BAB II

LANDASAN TEORI

2.1 *Auditing*

Menurut Arens (2011), *auditing* adalah suatu proses yang terpadu mengenai pengumpulan dan penilaian oleh seorang ahli yang bebas mengenai informasi yang dinyatakan dengan angka dari suatu kesatuan ekonomi tertentu (*specific economc entity*) dengan tujuan untuk menentukan dan melaporkan tingkat kesamaan antara iformasi yang dinyatakan dengan angka dengan ukuran atau kriteria yang ada (*establish criteria*).

Menurut Arens (2011) *Specific economi entity* (suatu kesatuan ekonomi tertentu) adalah batasan – batasan yang dapat memperjelas luasnya tanggung jawab pemeriksa dalam melakukan pemeriksaan. Dalam kebanyakan hal kesatuan ekonomi tertentu merupakan badan hukum seperti perusahaan (PT) atau unit – unit pemerintahan, partnership atau perusahaan perseorangan, akan tetapi didalam beberapa jenis pemerikasaan kesatuan ekonomi tertentu ini diberikan pengertian sebagai suatu bagian, devisi, department, atau individu, dan di dalam kesatuan ekonomi tertentu selalu dikaitkan dengan jangka waktunya (periode).

Menurut Wiley (2014) *Establish criteria* (ukuran / kriteria yang ada) adalah standard yang digunakan oleh auditor dalam menentukan tingkat kepastian dari pada informasi yang diperoleh, apakah cukup layak atau tidak untuk dapat menentukan apakah informasi yang didapatkan sudah memadai atau tidak, misalnya prinsip akuntansi berlaku umum (PABU), kebijaksanaan / peraturan –

peraturan yang dikeluarkan oleh pemerintah dan lain – lain. Jadi standar – standar untuk menilai informasi yang didapatkan dapat berbeda – beda dalam setiap pemeriksaan tergatung kriteria mana yang akan digunakan sesuai dengan maksud dan tujuan pemeriksaan.

2.2 Audit Sistem Informasi

Menurut George H. Bodnar (2009) auditing sistem informasi digunakan umumnya untuk menjelaskan perbedaan dua jenis aktivitas yang terkait dengan komputer. Salah satunya adalah untuk menjelaskan proses mengkaji ulang dan mengevaluasi pengendalian internal dalam sebuah sistem pemrosesan data elektronik. Jenis aktivitas ini umumnya dilakukan oleh para auditor selama menguji kelayakan dan dapat disebut auditing melalui komputer.

"*Information system auditing is generally used to explain the differences between two types of activities related to computers. One of them is to explain the process of reviewing and evaluating internal controls in an electronic data processing system. This type of activity is generally carried out by auditors while testing feasibility and can be called computer auditing*".

Ada beberapa aspek yang diperiksa pada audit sistem informasi yakni audit secara keseluruhan menyangkut efektifitas, efisiensi, *availability system*, *reliability*, *confidentiality*, dan *integrity*, aspek *security*, audit atas proses, modifikasi program, audit atas sumber data, dan data *file*.

Audit sistem informasi sendiri merupakan gabungan dari berbagai macam ilmu, antara lain traditional audit, manajemen sistem informasi, sistem informasi akuntansi, ilmu komputer, dan *behavioral science*.

2.2.1 Tujuan Audit Sistem Informasi

Menurut Agus Mulyanto, (2009) menyatakan tujuan audit sistem informasi adalah untuk meninjau dan mengevaluasi pengendalian internal yang melindungi sistem tersebut. Ketika melakukan audit sistem informasi, seorang auditor harus memastikan tujuan - tujuan ini terpenuhi:

1. Perlengkapan keamanan melindungi perlengkapan komputer, program,komunikasi, dan data dari akses yang tidak sah, modifikasi atau penghancuran.
2. Pengembangan dan perolehan program dilaksanakan sesuai dengan otorisasi khusus dan umum dari pihak manajemen.
3. Modifikasi program dilaksanakan dengan otorisasi dan persetujuan dari pihak manajemen.
4. Pemrosesan transaksi, file laporan dan catatan komputer lainnya telah akurat dan lengkap.
5. Data sumber yang tidak akurat atau yang tidak memiliki otorisasi yang tepat diidentifikasi dan ditangani sesuai dengan kebijakan manajerial yang telahditetapkan. File data komputer telah akurat, lengkap dan dijaga kerahasiaannya.

2.3 Golongan Audit

Menurut Sawyer's (2009) auditor diklasifikasikan dalam dua kategori berdasarkan siapa yang mempekerjakan mereka, yaitu : Auditor eksternal, dan auditor internal

2.3.1 Audit Internal

1. Merupakan karyawan perusahaan, atau bisa saja merupakan entitas independen.
2. Melayani kebutuhan organisasi, meskipun fungsinya harus dikelola perusahaan.
3. Fokus pada kejadian-kejadian dimasa depan dengan mengevaluasi kontrol yang dirancang untuk menyakinkan pencapaian organisasi.
4. Langsung berkaitan dengan pencegahan kecurangan dalam segala bentuknya atau perluasan dalam setiap aktivitas yang ditelaah.
5. Independen terhadap aktivitas yang diaudit, tetapi siap sedia untuk menanggapi kebutuhan dan keinginan dari semua tingkatan manajemen.
6. Menelaah aktivitas secara terus menerus.

2.3.2 Audit External

1. Merupakan orang yang independen diluar perusahaan.
2. Melayani pihak ketiga yang memerlukan informasi keuangan yang dapat diandalkan.
3. Fokus pada ketepatan dan kemudahan pemahaman dari kejadian-kejadian masa lalu yang dinyatakan dalam laporan keuangan.

4. Sekali-sekali memerhatikan pencegahan dan pendeteksian kecurangan secara umum, namun akan memberikan perhatian lebih bila kecurangan terebut akan memengaruhi laporan keuangan secara material.
5. Independen terhadap manajemen dan dewan direksi baik dalam kenyataan maupun secara mental.
6. Menelaah catatan-catatn yang mendukung laporan keuangan secara periodik-biasanya sekali dalam setahun.

walaupun audit internal dan eksternal sama-sama independen dalam menjalankan aktivitas jasanya, namun audit internal tetap merupakan bagian yang integral (tidak dapat dipisahkan) dari struktur organisasi perusahaan yang dimana perannya adalah memberikan pengawasan serta penilaian secara terus menerus. Audit internal dikatakan independen apabila audit internal dapat menjalankan pekerjaannya secara bebas dan objektif.

2.4 *IT Governance* (Tata Kelola TI)

2.4.1 Definisi Tata Kelola TI

Menurut IT Governance Institute (2012) menjelaskan bahwa Tata kelola TI merupakan tanggung jawab dari manajemen eksekutif atau direksi, dan merupakan bagian dari enterprise governance. Tata kelola TI berfokus pada dua hal yaitu bagaimana upaya TI memberikan nilai tambah bagi bisnis dan penanganan risiko ketika sudah dilaksanakan. Pelaksanaan tata kelola teknologi informasi dalam sebuah organisasi, dibangun dengan memberikan nilai tambah yang mungkin akan

bermanfaat bagi stakeholder. Contoh riil yang mungkin bisa diaplikasikan adalah berupa jaminan dalam hal akurasi dan ketepatan waktu laporan manajemen selama proses pengembangan teknologi informasi. Selain itu, pengembangan teknologi informasi harus bisa mengurangi risiko adanya kemungkinan terjadi fraud.

2.4.2 Pentingnya Tata Kelola TI

Menurut Utomo (2011) ata kelola TI atau IT (Information Technology) Governance merupakan struktur hubungan dan proses untuk mengarahkan dan mengendalikan organisasi untuk mencapai tujuannya dengan menambahkan nilai ketika menyeimbangkan risiko dibandingkan dengan TI dan prosesnya untuk memiliki keuntungan kompetetif perusahaan, seseorang harus mampu memanfaatkan Teknologi Informasi untuk membuat peluang dan juga inovasi pada bisnisnya. Teknologi Informasi juga dapat membantu membuat keputusan pada tingkatan manajerial, akan tetapi penerapan Teknologi Informasi membutuhkan biaya yang cukup besar dengan resiko kegagalan yang tidak kecil. Untuk membuat penerapan Teknologi Informasi di dalam perusahaan dapat digunakan secara maksimal, maka dibutuhkan pemahaman yang tepat mengenai konsep dasar dari sistem yang berlaku, teknologi yang dimanfaatkan, aplikasi yang digunakan dan pengelolaan serta pengembangan sistem yang dilakukan pada perusahaan tersebut. COBIT merupakan *a set of best practice* (framework) bagi pengelolan teknologi informasi (*IT management*) yang secara lengkap terdiri dari: *executive summary, framework, control objectives, audit guidelines, implementation tool set* serta *management guidelines* yang sangat berguna untuk proses sistem informasi strategis. *Control Objectives for Information and related Technology* (COBIT)

berguna bagi *IT users* dalam memperoleh keyakinan atas kehandalan sistem aplikasi yang dipergunakan. Sedangkan para manajer memperoleh manfaat dalam keputusan saat menyusun *strategic IT plan, menentukan information architecture*, dan keputusan atas procurement (pengadaan/pembelian) inventaris organisasi.

2.5 Fokus Area Tata Kelola TI

Memberikan 5 fokus area dalam tata kelola TI seperti di bawah ini menurut ITGI (*IT Governance Institute, 2012*):

1. Keselarasan Strategi (*Strategic Alignment*). "*IT Alignment is a journey not a destination*" – menggambarkan bahwa keselarasan strategi TI dengan strategi TI dengan strategi bisnis adalah sebuah proses untuk mencapai tujuan perusahaan. Dalam penerapan tata kelola TI dengan bisnis untuk masa sekarang dan masa yang akan dating saja yang menjadi pokok utama dalam *Stategic Alignment* , tetapi juga kemampuan untuk meningkatkan nilai bisnis yang dapat meningkatkan kinerja perusahaan.
2. Penciptaan Nilai (*Value Delivery*). Menurut ITGI (*IT Governance Institute*, 2006), Layan TI sendiri tidak akan mampu memberikan manfaat secara langsung terhadap bisnis. Manfaat tersebut hanya bisa dihasilkan bila TI (Teknologi Informasi) diimplementasikan bersama-sama dengan peningkatan dalam bisnis, bisnis proses, kompetensi dan prinsip kerja tiap individu dalam perusahaan, serta perubahan-perubahan yang dilakukan didalam perusahaan itu sendiri. Prinsip - prinsip dasar IT value adalah tepat waktu, sesuai anggaran dan dengan manfaat yang dimaksudkan. Oleh

karenanya proses TI harus dirancang, digunakan dan dioperasikan dengan cara yang efisien dan efektif yang memenuhi tujuan dan harapan perusahaan yang ditentukan oleh *business value driver* yang dipengaruhi oleh faktor lingkungan.

3. Manajemen Sumber Daya (*Resource Management*). Pengelolaan sumber daya TI harus dilakukan secara tepat untuk kebutuhan bisnis. Sumber daya TI tersebut meliputi: perangkat lunak, perangkat keras, infrastruktur IT, peningkatan kualitas SDM dalam bidang TI dan hal-hal yang berkaitan dengan pengembangan dalam bidang teknologi.
4. Manajemen Risiko (*Risk Management*). Manajemen resiko menitikberatkan pada hal-hal yang berkenaan dengan pengendalian internal dan hubungan antara perusahaan dengan pelanggan, stakeholder dan shareholder. Segala kemungkinan resiko harus dapat diidentifikasikan sehingga dapat dilakukan langkah-langkah antisipasi untuk mengurangi dampak dari terjadinya resiko tersebut. Untuk melaksanakan pengelolaan terhadap risiko, dibutuhkan kesadaran anggota organisasi dalam memahami adanya risiko, kebutuhan organisasi, dan risiko-risiko signifikan yang dapat terjadi, serta menanamkan tanggung jawab dalam mengelola risiko yang ada di organisasi. Manajemen risiko pada teknologi informasi merupakan hal yang sangat penting. Risiko yang biasa dihadapi pada teknologi informasi antara lain serangan virus yang dapat melumpuhkan kerja teknologi informasi, serangan pihak lain dengan tujuan untuk mengacaukan sistem maupun untuk mencuri data, kesalahan sistem, kerusakan sistem pendukung

misalnya jaringan listrik putus, dan lain-lain. Semua risiko yang mungkin dihadapi tersebut harus diantisipasi sehingga ketika risiko tersebut terjadi tidak menyebabkan kerugian yang fatal.

5. Pengukuran Kinerja (*Performance Measurement*). Pengukuran kinerja akan menjadi tolok ukur keberhasilan penerapan tata kelola teknologi informasi. Hal ini dapat memberikan gambaran apakah hasil kinerja terhadap domain tata kelola TI sudah sesuai dengan tujuan masing-masing. Pada *accountability*, investasi teknologi informasi harus dapat dipertanggung jawabkan. Pertanggungjawaban ini berdasarkan suatu ukuran / kriteria tertentu sehingga investasi tersebut dapat dipertanggungjawabkan. Kriteria tersebut dinilai berdasarkan kinerja yang dihasilkan oleh teknologi informasi terhadap proses bisnis dan tujuan organisasi secara keseluruhan. 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.

2.6 Model Tata Kelola TI

2.6.1 ITIL

Menurut Malone (2010) ITIL dikembangkan oleh *The Office of Government Commerce* (OGC) suatu badan di bawah pemerintah Inggris, dengan bekerja sama dengan *The IT Service* Management Forum (ITSMF) dan *British Standard Institute* (BSI). Itil merupakan suatu framework pengelolaan layanan TI (*IT Service Management* – ITSM) yang sudah diadopsi sebagai standar industri pengembangan industri perangkat lunak di dunia.

ITSM memfokuskan diri pada 3 (tiga) tujuan utama Menurut Malone (2010), yaitu:

A. Menyelaraskan layanan TI dengan kebutuhan sekarang dan akan datang dari bisnis dan pelanggannya.
B. Memperbaiki kualitas layanan-layanan TI.
C. Mengurangi biaya jangka panjang dari pengelolaan layanan-layanan tersebut.

Standar ITIL berfokus kepada pelayanan *customer*, dan sama sekali tidak menyertakan proses penyelarasan strategi perusahaan terhadap strategi TI yang dikembangkan.

2.6.2 ISO/IEC 17799

Menurut Hadiwibowo (2009) ISO/IEC 17799 dikembangkan oleh *The International Organization for Standardization (ISO)* dan *The International Electrotechnical Commission (IEC)* ISO/IEC 17799 bertujuan memperkuat 3 (tiga) element dasar keamanan informasi, yaitu:

A. *Confidentiality* – memastikan bahwa informasi hanya dapat diakses oleh yang berhak.
B. *Integrity* – menjaga akurasi dan selesainya informasi dan metode pemrosesan.
C. *Availability* – memastikan bahwa user yang terotorisasi mendapatkan akses kepada informasi dan aset yang terhubung dengannya ketika memerlukannya.

2.6.3 COSO

Menurut COSO ERM, (2013) COSO merupakan kependekan *dari Committee of Sponsoring Organization of the Treadway Commission*, sebuah organisasi di Amerika yang berdedikasi dalam meningkatkan kualitas pelaporan finansial mencakup etika bisnis, kontrol internal dan *corporate governance*

COSO framework terdiri dari 3 dimensi menurut COSO ERM (2013) yaitu:

A. Komponen Control COSO

COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kontrol internal:

a. *Monitoring*
b. *Information and communication*
c. *Control activities*
d. *Risk assesment*
e. *Control environtment*

B. Sasaran Kontrol Internal

Sasaran kontrol internal dikategorikan menjadi beberapa area sebagai berikut:

a. *Operations – efisisensi dan efektifitas operasi* dalam mencapai sasaran bisnis yang juga meliputi tujuan performansi dan keuntungan.
b. *inancial reporting – persiapan pelaporan* anggaran finansial yang dapat dipercaya.
c. *Compliance – pemenuhan hukum dan aturan* yang dapat dipercaya.

C. Unit / Aktivitas Terhadap Organisasi

Dimensi ini mengidentifikasikan unit/aktifitas pada organisasi yang menghubungkan kontrol internal.

Kontrol internal menyangkut keseluruhan organisasi dan semua bagian-bagiannya. Kontrol internal seharusnya diimplementasikan terhadap unit-unit dan aktifitas organisasi.

2.6.4 COBIT

Menurut Utomo (2011), COBIT *(Control Objective for Information and Related Technology*) adalah *framework* yang dikembangkan oleh *IT Governance Institute,* sebuah organisasi yang melakukan studi tentang model pengelolaan TI yang berbasis di Amerika Serikat

COBIT *Framework terdiri* atas 4 domain utama menurut utomo (2011):

A. *Planning and Organisastion*, Domain ini menitikberatkan pada proses perencanaan dan penyelarasan strategi TI dengan strategi perusahaan.
B. *Acquisition & Implementation*, Domain ini menitikberatkan pada proses pemilihan, pengadaaan dan penerapan teknologi informasi yang digunakan.
C. *Delivery & Support,* Domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya.
D. *Monitoring,* Domain ini menitikberatkan pada proses pengawasan pengelolaan TI pada organisasi.

COBIT mempunyai model kematangan (*maturity models), untuk mengontrol proses-proses TI* dengan menggunakan metode penilaian (*scoring)* sehingga suatu organisasi dapat menilai proses-proses TI yang dimilikinya dari skala *non-existent sampai* dengan *optimised (dari 0 sampai 5).*

COBIT juga mempunyai ukuran – ukuran lainnya sebagai berikut:

A. *Critical Success Factors* (CSF), mendefinisian hal-hal atau kegiatan penting yang dapat digunakan manajemen untuk dapat mengontrol proses-proses TI di organisasinya.

B. *Key Goal Indicators (KGI), Mendefinisikan* ukuran-ukuran yang akan memberikan gambaran kepada manajemen apakah proses-proses TI yang ada telah memenuhi kebutuhan proses bisnis yang ada. KGI biasanya berbentuk kriteria informasi:

   a. Ketersediaan informasi yang diperlukan dalam mendukung kebutuhan bisnis.
   b. Tidak adanya resiko integritas dan kerahasiaan data.
   c. Efisiensi biaya dari proses dan operasi yang dilakukan.
   d. Konfirmasi reliabilitas, efektifitas, dan compliance.

C. *Key Performance Indicators* (KPI), mendefinisikan ukuran-ukuran untuk menentukan kinerja proses-proses TI dilakukan untuk mewujudkan tujuan yang telah ditentukan. KPI biasanya berupa indikator kapabilitas, pelaksanaan, dan kemampuan sumber daya TI.

2.7 *Fishbone Diagram*

Menurut Heizer (2014), *Fishbone diagram* atau juga dikenal sebagai diagram Ishikawa merupakan sebuah diagram sebab-akibat yang diciptakan oleh Kaoru Ishikawa (1968) yang menunjukkan penyebab-penyebab dari *event-event* yang spesifik.

Menurut Heizer (2014), Diagram Ishikawa digunakan dalam perencanaan suatu produk untuk mencegah terjadinya cacat atau penurunan kualitas, dengan mengidentifikasi faktor-faktor penyebab cacat yang potensial yang menyebabkan efek tertentu. Setiap penyebab ketidaksempurnaan merupakan sumber terjadinya variasi. Penyebab-penyebab biasanya dikelompokkan dalam kategori utama untuk mengidentifikasi sumber-sumber variasi tersebut.

Kategori-kategori utama menurut Heizer dan Render (2014) ini biasanya berupa:

A. ***Man-Power*****:** siapapun yang terlibat dalam proses.
B. ***Methode*****:** bagaimana proses berjalan dan beberapa hal yang harus diperhatikan sebelum proses berjalan, seperti *policy*, prosedur, aturan, regulasi dan hukum.
C. ***Machine*** **:** peralatan, *equipment*, komputer, *tools*, yang dibutuhkan untuk melakukan pekerjaan.
D. ***Material*****:** *raw material*, *part*, kertas, pulpen, yang digunakan untuk memproduksi barang jadi.
E. ***Measurements*****:** data yang diambil dari proses yang digunakan untuk mengevaluasi kualitas proses tersebut.
F. ***Environment*****:** kondisi lingkungan seperti lokasi, waktu, temperatur, dan kultur dimana proses beroperasi.

2.8 COBIT 5.0

Menurut Tanuwijaya (2010) COBIT versi 5 atau dikenal dengan nama COBIT 5 adalah edisi terbaru dari Framework COBIT ISACA yang menyediakan penjabaran bisnis secara end-to-end dari tatakelola teknologi informasi perusahaan untuk menggambarkan peran utama dari informasi dan teknologi dalam menciptakan nilai perusahaan.

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

2.9 Prinsip – Prinsip COBIT 5.0

2.9.1 Prinsip COBIT 5.0

Gambar 2.1 Cobit 5.0 *Principle*

Sumber: isaca.org

Berdasarkan gambar 2.1 COBIT 5 didasari oleh 5 prinsip kunci dalam menjalankan *governance* dan *management* suatu IT *enterprise*. Kelima prinsip COBIT 5 tersebut menurut isaca.org yaitu:

1. **Prinsip COBIT 5 Pertama: *Meeting Stakeholder needs***

   COBIT 5 terdiri atas proses-proses dan enabler untuk mendukung penciptaan nilai bisnis melalui penerapan TI. Sebuah perusahaan dapat menyesuaikan COBIT 5 dengan konteks perusahaan tersebut**.**

2. **Prinsip COBIT 5 Kedua: *Convering the Enterprise end-to-end***

   COBIT 5 mengintegrasikan pengelolaan TI perusahaan terhadap tatakelola perusahaan. Hal ini dimungkinkan karena

A. COBIT 5 mencakup seluruh fungsi dan proses yang ada di perusahaan. COBIT 5 tidak hanya fokus pada fungsi TI, tapi menjadi teknologi dan informasi tersebut sebagai aset yang berhubungan dengan aset-aset lain yang dikelola semua orang di dalam sebuah perusahaan.

B. COBIT 5 mempertimbangkan seluruh enabler dari governance dan management terkait IT dalam sudut pandang perusahaan dan *end-to-end.* Artinya COBIT 5 mempertimbangkan seluruh entitas di perusahaan sebagai bagian yang saling mempengaruhi.

3. **Prinsip COBIT 5 Ketiga:** ***Applying a single, integrated framework***

   COBIT 5 selaras dengan standar-standar terkait yang biasanya memberi panduan untuk sebagian dari aktivitas IT. COBIT 5 adalah framework yang membahas *high* level terkait *governance* dan *management* dari IT perusahaan. COBIT 5 menyediakan panduan *high* level dan panduan detailnya disediakan oleh standar-standar terkait lainnya.

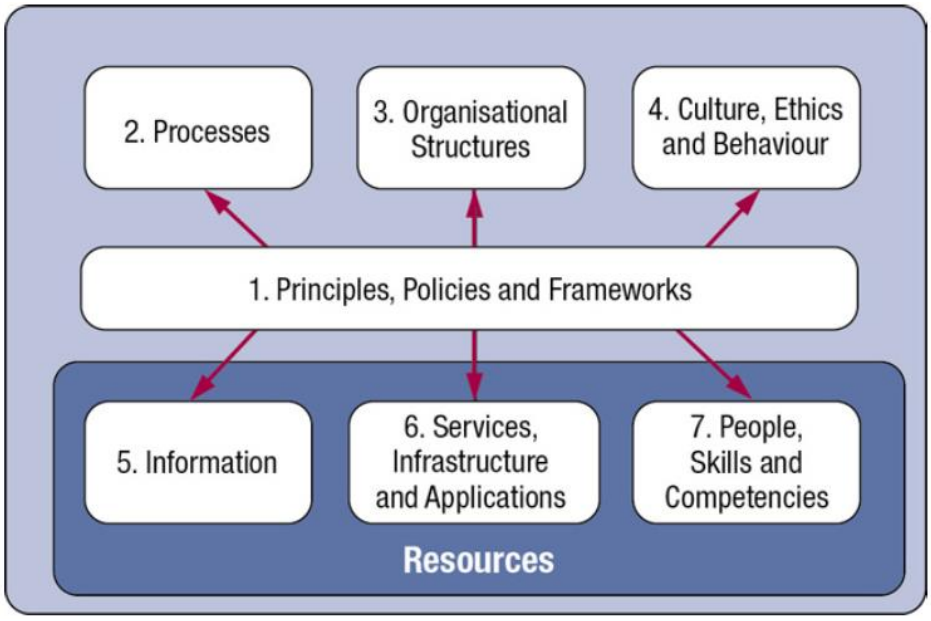
4. **Prinsip COBIT 5 Keempat:** ***Applying a single, integrated framework***

   Governance dan management IT perusahaan yang efektif dan efisien membutuhkan pendekatan yang bersifat menyeluruh, yaitu mempertimbangkan komponen-komponen yang saling berinteraksi. COBIT 5 mendefiniskan sekumpulan enabler untuk mendukung implementasi *governance* dan *management* sistem TI perusahaan secara komprehensif.

5. **Prinsip COBIT 5 Kelima: *Separating governance from management***

COBIT 5 memberikan pemisahan yang jelas antara management dan governance. Kedua hal ini meliputi aktivitas yang berbeda membutuhkan struktur organisasi yang berbeda dan melayani tujuan yang berbeda. Menurut COBIT 5, *governance* memastikan kebutuhan, kondisi dan pilihan dari stakeholder dievaluasi untuk menentukan objektif dari perusahaan yang akan disepakati untuk dicapai. *Governance* memberikan arah bagi penentuan prioritas dan pengambilan keputusan. Selain itu, governance juga me-monitor kinerja dan kesesuaian terhadap objektif yang telah disepakati. Sementara, *management* meliputi aktivitas merencanakan, membangun, menjalankan dan me-monitor aktivitas yang diselaraskan dengan arahan yang ditetapkan oleh organisasi *governance* untuk mencapai objektif dari perusahaan.

2.9.2 COBIT 5.0 *Enablers*



Gambar 2.2 Cobit 5.0 *Enablers*

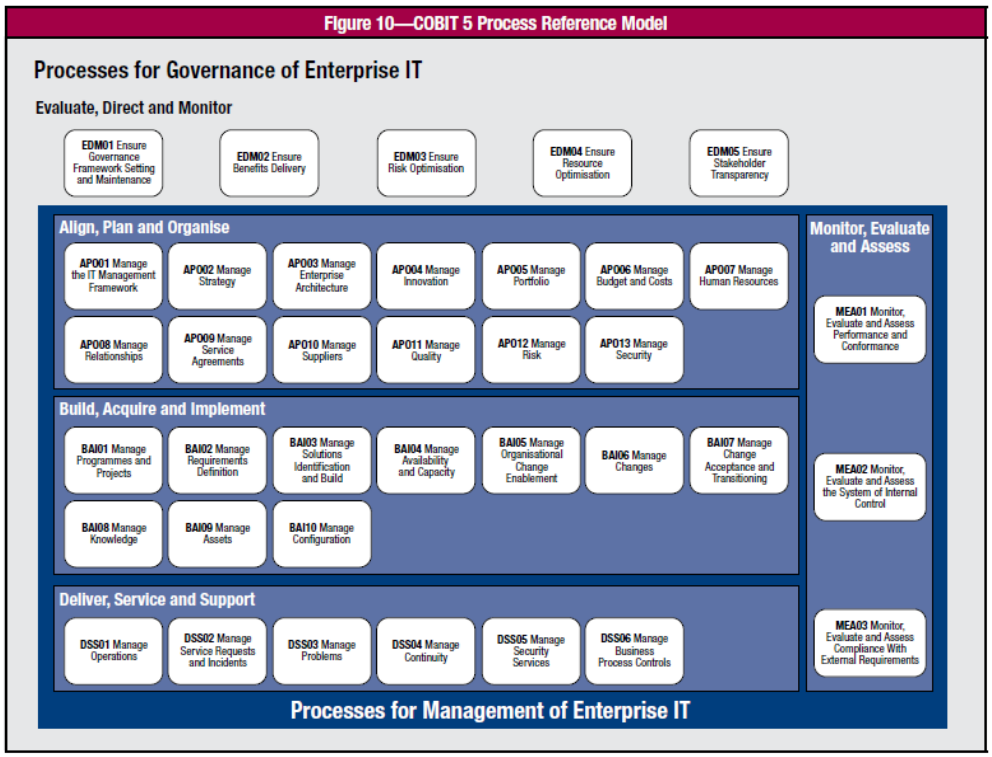
Sumber: ISACA 2014

Selain memiliki 5 prisip, COBIT 5 juga harus memiliki 7 *enablers* seperti pada gambar 2.2 agar bermanfaat untuk semua ukuran perusahaan, baik komersial maupun non-profit ataupun sektor publik. 7 *enablers* tersebut menurut ISACA (2014) yaitu :

1. Prinsip, kebijakan dan *framework*, adalah sarana untuk menterjemahkan tingkah laku yang diinginkan ke dalam petunjuk praktek untuk pelaksanaan manajemen harian.
2. Proses, menjelaskan sejumlah praktek dan aktifitas yang terorganisasi untuk mencapai objektif tertentu dan menghasilkan sejumlah *output* di dalam dukungan pencapaian seluruh tujuan yang terkait IT.

3. Struktur organisasi, merupakan entitas pembuat keputusan kunci di perusahaan.
4. Budaya, etika dan tingkah laku individu dan perusahaan sering dianggap sebagai faktor penghambat kesuksesan dalam aktifitas tata kelola dan manajemen.
5. Informasi, tersebar pada seluruh bagian organisasi dan juga termasuk seluruh informasi yang dihasilkan dan digunakan di perusahaan. Informasi diperlukan untuk menjaga agar organisasi berjalan dan dikelola dengan baik. Tetapi, di tingkat operasional, informasi sering dianggap sebagai hasil dari proses di perusahaan.
6. Layanan, infrastruktur dan aplikasi termasuk infrastuktur, teknologi dan aplikasi yang menyediakan layanan dan proses teknologi informasi bagi perusahaan.
7. Manusia, keahlian dan kompetensi, berhubungan dengan orang dan yang dibutuhkan untuk penyelesaian semua aktifitas yang berhasil dan pembuatan keputusan yang tepat serta mengambil aksi-aksi perbaikan.

2.10 *Process Reference Models* COBIT 5.0



Gambar 2.3 Proses *Reference* Model COBIT 5

Sumber: ISACA 2014

Pada gambar 2.3 terdapat 5 domain dan terdapat 37 proses COBIT 5 diantaranya sebagi berikut menurut ISACA (2014):

1. *Evaluated, Direct, and Monitor* (EDM) proses yang melakukan pengelolaan sasaran kepada stakeholder, nilai pengiriman, optimasi resiko dan sumber daya dan memberikan pengarahan teknologi informasi dan pemonitoran *outcome.* Di dalam domain EDM terbagi kembali ke beberapa domain yaitu:
   a. EDM01 *Ensure governance framework setting and maintenance* (Memastikan kerangka kerja tata kelola pengaturan dan pemeliharaan). Pada proses ini menganalisa syarat – syarat untuk tata kelola teknologi informasi dan mempertahankan struktur, prinsip, proses, dam praktek

yang efektif dengan kejelasan tanggung jawab dan wewenang untuk mencapai visi misi perusahaan.

b. EDM02 *Ensure benefits delivery* (Memastikan penyampaian yang bermanfaat). Pada proses ini mengoptimalkan kontribusi nilai untuk bisnis dari proses bisnis, layanan TI, dan asset TI yang dihasilkan dari investasi yang dibuat oleh TI dengan biaya yang dapat diterima.

c. EDM03 *Ensure risk optimisation* (memastikan optimasi risiko). Memastikan resiko dan toleransi perusahaan dapat dipahami dan dikomunikasikan dengan baik terhadap nilai perusahaan yang terkait dengan penggunaan TI diidentifikasi dan dikelola.

d. EDM04 *Ensure resource optimisation* (memastikan optimasi sumber daya). Memastikan bahwa kemampuan yang terkait TI (manusia, proses, dan teknologi) yang memadai untuk memdukung tujuan perusahaan secara efektif dengan biaya yang optimal.

e. EDM05 *Ensure stakeholder transparency* (memastikan transparansi stakeholder). Memastikan bahwa kinerja TI dalam perusahaan, pengukuran kesesuaian, dan pelaporan transparan dengan pemangku kepentingan dan menyetujui tujuan dan tindakan perbaikan yang diperlukan bagi perusahaan atau organisasi.

2. *Align, Plan, and Organise* (APO) domain ini mencakup strategy, taktik, dan berfokus untuk mengindentifikasi cara terbaik peran teknologi informasi untuk mencapai sasaran bisnis. Untuk merealisasikan visi perusahaan strategi harus direncanakan, dikomunikasikan, dan di kelola.

Pengorganisasian yang benar dan infrastruktur teknologi harus ditempatkan di tempat yang benar. Dan pada domain ini mencakup:

a. APO01 *Manage the IT management framework* (mengelola manajemen kerangka kerja IT). Perjelas dan mempertahankan tata kelola visi dan misi perusahaan serta menerapkan dan memelihara sistem informasi untuk mengelola penggunaan TI untuk mendukung tujuan tata kelola sesuai dengan prinsip dan kebijakan yang ada.
b. APO02 *Manage strategy* (mengelola strategi). Memberikan pandangan menyeluruh tentang lingkungan bisnis dan TI saat ini untuk ke masa depan yang diinginkan serta mengembangkan blok dan komponen arsitektur perusahaan, termasuk layanan yang disediakan secara eksternal dan kemampuan terkait untuk memungkinkan tanggapan yang cepat, handal, dan efisien terhadap tujuan strategis.
c. APO03 *Manage enterprise* architecture (mengelola arsitektur perusahaan). Pada proses ini menetapkan arsitektur umum yang terdiri dari lapisan proses bisnis, informasi, data, aplikasi, dan teknologi secara efektif dan efisien.
d. APO04 *Manage innovation* (mengelola inovasi). Menganalisis peluang untuk inovasi atau peningkatan bisnis yang dapat diciptakan oleh teknologi, layanan, atau inovasi bisnis yang berbasis TI.
e. APO05 *Manage portfolio* (mengelola portofolio). Mengevaluasi, memprioritaskan dan menyeimbangkan program dan layanan, mengelola permintaan dalam sumber daya dan kendala pendanaan,

berdasarkan keselarasan mereka dengan tujuan strategis, nilai perusahaan dan risiko.

f. APO06 *Manage budget and costs* (mengelola anggaran dan biaya). Berkonsultasi dengan para pemangku kepentingan untuk mengidentifikasi dan mengendalikan total biaya dan manfaat dalam konteks rencana strategis dan taktis TI, dan memulai tindakan korektif jika diperlukan.

g. APO07 *Manage human resources* (mengelola sumber daya manusia). Menyediakan pendekatan terstruktur untuk memastikan penataan, penempatan, hak keputusan, dan keterampilan sumber daya manusia yang optimal.

h. APO08 *Manage relationships* (mengelola hubungan). Mengelola hubungan antara bisnis dan TI dengan cara formal dan transparan yang memastikan fokus pada pencapaian tujuan bersama.

i. APO09 *Manage service agreements* (mengelola persetujuan service/layanan). Mensejajarkan layanan dan tingkat layanan yang didukung TI dengan kebutuhan dan harapan perusahaan, termasuk identifikasi, spesifikasi, desain, penerbitan, perjanjian, dan pemantauan layanan TI, tingkat layanan, dan indikator kinerja.

j. APO10 *Manage suppliers* (mengelola suppliers). Mengelola layanan terkait TI yang disediakan untuk memenuhi persyaratan perusahaan, manajemen hubungan, manajemen kontrak, dan peninjauan serta pemantauan kinerja untuk keefektifan dan kepatuhan.

k. APO11 *Manage quality* (mengelola kualitas). Menetapkan dan mengkomunikasikan persyaratan kualitas dalam semua proses, prosedur, dan hasil pada organisasi.

l. APO12 *Manage risk* (mengelola risiko). Mengidentifikasi, menilai dan megurangi resiko yang terjadi pada teknologi informasi dalam tingkat toleransi yang ditetapkan oleh manajemen perusahaan.

m. APO13 *Manage security* (mengelola keamanan). Mendefinisikan, operasikan dan memantau suatu sistem untuk manajemen keamanan informasi.

3. *Build, Acquire and Implement* (BAI)

Untuk merealisasi strategi dan solusi teknologi informasi dan dapat diimplementasikan dan diintegrasikan pada proses bisnis. Perbaikan atau *maintenance* dari sistem yang ada pada domain ini untuk memastikan solusi sesuai dengan tujuan bisnis.

a. BAI01 *Manage programmes and projects*. (mengelola program dan proyek). Menjelaskan mengenai pengelolaan program dan project dari portofolio yang sejalan dnegan strategi perusahaan.

b. BAI02 *Manage requirements definition* (mengelola definisi persyaratan). Identifikasi solusi dan analisis persyaratan sebelum pembuatan untuk memastikan bahwa sesuai dengan persyaratan strategis perusahaan yang mencakup proses bisnis, aplikasi, informasi / data, infrastruktur, dan layanan.

c. BAI03 *Manage solutions identification and build* (mengelola identifikasi solusi dan pembangunan). Membangun dan memelihara solusi yang teridentifikasi sesuai dengan persyaratan perusahaan yang meliputi desain, pengembangan, pengadaan / sumber dan bermitra dengan vendor.

d. BAI04 *Manage availability and capacity* (mengelola ketersediaan dan kapasitas). Menyeimbangkan kebutuhan saat ini dan masa depan untuk ketersediaan, kinerja, dan kapasitas dengan penyediaan layanan dengan biaya yang efektif.

e. BAI05 *Manage organisational change enablement* (mengelola pemberdayaan perubahan organisasi). Memaksimalkan kemungkinan berhasil dan menerapkan perubahan organisasi perusahaan yang luas secara berkelanjutan dengan cepat dan dengan risiko berkurang, mencakup siklus hidup lengkap dari perubahan dan semua pemangku kepentingan yang terkena dampak dalam bisnis dan TI.

f. BAI06 *Manage changes* (mengelola perubahan). Mengelola semua perubahan secara terkontrol, termasuk perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi, dan infrastruktur.

g. BAI07 *Manage change acceptance and transitioning* (mengelola penerimaan terhadap perubahan dan transisi). Menerima dan membuat solusi baru operasional, termasuk perencanaan implementasi, konversi sistem, konversi data, pengujian penerimaan, komunikasi, persiapan

rilis, promosi untuk produksi proses bisnis baru atau diubah dan layanan TI, dukungan produksi awal, dan tinjauan pasca-implementasi.

h. BAI08 *Manage knowledge* (mengelola pengetahuan). Mempertahankan ketersediaan pengetahuan yang relevan, terkini, divalidasi dan dapat diandalkan untuk mendukung semua kegiatan proses dan untuk memfasilitasi pengambilan keputusan.

i. BAI09 *Manage assets* (mengelolaasset/modal). Tujuan utama domain ini untuk memastikan bahwa penggunanya memberikan nilai pada biaya yang optimal, sesuai dengan tujuan organisasi.

j. BAI10 *Manage configuration* (mengelola konfigurasi). Mendefinisikan dan mempertahankan deskripsi hubungan antara sumber daya utama dan kemampuan yang dibutuhkan untuk memberikan layanan yang didukung IT, termasuk mengumpulkan informasi konfigurasi, memverifikasi dan mengaudit informasi konfigurasi, dan memperbarui repositori konfigurasi.

4. *Deliver, Service and Support* (DSS)

Domain ini berfokus kepada pengelolaan atas keamanaan dan kontinuitas, layanan bantuan untuk *user* dan manajemen atas data dan fasilitas operasional, dan mencakup:

a. DSS01 *Manage operations* (mengelola operasi). Mengkoordinasikan dan melaksanaan prosedur operasional yang dibutuhkan untuk memberikan pelayanan kepada customer.

b. DSS02 *Manage service requests and incidents* (mengelola permintaan service/layanan dan insiden). Memberikan balasan atau respon yang tepat waktu dan efektif.

c. DSS03 *Manage problems* (mengelola masalah). Pada proses ini melakukan indentifikasi dan klarifikasi masalah sampai ke akar penyebabnya dan memberikan solusi yang tepat untuk mencegah insiden terulang dan memberikan rekomendasi untuk perbaikan.

d. DSS04 *Manage continuity* (mengelola kontinuitas). Membangun dan memelihara rencana bisnis dan teknologi informasi serta menanggapi kejadian dan gangguan sehingga dapat melanjutkan proses operasi bisnis dan menjaga ketersediaan informasi pada organisasi.

e. DSS05 *Manage security service* (mengelola pelayanan keamanan). Menetapkan dan memelihara peran keamanan informasi dan hak akses dan melakukan pemantauan keamanan.

f. DSS06 *Manage business process control* (mengelola pengendalian proses bisnis). Mendefinisikan dan mepertahankan kontrol pada proses bisnis yang tepat untuk memastikan informasi memenuhi syarat atas pengendalian informasi yang relevan.

5. *Monitor, Evaluate and Assess* (MEA)

Memonitor semua proses untuk memastikan pengarahan yang diberikan sudah sesuai dan semua proses teknologi informasi harus diperiksa setiap waktu untuk memastikan kebutuhan kualitas dan ketaatan dengan kebutuhan pengendalian. Dan mencakup:

a. MEA01 *Monitor, evaluate and assess performance and conformance.* (memonitor, mengevaluasi dan mengukur kinerja dan kesesuaian). Mengumpulkan, memvalidasi, dan mengevaluasi proses bisnis sesuai tujuan serta memberikan pelaporan yang sistematis dan tepat waktu.

b. MEA02 *Monitor, evaluate and assess the system of internal control* (memonitor, mengevaluasi dan mengukur sistem dari pengendalian internal). Dilakukan proses pemantauan secara terus menerus dan mengidentifikasi kekurangan kontrol dan efisiensi untuk memulai tindakan perbaikan.

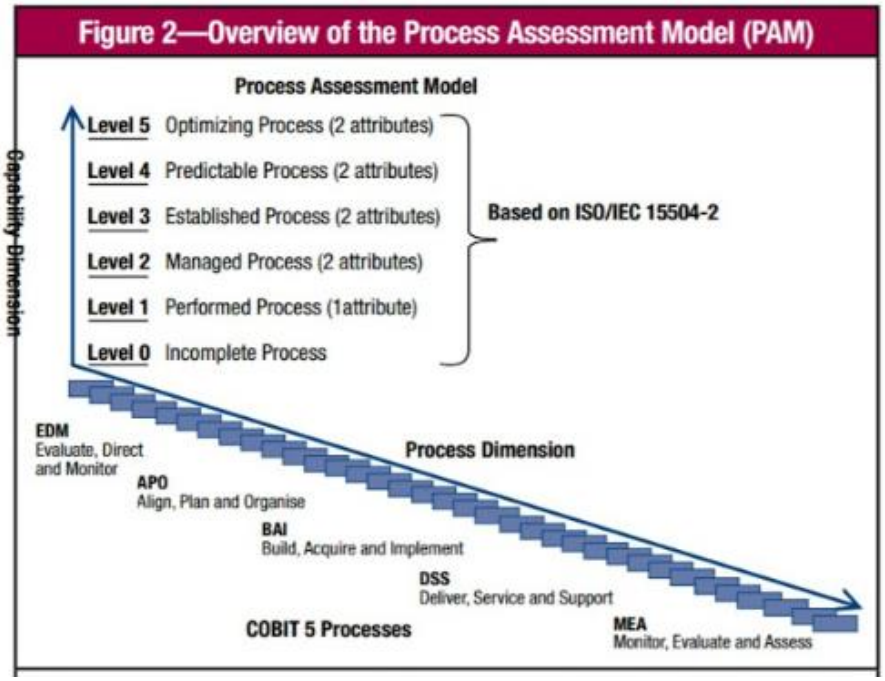
c. MEA03 *Monitor, evaluate and assess compliance with external requirements* (memonitor, mengevaluasi dan mengukur kecocokan dengan kebutuhan eksternal/luar). Proses yang menilai bahwa teknologi informasi dan bisnis sesuai dengan undang – undang, peraturan dan persyaratan kontrak.

2.11 Nilai Kapabilitas

Jika pada COBIT 4.1, menilai *maturity model* dengan menilai sejauh mana penerapan *control objective* dari setiap proses (ditambah Process Control) yang kemudian menggunakan petunjuk *management practices* untuk melakukan penilaiannya.

Maka, pada COBIT 5, setiap level menuntut pemenuhan level sebelumnya dahulu barulah domain bias naik level. Jadi, perlu dinilai dahulu untuk level 1-nya berdasarkan proses *outcome, base practices* dan *work products* setiap proses. Jika

telah memenuhi standar tersebut barulah dipertimbangkan parameter-parameter berikutnya.



Gambar 2.4 *Process Assesment Model* (PAM)

Sumber: iso.org

Gambar 2.4 menampilkan pemetaan kondisi nilai kapabilitas yang ditetapkan *framework* COBIT 5 ke dalam nilai skala 0 sampai 5.

Setiap 37 proses TI pada COBIT 5, mempunyai sebuah nilai kapabilitas yang telah didefinisikan dengan diberikan skala pengukuran bertingkat dari *Incomplete Process* (0) hingga *Optimising Process* (5). Pengembangan tersebut didasarkan pada deskripsi g*eneric* nilai kapabiltas sebagaimana dijelaskan pada Tabel 2.1.

Tabel 2.1 Deskripsi Nilai Kapabilitas

Sumber: ISACA 2014

0 *Incomplete Process*	Mengindikasikan bahwa proses tidak di implementasikan atau gagal untuk mencapai tujuan yang telah direncanakan.
1 *Performed process*	Proses telah diimplementasikan dan mencapai tujuan yang direncanakan.
2 *Managed process*	proses yang telah dijelaskan sebelumnya sekarang diimplementasikan dan dikelola dengan perencanaan, pemonitoran, penyesuaian terhadap produk kerjanya, adanya pengendalian dan pemeliharaan.
3 *Established Process*	mengindikasikan bahwa proses manajemen yang telah dideskripsikan sekarang telah diimplementasikan.
	menggunakan proses yang telah didefinisikan yang mampu mencapai hasil proses yang diinginkan
4 *Predictable process*	proses yang telah diterapkan sebelumnya sekarang beroperasi dalam batas-batas yang ditentukan untuk mencapai hasil prosesnya.
5 *Optimizing Process*	proses yang dijelaskan sebelumnya diprediksikan bahwa akan terus meningkatkan dan memenuhi tujuan bisnis yang relevan dan mencapai tujuan bisnis.

2.12 Metode Pegumpulan Data

Tujuan utama penelitian adalah pengumpulan data, teknik pengumpulan data penelitian dapat dilakukan dengan menurut Sugiyono, (2012) dengan cara:

A. Wawancara (*Interview*)

Wawancara digunakan sebagai teknik pengumpulan data apabila peneliti ingin melakukan studi pendahuluan untuk menemukan masalah yang harus diteliti dan juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam dan jumlah respondenya sedikit/kecil. Wawancara dapat dilakukan secara terstruktur (peneliti telah mengetahui dengan pasti tentang informasi apa yang akan diperoleh) maupun tidak terstruktur (peneliti tidak menggunakan pedoman wawancara yang telah tersusun secara sistematis dan lengkap sebagai pengumpul datanya) dan dapat dilakukan secara langsung (tatap muka) maupun secara tidak langsung (melalui media seperti telepon).

B. Kuesioner

Kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan atau pernyataan tertulis kepada responden untuk dijawabnya. Serta merupakan teknik pengumpulan data yang efisien bila peneliti tahu dengan pasti variabel yang akan diukur dan tahu apa yang diharapkan dari responden. Kuesioner juga cocok digunakan jika jumlah responden cukup besar dan terssebar diwilayah yang luas.

C. Observasi

Observasi merupakan teknik pengumpulan data yang mempunyai ciri yang spesifik bila dibandingkan dengan teknik yang lain yaitu wawancara dan kuesioner. Karena observasi tidak selalu dengan obyek manusia tetapi juga obyek-obyek alam yang lain. Sutrisno Hadi, dalam Sugiyono (2012) mengemukakan bahwa, observasi merupakan suatu proses yang kompleks, suatu proses yang tersusun dari berbagai proses biologis dan psikologis. Dua diantara yang terpenting adalah proses-proses pengamatan dan ingatan.

2.13 Penelitian terdahulu

Penelitian terdahulu dijadikan referensi sebagai pembuatan penelitian yang sedang dilakukan saat ini tentang pengukuran kapabilitas menggunakan kerangka kerja COBIT 5.0.

Penelitian terdahulu yang dijadikan referensi dapat dilihat pada tabel 2.2

Tabel 2.2 Penelitian Terdahulu

Nama	Judul	Jurnal	Hasil
Sepita Sari (2014)	Penerapan Framework COBIT 5 Pada Audit Tata Kelola Teknologi Informasi Di Dinas Komunikasi dan Informatika Kabupaten OKU	Jurnal Teknik Informatika Universitas Bina Darma April 2014	Tingkat model capability yang dicapai yaitu skala 3 (*Established Process*) dengan nilai 3.18
Tri Oktariana (2017)	Tata Kelola Teknologi Informasi Dengan Cobit 5.0	Jurnal Informatika, Volume 3 No.2, Juli-Desember 2017	Hasil dari penelitian ini menggunakan proses EDM04 dengan nilai EDM03, EDM04, APO01, APO02, APO06, APO07, DSS01, DSS03, MEA01

Tabel 2.2 Penelitian Terdahulu (Lanjutan)

			Nilai tertinggi didapat oleh APO07 dengan skor 3.70 dan terendah EDM04 dengan nilai 2.93
Abdul Hakim (2014)	Evaluasi Tata Kelola Teknologi Informasi Dengan *Framework* Cobit 5 Di Kementerian ESDM	Jurnal Sistem Informasi 2/10 (2014), 108-117.	Hasil domain EDM hanya mencapai rata – rata 2 Hasil domain APO mencapai rata – rata 2 Hasil domain BAI mencapai rata – rata 3