

BAB II

LANDASAN TEORI

2.1. Definisi Visi, Misi, dan Tujuan

Sebuah perusahaan atau instansi harus mempunyai visi, misi, dan tujuan untuk menentukan arah perkembangannya. Definisi dari visi (Indrajit, 2006) merupakan sesuatu yang dicanangkan oleh pendiri perusahaan. Namun yang harus diperhatikan, visi bukanlah mimpi, namun sesuatu yang mungkin terwujud. Sedangkan misi ditetapkan sebagai jawaban terhadap visi yang telah ditetapkan sebelumnya. Misi masih merupakan sesuatu yang memiliki arti global dan cenderung generik. Oleh karena itu, ditentukan beberapa objektif yang ingin dicapai dalam berbagai hal sehubungan dengan misi yang dicanangkan tersebut.

2.2. Visi, Misi, dan Tujuan Polisi Militer TNI AL

Polisi Militer TNI AL adalah korps / kesatuan teknis militer dari TNI AL yang berfungsi Penyidikan, Penyelidikan Kriminal, Penegakan Disiplin dan Tata Tertib, Penegakan Hukum, Pengamanan Fisik, Pembinaan Tuna Tertib Militer dan Pengurusan Tawanan Perang mempunyai visi, misi, dan tujuan yang tertuang sebagai berikut:

2.2.1. Visi POMAL

Terwujudnya TNI AL yang handal dan disegani dan menjadi pendukung operasional TNI AL dalam penegakan hukum.

2.2.2. Misi POMAL

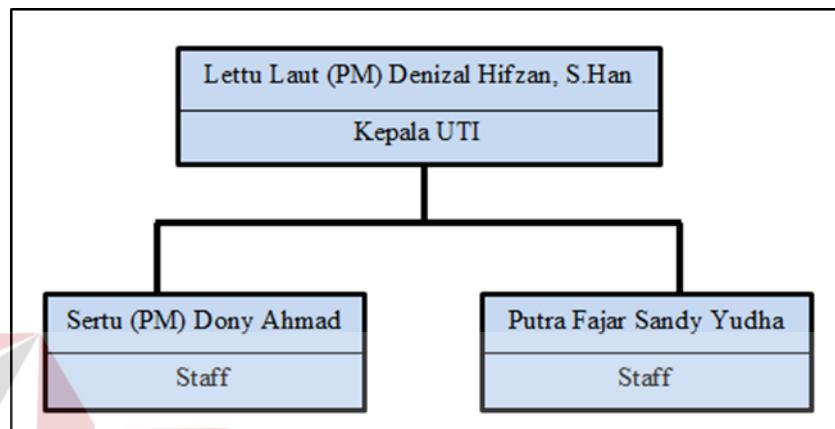
1. Penyelidikan kriminal dan Pengamanan fisik
2. Penegakan hukum, Penegakan disiplin dan tata tertib militer
3. Penyidikan, pengurusan tahanan dan tuna tertib militer
4. Pengurusan tahanan keadaaan bahaya atau operasi militer tawanan perang dan interniran perang
5. Pengawalan protokoler Kenegaraan
6. Pengendalian lalu lintas Militer
7. Penyelenggaraan Surat Izin Mengemudi (SIM) TNI AL

2.2.3. Tujuan POMAL

1. Melaksanakan tugas TNI matra laut di bidang pertahanan dan Hukum
2. Menegakkan hukum dan menjaga keamanan di wilayah laut yurisdiksi nasional sesuai dengan ketentuan hukum nasional dan hukum internasional yang telah diratifikasi
3. Melakukan pembinaan terhadapa tahanan agar menjadi TNI yang berkualitas
4. Menghasilkan penelitian inovatif, yang mendorong pengembangan ilmu pengetahuan dan teknologi dalam skala nasional dan internasional
5. Menghasilkan pengabdian masyarakat dalam bentuk penanganan bencana alam dan bantuan kepada masyarakat
6. Melakukan proses pembuatan SIM TNI AL
7. Melakukan proses Daftar Pencarian Orang

2.3. Profil Unit Teknologi Informasi dan Cyber Crime (UTI) POMAL

POMAL memiliki unit teknologi informasi (UTI) yang bertugas mendukung kegiatan operasionalnya. Adapun struktur organisasi dari UTI Pomal Surabaya sebagai berikut:



Gambar 2.1 Struktur Organisasi UTI POMAL Surabaya

2.4. Profil Unit Penegakan Hukum (GAKKUM)

POMAL memiliki unit penegakan hukum (GAKKUM) yang bertugas melaksanakan proses penegakan hukum terhadap setiap masalah yang terjadi di lingkungan TNI AL. Seperti melaksanakan proses penangkapan, penyelidikan dan penyidikan.

2.5. Profil Unit Harian Ketertiban (HARTIB)

POMAL memiliki unit Harian Ketertiban (HARTIB) yang bertugas melaksanakan proses ketertiban dan kedisiplinan terhadap seluruh Anggota TNI AL sesuai dengan peraturan.

2.6. Audit

Definisi secara umum tentang audit adalah bahwa “*Auditing is an independent investigation of some particular activity*”. Sebetulnya kata Audit itu sendiri berasal dari Bahasa Latin *Audire* yang dalam Bahasa Inggris berarti *to hear*. Makna yang dimaksud disini adalah “*hearing about the account's balances*” oleh para pihak terkait terhadap pihak ketiga yang netral (tidak ada *vested interest*) mengenai catatan keuangan perusahaan yang dikelola oleh orang-orang tertentu yang bukan sekaligus pemiliknya. *Auditing*, meskipun perkembangannya tidak terlepas dari perkembangan akunting, namun sebagai cabang ilmu *auditing* berada diluar lingkup ilmu akuntansi. *Auditing* memiliki sejarah/perkembangan panjang. Bahkan *Auditor* merupakan salah satu *the oldest profession in the world*. Berdasarkan makna kata *audire* (*to hear “the account balance”*) tersebut memang jenis audit yang berkaitan dengan pemeriksaan akuntansi memiliki peran dominan dan sejarah yang lebih lama. Namun pada saat ini dalam perkembangannya kemudian, perkembangan bidang audit yang lain juga telah mencapai tahapan yang signifikasi, misalnya audit internal, audit teknologi informasi, dan sebagainya (Gondodiyoto, 2007). Tujuan dari audit adalah untuk menentukan dan melaporkan tingkat kesamaan antara informasi yang dinilai dengan ukuran atau kriteria yang ada (Surendro, 2009).

Auditing adalah sebuah proses sistematis yang dilakukan oleh seorang yang memiliki kompetensi dan bersikap independent, mengenai perolehan dan penilaian atas bukti secara obyektif, yang dilakukan dengan melakukan pengumpulan dan penilaian atas bukti-bukti informasi yang dapat dikuantitasikan dan terkait pada suatu entitas ekonomi tertentu, berkenaan dengan pernyataan

mengenai tindakan-tindakan dan kejadian-kejadian ekonomi dengan tujuan untuk menentukan tingkat kesesuaian antara pernyataan tersebut dengan kriteria yang telah ditetapkan serta untuk mengkomunikasikan hasil-hasilnya kepada pihak-pihak yang berkepentingan (Purwono, 2007).

2.7. Audit Sistem Informasi

Definisi Audit Sistem Informasi (atau beberapa kalangan lebih menyukai untuk menyebut audit teknologi informasi) dapat dikemukakan sebagai berikut:

- a. *IS Control & Audit* (Weber, 2007)

“The process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintain data integrity, allows organizational goals to be achieved effectively, and uses resource efficiently”.

- b. *CISA Review Manual* (ISACA, 2007)

“The process of collecting and evaluating evidence to determine whether information systems and information technology environments adequately safeguards assets, maintain data and system integrity, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently, and have in effect internal controls that provide reasonable assurance that operational and control objectives will be meet”.

Proses audit SI sendiri dimulai dengan membuat batasan audit yang akan dilakukan. Batasan ini diperlukan agar proses audit tidak melebar sementara sumber daya dan waktu yang dimiliki terbatas. Proses ini kemudian dilanjutkan dengan evaluasi terhadap kontrol yang ada dan kemudian melakukan testing dan mengumpulkan bukti yang ada kemudian mengkomunikasikan hasilnya dengan pihak manajemen (Priandoyo, 2006).

2.8. COBIT 4.1

Information System Audit and Control Association (ISACA) memperkenalkan sebuah kerangka untuk mengelola *IT Governance* di sebuah perusahaan yang dikenal dengan nama COBIT (Indrajit, 2004). COBIT adalah *a set of best practices (framework)* bagi pengelolaan teknologi informasi (*IT management*). COBIT disusun oleh IT Governance Institute (ITGI) dan Information Systems Audit and Control Association (ISACA), tepatnya Information System Audit Control Foundation's (ISACF) pada tahun 1992. Edisi pertamanya dipublikasikan pada tahun 1996, edisi kedua pada tahun 1998, edisi ketiga tahun 2000 (versi *online* dikeluarkan tahun 2003) dan COBIT versi 4 diterbitkan pada Desember 2005.

COBIT dan ISO/IEC 17799:2005 merupakan standar yang sekarang banyak digunakan (ISO/IEC 17799:2005 adalah *code of practice for implementation security management*), dan keduanya bersifat saling melengkapi. Ruang lingkup ISO/IEC 17799:2005 adalah aspek *security*, sedangkan COBIT bersifat lebih luas, merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan dan dikenal sebagai acuan model (seperti: COSO), dan disejajarkan dengan standar industri (seperti: ITIL, CMM, BS7799, ISO9000), COBIT juga dilengkapi dengan *IT balance scorecard*. Paket produk COBIT terdiri dari: *executive summary, framework, control objectives, audit guidelines, implementation tool set*, serta *management guidelines*, yang sangat berguna atau dibutuhkan oleh auditor, para *IT user*, dan para manajer.

COBIT adalah sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu para auditor, pengguna (*user*), dan manajemen,

untuk menjembatani gap antara resiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI. COBIT bermanfaat bagi auditor karena merupakan teknik yang dapat membantu dalam identifikasi TI *controls issues*. COBIT berguna bagi *IT users* karena memperoleh keyakinan atas kehandalan sistem aplikasi yang digunakan. Sedangkan para manajer memperoleh manfaat dalam keputusan investasi di bidang TI serta infrastrukturnya, menyusun rencana strategi TI (*IT Strategic Plan*), menentukan *information architecture*, dan keputusan atas pembelian atau pengadaan mesin (*procurement*). Disamping itu, dengan keterandalan sistem informasi yang ada pada sebuah organisasi, diharapkan berbagai keputusan bisnis dapat didasarkan atas informasi yang ada.

COBIT dapat dipakai sebagai alat komprehensif untuk menciptakan IT *Governance* yang ada pada suatu perusahaan. COBIT mempertemukan dan menjembatani kebutuhan manajemen dari celah atau *gap* antara resiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI, serta menyediakan referensi *best business practices* yang mencakup keseluruhan TI dan kaitannya dengan proses bisnis perusahaan dan memaparkannya dalam struktur aktivitas-aktivitas logis yang dapat dikelola serta dikendalikan secara efektif.

COBIT mendukung manajemen dalam mengoptimalkan investasi TI-nya melalui ukuran-ukuran dan pengukuran yang akan memberikan sinyal bahaya bila suatu kesalahan atau resiko akan atau sedang terjadi. Manajemen perusahaan harus memastikan bahwa sistem kendali internal perusahaan bekerja dengan baik, artinya dapat mendukung proses bisnis perusahaan yang secara jelas menggambarkan bagaimana setiap aktivitas kontrol individu memenuhi tuntutan dan kebutuhan informasi serta efeknya terhadap sumber daya TI perusahaan.

Sumber daya TI merupakan suatu elemen yang sangat disoroti COBIT, termasuk pemenuhan kebutuhan bisnis terhadap: efektivitas, efisiensi, kerahasiaan, keterpaduan, ketersediaan, kepatuhan terhadap kebijaksanaan atau aturan dan keandalan informasi (*effectiveness, efficiency, confidentiality, integrity, availability, compliance, dan reliability*).

Dengan diperkenalkan COBIT, kini tujuan audit (Gondodiyoto, 2007) bukan hanya terbatas pada konsep 3E (Efektif, efisien, ekonomi) saja, melainkan kini menjadi:

Tabel 2.1 Tujuan Audit

Efektivitas	Untuk memperoleh informasi yang relevan dan berhubungan dengan proses bisnis seperti penyampaian informasi dengan benar, konsisten, dapat dipercaya dan tepat waktu.
Efisiensi	Memfokuskan pada ketentuan informasi melalui penggunaan sumber daya yang optimal.
Kerahasiaan	Memfokuskan proteksi terhadap informasi yang penting dari orang yang tidak mempunyai hak otorisasi.
Integritas	Berhubungan dengan keakuratan dan kelengkapan informasi sebagai kebenaran yang sesuai dengan harapan dan nilai bisnis.
Ketersediaan	Berhubungan dengan informasi yang tersedia ketika diperlukan dalam proses bisnis sekarang dan yang akan datang.
Kepatuhan	Sesuai menurut hukum, peraturan dan rencana perjanjian untuk proses bisnis.
Keakuratan informasi	Berhubungan dengan ketentuan kecocokan informasi untuk manajemen mengoperasikan entitas dan mengatur pelatihan keuangan dan kelengkapan laporan pertanggungjawaban.

Kerangka kerja (*Framework*) COBIT terdiri atas beberapa arahan (*guidelines*), yakni:

1. *Control Objectives*

Terdiri atas empat tujuan pengendalian tingkat-tinggi (*high-level control objectives*) yang tercermin dalam empat domain, yaitu: *plan & organize*, *acquisition & implementation*, *delivery & support*, dan *monitoring*. Empat domain COBIT dirinci lagi menjadi 34 *high-level control objectives*, antara lain:

a. *Plan and Organize*

Membahas mengenai strategi, taktik, dan pengidentifikasi teknologi informasi dalam mendukung tercapainya tujuan bisnis. Realisasi dari visi strategis perlu direncanakan, dikomunikasikan, dan dikelola untuk perspektif yang berbeda. Domain ini harus dapat menjawab pertanyaan-pertanyaan manajemen tentang:

1. Apakah strategi teknologi informasi dan bisnis selaras?
2. Apakah perusahaan memanfaatkan sumber daya yang ada secara optimal?
3. Apakah setiap orang dalam organisasi mengerti tujuan dari penerapan teknologi informasi?
4. Apakah resiko teknologi informasi telah dimengerti dan dikelola?
5. Apakah kualitas sistem teknologi informasi sesuai dengan kebutuhan bisnis?

Pada domain *Plan and Organize* (PO) terdapat sepuluh *high-level control objectives*, antara lain:

1. PO1: *Define a Strategic IT Plan*
2. PO2: *Define the Information Architecture*
3. PO3: *Determine Technological Direction*
4. PO4: *Define the IT Processes, Organisation and Relationships*
5. PO5: *Manage the IT Investment*
6. PO6: *Communicate Management Aims and Direction*
7. PO7: *Manage IT Human Resources*
8. PO8: *Manage Quality*
9. PO9: *Assess and Manage IT Risks*
10. PO10: *Manage Projects*

b. Acquire and Implement

Domain *Acquire and Implement* berfungsi untuk merealisasikan strategi teknologi informasi, solusi-solusi teknologi informasi perlu untuk diidentifikasi, dibangun atau dibeli, sebaik diimplementasikan dan diintegrasikan pada proses bisnis. Domain ini membahas tentang perubahan-perubahan dalam teknologi informasi dan perawatan terhadap sistem yang ada untuk memastikan bahwa solusi yang ada dapat memenuhi tujuan bisnis. Domain ini harus dapat menjawab pertanyaan-pertanyaan manajemen tentang:

1. Apakah proyek baru dapat memberikan solusi untuk menjawab kebutuhan bisnis?
2. Apakah proyek baru dapat memberikan solusi terhadap nilai ketepatan waktu dan nilai anggaran biaya (*budget*)?

3. Apakah sistem baru berjalan dengan baik ketika diimplementasikan?
4. Apakah perubahan yang dilakukan tidak mengganggu proses atau kegiatan operasional bisnis yang ada?

Pada domain *Acquire and Implement* (AI) terdapat tujuh *high-level control objectives*, antara lain:

1. AI1: *Identify Automated Solutions*
2. AI2: *Acquire and Maintain Application software*
3. AI3: *Acquire and Maintain Technology Infrastructure*
4. AI4: *Enable Operation and Use*
5. AI5: *Procure IT Resources*
6. AI6: *Manage Changes*
7. AI7: *Install and Accredit Solutions and Changes*
- c. *Deliver and Support*

Domain ini berfokus pada aspek penyampaian teknologi informasi dari layanan yang dibutuhkan, yang termasuk penyampaian teknologi informasi, manajemen keamanan dan kesinambungan, pendukung layanan bagi para pengguna, manajemen data dan fasilitas-fasilitas operasional.

Domain ini harus mampu menjawab pertanyaan tentang:

1. Apakah layanan teknologi informasi yang diberikan sesuai dengan prioritas-prioritas bisnis?
2. Apakah biaya untuk teknologi informasi sudah dioptimalkan?
3. Apakah pekerja mampu menggunakan sistem teknologi informasi secara produktif dan aman?

4. Apakah kerahasiaan, integritas, dan ketersediaan tersedia untuk keamanan informasi?

Pada domain *Deliver and Support* (DS) terdapat tiga belas *high-level control objectives*, antara lain:

1. DS1: *Define and Manage Service Levels*
2. DS2: *Manage Third-party Services*
3. DS3: *Manage Performance and Capacity*
4. DS4: *Ensure Continuous Service*
5. DS5: *Ensure Systems Security*
6. DS6: *Identify and Allocate Costs*
7. DS7: *Educate and Train Users*
8. DS8: *Service Desk and Incidents*
9. DS9: *Manage the Configuration*
10. DS10: *Manage Problems*
11. DS11: *Manage Data*
12. DS12: *Manage the Physical Environment*
13. DS13: *Manage Operations*

d. Monitor and Evaluate

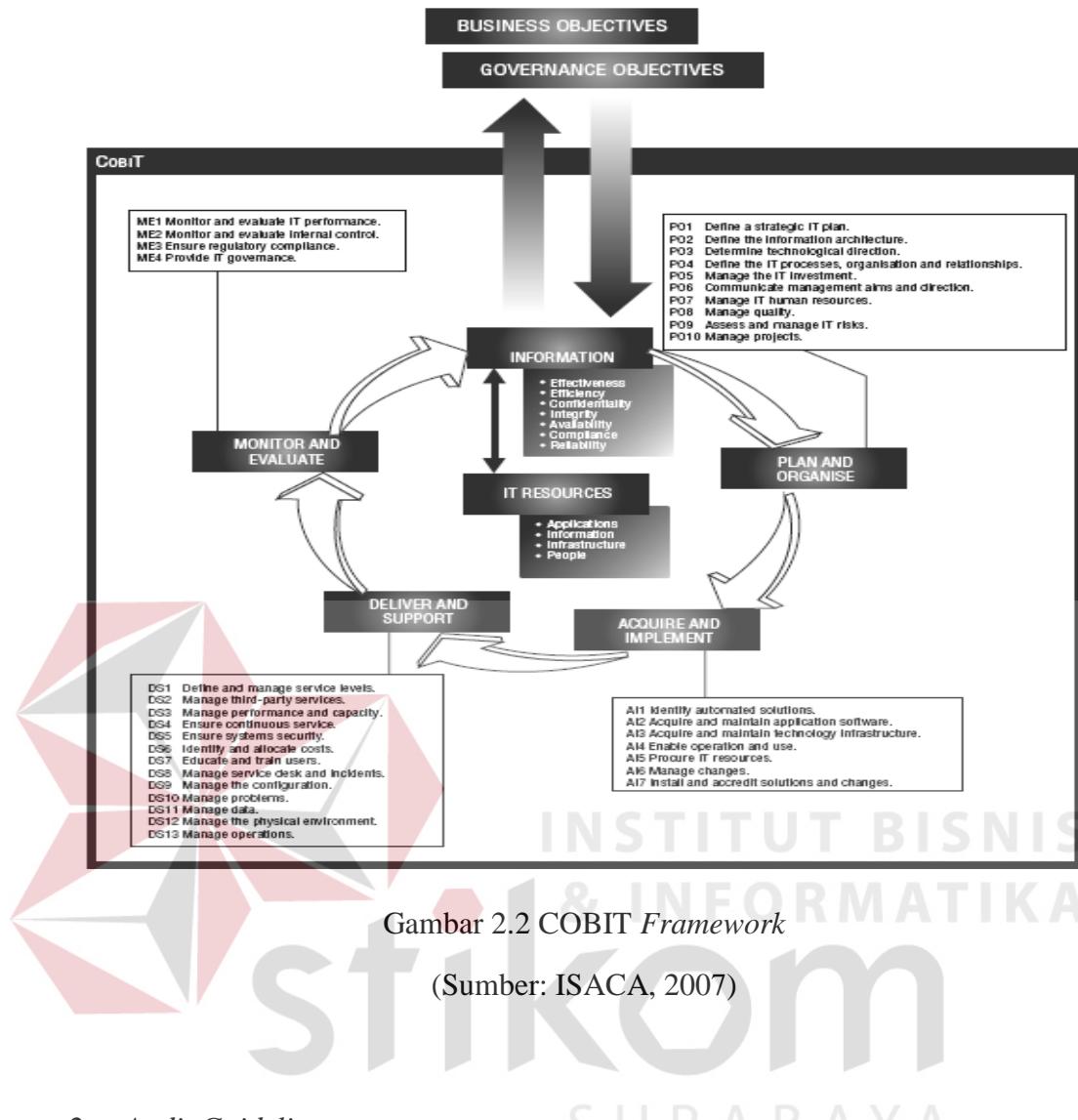
Semua proses teknologi informasi perlu dinilai secara teratur akan kualitas dan kesesuaiannya terhadap kebutuhan-kebutuhan kontrol. Domain ini membahas tentang manajemen performa, pengawasan terhadap kontrol internal, kesesuaian dengan peraturan, dan penyediaan tata kelola. Domain ini harus dapat menjawab pertanyaan-pertanyaan tentang:

1. Apakah performa teknologi informasi diukur untuk mendeteksi permasalahan-permasalahan sebelum terlambat?
2. Apakah manajemen memastikan bahwa kontrol internal benar-benar efektif dan efisien?
3. Dapatkah performa teknologi informasi dihubungkan kembali dengan tujuan bisnis (*business goals*)?
4. Apakah resiko, kontrol, kesesuaian, dan performa diukur dan dilaporkan?

Pada domain *Monitor and Evaluate* terdapat empat subdomain, antara lain:

1. ME1: *Monitor and Evaluate IT Performance*
2. ME2: *Monitor and Evaluate Internal Control*
3. ME3: *Ensure Regulatory Compliance*
4. ME4: *Provide IT Governance*

Gambaran kerangka COBIT 4.1 secara keseluruhan dapat dilihat pada Gambar 2.2 berikut ini :



Gambar 2.2 COBIT Framework

(Sumber: ISACA, 2007)

2. Audit Guidelines

Berisi sebanyak 210 tujuan pengendalian (*Control Objectives*) untuk membantu para auditor memberikan saran perbaikan (*Management Assurance*). *Audit Guidelines* digunakan sebagai materi tambahan untuk merancang prosedur audit. Perbedaan dengan versi COBIT 4.0 adalah pada COBIT 4.0 terdapat 215 *Control Objectives*, namun pada COBIT 4.1 materi yang sama secara umum dikumpulkan pada level *framework* dan tidak diulang pada masing-masing proses.

3. Management Guidelines

Berisi arahan, baik secara umum maupun spesifik, mengenai apa saja yang mesti dilakukan, terutama agar dapat menjawab pertanyaan-pertanyaan berikut:

1. Sejauh mana teknologi informasi harus dikembangkan, dan besar biaya yang dikeluarkan untuk pengembangan teknologi informasi telah sesuai dengan manfaat yang dihasilkan?
2. Apa saja indikator untuk suatu kinerja yang bagus?
3. Apa saja faktor atau kondisi yang harus diciptakan agar dapat mencapai sukses (*Critical Success Factor*)?
4. Apa saja resiko-resiko yang timbul, apabila kita tidak dapat mencapai sasaran yang ditentukan?
5. Bagaimana mengukur keberhasilan yang telah dicapai dan bagaimana membandingkannya?

COBIT framework juga memasukkan hal-hal berikut ini:

1. Maturity Models

Sebuah pengembangan teknologi informasi harus terukur dengan baik, agar mekanisme tata kelola teknologi informasi dapat berjalan secara baik dan efektif maka harus melalui tahap kematangan tertentu (Indrajit, 2006).

Dengan menggunakan Model *Maturity* sebuah perusahaan dapat mengukur posisi kematangannya dalam pengembangan teknologi informasi, dan secara kontinyu serta berkesinambungan harus berusaha untuk meningkatkan levelnya sampai pada tingkat tertinggi agar aspek tata kelola

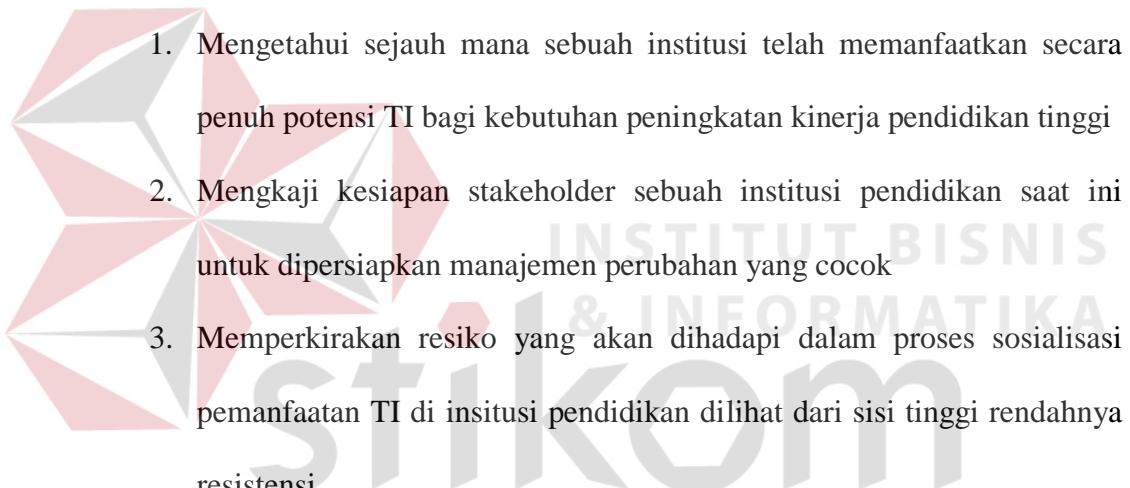
terhadap teknologi informasi dapat berjalan efektif dan sejalan dengan strategi yang telah ditetapkan. Sebuah kematangan sebuah perusahaan terkait dengan keberadaan dan kinerja proses tata kelola teknologi informasi dapat dikategorikan menjadi 6 (enam) tingkatan, yaitu (Indrajit, 2006):

Tabel 2.2 Skala Pengukuran Maturity Model

Skala	Penjelasan
0 <i>Non-existent</i>	Adalah posisi kematangan terendah, suatu kondisi dimana perusahaan merasa tidak membutuhkan adanya mekanisme proses investasi teknologi yang baku, sehingga tidak ada sama sekali pengawasan terhadap investasi teknologi informasi yang dikeluarkan oleh perusahaan.
1 <i>Initial/Ad Hoc</i>	Sudah ada beberapa inisiatif mekanisme perencanaan, tata kelola, dan pengawasan terhadap sejumlah investasi yang dilakukan, namun sifatnya masih <i>ad-hoc</i> , sporadis, tidak konsisten, belum formal, dan reaktif.
2 <i>Repeatable but Intuitive</i>	Kondisi dimana perusahaan telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola investasi teknologi informasi dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen format.
3 <i>Defined Process</i>	Pada tahapan ini, perusahaan telah memiliki mekanisme dan prosedur yang jelas mengenai tata cara dan manajemen proses investasi teknologi informasi, dan telah terkomunikasikan serta tersosialisasikan dengan baik di seluruh jajaran manajemen perusahaan.
4 <i>Managed and Measurable</i>	Menetapkan kondisi dimana manajemen perusahaan telah menerapkan sejumlah indikator pengukuran kinerja kuantitatif untuk memonitor efektifitas pelaksanaan manajemen investasi teknologi informasi

Skala	Penjelasan
5 <i>Optimised</i>	Level tertinggi ini diberikan kepada perusahaan yang telah berhasil menerapkan prinsip-prinsip tata kelola (<i>governance</i>) secara utuh dan mengacu pada <i>best practice</i> , dimana secara utuh telah diterapkan prinsip-prinsip <i>governance</i> , seperti: <i>transparency</i> , <i>accountability</i> , <i>responsibility</i> , dan <i>fairness</i> .

Seperti halnya pada konsep yang lain, mengukur tingkat kematangan pemanfaatan Teknologi Informasi di dunia pendidikan akan memberikan sejumlah manfaat sebagai berikut (Indrajit, 2006):

- 
1. Mengetahui sejauh mana sebuah institusi telah memanfaatkan secara penuh potensi TI bagi kebutuhan peningkatan kinerja pendidikan tinggi
 2. Mengkaji kesiapan stakeholder sebuah institusi pendidikan saat ini untuk dipersiapkan manajemen perubahan yang cocok
 3. Memperkirakan resiko yang akan dihadapi dalam proses sosialisasi pemanfaatan TI di institusi pendidikan dilihat dari sisi tinggi rendahnya resistensi
 4. Mengetahui target pola pikir dan pola tindak yang harus dimiliki oleh setiap *stakeholder* terkait dalam sebuah institusi pendidikan
 5. Menjadi indikator aktivitas peningkatan kinerja TI di sebuah institusi pendidikan dari waktu ke waktu
 6. Merupakan alat ukur perbandingan antara satu institusi

2.9. Key Performance Indicators (KPI) - Key Goal Indicators (KGI)

Key Performance Indicators (KPI) menjelaskan ukuran-ukuran untuk menentukan kinerja proses-proses TI dilakukan untuk mewujudkan tujuan yang

telah ditentukan. KPI biasanya berupa indikator-indikator kapabilitas, pelaksanaan, dan kemampuan sumber daya TI. KPI merupakan aplikasi sasaran mutu yang menjadi target pencapaian. Diawali dengan mendefinisikan sasaran/goal mutu dan proses yang diperlukan agar sesuai dengan persyaratan pelanggan dan kebijakan organisasi. (Wasilah, 2007)

Key Goal Indicators (KGI) menjelaskan ukuran-ukuran yang akan memberikan gambaran kepada manajemen apakah proses-proses TI yang ada telah memenuhi kebutuhan proses bisnis yang ada. KGI biasanya berbentuk kriteria informasi: (a) Ketersediaan informasi yang diperlukan dalam mendukung kebutuhan bisnis, (b) Tidak adanya resiko integritas dan kerahasiaan data, (c) Efisiensi biaya dari proses dan operasi yang dilakukan, (d) Konfirmasi reliabilitas, efektifitas dan kepatuhan (*compliance*). (Wasilah, 2007)

Process Key Goal Indicator (Process KGI) mendefinisikan bagaimana TI proses harus dilaksanakan untuk mendukung “*IT Objective*”. *Information Technology Key Goal Indicator* (ITKGI) mendefinisikan apa yang diharapkan bisnis dari TI (Swastika, 2007). Penetapan KPI dan KGI dilakukan dengan mengacu pada perincian target yang ingin dicapai pada masing-masing proses dan dipetakan pada KPI–Process KGI–ITKGI yang akan ditetapkan. Kemudian dilanjutkan dengan mengidentifikasi resiko yang mungkin timbul dari aktifitas yang bersangkutan. (Wasilah, 2007).

2.10. *Control Objective*

Control Objective merupakan tolok ukur untuk mencapai *business goal* yang berupa *statement*. *Control Objective* dilakukan dengan mengimplementasikan *control procedures* IT proses tertentu. *Control Objective*

merupakan *best practice management objectives* umum untuk semua aktivitas TI. (Swastika, 2007).

2.11. ISACA Assessment

Pengukuran tingkat kematangan pada COBIT diambil dari sistem kematangan yang ada pada ISACA. *Form* yang dibuat berisi pernyataan-pernyataan, dan dikelompokkan menurut tingkatnya. Setiap pernyataan memiliki bobot senilai 1 (satu) dan dapat diisi dengan gradasi nilai sebagai berikut: *Not At All* yang bernilai 0; *A Little* yang bernilai 0.33; *Quite a lot* yang bernilai 0.66; *Completely* yang bernilai 1. Kemudian, form penilaian tingkat kematangan diisi berdasarkan temuan yang didapatkan dari observasi lapangan, investigasi *hard data*, dll. Observasi dilakukan oleh auditor yang didampingi personil group TI yang bertanggung jawab atas pengelolaan TI yang diaudit, sebagai akses penyedia data yang dibutuhkan, dan disebut auditee.

Langkah-langkah melakukan *assessment maturity level* pada COBIT dijelaskan dalam contoh Gambar 2.3 – Gambar 2.9 berikut ini:

1. Memisahkan *statement* yang mempunyai makna ambigu atau makna ganda.

Figure 1—Questionnaire Construction for PO10 Managing Projects (maturity levels 0 and part of 1)

Maturity Level Description	Questionnaire Statements
0 Nonexistent —Project management techniques are not used and the organization does not consider business impacts associated with project mismanagement and development project failures.	<ul style="list-style-type: none"> The organization does not use project management techniques. The organization does not report on project mismanagement effects or development project failures.
1 Initial/Ad hoc —The organization is generally aware of the need for projects to be structured and it is aware of the risks of poorly managed projects. The use of project management techniques and approaches within IT is a decision left to individual IT managers. Projects are generally poorly defined.	<ul style="list-style-type: none"> The organization is generally aware of the need for projects to be structured. The organization is aware of the risks of poorly managed projects. The use of project management techniques and approaches within IT is a decision left to individual IT managers. Projects are generally poorly defined.

Gambar 2.3 Memisahkan *statement* ganda

(Sumber: Pederiva, 2010)

2. Melakukan *mapping* pada nilai kesesuaian (*compliance value*) yang ada, kemudian menjumlahkan nilai kesesuaian yang ada.

Figure 2—Compliance Level Numeric Values

Agreement with Statement	Compliance Value
Not at all	0
A little	0.33
Quite a lot	0.66
Completely	1

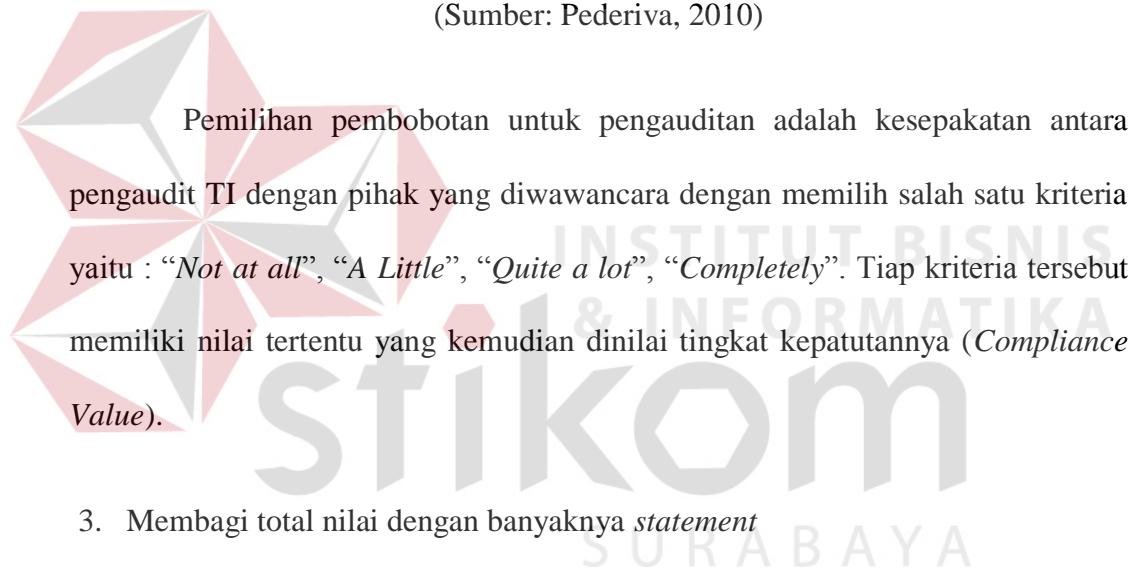
Gambar 2.4 Gradasi nilai untuk masing-masing *statement*

(Sumber: Pederiva, 2010)

Questionnaire for Level 0 Maturity Model of Process AI2						
Number	Statement	How much do you agree?				Statements compliance Value
		Not at all	A little	Quite a lot	Completely	
		0.00	0.33	0.66	1.00	
1	There is process for designing applications.	✓				0.00
2	There is process for specifying applications.	✓				0.00
3	Typically, applications are obtained based on vendor-driven offerings, with consideration of actual requirements.	✓				0.00
4	Typically, applications are obtained brand recognition or IT staff familiarity with specific products, with consideration of actual requirements.	✓				0.00
					total	0.00

Gambar 2.5 Mapping dan menjumlahkan nilai kesesuaian

(Sumber: Pederiva, 2010)



3. Membagi total nilai dengan banyaknya statement

Computation of the Maturity Level Compliance Value			
Maturity Level	Sum of statements compliance value	Number of maturity level statements (B)	Maturity level compliance value
0	0.00	4	0.00
1	0.66	14	0.05
2	0.00	10	0.00
3	1.00	13	0.08
4	0.00	17	0.00
5	0.00	19	0.00

Gambar 2.6 Menghitung nilai kesesuaian

(Sumber: Pederiva, 2010)

4. Melakukan normalisasi dengan menginputkan nilai kesesuaian pada masing-masing level yang telah dihitung sebelumnya. Kemudian, menjumlahkan *value* yang belum dinormalisasi. Untuk menghitung *value* yang telah dinormalisasi dengan cara membagi nilai yang belum dinormalisasi pada masing-masing level dengan total nilai yang belum dinormalisasi. Setelah pada masing-masing level telah dinormalisasi, dihitung nilai total semua level yang telah dinormalisasi.

Computation of The Normalized Compliance Value		
Level	Not normalized compliance value	Normalized Compliance Value
0	0.00	0.000
1	0.05	0.385
2	0.00	0.000
3	0.08	0.615
4	0.00	0.000
5	0.00	0.000
total:	0.13	1.000

Gambar 2.7 Menghitung normalisasi *maturity level*

(Sumber: Pederiva, 2010)

5. Mengalikan masing-masing level yang belum dinormalisasi dengan nilai yang telah dinormalisasi untuk menghasilkan nilai kontribusi pada masing-masing levelnya. Kemudian menjumlahkan nilai kontribusi pada semua level yang ada.

Computation of The Summary Maturity Level			
Level (A)	ML complian	Normalized compliance values	Contribution (A*B)
0	0.00	0.000	0.000
1	0.05	0.200	0.010
2	0.00	0.000	0.000
3	0.08	0.800	0.064
4	0.00	0.000	0.000
5	0.00	0.000	0.000
		Total Maturity	0.074

Gambar 2.8 Menghitung nilai kontribusi

(Sumber: Pederiva, 2010)

Form penilaian tingkat kematangan yang digunakan, cara pengisian dan perhitungannya merupakan metode yang diterbitkan oleh ISACA. Bentuk *form* yang digunakan adalah pada gambar berikut ini:

Level	Statements	How much do you agree?				Statements compliance values
		Not at all	A little	Quite a lot	Completely	
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
						Total level:

Gambar 2.9 Form Penilaian *Maturity Level*

(Sumber: Pederiva, 2010)