BAB II

LANDASAN TEORI

2.1. Pengertian Audit

Menurut Arens dan Loebbecke (2006), *"Auditing is the accumolatuin and evaluation of evidence about information to dtermine and report on the degree of correspondence between the information and establishe criteria. Examining ought to be finished by a skillful autonomous individual"*. Artinya audit adalah proses pengumpulan dan evaluasi terhadap bukti untuk menentukan derajat kesesuaian antara informasi dan kriteria yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan oleh seseorang yang kompeten dan independen. Hal ini berarti dalam pelaksanannya evaluasi dilakukan untuk menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan.

Menurut Sukrisno (2004) audit adalah suatu pemeriksaan yang dilakuakan secara kritis dan sistematis oleh pihak yang independen terhadap laporan keuangan yang telah disusun oleh manajemen berserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut".

Menurut Meisser (2003), *"Auditing is a systematic process with the purpose of evaluating evidence of economic action and occurrence to ensure a level of compliance between assignment and predetermined criteria, the results of the assignment communicated to the interested parties"*. Artinya proses yang

sistematik dengan tujuan mengevaluasi bukti mengenai tindakan dan kejadian ekonomi untuk memastikan tingkat kesesuaian antara penugasan dan kriteria yang telah ditetapkan, hasil dari penugasan tersebut dikomunikasikan kepada pihak pengguna yang berkepentingan.

Berdasarkan definisi dari para ahli diatas, dapat disimpulkan bahwa audit adalah proses sistematis yang dilakukan oleh orang yang kompeten dan independen dengan mengumpulkan dan mengevaluasi bahan bukti dan bertujuan memberikan pendapat mengenai kewajaran laporan keuangan tersebut.

2.2. Pengertian Audit Sistem Informasi

Menurut Gondodiyoto (2003), audit sistem informasi merupakan suatu pengevaluasian untuk mengetahui bagaimana tingkat kesesuaian antara aplikasi sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis, memiliki mekanisme pengamanan aset yang memadai, serta menjamin integritas data yang memadai.

Menurut Mulyadi (2002), audit sistem informasi adalah suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara obyektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian haisl-hasilnya kepada pemakai yang berkepentingan".

Menurut Maniah & Sri Lestari (2008) mengungkapkan bahwa audit sistem informasi adalah proses untuk mengumpulkan dan mengevaluasi bukti dalam menentukan apakah sistem informasi telah dibangun sehingga memelihara integritas data, menjaga aset, membuat sasaran organisasi dapat tercapai secara efektif, dan menggunakan sumber daya yang efisien. Integritas data berhubungan dengan akurasi dan kelengkapan infonnasi demikian pula kesesuaiannya dengan standar. Sistem informasi yang efektif membawa organisasi untuk mencapai objektifnya dan sebuah sistem informasi yang efisien menggunakan sumber daya yang minimum dalam mencapai objektif yang diinginkan.

Berdasarkan definisi dari para ahli, dapat disimpulkan bahwa audit sistem informasi adalah suatu prosedur atau kegiatan untuk memperoleh dan mengevaluasi suatu informasi dan bahan bukti, yang bertujuan untuk memberikan suatu rekomendasi mengenai hasil analisis yang ada untuk mencapai tujuan perusahaan.

2.3. Tujuan Audit Sistem Informasi

Menurut Ron Weber (1999), tujuan audit sistem informasi dapat dibagi menjadi empat, yaitu:

1. Meningkatkan keamanan *asset* perusahaan. *Asset* suatu peusahaan seperti perangkat keras *(hardware)*, perangkat lunak (*software)*, sumber daya manusia, dan *file* data harus mempunyai sistem pengendalian *intern* yang baik agar tidak terjadi penyalahgunaan *asset* perusahaan.
2. Meningkatkan integritas data. Integritas data adalah suatu konsep dasar yang sistem informasi. Data memiliki atribut – atribut tertentu seperti kelengkapan, kebenaran, dan keakuratan. Jika integritas data tidak terpelihara maka suatu perusahaan tidak akan memiliki laporan yang benar bahkan perusahaan dapat menderita kerugian.
3. Meningkatkan efektifitas sistem. Efektifitas sistem informasi perusahaan memiliki peranan dalam pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif apabila suatu sistem sudah sesuai dengan kebutuhan *user.*
4. Meningkatkan efisiensi. Suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya informasi minimal.

2.4. Tahapan Audit Sistem Informasi

Menurut Gallegos (2003), pelaksanaan audit sistem informasi dapat dibagi menjadi empat tahapan, yaitu:

1. Perencanaan *(Planning)*. Pada tahap ini menentukan ruang lingkup, objek yang akan di audit, standar evaluasi dari hasil audit dan komunikasi dengan manajemen pada organisasi yang bersangkutan dengan menganalisa visi, misi, sasaran dan tujuan objek yang diteliti. Aktivitas yang dilakukan saat perencanaan antara lain: penetapan ruang lingkup dan tujuan audit, pengorganisasian tim audit, pemahaman mengenai operasi bisnis klien, kaji ulang hasil audit sebelumnya, dan penyiapan program audit.
2. Pemeriksaan Lapangan (*Field Work*). Pada fase ini dapat dilakukan dengan cara wawancara, kuesioner, ataupun melakukan survei ke lokasi penelitian agar mendapatkan data dengan pihak-pihak yang terkait.
3. Pelaporan (*Reporting*). Pada tahap ini data-data yang diperoleh kemudian dikumpulkan dan dilakukan perhitungan *capability level* yang mengacu pada hasil wawancara, survey, dan rekapitulasi hasil penyebaran kuesioner. Berdasarkan hasil tersebut, kemudian dapat ditentukan seberapa tingkat kapabilitasnya dan kinerja ideal yang diharapkan untuk menjadi acuan selanjutnya.
4. Tindak Lanjut (*Follow Up*). Pada tahap ini auditor wajib memberikan

dokumentasi hasil audit berupa rekomendasi perbaikan yang telah diteliti. Namun selebihnya wewenang perbaikan akan menjadi tanggungjawab manajemen apakah akan diterapkan atau hanya menjadi acuan untuk perbaikan di masa mendatang.

2.5. Standar Audit Sistem Informasi

Berdasarkan *IT Audit and Assurance Standards and Guidelines* ISACA (2013), penerapan audit memiliki standar sebagai kode etik professional bagi para auditor yaitu sebagai berikut:

1. *Audit Charter*
   a. Tujuan, tanggung jawab, otoritas dan akuntabilitas fungsi audit SI pada suatu organisasi/perusahaan ataupun penugasan audit harus dengan dibuat tertulis (didokumentasikan) dalam audit charter atau *engagement letter*.
   b. *Audit charter* atau *engagement letter* harus disetujui dan ditandatangani oleh pemimpin organisasi.

2. *Independence*
    a. Independensi professional.
    b. Dalam segala hal yang berkaitan dengan audit, auditor harus independensi dalam sikap dan penampilan.
    c. Independensi organisasi.
    d. Fungsi audit SI harus bebas (tidak ada *conflict of interest*) dari area yang diperiksa untuk dapat menyelesaikan tugas audit dengan baik.
3. *Professional Ethics and Standards*
    a. Auditor SI harus menganut dan berpegang teguh pada kode etik profesi auditor SI (ISACA) dalam menjalankan tugas auditnya.
    b. Auditor SI harus menjalankan tugasnya secara seksama *(due professional care*) dan bekerja sesuai dengan standar professional audit.
4. *Professional Competence.*
    a. Auditor SI harus mampu secara professional, mempunyai pengetahhuan dan keahlian teknis untuk melakukan penugasan tugas audit.
    b. Auditor SI harus memelihara kemampuan profesionalnya dengan pendidikan dan pelatihan berkelanjutan.

5. *Planning*

    a. Auditor SI harus membuat rencana kerja audit SI, mencakup tujuan audit dan bahwa kegiatan-kegiatan auditnya akan sesuai dengan aturan, hukum, dan standar professional audit yang ada.

    b. Auditor SI harus melakukan teknik pendekatan audit berbasis resiko (risk based audit) dan mendokumentasikanya dengan baik.

    c. Auditor SI harus menyusun rencana kerja audit, mencakup rincian tentang hakekat dan tujuan audit periode atau waktu yang diperlukan dan sumber daya yang diperlukan dan sumber daya yang diperlukan untuk penugasan audit tersebut.

    d. Auditor SI harus menyusun rencana kerja audit dan atau program audit, mencakup prosedur audit yang diperlukan untuk penyelesaian tugas audit itu.

6. *Performance of Audit Work*

    a. Supervise: Staf audit SI harus disupervisi untuk memperoleh keyakinan memadai bahwa tujuan audit telah dicapai sesuai dengan standar professional.

    b. Bukti-audit: Dalam pelaksanaan tugasnya auditor SI harus memperoleh bukti yang cukup, dapat diandalkan dan relevan untuk mencapai tujuan audit. Temuan audit dan kesimpulan harus didukung oleh analisis yang tepat dan interpretasi bukti ini.

c. Dokumentasi: Proses audit harus didokumentasikan, menjelaskan pekerjaan audit yang dilakukan dan bukti audit yang mendukung temuan dan kesimpulan IS auditor.

7. *Reporting*

a. Auditor SI harus membuat laporan hasil audit dalam format yang tepat setelah selesai melakukan tugas auditnya. Laporan hasil audit harus memuat organisasi, pihak yang dituju, dan batasan – batasan sirkulasi.

b. Laporan audit harus menyebutkan ruang lingkup, tujuan, dan periode pelaksanaan pemeriksaan.

c. Laporan audit harus berisi temuan, kesimpulan dan rekomendasi, serta pengungkapan mengenai penyediaan, kualifikasi atau pembatasan cakupan audit yang dialami oleh auditor SI dalam melaksanakan tugasnya.

d. Temuan hasil audit yang dilaporkan harus didukung bukti audit yang cukup, lengkap dan kompeten untuk mendukung laporan hasil pemeriksaan itu.

e. Laporan hasil audit harus ditandatangani, dibubuhi tanggal pelaporan, dan didistribusikan sesuai ketentuan pada audit charter.

8. *Follow Up Activities*

a. Setelah laporan hasil audit yang mengemukakan temuan dan rekomendasi, auditor SI harus mengevaluasi informasi yang relevan untuk memperoleh keyakinan apakah tindak lanjut yang

diperlukan telah dilaksanakan oleh pihak manajemen sesuai jadwal yang diusulkan.

9. *Irregularities and Illegal Acts*
    a. Dalam perencanaan dan pelaksanaan audit untuk mengurangi resiko audit, auditor SI harus mempertimbangkan resiko ketidakteraturan dan *illegal acts*.
    b. Auditor SI harus bersikap profesional skeptis dalam pelaksanaan audit, paham kemungkinan misstatements yang material dapat saja terjadi karena adanya *irregularities* dan *illegal acts*, diluar evaluasi yang telah dilakukan.
    c. Auditor SI harus memahami organisasi dan lingkungannya, termasuk sistem pengendalian internal pada bidang yang diaudit.
10. *IT – Governance*
    a. Auditor SI harus melakukan peninjuan dan penilaian apakah fungsi SI sudah selaras dengan visi, misi, tata-nilai, dan strategis serta tujuan organisasi.
    b. Auditor SI melakukan peninjauan apakah fungsi SI memiliki pernyataan yang jelas mengenai kinerja yang diharapkan oleh organisasi dan nilai apakah hal – hal tersebuat sudah tercapai.
    c. Auditor SI harus meninjau dan menilai efektivitas sumber daya SI dan kinerja proses manajemennya.
11. *Use of Risk Assessment in Audit Planning*

a. Auditor SI harus menggunakan teknik penilaian resiko yang cocok dalam pengembangan rencana kerja audit SI, dan dalam menentukan prioritas alokasi sumberdaya audit yang efektif.
b. Ketika merencanakan peninjauan individual, auditor SI harus mengidentifikasi dan menilai resiko yang relevan dari area yang diperiksanya.

12. *Audit Materiality*
    a. Auditor SI harus mempertimbangkan konsep materialitas dalam hubungannya dengan resiko audit.
    b. Dalam merencanakan audit, auditor SI mempertimbangkan kelemahan – kelemahan potensial atau tidak adanya kontrol internal dan apakah hal itu dapat mempunyai dampak yang siginifikan pada SI.
    c. Auditor SI mempertimbangkan dampak kumulatif dari kelemahan atau ketiadaan pengendalian intern.
    d. Laporan SI harus mengungkapkan adanya pengendalian intern yang tidak efektif atau tidak adanya pengendalian intern.
13. *Using the Work of Other Experts*
    a. Auditor SI harus, jika memungkinkan, menggunakan hasil kerja auditor atau tenaga ahli lain.
    b. Auditor SI harus menilai kualifikasi profesional, kompetensi, pengalaman yang relevan, sumberdaya, independensi, dan proses pengawasan mutu dari ahli sebelum menerima tugas audit.

c. Audior SI harus menentukan dan menyimpulkan apakah hasil kerja tenaga ahli yang lain tersebut sebagai bagian dari audit dan menentukan tingkat penggunaan.

14. *Audit Evidence*
    a. Audior SI harus memiliki bukti audit yang cukup dan layak untuk dapat menarik kesimpulan hasil audit.
    b. Auditor SI harus mengevaluasi komptensi dan kecukupan bukti fisik.
15. *IT Controls.*
    a. Auditor SI harus mengevaluasi dan memonitor pengendalian IT yang merupakan bagian penting dalam lingkungan pengendalian dari perusahaan.
    b. Auditor SI harus membantu manajemen dengan memberikan saran mengenai desain, implementasi, operasi, dan peningkatan dari pengendalian IT.
16. *E-Commerce*. Auditor SI harus mengevaluasi pengendalian yang dapat diterapkan dan pengukuran resiko ketika membahas lingkungan *E-commerce* untuk memastikan transaksi *E-Commerce* sudah terkendali dengan benar.

2.6. Pengertian *IT Governance*

Menurut Standar COBIT dari lembaga ISACA di Amerika Serikat mendefinisikan *IT Governance as a "structure of relationships and processes to direct and control the enterprise in order to achieve the entreprise's goals by*

value while balancing risk versus return over IT and its processes" yang artinya adalah sebuah struktur dari hubungan relasi dan proses untuk mengarahkan dan mengendalikan suatu perusahaan dalam mencapai tujuan dengan memberikan nilai tambah ketika menyeimbangkan resiko dengan menyesuaikan TI dan proses bisnis perusahaan.

Menurut Tarigan (2006) *IT Governance* diartikan sebagai struktur dari hubungan dan prose syang mengarahkan dan mengatur organisasi dalam rangka mencapai tujuannya dengan memberikan nilai tambah dari pemanfaatan teknologi informasi sambil menyeimbangkan risiko dibandingkan dengan hasil yang diberikan oleh teknologi informasi dan prosesnya.

Menurut Weill & Ross (2004) *IT Governance* as a *"specifying the decision rights and accountability framework to encourage desirable behavior in using IT."*

Dari pengertian di atas dapat dilihat bahwa tata kelola teknologi informasi merupakan framework yang spesifik dalam pengambilan keputusan dan akuntabilitas untuk mendukung kebiasaan universitas dalam menggunakan teknologi informasi.

Dari beberapa definisi *IT Governance* dapat disimpulkan bahwa tujuan dibangunnya tata kelola TI adalah pada terciptanya keselarasan strategi organisasi antara teknologi informasi dengan tujuan bisnis yang ingin dicapai oleh suatu organisasi.

2.7. Pengertian COBIT

COBIT (*Control Objective for Information and related Technology)* merupakan sekumpulan dokumentasi dan panduan untuk mengimplementasikan *IT Governance*, kerangka kerja yang membantu auditor, manajemen, dan pengguna (*user*) untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan kontrol, dan permasalahan-permasalahan teknis. COBIT dikembangkan oleh *IT Governance Institute* (ITGI) yang merupakan bagian dari *Information Systems Audit and Control Association* (ISACA).

Menurut Tanuwijaya dan Sarno (2010), COBIT mendukung tata kelola TI dengan menyediakan kerangka kerja untuk mengatur keselarasan TI dengan bisnis. Selain itu, kerangka kerja juga memastikan bahwa TI memungkinkan bisnis, memaksimalkan keuntungan, resiko TI dikelola secara tepat, dan sumber daya TI digunakan secara bertanggung jawab.

Menurut Sasongko (2009), COBIT adalah sekumpulan dokumentasi *best practice* untuk *IT Governance* yang dapat membantu auditor, pengguna *(user)*, dan manajemen untuk menjembatani perbedaan antara risiko bisnis, kebutuhan kontrol, dan masalah-masalah teknis IT.

Dari beberapa definisi COBIT dari para ahli diatas, dapat disimpulkan bahwa COBIT adalah kerangka panduan tata kelola TI dan atau bisa juga disebut sebagai toolset pendukung yang bisa digunakan untuk menjembatani gap antara kebutuhan dan bagaimana teknis pelaksanaan pemenuhan kebutuhan tersebut dalam suatu organisasi.

2.7.1. Pengertian COBIT 4.1

COBIT versi 4.1 adalah model standar pengelolaan IT yang telah mendapatkan pengakuan secara luas, dikembangkan oleh *Information Technology Governance Institute (ITGI) dari Information System Audit and Control Association* (ISACA). Menurut *IT Governance Institute* (2007), menyatakan bahwa pada versi 4.1 ini diuraikan *good practices*, domain-domain dan proses kerangka kerja (*framework*) TI yang ada.

2.7.2. Pengertian COBIT 5.0

Menurut ISACA (2013) COBIT 5 adalah salah satu kerangka bisnis untuk tata kelola dan manajemen perusahaan IT. Versi evolusiner ini menggabungkan pemikiran terbaru dalam tata kelola perusahaan dan teknik manajemen, serta menyediakan prinsip-prinsip, praktek, alat-alat analisis dan model yang diterim secara global untuk membantu meningkatkan kepercayaan, dan nilai dari sistem informasi. COBIT 5 membangun dan memperluas COBIT 4.1 dengan mengintegrasikan kerangka besar lainnya, standar dan sumber daya, termasuk ISACA Val IT dan Risiko TI, *Technology Infrastructure Library* (ITIL®) dan standar yang terkait dari *International Organization for Standardization* (ISO).

COBIT 5 membantu perusahaan menciptakan nilai yang optimal dari TI dengan menjaga keseimbangan antara menyadari manfaatnya dan mengoptimalkan tingkat risiko serta penggunaan sumber daya. Kerangka kerja ini membahas bisnis dan area fungsional IT di suatu perusahaan dan

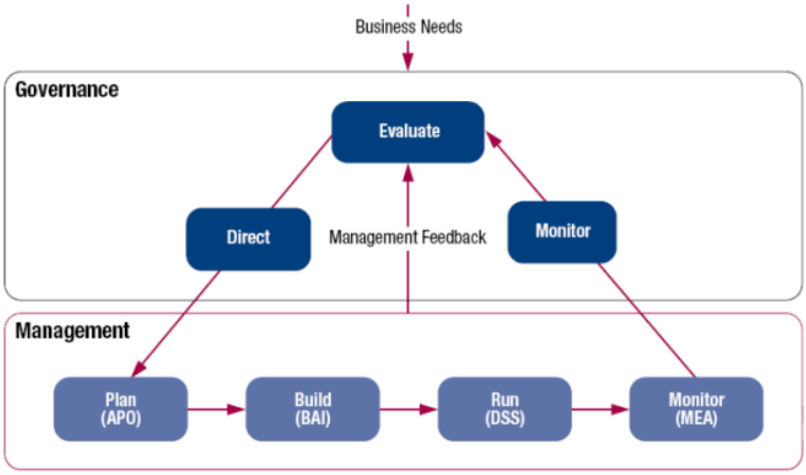
mempertimbangkan kepentingan yang berkaitan dengan IT secara internal dan eksternal bagi para *stakeholder*. Perusahaan dari semua ukuran, baik yang komersial, non-profit atau di sektor publik, bisa mendapatkan keuntungan dari COBIT 5.

Jadi pada dasarnya COBIT 5 adalah sebuah kerangka kerja untuk tata kelola dan manajemen teknologi informasi dan semua yang berhubungan, yang dimulai dari memenuhi kebutuhan stakeholder akan informasi dan teknologi pada suatu organisasi.

2.7.3. Perbedaan COBIT 4.1 dengan COBIT 5.0

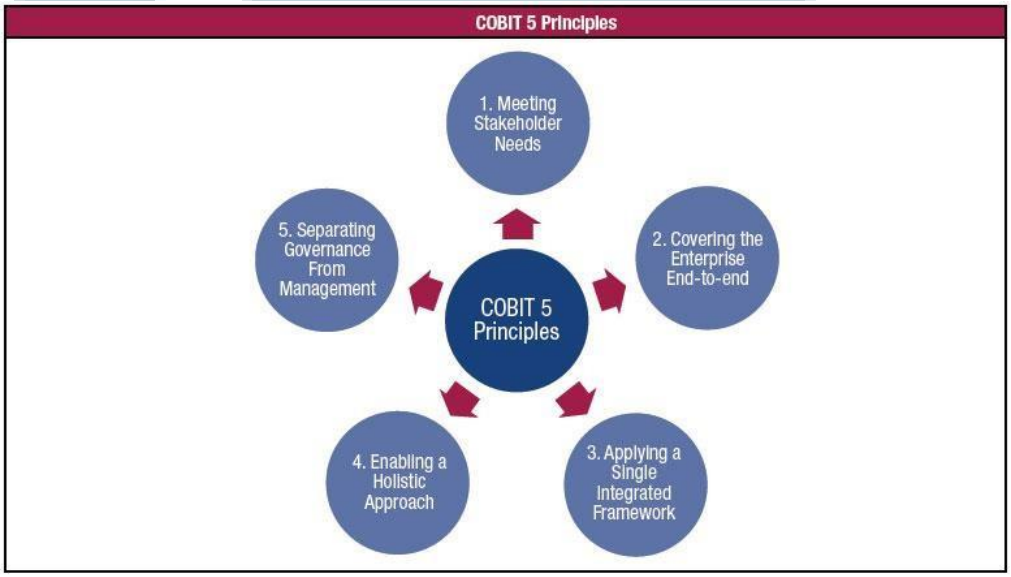
COBIT 4.1 dengan COBIT 5 mempunyai beberapa perbedaan, terutama dalam pembagian domain dan aktivitas proses kerjanya. Pada kerangka kerja COBIT 5, terdapat pemisahaan yang tegas antara tata-kelola dengan manajemen. Tata kelola pada sebagian besar perusahaan merupakan tanggung jawab dari dewan direksi yang dipimpin oleh pemilik, sedangkan pengaturan merupakan tanggung jawab semua manajer eksekutif yang dipimpin oleh direktur operasional dalam menjalankan operasional kerja.

Dengan adanya pemisahan ini di COBIT 5, maka akan memudahkan bagi institusi yang ingin secara jelas memisahkan antara tata kelola dengan proses operasional rutin.



Gambar 2.1 - Pemisahan Tata Kelola dan Manajemen (Sumber: *www.isaca.org/cobit*)

2.7.4. Prinsip-Prinsip COBIT 5.0



Gambar 2.2 - COBIT 5.0 Principle (*Sumber: isaca.org)*

Menurut ISACA (2013), COBIT 5.0 memiliki prinsip dan *enabler* yang bersifat umum dan bermanfaat untuk semua ukuran perusahaan/organisasi,

baik komersial maupun *non-profit* ataupun sektor publik. Lima prinsip tersebut adalah *Meeting stakeholder needs, covering enterprise end-to-end, Applying a single intergrated framework, Enabling a holistic approach* dan *Separating governance from management,* berikut penjelesannya:

Prinsip 1: *Meeting stakeholder needs.*

Perusahaan menciptakan nilai bagi *stakeholder* mereka dengan mempertahankan keseimbangan antara realisasi manfaat dan optimalisasi risiko serta penggunaan sumber daya. COBIT 5.0 menyediakan semua proses yang diperlukan dan *enabler* lain untuk mendukung penciptaan nilai bisnis melalui penggunaan teknologi informasi. Setiap perusahaan memiliki tujuan bisnis yang berbeda, perusahaan dapat menyesuaikan COBIT 5.0 sesuai dengan konteks yang ada melalui *enterprise goals*, menerjemahkan tujuan tertinggi perusahaan dikelola, khususnya *IT related goals* dan pemetaan dalam proses yang spesifik.

Prinsip 2: Covering Enterprise End-to-End

COBIT 5.0 mengintegrasikan tata kelola perusahaan teknologi informasi dalam tata kelola perusahaan, antara lain:

a. Mencakup semua fungsi dan proses dalam perusahaan, COBIT 5.0 tidak hanya fokus pada fungsi teknologi informasi tapi menjadikan teknologi dan informasi tersebut sebagai aset yang berhubungan dengan aset-aset lain yang dikelola semua orang di dalam sebuah perusahaan.

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

Prinsip 3: Applying a single integrated framework.

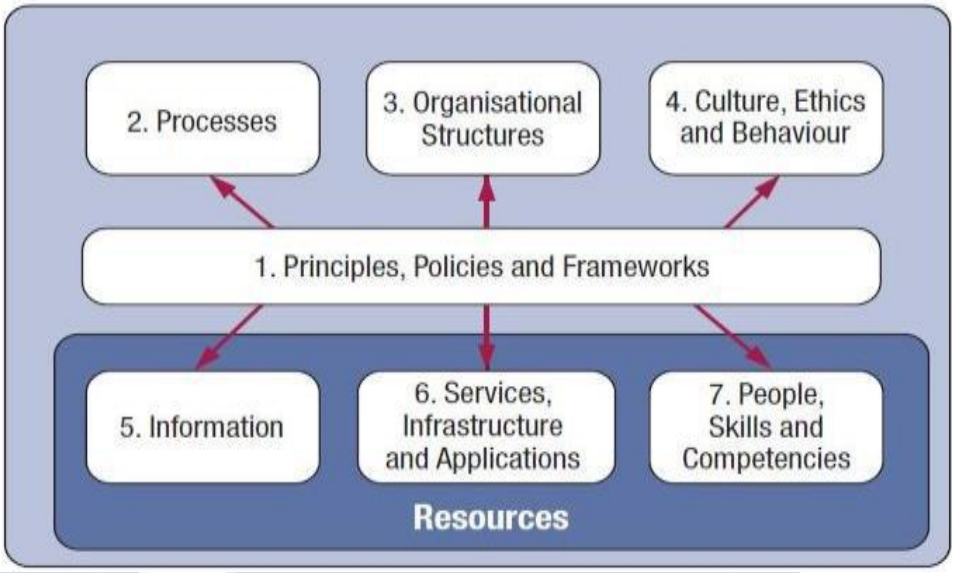
COBIT 5.0 selaras dengan standar-standar terkait yang biasanya memberikan panduan untuk sebagian dari aktivitas teknologi informasi. COBIT 5.0 adalah kerangka kerjayang membahas *high level* dan panduan detailnya disediakan oleh standar-standar terkait lainnya.

Prinsip 4: Enabling a holistic approach.

Governance dan *management* teknologi informasi perusahaan yang efektif dan efisien membutuhkan pendekatan yang bersifat menyeluruh, yaitu mempertimbangkan komponen-komponen yang saling berinteraksi. COBIT 5.0 mendefinisikan sekumpulan *enabler* untuk mendukung implementasi *governance* dan *management* sistem teknologi informasi secara komprehensif. *Enabler* yang didefinisikan secara luas sebagai sesuatu yang dapat membantu untuk mencapai tujuan organisasi/perusahaan. Prinsip untuk COBIT 5.0 menjelaskan tujuh kategori *enabler*:

1. Prinsip, kebijakan dan kerangka kerja.
2. Proses.
3. Struktur organisasi.
4. Budaya, etika dan perilaku.

5. Informasi.
6. Layanan, infrastruktur dan aplikasi meliputi infrastruktur.
7. Manusia, kemampuan dan kompetensi.



Gambar 2.3 - COBIT 5.0 Enterprise Enablers (*Sumber: COBIT 5: figure 12 ISACA, 2012)*

Prinsip 5: Separating governance from management

COBIT 5 memberikan pemisahan yang jelas antara *governance* dan *management*. Kedua hal ini meliputi aktivitas yang berbeda, membutuhkan struktur organisasi yang berbeda dan melayani tujuan yang berbeda. Perbedaan antara *governance* dan *management* adalah:

a. ***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 mengawasi kinerja dan kesesuaian terhadap objektif yang telah disepakati.
b. ***Management*** meliputi aktivitas merencanakan, membangun, menjalankan dan mengawasi aktivitas yang diselaraskan dengan arahan yang ditetapkan oleh organisasi *governance* untuk mencapai objektif dari perusahaan.

2.7.5. *Enabler* COBIT 5.0

Menurut ISACA (2012), *enabler* adalah sekumpulan faktor yang mempengaruhi sesuatu yang akan dikerjakan oleh organisasi. COBIT 5.0 menjelaskan tujuh kategori *enabler*, yaitu:

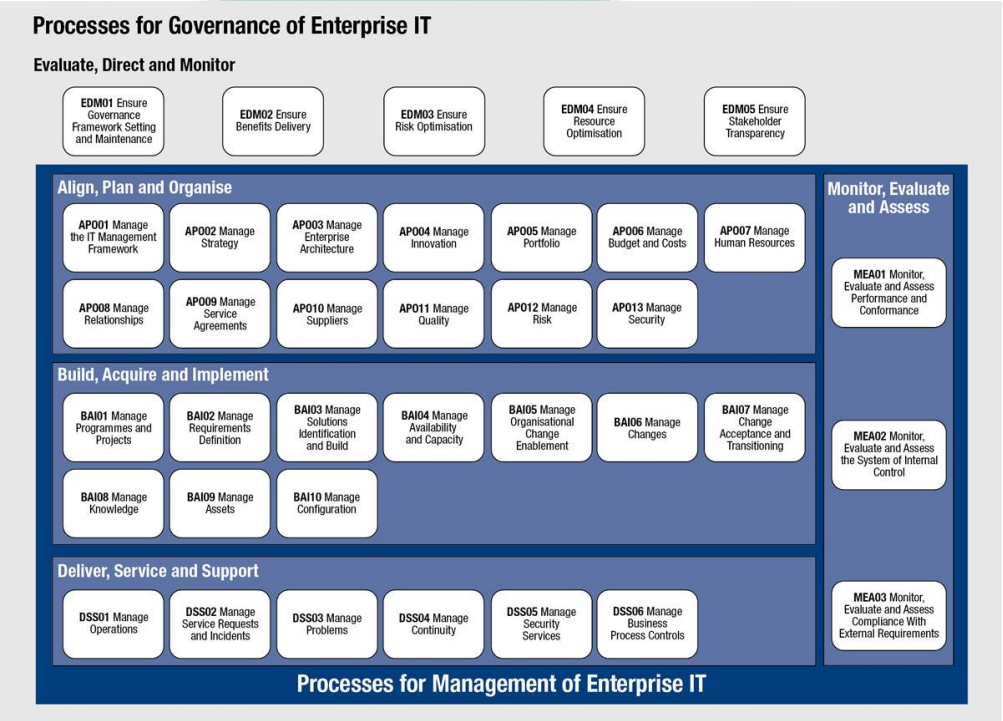
1. Prinsip, kebijakan dan kerangka kerja *(Principles, Policies and Framework)* adalah kendaraan untuk menerjemahkan perilaku yang diinginkan menjadi panduan praktis untuk keseharian manajemen.

2. Proses *(Process)*, menggambarkan praktik dan kegiatan yang terorganisir untuk mencapai tujuan tertentu dan menghasilkan *output* dalam mendukung pencapaian keseluruhan *IT related goals.*
3. Struktur organisasi *(Organizational Structure)* adalah entitas pengambilan keputusan kunci dalam suatu perusahaan.
4. Budaya *(Culture, Ethics and Behaviour),* etika dan perilaku individu dan perusahaan yang sangat sering diremehkan sebagai faktor keberhasilan dalam kegiatan tata kelola dan manajemen.
5. Informasi *(Information)* diperlukan untuk menjaga agar organisasi berjalan dengan baik dan dapat dikelola, tetapi pada tingkat operasional, informasi sering dianggap hasil dari proses perusahaan.
6. Layanan *(Service),* infrastruktur dan aplikasi meliputi infrastruktur, teknologi, dan aplikasi yang menyediakan layanan dan pengolahan informasi teknologi dan jasa.
7. Manusia, keterampilan dan kompetensi *(People, skills and competencies)* yang diperlukan untuk menyelesaikan semua kegiatan dengan berhasil, dan untuk membuat keputusan yang benar serta mengambil tindakan korektif.

2.7.6. Process Reference Model (PRM) COBIT 5.0

Dalam COBIT 5 terdapat suatu model referensi proses yang menentukan dan menjelaskan secara detail mengenai proses tata kelola dan manajemen. Model proses yang diberikan merupakan suatu model yang lengkap dan menyeluruh. COBIT 5 memiliki 2 area aktivitas utama yaitu *Governance*

dan *Management*, proses model referensi COBIT (PRM) terdiri adari 5 domain dan 37 proses yang menggambarkan siklus hidup untuk tata kelola teknologi informasi, seperti yang ditunjukkan pada gambar 2.4.



Gambar 2.4 - COBIT 5.0 Process Reference Model (Sumber: COBIT 5: Enabling Process ISACA, 2012)

COBIT 5 Process reference model terbagi dua aktivitas utama yaitu tata kelola dan manajemen:

a. Tata Kelola (*Governance*), area domain ini mengandung lima proses tata kelola dalam proses *Evaluate, Direct, Monitor* (EDM).

b. Manajemen (*Management*), Area domain ini mengandung empat domain yang selaras dengan area tanggung jawab dari aktivitas *Plan, Build, Run andMonitor* (PBRM).

Area *Governance* memiliki satu domain yaitu EDM (*Evaluate, Direct, Monitor*) dengan lima proses. Sedangkan area *Management* (PBRM) terdiri dari 14 empat domain yaitu APO (*Align, Plan and Organise*), BAI (*Build, Acquire and Implement*), DSS (*Deliver, Service, and Support*) dan MEA (*Monitoring, Evaluate and Assess*) dengan total 37 proses. Setiap proses memiliki beberapa practice atau management process. Berikut rincian 37 proses yang ada pada COBIT 5:

1. *Evaluate, Direct, and Monitor* (EDM)

Proses pengelolaan yang berhubungan dengan pengelolaan sasaran *stakeholder*, nilai pengiriman, optimasi resiko dan sumber daya, termasuk praktek dan aktivitas yang ditujukan pada pengevaluasian pilihan strategi, memberikan pengarahan teknologi informasi dan pemonitoran *outcome*.

a. EDM01 *Ensure governance framework setting and maintenance* (Memastikan kerangka kerja tata kelola pengaturan dan pemeliharaan). Pada proses ini dilakukan analisa terhadap persyaratan untuk tata kelola teknologi informasi di organisasi, prinsip-prinsip, proses dan praktek yang jelas terhadap tanggung jawab dan wewenang untuk mencapai visi, misi, tujuan dan objek organisasi.

b. EDM02 *Ensure benefits delivery* (Memastikan penyampaian yang bermanfaat). Pada proses ini mengoptimalkan kontribusi nilai

bisnis dari proses bisnis, layanan dan *asset* teknologi informasi yang dihasilkan dari investasi yang dilakukan oleh organisasi.

c. EDM03 *Ensure risk optimisation* (memastikan optimasi risiko). Pada proses ini memastikan bahwa risiko yang ada di organisasi dipahami, diartikulasikan dan dikomunikasikan dengan baik. Resiko terhadap nilai organisasi terkait dengan penggunaan teknologi informasi yang diidentifikasi dan dikelola.

d. EDM04 *Ensure resource optimisation* (memastikan optimasi sumber daya). Pada proses ini memastikan bahwa ketersediaan teknologi informasi yang ada memadai dan cukup. Ketersediaan sumber daya tersebut terdiri dari orang *(people),* proses *(process)* dan teknologi *(technology)* untuk mendukung tujuan organisasi secara efektif dengan biaya yang optimal.

e. EDM05 *Ensure stakeholder transparency* (memastikan transparansi *stakeholder*). Pada proses ini memastikan bahwa adanya kesesuaian terhadap pengukuruan kinerja TI organisasi dan adanya pelaporan yang transparan dengan para pemangku kepentingan. Para pemangku kepentingan menyetujui tujuan dan tindakan perbaikan yang diperlukan bagi organisasi.

2. *Align, Plan and Organise* (APO)

Memberi arahan pada solusi *delivery* (BAI) dan *service delivery and support* (DSS). Domain ini mencakup strategi dan taktik, serta berfokus pada pengidentifikasian cara terbaik pengkontribusian teknologi

informasi untuk pencapaian dari sasaran bisnis. Realisasi dari visi strategi harus direncanakan, dikomunikasikan, dan dikelola untuk prespektif yang berbeda. Pengorganisasian yang benar dan infrastruktur teknologi harus ditempatkan di tempat yang benar.

a. APO01 *Manage the IT management framework.* (mengelola manajemen kerangka kerja IT). Pada proses ini memperjelas visi, misi organisasi, dan memelihara tata kelola teknologi informasi. Menerapkan dan memelihara mekanisme untuk mengelola informasi dan penggunaan teknologi informasi di organisasi dalam mendukung tujuan pengelolaan yang sejalan dengan prinsip dan kebijakan yang ada.
b. APO02 *Manage strategy.* (mengelola strategi). Pada proses ini memberikan pandangan yang menyeluruh dari bisnis saat ini dan lingkungan teknologi informasi, arah masa depan dan inisiatif yang diperlukan untuk lingkungan di masa depan.
c. APO03 *Manage enterprise architecture.* (mengelola arsitektur perusahaan). Pada proses ini membangun arsitektur umum yang terdiri dari proses bisnis, informasi, data, aplikasi dan teknologi untuk mewujudkan strategi organisasi dan teknologi informasi yang efektif dan efisien.
d. APO04 *Manage innovation.* (mengelola inovasi). Pada proses ini menjelaskan kesadaran terhadap teknologi informasi dan tren

layanan terkait, mengidentifikasi peluang, inovasi dan merencanakan cara memperoleh keuntungan dari inovasi tersebut.

e. APO05 *Manage portfolio.* (mengelola portofolio). Pada proses ini menjelaskan tentang pengaturan strategi untuk investasi yang sejalan dengan visi, arsitektur dan karakteristik organisasi yang diinginkan dari investasi dan jasa terkait portofolio.

f. APO06 *Manage budget and costs.* (mengelola anggaran dan biaya). Pada proses ini menjelaskan tentang pengelolaan kegiatan keuangan yang berkaitan keuangan yang berkaitan dengan teknologi informasi dalam bisnis dan fungsi teknologi informasi yang meliputi anggaran, biaya, manfaat manajemen dan prioritas pengeluaran.

g. APO07 *Manage human resources.* (mengelola sumber daya manusia). Pada proses ini menjelaskan tentang melakukan pendekatan terstruktur untuk memastikan struktur yang optimal, penempatan, hak keputusan dan keterampilan sumber daya manusia.

h. APO08 *Manage relationships.* (mengelola hubungan). Pada proses ini menjelaskan tentang pengelolaan hubungan antara bisnis dan teknologi informasi secara formal dan transparan yang berfokus pada pencapaian tujuan bersama. Mendasarkan hubungan saling percaya dan terbuka.

i. APO09 *Manage service agreements.* (mengelola persetujuan *service*/layanan). Pada proses ini menjelaskan ketersediaan layanan teknologi informasi dan tingkat layanan dengan kebutuhan pada organisasi termasuk identifikasi, spesifikasi, desain, penerbitan, persetujuan dan pemantauan layanan teknologi informasi, tingkat pelayanan dan indikator kinerja.

j. APO10 *Manage suppliers.* (mengelola *supplier*). Pada proses ini menjelaskan tentang pengelolaan terkait layanan teknologi informasi yang diberikan oleh semua jenis pemasok untuk memenuhi kebutuhan organisasi. Termasuk di dalamnya pemilihan pemasok, pengelolaan hubungan, manajemen kontrak, dan pemantauan kinerja pemasok untuk efektivitas dan kepatuhan.

k. APO11 *Manage quality*. (mengelola kualitas). Pada proses ini menetapkan dan mengkomunikasikan persyaratan kualitas dalam semua proses, prosedur, dan hasil pada organisasi termasuk kontrol, pemantauan, dan penggunaan praktek dan standar dalam perbaikan, efisiensi upaya yang terus menerus.

l. APO12 *Manage risk.* (mengelola risiko). Pada proses ini mengidentifikasi, menilai dan mengurangi resiko teknologi informasi dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif organisasi.

m. APO13 *Manage security* (mengelola keamanan). Pada proses ini menjelaskan tentang proses penentuan, operasi dan *monitor* sistem manajemen keamanan informasi pada organisasi.

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

Memberikan solusi dan menjadikannya pelayanan. Untuk merealisasi strategi teknologi informasi, solusi teknologi informasi harus diidentifikasi, dikembangkan atau didapatkan, begitu pun diimplementasikan dan diintegrasikan pada proses bisnis. Perubahan dan *maintenance* dari sistem yang ada juga di lingkup domain ini, untuk memastikan solusi sesuai dengan tujuan bisnis.

a. BAI01 *Manage programmes and projects.* (mengelola program dan proyek). Pada proses ini menjelaskan tentang pengelolaan program dan proyek dari investasi portofolio yang sejalan dengan strategi organisasi yang terkoordinasi.

b. BAI02 *Manage requirements definition.* (mengelola definisi persyaratan). Pada proses ini mengidentifikasi solusi, menganalisa persyaratan sebelum akuisisi atau pembuatan untuk memastikan kesesuaian dengan persyaratan strategis organisasi yang meliputi proses bisnis, aplikasi, informasi/data, infrastruktur dan layanan.

c. BAI03 *Manage solutions identification and build.* (mengelola identifikasi solusi dan pembangunan). Pada proses ini menetapkan dan memelihara solusi yang diidentifikasi sesuai dengan kebutuhan

organisasi yang meliputi desain, pengembangan, pengadaan/sumber dan bekerja sama dengan pemasok/*vendor*.

d. BAI04 *Manage availability and capacity*. (mengelola ketersediaan dan kapasitas). Pada proses ini mengatur ketersediaan kebutuhan saat ini dan masa depan, kinerja, dan kapasitas dengan penyedia layanan yang hemat biaya.

e. BAI05 *Manage organisational change enablement.* (mengelola pemberdayaan perubahan organisasi). Pada proses ini memaksimalkan kemungkinan keberhasilan dalam penerapan perubahan pada organisasi yang berkelanjutan dengan cepat dan mengurangi risiko.

f. BAI06 *Manage changes*. (mengelola perubahan). Pada proses ini mengelola semua perubahan secara terkontrol termasuk standar perubahan dan prosedur, penilaian dampak, prioritas dan otoritas, pelacakan, pelaporan, perawatan darurat yang berkaitan dengan proses bisnis, aplikasi dan infrastruktur, penutupan dan dokumentasi.

g. BAI07 *Manage change acceptance and transitioning.* (mengelola penerimaan terhadap perubahan dan transisi). Pada proses ini menerima dan membuat solusi operasional yang baru termasuk perencanaan pelaksanaan, sistem dan konversi data, persiapan rilis, promosi untuk produksi proses bisnis baru dan layanan teknologi informasi, dukungan produksi awal dan pasca pelaksanaan.

h. BAI08 *Manage knowledge.* (mengelola pengetahuan). Pada proses ini menjaga ketersediaan pengetahuan yang relevan saat ini, divalidasi, dan dapat diandalkan untuk menunjang kegiatan proses dan memfasilitasi pengambilan keputusan.

i. BAI09 *Manage assets.* (mengelola *asset*/modal). Pada proses ini mengelola *asset* teknologi informasi melalui siklus hidupnya untuk memastikan bahwa penggunanya memberikan nilai pada biaya yang optimal, sesuai dengan tujuan organisasi.

j. BAI10 *Manage configuration.* (mengelola konfigurasi). Pada proses ini mendefinisikan dan memelihara hubungan antara sumber daya dan kemampuan yang diperlukan untuk memberikan ketersediaan layanan teknologi informasi termasuk pengumpulan informasi konfigurasi, menetapkan *baseline*, memverifikasi dan memperbaharui repositori konfigurasi.

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

Domain ini berfokus dengan *actual delivery* and *support of required services*, yang temasuk *service delivery*, pengelolaan atas keamanan dan kontinuitas, layanan bantuan untuk *users*, dan manajemen atas data dan fasilitas operasional.

a. DSS01 *Manage operations* (mengelola operasi). Pada proses ini mengkoordinasikan dan melaksanakan kegiatan dan prosedur operasional yang dibutuhkan untuk memberikan layanan.

b. DSS02 *Manage service requests and incidents.* (mengelola permintaan *service*/layanan dan insiden). Pada proses ini memberikan respon yang tepat waktu dan efektif untuk permintaan pengguna dan resolusi semua jenis kejadian.

c. DSS03 *Manage problems.* (mengelola masalah). Pada proses ini mengidentifikasi dan mengklasifikasikan masalah, akar penyebab masalah dan memberikan solusi perbaikan yang tepat.

d. DSS04 *Manage continuity*. (mengelola kontinuitas). Pada proses ini membangun dan memelihara rencana yang memungkinkan bisnis dan teknologi informasi menanggapi kejadian dan gangguan sehingga dapat melanjutkan proses operasi bisnis penting, menjaga ketersediaan informasi pada organisasi.

e. DSS05 *Manage security services.* (mengelola pelayanan keamanan). Pada proses ini melindungi informasi organisasi untuk mempertahankan tingkat risiko keamanan informasi yang dapat diterima organisasi sesuai dengan kebijakan keamanan.

f. DSS06 *Manage business process controls.* (mengelola pengendalian proses bisnis). Pada proses ini mendefinisikan dan mempertahankan kontrol proses bisnis yang tepat untuk memastikan bahwa informasi memenuhi persyaratan pengendalian informasi yang relevan.

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

Memonitor semua proses untuk memastikan pengarahan yang diberikan ditaati. Semua proses teknologi informasi harus diperiksa secara regular tiap waktu untuk memastikan kebutuhan kualitas dan ketaatan dengan kebutuhan pengendalian. Domain mengajukan manajemen kinerja, monitor dari internal kontrol, ketaaatan dan tata kelola yang regular.

a. MEA01 *Monitor, evaluate and assess performance and conformance.* (memonitor, mengevaluasi dan mengukur kinerja dan kesesuaian). Pada proses ini mengumpulkan, memvalidasi dan mengevaluasi bisnis teknologi informasi dan tujuan. Memantau proses kinerja sesuai dengan tujuan dan memberikan pelaporan yang sistematis dan tepat waktu.

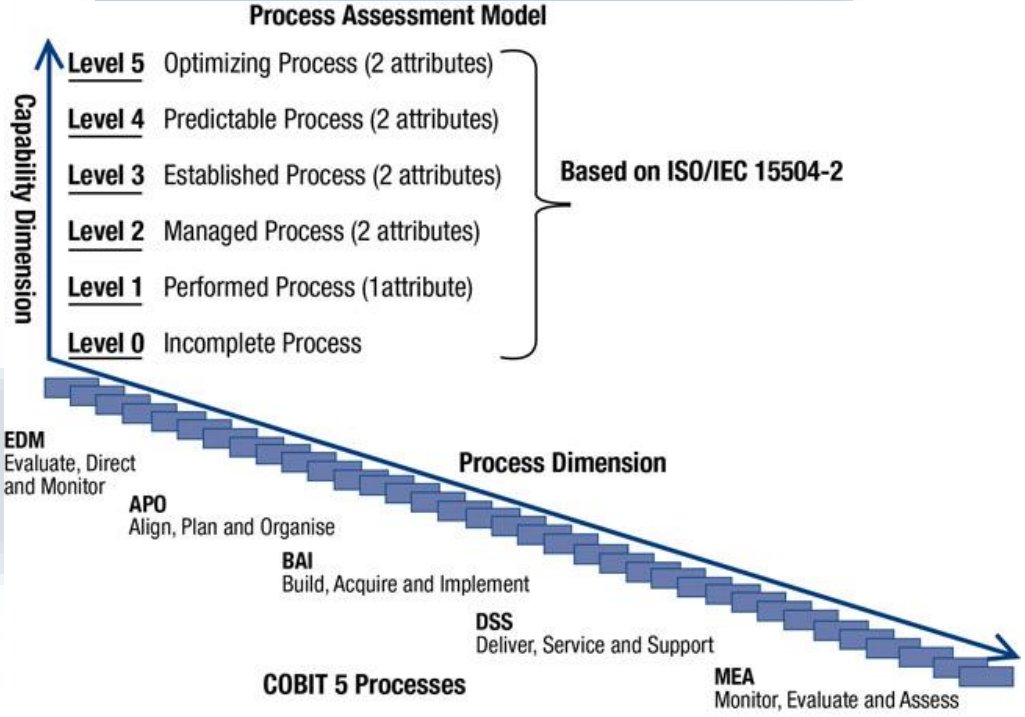
b. MEA02 *Monitor, evaluate and assess the system of internal control*. (memonitor, mengevaluasi dan mengukur sistem dari pengendalian internal). Pada proses ini dilakukan pemantauan secara terus menerus dan evaluasi lingkungan pengendalian untuk mengidentifikasi kekurangan kontrol dan efisiensi untuk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

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

Memperoleh keyakinan bahwa persyaratan telah diidentifikasi dan dipenuhi.

2.8. Capability Process Model

Pada *framework* COBIT 5 tidak lagi menggunakan *Maturity Level* seperti pada COBIT 4.1 sebelumnya. Namun diganti menjadi *Capability Model* yang mengadopsi dari ISO/IEC 15504-2:2003, dimana proses penilaian akan berdasarkan tingkat kemampuan sebuah organisasi dalam melakukan proses-proses yang telah didefinisikan dalam model assessment. Menurut ISACA, *COBIT® Process Assessment Model (PAM): Using COBIT®5*, (2013), adalah kemampuan proses dalam meraih tingkat kapabilitas yang ditentukan oleh atribut proses.



Gambar 2.5 - COBIT 5.0 *Process Assessment Model* (PAM) (Sumber: COBIT 5: Process Assessment Model, 2013.)

Kapabilitas proses dijelaskan dalam atribut proses yang telah dikelompokkan ke dalam *capability level* seperti yang ditunjukkan gambar 2.5. Tujuan dari kapabilitas proses adalah membantu organisasi untuk meningkatkan kapabilitas agar mampu secara konsisten. Atribut proses digunakan untuk menentukan apakah suatu proses telah mencapai kapabilitas tertentu. Berikut ini tingkatan *Capability Model* yang dimiliki sebuah organisasi, antara lain:

a. Level 0 Incomplete process

Proses belum diimplementasikan atau gagal mencapai tujuanya. Dalam level ini hanya ada sedikit atau tidak ada bukti dari pencapaian sistematis dari tujuan proses.

b. Level 1 Performed process (one attribute)

Proses area tersebut sudah menjadi bagian dari sesuatu yang wajib dalam menjalankan kegiatan. Walaupun masih terdapat kekurangan dalam pelaksanaannya baik di sisi kualitas maupun *schedule*. Prinsipnya proses sudah berjalan dan menjadi sesuatu yang wajib sebagai titik awal.

c. Level 2 Managed process (two attributes)

Sebuah proses berada pada level ini, jika proses ini selalu direncanakan, dilakukan, dimonitor dan berjalan pada setiap aktifitas pengembangan. Ini berarti bahwa organisasi selalu menjalankan proses ini di setiap proyek pengembangannya dan terdapat fungsi perencanaan dan kontrol.

d. Level 3 Established process (two attributes)

Proses yang sudah terkelola sekarang diimplementasikan menggunakan proses terdefinisi yang mampu mencapai hasil prosesnya.

e. Level 4 PredicTabel process (two attributes)

Proses yang telah mapan sekarang beroperasi dengan batasan yang terdefinisi untuk mencapai hasil prosesnya.

f. ***Level 5 Optimizing process (two attributes)***

Proses yang terprediksi telah diimprovisasi dengan berkelanjutan untuk mencapai tujuan bisnis perusahaan saat ini.

2.9. Metode Pengumpulan Data

Menurut Darmadi (2013) metode pengumpulan data dalam penelitian adalah suatu cara ilmiah untuk mendapatkan data dengan tujuan kegunaan tertentu. Pada penelitian ini dilakukan pengumpulan data terdiri dari observasi, wawancara, dan kuesioner. Berikut adalah penjelasan para ahli dari metode pengumpulan data:

1. **Observasi**: Menurut Margono (2007), teknik observasi digunakan untuk melihat dan mengamati perubahan fenomena–fenomena social yang tumbuh dan berkembang yang kemudian dapat dilakukan perubahan atas penilaian tersebut, bagi pelaksana observaser untuk melihat obyek pada *moment* tertentu, sehingga mampu memisahkan antara yang diperlukan dengan yang tidak diperlukan.
2. **Wawancara:** Menurut Esterberg dalam Sugiyono (2013), wawancara merupakan pertemuan dua orang untuk bertukar informasi dan ide melalui tanya jawab, sehingga dapat dikontruksikan makna dalam suatu topik tertentu.

3. **Kuesioner:** Menurut Wijaya Kusumah (2011), kuesioner adalah daftar pertanyaan tertulis yang diberikan kepada subjek yang diteliti untuk mengumpulkan informasi yang dibutuhkan peneliti.

2.10. Penelitian Terdahulu

Penelitian yang dilakukan saat ini memiliki kesamaan dengan penelitian terdahulu yang telah dilakukan oleh beberapa orang sebelumnya, karena sudah banyak penelitian yang membahas tentang pengukuran kapabilitas tata kelola teknologi informasi menggunakan *framework* COBIT 5.0. Pada tahapan ini mengambil hasil penelitian dari Rahmat Hidayat (2015), Soni Susanto dan Hari Ginardi (2015), Titus Kristanto, dkk (2014), Sepita Sari, dkk (2014), Christina Juliane, dkk (2014). Penelitian tersebut antara lain:

Tabel 2.1 - Penelitian Terdahulu 0-1

1.	
Nama	Soni Susanto dan Hari Ginardi (2015).
Judul	Perancangan Tata Kelola TI Untuk Pelayanan Publik Pada Dinas Komunikasi Dan Informatika Surabaya Dengan Kerangka Kerja COBIT 5.0.
Metodologi	Menggunakan *framework COBIT 5.0.* Proses Domain: EDM03, EDM04, APO01, APO03, APO04, APO05, APO08, APO09, APO11, APO12, APO13, BAI06, DSS05, BAI01, BAI02, BAI04, BAI05, BAI06, BAI07, BAI08, BAI09, BAI10, DSS01, DSS03, DSS04, DSS05, MEA01, MEA02. Objek: Dinas Komunikasi Dan Informatika Surabaya.

Hasil dan Kesimpulan	Hasil dari audit keamanan sistem informasi pada kantor pemerintah kota yogyakarta Dari hasil penelitian, didapatkan bahwa tingkat kapabilitas proses yang dipilih dalam penelitian ini yaitu EDM03 dan APO12 berada pada tingkat 1 (*Performed*). Untuk EDM04, APO01, APO03, APO04, APO05, APO08, APO09, APO11, APO13, BAI01, BAI05, BAI08, BAI10, DSS05, MEA01 berada tingkat 2 (*Managed*). Sedangkan BAI02, BAI04, BAI06, BAI07, BAI09, DSS01, DSS03, DSS04, MEA02 berada pada tingkat 3 (*Established*).
2.	
Nama	Hidayat (2015)
Judul	Audit Control Capability Level Tata Kelola Sistem Informasi Menggunakan COBIT 5.0 pada Direktorat TIK UPI BANDUNG.
Metodologi	Menggunakan *framework* COBIT 5.0 Proses: pengukuran capability level tata kelola system informasi di *Direktorat TIK UPI BANDUNG* menggunakan COBIT 5.0 dari 10 proses yang terdapat pada domain EDM dan DSS Sistem informasi di *Direktorat TIK UPI Bandung* (Objek) berada pada level 1 (Performend Process) dengan nilai 1,72 yang dilakukan assessment. Proses tersebut terdapat 3 proses (DSS01, DSS04, DSS05) di level 1, (EDM04, EDM05, DSS02, DSS06) 4 proses di level 2 (Managed Process) dan 3 Proses (EDM01, EDM02, DSS03) di level 3 (Established Process).

Hasil dan Kesimpulan	Hasil evaluasi pengukuran capability level tata kelola system informasi di *Direktorat TIK UPI BANDUNG* menggunakan COBIT 5.0 dari 10 (sebelas) proses yang terdapat pada domain EDM dan DSS Sistem informasi di Direktorat TIK UPI Bandung berada pada level 1 (Performend Process) dengan nilai 1,72 yang dilakukan assessment. Proses tersebut terdapat 3 proses (DSS01, DSS04, DSS05) di level 1, 4 (EDM04, EDM05, DSS02, DSS06) proses di level 2 (Managed Process) dan 3 Proses (EDM01, EDM02, DSS03) di level 3 (Established Process). Rekomendasi yang diberikan ada dua yaitu dilakukan sepenuhnya dengan membuat petunjuk SOP yang sesuai dengan COBIT untuk proses yang belom memiliki SOP terutama untuk proses yang saat ini masih berada pada level 0 dan tentunya harus menentukan target untuk naik ke level selanjutnya.
3.	
Nama	Kristanto, dkk (2016).
Judul	Analisis Tingkat Kematangan E-Government Menggunakan Framework Cobit 5 (Studi Kasus: Dinas Perdagangan Dan Perindustrian Kota Surabaya).
Metodologi	Menggunakan *framework* COBIT 5.0 Proses: Domain Proses DSS05 (Mengelola Layanan Keamanan). Tingkat kematangan dari penilaian terhadap 5 responden pada domain DSS05 yaitu 3,05, menunjukkan berada pada posisi Level 3 *(Established Process).* Berarti proses sudah berhasil dijalankan, namun harus diikuti dan disosialisasikan. Domain Proses APO013 (Mengelola Keamanan). Tingkat kematangan dari penilaian terhadap 5 responden

	pada domain APO13 yaitu 3,08, menunjukkan berada pada posisi Level 3 *(Established Process).* Berarti proses sudah berhasil dijalankan, namun harus diikuti dan disosialisasikan. Domain Proses DSS04 (Mengelola Keberlangsungan). Tingkat kematangan dari penilaian terhadap 5 responden pada domain DSS04 yaitu 2,13, menunjukkan berada pada posisi Level 2 *(Managed Process).* Berarti proses sudah mencakup perencanaan, monitor, dan penyesuaian. Domain Proses APO01 (Mengelola Kerangka Kerja Manajemen IT) Tingkat kematangan dari penilaian terhadap 5 responden pada domain APO01 yaitu 2,16, menunjukkan berada pada posisi Level 2 *(Managed Process).* Berarti proses sudah mencakup perencanaan, monitor, dan penyesuaian. Domain Proses MEA01 (Memonitor, mengevaluasi, menilai kinerja, dan kesesuaian). Tingkat kematangan dari penilaian terhadap 5 responden pada domain MEA01 yaitu 3,12, menunjukkan berada pada posisi Level 3 *(Established Process).* Berarti proses sudah berhasil dijalankan, namun harus diikuti dan disosialisasikan.
Hasil dan Kesimpulan	Divisi TI Dinas Perindustrian dan Perdagangan Kota Surabaya. Berdasarkan hasil penelitian dari proses domain, dapat disimpulkan bahwa domain proses DSS05 (mengelola layanan keamanan), APO13 (mengelola keamanan), dan MEA01 (memantau, mengevaluasi, menilai kinerja, dan kesesuaian) mencapai tingkat kematangan Level 3 *(Established Process).* Domain proses *DSS04* (mengelola keberlangsungan) dan APO01 (mengelola kerangka kerja manajemen TI) mencapai tingkat kematangan Level 2 *(Managed Process).*

4.	
Nama	Sari, dkk (2014)
Judul	Penerapan *Framework COBIT 5.0* Pada Pengukuran kapabilitas Tata Kelola Teknologi Informasi di Dinas Komunikasi dan Informatika Kabupaten OKU.
Metodologi	Mengunakan *framework COBIT 5.0.* Objek: Dinas Komunikasi dan Informatika Kabupaten OKU. Proses: Dalam penelitian ini menggunakan model kapabilitas sebagai alat ukur terhadap jawaban responden dari kuesioner yang dibuat berdasarkan *framework cobit* 5. Kuesioner ini berisi tentang pertanyaan-pertanyaan dari domain *Monitor, Evaluate, and Access (MEA),* yaitu: 1. *Monitor, Evaluate, and Access (MEA01): Pengawasan serta evaluasi penilaian kinerja pada proses TI.* 2. *Monitor, Evaluate, and Access (MEA02): Pengawasan, evaluasi dan penilaian sistem pengendalian internal.* 3. *Monitor, Evaluate, and Access (MEA03): Pengawasan, evaluasi dan penilaian sistem pengendalian eksternal.*
Hasil dan Kesimpulan	Hasil dari rekapitulasi tingkat model capability skala penelitian pengukuran kapabilitas tata kelola Teknologi Informasi di Dinas Komunikasi dan Informatika Kabupaten OKU yaitu skala 3 (established process) dengan nilai 3,18, yang artinya Dinas Komunikasi dan Informatika Kabupaten OKU ini sudah mengimplementasikan tata kelola Teknologi

	Informasi dengan menggunakan proses pelatihan yang telah ditentukan dan sudah mencapai target yang diharapkan.
5.	
Nama	Juliane (2014)
Judul	Pengukuran Kinerja Sistem Informasi Kios (SIOS) di PT. Rancek Sukses Bandung Dengan Menggunakan *Framework* COBIT 5.0.
Metodologi	Mengunakan *framework COBIT 5.0* *Proses:* Pengujian kinerja SIOS dilakukan dengan menyebarkan kuesioner dengan pertanyaan seputar domain APO01 – APO13(*Align, Plan, & Organize*).
Hasil dan Kesimpulan	Hasil dari pengukuran kinerja dari SIOS yang didapat dari kuesioner, dipetakan dalam bentuk jaring laba-laba sesuai dengan domain proses APO. Pengukuran SIOS dengan *Framework* COBIT 5.0 di PT. Rancek Sukses/RTC Bandung (Objek) yang telah dilakukan, dapat disimpulkan bahwa SIOS yang telah berjalan sampai pada level 0,30 yang termasuk kisaran level 0 yaitu *Incomplete Process* yang berarti proses yang tidak lengkap, hanya ada sedikit bukti atau bahkan tidak ada bukti adanya pencapaian sistematik dari prosesnya. Hasil penelitian terhadap SIOS dengan menggunakan *framework* COBIT 5.0 dapat disimpulkan bahwa: 1. Nilai *capability process dari* SIOS yang sedang berjalan

	mencapai level 1 dengan 4 proses yaitu APO04, APO08, APO12, APO13 yang berada pada level *Performed Process*, hal ini mengindikasikan bahwa sistem informasi yang sekarang sedang berjalan belum sempurna. 2. Hasil wawancara dan diskusi dengan staf yang berwenang diperoleh kesimpulan bahwa aktivitas SIOS selama ini belum memperhatikan faktor resiko dan pengendalian secara terstruktur. 3. Sistem Informasi yang telah berjalan di RTC/PT. Rancek Sukses belum membantu dalam mencapai tujuan perusahaan.

Berdasarkan data pada Tabel 2.1, diuraikan lima jurnal penelitian terdahulu dengan permasalahan yang hampir sama untuk kemudian diteliti. Susanto (2015), Hidayat (2015), Kristanto (2016), Sari (2014), dan Juliane (2014) dalam penelitiannya menggunakan metode penelitian yaitu pengerjaan COBIT 5.0. Setiap penelitian memiliki objek dan fokus domain yang berbeda-beda. Pada jurnal Susanto yang berjudul "Perancangan Tata Kelola TI Untuk Pelayanan Publik Pada Dinas Komunikasi Dan Informatika Surabaya Dengan Kerangka Kerja COBIT 5.0" fokus prosesnya kepada meningkatkan tingkat kapabilitas sesuai dengan yang diharapkan instansi untuk memperbaiki TI dalam hal pelayanan publik. pada domain (EDM03, EDM04, APO01, APO03, APO04, APO05, APO08, APO09, APO11, APO12, APO13, BAI06, DSS05, BAI01, BAI02, BAI04, BAI05, BAI06, BAI07, BAI08, BAI09, BAI10, DSS01, DSS03, DSS04, DSS05, MEA01, MEA02). Sedangkan Hidayat memiliki 10 proses dengan fokus pada domain (DSS01, DSS04, DSS05) , (EDM04, EDM05, DSS02,

DSS06) dan (EDM01, EDM02, DSS03) untuk jurnal pengukuran capability level tata kelola system informasi di “Direktorat TIK UPI Bandung”. Selanjutnya pada jurnal Kristanto penelitiannya memiliki fokus pada domain (DSS05, APO013, DSS04, APO01, MEA01) dengan objek “Divisi TI Dinas Perindustrian dan Perdagangan Kota Surabaya”. Sedangkan Sepita memiliki fokus pada domain (MEA01, MEA02, MEA03) pada penelitiannya di “Dinas Komunikasi dan Informatika Kabupaten OKU”. Juliane dalam penelitiannya di “PT. Rancek Sukses Bandung” memiliki fokus pada domain seputar domain APO01 - APO13 (*Align, Plan, & Organize*).

Yang dapat diadopsi dari masing-masing penelitian tersebut adalah dapat menggunakan penelitan terdahulu sebagai referensi mengenai metode penelitian yang menggunakan COBIT 5.0 dan cara perhitungan *Capability Level* yang ada di masing-masing penelitian tersebut. Sehingga akan memudahkan kedepannya untuk menyempurnakan penelitian ini.

Perbedaan penelitian ini dengan penelitian terdahulu pada Tabel 2.1 diatas adalah pada penelitian ini menggunakan tahapan pengukuran kapabilitas tata kelola TI dari Gallegos dalam memaparkan hasil penelitian ini. Penelitian ini memilih tahapan dari Gallegos karena adanya tahapan yang sederhana namun mendalam serta ruang lingkup yang sudah jelas untuk diteliti yang sesuai dengan kebutuhan perusahaan dan menggunakan fokus pada proses domain yang berbeda.