BAB II

LANDASAN TEORI

2.1 Sistem

Menurut Jogiyanto (2005), sistem adalah suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan dan berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu tujuan tertentu.

Menurut Sutanta (2009), istilah sistem secara umum dapat didefinisikan sebagai kumpulan hal atau elemen yang saling bekerja sama atau yang dihubungkan dengan cara-cara tertentu sehingga membentuk satu kesatuan untuk melaksanakan suatu fungsi guna mencapai suatu tujuan. Sistem mempunyai karakteristik atau sifat-sifat tertentu, yaitu komponen sistem, batasan sistem, lingkungan luar sistem, penghubung sistem, masukan sistem, keluaran sistem, pengolahan sistem dan tujuan sistem.

Dapat disimpulkan bahwa pengertian sistem adalah sekelompok elemen atau subsistem yang terintegrasi untuk mencapai tujuan tertentu.

2.2 Informasi

Menurut Jogiyanto (2005), Informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya. Sumber dari informasi adalah data yang merupakan bentuk jamak dari bentuk tunggal atau *data item*. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata.

Menurut Sutanta (2009), Informasi adalah data yang diolah menjadi bentuk yang berguna dan menjadi berarti bagi penerimanya. Kegunaan informasi adalah untuk mengurangi ketidakpastian di dalam proses pengambilan keputusan tentang suatu keadaan. Suatu informasi dikatakan bernilai bila manfaatnya lebih efektif dibandingkan dengan biaya untuk mendapatkan informasi tersebut. Kualitas informasi sangat dipengaruhi atau ditentukan oleh beberapa hal yaitu relevan (*relevancy*), akurat (*accurancy*), tepat waktu (*time liness*), ekonomis (*economy*), efisien (*efficiency*), ketersediaan (*availabilit*y), dapat dipercaya (*reliability*), konsisten.

Dari pendapat di atas maka dapat disimpulkan bahwa informasi adalah data yang telah diolah sehingga memiliki arti atau sesuatu yang berarti dan dibutuhkan bagi manajemen untuk membantu dalam pengambilan keputusan yang menentukan keberhasilan atau kesuksesan organisasi untuk masa yang akan dating dan juga kualitas informasi ditentukan oleh mutu *Reliable, Relevan, Timely, Complete,* serta *Understandable*.

2.3 Sistem Informasi

A. Definisi Sistem Informasi

Menurut Nash (1995), sistem informasi adalah kombinasi dari manusia, fasilitas atau alat teknologi, media, prosedur dan pengendalian yang ditujukan untuk mengatur jaringan komunikasi yang penting, proses transaksi tertentu dan rutin, membantu manajemen juga *user* internal dan eksternal, dan juga menyediakan dasar untuk pengambilan keputusan yang tepat.

Menurut Sutabri (2005), sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang

mendukung fungsi operasi organisasi yang bersifat manajerial dengan kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan-laporan yang diperlukan.

Sedangkan menurut Gordon (1991), sistem informasi adalah suatu sistem yang menerima input data dan instruksi, mengolah data sesuai dengan instruksi dan mengeluarkan hasilnya.

Dari beberapa pendapat berikut dapat disimpulkan bahwa sistem informasi adalah beberapa komponen, antara lain rangkaian prosedur dimana informasi itu sendiri diolah sedemikian rupa sehingga dapat berguna bagi para pemakai untuk mencapai tujuan perusahaan.

B. Komponen Sistem Informasi

Menurut Kusrini dan Koniyo (2007), sistem informasi terdiri dari enam sumber daya yang dikenal sebagai komponen sistem informasi. Ke-enam sumber daya tersebut adalah manusia, *hardware, software,* data, prosedur dan jaringan. Komponen-komponen tersebut memainkan peranan yang sangat penting dalam suatu sistem informasi. Berikut merupakan penjelasan komponen dari sistem informasi:

1. **Perangkat keras *(hardware):*** mencakup peranti-peranti fisik seperti komputer dan printer.
2. **Perangkat lunak *(software)* atau program:** sekumpulan instruksi yang memungkinkan perangkat keras untuk dapat memproses data.
3. **Prosedur:** sekumpulan aturan yang dipakai untuk mewujudkan pemrosesan data dan pembangkitan keluaran yang dikehedaki.

4. **Orang (*user)*:** semua pihak yang bertanggung jawab dalam pengembangan sistem informasi, pemrosesan, dan penggunaan keluaran sistem informasi.
5. **Basis data *(database):*** sekumpulan tabel, hubungan, dan lain-lain yang berkaitan dengan penyimpanan data.
6. **Jaringan komputer dan komunikasi data *(network)*:** sistem penghubung yang memungkinkan sesumber *(resources)* dipakai secara bersama atau diakses oleh sejumlah pemakai.

2.4 Audit

A. Definisi Audit

Audit atau pemeriksaan dalam arti luas bermakna evaluasi terhadap suatu organisasi, sistem, proses, atau produk. Audit dilaksanakan oleh pihak yang kompeten, objektif, dan tidak memihak, yang disebut auditor. Berikut ini beberapa pendapat para pakar mengenai definisi audit yang berkembang saat ini:

Menurut Arens dan Loebbecke (2000), audit adalah kegiatan mengumpulkan dan mengevaluasi dari bukti-bukti mengenai informasi untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dengan kriteria yang telah ditetapkan. Proses audit harus dilakukan oleh orang yang kompeten dan independen.

Menurut *The American Accounting Association's Committee on Basic Auditing Concepts* (2001), audit merupakan suatu proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara obyektif mengenai pernyataan tentang kegiatan dan kejadian ekonomi dengan tujuan umtuk menetapkan tingkat

kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan serta menyampaikan hasilnya kepada pemakai yang berkepentingan.

Menurut Meisser (2003), audit adalah proses yang sistematik dengan tujuan mengevaluasi bukti mengenai tindakan dan kejadian ekonomi untuk memastikan tingkat kesesuaian antara penugasan dan kriteria yang telah ditetapkan, hasil dari penugasan tersebut dikomunikasikan kepada pihak pengguna yang berkepentingan.

Secara umum pengertian di atas dapat diartikan bahwa audit adalah proses sistematis yang dilakukan oleh orang yang kompeten dan independen dengan mengumpulkan dan mengevaluasi bahan bukti dan bertujuan memberikan pendapat mengenai kewajaran laporan keuangan tersebut. Audit merupakan suatu rangkaian kegiatan yang menyangkut proses pengumpulan dan evaluasi bukti, informasi yang dapat diukur, dilakukan oleh orang yang atau organisasi yang kompeten dan independen yang disebut auditor, juga menentukan kesesuaian informasi dengan kriteria penyimpangan yang ditemukan, dan melaporan hasil temuan.

2.5 Audit Sistem Informasi

Menurut Weber (2007), audit sistem informasi (*Information System Audit*) atau EDP audit (*Electronic Data Processing Audit*) atau komputer audit adalah proses pengumpulan data dan pengevaluasian bukti-bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian internal yang memadai, semua aktiva dilindungi dengan baik atau disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efesiensi penyelenggaraan sistem informasi berbasis komputer.

Menurut Arens dan Loebbecke (2000), audit sistem informasi adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan oleh seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi yang dimaksud dengan standar-standar yang telah ditetapkan.

Dapat disimpulkan pengertian audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti oleh orang yang kompeten dan independen untuk menentukan apakah sistem yang dijalankan sesuai dengan kriteria/standar yang ditentukan.

2.6 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Gondodiyoto (2007) adalah:

1. Pengamanan Aset

   Aset sistem informasi suatu perusahaan seperti *hardware*, *software*, sumber daya manusia, *file* data harus dijaga oleh suatu sistem pengendalian internal yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Oleh karena itu sistem pengamanan aset merupakan suatu hal fundamental yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Menjaga Integritas Data

   Integritas data adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti kelengkapan dan keakuratan. Jika tidak dipelihara, maka suatu perusahaan tidak akan lagi memiliki informasi atau laporan yang benar bahkan perusahaan dapat menderita kerugian dari kesalahan dalam membuat atau mengambil keputusan.

3. Efektifitas Sistem

   Efektifitas sistem perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan *user*.

4. Efisiensi Sistem

   Efisiensi menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya informasi yang minimal.

5. Ekonomis

   Ekonomis mencerminkan kalkulasi untuk c*ost* atau *benefit* yang lebih bersifat kuantifikasi terhadap nilai moneter (uang).

2.7 Standar Audit Sistem Informasi

Menurut Gondodiyoto (2007), *Information Systems Audit and Control Association (ISACA)* memiliki standar untuk audit sistem informasi, antara lain:

1) Audit Chapter

   a. Responsibility, Authority and Accountability

      Definisi dari tanggung jawab, otoritas, dan *accountability* dari fugsi audit sistem informasi lebih tepat bila di dokumentasi dalam suatu surat perjanjian.

2) *Independence*

a. *Professional Independence*

Dalam permasalahan yang berkaitan dengan audit, auditor sistem informasi harus bersikap independen dalam tingkah laku dan tindakannya.

b. *Organizational Relationship*

Fungsi audit sistem informasi harus berada independen dari area yang diaudit untuk mencapai tujuan objektivitas dari suatu proses audit.

3) *Professional Ethics and Standards*

a. *Code of Professional Ethics*

Auditor dari sistem informasi harus menghormati dan menaati etika profesional dari *Information Systems Audit and Control Association.*

b. *Due Professional Care*

Standar audit profesional harus diterapkan dalam segala aspek dalam pekerjaan yang dilakukan oleh auditor sistem informasi.

4) *Competence*

a. *Continuing Professional Education*

Auditor sistem informasi harus menjaga kompetensi teknikal melalui pendidikan lanjut profesional.

5) *Planning*

a. *Audit Planning*

Auditor sistem informasi harus merencanakan perencanaan audit

sistem untuk menempatkan tujuan audit dan melengkapi standar profesional audit.

6) *Performance of Audit Work*

a. *Supervision*

Staf dari audit sistem informasi harus tepat untuk dapat menjamin tujuan dari audit dijalankan dan standar profesional audit dapat terpenuhi.

b. *Evidence*

Selama masa pekerjaan audit auditor sistem infromasi harus mendapatkan bukti yang tepat, dapat dipercaya, relevan dan berguna untuk mencapai tujuan objektif dari suatu audit.

7) *Reporting*

a. *Report Content and Form*

Auditor sistem informasi harus menyediakan *report* dalam bentuk yang tepat pada saat penyelesaian tugas audit. Laporan audit berupa lingkup, tujuan, periode audit, dan lingkungan dimana audit dijalankan. Laporan audit harus mengidentifikasi permasalahan yang terjadi dalam jangka waktu audit. Laporan audit juga memberikan rekomendasi dari layanan atau kualisifikasi yang diberikan auditor terhadap tugas audit yang dijalankan.

8) *Follow Up Activities*

a. *Follow Up*

Auditor sistem informasi harus meminta dan mengevaluasi informasi yang sesuai dari penemuan yang terdahulu dan

rekomendasi yang dihasilkan pada periode audit terdahulu untuk mendefinisikan tindakan yang tepat yang harus diimplementasikan dalam suatu periode tertentu.

2.8 Tahapan Audit Sistem Informasi

Menurut Hermawan (2011), tahapan audit sistem informasi dibagi menjadi 4 (empat) tahapan yaitu:

1. Tahap Perencanaan Audit Sistem Informasi

   Tahap perencanaan ini dilakukan oleh auditor untuk mengetahui tentang auditee (how your auditee) dan mempelajari tentang proses bisnis perusahaan yang diaudit. Pada tahap ini ditentukan ruang lingkup dan tujuan dari audit sistem informasi yang hendak dikerjakan.

2. Tahap Persiapan Audit Sistem Informasi

   Pada tahap persiapan, auditor merencanakan dan memantau pelaksanaan audit sistem informasi secara terperinci, kemudian mempersiapkan kertas kerja audit sistem informasi yang akan dipakai.

3. Tahap Pelaksanaan Audit Sistem Informasi

   Pada tahap pelaksanaan, auditor melakukan pengumpulan dan evaluasi bukti dan data audit sistem informasi yang dilakukan, serta melakukan uji kepatutan (complience test), yakni dengan menyesuaikan keadaan ada dengan standar pengelolaan proses TI yang didefinisikan dalam kerangka kerja ISO 27002. Selanjutnya dilakukan penyusunan temuan serta rekomendasi guna diberikan kepada auditee.

4. Tahap Pelaporan Audit Sistem Informasi

Pada tahap pelaporan, auditor membuat draft pelaporan yang obyektif dan komperehensif yang nantinya ditunjukan ke auditor.

2.9 Kerangka Audit

Berikut merupakan contoh aplikasi standarisasi audit:

2.9.1 ITSM (*Information Technology Service Management)*

A. Definisi ITSM *(Information Technology Service Management)*

Menurut Orand (2011) mendefinisikan *bahwa "service management as a set of specialized organizational capabilities for providing value to customers in the form of services".*

Menurut Menken (2010), *IT Service Management* merupakan manajemen dari semua proses yang bekerja sama untuk memastikan kualitas layanan, sesuai dengan tingkat layanan yang telah disepakati dengan pelanggan.

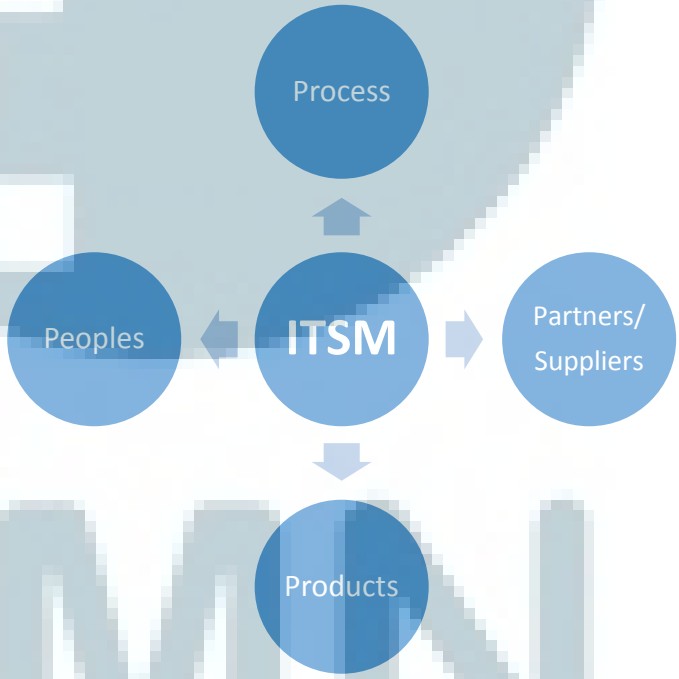
Dari definisi para ahli dapat disimpulkan bahwa ITSM merupakan semua proses yang digunakan untuk meningkatkan kualitas sesuai dengan tingkat yang telah disepakati bersama pelanggan, guna memberi suatu layanan yang bernilai dan sesuai dengan kebutuhan-kebutuhan pelanggan.

Secara garis besar ITSM memiliki 2 (dua) *level* yaitu:

1. *Level* pengambil keputusan yang menetapkan sasaran-sasaran organisasi kemudian menurunkannya menjadi aktifitas-aktifitas besar yang harus dilaksanakan sesuai dengan hasil-hasil yang diharapkan nantinya yang dapat diukur

2. *Level* operasional merupakan *level* yang lebih rinci yang menetapkan proses-proses yang harus dijalankan oleh setiap unit organisasi berdasarkan masukan-masukan (*input)* prosesnya dan harus menghasilkan (*output)* sesuatu yang ditentukan. Secara sederhana *level* ITSM menggunakan metodologi Deming (*Plan* - rencana proyek; *Do* – proyek; *Check* – audit; *Act* - pelaksanaan) sebagai siklus peningkatan kualitasnya secara terus-menerus dan bertahap.

Menken (2010) menerangkan bahwa *IT Service Management* memiliki 4 perspektif/attribut yang menjelaskan tentang konsep ITSM. Hubungan masing-masing perspektif sebagai berikut:



Perspektif atau attribut yang ditunjukkan terdiri dari *people, product/technology, partners/suppliers* dan *process* dengan penjelasan sebagai berikut:

a. *Partners/Suppliers*

Perspektif *partners/suppliers* memperhitungkan pentingnya mitra dan hubungan dengan *supplier*/pemasok eksternal demi membangun kontribusi yang positif pada layanan.

b. *People*

Perspektif *people* berkaitan dengan bagaimana mengelola sumber daya manusia seperti staf TI, pelanggan dan *stakeholder* lainnya guna memenuhi kebutuhan layanan TI.

c. *Product/Technology*

Perspektif *product/technology* fokus pada memperhitungkan teknologi yang digunakan, perangkat keras dan perangkat lunak, anggaran dan infrastruktur layanan TI.

d. *Process*

Perspektif *process* berkaitan dengan menjaga proses layanan agar dapat disampaikan kepada pengguna sesuai dengan aliran proses yang telah direncanakan sehingga dapat memuaskan pelanggan.

Perspektif ITSM menjadi landasan untuk memberi kepuasan dalam menyelenggarakan layanan TI. Layanan yang berhasil dan bermanfaat bagi pengguna akan meningkatkan kualitas dan mutu layanan TI itu sendiri. Manfaat yang dimiliki ITSM adalah meningkatkan kualitas penyediaan layanan, menyesuaikan biaya dan kualitas layanan, menghasilkan layanan yang memenuhi kebutuhan dan tuntutan bisnis, pelanggan dan pengguna,

proses yang terintegrasi terpusat; setiap orang mengetahui peran dan tanggung jawab dalam penyediaan layanan, selalu belajar dari pengalaman, dan dibuktikan dalam indikator kinerja.

B. Manfaat ITSM

Manfaat dari ITSM, yaitu:

1) Peningkatan mutu penyediaan layanan.
2) Biaya kualitas pelayanan dapat dibenarkan.
3) Pelayanan yang memenuhi bisnis, pelanggan dan tuntutan dari user.
4) Proses Bisnis yang terjadi dapat lebih terpusat.
5) Setiap orang mengetahui peran dan tanggung jawab mereka dalam penyediaan layanan.
6) Belajar dari pengalaman sebelumnya.
7) Indikator kinerja dapat dibuktikan.

2.9.2 ITIL *(IT Infrastructure Library)*

A. Definisi ITIL

Menurut Catlidge (2007), ITIL (*IT Infrastructure Library*) adalah sebuah kerangka kerja (*framework*) umum yang menggambarkan *best practice* dalam *IT Service Management*. ITIL menyediakan kerangka kerja untuk manajemen TI dan berfokus pada pengukuran dan perbaikan secara terus menerus dari layanan TI yang diberikan, baik dari sudut pandang bisnis maupun konsumen. Fokus ini yang telah menjadikan faktor keberhasilan implementasi ITIL secara global.

Menurut Addy (2007), ITIL merupakan kumpulan dari petunjuk-petunjuk yang dikembangkan *United Kingdom's Office of Government Commerce* (OGC). Petunjuk-petunjuk ini, yang menggambarkan proses-proses yang terintegrasi, yang menyediakan pendekatan praktik terbaik untuk mengelola layanan TI.

Dari pengertian beberapa ahli dapat disimpulkan bahwa ITIL memberikan pengaruh kepada manajemen termasuk di dalamnya manajemen manusia dan proses, efektifitas teknologi, serta efisiensi dan ekonomis dalam memberikan pelayanan bisnis dengan *service level* yang telah disetujui bersama antara TI dengan bisnis.

B. Keuntungan ITIL

Menurut Cartlidge (2007), beberapa keuntungan dari ITIL antara lain:

1. Meningkatkan kepuasan *user* dan pelanggan terhadap layanan TI.
2. Memperbaiki ketersediaan layanan, yang berpengaruh secara langsung dalam meningkatkan keuntungan dan pendapatan bisnis.
3. Menghemat keuangan, dari pengurangan kerja, kehilangan waktu.
4. Memperbaiki manajemen sumber daya dan kegunaan.
5. Memperbaiki pembuatan keputusan dan mengoptimalkan risiko.
6. Memperbaiki waktu terhadap pasar untuk produk baru dan layanan.

2.9.3 COSO *(Committee of Sponsoring Organizations of the Treadway Commission)*

A. Definisi COSO

COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) sebuah *framework* yang dibuat oleh sektor swasta untuk menghindari tindak korupsi yang sedang marak terjadi di Amerika pada sekitar tahun 1970. COSO berkaitan dengan FCPA yang dikeluarkan oleh SEC dan US Congress pada tahun 1977 yang bertujuan untuk melawan *fraud* dan korupsi yang sedang maraknya terjadi di Amerika sekitar tahun 70an. Yang membedakannya adalah FCPA merupakan inisiatif dari eksekutif-legislatif, sedangkan COSO merupakan inisiatif dari sektor swasta.

Sektor swasta ini membentuk *National Commission on Fraudulent Financial Reporting* atau dikenal juga dengan *The Treadway Commission*di tahun 1985. Komisi ini disponsori oleh 5 professional association yaitu: AICPA (*The American Institute of Certified Public Accountants*), AAA (*The American Accounting Association*), FEI (*Financial Executives International*), IIA (*The Institute of Internal Auditors*), IMA (*The Institute of Management Accountants*). Tujuan komisi ini adalah melakukan riset mengenai fraud dalam pelaporan keuangan (*fraudulent on financial reporting*) dan membuat rekomendasi yang terkait dengannya untuk perusahaan publik, auditor independen, SEC, dan institusi pendidikan.

Misi utama dari COSO adalah "Memperbaiki atau meningkatkan kualitas laporan keuangan entitas melalui etika bisnis, pengendalian internal yang efektif, dan *corporate governance*. COSO mengembangkan studi mengenai

sebuah model untuk mengevaluasi pengendalian internal. Pada tehun 1992, telah diselesaikan studi tersebut dengan memperkenalkan sebuah "kerangka kerja pengendalian internal" yang akhirnya menjadi sebuah pedoman bagi para eksekutif, dewan direksi, regulator, penyusun standar, organisasi profesi, dan lainnya sebagai kerangka kerja yang komprehensif untuk mengukur efektifitas pengendalian internal.

B. 8 Komponen dari COSO

Dijelaskan ada delapan (8) komponen dalam *Enterprise Risk Management*, yaitu:

1. 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, nilai-nilai etika dan integritas, dan lingkungan dimana kesemuanya tersebut berjalan. *Risk Management Philosophy – Risk Appetite – Board of Directors – Integrity and Ethical Values Commitment to Competence –Organizational Structure – Assignment of Authority andResponsibility – Human Resource Standards.*

2. 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. *Strategic Objectives – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerances.*

3. 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. *Vents – InfluencingEvent Interdependencies – Event Categories – Distinguishing Risks and Opportunities.*

4. Penilaian Risiko (*Risiko Assessment*)

   Risiko dianalisis dengan memperhitungkan kemungkinan terjadi (*likelihood*) dan dampaknya (*impact*), sebagai dasar bagi penentuan pengelolaan risiko. *Inherent and Residual Risk – Establishing Likelihood and Impact – Data Sources – Assessment Techniques – Event.*

5. 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*. *Evaluating Possible Responses – Selected Responses – Portfolio View.*

6. Kegiatan Pengendalian (*Control Activities*)

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

Integration with Risk Response – Types of Control Activities – Policies and Procedures – Controls over Information Systems – Entity Specific.

7. Informasi dan Komunikasi (*Information and Communication*)

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

8. 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. *Ongoing Monitoring Activities – Separate Evaluations – Reporting Deficiencies.*

2.9.4 COBIT (*Control Objective for Information & Related Technology)*

A. Definisi COBIT

Menurut Sasongko (2009), *Control Objective for Information & Related Technology* (COBIT) adalah sekumpulan dokumentasi *best practice* untuk *IT Governance* yang dapat membantu auditor, pengguna (*user*), dan manajemen, untuk menjembatani *gap* antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI.

Gondodiyoto (2007) menjabarkan bahwa COBIT adalah sekumpulan dokumentasi *best practice* untuk tata kelola TI yang dapat membantu auditor, pengguna sistem, dan manajemen dalam menjembatani risiko organisasi, kebutuhan pengendalian, dan masalah-masalah teknis TI. Gondodiyoto (2007) membuat arahan terhadap audit Sistem Informasi untuk suatu organisasi.

Karena adanya arahan yang dibuat oleh Gondodiyoto (2007) maka diharapkan para manajer, *auditor*, *user* memanfaatkan arahan tersebut dengan baik.

Menurut COBIT, untuk memenuhi tujuan bisnis perusahaan informasi harus sesuai dengan kriteria pengendalian tertentu yang disebut sebagai kriteria informasi COBIT, yaitu:

- *Effectiveness* (Efektifitas)

  Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, disampaikan tepat waktu, tepat, konsisten, dan dapat dipercaya.

- *Efficiency* (Efisiensi)

  Penyediaan informasi melalui penggunaan sumber daya (yang paling produktif dan ekonomis) yang optimal.

- *Confidentiality* (Kerahasiaan)

  Berkaitan dengan proteksi pada informasi penting dari pengungkapan yang tidak sah atau pihak-pihak yang tidak memiliki otorisasi.

- *Integrity* (Integritas)

  Berkaitan dengan keakuratan dan kelengkapan informasi serta validitas yang sesuai dengan nilai-nilai bisnis dan ekspektasi.

- *Availability* (Ketersediaan)

  Fokus terhadap ketersediaan informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun di masa yang akan datang. Ini

juga terkait dengan pengamanan sumber daya yang diperlukan dan terkait.

- *Compliance* (Kepatuhan)

  Pemenuhan informasi yang sesuai dengan ketentuan hukum, peraturan dan rencana perjanjian/kontrak untuk proses bisnis.

- *Reliability* (Handal)

  Pemberian informasi yang tepat bagi manajemen untuk mengoperasikan perusahaan dan pemenuhan kewajiban mereka untuk membuat laporan keuangan dan tanggung jawab kepada pemerintah.

B. Sejarah COBIT

COBIT pertama kali diterbitkan pada tahun 1996, kemudian edisi kedua dari COBIT diterbitkan pada tahun 1998. Pada tahun 2000 dirilis COBIT 3.0 dan COBIT 4.0 pada tahun 2005. Kemudian COBIT 4.1 dirilis pada tahun 2007 dan saat ini COBIT yang terakhir dirilis adalah COBIT 5 yang dirilis pada tahun 2012. COBIT merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan yang dilengkapi dengan *balance scorecard* dan dapat digunakan sebagai acuan model (seperti COSO) dan disejajarkan dengan standar industri, seperti ITIL, CMM, BS779, ISO 9000.

COBIT *Framework* dikembangkan oleh *IT Governance Institute*, sebuah organisasi yang melakukan studi tentang model pengelolaan TI yang berbasis di Amerika Serikat. COBIT berorientasi pada bisnis yang di-*design* dan dikerjaan tidak hanya oleh *user* dan *auditor*, tetapi juga sebuah panduan komprehensif bagi pihak manajemen maupun pemilik bisnis proses tersebut.

COBIT memberikan sebuah *Maturity process* untuk mengendalikan proses TI sehingga pihak manajemen dapat memetakan dimana posisi perusahaan tersebut, keadaaan perusahaan sesuai tidaknya dengan *class industry* ataupun terhadap standar internasional, faktor kritikal sukses organisasi yang mendefinisikan prioritas manajemen *key goal indicator* dan *key performance indicator* untuk menjadi landasan tolak ukur untuk mengukur keberhasilan TI dalam mencapai tujuan dan kesesuaiannya dengan kebijakan organisasi.

C. Manfaat Penerapan COBIT

Menurut *The IT Governance Institute (ITGI),* manfaat dari penerapan COBIT sebagai kerangka tata kelola TI meliputi:

a) Penggunan bahasa yang umum bagi para eksekutif, manajemen dan profesional TI.
b) Pemahaman yang lebih baik tentang bagaimana bisnis dan TI dapat bekerja sama untuk keberhasilan pengiriman inisiatif TI.
c) Peningkatan efisiensi dan optimalisasi biaya.
d) Mengurangi risiko operasional.
e) Pengembangan kebijakan yang jelas.
f) Audit yang lebih efisien dan sukses.
g) Kepemilikan dan tanggung jawab yang jelas, berdasarkan proses orientasi.

2.10 COBIT 5

COBIT versi 5 atau dikenal dengan nama COBIT 5 adalah edisi terbaru dari *Framework* COBIT ISACA yang menyediakan penjabaran bisnis secara *end-to-*

end dari tata kelola teknologi informasi perusahaan untuk menggambarkan peran utama dari informasi dan teknologi dalam menciptakan nilai perusahaan.

COBIT 5 adalah sebuah versi pembaharuan yang menyatukan cara berpikir yang mutakhir di dalam teknik-teknik dan tata kelola TI perusahaan. Menyediakan prinsip-prinsip, praktik-praktik, alat-alat analisa yang telah diterima secara umum untuk meningkatkan kepercayaan dan nilai sistem-sistem informasi. COBIT 5 dibangun berdasarkan pengembangan dari COBIT 4.1 dengan mengintegrasikan Val IT dan Risk IT dari ISACA, ITIL, dan standar-standar yang relevan dari ISO.

2.10.1 Keunggulan COBIT 5

Menggunakan COBIT 5 *for Information Secutiry* memberikan sejumlah kemampuan yang berhubungan dengan keamanan informasi untuk perusahaan sehingga dapat menghasilkan manfaat perusahaan seperti:

- Mengurangi kompleksitas dan meningkatkan efektivitas biaya karena integrasi yang lebih baik dan lebih mudah.
- Meningkatkan kepuasan pengguna.
- Meningkatkan integrasi keamanan informasi dalam perusahaan.
- Menginformasikan risiko keputusan dan risk awareness.
- Meningkatkan pencegahan, deteksi dan pemulihan.
- Mengurangi insiden (dampak) keamanan informasi.
- Meningkatkan dukungan untuk inovasi dan daya saing.
- Meningkatkan pengelolaan biaya yang berhubungan dengan fungsi keamanan informasi.
- Pemahaman yang lebih baik dari keamanan informasi.

2.10.2 Keamanan Informasi dari COBIT 5

ISACA mendefinisikan keamanan informasi sebagai berikut:

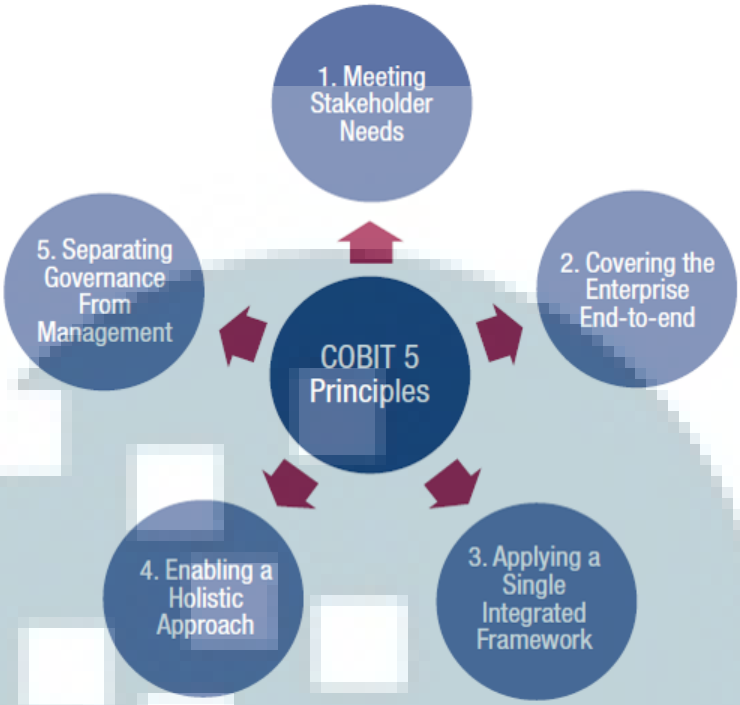
"Ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when required (availability)."

Dari pernyataan ISACA tersebut di dapatkan 3 poin utama, yaitu:

- *Confidentiality* berarti menjaga hak akses dan penggunaan wewenang untuk melindungi privacy dan kepemilikan informasi.
- *Integrity* berarti menjaga informasi dari modifikasi atau perusakan dan termasuk memastikan bahwa informasi yang ada merupakan informasi asli dan tidak ada penolakan (non-repudiation) jika akan dilakuan pembuktian terhadap sistem.
- *Availability* berarti memastikan dalam hal waktu dan kehandalan dalam mengakses dan menggunakan informasi agar selalu tersedia.

2.10.3 Prinsip-prinsip COBIT 5

COBIT 5 memiliki prinsip dan *enabler* yang bersifat umum dan bermanfaat untuk semua ukuran perusahaan, baik komersial maupun non-profit ataupun sektor publik. 5 Prinsip tersebut adalah *Meeting stakeholder needs*, *Covering enterprise end-to-end*, *Applying a single intergrated framework*, *Enabling a holistic approach* dan *Separating governance from management*. Gambar prinsip-prinsip COBIT 5 dapat dilihat pada Gambar 2.1.



Gambar 2.1 Prinsip COBIT 5

Sumber: COBIT 5 Framework – ISACA

- **Prinsip 1: *Meeting stakeholder needs.***

Perusahaan menciptakan nilai bagi *stakeholder* mereka dengan mempertahankan keseimbangan antara realisasi manfaat dan optimalisasi risiko serta penggunaan sumber daya. COBIT 5 menyediakan semua proses yang diperlukan dan *enabler* lain untuk mendukung penciptaan nilai bisnis melalui penggunaan TI. Karena setiap perusahaan memiliki tujuan yang berbeda, perusahaan dapat menyesuaikan COBIT 5 sesuai konteksnya sendiri melalui tujuan perusahaan, menerjemahkan tujuan tertinggi perusahaan tingkat tinggi menjadi dapat dikelola dikelola, khususnya tujuan TI dan pemetaan ini untuk proses tertentu dan praktek.

- **Prinsip 2:** ***Covering enterprise end-to-end.***

COBIT 5 mengintegrasikan tata kelola perusahaan TI dalam tata kelola perusahaan:

  - Mencakup semua fungsi dan proses dalam perusahaan; COBIT 5 tidak hanya berfokus pada fungsi TI, namun memperlakukan informasi dan teknologi yang terkait dengan aset yang ditangani sama seperti aset lainnya oleh semua orang dalam perusahaan.
  - Menganggap semua tata kelola dan manajemen yang aktif berhubungan dengan TI menjadi perusahaan yang luas dan keseluruhan, termasuk segala sesuatu dan semua orang *internal* dan *eksternal* yang relevan dengan tata kelola dan manajemen informasi perusahaan dan terkait dengan TI.

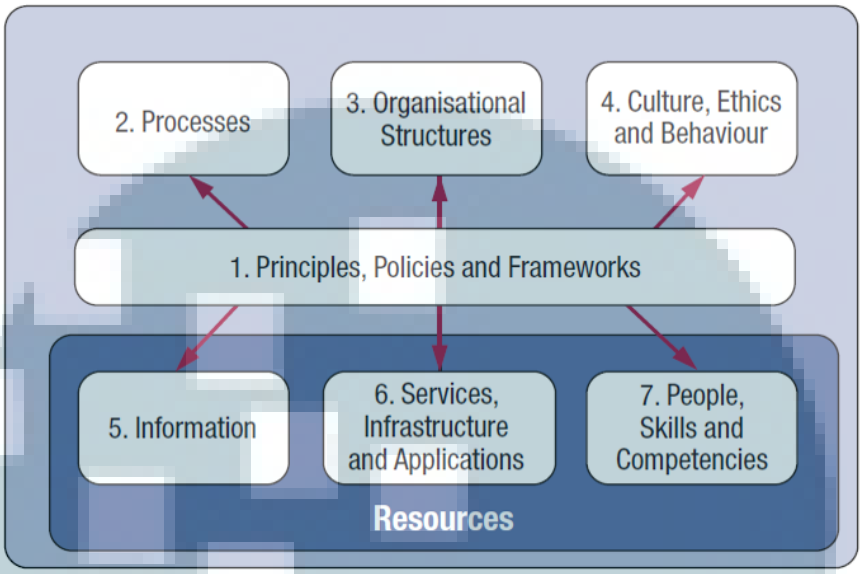
- **Prinsip 3:** ***Applying a single integrated framework.***

Ada banyak hal yang berkaitan dengan IT standar dan praktik terbaik, masing-masing memberikan bimbingan pada subset dari kegiatan TI. COBIT 5 sejalan dengan standar lain yang relevan dan kerangka pada *level* yang paling tinggi/rumit, dengan demikian dapat berfungsi sebagai kerangka kerja menyeluruh untuk tata kelola dan manajemen perusahaan TI.

- **Prinsip 4:** ***Enabling a holistic approach.***

Manajemen TI perusahaan yang efisien dan efektif memerlukan pendekatan yang menyeluruh, mempertimbangkan beberapa komponen yang berinteraksi. COBIT 5 mendefinisikan satu set *enabler* untuk mendukung pelaksanaan tata kelola yang komprehensif dan sistem

manajemen TI untuk perusahaan. *Enabler* yang didefinisikan secara luas sebagai sesuatu yang dapat membantu untuk mencapai tujuan perusahaan.



Gambar 2.2 Prinsip 4: Enabling a Holistic Approach
Sumber: COBIT 5 Framework – ISACA

Kerangka COBIT 5 menjelaskan tujuh kategori *enebler*:

a. Prinsip, kebijakan dan kerangka kerja adalah kendaraan untuk menerjemahkan perilaku yang diinginkan menjadi panduan praktis untuk sehari-hari manajemen.
b. Proses menggambarkan set terorganisir praktek dan kegiatan untuk mencapai tujuan tertentu dan menghasilkan set output dalam mendukung pencapaian keseluruhan TI-tujuan yang terkait.
c. Struktur organisasi adalah pengambilan keputusan kunci entitas dalam suatu perusahaan.
d. Budaya, etika dan perilaku individu dan perusahaan yang sangat sering diremehkan sebagai faktor keberhasilan dalam kegiatan tata kelola dan manajemen.

e. Informasi diperlukan untuk menjaga organisasi berjalan dengan baik dan diatur, tetapi pada tingkat operasional, informasi sangat sering produk utama dari perusahaan itu sendiri.

f. Layanan, infrastruktur dan aplikasi meliputi infrastruktur, teknologi dan aplikasi yang menyediakan perusahaan dengan pengolahan informasi teknologi dan jasa.

g. Manusia, keterampilan dan kompetensi yang diperlukan untuk berhasil menyelesaikan semua kegiatan, dan untuk membuat keputusan yang benar dan mengambil tindakan korektif.

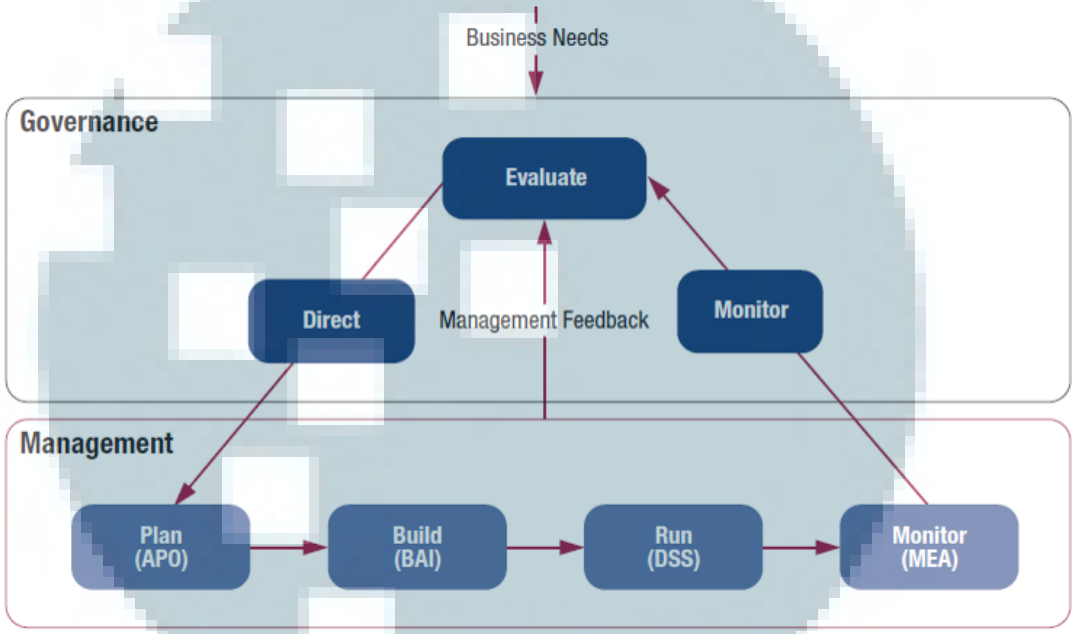
- **Prinsip 5:** ***Separating governance from management.***

COBIT 5 membagi dengan jelas antara tata kelola dengan manajemen, dimana kedua hal tersebut mencakup berbagai jenis kegiatan, memerlukan struktur organisasi yang berbeda dan melayani tujuan yang berbeda. Perbedaan utama *governance* (tata kelola) dan *management* (manajemen):

- *Governance* adalah tata kelola yang memastikan bahwa tujuan perusahaan dapat dicapai dengan melakukan evaluasi terhadap kebutuhan, kondisi, dan pilihan stakeholder, menerapkan arah melalui prioritas dan pengambilan keputusan terhadap arah dan tujuan yang telah disepakati. Pada Kebanyakan perusahaan, tata kelola adalah tanggung jawab dari dewan direksi dibawah kepemimpinan ketua.
- *Management* (Manajemen) berfungsi sebagai perencana, membangun, menjalankan dan memonitor aktifitas-aktifitas yang sejalan dengan arah yang ditetapkan oleh badan tata kelola untuk

mencapai tujuan perusahaan. Pada kebanyakan perusahaan, manajemen menjadi tanggung jawab eksekutif manajemen di bawah pimpinan CEO.

2.10.4 Proses Model COBIT 5



Gambar 2.3 Proses Model COBIT

Sumber: COBIT 5 Framework – ISACA

Model Referensi Proses dalam COBIT 5 membagi proses tata kelola dan manajemen TI perusahaan menjadi dua domain proses utama:

1. Tata Kelola, memuat lima proses tata kelola, dimana akan ditentukan praktik-praktik dalam setiap proses Evaluate, Direct, dan Monitor (EDM) telah didefinisikan sebagai 5 praktek.
2. Manajemen, memuat empat domain, sejajar dengan area tanggung jawab dari Merencanakan, Membangun, Menjalankan dan Memantau (PBRM), dan menyediakan ruang lingkup TI yang menyeluruh dari ujung ke ujung.

Domain ini merupakan evolusi dari domain dan struktur proses dalam COBIT 5, yaitu:

- *Align, Plan, and Organize (APO)* – Penyelarasan, Perencanaan, dan Pengaturan
- *Build, Acquire, and Implement (BAI)* – Membangun, Memperoleh, dan Mengimplementasikan
- *Deliver, Service and Support (DSS)* – Mengirimkan, Layanan, dan Dukungan
- *Monitor, Evaluate, and Assess (MEA)* – Pengawasan, Evaluasi, dan Penilaian

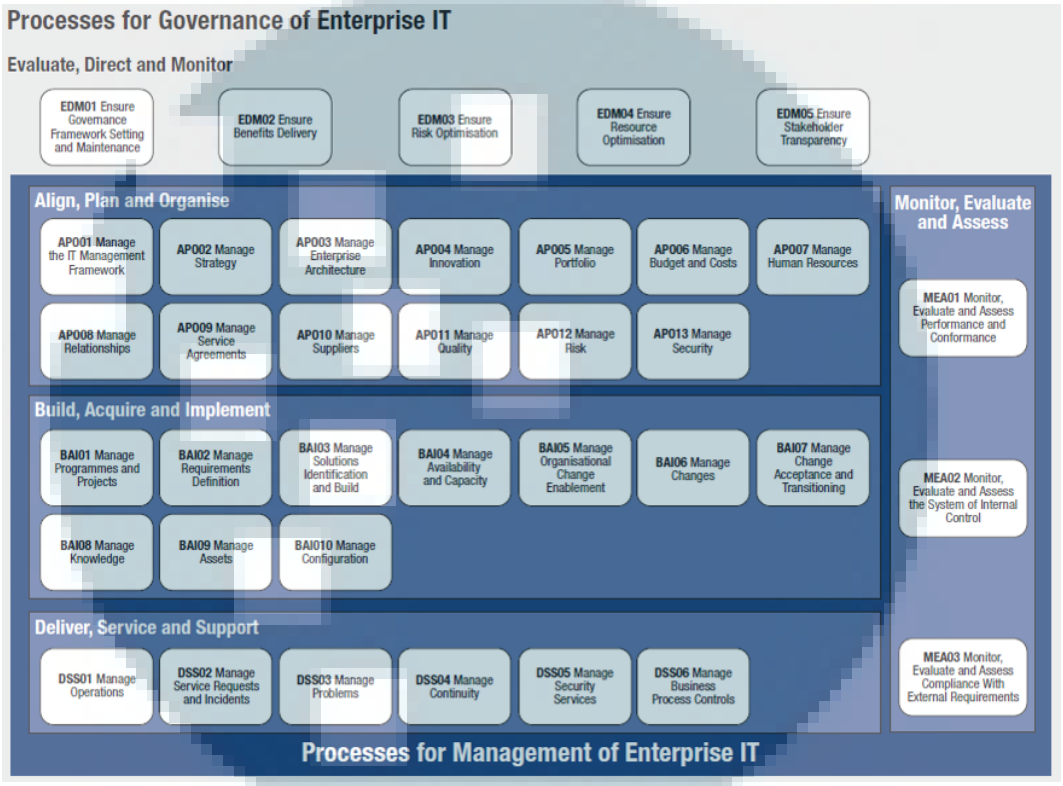
2.10.5 Proses Referensi Model COBIT 5

COBIT 5 membantu perusahaan menciptakan nilai yang optimal dari TI dengan menjaga keseimbangan antara menyadari manfaatnya dan mengoptimalkan tingkat risiko serta penggunaan sumber daya. Kerangka kerja ini membahas bisnis dan area fungsional IT di suatu perusahaan dan mempertimbangkan kepentingan yang berkaitandengan IT secara internal dan eksteranl bagi para stake holder. Perusahaan dari semua ukuran, baik yang komersial, non-profit atau di sektor publik, bisa mendapatkan keuntungan dari COBIT 5. COBIT 5 didasarkan pada lima prinsip utama tata kelola dan manajemen perusahaan TI yaitu:

1. Prinsip 1: Memenuhi Kebutuhan Stakeholder.
2. Prinsip 2: Melingkupi End-to-End Perusahaan.
3. Prinsip 3: Menerapkan Satu, Kerangka Terintegrasi.
4. Prinsip 4: Memungkinkan Pendekatan Holistik.
5. Prinsip 5: Memisahkan Tata Kelola dari Manajemen

COBIT 5 memberikan definisi dari proses-proses dalam siklus hidupnya (model referensi proses), bersamaan dengan arsitektur yang menggambarkan

hubungan antara proses. 5 Proses model referensi COBIT (PRM) terdiri dari 37 proses menggambarkan siklus hidup untuk tata kelola TI, seperti yang ditunjukkan pada gambar 2.4.



Gambar 2.4 Proses Referensi Model COBIT 5

Sumber: COBIT 5 Framework – ISACA

Pada gambar 2.4 menunjukan lengkap 37 set tata kelola dan manajemen proses dalam COBIT 5. Semua rincian proses, sesuai dengan model proses yang diuraikan sebelumnya, termasuk dalam COBIT 5. Berikut adalah 37 set tata kelola dan manajemen proses yang terbagi menjadi 5 domain utama dalam COBIT 5, diantaranya:

1. ***Evaluate, Direct, and Monitor (EDM):*** proses pengelolaan yang berhubungan dengan pengelolaan sasaran stakeholder, nilai pengiriman, optimisasi risiko dan sumber daya, termasuk praktek dan aktivitas yang

ditujukan pada pengevaluasian pilihan strategi, memberikan pengarahan IT dna pemonitoran *outcome*.

2. ***Align, Plan and Organise (APO):*** memberi arahan pada solusi *delivery* (BAI) dan *service delivery and support* (DSS). Domain ini mencakup strategi dan taktik, serta berfokus pada pengidentifikasian cara terbaik pengkontribusian IT untuk pencapaian dari sasaran bisnis. Realisasi dari visi strategi harus direncanakan, dikomunikasikan, dan dikelola untuk prespektif yang berbeda. Pengorganisasian yang benar dan infrastruktur teknologi harus ditempatkan di tempat yang benar.
3. ***Build, Acquire and Implement (BAI):*** memberikan solusi dan menjadikanya pelayanan. Untuk merealisasi strategi TI, solusi TI harus diidenttifikasi, dikembangkan atau didapatkan, begitupun diimplementasikan dan di integrasikan pada proses bisnis. Perubahan dan maintenance dari sistem yang ada juga dilingkup domain ini, untuk memastikan solusi sesuai dengan tujuan bisnis.
4. ***Deliver, Service and Support (DSS):*** domain ini berfokus dengan *actual delivery* and *support of required services*, yang temasuk *service delivery*, pengelolaan atas keamanan dan kontinuitas, layanan bantuan untuk users, dan manajemen atas data dan fasilitas operasional.
5. ***Monitor, Evaluate and Assess (MEA):*** memonitor semua proses untuk memastikan pengarahan yang diberikan ditaati. Semua proses IT harus diperiksa secara regular tiap waktu untuk memastikan kebutuhan kualitas dan ketaatan dengan kebutuhan pengendalian. Domain mengajukan

manajemen kinerja, monitor dari internal kontrol, ketaaatan dan tata kelola yang regular.

Pada seluruh lima domain ada 37 proses IT yang terdefinisi, proses COBIT 5 diantaranya adalah sebagai berikut:

1. EDM01: *Ensure governance framework setting and maintenance*. (Memastikan kerangka kerja tata kelola pengaturan dan pemeliharaan).
2. EDM02: *Ensure benefits delivery*. (Memastikan penyampaian yang bermanfaat).
3. EDM03: *Ensure risk optimisation*. (memastikan optimisasi risiko).
4. EDM04: *Ensure resource optimisation*. (memastikan optimisasi sumber daya).
5. EDM05: *Ensure stakeholder transparency*. (memastikan transparansi stakeholder).
6. APO01: *Manage the IT management framework*. (mengelola manajemen kerangka kerja IT).
7. APO02: *Manage strategy*. (mengelola strategi).
8. APO03: *Manage enterprise architecture*. (mengelola arsitektur perusahaan).
9. APO04: *Manage innovation*. (mengelola inovasi).
10. APO05: *Manage portfolio*. (mengelola portofolio).
11. APO06: *Manage budget and costs*. (mengelola anggaran dan biaya).

12. APO07: *Manage human resources*. (mengelola sumberdaya manusia).
13. APO08: *Manage relationships*. (mengelola hubungan).
14. APO09: *Manage service agreements*. (mengelola persetujuan service/layanan).
15. APO10: *Manage suppliers*. (mengelola suppliers).
16. APO11: *Manage quality*. (mengelola kualitas).
17. APO12: *Manage risk*. (mengelola risiko).
18. APO13: *Manage security*. (mengelola keamanan).
19. BAI01: *Manage programmes and projects*. (mengelola program dan proyek).
20. BAI02: *Manage requirements definition.* (mengelola definisi persyaratan).
21. BAI03: *Manage solutions identification and build.* (mengelola identifikasi solusi
    dan pembangunan).
22. BAI04: *Manage availability and capacity.* (mengelola ketersediaan dan kapasitas).
23. BAI05: *Manage organisational change enablement.* (mengelola pemberdayaan perubahan organisasi).
24. BAI06: *Manage changes*. (mengelola perubahan).
25. BAI07: *Manage change acceptance and transitioning*. (mengelola penerimaan terhadap perubahan dan transisi).
26. BAI08: *Manage knowledge*. (mengelola pengetahuan).

27. BAI09: *Manage assets*. (mengelola asset/modal).
28. BAI10: *Manage configuration*. (mengelola konfigurasi).
29. DSS01: *Manage operations*. (mengelola operasi).
30. DSS02: *Manage service requests and incidents*. (mengelola permintaan layanan dan insiden).
31. DSS03: *Manage problems*. (mengelola masalah).
32. DSS04: *Manage continuity*. (mengelola kontinuitas).
33. DSS05: *Manage security services*. (mengelola pelayanan keamanan).
34. DSS06: *Manage business process controls*. (mengelola pengendalian proses bisnis).
35. MEA01: *Monitor, evaluate and assess performance and conformance*. (memonitor, mengevaluasi dan mengukur kinerja dan kesesuaian).
36. MEA02: *Monitor, evaluate and assess the system of internal control*. (memonitor, mengevaluasi dan mengukur sistem dari pengendalian internal).
37. MEA03: *Monitor, evaluate and assess compliance with external requirements*.
    (memonitor, mengevaluasi dan mengukur kecocokan dengan kebutuhan
    eksternal/luar).