

BAB II

LANDASAN TEORI

2.1 Tinjauan Pustaka

Bab ini membahas teori-teori terkait IT *governance*, Audit Sistem Informasi, dan COBIT 4.1 sebagai pedoman yang digunakan dalam penilaian kinerja TI di kampus Universitas Internasional Batam.

2.2 IT Governance

2.2.1 Definisi IT Governance

Menurut *IT Governance Institute* (2007): “*IT governance is the responsibility of the Board of Directors and Executive Management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategy and objectives*”. Dijelaskan bahwa *IT governance* merupakan tanggung jawab dari pimpinan puncak eksekutif manajemen dari suatu perusahaan. *IT Governance* merupakan bagian dari pengelolaan perusahaan secara keseluruhan yang terdiri dari kepemimpinan dan struktur organisasi dan proses yang ada untuk memastikan kelanjutan TI organisasi dan pengembangan strategi dan tujuan dari organisasi.

Sedangkan menurut Well dan Ross (2004),: ”*Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT.*”.

Dijelaskan bahwa *IT Governance* adalah *framework* yang spesifik dalam pengambilan keputusan dan akuntabilitas untuk mendukung kebiasaan perusahaan dalam menggunakan TI. Definisi tersebut menitikberatkan bahwa *IT Governance* harus mampu mengarahkan perilaku penggunaan TI sesuai dengan perilaku yang diinginkan atau ditetapkan (perilaku yang sesuai dengan visi misi, nilai-nilai, strategi dan budaya organisasi). Sedangkan definisi menurut Lab *IT Governance* Fasilkom UI: “Wewenang & tanggung jawab dari komisaris, direktur dan manajer TI terkait dengan upaya TI menunjang strategi & tujuan organisasi yang memanfaatkan mekanisme struktural, mekanisme komunikasi dan proses-proses tertentu”.

Sayonto Gondodiyoto (2007) menyatakan bahwa *IT Governance* merupakan salah satu bagian terpenting dari kesuksesan penerapan *good corporate governance*. *IT Governance* memastikan pengukuran efektifitas dan efisiensi peningkatan proses bisnis perusahaan melalui struktur yang terkait dengan TI menuju ke arah tujuan strategis perusahaan. *IT Governance* memadukan best practice proses perencanaan, pengelolaan, penerapan, pelaksanaan dan pengawasan kinerja untuk memastikan bahwa TI benar mendukung pencapaian perusahaan.

Dengan keterpaduan tersebut, diharapkan perusahaan dapat mendayakan informasi yang dimilikinya sehingga dapat mengoptimumkan segala sumber daya dan proses bisnis mereka untuk menjadi lebih kompetitif. Keputusan bisnis yang baik harus didasarkan pada *knowledge* yang berasal dari informasi yang relevan, komprehensif dan

tepat waktu. Dimana informasi tersebut harus memenuhi kriteria: efektif, efisien, kerahasiaan, keterpaduan, ketersediaan, kepatuhan terhadap rencana/ aturan, serta keakuratan informasi yang dihasilkan. Karena kunci utama di dalam mengelola bisnis pada kondisi lingkungan yang berubah pesat, khususnya perkembangan teknologi, adalah bagaimana kita mengelola kontrol.

2.2.2 Area Fokus IT Governance

Terdapat 5 area yang menjadi fokus menurut IT Governance, diantaranya:



Gambar 2.1: Area Fokus IT Governance (IT Governance Institute, 2007)

Keterangan:

- *Strategic Alignment* (Penyelarasan Strategis)

Berfokus pada hubungan bisnis dan IT *Plans*; mendefinisikan, mempertahankan dan memvalidasi proposisi nilai teknologi informasi, dan menyelaraskan IT *operations* dengan operasi perusahaan secara keseluruhan.

- *Value Delivery* (Penyampaian Nilai)

Adalah tentang menjalankan proposisi nilai seluruh siklus *information delivery*, memastikan bahwa informasi yang disampaikan melalui teknologi informasi, memberikan manfaat yang dijanjikan, fokus pada pengoptimalan biaya dan nilai intrinsik TI.

- *Resource Management* (Pengelolaan Sumber Daya)

Adalah tentang mengoptimalkan investasi, dan pengelolaan yang tepat. Sumber daya TI yang penting diantaranya: aplikasi, informasi, infrastruktur dan manusia, serta yang berkaitan dengan optimalisasi pengetahuan dan infrastruktur.

- *Risk Management* (Manajemen Risiko)

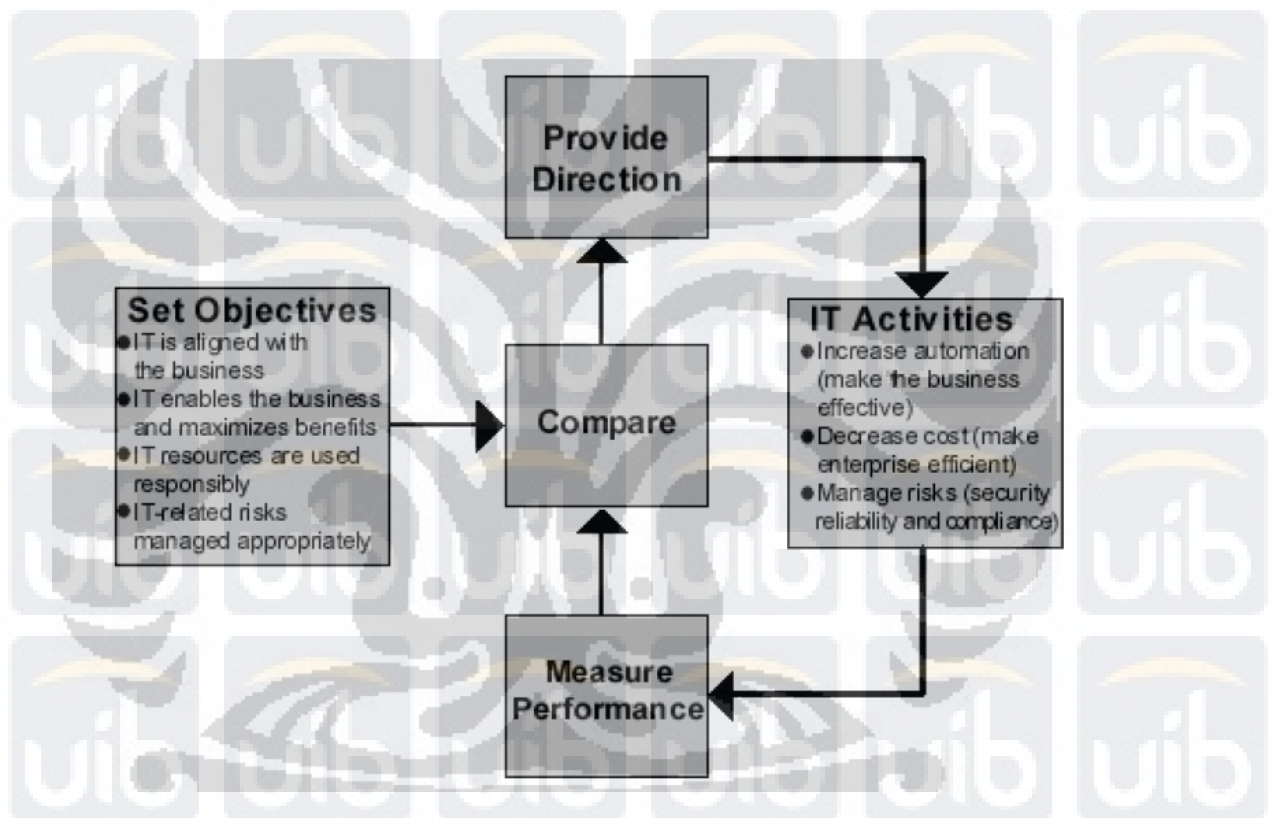
Adanya peringatan risiko oleh senior *corporate officer*, pemahaman yang jelas mengenai *enterprise's appetite for risk*, memahami kepatuhan persyaratan, adanya transparansi tentang risiko yang signifikan di perusahaan.

- *Performance Measurement* (Pengukuran Kinerja)

Meliputi aktivitas audit dan penilaian, serta pengukuran terhadap kinerja secara berkelanjutan.

2.2.3 Proses IT Governance

Proses tata kelola TI dimulai dengan menetapkan tujuan bagi teknologi informasi perusahaan atau dengan kata lain mempersiapkan tujuan awal. Kemudian, dari aktivitas TI yang terjadi: kinerja diukur dan dibandingkan dengan tujuan, sehingga dihasilkan pengalihan aktivitas jika diperlukan atau melakukan perubahan tujuan yang disesuaikan. Tujuan perusahaan yang merupakan tanggung jawab utama dewan direksi dan kinerja perusahaan yang merupakan tanggung jawab pihak manajemen, tentunya menyebabkan mereka harus terus melakukan pengembangan, sehingga tujuan dapat dicapai dan pengukurannya dapat merepresentasikan tujuan yang benar.



Gambar 2.2: Proses IT Governance (IT Governance Institute, 2007)

Dalam menanggapi tujuan yang diterima, fungsi TI perlu fokus pada mencapai keuntungan dengan meningkatkan otomasi dan membuat perusahaan lebih efektif, dan dengan mengurangi biaya agar perusahaan lebih efisien, serta dengan mengelola risiko (keamanan, keandalan dan kepatuhan).

2.2.4 IT Governance dan Corporate Governance

Meningkatnya minat pada tata kelola TI sebagian besar muncul karena adanya prakarsa kepatuhan (seperti Sarbanes-Oxley di Amerika Serikat dan Basel di Eropa)

serta semakin diakuinya kemudahan proyek TI yang dapat berakibat besar terhadap kinerja suatu organisasi. Tujuan penerapan tata kelola TI dapat digunakan untuk menekan biaya operasional TI dengan cara mengoptimalkan operasional TI melalui kendali-kendali yang diterapkan pada setiap proses penggunaan sumber daya TI dan penanganan resiko-resiko yang terkait TI. Sumber Wikipedia (2011) menyebutkan bahwa tata kelola TI (*IT Governance*) adalah suatu cabang dari tata kelola perusahaan yang terfokus pada sistem teknologi informasi (TI) serta manajemen kinerja dan risikonya.

Henderi dan Sunarya Abas (2008) menjelaskan relasi antara tujuan *IT governance*, dengan karakteristik dan tujuan *good governance* untuk memberikan gambaran bentuk dukungan *IT governance* terhadap prinsip dan cara kerja *good governance* dalam tabel sebagai berikut:

No.	Tujuan IT Governance (Henderi, et. All: 2008)	Tujuan dan 8 Karakteristik Utama Good Governance (Anonim, 2007)
1.	Meningkatkan peranan IT terhadap kinerja organisasi dalam mencapai tujuan dan sasarannya	Menciptakan tata kelola atau sistem pengelolaan organisasi (perusahaan, pemerintahan atau organisasi) secara baik

2.	Menyelaraskan investasi IT dan prioritas-prioritas bisnis dengan lebih teliti	Partisipatif. Meningkatkan keterlibatan dan peranan masyarakat, mendengarkan keluhan, dan banyak berinteraksi dengan masyarakat
3.	Mengelola, mengevaluasi, membuat prioritas, membiayai, mengukur dan mengamati permintaan-permintaan pelayanan IT dan hasil kerja dan memenuhinya, dengan lebih konsisten dan berulang sesuai dengan <i>behavior</i> yang dapat mengoptimalkan keuntungan bisnis	<i>Rule of law</i> . Penegakan hukum yang adil bagi semua pihak tanpa pengecualian, menjunjung tinggi HAM dan memperhatikan nilai-nilai yang hidup dalam masyarakat
4.	Mengelola utilisasi pertanggungjawaban sumber daya dan aset	Keterbukaan. Menjamin penyediaan informasi dan kemudahan di dalam memperoleh informasi yang akurat dan memadai sehingga tercipta kepercayaan timbal balik antara pemerintah dan masyarakat
5.	Menjamin penyediaan dan penyelesaian IT sesuai dengan perencanaan, pembiayaan dan	Responsif. Meningkatkan kepekaan para penyelenggara pemerintahan terhadap aspirasi

	tanggung jawab	masyarakat tanpa terkecuali
6.	Membuat, menetapkan dan menjelaskan keadaan yang diminta untuk dipertanggung jawabkan dan diputuskan secara benar (mendefinisikan dan mengotorisasi peraturan secara jelas)	Berorientasi konsensus. Mengambil keputusan berdasarkan kesepakatan dan hasil musyawarah bersama
7.	Mengelola resiko, tantangan dan kemungkinan secara proaktif	Kesetaraan. Memberi peluang yang sama bagi setiap anggota masyarakat untuk meningkatkan kesejahteraannya
8.	Memperbaiki kinerja organisasi IT, memenuhi permohonan, mengembangkan dan mendewasakan staf	Efektif dan efisien. Menjamin terselenggaranya pelayanan kepada masyarakat dengan menggunakan sumber daya yang tersedia secara optimal dan bertanggung jawab
9.	Memperbaiki pelayanan dan mau mendengarkan pelanggan secara keseluruhan	Akuntabilitas. Meningkatkan akuntabilitas para pengambil keputusan dalam segala bidang yang menyangkut kepentingan

	masyarakat luas
--	-----------------

Tabel 2.1: Perbandingan Tujuan IT *Governance* dengan Tujuan dan Karakteristik *Good Governance* (Henderi et.al, 2008)

Berdasarkan tabel di atas, diidentifikasi bahwa ada beberapa tujuan penerapan IT *governance* yang memiliki korelasi yang sangat erat dengan tujuan dan karakteristik *good governance*. Salah satunya terjadi antara tujuan IT *governance* butir 1 dengan butir 1 tujuan *good governance*, butir 5 tujuan IT *governance* dengan butir 4 tujuan dan karakteristik *good governance*, dan tujuan IT *governance* butir 9 dengan butir 8 tujuan dan karakteristik *good governance*.

Sedangkan tujuan *good governance* (tujuan 2) yaitu meningkatkan keterlibatan dan peranan masyarakat, mendengarkan keluhan, dan banyak berinteraksi dengan masyarakat memiliki korelasi terhadap penerapan prinsip dan cara kerja IT *governance* pada berbagai bidang yang berhubungan dengan pelayanan publik, karena melalui penerapan IT *governance*, keterlibatan peran (partisipasi) masyarakat dapat ditingkatkan, para pengambil kebijakan dapat mengetahui keluhan dari masyarakat/ *customer* dengan cara membaca saran dan kritik yang dikirimkannya melalui *e-mail* kepada sistem yang dibangun (mendengarkan keluhan), dan frekwensi interaksi dengan masyarakat juga dapat ditingkatkan dengan menggunakan telewicara atau teleconference publik, sehingga bentuk dukungan ini sejalan dengan tujuan penerapan IT *governance* (tujuan 8)

pada perusahaan atau organisasi, yaitu memperbaiki pelayanan dan mau mendengarkan pelanggan secara keseluruhan.

Selain dapat meningkatkan partisipasi masyarakat, penerapan prinsip dan cara kerja *IT governance* pada sistem pelayanan publik juga mendukung prinsip dan karakteristik *good governance* (tujuan 4) mengenai keterbukaan, karena sistem yang didukung dengan prinsip dan cara kerja *IT governance* dapat menjadi penyedia informasi dan memberi kemudahan dalam memperoleh informasi yang akurat dan memadai, sehingga tercipta kepercayaan timbal-balik antara organisasi dan *customer* (masyarakat), sekaligus mendukung karakteristik *good governance* (tujuan 5) yaitu *responsive*, karena sistem pelayanan publik yang menerapkan prinsip *IT governance* juga dapat berfungsi sebagai *tools* dalam menampung aspirasi masyarakat secara cepat sehingga tindakan lanjutan dapat segera dilakukan.

Menurut Henderi et.al (2008), *IT governance* dapat memberikan *supporting* terhadap penerapan *good governance* pada semua perusahaan dan organisasi (termasuk organisasi pemerintahan) yang menerapkannya. Bentuk dukungan *IT governance* kepada penerapan prinsip dan cara kerja *good governance* diberbagai perusahaan atau organisasi diantaranya dilakukan dalam bentuk penerapan prinsip dan cara kerja *IT governance* pada berbagai bidang yang berhubungan dengan pelayanan publik, sistem pengelolaan aset organisasi dan *customer*, sistem pelayanan dan kegiatan operasional bisnis, dan membangun sistem pengukur pencapaian kinerja dan efisiensi organisasi pada aspek-aspek kritis tertentu.

2.3 Audit Sistem Informasi

Ron Weber (2000) mendefinisikan Audit Sistem Informasi (SI)/TI sebagai proses pengumpulan dan pengevaluasian bukti untuk menentukan apakah sistem informasi dapat melindungi aset, teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efisien.

Sanyoto Gondodiyoto (2007) menjelaskan bahwa pada hakekatnya, audit sistem informasi sebagai audit tersendiri dan bukan merupakan bagian dari audit laporan keuangan, perlu dilakukan untuk memeriksa tingkat kematangan atau kesiapan suatu organisasi dalam melakukan pengelolaan teknologi informasi (*IT governance*). Tingkat kesiapan (*level of maturity*) dapat dilihat dari tata kelola informasi, tingkat kepedulian seluruh *stakeholders* tentang posisi sekarang dan arah yang diinginkan di masa yang akan datang. Sehingga perencanaan teknologi informasi hendaknya dilakukan tidak dengan asal-asalan. Oleh karenanya, audit sistem informasi (berbasis teknologi informasi) ini mencakup 2 hal, yaitu:

1. Audit sistem informasi atau yang dilaksanakan dalam rangka audit laporan keuangan (*general financial audit*), adalah pemeriksaan terhadap aspek-aspek TI pada sistem informasi akuntansi. Panduan yang digunakan adalah Standar Profesional Akuntan Publik (SPAP). *Test of control* dilakukan terhadap program-program komputer dan substantive test dengan pemeriksaan terhadap data/file/database perusahaan. *Audit objectives*-nya ialah kesesuaian dengan

standar akuntansi keuangan dan tidak adanya salah saji yang material pada laporan keuangan. Sedangkan referensi model sistem pengendalian internal lazimnya adalah *Committee of Sponsoring Organization (COSO)*.

2. Audit sistem informasi yang dilakukan dalam kaitannya dengan *IT Governance*, adalah audit operasional terhadap manajemen/ pengelolaan sumber daya informasi atau audit terhadap kehandalan sistem informasi berbasis TI mengenai aspek-aspek: efektivitas, efisiensi, ekonomis tidaknya unit fungsional sistem informasi, data *integrity*, *safeguarding asses*, *reliability*, *confidentiality*, *availability dan security*. Panduan yang digunakan adalah standar atestasi.

Sedangkan model referensi sistem pengendalian internal lazimnya ialah *Control Objective for Information and related Technology (COBIT)*.

Berbeda dengan general audit yang bersifat mandatory, audit TI bersifat memberikan keyakinan kepada *top management* apakah pengelolaan sistem informasi di perusahaan sudah *on the right track* (kecuali ditetapkan berbeda)

Dan besarnya peranan audit dalam tata kelola TI diantaranya untuk pendeteksian terhadap:

1. Komputer yang tidak dikelola secara kurang terarah, tidak ada visi-misi, perencanaan TI, pucuk pimpinan organisasi kurang peduli, tidak ada pelatihan dan pola karier personil yang baik, dan sebagainya.
2. Risiko kehilangan data.

3. Risiko kesalahan dalam pengambilan keputusan akibat informasi hasil proses sistem komputerisasi salah/lambat/ tidak lengkap.
4. Risiko kebocoran data.
5. Penyalahgunaan komputer (*fraud*).
6. Kerugian akibat kesalahan proses perhitungan.
7. Keamanan aset perusahaan karena tingginya nilai investasi hardware dan software.
8. Peningkatan pengendalian penggunaan komputer agar tidak terjadi pemborosan.

2.4 COBIT 4.1

2.4.1. Definisi COBIT

COBIT (*Control Objective for Information and Related Technology*) merupakan *a set of best practices (framework)* bagi pengelolaan teknologi informasi (TI). COBIT disusun oleh *The IT Governance Institute (ITGI)* dan *Information System Audit and Control Association (ISACA)*, tepatnya dulu disebut *Information System Audit and Control Foundation (ISACF)* pada tahun 1992.

Pada tahun 1996 diterbitkanlah COBIT edisi pertama, kemudian edisi kedua dari COBIT diterbitkan pada tahun 1998. Pada tahun 2000 dirilis COBIT 3.0 dan COBIT 4.0 pada tahun 2005. Kemudian terakhir COBIT 4.1 dirilis pada tahun 2007. Dan saat ini sedang dilakukan pengembangan dalam COBIT 5.0 yang akan rilis di tahun 2012. COBIT merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan yang

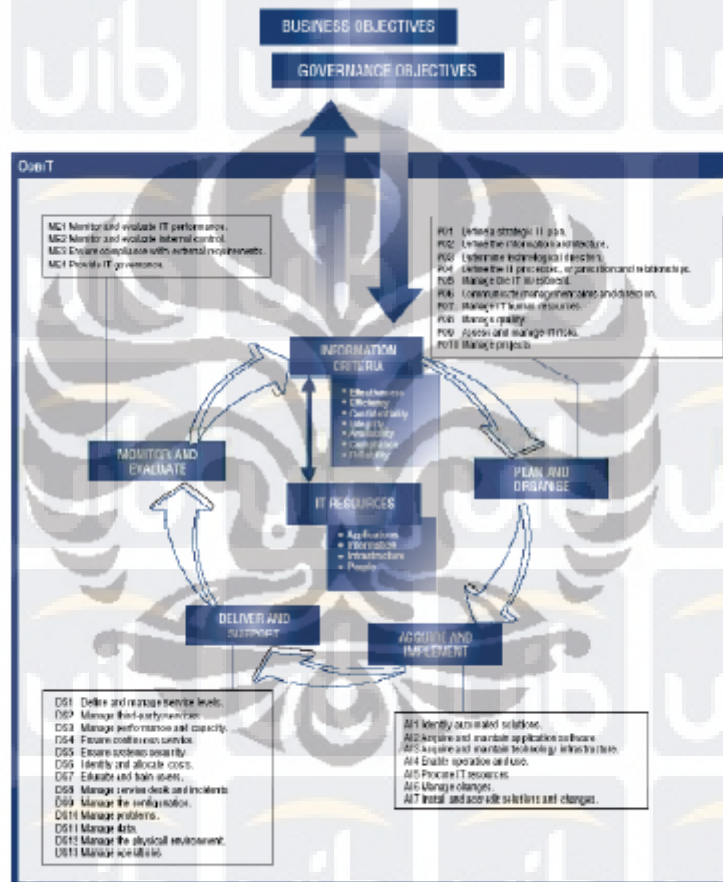
dilengkapi dengan *balance scorecard* dan dapat digunakan sebagai acuan model (seperti COSO) dan disejajarkan dengan standar industri, seperti ITIL, CMM, BS779, ISO9000.

COBIT juga bermanfaat bagi Manajemen untuk membantu mereka menyeimbangkan antara resiko dan investasi pengendalian dalam sebuah lingkungan TI yang sering tidak dapat diprediksi. Bagi user, ia sangat berguna untuk memperoleh keyakinan atas layanan keamanan dan pengendalian TI yang disediakan oleh pihak internal atau pihak ketiga. Sedangkan bagi Auditor untuk mendukung atau memperkuat opini yang dihasilkan dan memberikan saran kepada manajemen atas pengendalian internal yang ada.

Menurut COBIT, keputusan bisnis yang baik harus didasarkan pada *knowledge* yang berasal dari informasi yang relevan, komprehensif dan tepat waktu, yang dapat dihasilkan jika informasi memenuhi 7 kriteria yang akan dibahas pada subbab selanjutnya.

2.4.2. COBIT Framework

Secara keseluruhan, hubungan antara *Business Objectives*, *IT Governance*, *Information*, *IT Resource*, dengan 4 *domain* dan 34 *high level control objectives* dideskripsikan dalam gambar sebagai berikut:



Gambar 2.3: COBIT framework (IT Governance Institute, 2007)

2.4.2.1. Kriteria Informasi COBIT

Demi memenuhi tujuan bisnis, informasi perlu memenuhi kriteria tertentu, 7 kriteria informasi yang menjadi perhatian COBIT adalah sebagai berikut:

Effectiveness (Efektifitas)	Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, konsisten, dapat dipercaya, dan tepat
------------------------------------	--

	waktu.
Efficiency (Efisiensi)	Penyediaan informasi melalui penggunaan sumber daya (yang paling produktif dan ekonomis) yang optimal.
Confidentiality (Kerahasiaan)	Berkaitan dengan proteksi pada informasi penting dari pihak-pihak yang tidak memiliki hak otorisasi/tidak berwenang.
Integrity (Integritas)	Berkaitan dengan keakuratan dan kelengkapan data / informasi dan tingkat validitas yang sesuai dengan ekspektasi dan nilai bisnis.
Availability (Ketersediaan)	Fokus terhadap ketersediaan data/ informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun di masa yang akan datang. Ini juga terkait dengan pengamanan atas sumber daya diperlukan dan terkait.
Compliance (Kepatuhan)	Pemenuhan data/ informasi yang sesuai dengan ketentuan hukum, peraturan,

	dan rencana perjanjian/ kontrak untuk proses bisnis.
Reliability (Handal)	Fokus pada pemberian informasi yang tepat bagi manajemen untuk mengoperasikan perusahaan dan pemenuhan kewajiban mereka untuk membuat laporan keuangan.

Tabel 2.2: Kriteria Informasi COBIT

2.4.2.2. Elemen IT Resources

Elemen-elemen sumber daya TI merupakan hal yang sangat penting didalam pencapaian tujuan bisnis. Karena itu dibutuhkan dukungan sumber daya informasi yang memadai. Fokus terhadap pengelolaan sumber daya teknologi informasi dalam COBIT

4.1 diantaranya:

- *Applications* (Aplikasi)

Merupakan sistem otomatis yang digunakan dan prosedur manual mengenai proses informasi.

- *Information* (Informasi)

Merupakan data, dalam segala bentuk yang melalui tahap input, *processed* dan output / dihasilkan oleh sistem informasi dalam berbagai bentuk yang nantinya akan digunakan oleh perusahaan.

- *Infrastructure* (Infrastruktur)

Merupakan teknologi dan fasilitas (*hardware, operating systems, database management system, networking, multimedia* dan lingkungan pendukung lainnya) yang dapat memproses aplikasi.

- *People* (Manusia)

Personil yang dibutuhkan untuk melakukan perencanaan , mengorganisasikan, memperoleh, mengimplementasikan, menyampaikan, mendukung, mengawasi dan mengevaluasi sistem dan layanan informasi.

2.4.2.3. Komponen *Control Objectives*

Framework COBIT disusun dengan karakteristik yang berfokus pada bisnis (*business-focused*), berorientasi pada proses (*process-oriented*), berbasis pada pengendalian (*controls-based*) dan terarah kepada pengukuran (*measurement-driven*). Pada edisi keempatnya ini, COBIT *framework* terdiri dari 34 *high level control objectives* dan kemudian mengelompokkan proses tersebut menjadi 4 *domain*, keempat

domain tersebut adalah: *Planning and Organization, Acquisition and Implementation, Delivery and Support, dan Monitoring and Evaluation*, yang mencakup:

- *Plan and Organise* (Perencanaan dan Organisasi)

Mencakup strategi, taktik dan identifikasi kontribusi terbaik TI demi pencapaian tujuan kampus. *Domain* ini meliputi pertanyaan-pertanyaan sebagai berikut:

- Apakah proses TI dan strategi bisnis telah sesuai?
- Apakah kampus mencapai penggunaan yang optimum dengan sumber dayanya?
- Apakah setiap karyawan dikampus memahami tujuan TI?
- Apakah resiko TI dipahami dan dikelola?
- Apakah kualitas sistem TI sesuai dengan kebutuhan bisnis?

- *Acquire and Implement* (Pengadaan dan Implementasi)

Untuk merealisasikan strategi TI, perlu dilakukan pengidentifikasian, pengembangan dan perolehan solusi IT, sesuai dengan yang akan diimplementasikan dan diintegrasikan ke dalam proses bisnis. *Domain* ini meliputi pertanyaan-pertanyaan sebagai berikut:

- Apakah proyek baru kemungkinan akan memberikan solusi yang dibutuhkan?
- Apakah proyek baru kemungkinan akan dikirim tepat waktu dan sesuai dengan anggaran?
- Apakah sistem baru dapat bekerja dengan baik ketika diimplementasikan?

- Apakah perubahan dilakukan tanpa mengganggu operasi sistem yang sedang berjalan?

- *Deliver and Support* (Pengiriman Layanan dan Dukungan)

Domain ini fokus terhadap penyampaian jasa yang sesungguhnya diperlukan, termasuk penyediaan layanan, manajemen keamanan dan kontinuitasnya, jasa dukungan kepada user dan manajemen data dan fasilitas operasi. *Domain* ini meliputi pertanyaan-pertanyaan sebagai berikut:

- Apakah jasa TI yang disampaikan sejalan dengan prioritas kuliah?
- Apakah biaya TI teroptimisasi?
- Apakah sistem TI bekerja secara produktif dan aman?
- Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

- *Monitor and Evaluate* (Pengawasan dan Evaluasi)

Berkenaan dengan manajemen kinerja, pemantauan *internal control*, kepatuhan terhadap regulasi dan pelaksanaan tata kelola. *Domain* ini meliputi pertanyaan-pertanyaan sebagai berikut:

- Apakah kinerja TI diukur untuk mendeteksi permasalahan sebelum terlambat?
- Apakah pihak manajemen memastikan bahwa internal control efektif dan efisien?
- Dapatkah kinerja TI dihubungkan dengan tujuan kampus?

- Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

2.4.2.4. *Maturity Model*

Merupakan alat bantu yang dapat digunakan untuk memetakan status *maturity* proses (dalam skala 0-5), diantaranya:

- Skala 0 – *Not Existence*

Kampus tidak menyadari pentingnya membuat perencanaan strategis di bidang teknologi informasi. Dalam skala ini penting untuk dilakukan evaluasi pengendalian dan dijadikan sebagai temuan yang penting.

- Skala 1 – *Initial*

Kampus telah menyadari akan pentingnya pembuatan perencanaan strategis di bidang teknologi informasi . Namun, tidak ada proses yang distandarisasi; perencanaan, perancangan dan manajemen masih belum terorganisir dengan baik. Dalam skala ini keperluan untuk dijadikan temuan tidak diutamakan, karena tingkat kemungkinan terjadinya resiko tidak sebesar skala nol.

- Skala 2 – *Repeatable*

Kampus telah menetapkan prosedur untuk dipatuhi oleh karyawan, namun belum dikomunikasikan dan belum adanya pemberian latihan formal kepada setiap karyawan mengenai prosedur; dan tanggung jawab diberikan sepenuhnya

kepada individu sehingga pemberian kepercayaan sepenuhnya kemungkinan dapat terjadi penyalahgunaan.

- Skala 3 – *Defined*

Seluruh proses telah didokumentasikan dan telah dikomunikasikan, serta dilaksanakan berdasarkan metode pengembangan sistem komputerisasi yang baik, namun belum ada proses evaluasi terhadap sistem tersebut, sehingga masih ada kemungkinan terjadinya penyimpangan.

- Skala 4 – *Managed*

Proses komputerisasi telah dapat dimonitor dan dievaluasi dengan baik, manajemen proyek pengembangan sistem komputerisasi sudah dijalankan dengan lebih terorganisir.

- Skala 5 – *Optimised*

Best Practices (pedoman terbaik) telah diikuti dan diotomatisasi pada sistem berdasarkan proses yang terencana, terorganisir dan menggunakan metodologi yang tepat.