BAB II

LANDASAN TEORI

2.1. Penelitian Sebelumnya

Penelitian sebelumnya yang dijadikan referensi berjudul "Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27002 Pada PT Aneka Jaya Baut Sejahtera (PT AJBS)". Audit yang digunakan pada penelitian tersebut yaitu audit keamanan informasi. *Framework* yang digunakan pada penelitian ini yaitu ISO 27002. Tujuan dilakukannya audit keamanan sistem informasi ini yaitu untuk mengetahui sampai di mana tingkat keamanan sistem informasi yang dimiliki oleh sistem informasi *Integrated Technology Services* (ITS) yang digunakan oleh PT AJBS (Halim, 2012).

Penelitian selanjutnya yang digunakan sebagai referensi berjudul Audit Sistem Informasi Manajemen Aset berdasarkan Perspektif Proses Bisnis *Internal Balanced Scorecard* dan Standar COBIT 4.1. pada PT Pertamina (Persero). Audit yang digunakan pada penelitian tersebut yaitu audit sistem informasi. *Framework* yang digunakan pada penelitian ini yaitu COBIT 4.1. Tujuan dilakukannya audit ini yaitu untuk memastikan keselarasan sistem informasi dengan tujuan bisnis (Dewi, dkk, 2012).

Perbedaan penelitian ini dengan penelitian sebelumnya terletak pada area audit. Pada penelitian yang berjudul "Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27002 Pada PT Aneka Jaya Baut Sejahtera (PT AJBS)" lebih menangani kepada evaluasi tentang keamanan sistem informasi *Integrated Trading System* (ITS) yang digunakan oleh PT AJBS serta *framework* yang

digunakan berbeda dengan penelitian ini. Sedangkan pada penelitian selanjutnya yang dijadikan referensi memiliki perbedaan pada penanganan audit sistem informasi yang hanya menangani audit pada manajemen aset saja.

2.2. Audit

Audit dapat didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokementasi untuk menemukan suatu bukti-bukti (audit *evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (Cannon, 2006).

2.3. Audit sistem dan teknologi informasi

Audit sistem dan teknologi informasi adalah proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif. Beberapa elemen utama tinjauan penting dalam audit sistem dan teknologi informasi yaitu dapat diklasifikasikan sebagai berikut (Riyanarto, 2009):

a. Tinjauan terkait dengan fisik dan lingkungan, yakni: hal-hal yang terkait dengan keamanan fisik, suplai sumber daya, temperatur, kontrol kelembaban dan faktor lingkungan lain.

b. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen *database*, seluruh prosedur administrasi sistem dan pelaksanaannya.

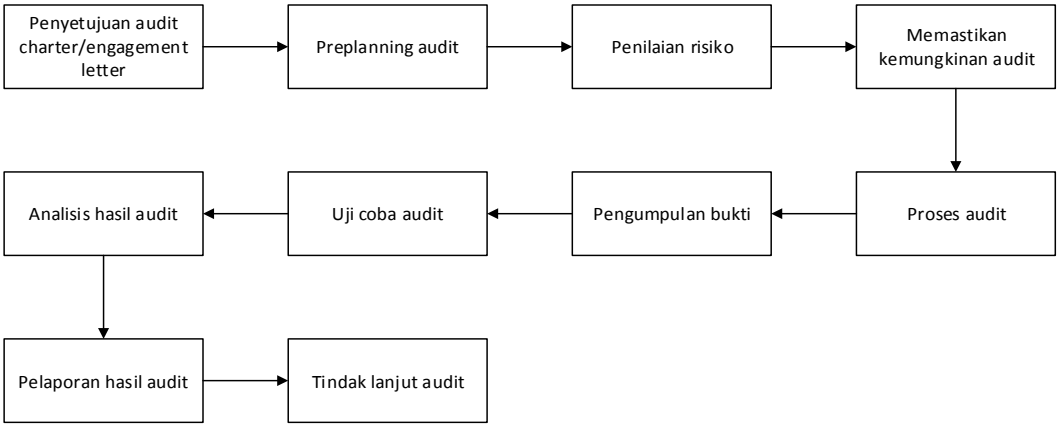
c. Tinjauan perangkat lunak. Perangkat lunak yang dimaksud merupakan aplikasi bisnis. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses bisnis dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.

d. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap *firewall*, daftar kontrol akses *router*, *port scanning* serta pendeteksian akan gangguan maupun ancaman terhadap sistem.

e. Tinjauan kontinuitas bisnis dengan memastikan ketersediaan prosedur *backup* dan penyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana/kontinuitas bisnis yang dimiliki.

f. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

Tahapan audit sistem dan teknologi informasi berdasarkan (Cannon, 2006) dapat dilihat pada gambar 2.1:



Gambar 2.1 Tahapan audit menurut Cannon (2006)

Di dalam proses audit ada tahapan yang harus dilalui untuk mencapai hasil akhir dari proses audit tersebut. Tahapan audit menurut Cannon (2006):

1. Penyetujuan *audit charter* atau *engagement letter*

   Tahap pertama di dalam proses audit ini adalah membuat *audit charter* atau *engagement letter* untuk disetujui. Auditor harus mengantongi persetujuan dari *audit charter* atau *engagement letter* ini agar mendapatkan wewenang untuk melakukan proses audit. *Audit charter* harus berisi tentang:

   a. Tanggung jawab (*responsibility*): berisi tentang ruang lingkup dengan tujuan dan sasaran audit

   b. Kewenangan (*authority*): memberikan wewenang untuk melakukan audit dan hak untuk mendapatkan akses yang relevan di dalam proses audit

   c. Pertanggungjawaban (*accountability*): mendefinisikan tindakan yang disepakati bersama antara komite audit dan auditor, lengkap dengan kebutuhan pelaporan

2. Preplanning audit

   Tahap kedua di dalam proses audit yaitu untuk merencanakan kebutuhan audit secara spesifik untuk mendapatkan sasaran audit. Auditor harus memikirkan dampak audit di dalam proses bisnis di suatu perusahaan.

3. Melakukan penilaian risiko

   Melakukan penilaian risiko adalah tahap selanjutnya di dalam melakukan proses audit dan dilakukan setelah sasaran audit telah diidentifikasi. Tujuan dari penilaian risiko ini adalah untuk memastikan bukti yang cukup akan dikumpulkan selama proses audit.

4. Memastikan kemungkinan dilakukannya audit

   Memastikan kemungkinan dilakukannya audit dilakukan setelah menilai risiko audit dan memastikan bahwa prioritas telah terpenuhi. Jika tidak dapat melakukan fungsi audit yang diperlukan, masalah akan dikomunikasikan kepada manajemen dan komite audit. Audit tanpa bukti yang adalah sia-sia.

5. Melakukan proses audit

   Tahap selanjutnya yaitu melakukan audit. Di dalam ini audit quality control harus sudah dipastikan, mendefinisikan komunikasi dengan *auditee*, melakukan pengumpulan data, dan mengulas kontrol yang telah ada

6. Pengumpulan bukti

   Tiap auditor harus mengetahui kebutuhan untuk mengumpulkan bukti. Laporan audit haus didasarkan pada bukti untuk mendukung pernyataan

audit. Menurut temuan dan bukti-bukti yang ada harus dikonfirmasikan terlebih dahulu kepada *auditee* sebelum dilaporkan secara formal kepada Direksi dalam bentuk laporan audit TI (Cannon, 2011).

7. Melakukan uji coba audit

   Metode untuk melakukan uji coba audit yaitu:

   a. *Compliance testing:* melakukan uji coba pada ada atau tidaknya sesuatu yang terdapat pada bukti yang ditemukan

   b. *Substantive testing*: melakukan verifikasi isi dan integritas dari bukti yang telah dikumpulkan pada tahap sebelumnya

8. Menganalisis hasil audit

   Tahap selanjutnya adalah menganalisis bukti dan temuan yang dikumpulkan di tahap sebelumnya untuk menemukan rekomendasi dari temuan yang ada.

9. Melaporkan hasil audit

   Setelah melakukan proses audit, tahap selanjutnya adalah melaporkan temuan yang ada. Pelaporan adalah sebuah proses yang dilakukan auditor untuk mengatur temuan audit, termasuk:

   a. Ruang lingkup audit

   b. Sasaran adit

   c. Metode dan kriteria yang digunakan

   d. Sifat temuan

   e. Besar pekerjaan yang dilakukan

10. Melakukan tindak lanjut dari hasil audit

    Setelah mengeluarkan laporan, auditor diwajibkan untuk melakukan wawancara keluar dengan manajemen untuk memperoleh komitmen untuk rekomendasi yang dibuat dalam audit. Manajemen bertanggung jawab untuk mengakui rekomendasi, dan menunjuk apa pun tindakan korektif akan diambil, termasuk tanggal taksiran tindakan.

Dalam audit berikutnya, akan memeriksa apakah manajemen diberikan komitmen untuk memperbaiki atau memulihkan kekurangan yang ditemukan dalam audit sebelumnya. Jika tidak, Anda mengharapkan manajemen untuk bertindak pada waktu yang tepat untuk memperbaiki kekurangan seperti yang dilaporkan.

2.4. Analisis Risiko

Analisis risiko yaitu suatu prosedur yang digunakan untuk mengenali satu ancaman untuk kemudian dianalisis untuk memastikan bagaimana dampak yang diimbulkan dapat dihilangkan atau dikurangi. Penelitian ini menggunakan metode analisis risiko kualitatif karena analisis risiko kualitatif digunakan untuk meningkatkan kesadaran atas masalah sistem informasi dan sikap dari sistem yang sedang dianalisis Beberapa hal yang harus diperhatikan dalam menerapkan analisis risiko (Merritt, 2014):

1. Menentukan ruang lingkup
2. Mengklasifikasikan sistem informasi ke dalam ruang lingkup yang telah ditentukan
3. Risiko dan ancaman

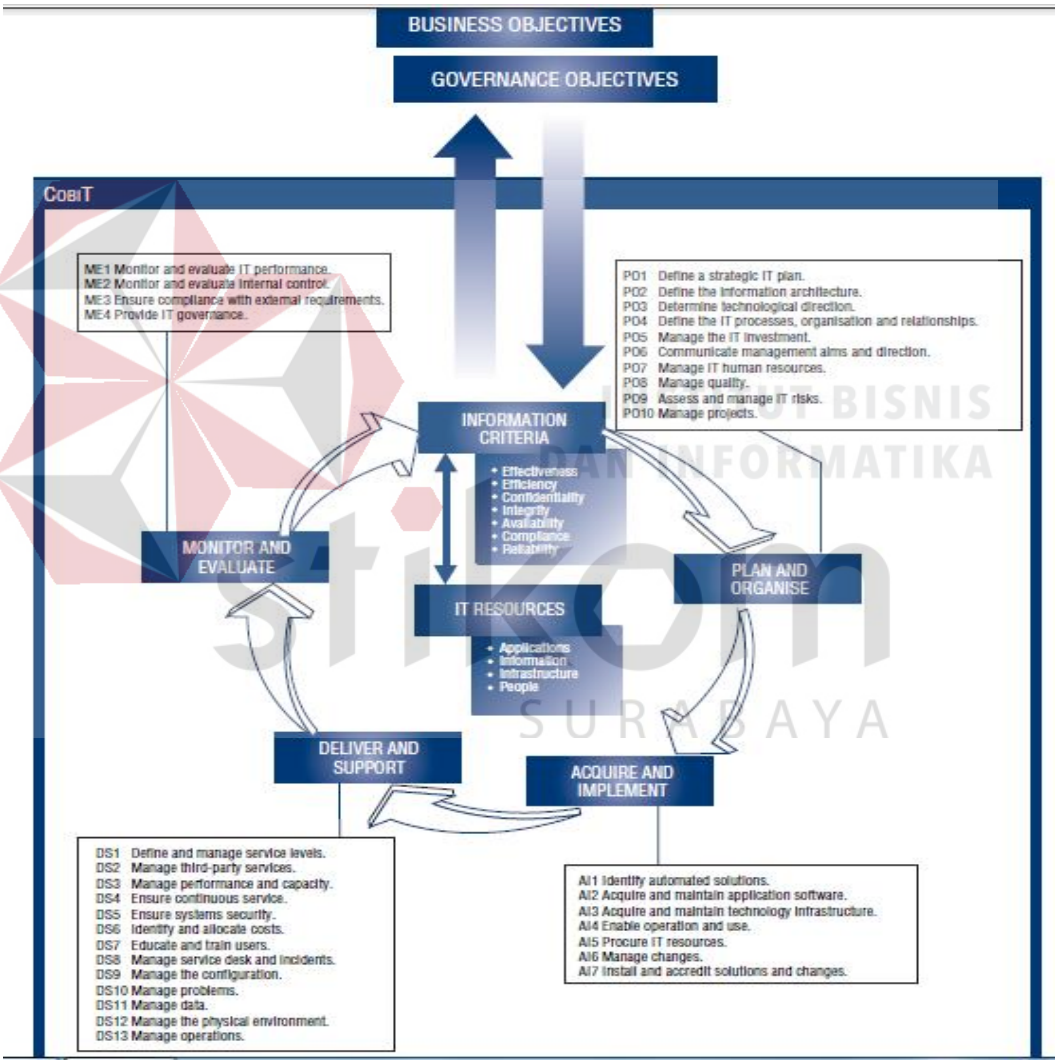
4. Menentukan koefisien dampak. Semua aset sistem informasi memiliki kerentanan yang tidak sama terhadap sebuah risiko.
5. *Single loss expentancy*. Aset sistem informasi yang berbeda memiliki respon yang berbeda kepada tiap ancaman yang ada.
6. Melakukan evaluasi.
7. Melakukan perhitungan dan analisis. Terdiri dari *acros asset* yang berarti analisis yang memiliki tujuan untuk menunjukkan aset tertentu yang harus mendapat prioritas paling utama. Analisis yang kedua disebut *across risk* yang berarti analisis yang bertujuan untuk menunjukkan ancaman apa dan bagaimana ancaman yang memiliki prioritas paling utama.
8. Pengendalian risiko.
9. Analisis terhaddap pengendalian.

2.5. COBIT

COBIT (*Control Objectives for Information and related Technology*) merupakan model tata kelola TI dalam menilai TI serta memahami dan mengelola risiko terkait TI untuk membantu auditor, manajemen, dan pengguna lainnya dalam menjembatani jarak antara harapan dengan kenyataan risiko bisnis, kebutuhan kontrol, dan permasalahan-permasalahan teknis sehingga dapat memenuhi kebutuhan tata kelola TI dan menjamin integritas informasi dan sistem informasi perusahaan. Dengan kata lain COBIT (*Control Objectives for Information and Related Technology*) adalah sekumpulan dokumentasi *best practices* untuk *IT Governance* yang dapat membantu auditor, pengguna (*user*), dan manajemen,

untuk menjembatani jarak antara risiko bisnis, kebutuhan control dan masalah-masalah teknis IT (Riyanarto, 2009). Skema COBIT dapat dilihat pada Gambar 2.2.

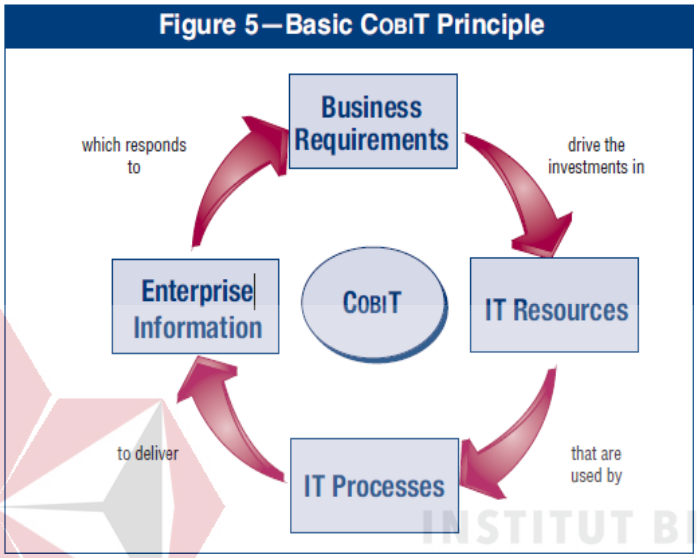
Orientasi bisnis adalah tema utama COBIT. Hal ini dirancang tidak hanya yang akan digunakan oleh layanan TI penyedia, pengguna dan auditor, tetapi juga, dan yang lebih penting, untuk memberikan bimbingan komprehensif untuk manajemen dan proses bisnis. Kerangka COBIT dapat dilihat pada gambar 2.2.



Gambar 2.2 Kerangka COBIT (Sumber: (ITGI, 2007))

Kerangka COBIT didasarkan pada prinsip untuk memberikan informasi bahwa perusahaan membutuhkan untuk mencapai tujuannya, perusahaan perlu untuk berinvestasi dalam dan mengelola dan mengendalikan sumber daya TI

menggunakan satu set terstruktur proses untuk memberikan layanan yang memberikan informasi perusahaan yang diperlukan. Mengelola dan mengendalikan informasi adalah inti dari kerangka COBIT dan membantu memastikan keselarasan dengan kebutuhan bisnis (ITGI, 2007).



Gambar 2.3 Dasar COBIT 4.1 (Sumber: (ITGI, 2007))

1. Tujuan COBIT

   Tujuan COBIT:

   a. Diharapkan dapat membantu menemukan berbagai kebutuhan manajemen yangberkaitan dengan TI.

   b. Agar dapat mengoptimalkan investasi TI Menyediakan ukuran atau kriteria ketika terjadi penyelewengan atau penyimpangan. Adapun manfaat jika tujuan tersebut tercapai adalah:

      1) Dapat membantu manajemen dalam pengambilan keputusan.

      2) Dapat mendukung pencapian tujuan bisnis.

      3) Dapat meminimalisasikan adanya tindak kecurangan/fraud yang merugikan perusahaan yang bersangkutan.

2. Landasan COBIT

   a. Menyediakan informasi yang dibutuhkan untuk mencapai sasaran-sasaran

   b. Suatu organisasi harus mengelola sumberdaya TI nya melalui satu kumpulan proses-proses yang dikelompokkan secara alami.

   c. Kelompok-kelompok proses COBIT disusun secara sederhana dan berorientasi pada hirarki bisnis.

   d. Setiap proses merujuk sumberdaya TI, dan persyaratan-persyaratan kualitas, fiduciary/kepercayaan, dan keamanan dari informasi.

3. Kerangka Kerja COBIT

   Karakteristik utama kerangka kerja COBIT menurut adalah sebagai berikut (Riyanarto, 2009).

   a. *Control objectives* terdiri atas 4 tujuan pengendalian tingkat tinggi (*high level control objectives)* yang tercermin dalam 4 *domain*, yaitu: *planning & organization, acquisition & implementation, delivery & support, dan monitoring*.

   b. *Audit guidelines* berisi sebanyak 318 tujuan-tujuan pengendali rinci (*detailed control objectives*) untuk membantu para auditor dalam memberikan *management assurance* atau saran perbaikan.

   c. *Management guidelines* berisi arahan baik secara umum maupun spesifik mengenai apa saja yang mesti dilakukan, seperti : apa saja indikator untuk suatu kinerja yang bagus, apa saja resiko yang timbul, dan lain-lain.

   d. *Maturity models* berfungsi untuk memetakan status *maturity* proses-proses IT (dalam skala 0 – 5).

4. Kaitan audit dengan COBIT yaitu sebagai alat untuk mencari bukti dalam pelaksanaan audit teknologi informasi yang ada dalam suatu organisasi yang disesuaikan dan mengacu pada standar proses teknologi informasi yang didefinisikan dalam COBIT. Bukti audit tersebut digunakan untuk melaksanakan uji kepatutan sehingga didapatkan temuan sebagai kepatutan terhadap standar yang berlaku (Riyanarto, 2009).
5. Makna dari hasil uji kematangan 0-5 berdasarkan COBIT 4.1 yaitu:
   a. Uji kematangan 0: terjadi kekurangan secara keseluruhan pada proses. Manajemen masih belum menyadari bahwa ada masalah yang harus diperhatikan.
   b. Uji kematangan 1: sudah ada bukti bahwa manajemen telah menyadari masalah yang ada dan perlu diperhatikan tetapi masih belum ada proses yang terstandarisasi. Sudah terdapat pendekatan yang disusun dan diterapkan pada setiap individual. Pendekatan keseluruhan pada manajemen masih belum terorganisir.
   c. Uji kematangan 2: proses sudah dikembangkan pada tahap dimana prosedur yang sama telah diikuti oleh orang berbeda yang melakukan tugas yang sama. Masih belum ada pelatihan atau komunikasi pada prosedur secara formal. sudah terjadi ketergantungan yang tinggi pada pengetahuan pada individual tetapi masih sering terjadi kesalahan.
   d. Uji kematangan 3: prosedur telah terstandarisasi, terdokumentasikan, dan dikomunikasikan melalui pelatihan. Sudah ada kewajiban bahwa prosedur tersebut harus diikuti oleh setiap individu pada keseluruhan manajemen. Masih terjadi penyimpangan walau tidak terlalu banyak.

e. Uji kematangan 4: manajemen telah memantau dan mengukur kepatuhan individu dengan prosedur dan mengambil tindakan apabila sebuah prosedur tidak bekerja secara efektif. Proses berada di bawah peningkatan berkelanjutn dan menyediakan pelatihan pada prosedur tersebut. Alat yang terotomatisasi telah digunakan secara terbatas.

f. Uji kematangan 5: proses sudah disempurnakan pada tahap kebiasaan yang baik, berdasarkan hasil pada peningkatan secara berkelanjutan dan uji kematangan dengan manajemen lain. TI telah digunakan secara terintegrasi untuk mengotomatisasi alur kerja, menyediakan laat untuk meningkatkan kualitas dan efektivitas, membuat manajemen beradaptasi dengan cepat.

6. Perbedaan COBIT 4.1 dan COBIT 5 menurut ISACA

COBIT 5 merupakan pengembangan dari COBIT 4.1 yang diperkenalkan pada tahun 2012. Namun, IT M&T PT Pertamina (Persero) MOR V Surabaya masih belum mengadopsi COBIT 5 secara penuh, sehingga di IT M&T masih menggunakan *framework* COBIT 4.1. terdapat beberapa perbedaan antara COBIT 4.1 dan COBIT 5 yang telah dicantumkan di dalam tabel 2.1.

Tabel 2.1 Perbandingan COBIT 4.1 dan COBIT 5

No.	Perbandingan	Cobit 4.1	Cobit 5
1	Prinsip tata kelola perusahaan	Ada 4 prinsip, yaitu *business requirements, IT resources, IT Processes,* dan *Enterprise Information*. (ITGI, 2007)	Ada 5 prinsip yaitu *meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach*, dan *separating governance from management*. (ITGI, 2012)

Lanjutan Tabel 2.1 Perbandingan COBIT 4.1 dan COBIT 5

No.	Perbandingan	Cobit 4.1	Cobit 5
2	*Enabler*	Ada *enabler*, tapi tidak disebutkan secara spsesifik melainkan tersebar diantara proses yang ada pada cobit 4.1 (ITGI, 2007)	*Enabler* pada Cobit 5 (ITGI, 2012): 1) Prinsip, kebijakan dan kerangka kerja adalah kendaraan untuk menerjemahkan perilaku yang diinginkan menjadi panduan praktis untuk sehari-hari manajemen. 2) Proses menggambarkan set terorganisir praktek dan kegiatan untuk mencapai tujuan tertentu dan menghasilkan set output dalam mendukung pencapaian keseluruhan TI-tujuan yang terkait. 3) Struktur organisasi adalah pengambilan keputusan kunci entitas dalam suatu perusahaan. 4) Budaya, etika dan perilaku individu dan perusahaan yang sangat sering diremehkan sebagai faktor keberhasilan dalam kegiatan tata kelola dan manajemen. 5) Informasi diperlukan untuk menjaga organisasi berjalan dengan baik dan diatur, tetapi pada tingkat operasional, informasi sangat sering produk utama dari perusahaan itu sendiri. 6) Layanan, infrastruktur dan aplikasi meliputi infrastruktur, teknologi dan aplikasi yang menyediakan perusahaan dengan pengolahan informasi teknologi dan jasa. 7) Manusia, keterampilan dan kompetensi yang diperlukan untuk berhasil menyelesaikan semua kegiatan, dan untuk membuat keputusan yang benar dan mengambil tindakan korektif.
3	Pengaturan tata kelola dan manajemen	Tata kelola tidak dipisah dengan manajemen (ITGI, 2007)	Tata kelola dipisah dengan manajemen. Tata kelola pada sebagian besar perusahaan merupakan tanggung jawab dari dewan direksi yang dipimpin oleh pemilik. Manajemen merupakan tanggung jawab semua manajer eksekutif yang dipimpin oleh direktur operasional dalam menjalankan operasional kerja. (ITGI, 2012)

Lanjutan Tabel 2.1 Perbandingan COBIT 4.1 dan COBIT 5

No.	Perbandingan	Cobit 4.1	Cobit 5
4	Model referensi	Model Referensi pada Cobit 4.1 yaitu *Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS),* dan *Monitor and Evaluate (ME)* (ITGI, 2007)	Model referensi cobit 4.1 ditambah model referensi baru yang berdasarkan pada pemisahan tata kelola dengan manajemen yaitu *Evaluate Direct and Monitor (EDM), Align Plan and Organise (APO), Build Acquire and Implement (BAI), Deliver Service and Support (DSS),* dan *Monitor Evaluate and Assess.* (ITGI, 2012)
5	Aktivitas dan praktek	Cobit 4.1 mencakup *control objective, Value IT dan Risk IT* (ITGI, 2007)	Cobit 5 sudah mencakup control objective dari cobit 4.1, *Val IT*, dan *Risk IT* (ITGI, 2012)
6	Tujuan dan pengukuran	Terdapat pada *control objective, Val IT, dan Risk IT* (ITGI, 2007)	Sama dengan Cobit 4.1, tetapi terdapat perbedaan nama yaitu *control objective* menjadi tujuan perusahaan (*enterprise goal*), Val IT menjadi *IT-related goals*, dan Risk IT menjadi tujuan proses (process goal) (ITGI, 2012)
7	Input dan output	Cobit 4.1 hanya mencakup *input* dan *output* di level proses (ITGI, 2007)	Cobit 5 mencakup *input* dan *output* di setiap level praktek manajemen (ITGI, 2012)
8	RACI chart	Menyediakan pemain peran bisnis dan TI yang tidak selengkap COBIT 5 (ITGI, 2007)	COBIT 5 menyediakan pemain peran bisnis dan TI yang umum dengan lebih lengkap, rinci dan jelas dan grafik dari COBIT 4.1 untuk setiap praktek manajemen, memungkinkan definisi yang lebih baik dari tanggung jawab pemain peran atau tingkat keterlibatan ketika merancang dan melaksanakan proses. (ITGI, 2012)