BAB II

LANDASAN TEORI

Teknologi Informasi (TI) yang sejak lama dianggap sebagai pendorong dan pendukung strategi perusahaan, saat ini dianggap sebagai bagian terintegrasi dari strategi bisnis. Para pimpinan perusahaan sepakat bahwa keselarasan antara tujuan bisnis dan TI merupakan faktor sukses kritis (*Critical Success Factor)* di perusahaan. Keberadaan Tata Kelola TI membantu pemenuhan faktor tersebut dengan secara efisien dan efektif mengembangkan pengaplikasian teknologi dan pemenuhan kebutuhan akan informasi yang dapat diandalkan dan terjamin. Karena keberadaan TI yang kritis, pengelolaan TI seharusnya mendapatkan perhatian yang saling berkesinambungan antara pemangku kepentingan (*stakeholder*) dengan operasional yang terlibat langsung dalam eksekusi Proses TI di lapangan. Sarno (2009 : 1)

II.1 Tata Kelola

Peningkatan efektivitas dan efisiensi organisasi, baik organisasi bisnis maupun organisasi pemerintah, dapat dilakukan melalui upaya penataan organisasi yang baik. Upaya tersebut dilakukan tidak hanya melalui proses pengaturan (*manage*) tetapi lebih luas pada penatakelolaan seluruh proses bisnis (*governance*). Untuk dapat berhasil, TI tidak cukup hanya diatur (*manage*) oleh departemen TI saja, tetapi harus ditata kelola (*govern*) di tingkat korporasi.

Tata kelola yang diterapkan di level organisasi disebut Tata Kelola Korporat (*Corporate Governance)*. Tata Kelola Korporat merujuk pada proses dan struktur untuk merencanakan arah pengelolaan organisasi untuk mencapai tujuan secara efektif. Penataan organisasi dengan menerapkan model dan prinsip tata kelola organisasi yang baik disebut *Good Corporate Governance* (organisasi bisnis) dan *Good Government Governance* (organisasi pemerintah). Jogiyanto (2011 : 13)

> Menurut Weill & Ross (2004) Ada perbedaan mendasar antara mengatur (*manage*) dengan menatakelola (*govern*). Makna mengatur lebih sempit dibanding menatakelola, karena mengatur merupakan bagian dari menatakelola. Mengatur TI oleh departemen TI merupakan bagian dari menatakelola TI oleh korporasi. Mengatur TI hanya menunjuk pada serangkaian mekanisme di departemen TI untuk menghasilkan suatu keputusan spesifik TI, sedangkan menatakelola TI lebih luas lagi. Jogiyanto (2011 : 9)

> Bank Dunia mendefinisikan Tata Kelola (*governance*) sebagai pelaksanaan otoritas politis dan penggunaan sumber-sumber daya institusional untuk mengelola permasalahan-permasalahan dan urusan-urusan masyarakat. Sedangkan definisi lainnya adalah penggunaan institusi-institusi, struktur-struktur otoritas dan bahkan kolaborasi untuk mengalokasi sumber-sumber data dan mengkoordinasi atau mengendalikan aktivitas di masyarakat atau suatu ekonomi. Jogiyanto (2011 : 12)

II.2 Tata Kelola TI

Tata Kelola TI memiliki definisi inklusif yang mencakup Sistem Informasi (SI), teknologi dan komunikasi, bisnis dan hukum serta isu-isu lain yang melibatkan hampir seluruh pemangku kepentingan *(stakeholder]*, baik direktur, manajemen eksekutif, pemilik proses, suplier, pengguna TI bahkan pengaudit SI/TI. Pembentukan dan penyusunan tata kelola tersebut merupakan tanggung jawab dari jajaran direksi dan manajemen eksekutif.

II.2.1 Pengertian Tata Kelola TI

Definisi dari *Board Briefing on IT Governance 2nd Edition*, ITGI, (2004) Tata Kelola TI memiliki definisi inklusif yang mencakup Sistem Informasi (SI), teknologi dan komunikasi, bisnis dan hukum serta isu-isu lain yang melibatkan hampir seluruh pemangku kepentingan (*stakeholder*), baik direktur, manajemen eksekutif, pemilik proses, supplier, pengguna TI bahkan pengaudit SI/TI. Pembentukan dan penyusunan tata kelola tersebut merupakan tanggung jawab dari jajaran direksi dan manajemen eksekutif. Panduan tersebut merupakan bagian terintegrasi dari Tata Kelola Perusahaan yang terdiri dari kepemimpinan dan struktur organisasi serta proses yang memastikan bahwa pengelolaan TI akan menopang dan memperluas strategi dan tujuan perusahaan. Sarno (2009 : 12)

Menurut *The Ministry of International Trade & Industry* (1999) Tata Kelola TI adalah kapasitas organisasi untuk mengendalikan formulasi dan implementasi strategi TI dan mengarahkan kepada kepentingan pencapaian daya saing korporasi. Sedangkan menurut Van Grembergen (2002) Tata Kelola TI adalah penilaian kapasitas organisasi oleh dewan direksi, manajemen eksekutif, manajemen TI untuk mengendalikan formulasi dan implementasi strategi TI dalam rangka mendukung bisnisnya. Surendro (2009 : 3)

Menurut Peterson (2001) Tata Kelola TI merupakan sistem di mana portofolio TI organisasi diarahkan dan dikontrol. Tata kelola TI menggambarkan (a) distribusi hak-hak pengambilan keputusan seputar TI dan tanggung jawab diantara para stakeholder yang berbeda di dalam organisasi, dan (b) aturan dan juga prosedur untuk membuat dan memonitor keputusan yang terkait dengan strategi TI. Surendro (2009 : 31)

Tata Kelola TI adalah tanggung jawab dewan direksi dan manajemen eksekutif organisasi. Tata Kelola TI merupakan bagian terintegrasi dari pengelolaan perusahaan yang mencakup kepemimpinan, struktur serta proses organisasi yang memastikan bahwa TI perusahaan dipergunakan untuk mempertahankan dan memperluas strategi dan tujuan organisasi. Surendro (2009 : 127)

Menurut Weill & Ross (2004) Tata Kelola TI adalah serangkaian sistem dan mekanisme yang menentukan pihak-pihak, baik di Departemen TI maupun di luar Departamen TI, yang membuat dan berkontribusi dalam pembuatan keputusan TI. Jogiyanto (2011 : 9)

Menurut Sohal & Fitzpatrick (2002) Manajemen TI berfokus pada keefektifan operasi internal produk dan jasa, termasuk administrasi operasi TI yang ada saat ini. Perbedaan utama lainnya adalah manajemen TI umumnya fokus pada proses internal dan diselesaikan pada jenjang unit atau departemen, sedangkan Tata Kelola TI memiliki aspek yang lebih luas, yaitu pada jenjang korporat dan fokus pada tujuan eksternal. Jogiyanto (2011 : 8)

II.2.2 Pentingnya Tata Kelola TI

Dengan keberadaan TI sekarang yang sangat terkait dan menjalar di berbagai bidang di perusahaan, pengelolaan harus memberikan perhatian yang lebih terhadap TI, menelaah sebesar apa ketergantungan perusahaan terhadap TI dan sepenting apa TI bagi pelaksanaan strategi bisnis, maka TI sangat penting dalam mendukung dan mencapai tujuan perusahaan dan sangat strategis terhadap bisnis (perkembangan dan inovasi).

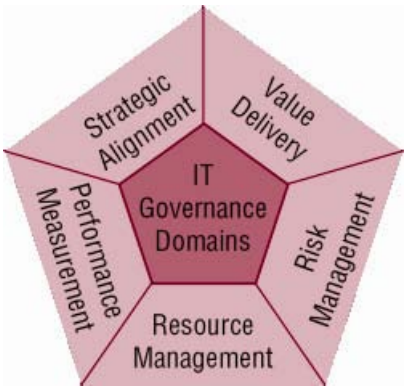
Alasan pentingnya Tata Kelola TI seperti yang diungkapkan Jogiyanto (2011 : 7) :

1. Adanya perubahan peran TI, dari peran efisiensi ke peran strategik yang harus ditangani di level korporat.
2. Banyak proyek TI strategik yang penting namun gagal dalam pelaksanaannya karena hanya ditangani oleh teknisi TI.
3. Keputusan TI di dewan direksi sering bersifat *adhoc* atau tidak terencana dengan baik.
4. TI merupakan pendorong utama proses transformasi bisnis yang memberi imbas penting bagi organisasi dalam pencapaian misi, visi dan tujuan strategik.
5. Kesuksesan pelaksanaan TI harus dapat terukur melalui metrik Tata Kelola TI.

II.2.3 Ruang Lingkup Tata Kelola TI

Pada dasarnya, Tata Kelola TI berkaitan dengan dua permasalahan utama, bahwa TI akan memberikan nilai terhadap bisnis yang didorong oleh penyelarasan TI dengan bisnis dan bahwa risiko yang terkait dengan TI akan ditangani dengan penentuan penanggung jawab permasalahan tersebut dalam perusahaan.

Adapun fokus utama dari area Tata Kelola TI dapat dibagi menjadi 5 area seperti pada Gambar II.1. ITGI, COBIT 4.1 (2007)



Gambar II.1 Fokus Area Tata Kelola TI

Penjelasan singkat mengenai area utama dalam Tata Kelola TI pada Gambar II.1 akan dipaparkan sebagaimana berikut:

1. *Strategic Alignment* (penyelarasan strategis)

   Memfokuskan kepastian terhadap keterkaitan antara strategi bisnis dan TI serta penyelarasan antara operasional TI dengan bisnis.

2. *Value Delivery* (penyampaian nilai)

   Mencakup hal-hal yang terkait dengan penyampaian nilai yang memastikan bahwa TI memenuhi manfaat yang dijanjikan dengan memfokuskan pada pengoptimalan biaya dan pembuktian nilai hakiki akan keberadaan TI.

3. *Resource Management* (pengelolaan sumber daya)

   Berkaitan dengan pengoptimalan investasi yang dilakukan dan pengelolaan secara tepat dari sumber daya TI yang kritis mencakup: aplikasi, informasi, infrastruktur dan Sumber Daya Manusia (SDM). Isu kunci area ini berhubungan dengan pengoptimalan pengetahuan dan infrastruktur.

4. *Risk Management* (pengelolaan risiko)

   Membutuhkan kepekaan akan risiko oleh manajemen senior, pemahaman yang jelas akan perhatian perusahaan terhadap keberadaan risiko, pemahaman kebutuhan akan kepatutan, transparansi akan risiko yang signifikan terhadap proses bisnis perusahaan dan tanggung jawab pengelolaan risiko ke dalam organisasi itu sendiri.

5. *Performance Measurement* (pengukuran kinerja)

   Penelusuran dan pengawasan implementasi dari strategi, pemenuhan proyek yang berjalan, penggunaan sumber daya, kinerja proses dan penyampaian layanan dengan menggunakan kerangka kerja seperti *Balanced Scorecard* yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan terukur dibandingkan dengan akuntansi konvensional.

II.2.4 Kerangka Kerja Tata Kelola TI

Berbagai kerangka kerja Tata Kelola TI tersedia dan sudah dibakukan serta diakui di seluruh dunia, sebagai contoh: *Information Technology Infrastructure Library* (ITIL) (Davies, 2003), ISO 17799 (ISO, 2005) dan *Control Objectives for Information and related Technology* (COBIT) (ISACA, COBIT4.1, 2007).

Kerangka kerja tersebut memiliki peran dan fungsi masing-masing dalam Tata Kelola TI. Peran dan fungsi utama dalam Tata Kelola TI mencakup dua hal utama, yaitu: pengaturan (*govern*) dan pengelolaan (*manage*). Pengaturan (*govern*) mencakup hal-hal apa yang mendasari tata kelola tersebut yang ditentukan melalui pendefinisian strategi dan kontrol.

Namun perusahaan perlu menentukan *best practice* (contoh yang baik) yang sesuai dengan kebutuhan bisnisnya dan dapat dijadikan sebagai panduan dalam pengelolaan TI. Penentuan contoh yang baik tersebut dilakukan dengan pemilihan terhadap kerangka kerja pengelolaan TI yang sudah dibakukan. Penentuan *best practice* yang mengacu pada kerangka yang baku dan standar dapat memudahkan dalam penyusunan standar pengelolaan proses yang baik sekaligus memberikan kepastian bagi perusahaan dalam menentukan Tata Kelola TI yang paling sesuai dengan bisnisnya namun tidak menyimpang dari praktik pengelolaan TI yang umum. Lebih jauh lagi, studi banding (*benchmark*) terhadap penerapan kerangka kerja Tata Kelola TI yang sukses di perusahaan lain perlu dilakukan untuk memberikan jaminan bahwa *best practice* yang disusun mampu memberikan kesuksesan terhadap bisnis di masa mendatang. Sarno (2009 : 14-16)

II.2.5 Kerangka Kerja Tata Kelola Keamanan

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis.

Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan.

Contoh dari keamanan informasi antara lain. Sarno dan Iffano (2009) :

1. *Physical security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal security* adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup physical security.
3. *Operational security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
4. *Communication security* adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. *Network security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Karena pentingnya pengetahuan akan kerangka kerja tersebut, maka berikut akan dipaparkan mengenai beberapa contoh kerangka kerja Tata Kelola TI khususnya yang menyangkut keamanan selain COBIT.

II.2.5.1 ITIL

IT Infrastructure Library (ITIL) merupakan standar yang dikeluarkan pemerintah *United Kingdom* (UK) sebagai kerangka kerja yang diacu oleh *best practice* proses dan prosedur manajemen operasional. Lebih spesifik, ITIL terutama memfokuskan terhadap pendefinisian fungsi, operasional dan atribut organisasi yang diperlukan agar manajemen operasional dapat dioptimasi secara penuh ke dalam dua kategori utama pengelolaan Aktivitas TI dalam perusahaan yaitu: *Service Support Management* dan *Service Delivery Management*.

Kedua kategori utama tersebut memiliki masing-masing sub kategori. *Service Support Management* mencakup beberapa sub kategori, antara lain *Service Desk, Incident, Problem, Configuration* serta *Change and Release Management.* Sedangkan kategori yang lain, yaitu *Service Delivery Management* meliputi sub kategori berikut : *Service Level, Financial, Capacity* dan *Service Continuity and Availability*. Setiap definisi sub kategori tersebut melingkupi kriteria di beberapa area, termasuk dukungan terhadap organisasi, integrasi komponen lintas manajemen, pelaporan manajemen, kapabilitas produk, kualitas implementasi dan kualitas layanan pelanggan. Sarno (2009 : 20)

Proses manajemen keamanan menurut ITIL meliputi proses antara lain :

1. Kontrol, meliputi aktivitas implementasi kebijakan, organisasi keamanan dan pelaporan.
2. Rencana, meliputi aktivitas keamanan tentang SLA (*Service Level Agreement*), dasar-dasar kontrak, OLA (*Operational Level Agreements*) dan pelaporan.

3. Implementasi, meliputi aktivitas klasifikasi dan pengelolaan aplikasi TI, personil keamanan, manajemen keamanan, akses kontrol dan pelaporan.
4. Evaluasi, meliputi aktivitas introspeksi sendiri, audit internal dan eksternal, evaluasi berdasarkan insiden keamanan dan pelaporan.
5. Pemeliharaan, meliputi aktivitas pemeliharaan dan revisi SLA dan OLA, serta pelaporan.
6. Model Proses Data yang lengkap, merupakan model proses data yang lengkap dari kelima proses di atas.

II.2.5.2 ISO

International Standards Organization (ISO) mengelompokkan standar keamanan informasi yang umum dikenali secara internasional ke dalam struktur penomoran yang standar yakni: ISO 17799. Pada awalnya standar tersebut disusun oleh sekelompok perusahaan besar seperti *Board of Certification, British Telecom, Marks & Spencer, Midland Bank, Nationwide Building Society, Shell* dan *Unilever* yang bekerja sama untuk membuat suatu standar yang dinamakan *British Standard* 7799 (BS 7799) sekitar awal tahun 1995.

BS 7799 terdiri dari dua bagian, yaitu: *The Code of Practice for Information Security Management* (Part 1) dan *The Specification for Information Security Management Systems*/ISMS (Part 2). Kemudian sekitar tahun 2000, ISO *dan International Electro-Technical Commission* (IEC) mengadopsi BS 7799 Part 1 dan menerbitkannya sebagai standar ISO/IEC 17799:27000 dan BS 7799 Part 2 sebagai standar ISO/IEC 17799:27001 yang diakui secara internasional.

Standar tersebut memiliki fungsi dan peran masing-masing dan berkembang ke seri lain sebagaimana berikut :

1. ISO/IEC 27000 : merupakan dokumen yang berisikan definisi-definisi dalam bidang keamanan informasi yang digunakan sebagai istilah dasar.
2. ISO/IEC 27001 : mencakup aspek-aspek pendukung realisasi dan implementasi sistem manajemen keamanan informasi perusahaan.
3. ISO/IEC 27002 : panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan berdasarkan ISO/IEC 27001.

ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di perusahaan. Secara umum terdapat 11 aspek yang seharusnya ada dalam setiap perusahaan dalam mengimplementasikan konsep keamanan informasi tersebut. Sarno (2009 : 21-22)

SMKI merupakan bagian dari sistem manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara keamanan informasi.

Keamanan Informasi adalah penjagaan kerahasiaan, integritas dan kesediaan informasi; sebagai tambahan, sifat/keadaan informasi lainnya seperti keaslian, akuntabilitas, nirsangkal dan kehandalan dapat juga dimasukkan. BSN (2009)

Klausul sasaran pengendalian dan pengendalian menurut SNI ISO/IEC 27001:2009 tersebut antara lain. BSN (2009) :

1. Kebijakan keamanan

   Kebijakan keamanan informasi, untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi menurut persyaratan bisnis dan hukum serta regulasi yang relevan.

2. Organisasi keamanan informasi
   a. Organisasi internal, untuk mengelola keamanan informasi dalam organisasi.
   b. Pihak eksternal, untuk memelihara keamanan informasi organisasi dan fasilitas pengolahan informasi yang diakses, diolah, dikomunikasikan kepada atau dikelola oleh pihak eksternal.

3. Pengelolaan aset
   a. Tanggung jawab terhadap aset, untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi.
   b. Klasifikasi informasi, untuk memastikan bahwa informasi menerima tingkat perlindungan yang tepat.

4. Keamanan sumberdaya manusia
   a. Sebelum dipekerjakan, untuk memastikan bahwa pegawai, kontraktor dan pengguna pihak ketiga memahami tanggung jawab sesuai dengan perannya, dan untuk mengurangi risiko pencurian, kecurangan atau penyalahgunaan fasilitas.

b. Selama bekerja, untuk memastikan bahwa semua pegawai, kontraktor dan pengguna pihak ketiga telah peduli terhadap ancaman dan masalah keamanan informasi, tanggung jawab dan pertanggung-gugatan mereka, dan disediakan perlengkapan yang memadai untuk mendukung kebijakan keamanan organisasi selama bekerja dan untuk mengurangi risiko kesalahan manusia.

c. Pengakhiran atau perubahan pekerjaan, untuk memastikan bahwa pegawai, kontraktor dan pengguna pihak ketiga keluar dari organisasi atau adanya perubahan pekerjaan dengan cara yang sesuai.

5. Keamanan fisik dan lingkungan

a. Area yang aman, untuk mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interferensi terhadap lokasi dan informasi organisasi.

b. Keamanan peralatan, untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi.

6. Manajemen komunikasi dan operasi

a. Prosedur operasional dan tanggung jawab, untuk memastikan pengoperasian fasilitas pengolahan informasi secara benar dan aman.

c. Manajemen pelayanan jasa pihak ketiga, untuk menerapkan dan memelihara tingkat keamanan informasi dan pelayanan jasa yang sesuai dengan perjanjian pelayanan jasa pihak ketiga.

d. Perencanaan dan keberterimaan sistem, untuk mengurangi risiko kegagalan sistem.

e. Perlindungan terhadap *malicious and mobile code*, untuk melindungi integritas perangkat lunak dan informasi.
f. *Back-up*, untuk memelihara integritas dan ketersediaan informasi dan fasilitas pengolahan informasi.
g. Manajemen keamanan jaringan, untuk memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung.
h. Penanganan media, untuk mencegah pengungkapan, modifikasi, pemindahan atau pemusnahan aset yang tidak sah, dan gangguan kegiatan bisnis.
i. Pertukaran informasi, untuk memelihara keamanan informasi dan perangkat lunak yang dipertukarkan dalam suatu organisasi dan dengan setiap entitas eksternal.
j. Layanan *electronic commerce*, untuk memastikan keamanan layanan *electronic commerce* dan keamanan penggunaannya.
k. Pemantauan, mendeteksi kegiatan pengolahan informasi yang tidak sah.

7. Pengendalian akses
   a. Persyaratan bisnis untuk pengendalian akses, untuk mengendalikan akses kepada informasi.
   b. Manajemen akses pengguna, untuk memastikan akses oleh pengguna yang sah dan untuk mencegah pihak yang tidak sah pada sistem informasi.
   c. Tanggung jawab pengguna, untuk mencegah akses pengguna yang tidak sah dan gangguan atau pencurian atas informasi dan fasilitas pengolahan informasi.

d. Pengendalian akses jaringan, untuk mencegah akses yang tidak sah ke dalam layanan jaringan.
e. Pengendalian akses sistem operasi, untuk mencegah akses tidak sah ke dalam sistem operasi.
f. Pengendalian akses aplikasi dan informasi, untuk mencegah akses yang tidak sah terhadap informasi pada sistem aplikasi.
g. *Mobile computing* dan kerja jarak jauh (*teleworking*), untuk memastikan keamanan informasi ketika menggunakan fasilitas *mobile computing* dan kerja jarak jauh (*teleworking*).

8. Akuisisi, pengembangan dan pemeliharaan sistem informasi
   a. Persyaratan keamanan dari sistem informasi, untuk memastikan bahwa keamanan merupakan bagian yang utuh dari sistem informasi.
   c. Pengolahan yang benar dalam aplikasi, untuk mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi.
   d. Pengendalian dengan cara kriptografi, untuk melindungi kerahasiaan, keasliaan atau integritas informasi dengan cara kriptografi.
   e. Keamanan *system files*, untuk memastikan keamanan *system files*.
   f. Keamanan dalam proses pengembangan dan pendukung, untuk memelihara keamanan perangkat lunak sistem aplikasi dan informasi.
   g. Manajemen kerawanan teknis, untuk mengurangi risiko terhadap ekploitasi kerawanan teknis yang dipublikasikan.

9. Manajemen insiden keamanan informasi
    a. Pelaporan kejadian dan kelemahan keamanan informasi, untuk memastikan kejadian dan kelemahan keamanan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dilakukan tepat waktu.
    b. Manajemen insiden keamanan informasi dan perbaikan, untuk memastikan pendekatan yang konsisten dan efektif diterapkan untuk manajemen insiden keamanan informasi.
10. Manajemen keberlanjutan bisnis (Business continuity management)

    Aspek keamanan informasi dari manajemen keberlanjutan bisnis, untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama sistem informasi atau bencana dan untuk memastikan keberlanjutannya secara tepat waktu.
11. Kesesuaian
    a. Kesesuaian dengan persyaratan hukum, untuk mencegah pelanggaran terhadap undang-undang, peraturan perundang-undangan atau kewajiban kontrak dan setiap persyaratan keamanan.
    b. Pemenuhan terhadap kebijakan keamanan dan standar, dan pemenuhan teknis, untuk memastikan pemenuhan sistem terhadap kebijakan dan standar keamanan organisasi.
    c. Pertimbangan audit sistem informasi, memaksimalkan keefektifan dari dan untuk meminimalkan interferensi kepada/dari proses audit sistem informasi.

II.2.5.3 NIST

NIST (*National Institute of Standards and Technology*) atau Badan Nasional Standar dan Teknologi Amerika Serikat yang dulunya dikenal sebagai *The National Bureau of Standards* (NBS) atau Biro Standar Nasional adalah sebuah badan non-regulator dari bagian Administrasi Teknologi dari Departemen Perdagangan Amerika Serikat. Misi dari badan ini adalah untk membuat dan mendorong pengukuran, standar, dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan, dan memperbaiki kualitas hidup semua orang. Inovasi dan kemajuan teknologi di Amerika Serikat bergantung pada keahlian dan kemampuan unik dari NIST di empat bidang utama yaitu bioteknologi, nanoteknologi, teknologi informasi, dan manufakturing modern.

Menurut NIST keamanan adalah sebuah kondisi yang dihasilkan dari pembentukan dan pemeliharaan langkah-langkah protektif yang memungkinkan perusahaan untuk melakukan misinya atau fungsi kritis terhadap risiko yang ditimbulkan oleh ancaman terhadap penggunaan sistem informasi. Langkah-langkah perlindungan yang melibatkan kombinasi dari pencegahan, penghindaran, pencegahan, deteksi, pemulihan, dan koreksi yang menjadi bagian dari pendekatan manajemen risiko perusahaan.

Sedangkan keamanan informasi adalah perlindungan informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan dalam rangka untuk menyediakan kerahasiaan, integritas, dan ketersediaan. NIST (2013)

Untuk kemudahan penggunaan dalam pemilihan kontrol keamanan dan spesifikasi proses yang ada dalam NIST, disusun dalam 18 kontrol keamanan terkait dengan topik keamanan umum. Kontrol keamanan tersebut antara lain. NIST (2013) :

1. Kontrol Akses
2. Audit dan Akuntabilitas
3. Identifikasi dan Otentikasi
4. Sistem dan Proteksi Komunikasi
5. Kesadaran dan Pelatihan
6. Manajemen Konfigurasi
7. Perencanaan Kontijensi
8. Sistem dan Informasi Integritas Operasional
9. Respon Insiden
10. Pemeliharaan
11. Proteksi Media
12. Proteksi Fisik dan Lingkungan
13. Personil Keamanan
14. Pengkajian Keamanan dan Manajemen Otorisasi
15. Manajemen Program
16. Perencanaan Manajemen
17. Manajemen Penilaian Risiko
18. Sistem dan Pelayanan Manajemen Akuisisi.

II.3 COBIT

Control Objectives for Information and related Technology (COBIT) adalah seperangkat pedoman umum (*best practice*) untuk manajemen TI yang dibuat oleh *Information Systems Audit and Control Association* (ISACA), dan *IT Governance Institute* (ITGI) pada tahun 1996. Hingga saat ini setidaknya sudah ada 5 versi COBIT yang sudah diterbitkan, versi pertama diterbitkan pada tahun 1996, versi kedua tahun 1998, versi 3.0 di tahun 2000, COBIT 4.0 pada tahun 2005, COBIT 4.1 tahun 2007 dan yang terakhir ini adalah Cobit versi 5 tahun 2012.

COBIT memberi manajer, auditor dan pengguna TI, serangkaian langkah yang diterima secara umum, indikator, proses dan praktik terbaik untuk membantu mereka dalam memaksimalkan manfaat yang diperoleh melalui penggunaan TI dan pengembangan tatakelola TI yang sesuai dan pengendalian dalam perusahaan. COBIT menyediakan standar dalam kerangka kerja *domain* yang terdiri dari sekumpulan Proses TI yang merepresentasikan aktivitas yang dapat dikendalikan dan terstruktur. Kerangka kerja tersebut memfokuskan pada lebih banyak kontrol dan sedikit eksekusi sehingga kepentingannya lebih ditujukan kepada pendefinisian strategi dan kontrol yang biasanya dilakukan oleh manajemen tingkat atas, namun tidak detil menjelaskan bagaimana memenuhi keduanya dipenuhi yang dapat dipakai sebagai acuan pengguna yang langsung terkait dengan pengelolaan TI. Sarno (2009 : 17)

II.3.1 Produk COBIT 4.1

Produk-produk COBIT seperti pada Gambar II.2, ITGI, COBIT 4.1 (2007) :

1. *Board Briefing on IT Governance, 2nd Edition*

   Membantu para eksekutif memahami betapa pentingnya Tata Kelola TI, apa yang menjadi masalah dan tanggung jawab mereka dalam pengelolaannya.

2. *Management Guidelines/Maturity Models*

   Membantu menentukan tanggung jawab, pengukuran kinerja, tolak ukur dan menemukan *gap* dalam kapabilitasnya.

3. *Frameworks*

   Mengorganisasikan objektif Tata Kelola TI dan *good practices* pada *domain* dan Proses TI serta menghubungkannya dengan kebutuhan bisnis.

4. *Control Objectives*

   Menyediakan sebuah kumpulan yang lengkap dari kebutuhan tingkat tinggi yang akan dipertimbangkan oleh manajemen guna mengendalikan setiap proses TI agar lebih efektif.

5. *IT Governance Implementation Guide: Using COBIT® and Val IT TM, 2nd Edition*

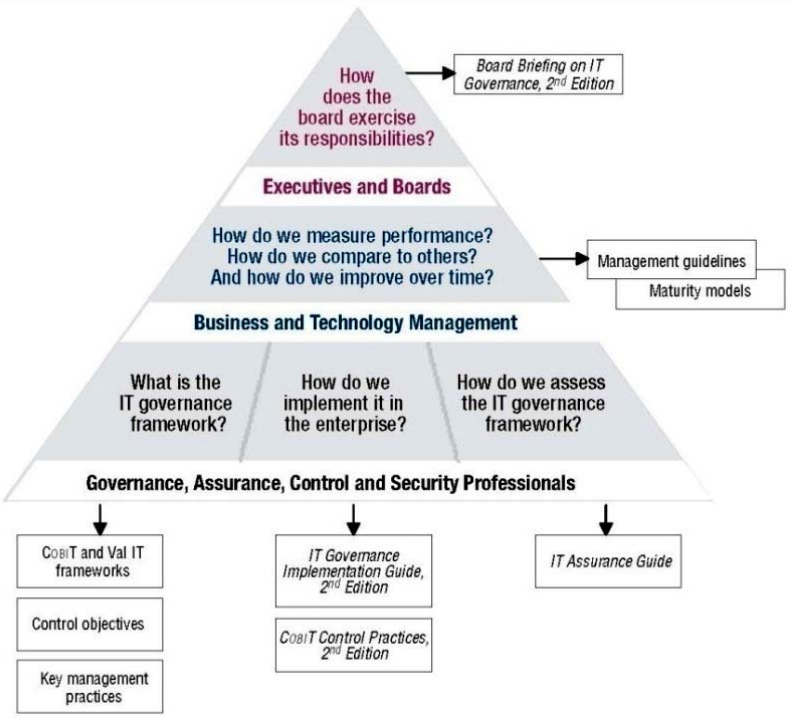
   Menyediakan tahapan umum untuk mengimplementasikan Tata Kelola TI dengan menggunakan COBIT dan Val IT TM *Resources*.

6. *COBIT ® Control Practices: Guidance to Achieve Control Objectives for Sucessful IT Governance, 2nd Edition*

   Menyediakan petunjuk mengenai mengapa kontrol sangat penting untuk perlu diimplementasikan dan bagaimana untuk mengimplementasikannya.

7. *IT Assurance Guide: Using COBIT ®*

   Menyediakan pedoman mengenai bagaimana COBIT dapat digunakan untuk mendukung jaminan dari keanekaragaman aktifitas bersama dengan langkah pengujian yang diusulkan dalam Proses TI dan *control objectives.*



Gambar II.2 Produk COBIT
Sumber: ITGI, COBIT 4.1 (2007)

Manfaat mengimplementasikan COBIT sebagai kerangka kerja Tata Kelola TI adalah sebagai berikut, ITGI, COBIT 4.1 (2007) :

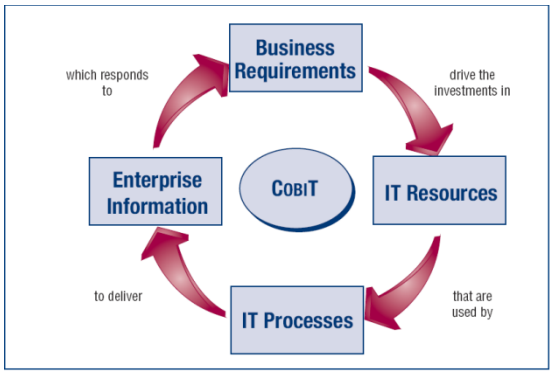
1. Pengelolaan TI menjadi sejalan dengan fokus bisnis.
2. Pihak manajemen dapat memahami manfaat penerapan TI dalam perusahaan.
3. Adanya kepemilikan dan tanggungjawab yang jelas karena berdasarkan pada orientasi proses.
4. Adanya penerimaan terhadap pihak ketiga dan *regulators.*

5. Saling berbagi pemahaman di antara semua *stakeholder* dengan berdasarkan pada pemahaman akan tujuan yang sama.
6. Pemenuhan dari keperluan *COSO* (*Committee of Sponsoring Organisations of the Treadway Commission*) untuk lingkungan pengendalian TI.

COBIT mendukung manajemen dalam mengoptimumkan investasi TI melalui ukuran-ukuran dan pengukuran yang akan memberikan sinyal bahaya bila suatu kesalahan atau risiko 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 individual memenuhi tuntutan dan kebutuhan informasi serta efek terhadap sumber daya TI perusahaan.

II.3.2 Prinsip Dasar COBIT 4.1

Untuk memberikan informasi yang dibutuhkan perusahaan untuk mencapai tujuannya, perusahaan perlu berinvestasi untuk mengelola dan mengendalikan sumber daya TI dengan menggunakan seperangkat proses yang terstruktur.



Gambar II.3 Prinsip Dasar COBIT 4.1
Sumber: ITGI, COBIT 4.1 (2007)

Kriteria informasi yang berkualitas untuk mencapai tujuan bisnis mempunyai tujuh aspek utama. ITGI, COBIT 4.1 (2007) :

1. *Effectiveness*, berkaitan dengan informasi yang dihasilkan haruslah relevan dan dapat memenuhi kebutuhan dari setiap proses bisnis terkait dan tersedia secara tepat waktu, akurat, konsisten dan dapat dengan mudah diakses.
2. *Efficiency*, mencakup informasi yang dapat diperoleh dan disediakan melalui cara yang ekonomis, terutama terkait dengan konsumsi sumber daya yang dialokasikan.
3. *Confidentiality*, mencakup informasi yang rahasia dan bersifat sensitif harus dapat dilindungi atau dijamin keamanannya, terutama dari pihak-pihak yang tidak berhak mengetahuinya.
4. *Integrity*, berkaitan dengan keakuratan dan kelengkapan informasi serta validitas sesuai dengan nilai-nilai dan harapan bisnis.
5. *Avaibility*, berkaitan dengan informasi yang harus tersedia bilamana dibutuhkan dengan kinerja waktu dan kapabilitas yang diharapkan.
6. *Compliance*, informasi yang dimiliki harus dapat dipertanggungjawabkan kebenarannya dan mengacu pada hukum maupun regulasi yang berlaku, termasuk di dalamnya mengikuti standar nasional atau internasional yang ada.
7. *Reliability*, berkaitan dengan informasi yang dihasilkan haruslah berasal dari sumber yang dapat dipercaya sehingga tidak menyesatkan para pengambil keputusan yang menggunakan informasi tersebut.

Kaitannya tujuan bisnis dan TI dalam COBIT dibagi menjadi 4 perspektif, yaitu:

1. Perspektif Keuangan
    a. Memberikan hasil yang baik dalam investasi pada TI memungkinkan investasi bisnis.
    b. Mengelola TI berhubungan dengan risiko bisnis.
    c. Meningkatkan penguasaan perusahaan dan ketransparanan.

2. Perspektif Pelanggan
    a. Meningkatkan kepuasan pelanggan dan pelayanan.
    b. Memajukan produk untuk dapat bersaing dan pelayanan.
    c. Memperkenalkan kelancaran pelayanan dan ketersediaan.
    d. Cepat tanggap dalam merespon perubahan bisnis.
    e. Mencapai biaya optimal dalam layanan pengiriman.
    f. Memperoleh kepercayaan dan informasi yang berguna untuk strategi pembuatan keputusan.

3. Perspektif Internal
    a. Meningkatkan dan menjaga fungsi-fungsi proses bisnis.
    b. Meminimalkan biaya proses.
    c. Mematuhi hukum eksternal, peraturan dan kontrak.
    d. Mematuhi kebijakan internal.
    e. Mengatur perubahan bisnis.
    f. Meningkatkan dan memelihara produktifitas operasional dan staf.

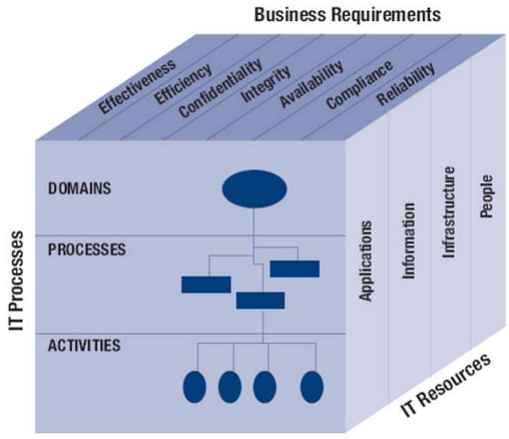
4. Perspektif Pembelajaran dan Pertumbuhan
    a. Mengelola produk dan bisnis inovasi.
    b. Memperoleh dan memelihara kemampuan dan motivasi orang.

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

1. Aplikasi, yang merupakan sekumpulan program untuk mengolah dan menampilkan data maupun informasi yang dimiliki oleh organisasi.
2. Informasi, yang merupakan hasil pengolahan dari data yang merupakan bahan mentah dari setiap informasi yang dihasilkan, dimana di dalamnya terkandung fakta dari aktivitas transaksi dan interaksi seharihari masingmasing proses bisnis yang ada di organisasi.
3. Infrastruktur, yang terdiri dari sejumlah perangkat keras, infrastruktur TI sebagai teknologi pendukung untuk menjalankan *portfolio* aplikasi yang ada. Selain itu yang termasuk dalam infrastruktur dapat berupa sarana fisik seperti ruangan dan gedung dimana keseluruhan perangkat sistem dan TI ditempatkan.
4. Manusia, yang merupakan pemakai dan pengelola dari sistem informasi yang dimiliki.

Pada dasarnya kerangka kerja COBIT terdiri dari 3 tingkat *control objectives*, yaitu *activities* dan *tasks, process, domains*. *Activities* dan *tasks* merupakan kegiatan rutin yang memiliki konsep daur hidup, sedangkan *task* merupakan

kegiatan yang dilakukan secara terpisah. Selanjutnya kumpulan *activity* dan *task* ini dikelompokan ke dalam proses TI yang memiliki permasalahan pengelolaan TI yang sama dikelompokan ke dalam *domains*.



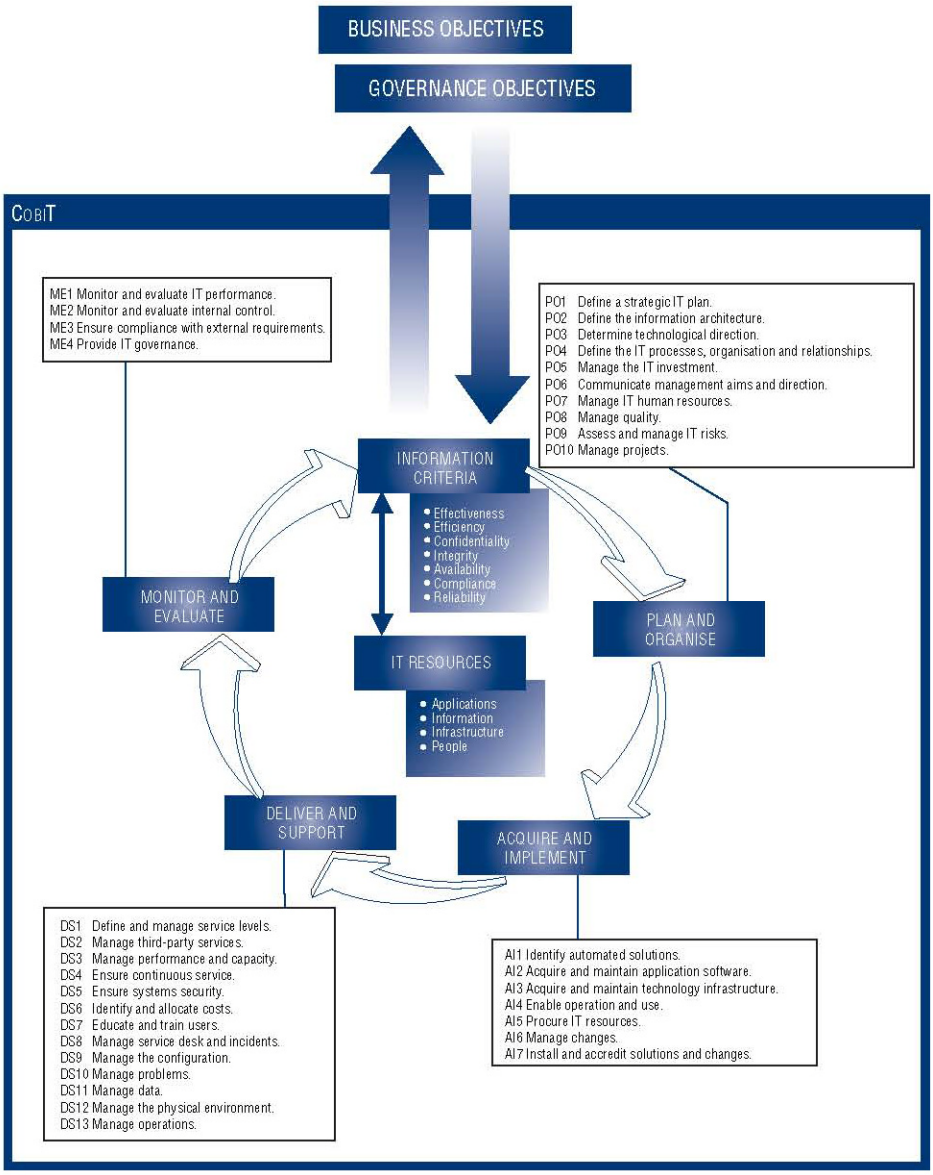
Gambar II.4 COBIT *Cube*
Sumber: ITGI, COBIT 4.1 (2007)

COBIT diperuntukkan bagi pengguna-pengguna :

1. Manajemen Eksekutif, untuk mendapatkan nilai dari investasi TI dan penyeimbangan risiko dan pengendalian investasi dalam lingkungan TI yang tidak dapat diprediksi.
2. Manajemen Bisnis, untuk memperoleh keyakinan dari manajemen atas pengendalian layanan TI yang diberikan oleh internal atau pihak ketiga.
3. Manajemen TI, untuk menyediakan layanan TI yang dibutuhkan oleh bisnis untuk mendukung strategi bisnis yang terkontrol dan terkelola.
4. Auditor, untuk memperkuat dan memberikan pendapat atau saran kepada manajemen mengenai pengendalian internal.

II.3.3 Kerangka Kerja COBIT 4.1

Kerangka kerja COBIT 4.1 menyediakan model proses yang umumnya ditemukan dalam aktivitas TI dalam 4 *Domain* yang di dalamnya terdapat 34 Proses TI dan 318 *control objectives*, serta 1547 *control practices*. ITGI, COBIT 4.1 (2007)



Gambar II.5 Kerangka Kerja Cobit 4.1
Sumber: ITGI, COBIT 4.1 (2007)

Berikut 4 *Domain* yang di dalamnya terdapat 34 Proses TI dan 318 *control objectives*. ITGI, COBIT 4.1 (2007) :

1. *Plan and Organize* (PO) – Perencanaan dan Organisasi

   Domain ini mencakup strategi dan taktik, dan mengidentifikasi cara TI terbaik yang dapat memberikan kontribusi pada pencapaian tujuan bisnis. Selain itu, realisasi dari visi strategis yang perlu direncanakan, dikomunikasikan dan dikelola dari berbagai perspektif. Organisasi yang tepat harus meletakkan teknologi infrastruktur di tempat yang tepat. *Domain* ini biasanya membahas pertanyaan manajemen sebagai berikut :

   a. Apakah TI dan strategi bisnis sudah ditetapkan?
   b. Apakah perusahaan sudah menggunakan secara maksimum sumber dayanya?
   c. Apakah semua orang di dalam organisasi sudah memahami sasaran TI?
   d. Apakah risiko TI sudah dipahami dan diatur?
   e. Apakah mutu sistem TI sudah sesuai dengan kebutuhan bisnis?

   Domain PO terdiri dari 10 Proses TI, yang meliputi :

   PO1 *Define a strategic IT plan*

   PO2 *Define the information architecture*

   PO3 *Determine technological direction*

   PO4 *Define the IT processes, organization and relationships*

   PO5 *Manage the IT investment*

   PO6 *Communicate management aims and direction*

PO7 *Manage IT human resources*

PO8 *Manage quality human resource*

PO9 *Asses and manage IT Risks*

PO10 *Manage projects*

2. *Acquire and Implement* (AI) – Akuisisi dan Implementasi

   Untuk merealisasikan strategi TI, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan terintegrasi ke dalam proses bisnis. Selain itu, perubahan serta pemeliharaan sistem yang ada harus dicakup dalam *domain* ini untuk memastikan bahwa penyelesaian yang berkelanjutan dalam memenuhi tujuan-tujuan bisnisnya. *Domain* ini biasanya membahas pertanyaan manajemen sebagai berikut :

   a. Apakah proyek baru dapat memberikan solusi terhadap kebutuhan bisnis?
   b. Apakah proyek baru dapat selesai tepat waktu dan sesuai anggaran?
   c. Apakah sistem kerja yang baru bisa diterapkan dengan baik?
   d. Apakah perubahan yang dibuat tidak mengganggu kegiatan bisnis yang berjalan?

   Domain AI terdiri dari 7 Proses TI, meliputi :

   AI1 *Identify automated solutions*

   AI2 *Acquire and maintain application software*

   AI3 *Acquire and maintain technology infrastructure*

   AI4 *Enable operation and use*

AI5 *Procure IT resources*

AI6 *Manage changes*

AI7 *Install and accredit solutions and changes*

3. *Deliver and Support* (DS) – Penyampaian dan Dukungan

   Domain ini berkaitan dengan penyampaian layanan yang diperlukan, yang meliputi penyampaian layanan, pengelolaan keamanan dan kontinuitas, dukungan layanan bagi pengguna dan manajemen data serta fasilitas operasional. *Domain* ini biasanya membahas pertanyaan manajemen sebagai berikut :

   a. Apakah layanan TI yang diberikan sesuai dengan prioritas bisnis?
   b. Apakah biaya TI dapat dioptimalkan?
   c. Apakah pekerja mampu menggunakan sistem TI lebih produktif dan aman?
   d. Apakah kerahasiaan yang memadai, integritas dan ketersediaan sudah sesuai dengan keamanan informasi?

   Domain DS terdiri dari 13 Proses TI, meliputi :

   DS1 *Define and manage service levels*

   DS2 *Manage third-party services*

   DS3 *Manage performance and capacity*

   DS4 *Ensure continuous service*

   DS5 *Ensure systems security*

   DS6 *Identify and allocate costs*

DS7 *Educate and train users*

DS8 *Manage service desk and incidents*

DS9 *Manage the configuration*

DS10 *Manage problems*

DS11 *Manage data*

DS12 *Manage the physical environment*

DS13 *Manage operations*

4. *Monitor and Evaluate* (ME) – Pemantauan dan Evaluasi

   Semua proses TI perlu dinilai secara berkala sepanjang waktu untuk menjaga kualitas dan pemenuhan atas syarat pengendalian. *Domain* ini menunjuk pada perlunya manajemen kinerja, proses pengendalian dalam organisasi serta kepatuhan terhadap peraturan dan tata kelola. *Domain* ini biasanya membahas pertanyaan manajemen sebagai berikut :

   a. Apakah jaminan kemandirian yang diperlukan memastikan bidang-bidang kritis bisa beroperasi sesuai dengan yang diharapkan?
   b. Apakah kinerja TI diukur untuk mendeteksi masalah sebelum terlambat?
   c. Apakah manajemen dapat memastikan bahwa pengendalian internal yang efektif dan efisien?
   d. Dapatkah kinerja TI dihubungkan kembali ke tujuan bisnis?
   e. Apakah kerahasiaan, integritas dan ketersediaan kontrol yang memadai sudah sesuai dengan keamanan informasi?

Domain ME terdiri dari 4 Proses TI, meliputi :

ME1 *Monitor and evaluate IT performance*

ME2 *Monitor and evaluate internal control*

ME3 *Ensure Compliance With External Requirements*

ME4 *Provide IT Governance*

Maka dengan melakukan kontrol terhadap 34 *control objectives* tersebut, organisasi dapat memperoleh keyakinan akan kelayakan tata kelola dan kendali yang diperlukan untuk lingkungan TI. Karena COBIT dirancang beriorientasi bisnis agar bisa digunakan banyak pihak, tetapi lebih penting lagi adalah sebagai panduan yang komprehensif bagi manajemen dan pemilik bisnis. Kebutuhan bisnis akan tercermin dari adanya kebutuhan informasi, dan informasi itu sendiri perlu memenuhi kriteria pengendalian tertentu, untuk mencapai tujuan bisnis.

II.3.4 Proses TI Pendukung Tata Kelola TI

COBIT menyediakan keterkaitan yang jelas antara kebutuhan Tata Kelola TI, Proses TI dan objektif kontrol TI. COBIT mendukung Tata Kelola TI dengan penyediaan kerangka kerja yang memastikan bahwa TI selaras dengan kebutuhan bisnis, TI yang mendukung bisnis dengan lebih baik dan mampu memaksimumkan manfaat, penggunaan sumber daya TI yang bertanggung jawab serta risiko TI dikelola dengan tepat. Proses-proses TI yang didefinisikan dalam kerangka kerja COBIT akan mendukung pemenuhan fokus area yang berbeda-beda dalam Tata Kelola TI.

Dukungan dan pemenuhan tersebut dapat dikelompokkan menjadi dua jenis, yakni dukungan primer (P) dan sekunder (S) seperti yang terlihat dalam Tabel II.1. Sarno (2009 :19)

Tabel II.1 Proses TI COBIT 4.1 Pendukung Tata Kelola TI

Fokus Area Tata Kelola TI	**Proses-proses Pendukung**	
	Secara Primer	**Secara Sekunder**
Strategic alignment	PO1, PO2, PO6, PO7, PO8, PO9, PO10, AI1, AI2, DS1, ME3, ME4	PO3, PO4, PO5, AI4, AI7, DS3, DS4, DS7, ME1
Value delivery	PO5, AI1, AI2, AI4, AI6, AI7, DS1, DS2, DS4, DS7, DS8, DS9, DS10, DS11, ME2, ME4	PO2, PO3, PO8, PO10, AI5, DS3, DS6, ME1
Resource management	PO2, PO3, PO4, PO7, AI3, AI5, DS1, DS3, DS6, DS9, DS11, DS13, ME4	PO1, PO5, PO10, AI1, AI4, AI6, AI7, DS2, DS4, DS7, DS12, ME1
Risk management	PO4, PO6, PO9, DS2, DS4, DS5, DS11, DS12, ME2, ME3, ME4	PO1, PO2, PO3, PO7, PO8, PO10, AI1, AI2, AI4, AI7, DS3, DS7, DS9, DS10, ME1
Performance measurement	DS1, ME1, ME4	PO5, PO7, PO10, AI7, DS2, DS3, DS4, DS6, DS8, DS10

II.3.5 DS5 (Memastikan Keamanan Sistem)

Proses TI DS5 (Memastikan Keamanan Sistem), merupakan proses untuk mempertahankan integritas informasi dan melindungi aset-aset yang diperlukan dalam proses manajemen keamanan. Proses ini meliputi peran dalam membangun dan memelihara peraturan dan tanggung jawab, kebijakan, standar dan prosedur keamanan TI. Termasuk dalam manajemen keamanan juga melakukan pemantauan keamanan dan pengujian berkala dan melaksanakan tindakan korektif untuk mengidentifikasi kelemahan keamanan atau insiden. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis terhadap kerentanan keamanan dan insiden.

Berikut ini 11 *control objectives* yang terdapat dalam proses DS5 (Memastikan Keamanan Sistem). ITGI, COBIT 4.1 (2007) :

DS5.1: Manajemen Keamanan TI

Pengelolaan keamanan TI di tingkat organisasi tertinggi yang cocok, sehingga tindakan pengelolaan keamanan selaras dengan kebutuhan bisnis.

DS5.2 : Rencana Keamanan TI

1. Penerjemahan bisnis, risiko dan kebutuhan akan kepatutan terhadap seluruh rencana keamanan TI, yang mempertimbangkan infrastruktur TI dan budaya keamanan.
2. Kepastian bahwa rencana keamanan diimplementasikan dalam kebijakan keamanan dan prosedur bersama dengan investasi yang sesuai terhadap layanan, Sumber Daya Manusia (SDM), perangkat lunak dan perangkat keras.
3. Pengkomunikasian kebijakan keamanan dan prosedur kepada pemangku kepentingan *(stakeholder)* dan pengguna.

DS5.3 : Manajemen Identitas

1. Kepastian bahwa semua pengguna (internal, eksternal dan sementara) dan aktivitasnya dalam sistem TI (aplikasi bisnis, lingkungan TI, sistem operasi, pengembangan dan pemeliharaan) secara spesifik teridentifikasi.
2. Memungkinkan pengenalan pengguna melalui mekanisme yang otentik.
3. Konfirmasi bahwa pengguna menggunakan hak terhadap sistem dan data yang selaras dengan kebutuhan bisnis yang terdokumentasi dan terdefinisi serta kebutuhan kerja dilampirkan dalam identitas pengguna.

4. Kepastian bahwa hak akses pengguna yang diminta oleh manajemen pengguna dan disetujui oleh pemilik sistem dan diimplementasikan oleh pihak yang bertanggung jawab terhadap keamanan.
5. Pemeliharaan identitas pengguna dan hak akses ke dalam tempat penyimpanan utama.
6. Penyebaran pengukuran prosedur dan teknis yang efektif secara biaya dan membuatnya tetap mutakhir untuk penetapan identifikasi pengguna, pengimplementasian otentifikasi dan penggunaan hak akses.

DS5.4 : Manajemen Akun Pengguna

1. Penempatan permintaan, penetapan, permasalahan, penundaan, pemodifikasian dan penutupan akun pengguna beserta hak-hak terkait dengan prosedur pengelolaan akun pengguna. Hal tersebut termasuk prosedur persetujuan yang menguraikan pemilik data atau sistem memberi hak akses istimewa. Prosedur yang dibuat dapat digunakan untuk semua pengguna, termasuk admin serta pengguna internal dan eksternal untuk kasus normal atau keadaan darurat.
2. Hak dan kewajiban bersifat relatif untuk pengaksesan terhadap sistem perusahaan dan informasi seharusnya diatur secara kontrak untuk semua tipe pengguna.
3. Pelaksanaan tinjauan manajemen secara rutin terhadap semua akun dan hak istemewa terkait.

DS5.5 : Pengujian, Pengamatan dan Pengawasan Keamanan

1. Pengujian dan pengawasan implementasi keamanan TI dengan cara proaktif.
2. Keamanan TI seharusnya kembali diakui secara tepat waktu untuk kepastian bahwa dasar keamanan informasi perusahaan yang disetujui telah dipelihara.
3. Daftar historis dan fungsi pengawasan akan memungkinkan pencegahan dini dan/atau pendeteksian dan pelaporan berikutnya yang tepat waktu dari aktivitas yang tidak normal dan/atau tidak biasanya yang mungkin perlu diperhatikan.

DS5.6 : Definisi Insiden Keamanan

Secara jelas mendefinisikan dan mengkomunikasikan karakteristik dari insiden keamanan yang potensial sehingga dapat diklasifikasikan secara benar dan ditangani oleh proses pengelolaan insiden dan permasalahan.

DS5.7 : Perlindungan Teknologi Keamanan

Pembuatan teknologi terkait dengan keamanan yang resisten terhadap perusakan dan tidak memperlihatkan dokumentasi keamanan yang tidak perlu.

DS5.8 : Manajemen Kunci Kriptografi

Penentuan bahwa prosedur dan kebijakan telah ditempatkan untuk pengorganisasian pembangkitan, perubahan, pembatalan, perusakan, distribusi, sertifikasi, pemasukan, penggunaan dan penyimpanan kunci

kriptografi untuk memastikan bahwa kunci terproteksi dari penyingkapan yang tidak terotorifikasi dan modifikasi.

DS5.9 : Pencegahan, Pendektesian dan Koreksi terhadap *Malicious Software* yang Berbahaya

Pencegahan, penyelidikan dan pengukuran perbaikan ditempatkan (khususnya *security patches* dan kontrol virus yang *up-to-date)* di seluruh perusahaan untuk proteksi sistem informasi dan teknologi dari *malware* (contohnya: virus, *worm, spy ware, spam).*

DS5.10 : Keamanan Jaringan

Penggunaan teknik keamanan dan prosedur pengelolaan terkait (contoh: *firewall,* alat-alat keamanan, segmentasi Jaringan, deteksi gangguan) untuk pengotorisasian akses dan aliran informasi kontrol dari dan ke jaringan.

DS5.11 : Pertukaran Data Sensitif

Pertukaran data transaksi yang sensitif hanya melalui jalur yang dipercaya dengan kontrol untuk penyediaan kebenaran isi, bukti kepatuhan, bukti penerimaan dan penolakan ketidakaslian.

DS5 (Memastikan Keamanan Sistem) memiliki kriteria informasi *Confidentiality* dan *Integrity* untuk kategori primer sedang *Avaibility*, *Compliance* dan *Reliability* untuk kategori sekunder. Sedangkan komponen sumber daya TI DS5 (Memastikan Keamanan Sistem) antara lain Aplikasi, Informasi, Infrastruktur dan Manusia.

II.3.6 Pedoman Manajemen dalam COBIT 4.1

Pedoman manajemen untuk COBIT terdiri dari model kematangan, CSFs, KGIs dan KPIs. Pedoman manajemen berisi arahan, baik secara umum maupun spesifik, mengenai apa saja yang mesti dilakukan, terutama agar dapat menjawab pertanyaan-pertanyaan berikut :

1. Sejauh mana TI harus bergerak dan apakah biaya TI yang dikeluarkan sesuai dengan manfaat yang dihasilkannya?
2. Apa saja indikator untuk suatu kinerja yang bagus?
3. Apa saja faktor yang harus diciptakan agar dapat mencapai sukses?
4. Apa saja risiko-risiko yang timbul, apabila tidak tercapai sasaran yang ditentukan?
5. Bagaimana dengan perusahaan lainnya, apa yang mereka lakukan?
6. Bagaimana mengukur keberhasilan dan bagaimana pula membandingkannya?

III.3.6.1 Model Kematangan

Model kematangan untuk pengelolaan dan kontrol pada Proses TI didasarkan pada metode evaluasi organisasi, sehingga dapat mengevaluasi sendiri dari level tidak ada (0) hingga optimis (5). Pendekatan ini diperoleh dari model kematangan dari *Software Engineering Institute* yang mendefinisikannya untuk kapabilitas pengembangan perangkat lunak. Model kematangan dimaksudkan untuk mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan. Model kematangan dirancang sebagai profil proses TI, sehingga organisasi akan dapat mengenali sebagai deskripsi kemungkinan keadaan

sekarang dan mendatang. Penggunaan model kematangan yang dikembangkan untuk setiap 34 Proses TI, memungkinkan manajemen dapat mengidentifikasi :

1. Kinerja sesungguhnya perusahaan, di mana kondisi perusahaan sekarang.
2. Kondisi sekarang dari industri sebagai perbandingan.
3. Target peningkatan perusahaan, di mana kondisi yang diinginkan perusahaan.

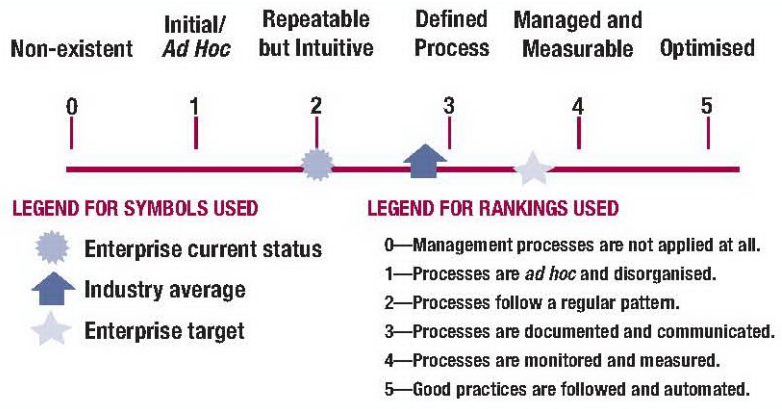
Setiap 34 proses TI mempunyai sebuah model kematangan yang telah didefinisikan dengan diberikan skala pengukuran bertingkat dari 0 (tidak ada) hingga 5 (optimis). Model kematangan yang dibangun berawal dari *generic qualitative model*, di mana prinsip dari atribut berikut ditambahkan dengan cara bertingkat :

1. Kepedulian dan komunikasi (*awareness and communication*).
2. Kebijakan, standar dan prosedur (*policies, standards and procedures*).
3. Perangkat bantu dan otomatisasi (*tools and automation*).
4. Ketrampilan dan keahlian (*skills and expertise*).
5. Pertanggungjawaban internal dan eksternal (*responsibility and accountability*).
6. Penetapan tujuan dan Pengukuran (*goal setting and measurement*).

Beberapa hal berikut memberikan gambaran singkat terkait dengan model kematangan dalam COBIT, sebagai berikut :

1. Menunjukkan tingkat seberapa baik aktivitas untuk mengelola proses TI tersebut dilakukan.
2. Terdiri dari 6 level yang berisi beberapa pernyataan.

3. Pernyataan menguraikan kondisi yang harus dipenuhi untuk mencapai level tersebut.
4. Pernyataan tersebut memiliki referensi kepada aktivitas yang ada dalam diagram *Responsible, Accountable, Consulted and/or Informed* (RACI).
5. Dari pernyataan tersebut dibuat pertanyaan-pertanyaan kepada pihak yang berkaitan (dengan mereferensi pada diagram RACI).
6. Dilakukan penilaian yang menghasilkan tingkat kematangan.



Gambar II.6 Skala Model Kematangan
Sumber: ITGI, COBIT 4.1 (2007)

Pendefinisian model kematangan suatu proses TI mengacu pada kerangka kerja COBIT secara umum adalah sebagai berikut:

Level 0 : Tidak ada (*Non-existent*)

1. Kondisi di mana perusahaan sama sekali tidak perduli terhadap pentingnya TI untuk dikelola secara baik oleh manajemen.

Level 1 : Awal (*Initial/Ad Hoc*)

1. Kondisi di mana perusahaan secara reaktif melakukan penerapan dan implementasi TI sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelumnya.

Level 2 : Berulang tapi intuitif (*Repeatable but Intuitive*)

1. Kondisi di mana perusahaan telah memiliki pola yang berulang kali dilakukan dalam melakuan manajemen aktivitas terkait dengan tata kelola TI, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidakkonsistenan.
2. Sudah mulai ada prosedur namun tidak seluruhnya terdokumentasi dan tidak seluruhnya disosialisasikan kepada pelaksana.
3. Belum ada pelatihan formal untuk mensosialisasikan prosedur tersebut.
4. Tanggung jawab pelaksanaan berada pada masing-masing individu.

Level 3 : Proses Terdefinisi (*Defined*)

1. Kondisi di mana perusahaan telah memiliki prosedur standar formal dan tertulis yang telah disosialisasikan ke segenap jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.
2. Tidak ada pengawasan untuk menjalankan prosedur, sehingga memungkinkan terjadinya banyak penyimpangan.

Level 4 : Terkelola dan Terukur (*Managed and Measurable*)

1. Kondisi di mana perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun objektif terhadap kinerja proses TI.
2. Terdapat fasilitas untuk memonitor dan mengukur prosedur yangj sudah berjalan, yang dapat mengambil tindakan, jika terdapat proses yang diindikasikan tidak efektif.
3. Proses diperbaiki terus menerus dan dibandingkan dengan praktik-praktik terbaik.
4. Terdapat perangkat bantu dan otomatisasi untuk pengawasan proses.

Level 5 : Optimis (*Optimised*)

1. Kondisi di mana perusahaan dianggap telah mengimplementasikan tata kelola manajemen TI yang mengacu pada praktik terbaik.
2. Proses telah mencapai level terbaik karena perbaikan yang terusj menerus dan perbandingan dengan perusahaan lain.
3. Perangkat bantu otomatis digunakan untuk mendukung workflow, menambah efisiensi dan kualitas kinerja proses.
4. Memudahkan perusahaan untuk beradaptasi terhadap perubahan.

Dalam melakukan pengukuran kematangan pada suatu proses, terlebih dulu perlu kejelasan tentang tujuan pengukuran itu sendiri. Dalam hal ini perlu dipahami secara jelas apa yang perlu diukur dan apa yang akan dilakukan pada saat melakukan pengukuran, karena pengukuran kematangan sebagai pendukung.

Beberapa tujuan pengukuran kematangan adalah untuk :

1. Menumbuhkan kepedulian (*awareness*).
2. Melakukan identifikasi kelemahan (*weakness*).
3. Melakukan identifikasi kebutuhan perbaikan (*improvement*).

Metode pendekatan dalam melakukan penilaian kematangan di antaranya adalah:

1. Pendekatan multidisiplin kelompok orang yang mendiskusikan dan menghasilkan kesepakatan tingkat kematangan kondisi sekarang.
2. Dekomposisi deskripsi kematangan kedalam beberapa pernyataan sehingga manajemen dapat memberikan tingkat persetujuannya.
3. Penggunaan matriks atribut kematangan sebagaimana didokumentasikan dalam *COBIT's Management Guidelines* dan memberikan nilai masing-masing atribut dari setiap proses.

Dengan mempertimbangkan bahwa tujuan penelitian ini lebih ditekankan untuk dapat mendefinisikan secara komprehensif suatu usulan perbaikan tata kelola pada proses pengelolaan data, maka metode pendekatan yang digunakan dalam pengukuran tingkat kematangan proses pengelolaan data adalah dengan melakukan penilaian dan pengukuran terhadap keseluruhan atribut kematangan yang telah didefinisikan dalam COBIT.

Pederiva (2003) menyatakan bahwa dalam pemetaan tingkat kematangan terdapat 4 kemungkinan dalam menjawab pernyataan persetujuan kuesioner, dan tiap tingkat kematangan masing-masing mempunyai kontribusi yang berbeda-beda, seperti yang terdapat dalam Tabel II.2, Tabel II,3 dan Tabel II.4.

Tabel II.2 Bobot Kepatuhan Pernyataan

Pernyataan Persetujuan	Bobot Kepatuhan
Tidak sama sekali	0
Sedikit	0,33
Dalam Tingkatan Tertentu	0,66
Seluruhnya	1

Tabel II.3 Kontribusi Tiap Tingkat Kematangan

Tingkat Kematangan	Kontribusi
1	0,33
2	0,66
3	1
4	1,33
5	1,66

$$\text{Kepatuhan Tiap Tingkat} = \frac{\Sigma \text{ (Total Jawaban Pernyataan x Bobot)}}{\Sigma \text{ Total Jawaban}}$$

Indeks Kematangan = Σ (Kepatuhan Tiap Tingkat x Bobot Kontribusi)

Tabel II.4 Representasi Indeks Kematangan

Indeks Kematangan	Tingkat Kematangan
0 – 0,50	0 - *Non-Existent*
0,51 – 1,50	1 - *Initial / ad Hoc*
1,51 – 2,50	2 - *Repeatable But Intuitive*
2,51 – 3,50	3 - *Defined Process*
3,51 – 4,50	4 - *Managed and Measurable*
4,51 – 5,00	5 - *Optimized*

III.3.6.2 Pengukuran Kinerja

Tujuan dan ukuran didefinisikan dalam COBIT pada tiga tingkat :

1. Tujuan dan ukuran TI, yang mendefinisikan apa yang diharapkan bisnis dari TI (apa yang akan bisnis gunakan untuk mengukur TI?).
2. Tujuan dan ukuran proses, yang mendefinisikan proses apa yang harus diberikan untuk mendukung tujuan TI (bagaimana pemilik proses TI akan diukur?).
3. Ukuran kinerja proses (untuk mengukur seberapa baik proses dilakukan untuk menunjukkan jika tujuan kemungkinan besar terpenuhi).

COBIT menggunakan 2 jenis ukuran yaitu *Key Goal Indicators* (KGIs) dan *Key Performance Indicators* (KPIs). KGIs pada tingkat yang lebih rendah menjadi KPIs pada tingkat yang lebih tinggi.

1. *Key Goal Indicators* (KGIs)

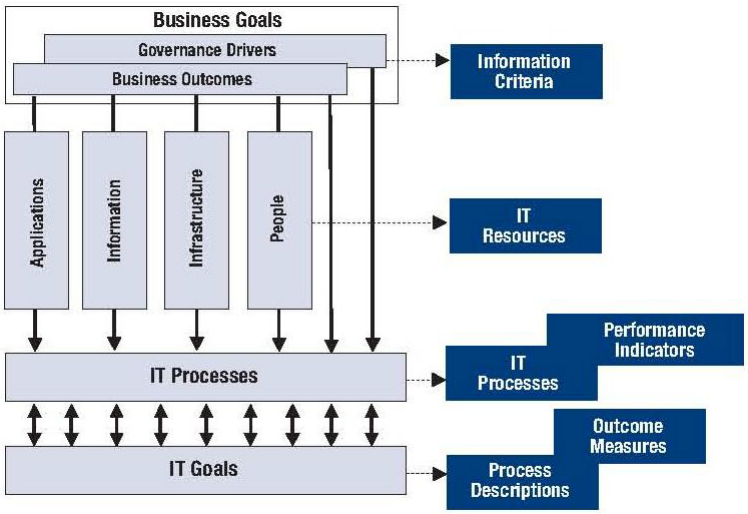
KGIs atau Indikator Tujuan Utama mendefinisikan pengukuran yang menginformasikan kepada manajemen sesudah terjadinya fakta/aktivitas apakah suatu proses TI telah mencapai kebutuhan bisnisnya, biasanya dinyatakan berkaitan dengan kriteria informasi sebagai berikut:

a. Ketersediaan informasi yang diperlukan untuk mendukung kebutuhan bisnis.
b. Ketiadaan integritas dan risiko kerahasiaan.
c. Efisiensi biaya proses dan operasi.
d. Konfirmasi keandalan, efektivitas dan kepatuhan.

2. *Key Performance Indicators* (KPIs)

KPIs atau Indikator Kinerja Utama mendefinisikan pengukuran yang menentukan seberapa baik Proses TI dilakukan. Hal ini, mengindikasikan kemungkinan pencapaian tujuannya. KPIs di samping merupakan indikator petunjuk, apakah tujuan sepertinya akan dicapai atau tidak, juga merupakan indikator kapabilitas, praktik dan ketrampilan yang baik. KPIs mengukur tujuan aktivitas yang merupakan tindakan yang harus diambil pemilik proses untuk mencapai proses yang efektif.

Model proses COBIT memungkinkan aktivitas TI dan sumber daya yang mendukungnya dikelola dan dikontrol dengan tepat berdasarkan tujuan kendali COBIT, serta diselaraskan dan dimonitor menggunakan ukuran KGIs dan KPIs, sebagaimana terlihat pada Gambar II.6. Surendro (2009 : 247-254)



Gambar II.7 Manajemen, Kontrol, Keselarasan dan Monitoring
Sumber: ITGI, COBIT 4.1 (2007)

3. *Critical Success Factors* (CSFs)

CSFs berfungsi sebagai panduan bagi manajemen dalam menerapkan kendali untuk TI dan proses-prosesnya. CSFs merupakan hal yang paling penting dilakukan serta berkontribusi dalam mencapai tujuan yang akan dicapai oleh proses-proses TI. CSFs merupakan aktivitas yang dapat bersifat strategis, teknis, organisasional, proses atau kebiasaan prosedural. CSFs umumnya terkait dengan kemampuan dan keahlian serta harus bersifat singkat, terfokus dan berorientasi pada tindakan, serta mempengaruhi sumberdaya yang sangat penting dalam sebuah proses.

Model kendali standar berikut ini mengidentifikasi sejumlah CSFs yang umumnya diterapkan untuk keseluruhan proses karena terkait dengan apa yang dimaksud dengan standar, pihak mana yang menyusun, mengontrol atau mengambil tindakan, dan sebagainya. Prinsip-prinsip dari model kendali tersebut antara lain :

a. Proses yang terdefinisi dan terdokumentasi.
b. Kebijakan yang terdefinisi dan terdokumentasi.
c. Akuntabilitas yang jelas.
d. Dukungan/komitmen yang kuat dari manajemen.
e. Komunikasi yang tepat ke pihak internal dan eksternal.
f. Pelaksanaan pengukuran secara konsisten.

II.4 AHP (*Analytical Hierarchy Process*)

Proses Hierarki Analitik (*Analytical Hierarchy Process* - AHP) dikembangkan oleh Dr. Thomas L. Saaty dari *Wharton School of Business* pada tahun 1970-an untuk mengorganisir informasi dan pendapat ahli (*judgment*) dalam memilih alternatif yang paling disukai (Saaty 1983). Dengan menggunakan AHP, suatu persoalan akan diselesaikan dalam suatu kerangka pemikiran yang terorganisir, sehingga dapat diekspresikan untuk mengambil keputusan yang efektif atas persoalan tersebut. Persoalan yang kompleks dapat disederhanakan dan dipercepat proses pengambilan keputusannya.

Secara grafis, persoalan keputusan AHP dapat dikonstruksikan sebagai diagram bertingkat (hierarki). AHP dimulai dengan *goal*/sasaran lalu kriteria level pertama, subkriteria dan akhirnya alternatif. Terdapat berbagai bentuk hierarki keputusan yang disesuaikan dengan subtansi dan persoalan yang yang dapat diselesaikan dengan AHP. AHP memungkinkan pengguna untuk memberikan nilai bobot relatif dari suatu kriteria majemuk atau alternatif majemuk terhadap suatu kriteria. Pemberian bobot tersebut secara intuitif, yaitu dengan melakukan perbandingan berpasangan (*pairwise comparisons*). Dr. Thomas Saaty, kemudian menentukan cara yang konsisten untuk mengubah perbandingan berpasangan/*pairwise* menjadi suatu himpunan bilangan yang merepresentasikan prioritas relatif dari setiap kriteria dan alternatif. AHP juga menguji konsistensi penilaian bila terjadi penyimpangan yang terlalu jauh dari nilai konsistensi sempurna, maka hal ini menunjukkan penilaian perlu diperbaiki, atau hierarki harus distruktur ulang.

II.4.1 Langkah AHP

Terdapat tiga prinsip dalam memecahkan persoalan dengan analisis logis eksplisit, yaitu penyusunan hierarki, penetapan prioritas, dan konsistensi logis.

1. Penyusunan Hierarki

   Penilaian setiap level hierarki dinilai melalui perbandingan berpasangan. Menurut Saaty (1983), untuk berbagai persoalan, skala 1 sampai 9 adalah skala terbaik dalam mengekspresikan pendapat. Skala 1-9 ditetapkan sebagai pertimbangan dalam membandingkan pasangan elemen di setiap level hierarki terhadap suatu elemen yang berada di level atasnya. Skala dengan sembilan satuan dapat menggambarkan derajat sampai mana kita mampu membedakan intensitas tata hubungan antarelemen.

   Perbandingan berpasangan ini dilakukan dalam sebuah matriks. Matriks merupakan tabel untuk membandingkan elemen satu dengan elemen lain terhadap suatu kriteria yang ditentukan. Matriks memberi kerangka untuk menguji konsistensi, membuat segala pembandingan yang mungkin, dan menganalisis kepekaan prioritas menyeluruh terhadap perubahan dalam pertimbangan. Matriks secara unik menggambarkan prioritas saling mendominasi antara satu elemen dengan elemen lainnya.

Nilai dan definisi pendapat kualitatif dari skala perbandingan Saaty dapat dilihat pada Tabel II.5 berikut :

Tabel II.5 Skala perbandingan berpasangan

Nilai/Tingkat Kepentingan	**Keterangan**	**Definisi**
1	Faktor vertikal sama penting dengan faktor horizontal	Kedua kriteria sama pentingnya (*equal*).
3	Faktor vertikal lebih penting dari faktor horisontal	Kriteria yang satu sedikit lebih penting dibandingkan kriteria lainnya (*moderat*e).
5	Faktor vertikal jelas lebih penting faktor horisontal	Kriteria yang satu esensial atau sangat penting dibanding kriteria lainnya (*strong*).
7	Faktor vertikal sangat jelas lebih penting dari faktor horisontal	Kriteria yang satu jelas lebih penting dibanding kriteria lainnya (*very strong*).
9	Faktor vertikal mutlak lebih penting dari faktor horisontal	Kriteria yang satu mutlak lebih penting dibanding kriteria lainnya (*extreme*).
2, 4, 6, 8	Apabila ragu-ragu antara dua nilai elemen yang berdekatan	Nilai-nilai tengah (*intermediate*).
1/(2-9)	Kebalikan dari keterangan nilai 2-9	

2. Penentuan Prioritas

   Untuk setiap level hierarki, perlu dilakukan perbandingan berpasangan (*pairwise comparisons*) untuk menentukan prioritas. Sepasang elemen dibandingkan berdasarkan kriteria tertentu dan menimbang intensitas preferensi antarelemen. Hubungan antarelemen dari setiap tingkatan hierarki ditetapkan dengan membandingkan elemen itu dalam pasangan. Hubungannya menggambarkan pengaruh relatif elemen pada tingkat hierarki terhadap setiap elemen pada tingkat yang lebih tinggi. Dalam konteks ini, elemen pada tingkat yang tinggi tersebut berfungsi sebagai suatu kriteria disebut sifat (*property*).

Hasil dari proses pembedaan ini adalah suatu vektor prioritas atau relatif pentingnya elemen terhadap setiap sifat. Perbandingan berpasangan diulangi lagi untuk semua elemen dalam tiap tingkat. Langkah terakhir adalah dengan memberi bobot setiap vektor dengan prioritas sifatnya. Proses perbandingan berpasangan dimulai pada puncak hierarki (*goal*) digunakan untuk melakukan pembandingan yang pertama lalu dari level tepat di bawahnya (kriteria).

Dalam membandingkan antarelemen, tanyakanlah seberapa kuat suatu elemen mempengaruhi *goal* dibandingkan dengan eleman lain yang sedang dibandingkan. Susunan pertanyaan ini harus mencerminkan tata hubungan yang tepat antara elemen-elemen di suatu level dengan sebuah elemen yang ada di level atasnya.

Bila membandingkan suatu elemen dalam matriks dengan elemen itu sendiri, perbandingan tersebut bernilai 1, maka isilah diagonal matriks tersebut dengan bilangan 1. Selalu bandingkan elemen pertama dari suatu pasangan (elemen di kolom sebelah kiri matriks) dengan elemen yang kedua (elemen di baris puncak) dan taksir nilai numeriknya dari skala. Nilai kebalikannya digunakan untuk perbandingan elemen kedua dengan elemen pertamanya tadi. Misalnya, jika kedua elemen itu adalah x dan x1 lima kali x2, maka x2 adalah 1/5 kali dari x1. Nilai-nilai perbandingan relatif kemudian diolah untuk menentukan peringkat relatif dari seluruh alternatif. Setiap level hierarki baik kuantitatif dan kualitatif dapat dibandingkan sesuai dengan *judgement* yang telah ditentukan untuk menghasilkan bobot dan prioritas. Bobot atau prioritas dihitung dengan manipulasi matrik atau melalui penyelesaiaan persamaan matematik.

3. Konsistensi Logis

   Semua elemen dikelompokkan secara logis dan diperingkatkan secara konsisten sesuai dengan suatu kriteria yang logis. Penilaian yang mempunyai konsisten tinggi sangat diperlukan dalam persoalan pengambilan keputusan agar hasil keputusannya akurat. Dalam kehidupan nyata, konsistensi sempurna sukar dicapai. Konsistensi sampai batas tertentu dalam menetapkan pioritas sangat diperlukan untuk memperoleh hasil-hasil yang sahih dalam dunia nyata. AHP mengukur konsistensi menyeluruh dari berbagai pertimbangan melalui suatu rasio konsistensi. Nilai rasio konsistensi harus 10 persen atau kurang. Jika lebih dari 10 persen, maka penilaiannya masih acak dan perlu diperbaiki. Marimin & Maghfiroh (2010 : 91-96)

II.4.2 Penyelesaian AHP dengan Expert Choice

Expert Choice merupakan salah satu software AHP yang memiliki kelebihan antara lain memiliki tampilan antarmuka yang lebih menarik, mampu untuk mengintegrasikan pendapat pakar dan tidak membatasi level dari struktur hierarki. Tahapan-tahapan perhitungan AHP dengan hierarki goal, kriteria dan alternatif menggunakan Expert Choice 11, Marimin & Maghfiroh (2010 : 116-126) :

1. Jalankan program dengan perintah: **Start/Program/Expert Choice 11**.
2. Buat File, dengan perintah **File/New**, lalu ketik nama file dan buka file dengan perintah **Open**.
3. Ketikkan *Goal* atau sasaran yang ingin dicapai di kotak "*Goal Description*" dengan nama tertentu.

4. Buat alternatif dengan cara klik kiri pada tanda +A di pojok kanan atas, kemudian masukkan nama-nama alternatif sesuai dengan hierarki. Setiap akan menambahkan alternatif, klik +A.
5. Buat kriteria dengan cara klik kanan pada *Goal*, kemudian pilih *Insert Child of current node*, ketikkan nama-nama kriteria.
6. Lakukan penilaian perbandingan berpasangan kriteria dengan *Pairwaise Numerical Comparisons* (**3:1**), lalu pilih *Record Judgement* untuk menyimpan hasil penilaian.
7. Lakukan penilaian perbandingan berpasangan alternatif pada tiap kriteria dengan *Pairwaise Numerical Comparisons* (**3:1**), lalu pilih *Record Judgement* untuk menyimpan hasil penilaian.
8. Untuk melihat hasil *Goal*, klik *Synthesize-With Respect to Goal*, maka akan muncul alternatif mana yang paling tinggi nilainya dan *Inconsistency Ratio*. Syarat *Inconsistency* itu harus ≤ 10% (0,10). Jika lebih dari 10%, perbandingan itu berarti acak dan harus diperbaiki dengan melakukan perbandingan ulang.

II.5 Pengumpulan Data dan Skala Pengukuran

Dalam riset terdapat beberapa teknik pengumpulan data, yaitu studi kepustakaan, dokumentasi, observasi, wawancara dan kuesioner.

1. Angket (kuesioner) adalah suatu cara pengumpulan data dengan menyebarkan daftar pertanyaan kepada responden, dengan harapan mereka akan memberikan respons terhadap daftar pertanyaan tersebut. Daftar pertanyaan disebut bersifat

terbuka jika jawaban tidak ditentukan sebelumnya, dan bersifat tertutup jika alternatif-alternatif jawaban telah disediakan.

2. Wawancara adalah salah satu teknik pengumpulan data. Pelaksanaannya dapat dilakukan secara langsung berhadapan muka dengan orang yang diwawancarai. Dan dikatakan tidak langsung apabila daftar pertanyaan yang diberikan dapat dijawab pada kesempatan lain. Instrumen yang digunakan dapat berupa pedoman wawancara atau checklist.
3. Observasi, teknik ini menuntut adanya pengamatan dari si periset terhadap objek risetnya, misalnya dalam melakukan eks-perimen. Instrumen yang dipakai dapat berupa lembar pengamatan, panduan pengamatan, dan lainnya.

Aspek yang harus diperhatikan dalam menyusun suatu kuesioner :

1. Komponen inti kuesioner
   a. Subyek, yaitu individu atau lembaga yang melaksanakan riset.
   b. Ajakan, yaitu permohonan dari periset kepada responden untuk turut serta mengisi kuesioner secara aktif dan objektif.
   c. Petunjuk pengisian kuesioner yang mudah dimengerti dan tidak bias.
   d. Pertanyaan atau pernyataan beserta tempat mengisi jawaban, baik secara tertutup, semi tertutup, ataupun terbuka. Dalam kuesioner jangan dilupakan isian untuk identitas responden.

2. Kuesioner sebagai kertas kerja

   Kuesioner adalah sebuah alat pengumpulan data yang nantinya data tersebut akan diolah untuk menghasilkan informasi tertentu.

3. Kriteria instrumen yang baik

   Instrumen pengumpul data yang baik, seperti kuesioner, menurut Sevilla (1988) minimal memenuhi lima kriteria, yaitu :

   a. Validitas, adalah pernyataan sampai sajauh mana data yang ditampung pada suatu kuesioner dapat mengukur apa yang ingin diukur.
   b. Reliabilitas, adalah istilah yang dipakai untuk menunjukkan sejauh mana suatu hasil pengukuran relatif konsisten apabila digunakan berulang kali.
   c. Sensitivitas, dijelaskan sebagai kemampuan suatu instrumen untuk melakukan diskriminasi. Bila reliabilitas dan validitas suatu instrumen tinggi, atau dengan kata lain sensitif, perbedaan atas tingkat variasi-variasi karakteristik yang diukur dapat mempertajam.
   d. Objektivitas, mengacu pada terbebasnya data yang diisikan pada kuesioner dari penilaian yang subyektif, misalnya perasaan responden yang cenderung mempengaruhi objektivitas data.
   e. Fisibilitas, berhubungan dengan teknis pengisian kuesioner, serta penggunaan sumber daya dan waktu.

Skala pengukuran terhadap suatu objek terdiri atas empat macam, yaitu Skala Nominal, Skala Ordinal, Skala Interval, dan Skala Rasio.

1. Skala nominal adalah skala yang paling sederhana. Angka yang diberikan untuk suatu kategori tidak menggambarkan kedudukan kategori tersebut terhadap kategori lainnya, tetapi angka tersebut hanya sekadar kode maupun label.

2. Skala Ordinal, skala ini mengurutkan data dari tingkat yang paling rendah ke tingkat yang paling tinggi atau sebaliknya dengan tidak memperhatikan interval data tersebut. Angka-angka hasil pengurutan ini berskala ordinal.
3. Skala Interval, skala ini mirip dengan skala ordinal di atas, tetapi jarak antardata harus memiliki interval yang relatif sama.
4. Skala Rasio, skala ini mencakup ketiga skala yang disebutkan di atas ditambah dengan sifat lain, yaitu bahwa ukuran ini mempunyai nilai nol yang sama.

Keempat skala ini, jika akan digunakan dalam kuesioner dapat dilakukan dengan berbagai pendekatan, misalnya skala Likert, Guttmann, Bogardus, Throstone, Stipel, *Rank-Order*, *Paired-Comparison*, dan *Semantic Differentials*.

Menurut Kinnear (1988), skala Likert berhubungan dengan pernyataan tentang sikap seseorang terhadap sesuatu. Alternatif pernyataannya, misalnya adalah dari setuju sampai tidak setuju, senang sampai tidak senang, puas sampai tidak puas atau baik sampai tidak baik. Umar (2003 : 92-102)

Menurut Widhiarso (2010) berapa kategori opsi yang disediakan dalam skala psikologi masih dalam perdebatan. Namun sebagian besar sudah menunjukkan beberapa kesepakatan yang ditunjukkan dengan hasil-hasil penelitian yang konsisten.

1. Lima kategori respons ataukah empat kategori respons?

   Meski Likert menyarankan lima alternatif respons, namun banyak ahli yang menyarankan untuk menggunakan bermacam-macam jumlah kategori respon.

Sebuah studi empiris menemukan bahwa 5 atau 7 alternatif respon skala titik dapat menghasilkan nilai rata-rata sedikit lebih tinggi (secara relatif dari skor tertinggi yang mungkin dicapai) jika dibandingkan dengan skala yang menyediakan 10 alternatif. Artinya, semakin sedikit jumlah respons variasi data semakin berkurang. Masalahnya adalah apakah setiap responden bisa memahami perbedaan kategori hingga 10 level? Jumlah pilihan di sekitar 5 hingga 7 kategori lebih disarankan dibanding alternatif di atas jumlah tersebut.

2. Mengapa responden memilih kategori tengah?

   Alternatif tengah respons disediakan untuk memfasilitasi sikap responden yang moderat, akan tetapi responden tidak hanya memilih kategori ini untuk menunjukkan traitnya yang moderat (Hofacker, 1984), namun dipengaruhi oleh banyak faktor.

   Beberapa ahli telah meneliti mengapa responden memilih alternatif tengah kategori. Shaw dan Wright (1967) mengemukakan tiga kemungkinan responden kategori tengah, yaitu :

   1. Mereka tidak memiliki sikap atau pendapat,
   2. Mereka ingin memberikan penilaian secara seimbang, atau
   3. Mereka belum memberikan sikap atau pendapat yang jelas.

   Kulas & Stachowski (2009) menjelaskan faktor lain seperti ragu, tidak memahami pernyataan dalam butir, respons mereka kondisional, atau mereka memiliki berdiri netral, moderat, atau rata-rata.

Ahli lain menjelaskan bahwa pemilihan kategori tengah menunjukkan keengganan responden untuk memilih arah tanggapan terhadap pernyataan. Bisa jadi mereka memilih respons tengah karena kesulitan menginterpretasi butir pernyataan (Goldberg, 1981). Yang et al. (2002) menemukan bahwa responden cenderung memilih kategori tengah ketika mendapati butir yang sulit dipahami.

Kesimpulannya bahwa skor skala bisa menjadi bias jika responden yang cenderung memilih kategori tengah, dikarenakan tidak memahami butir dan merasa tidak nyaman dengan pernyataan yang diberikan. Oleh karena itu bagi penyusun skala psikologi diharapkan untuk menyusun butir yang mudah dipahami dan membangun interaksi yang hangat dengan responden agar mereka merasa tidak terintervensi.

3. Dampak penyediaan kategori tengah

   Andrews (1984) menemukan bahwa keberadaan alternatif tengah eksplisit dalam kategori jawaban tidak memiliki efek yang signifikan pada kualitas data. Rerata respon terhadap butir akan meningkat secara linear dan varians item meningkat kurvelinier dengan meningkatnya jumlah kategori jawaban. Peningkatan rerata adalah wajar dan tidak menjadi masalah karena jumlah alternatif menjadi bertambah yang diiringi dengan peningkatan varians. Peningkatan varians inilah yang banyak menjadi ketertarikan kita, karena menunjukkan informasi yang kita miliki semakin bervariasi.

Di sisi lain, nilai konsistensi internal (*alpha*) tidak berubah secara sistematis dengan meningkatnya jumlah kategori respon (Aiken, 1983). Oleh karena itu, dapat disimpulkan bahwa jumlah kategori jawaban tidak membuat perbedaan dalam *mean* dan varians respon item dan skor total skala.

Kulas et al. (2008) menemukan bahwa korelasi skor antar variabel yang dihitung antara skala yang menyediakan alternatif titik tengah maupun tidak menyediakan memiliki korelasi yang tinggi, bergerak antara 0.94 hingga 1.0. Artinya, skornya yang dihasilkan sama saja sehingga validitas kriteria yang didapatkan dari korelasi dengan skor kriteria dipastikan akan tetap tidak berubah.

Mattel dan Jacoby (1971) menemukan bahwa reliabilitas pengukuran dan validitas skala independen terhadap jumlah alternatif respons.

Jadi kesimpulannya bahwa skor skala yang menyediaan kategori tengah dengan yang tidak memiliki kategori tengah, tidak memiliki perbedaan yang berarti. Reliabilitas pengukuran dan validitas butir tidak mengalami perbedaan, yang berbeda adalah varian skor. Dengan adanya kategori tengah, variasi data lebih tinggi dibanding dengan yang tidak. Oleh karena itu menyediakan kategori tengah akan menghasilkan data yang lebih bervariasi.

4. Jumlah alternatif ganjil dan genap

   Beberapa penulis secara eksplisit telah membahas masalah jumlah alternatif respon kategori yang ganjil versus genap.

Kalton, Roberts, dan Holt (1980) menunjukkan bahwa ketika inves tigators memutuskan untuk tidak menawarkan alternatif tengah eksplisit, mereka biasanya menganggap bahwa kategori tengah terdiri sebagian besar tanggapan dari orang-orang yang bersandar terhadap satu atau kutub alternatif lain, meskipun mungkin dengan sedikit intensitas.

Klopfer (1980) berpendapat bahwa penyelidik yang menawarkan alternatif yang mungkin tengah berasumsi bahwa responden benar-benar mendukung posisi tengah. Akibatnya, jika responden dipaksa untuk memilih alternatif yang ada, pilihan ini akan memberikan kontribusi kesalahan pengukuran sistematis.

Jadi kesimpulannya bahwa jumlah opsi genap akan memaksa responden untuk memilih sikap yang jelas terhadap pernyataan yang diberikan sedangkan jumlah opsi ganjil memfasilitasi responden yang belum memiliki sikap yang jelas. Pemaksaan tersebut dapat menimbulkan eror pengukuran, karena skor yang dihasilkan tidak benar-benar menggambarkan diri responden.

5. Menyediakan alternatif tengah meningkatkan jumlah pemilihnya

   Kalton, Roberts, dan Holt (1980) melaporkan bahwa pilihan kategori respon tengah berkisar antara 15 dan 49 persen ketika item kuesioner menyediakan titik tengah secara eksplisit dalam kategori respons yang berjumlah ganjil. Di sisi lain Presser dan Schuman (1980) menemukan jumlah yang lebih sedikit yaitu antara 10 dan 20 persen. Hal ini menunjukkan bahwa penyediaan alternatif respon tengah meningkatkan proporsi responden yang menyatakan

pandangan netral secara substansial. Kecenderungan ini bahkan meningkat ketika isu-isu sensitif pertanyaan perhatian (Kalton & Schuman, 1982).

DuBois dan Burns (1975) berargumen bahwa responden memilih alternatif tengah karena merasa ambivalen (tidak dapat memutuskan apakah akan setuju atau tidak setuju), indiferen (tidak peduli) atau tidak merasa cukup kompeten atau cukup informasi untuk mengambil sikap.

Jadi kesimpulannya bahwa menyediakan alternatif tengah memang akan meningkatkan jumlah pemilihnya, tapi kecenderungan itu meningkat tajam jika pernyataan yang tertulis dalam butir kurang mudah dipahami, membingungkan atau mengurangi kenyamanan/keamanan responden. Untuk mengatasi hal ini penulis butir diharapkan menulis butir dengan pernyataan yang jelas dan tidak mengintervensi responden.

Sebagai kesimpulan akhir bahwa penulis kuesioner harus memutuskan apakah memasukkan titik tengah atau tidak sesuai dengan pernyataan yang diberikan kepada responden (Brace, 2004). Meskipun penggunaan respon kategori tengah tidak mempengaruhi reliabilitas dan validitas dalam penelitian ini, namun direkomendasikan bahwa penilaian pengembang kuesioner untuk memasukkan alternatif tengah (Kulas, et al., 2008). Ahli lain bahwa menyediakan kategori tengah memungkinkan responden untuk menunjukkan respon yang netral dan lebih diskriminatif dalam respon mereka, membuat nilai skala yang lebih handal dan skala yang lebih disukai oleh responden (Cronbach, 1950).

Banyak peneliti menyimpulkan bahwa berapa jumlah optimal kategori skala tergantung dari spesifik isi dan fungsi dari kondisi pengukuran (e.g. Friedman, Wilamowsky, & Friedman, 1981). Misalnya dalam konteks seleksi karyawan, penggunaan skala tanpa kategori tengah lebih mampu mereduksi kepatutan sosial (social desirability) dibanding dengan yang menggunakan kategori tengah (Garland, 1991). Widhiarso (2010)