier Contract Management* *AI5.3 Supplier Selection* *AI5.4 IT Resources Acquisition*
6	*AI6 Manage Changes*	*AI6.1 Change Standards and Procedures* *AI6.2 Impact Assement, Prioritisation and Authorisation* *AI6.3 Emergency Changes* *AI6.4 Change Status Tracking and Reporting* *AI6.5 Change Closure and Documentation*
7	*AI7 Install and Accredit Solutions and Changes*	*AI7.1 Training* *AI7.2 Test Plan* *AI7.3 Implentation Plan* *AI7.4 Test Environment* *AI7.5 System and Data Conversion* *AI7.6 Testing of Change*

No	Domain	Sub-Domain
		AI7.7 Final Acceptance Test *AI7.8 Promotion to Production* *AI7.9 Post Implementation Review*

Domain DS (Delivery and Support)

Bagian dari domain DS adalah proses pemenuhan layanan teknologi informasi (TI) dan keamanan sistem hingga keberlanjutan dari layanan, *training* (pelatihan) dan pendidikan untuk pengguna serta pemenuhan proses data. Domain DS terdiri dari 13 sub proses dan 71 sub-sub proses pada tabel 7.3.

Tabel 7.3 Domain DS (Delivery and Support)

No	Domain	Sub-Domain
1	*DS1 Define and Manage Service Levels*	*DS1.1 Service Level Management Framework* *DS1.2 Definition of Services* *DS1.3 Service Level Agreements* *DS1.4 Operating Level Agreements* *DS1.5 Monitoring and Reporting of Service Level Achievements* *DS1.6 Review of Service Level Agrements and Contracts*

No	Domain	Sub-Domain
2	*DS2 Manage Third Party Services*	*DS2.1 Indentification of All Supplier Relationships* *DS2.2 Supplier Relationship Management* *DS2.3 Supplier Risk Management* *DS2.4 Supplier Performance Monitoring*
3	*DS3 Manage Performance and Capacity*	*DS3.1 Performance and Capacity Planning* *DS3.2 Current Performance and Capacity* *DS3.3 Future Performance and Capacity* *DS3.4 IT Resources Availability* *DS3.5 Monitoring and Reporting*
4	*DS4 Ensure Continuous Service*	*DS4.1 IT Continuity Framework* *DS4.2 IT Continuity Plans* *DS4.3 Critical IT Resources* *DS4.4 Maintenance of the IT Continuity Plan* *DS4.5 Testing of the IT Continuity Plan* *DS4.6 IT Continuity Plan Training* *DS4.7 Distribution of the IT Continuity Plan* *DS4.8 IT Services Recovery and Resumption*

No	Domain	Sub-Domain
		DS4.9 Offsite Backup Strorage *DS4.10 Post Resumption Review*
5	*DS5 Ensure System Security*	*DS5.1 Management of IT Security* *DS5.2 IT Security Plan* *DS5.3 Identity Management* *DS5.4 User Account Management* *DS5.5 Security Testing, Surveillance and Monitoring* *DS5.6 Security Incident Definition* *DS5.7 Protection of Security Technology* *DS5.8 Cryptographic Key Management* *DS5.9 Malicious Software Prevention, Detection and Correction* *DS5.10 Networking Security* *DS5.11 Exchange of Sensitive Data*
6	*DS6 Identify and Allocate Costs*	*DS6.1 Definition of Services* *DS6.2 IT Accounting* *DS6.3 Cost Modelling and Charging* *DS6.4 Coat Medel Maintenance*

No	Domain	Sub-Domain
7	*DS7 Educate and Train Users*	*DS7.1 Identification of Education and Training Needs* *DS7.2 Delivery of Training and Education* *DS7.3 Evaluation of Training Received*
8	*DS8 Manage Service Desk and Incidents*	*DS8.1 Service Desk* *DS8.2 Registration of Customer Queries* *DS8.3 Incident Escalation* *DS8.4 Incident Closure* *DS8.5 Reporting and Trend Analysis*
9	*DS9 Manage the Configuration*	*DS9.1 Configuration Repository and Baseline* *DS9.2 Identification and Maintenance of Configuration* *DS9.3 Configuration Integrity Review*
10	*DS10 Manage Problems*	*DS10.1 Identification and Classification of Problems* *DS10.2 Problem Tracking and Resolution* *DS10.3 Problem Closure* *DS10.4 Integration of Configuration, Incident and Problem Management*

No	Domain	Sub-Domain
11	*DS11 Manage Data*	*DS11.1 Business Requitments for Data Management* *DS11.2 Storage and Retention Arrangements* *DS11.3 Media Library Management System* *DS11.4 Disposal* *DS11.5 Backup and Restoration* *DS11.6 Security Requitments for Data Management*
12	*DS12 Manage the Physical Environment*	*DS12.1 Site Selection and Layout* *DS12.2 Physical Security Measure* *DS12.3 Physical Access* *DS12.4 Protection Against Enviromentak Factors* *DS12.5 Physical Facilities Management*
13	*DS13 Manage Operation*	*DS13.1 Operations Procedures and Instructions* *DS13.2 Job Scheduling* *DS13.3 IT Infrastructure Monitoring* *DS13.4 Sensitive Documents and Output Devices* *DS13.5 Preventive Maintenance for Hardware*

Domain ME (Monitor and Evaluate)

Pada domain ini memfokuskan pada masalah-masalah tentang pengendalian menyeluruh yang diterapkan pada suatu organisasi, pemeriksaan internal dan eksternal serta jaminan (*assurance*) independen dari proses-proses pemeriksaan yang sudah dilakukan. Domain ini terdiri dari 4 sub proses dan 25 sub-sub proses pada tabel 7.4.

Tabel 7.4 Domain ME (Monitor and Evaluate)

No	Domain	Sub-Domain
1	*ME1 Monitor and Evaluate IT Performance*	*ME1.1 Monitoring Approach* *ME1.2 Definition and Collection of Monitoring Data* *ME1.3 Monitoring Method* *ME1.4 Performance Assessment* *ME1.5 Board and Executive Reporting* *ME1.6 Remedial Actions*
2	*ME2 Monitor and Evaluate Internal Control*	*ME2.1 Monitoring of Internal Control Framework* *ME2.2 Supervisory Review* *ME2.3 Control Exceptions* *ME2.4 Control Self Assessment* *ME2.5 Assurance of Internal Control* *ME2.6 Internal Control at Third Parties* *ME2.7 Remedial Actions*

No	Domain	Sub-Domain
3	*ME3 Ensure Compliance With External Requitments*	*ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements* *ME3.2 Optimisation of Response to External Requirements* *ME3.3 Evaluation of Compliance With External* *ME3.4 Positive Assurance of Compliance* *ME3.5 Integrated Reporting*
4	*ME4 Provide IT Governance*	*ME4.1 Establishment of an IT Governance Framework* *ME4.2 Strategic Alignment* *ME4.3 Valur Delivery* *ME4.4 Resource Management* *ME4.5 Risk Management* *ME4.6 Performance Measurement* *ME4.7 Independent Assurance*

BAB 8

Control Ojective for Information and Related Technology (COBIT) 5

COBIT 5 merupakan versi terbaru dari COBIT yang dikembangkan oleh ISACA. Layanan kerangka kerja yang disediakan oleh COBIT 5 akan mengatur hal-hal yang terkait dengan informasi dan teknologi di dalam perusahaan, pengaturan dilakukan secara holistik berdasarkan fungsi dan tanggung jawab bisnis.

Teknologi Informasi dapat membantu membuat keputusan pada tingkatan manajerial, akan tetapi penerapan teknologi informasi membutuhkan biaya yang cukup besar dengan resiko kegagalan yang tidak kecil. Untuk melakukan implementasi teknologi informasi pada sebuah enterprise dapat digunakan secara maksimal, maka dibutuhkan pemahaman yang tepat mengenai konsep dasar dari sistem yang berlaku, teknologi yang dimanfaatkan, aplikasi yang digunakan dan pengelolaan serta pengembangan sistem yang dilakukan.

COBIT 5 merupakan a set of best practice *(framework)* bagi pengelolaan teknologi informasi yang secara lengkap terdiri dari *executive summary, framework, control objectives, audit guidelines, implementation tool set* serta *management guidelines* sangat berguna untuk proses sistem informasi strategis.

COBIT 5 merupakan sebuah kerangka kerja atau panduan tata kelola dan menajamen teknologi informasi dan semua yang berhubungan, dimulai dengan memenuhi kebutuhan stakeholder akan informasi dan teknologi.

COBIT 5 menyediakan kerangka kerja yang komprehensif yang membantu perusahaan dalam mencapai tujuan mereka untuk pemerintahan dan manajemen TI perusahaan.

Secara sederhana, hal ini membantu perusahaan menciptakan nilai yang optimal dari TI dengan menjaga keseimbangan antara mewujudkan manfaat dan mengoptimalkan tingkat resiko dan penggunaan sumber daya. COBIT 5 memungkinkan TI untuk diatur dan dikelola secara holistik untuk seluruh perusahaan, dengan mengambil penuh *end-to-end* bisnis dan TI area fungsional tanggung jawab, mengingat kepentingan yang berkaitan dengan TI pemangku kepentingan inernal dan eksternal.

COBIT 5 merupakan generasi terbaru dari panduan ISACA yang membahas mengenai tata kelola dan manajemen TI. COBIT 5 dibuat berdasarkan pengalaman penggunaan COBIT selama lebih dari 15 tahun oleh banyak organisasi dan pengguna dari bidang bisnis, komunitas TI, resiko, asuransi, dan keamanan.

Menurut ISACA (2012) COBIT 5 dikembangkan untuk mengatasi kebutuhan-kebutuhan penting seperti :

- Membantu stakeholder dalam menentukan apa yang mereka harapkan dari informasi dan teknologi terkait seperti keuntungan apa, pada tingkat resiko berapa, dan pada biaya berapa dan bagaimana prioritas mereka dalam menjamin bahwa nilai tambah yang diharapkan benar-benar tersampaikan.
- Membahas peningkatan ketergantungan kesuksesan perusahaan pada perusahaan lain dan rekan TI, seperti outsource, pemasok, konsultan, klien, cloud, dan penyedia layanan lain, serta pada beragam alat internal dan mekanisme untuk memberikan nilai tambah yang diharapkan.
- Mengatasi jumlah informasi yang meningkat serta signifikan. Bagaimana organisasi memilih informasi yang relevan dan kredibel yang akan mengarahkan kepada keputusan bisnis yang efektif dan efisien.
- Mengatasi TI yang semakin meresap ke dalam organisasi. TI semakin menjadi bagian penting dari bisnis. Seringkali TI

yang terpisah tidak cukup memuaskan walaupun sudah sejalan dengan bisnis. TI perlu menjadi bagian penting dari proyek bisnis, struktur organisasi, manajemen resiko, kebijakan, kemampuan proses, dan sebagainya.

- Menyediakan panduan lebih jauh dalam area inovasi dan teknologi baru. Hal ini berkaitan dengan kreativitas, penemuan, pengembangan produk baru, membuat produk saat ini lebih menarik bagi pelanggan, dan meraih tipe pelanggan baru.
- Mendukung perpaduan bisnis dan TI secara menyeluruh, dan mendukung semua aspek yang mengarah pada tata kelola dan manajemen TI perusahaan secara efektif, seperti struktur organisasi, kebijakan, dan budaya.
- Mendapatkan control yang lebih baik berkaitan dengan solusi TI.
- Menghubungkan dan bila relevan, menyesuaikan dengan framework dan standar lain seperti ITIL, TOGAF, PMBOOK, PRINCE2, COSO, dan ISO.
- Mengintegrasikan semua framework dan panduan ISACA dengan focus pada COBIT, Val IT, dan Risk IT, tetapi juga mempertimbangkan BMIS, ITAF, dan TGF, sehingga COBIT 5 mencakup seluruh perusahaan dan menyediakan dasar untuk integrasi dengan framework dan standar lain menjadi satu kesatuan *framework*.

Menurut ISACA (2012) beberapa perbedaan antara COBIT 5 dengan versi sebelumnya adalah sebagai berikut :

- Prinsip baru dalam tata kelola TI organisasi yaitu Governance of Enterprise IT (GEIT). COBIT 5 lebih berorientasi pada prinsip dibandingkan dengan proses.
- COBIT menekankan pada enabler. Pada COBIT 4.1 tidak menyebutnya sebagai enabler sedangkan pada COBIT 5 menyebutkan secara spesifik bagian-bagian enabler.

- COBIT 5 mendefinisikan model referensi proses yang baru dengan tambahan domain governance dan beberapa proses yang baru dan dimodifikasi dari proses pada versi sebelumnya, serta COBIT 5 mengintegrasikan konten pada COBIT 4.1, Risk IT dan Val IT.
- COBIT 5 menyelaraskan dengan best practices yang ada seperti ITIL v3 dan TOGAF.

8.1. Prinsip Dalam COBIT 5

Menurut ISACA (2012) COBIT 5 didasarkan pada 5 (lima) prinsip utama yaitu adalah *Meeting Stakeholder Needs, Covering Enterprise End-To-End, Applying a Single Integrated Framework, Enabling a Holistic Approach*, dan *Seperating Governance From Management*.

Gambar 8.1 Prinsip COBIT 5

• *Meeting Stakeholder Needs*

Untuk mendefinisikan prioritas untuk implementasi, perbaikan dan jaminan. Kebutuhan stakeholder diterjemahkan ke dalam *goals cascade* menjadi tujuan yang lebih spesifik, dapat ditindak lanjuti dan disesuaikan dalam konteks tujuan organisasi, tujuan yang terkait TI, tujuan yang akan dicapai *enabler*. Selain itu sistem tata kelola harus mempertimbangkan seluruh stakeholder ketika membuat keputusan mengenai penilaian manfaat, sumber daya, dan resiko.

Gambar 8.2 *The Governance Objective*: *Value Creation*

- *Covering Enterprise End-To-End*

  Pada prinsip ini menjelaskan bahwa COBIT 5 mengintegrasikan tata kelola TI perusahaan ke dalam tata kelola perusahaan. Sistem tata kelola TI yang diusung COBIT 5 dapat menyatu dengan sistem tata kelola perusahaan dengan mulus. Prinsip kedua ini juga meliputi semua fungsi dan proses yang dibutuhkan untuk mengatur dan mengelola TI perusahaan dimanapun informasi diproses. Dalam lingkup perusahaan, COBIT 5 menangani semua layanan TI internal maupun eksternal, dan juga proses bisnis integral dan eksternal.

- *Applying a Single Integrated Framework*

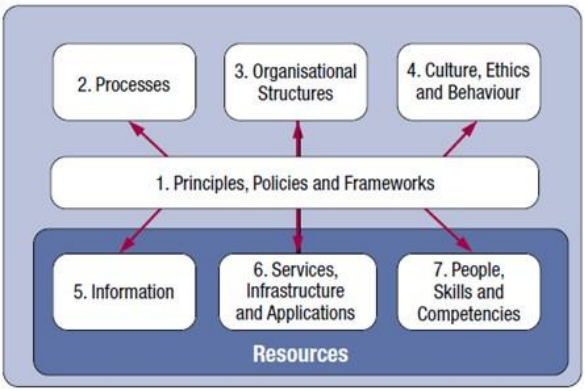
  Sebagai penyelarasan diri dengan standar dan framework relevan lain, sehingga organisasi mampu menggunakan COBIT 5 sebagai *framework* tata kelola umum dan integrator. Selain itu prinsip ini menyatukan semua pengetahuan yang sebelumnya tersebar dalam berbagai *framework* ISACAseperti COBIT, VAL IT, Risk IT, BMIS, ITAF, dll).

- *Enabling a Holistic Approach*

  Pada prinsip ini, COBIT 5 memandang bahwa setiap enabler saling mempengaruhi satu sama lain dan menentukan apakah penerapan COBIT 5 akan berhasil. Pengetahuan yang sebelumnya tersebar dalam berbagai *framework* ISACA seperti COBIT, VAL IT, Risk IT, BMIS, ITAF, dll).

- *Enabling a Holistic Approach*

  Pada prinsip ini, COBIT 5 memandang bahwa setiap *enabler* saling mempengaruhi satu sama lain dan menentukan apakah penerapan COBIT 5 akan berhasil.



Gambar 8.3 COBIT 5 Enterprise Enablers

Enabler adalah sekumpulan faktor yang mempengaruhi sesuatu yang akan dikerjakan oleh suatu organisasi atau enterprise (ISACA, 2012). Dalam COBIT 5 dijelaskan pada kerangka kerja COBIT 5 di dalam 7 kategori *enabler*, yaitu :

- Prinsip, kebijakan dan kerangka kerja *(principles, policies and framework)*, merupakan alat atau pendorong untuk menterjemahkan tingkah laku ke dalam panduan praktis untuk menajemen sehari-hari.

- Proses *(processes)*, menjelaskan tentang sekumpulan kegiatan yang terorganisir untuk mencapai tujuan tertentu dan menghasilkan sekumpulan output dalam mendukung pencapaian tujuan TI.

- Struktur organisasi *(organizational structure)*, merupakan entitas dalam organisasi sebagai kunci dalam membuat keputusan.

- Budaya, etika, dan perilaku *(culture, ethics and behavior)*, merupakan faktor keberhasilan dalam kegiatan tata kelola dan manajemen.

- Informasi *(information)*, dalam organisasi informasi terdiri dari informasi yang dihasilkan dan digunakan informasi dibutuhkan agar organisasi dapat berjalan dengan baik.

- Layanan, infrastuktur dan aplikasi *(Service, Infrastructure and Applications)*, melibatkan infrastruktur teknologi dan aplikasi yang menyediakan proses dan layanan teknologi informasi bagi organisasi.

- Orang, kemampuan dan kompetensi *(people, skills and competencies)*, berhubungan dengan seorang individu dan kebutuhan untuk memenuhi semua aktifitas untuk mencapai kesuksesan dan membuat keputusan yang tepat dengan langkah yang tepat.

- *Seperating Governance From Management*

  Pada prinsip ini COBIT membuat perbedaan yang cukup jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup berbagai kegiatan yang berbeda, memerlukan struktur organisasi yang berbeda, dan melayani untuk tujuan yang berbeda pula.

  Adapun perbedaan antara tata kelola dengan manajemen yaitu :

  - Tata Kelola; dalam kebanyakan perusahaan, tata kelola merupakan tanggung jawab dewan direksi dibawah kepemimpinan ketua yang bertugas untuk memastikan tujuan perusahaan dapat dicapai dengan melakukan evaluasi kebutuhan, kondisi dan pilihan *stakeholder*, serta bertugas dalam pengambilan keputusan yang sesuai dengan arah dan tujuan yang telah disepakati.
  - Manajemen; dalam kebanyakan perusahaan, manajemen merupakan tanggung jawab dari manajemen eksekutif di bawah kepemimpinan CEO yang bertugas untuk merencanakan, membangun, menjalankan dan memonitor aktifitas-aktifitas yang sesuai dengan arah dan tujuan yang telah disepakati oleh badan tata kelola.

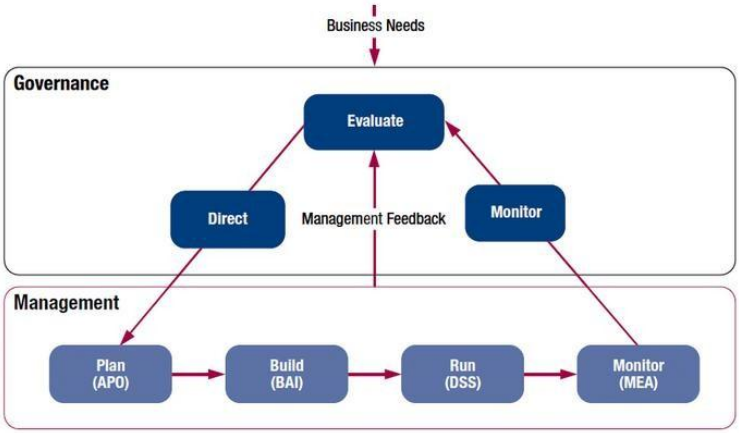
8.2. Model Referensi Proses COBIT 5

COBIT 5 mencakup proses model referensi, yang mendefinisikan dan menjalankan secara rinci sejumlah proses tata kelola dan manajemen yang mewakili semua proses yang biasanya ditemukan di suatu organisasi yang berkaitan dengan aktivitas TI. COBIT 5 menyediakan model referensi umum yang dapat dipahami operasional TI dan manajer bisnis. Model proses yang diusulkan adalah model yang lengkap, komprehensif, tetapi bukan satu-

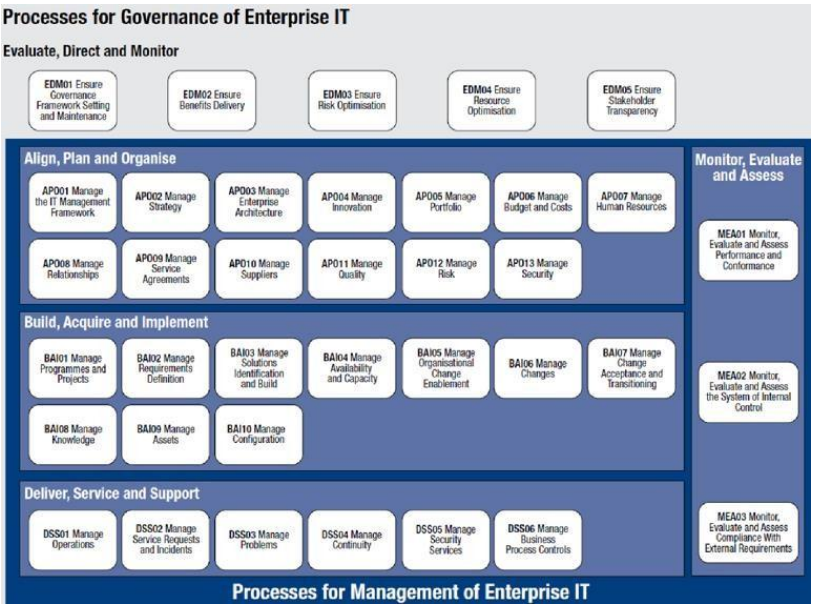
satunya model proses. Setiap organisasi harus menentukan sendiri proses yang sesuai dengan mempertimbangkan situasi spesifik.

COBIT 5 (ISACA, 2012) membagi proses tata kelola dan manajemen TI enterprise menjadi dua area proses utama :

- Tata kelola *(governance)*, yang memuat lima proses tata kelola akan ditentukan praktek-praktek dalam setiap proses *Evaluate*, *Direct*, dan *Monitor* (EDM).
- Manajemen, memuat empat domain, sejajar dengan area tanggung jawab dari *Plan, Build, Run, and Monitor* (PBRM), dan menyediakan ruang lingkup TI yang menyeluruh. Domain ini merupakan evolusi dari domain dan struktur proses dalam COBIT 4.1, yaitu *Align*, *Plan*, *and Organize* (APO), *Build*, *Acquare*, and *Implement* (BAI), *Deliver*, *Service and Support* (DSS), *Monitor*, *Evaluate*, *and Assess* (MEA).



Gambar 8.4 COBIT 5 *Governance and Management Key Areas*



Gambar 8.5 COBIT 5 Process Reference Model

Domain EDM (Evaluate, Direct, and Monitor)

ISACA (2012) menjelaskan bahwa proses tata kelola EDM berurusan dengan tujuan stakeholder dalam melakukan penilaian, optimasi risiko dan sumber daya, mencakup praktek dan kegiatan yang bertujuan untuk mengevaluasi pilihan strategis, memberikan arahan kepada TI dan pemantauan hasilnya.

Berikut ini merupakan domain proses EDM :

- EDM01 *Ensure Governance Framework Setting and Maintenance* (memastikan pengaturan dan pemeliharaan kerangka tata kelola).

- EDM02 *Ensure Benefits Delivery* (memastikan penyampaian manfaat).
- EDM03 *Ensure Risk Optimisation* (memastikan pengoptimalan risiko).
- EDM04 *Ensure Resource Optimisation* (memastikan pengoptimalan sumber daya).
- EDM05 *Ensure Stakeholder Transparency* (memastikan transparansi pemangku kepentingan).

Domain APO (Align, Plan, and Organise)

ISACA (2012) menjelaskan dalam COBIT 5 bahwa proses manajemen APO memberikan arah untuk penyampaian solusi (BAI) dan penyediaan layanan dan dukungan (DSS). Domain ini mencakup strategi dan taktik, dan identifikasi cara terbaik agar TI dapat berkontribusi pada pencapaian tujuan bisnis.

Berikut ini merupakan domain proses APO :

- APO01 *Manage The IT Management Framework* (MengelolaKerangka Manajemen IT)
- APO02 *Manage Strategy* (Mengelola Strategi)
- APO03 *Manage Enterprise Architecture* (Mengelola Arsitektur Bisnis)
- APO04 *Manage Innovation* (Mengelola Perubahan)
- APO05 *Manage Portfolio* (Mengelola Dokumen)
- APO06 *Manage Budget and Costs* (Mengelola Anggaran dan Biaya)
- APO07 *Manage Human Resources* (Mengelola Sumber Daya Manusia)24
- APO08 *Manage Relationships* (Mengelola Relasi)
- APO09 *Manage Service Agreements* (Mengelola Perjanjian Layanan)
- APO10 *Manage Suppliers* (Mengelola Pemasok)
- APO11 *Manage Quality* (Mengelola Kualitas)

- APO12 *Manage Risk* (Mengelola Risiko)
- APO13 *Manage Security* (Mengelola Keamanan)

Domain BAI (Build, Acquire, and Implement)

ISACA (2012) menjelaskan dalam COBIT 5 bahwa proses manajemen BAI memberikan solusi dan mengimplementasikan, sehingga berubah menjadi layanan. Untuk mewujudkan strategi TI, solusi TI perlu diidentifikasikan, dikembangkan, serta diimplementasikan dan diintegrasikan ke dalam proses bisnis.

Berikut ini merupakan domain proses BAI :

- BAI01 *Manage Programmes and Project* (Mengelola Program dan Proyek)
- BAI02 *Manage Requirements Definition* (Mengelola Kebutuhan)
- BAI03 *Manage Solutions Identification and Build* (Mengelola Identifikasi Solusi dan Pembangunan)
- BAI04 *Manage Availability and Capacity* (Mengelola Ketersediaan danKapasitas)
- BAI05 *Manage Organisational Change Enablement* (Mengelola Pemberdayaan Organisasi Perubahan)
- BAI06 *Manage Changes* (Mengelola Perubahan)
- BAI07 *Manage Change Acceptance and Transitioning* (Mengelola Penerimaan Perubahan dan Transisi)
- BAI08 *Manage Knowledge* (Manajemen Pengetahuan)
- BAI09 *Manage Assets* (Mengelola Aset Kepemilikan)
- BAI10 *Manage Configuration* (Mengelola Konfigurasi)

Domain DSS (Deliver, Service, and Support)

ISACA (2012) menjelaskan dalam COBIT 5 bahwa proses manajemen DSS menyampaikan solusi yang dapat digunakan bagi pengguna akhir. Domain ini berkaitan dengan penyampaian dan dukungan layanan aktual yang dibutuhkan, yang meliputi pelayanan serta pengelolaan keamanan dan keberlangsungan,

dukungan layanan bagi pengguna, dan manajemen data dan fasilitas operasional.

Berikut ini merupakan domain proses DSS:

- DSS01 *Manage Operations* (Mengelola Operasi)
- DSS02 *Manage Service Requests and Incidents* (Mengelola Permintaan Layanan dan Insiden)
- DSS03 *Manage Problems* (Mengelola Masalah)
- DSS04 *Manage Continuity* (Mengelola Keberlangsungan)
- DSS05 *Manage Security Services* (Mengelola Layanan Keamanan)
- DSS06 *Manage Business Process Controls* (Mengelola Kontrol Proses Bisnis)

Domain MEA (Monitor, Evaluate, Assess)

ISACA (2012) menjelaskan dalam COBIT 5 bahwa proses manajemen MEA memonitor semua proses untuk memastikan bahwa pengarahan yang disediakan domain yang sebelumnya diikuti. Semua proses TI perlu dinilai secara teratur dari waktu ke waktu untuk mengontrol kualitas dan kepatuhannya. Domain ini merujuk pada manajemen kinerja, pemantauan pengendalian internal, kepatuhan terhadap peraturan dan tata kelola.

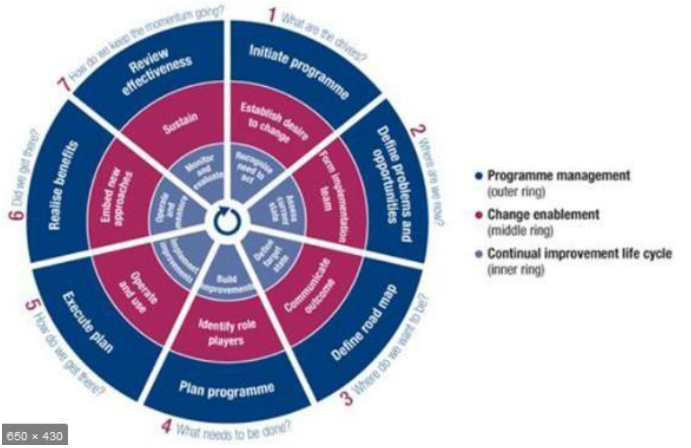
Berikut ini merupakan domain proses MEA :

- MEA01 Monitor, *Evaluate and Assess Performance and Conformance* (Memantau, Mengevaluasi dan Menilai Kinerja dan Penyesuaian)
- MEA02 *Monitor, Evaluate and Assess The System of Internal Control* (Memantau, Mengevaluasi dan Menilai Sistem Pengendalian Internal)
- MEA03 *Monitor, Evaluate and Assess Compliance with External Requirements* (Memantau, Mengevaluasi dan Menilai Kepatuhan terhadap Persyaratan Eksternal)

8.3. Model Referensi Proses COBIT 5

Metode implementasi tata kelola teknologi informasi pada COBIT

5 memiliki 5 tahapan yang terus berulang mulai dari tahap *initiate programme* sampai tahap *review effectiveness*.



Gambar 8.6 COBIT 5 *Implementation Life Cycle*

Berikut ini merupakan tahapan-tahapan metode implementasi tata kelola teknologi informasi pada COBIT 5 adalah :

- Tahap 1 - *Initiate Programme*
  Tahap ini menjelaskan tentang faktor apa yang mungkin menjadi penggerak suatu organisasi dan identifikasi faktor pendorong perubahan saat ini. Tujuan dari tahap ini adalah memperoleh pemahaman tentang organisasi yang terdiri dari tujuan, tugas dan wewenang, pendekatan pengelolaan organisasi saat ini dan konsep program organisasi.

- Tahap 2 - *Define Problems and Opportunities*
  Tahap ini menjelaskan tentang posisi organisasi saat ini yang berhubungan dengan IT. Organisasi perlu mengetahui kemampuan saat ini dan di mana kekurangan mereka, hal inidicapai dengan penilaian kemampuan proses terhadap status proses yang dipilih. Tujuan dari tahap ini adalah untuk menyelaraskan tujuan IT dengan strategi organisasi.

- Tahap 3 - *Define Road Map*
  Tahap ini menjelaskan tentang target perbaikan yang akan dilakukan organisasi dan analisis gap untuk mengidentifikasi solusi potensial. Tujuan dari tahap adalah untuk menetapkan target kemampuan untuk proses yang dipilih.

- Tahap 4 - *Plan Programme*
  Tahap ini menjelaskan tentang apa yang harus dilakukan organisasi yang berupa solusi perbaikan dan rekomendasi. Tujuan tahap ini adalah memberikan kesempatan untuk memperbaiki kinerja pada proses yang dipilih sehingga mencapai target.

- Tahap 5 - *Execute Plan*
  Tahap ini menjelaskan tentang pelaksanaan solusi yang diusulkan kedalam praktek sehari-hari pada organisasi dan dilakukan pemantauan terhadap keselarasan yang dicapai dengan pengukuran kinerja.

- Tahap 6 - *Release Benefits*
  Tahap ini menjelaskan tentang keuntungan berkelanjutan yang didapat dari perbaikan tata kelola teknologi informasi pada organisasi.

- Tahap 7 - *Review Effectiveness*
  Tahap ini menjelaskan tentang evaluasi dari setiap pencapaian kesuksesan pada organisasi dan identifikasi tata kelola untuk meningkatkan kebutuhan untuk perbaikan secara terus menerus.

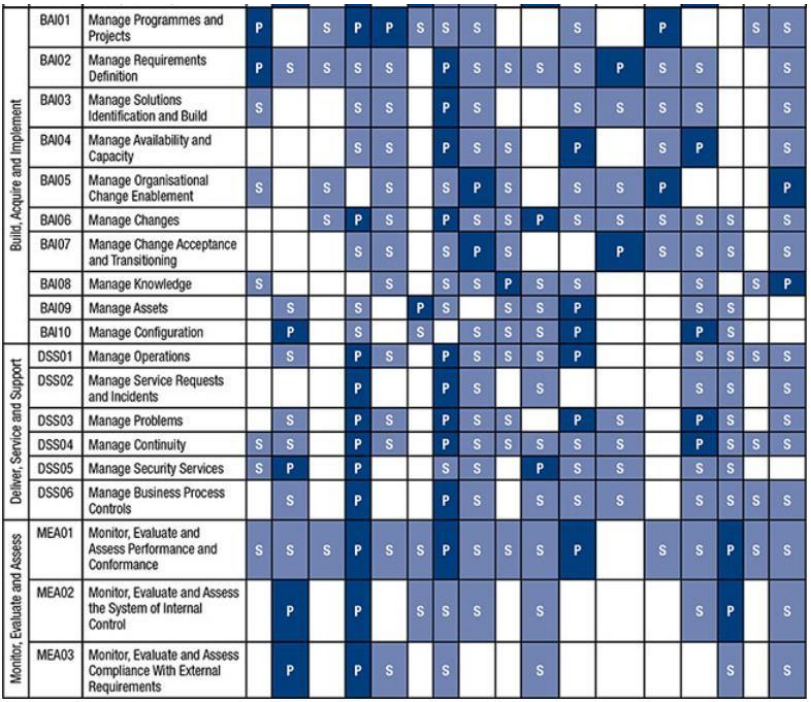
8.4. Pemetaan COBIT 5

Adapaun pemetaan COBIT 5 yang akan digunakan untuk menentukan tata kelola TI adalah :

- Pemetaan Enterprise Goals terhadap IT-related Golas COBIT 5

  Pemetaan ini bertujuan untuk menunjukkan bagaimana enterprise *goals* didukung (atau diartikan ke dalam) *IT-related goals*.

			IT-related Goal																
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		COBIT 5 Process	Financial						Customer		Internal							Learning and Growth	
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Ensure Benefits Delivery	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S		S
Align, Plan and Organise	AP001	Manage the IT Management Framework	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	AP002	Manage Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	AP003	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S
	AP004	Manage Innovation	S			S	P			P	P		P	S		S			P
	AP005	Manage Portfolio	P		S	S	P	S	S	S	S		S		P				S
	AP006	Manage Budget and Costs	S		S	S	P	P	S	S			S		S				
	AP007	Manage Human Resources	P	S	S	S			S		S	S	P		P		S	P	P
	AP008	Manage Relationships	P		S	S	S	S	P	S			S	P	S		S	S	P
	AP009	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	P	S		
	AP010	Manage Suppliers		S		P	S	S	P	S	P	S	S		S	S	S		S
	AP011	Manage Quality	S	S		S	P		P	S	S		S		P	S	S	S	S
	AP012	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S
	AP013	Manage Security		P		P		P	S	S		P				P			



Build, Acquire and Implement	BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
	BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S
	BAI05	Manage Organisational Change Enablement	S		S		S		S	P	S		S	S	P				P
	BAI06	Manage Changes			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Manage Change Acceptance and Transitioning				S	S		S	P	S			P	S	S	S		S
	BAI08	Manage Knowledge	S				S		S	S	P	S	S			S		S	P
	BAI09	Manage Assets		S		S		P	S		S	S	P			S	S		
	BAI10	Manage Configuration		P		S		S		S	S	S	P			P	S		
Deliver, Service and Support	DSS01	Manage Operations		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Manage Service Requests and Incidents				P			P	S		S				S	S		S
	DSS03	Manage Problems		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Manage Continuity	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Manage Security Services	S	P		P			S	S		P	S	S		S	S		
	DSS06	Manage Business Process Controls		S		P			P	S		S	S	S		S	S	S	S
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitor, Evaluate and Assess the System of Internal Control		P		P		S	S	S		S				S	P		S
	MEA03	Monitor, Evaluate and Assess Compliance With External Requirements		P		P	S		S			S					S		S

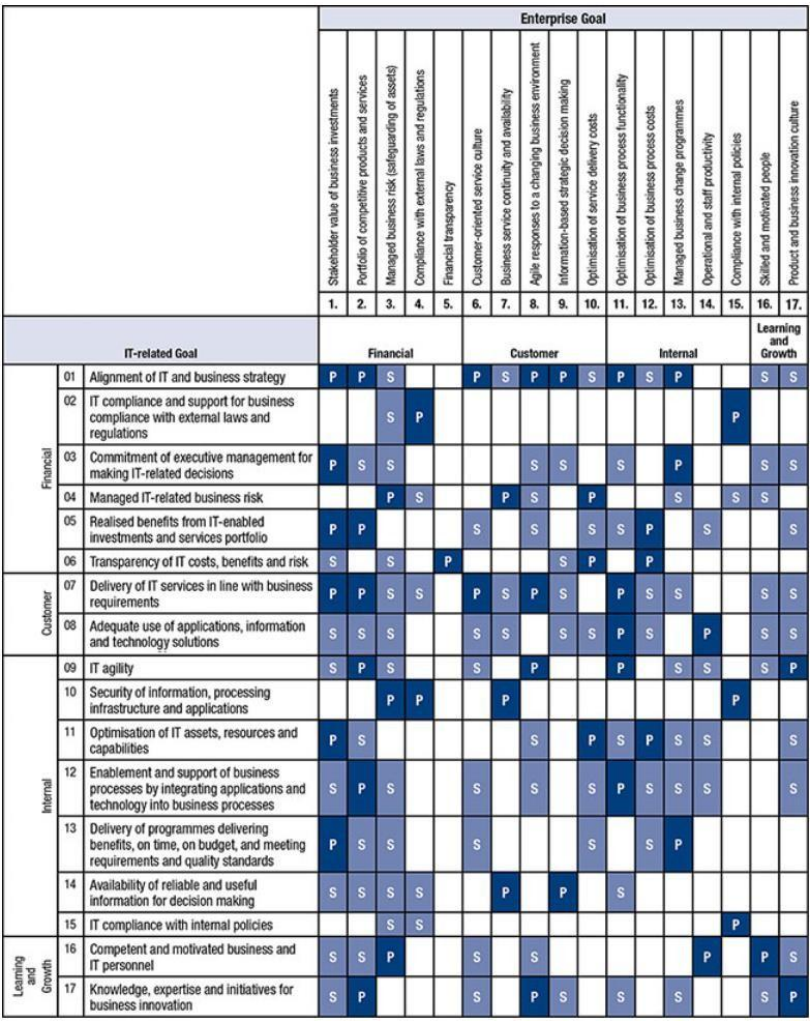
Gambar 8.7 *Pemetaan Enterprise Goals*

Keterangan P = Primary, S = Secondary

Dari gambar diatas diketahui bahwa terdapat 17 *IT-related goals* pada COBIT 5 serta hubungan *primary* maupun *secondary* antara masing-masing *IT-related goals* COBIT yang ada dengan panduan *enterprise goals* secara umum.

- Pemetaan IT-related Goals terhadap Proses COBIT 5

  Berikut ini adalah gambaran pemetaan IT goals terhadap proses COBIT 5



Gambar 8.8 Pemetaan COBIT 5 Process

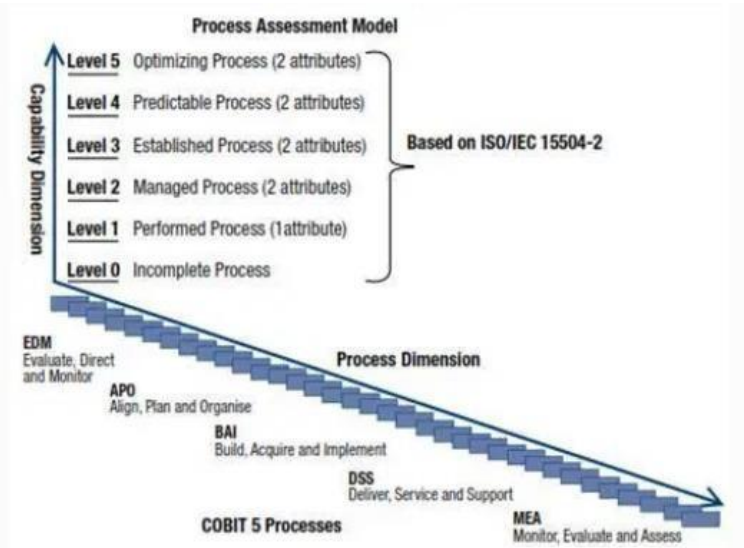
Dari gambar tersebut dapat terlihat 37 proses COBIT serta hubungan *primary* maupun *secondary* antara proses-proses COBIT yang ada dengan panduan *IT goals* secara umum. Untuk

penjelasan mengenai *primary* dan *secondary* yaitu sebagai berikut :

- Primary: memiliki hubungan penting dan merupakan dukungan utama untuk pencapaian tujuan yang berhubungan dengan TI.
- Secondary: masih memiliki hubungan yang kuat, namun kurang penting dan merupakan dukungan sekunder untuk pencapaian tujuan yang berhubungan dengan TI.

8.5. Process Capability Model

Pada *framework* COBIT 5 yang dikeluarkan oleh ISACA (2012), tidak lagi menggunakan Maturity Level seperti pada COBIT 4.1 (2007) sebelumnya. Maturity Level diganti menjadi Process Capability Model yang diadopsi dari ISO/IEC 15504-2, dimana proses penilaian akan berdasarkan tingkat kemampuan sebuah organisasi dalam melakukan proses-proses yang telah didefinisikan dalam model *assessment*.



Gambar 8.9 *Process Capability Level*

Berikut ini tingkatan *Process Capability Model* yang dimiliki sebuah organisasi, antara lain adalah :

- Level 0 : *Incomplete Process*
  Organisasi pada tahap ini tidak melaksanakan proses tata kelola TI yang seharusnya ada atau belum berhasil mencapai tujuan dari proses TI.

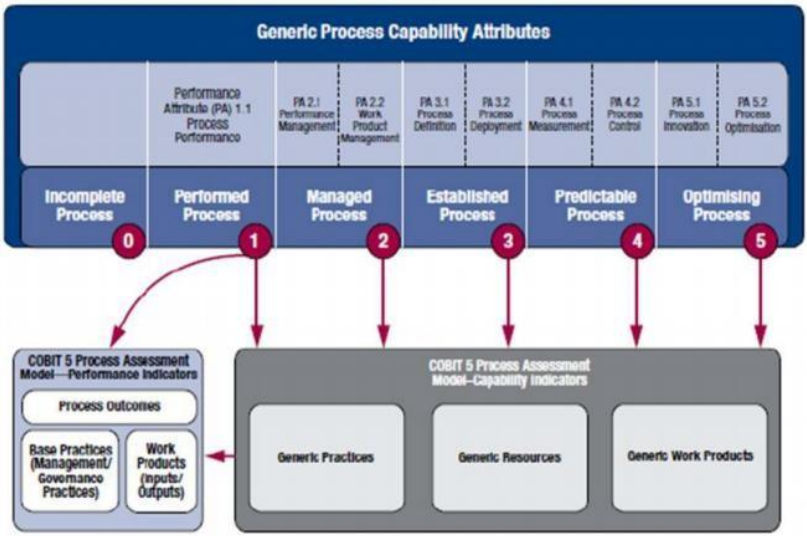
- Level 1 : *Performed Process*
  Organisasi pada tahap ini telah berhasil melaksanakan proses tata kelola TI dan tujuan proses TI tersebut benar- benar tercapai.

- Level 2 : *Managed Process*
  Organisasi pada tahap ini dalam melaksanakan proses tata kelola TI dan mencapai tujuannya dilaksanakan secara terkelola dengan baik, sehingga ada penilaian lebih karena pelaksanaan dan pencapaiannya dilakukan dengan pengelolaan yang baik. Pengelolaan berupa proses perencanaan, evaluasi dan penyesuaian untuk ke arah yang lebih baik lagi.

- Level 3 : *Established Process*
  Organisasi pada tahap ini memiliki proses-proses tata kelola TI yang sudah distandarkan dalam lingkup organisasi secara keseluruhan. Artinya sudah memiliki standar proses yang berlaku diseluruh lingkup organisasi.

- Level 4 : *Predictable Process*
  Organisasi pada tahap ini telah menjalankan proses tata kelola TI dalam batasan-batasan yang sudah pasti (misalkan batasan waktu) dan proses yang dijalankan telah memiliki hasil. Batasan-batasan yang ada dihasilkan daripengukuran yang telah dilakukan pada saat pelaksanaan proses TI sebelumnya.

- Level 5 : *Optimizing Process*
  Pada tahap ini, organisasi telah melakukan inovasi-inovasi dan melakukan perbaikan yang berkelanjutan untuk meningkatkan kemampuannya.



Gambar 8.10 COBIT 5 *Process Capability Model*

DAFTAR PUSTAKA

Bauchspies, R.W.Jr. 2006. Mail List Discussion Information Culture: Concept and Application.

Henderson, J., Venkatraman, N. (1993). Strategic Alignment : Leveraging Information Technology for Transforming Organizations, IBM Systems Journal, vol. 32, 1.

Indrajit, 2016. "Tata Kelola Teknologi Informasi". Preinexus.Yogyakarta.

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

ISACA. (2012). Process Assessment Model (PAM): Using COBIT 5. USA: IT Governance Institute.

ISACA. (2012). COBIT 5 Enabling Processes. USA: IT Governance Institute.

ISACA. (2012). COBIT 5 Implementation. USA: IT Governance Institute.

IT Governance Institute, COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Ed., 2007.

IT Governance Institute, Board Briefing on IT Governance, 2nd ed.,2003.

ITGI. (2008). Aligning COBIT 4.1, ITILv3, and ISO/IEC 27002 for Business Benefit. England and USA: IT Governance Institute.

ITGI. (2007). COBIT 4.1. USA: IT Governance Institute.

Jablonski, J.A. 2006. Mailing List Discussion-Information Culture: Concept and Application.

Kusbandono, Hendrik dkk. 2019. Tata Kelola Teknologi Informasi. Ponorogo: Nata Karya.

Luftman, J.N (2004). Managing the Information Technology Resource, Leadership in the Information Age. Pearson Education, inc. New Jersey.

Moeller, Robert R. 2013. Executive's Guide to IT Governance. John Wiley and Sons Inc. New Jersey.

Notoatmodjo, Soekidjo. 2003. Pendidikan dan Perilaku Kesehatan. Jakarta : Rineka Cipta.

Peterson, R. (2001). Configurations and coordination for global information governance: Complex designs in a transnational European context. Proceedings of the 34th HICSS Conference. Hawaii.

Peterson. 2003. "Information Strategies and Tactics for Information Technology." Idea Group Publishing.

Suroso, Arif Imam dan Aji Hermawan. 1998. Manajemen Budaya Informasi. Amal Agrimedia. Vol.4 No 3. ISSN: 0853-846-8.

Tarigan, J., 2006, Merancang IT Governance Dengan COBIT & Sarbanes Oxley Act Dalam Konteks Budaya Indonesia, Universitas Kristen Petra Surabaya.

Terry (1962). Office Management and Control, Fourth Edition. Homewood, Ilinois: Richard D. Irwin Inc.

Wang, Mei -Yu. 2005. The impact of Information Culture on Managing Knowledge: a double case study of pharmaceutical manufacturers in Taiwan. Library Review. Vol. 55. No 3 pp 209-2 221.

Weill, P., & Ross, J. W. (2004). IT Governance How Top Performers