BAB II LANDASAN TEORI

2.1 Audit Teknologi Informasi

Audit atau pemeriksaan dalam arti luas bemakna evaluasi terhadap suatu organisasi, sistem, proses atau produk. Audit dilaksanakan oleh pihak yang kompeten, objektif, tidak memihak, yang dikenal dengan sebutan auditor. Tujuanya adalah untuk melaksanakan verifikasi bahwa subjek dai audit telah diselesaikan atau berjalan dengan standar, regulasi, dan praktek yang telah disetujui dan diterima [3].

Audit teknologi informasi adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknlogi informasi ini dapat berjalan bersama – sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis.

Ada beberap asepek yang diperiksa pada audit TI secara keseluruhan menyangkut efektifitas, efisiensi, *avability system, reliability, contidentiality* dan *integrity*, serta aspek *security*. Selenjutnya adalah audit atas proses, modifikasi program, audit atas sumber data dan data *file* [4].

Tata kelola TI (*IT Governance*) adalah tanggung jawab dari eksekutif dan *boar of direction*, yang terdiri dari kepemimpinan, struktur organisasi dan proses- proses yang memastikan bahwa TI di perusahaan menopang dan memperluas strategi dan tujuan organisasi. Tata kelola TI mengintegrasikan *best practices* untuk memastikan bahwa TI disebuah perusahaan mendukung tujuan bisnis. Tata kelola TI memungkinkan perusahaan untuk mengambil keuntungan penuh dari informasi yang dimilikinya, sehingga memaksimalkan keuntungan, memanfaatkan peluang dan mendapat keuntungan kompetitif [5].

Tujuan audit adalah mendapatkan informasi faktual dan signifikan berupa data hasil analisa, penilaian, rekomendasi auditor yang dapat digunakan oleh auditee atau manjemen untuk berbagai keperluan misalnya untuk dasar pengambilan keputusan, pengendalian manajemen, perbaikan dan ata perubahan dalam berbagai aspek dalam upaya mengamankan kebijakan dan mencapai tujuan organisasi secara keseluruhan [6].

Dalam penelitian Vlasta Ron Weber menyatakan beberapa alasan penting mengapa audit TI perlu dilakukan, antara lain :

1. Kerugian akibat kehilangan data.
2. Kesalahan dalam pengambilan keputusan
3. Risiko kebocoran data
4. Penyalahgunaan komputer
5. Kerugian akibat kesalahan proses perhitungan
6. Tingginya nilai investasi perangkat keras dan perangkat lunak komputer

2.2 Konsep Dasar Sistem Informasi

Sistem Informasi dapat didefinisikan sebagai suatu sistem didalam suatu organisasi yang merupakan kombinasi manuasia (SDM), fasilitasi teknologi, media, prosedur – prosedur, dan pengendalian yang ditujukan untuk mendapatkan jalur komunikasi penting, memproses tipe transaksi rutin tertentu, memberi sinya kepada manajemen dan lainnya terhadap kejadian – kejadian internal dan eksternal yang penting dan menyajikan suatu dasar informasi untuk mengambil keputusan yang baik. Informasi didapatkan dari sistem informasi atau disebut juga dengan *processing system* atau *information processing systems* [7].

2.3 Pengertian COBIT

Control Objective for Information and Related Technology (COBIT) telah menjadi standar pengendalian manajemen pada teknologi informasi yang dikeluarkan pada tahun 1966 oleh badan audit ISACA (*The Information System Audit and Control Association*). Pada tahun yang sama ISACA dan ITGI melebur menjadi satu entitas dan mempublikasikan COBIT edisi ketiga pada tahun 2000 dan diikuti versi ke empat pada tahun 2006.

COBIT merupakan suatu cara untuk menerapkan *IT Governance*. COBIT berupa kerangka kerja yang harus digunakan oleh suatu organisasi bersamaan dengan sumber daya lainnya untuk membentuk suatu standar yang umum berupa panduan pada lingkungan yang lebih spesifik. Secara terstruktur, COBIT terdiri dari seperangkat *control objectives* untuk bidang teknologi informasi, dirancang untuk memungkinkan tahapan bagi audit [8].

COBIT merupakan sekumpulan dokumentasi best practies ntuk IT Governance yang dapat membantu auditor, pengguna (user), dan manjemen, untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol da masalah – masalah teknis TI. COBIT bermanfaat bagi

auditor karena merupakan teknik yang dapat membantu dalam identifikasi IT control issues. Adapun menurut ISACA standar untuk audit sistem informasi adalah [8] :

Table 2.1 Standar Audit sistem Informasi ISACA

010	*Audit Chapter*
010.010	*Responsibility, Authority and Accountability* Definisi dari tanggungjawab, otoritas, dan *accountability* dari fungsi audit sistem informasi lebih tepat bila didokumnetasikan dalam surat
020	*Independence*
020.010	*Profesional Independence* Dalam permasalahan yang berkaitan dengan audit, auditor sistem informasi harus bersikap independen dalam tingkah laku dan tindakannya.
020.020	*Organizational Relationship* Fungsi audit sistem informasi harus berada independen dari area yang diaudit untuk mencapai tujuan objektivitas dari suatu proses.
030	*Profesional Ethics and Standards*
030.010	*Code of Profesional Ethics* Auditor dari sistem informasi harus menghormati dan manaati etika profesional dari ISACA.
030.020	*Due Profesional Core* Standar *auditing* profesional harus diterapkan dalam segala aspek dalam pekerjaan yang dilakukan oleh auditor sistem informasi.
040	*Competence*
040.010	*Continuing Professional Education*
040.020	Auditor sistem informasi harus memaintain kompetensi teknikal melalui pendidikan lanjut profesional.
050	*Planning*
050.010	*Audit Planning* Auditor sistem informasi harus merencanakan perencanaan audit sistem untuk menempatkan tujuan audit dan untuk melengkapi standar profesioanl

060	*Performance of Audit Work*
060.010	*Supervision* Staf dari audit system informasi harus tepat untuk dapat menjamin tujuan dari audit dijalankan dan standar profesional *auditing* dapat terpenuhi.
060.020	*Evidence* Selama masa pekerjaan audit, auditor system informasi harus mendapatkan bukti yang tepat, dapat dipercaya, relevan dan berguna untuk mencapai
070	*Reporting*
070.010	*Report Content and Form* Auditor system informasi harus menyediakan *report* dalam bentuk yang tepat pada saat penyelesaian tugas audit. Laporan audit berupa ruang lingkup, tujuan periode audit, dan lingkungan dimana audit dijalankan. Laporan audit harus mengidentifikasikan permasalahan yang terjadi dalam jangka waktu audit. Laporan audit juga untuk memberikan rekomendasi dari layanan atau kualifikasi yang diberikan auditor terhadap tugas audit yang dijalankan.
080	*Follow Up Activities*
080.010	*Follow Up* Auditor system informasi harus meminta dan mengevaluasi informasi yang sesuai dari penemuan yang terdahulu dan rekomendasi yang dihasilkan pada periode audit terdahulu untuk mendefinisikan tindakan yang tepat yang harus diimplementasikan dalam suatu periode waktu.

2.4 Kerangka COBIT 5

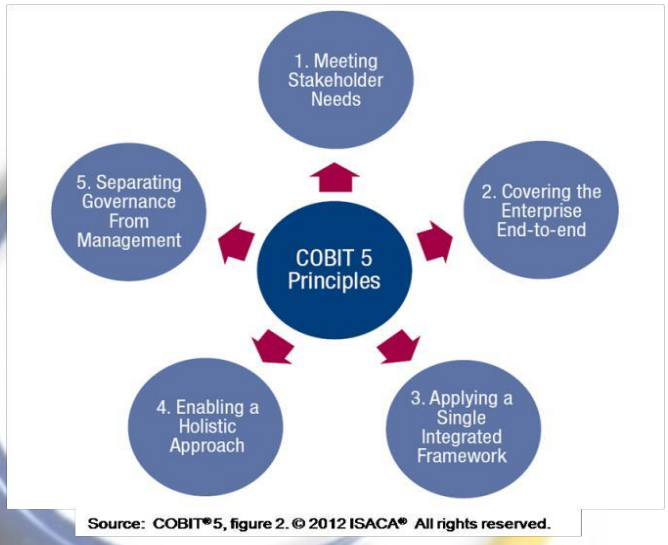
Secara sederhana COBIT 5 membantu *enterprise* membangun nilai yang optimal dari TI dengan mengelola keseimbangan antara realisasi manfaat dan optimasi Level resiko dan penggunaan sumberdaya.

COBIT 5 memungkinkan informasi dan teknologi yang terkait untuk dikelola secara holistic bagi keseluruhan enterprise, mencakup area bisnis dan fungsional secara keseluruhan, dengan mempertimbangkan manfaat TI bagi stakeholder internal dan eksternal [9].

2.4.1 Prinsip – Prinsip COBIT 5

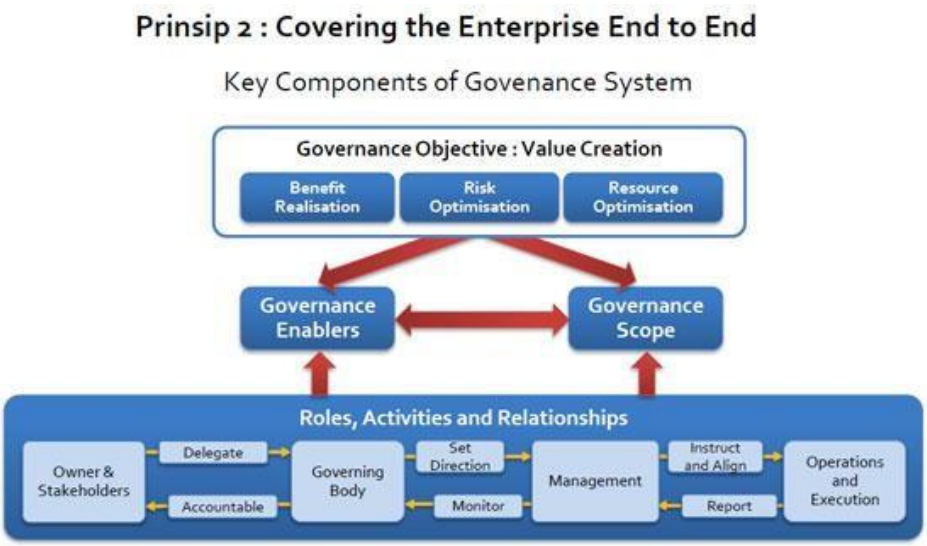
COBIT 5 memiliki 5 prinsip dasar yaitu [9] :

1. Memenuhi kebutuhan stakeholder.
2. Melingkupi tata kelola dan proses kerja End-to End Enterprise
3. Mengaplikasikan sebuah kerangka-kerja yang terintegrasi.
4. Pendekatan keseluruhan untuk kemampuan tata kelola dan manajemen atau pengaturan.
5. Pemisahan antara tata-kelola dengan manajemen atau pengaturan.



Gambar 2.1 Prinsip Dasar COBIT 5 [9]

1. ***Meeting stakeholder needs***, berguna untuk pendefinisan prioritas untuk implementasi, perbaikan, dan jaminan. Kebutuhan *stakeholder* diterjemahkan ke dalam *Goals Cascade* menjadi tujuan yang lebih spesifik, dapat ditindaklajuti dan disesuaikan, dalam konteks : Tujuan perusahaan (*Enterprise Goal*), Tujuan yang terkait IT (*IT-related Goal*), Tujuan yang akan dicapai *enabler (Enabler Goal).* Selain itu sistem tata kelola harus mempertimbangkan seluruh *stakeholder* ketika membuat keputusan mengenai penilaian manfaat, *resource* dan risiko [9].
2. ***Covering enterprise end-to-end***, bermanfaat untuk mengintegrasikan tata kelola TI perusahaan kedalam tata kelola perusahaan. Sistem tata kelola TI yang diusung COBIT 5 dapat menyatu dengan sistem tata kelola perusahaan dengan mulus [9].



Gambar 2.2 Komponen – Komponen Inti Dari Sistem Tata Kelola [9]

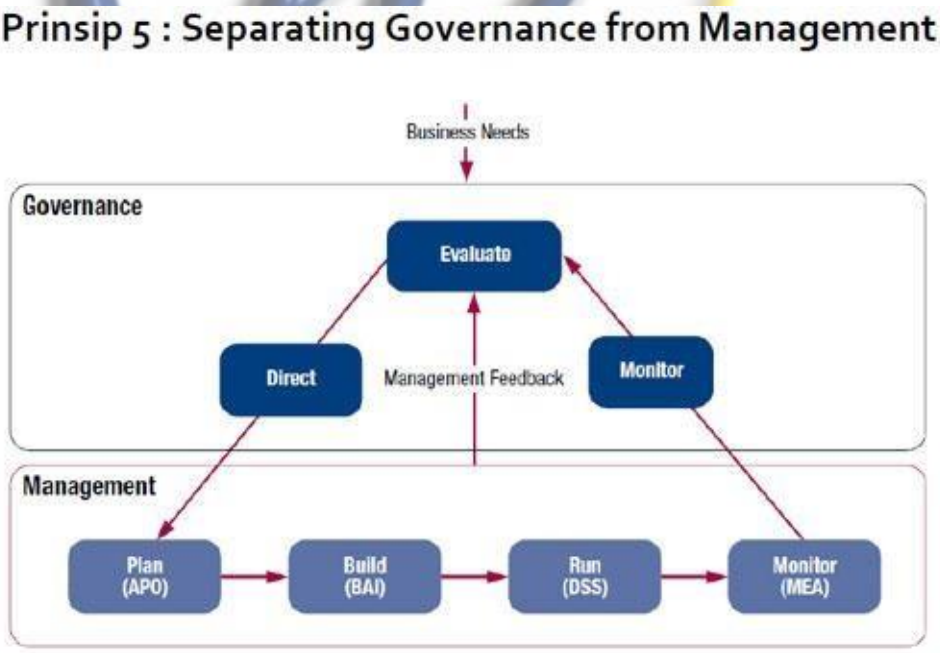
Prinsip kedua ini juga meliputi semua fungsi dan proses yang dibutuhkan untuk mengatur dan mengelola TI perusahaan dimanapun informasi diproses. Dalam lingkup perusahaan, COBIT 5 menangani semua layanan TI internal maupun eksternal, dan juga proses bisnis internal dan eksternal.

3. ***Applying a single intergrated framework***, sebagai penyelarasan diri dengan standar dan *framework* relevan lain, sehingga perusahaan memapu menggunakan COBIT 5 *framework* tata kelola umum dan *integrator*. Selain itu prinsip ini menyatukan semua pengetahuan yang sebelumnya tersebar dalam berbagai *framework* ISACA (COBIT, VAL IT, Risk IT, BMIS, ITAF).
4. ***Enabling a holistic approach***, yakni COBIT 5 memandang bahwa setiap *enabler* saling memperngaruhi satu sama lain dan menentukan apakah penerapan COBIT 5 akan berhasil.

Gambar 2.3 Saling Berpengaruh Enabler [9]

5. ***Separating governance from management***,

   COBIT membuat perbedaan yang cukup jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup brbagai kegiatan yang berbeda, memerlukan struktur organisasi yang berbeda, dan melayani untuk tujuan yang berbeda pula.



Gambar 2.4 Pemisahan tata kelola dan manajemen [9]

Perbedaan *Governance* (Tata kelola) dengan *Management* (Manajemen)

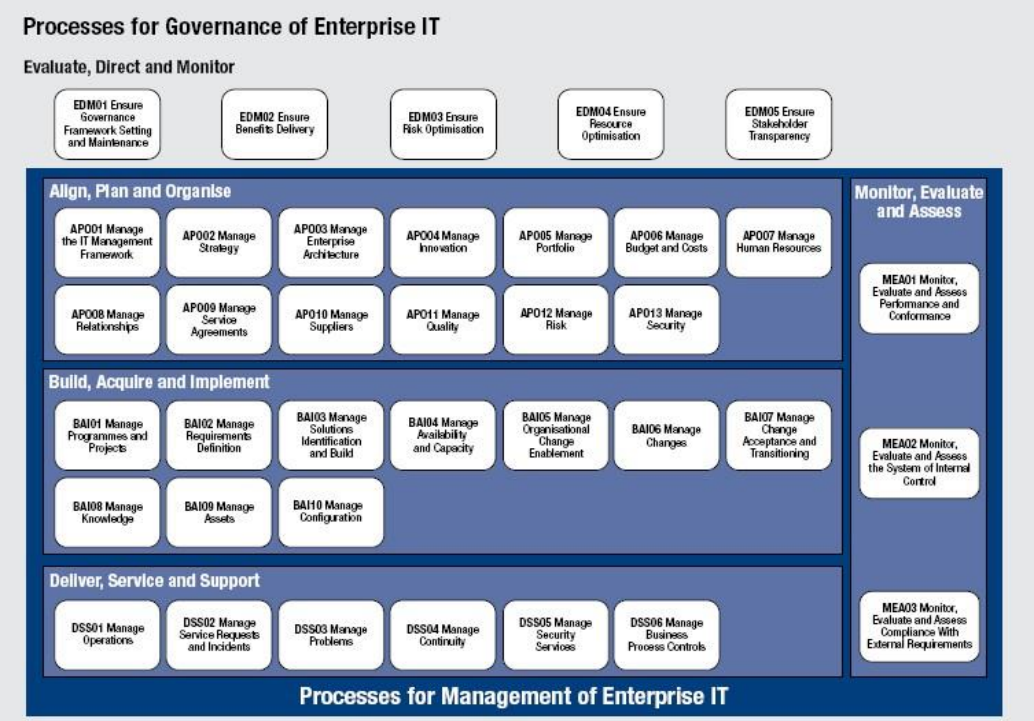
- *Governance* adalah tata kelola yang memastikan bahwa tujuan perusahaan dapat dicapai dengan melakukan evaluasi terhadap kebutuhan, kondisi, dan pilihan *stakeholder*, menerapkan arah melaluiprioritas dan pengambilan keputusan terhadap arah dan tujuan yang telah disepakati. Pada perusahaan secara normatif, tata kelola adalah tanggung jawab dari dewan direksi dibawah kepemimpinan ketua. Tata kelola berisi lima proses yaitu proses itu sendiri, mengevaluasi, dan pemantauan langsung.
- *Management* (Manajemen) berfungsi sebagai perencana, membangun, menjalankan dan memonitor aktifitas-aktifitas yang sejalan dengan arah yang ditetapkan oleh badan tata kelola untuk mencapai tujuan perusahaan. Manajemen-Berisi empat domain, sesuai dengan Bagian tanggung jawabnya yaitu merencanakan, membangun, menjalankan dan memantau (PBRM) falam cakupan *end-to-end*. 4 domain tersebut yaitu:
  1) *Align, Plan and Organise (APO)*
  2) *Build, Acquire and Implement (BAI)*
  3) *Deliver, Service and Support (DSS)*
  4) *Monitor, Evaluate and Assess (MEA)*

2.4.2 Domain dan Proses pada COBIT 5

COBIT 5 memiliki 5 domain yang terbagi dalam domain *governance* dan *management*, masing- masing domain memiliki proses yang memungkinkan untuk mencapai tujuannya [10]. Satu domain berasal dari *governance* dan empat lainnya berasal dari *management*. Domain yang berasal dari area *governance of enterprise* IT adalah (*Evaluate, Direct, and Monitor*) EDM yang terdiri dari 5 proses. Sedangkan domain yang berasal dari *management of enterprise* IT sejalan dengan tanggung jawab pada area *plan, build, run, and monitor* (PBRM). Terdapat 32 proses yang dipecah kedalam masing-masing domain sebagai berikut.

1. *Align, Plan and Organize* (APO) dengan13 proses.

2. *Build, Acquire and Implement* (BAI) dengan 10 proses.
3. *Deliver, Service and Support* (DSS) dengan 6 proses.
4. *Monitor, Evaluate and Assess* (MEA) dengan 3 proses.



Gambar 2.5 Domain dan Proses COBIT 5 [11]

1. Domain Evaluate, Direct and Monitor

Pada proses tata kelola ini berkaitan dengan tujuan stakeholder dalam melakukan penilaian, optimasi risiko sumber daya, mencakup praktik dan kegiatan yang bertujuan untuk mengevaluasi pilihan strategis, meberikan arahan kepada TI dan pemantauan hasilnya. Terdiri dari 5 sub domain yaitu :

1) *Ensure Governance Framework Setting and Maintance*
2) *Ensure Benefit Delivery*
3) *Ensure Risk Optimisation*
4) *Ensure Resource Optimisation*
5) *Ensure Stakeholder Transparancy*

2. Domain Align, Plan and Organize

Domain Align, Plan and Organise (APO) ini menjangkau strategi dan taktik, serta mengidentifikasi resiko yang merupakan cara terbaik TI agar dapat berkontribusi pada pencapaian tujuan bisnis. Penerapan visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perspektif yang berbeda. Sebuah organisasi yang tepat, serta insfratuktur teknologi, harus dimaskukkan ke dalam tempatnya. Domain (APO) memberikan arah untuk pengiriman solusi pada domain (BAI) dan penyediaan layanan dan dukungan (DSS). Sub domain (APO) ada 13 yaitu :

1) *Manage the IT Managemen Framework*
2) *Manage Strategy*
3) *Manage Enterprise Architecture*
4) *Manage Innovation*
5) *Manage Portfolio*
6) *Manage Budget and Costs*
7) *Manage Human Resources*
8) *Manage Relationships*
9) *Manage Service Agreements*
10) *Manage Suppliers*
11) *Manage Quality*
12) *Manage Risk*
13) *Manage Security*

3. Domain Build, Acquire and Implement

Domain *Build, Acquire and Implement* (BAI) memberikan solusi yang tepat sehingga akan berubah menjadi layanan. Perlu adanya identifikasi dan implementasi yang terintegrasi kedalam proses bisnis dalam mewujudkan strategi TI. Perubahan dan pemeliharaan sistem yang ada juga dicakup oleh domain ini, untuk memastikan bahwa solusi terus memenuhi tujuan bisnis. Sub domain *Build, Acquire and Implement* (BAI) terdiri dari:

1) *Manage Programmes and Projects*
2) *Manage Requirements Definition*

3) *Manage Solutions Identification and Build*
4) *Manage Availability and Capacity*
5) *Manage Organisational Change Enablement*
6) *Manage Changes*
7) *Manage Change Acceptance and Transitioning*
8) *Manage Knowledge*
9) *Manage Assets*
10) *Manage Configuration.*

4. Domain Deliver, Service and Support

Berkaitan dengan aspek pengiriman teknologi informasi. Domain DSS menjangkau bidang-bidang seperti kinerja aplikasi dalam sistem TI dan hasil-hasilnya serta proses yang memungkinkan pelaksanaan yang efektif dan efisien dari sistem TI. Sub domainnya terdiri dari :

1) *Manage Operations*
2) *Manage Service Requests and Incidents*
3) *Manage Problems*
4) *Manage Continuity*
5) *Manage Security Services*
6) *Manage Business Process Controls.*

5. Domain Monitor, Evaluate and Asses

Memperkenankan solusi oleh pengguna akhir. Domain ini berurusan dengan pengiriman aktual dan dukungan layanan yang dibutuhkan, yang meliputi pelayanan, pengelolaan keamanan dan kelangsungan, dukungan layanan bagi pengguna, dan manajemen data dan fasilitas operasional. Sub domainnya yang terdiri dari :

1) *Monitor, Evaluate and Assess Performance and Conformance*
2) *Monitor, Evaluate and Assess the System of Internal Control*
3) *Monitor, Evaluate and Assess Compliance with External Requirements.*

2.3.3 Domain Delivery, Service and Support (DSS)

Deliver, Service, and Support yang biasa dikenal dengan singkatan DSS merupakan salah satu domain di *framework* COBIT 5. Domain ini merupakan

perluasan dari domain *Deliver and Support* (DS) pada versi COBIT sebelumnya, yakni COBIT 4.1. Domain DSS menitikberatkan pada proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan, dan pengelolaan data yang sedang berjalan.

Sementara fokus domain DSS pada COBIT 5 yakni pada aspek pengiriman teknologi informasi, proses, dan dukungan yang memungkinkan untuk pelaksanaan system TI yang efektif dan efisien. Domain DSS terdiri dari 6 *control objective*, yakni sebagai berikut [11].

1) *Manage Operations* (Mengelola Operasi – DSS01)
2) *Manage Service Requests and Incidents* (Mengelola Permintaan Layanan dan Insiden – DSS02)
3) *Manage Problems* (Mengelola Masalah – DSS03)
4) *Manage Continuity* (Mengelola Keberlanjutan – DSS04)
5) *Manage Security Services* (Mengelola Keamanan – DSS05)
6) *Manage Business Process Controls* (Mengelola Kontrol Proses Bisnis – DSS06)

2.5 RACI Chart

Untuk melakukan penilaian dengan domain DSS, maka dilakukan *mapping* antara *sub control objective*s dan sumber daya manusia (SDM) yang ada di bagian pelaksana TI dengan menggunakan RACI Chart. RACI Chart adalah bagian dari *Rensponsibility Assignment Matrix* (RAM) yang merupakan suatu bentuk pemetaan antara sumber daya dengan aktivitas dalam setiap prosedur. Berikut merupakan contoh salah satu RACI Chart pada DSS01 [12].

DSS01 RACI Chart																											
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS01.01 Perform operational procedures.																					A		C	C	C	
DSS01.02 Manage outsourced IT services.											I							A			R					
DSS01.03 Monitor IT infrastructure.				I		C					I						C	I		C	A		C	C		
DSS01.04 Manage the environment.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS01.05 Manage facilities.						I					C	A				C	C	C	I	C	R		I	R	I	

Gambar 2.6 Raci Chart DSS01 [12]

Mapping tersebut dilakukan untuk seluruh *control objective* yang ada pada domain DSS. *Mapping* menggunakan diagram RACI. RACI merupakan singkatan dari *Responsible* (R), *Accountable* (A), *Consulted* (C), dan *Informed* (I). Berikut merupakan arti dari diagram RACI [12].

a. *Responsible* (R) menunjukkan bahwa bagian tersebut merupakan pihak pelaksana yang harus bertanggungjawab melaksanakan dan menyelesaikan aktivitas yang menjadi tanggung jawabnya.
b. *Accountable* (A) menunjukkan bahwa bagian tersebut merupakan pihak yang harus mengarahkan jalannya pelaksanaan aktivitas.
c. *Consulted* (C) menunjukkan bahwa bagian tersebut merupakan pihak yang akan menjadi tempat konsultasi selama pelaksanaan aktivitas.
d. *Informed* (I) menunjukkan bahwa bagian tersebut merupakan pihak yang diberikan informasi mengenai pelaksanaan aktivitas.

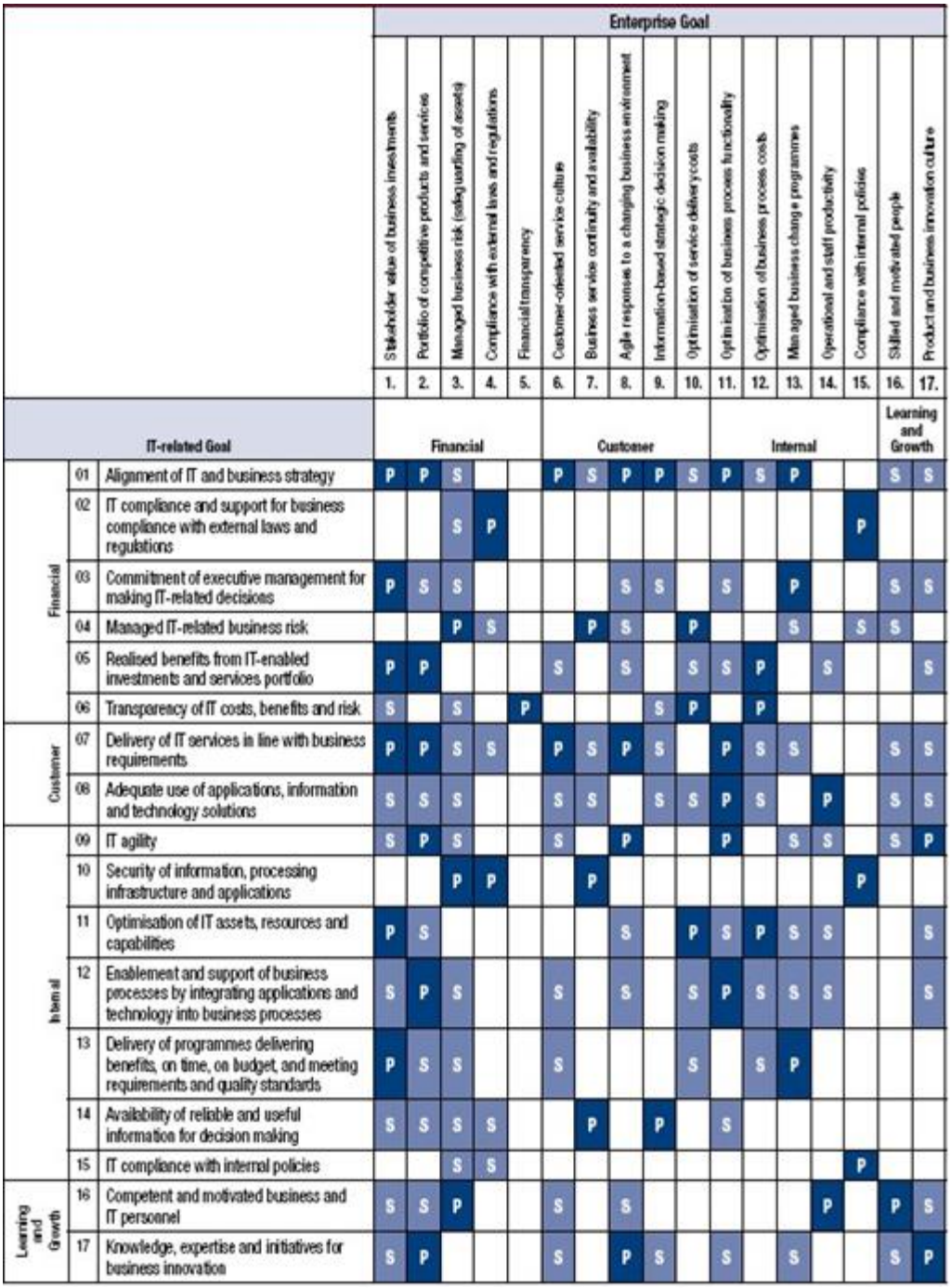
2.6 Goals Casecade Untuk Perencanaan Audit

Hubungan antara tujuan dan strategi bisnis dengan tujuan TI harus sejalan, untuk itu tujuan TI harus mendukung tujuan bisnis. Untuk melakukan perencanaan audit, terlebih dahulu melakukan mapping enterprise goal dengan IT – related goal guna memaparkan tujuan bisnis secara umum dengan beberapa tujuan TI yang mendukung tujuan bisnis organisasi. IT – related goals merupakan IT balance

scorecard yang memandang TI berdasarkan empat perspektif, sedangkan enterprise goal merupakan balance scorecard yang memandang tujuan organisasi secara keseluruhan berdasarkan empat perspektif [12]. Hasil dari mapping ini tidak digunakan semua tetapi hanya yang relevan dengan kondisi objek audit. Untuk melakukan proses audit, sebelumnya dilakukan beberapa langkah sebagai berikut.

a. Mapping antara tujuan bisnis perusahaan dengan tujuan TI.

   Mapping dilakukan kedalam perspektif IT Balance Scorecard (IT BSC). Jika hubungan keterkaitan antara tujuan bisnis dan tujuan TI sangat kuat, maka diberi tanda "P" yang berarti primary (strong relationship). Jika terdapat hubungan antara tujuan bisnis dengan tujuan TI tetapi hubungan tersebut tidak dominan, maka diberi tanda "S" yang berarti secondary (medium relationship). Jika tidak ada hubungan sama sekali, maka dikosongkan.

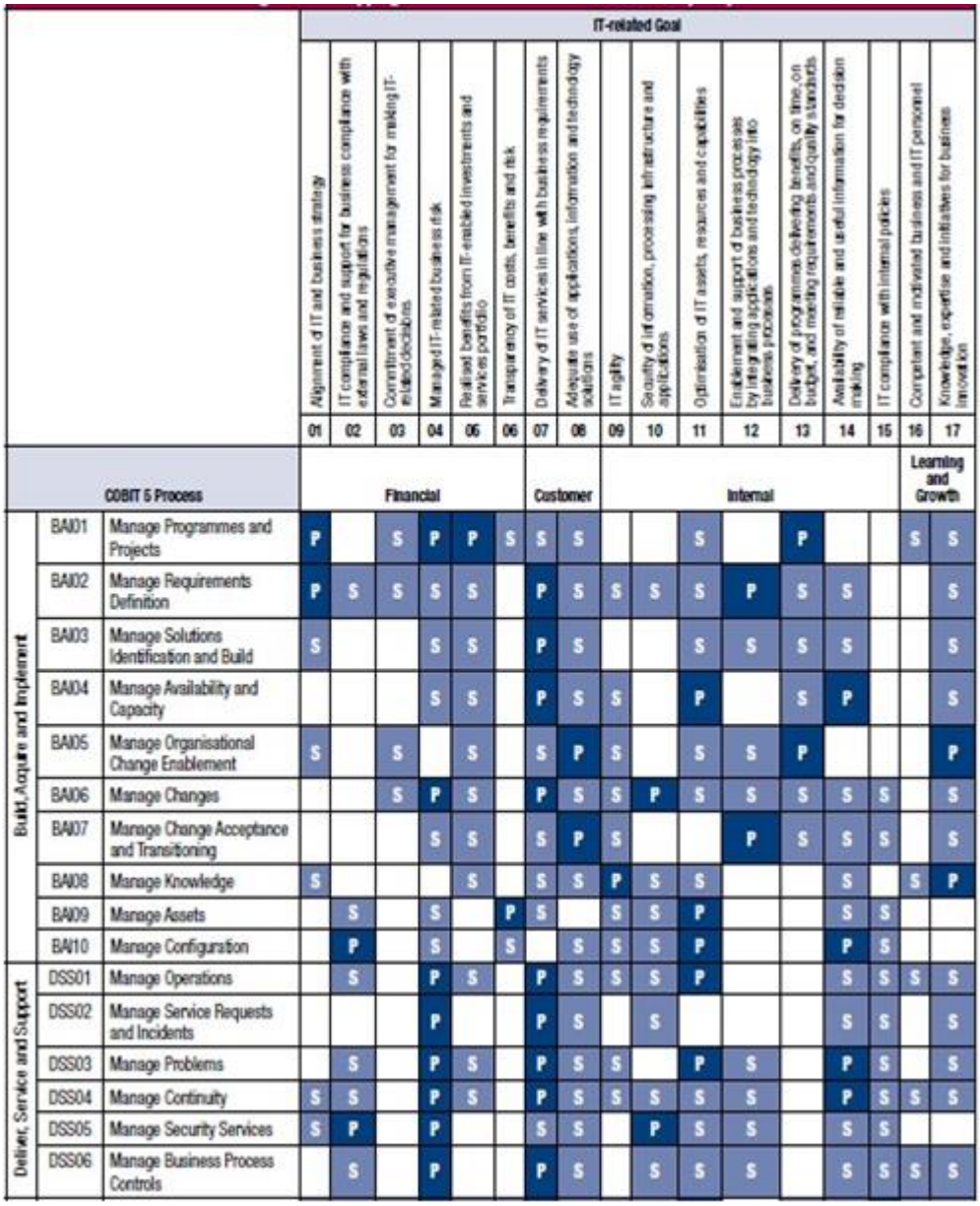


		Enterprise Goal																
		Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
IT-related Goal		Financial					Customer					Internal					Learning and Growth	
Financial	01 Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03 Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04 Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05 Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06 Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07 Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09 IT agility	S	P	S			S		P			P		S	S		S	P
	10 Security of information, processing infrastructure and applications			P	P			P								P		
	11 Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12 Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14 Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15 IT compliance with internal policies			S	S											P		
Learning and Growth	16 Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17 Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Gambar 2.7 Mapping Enterprise Goals dengan IT-related Goals [12]

b. Melakukan mapping antara tujuan TI dengan proses TI

Setiap tujuan TI memiliki masing-masing proses TI yang relevan. Setelah dilakukan mapping terhadap tujuan bisnis perusahaan dengan tujuan TI, selanjutnya dilakukan mapping tujuan TI dengan proses TI [12].



			IT-related Goal																
			01 Alignment of IT and business strategy	02 IT compliance and support for business compliance with external laws and regulations	03 Commitment of executive management for making IT-related decisions	04 Managed IT-related business risk	05 Realised benefits from IT-enabled investments and services portfolio	06 Transparency of IT costs, benefits and risk	07 Delivery of IT services in line with business requirements	08 Adequate use of applications, information and technology solutions	09 IT agility	10 Security of information, processing infrastructure and applications	11 Optimisation of IT assets, resources and capabilities	12 Enablement and support of business processes by integrating applications and technology into business processes	13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	14 Availability of reliable and useful information for decision making	15 IT compliance with internal policies	16 Competent and motivated business and IT personnel	17 Knowledge, expertise and initiatives for business innovation
	COBIT 5 Process		Financial						Customer		Internal							Learning and Growth	
Build, Acquire and Implement	BAI01	Manage Programmes and Projects	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Manage Requirements Definition	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Manage Solutions Identification and Build	S			S	S		P	S			S	S	S	S			S
	BAI04	Manage Availability and Capacity				S	S		P	S	S		P		S	P			S
	BAI05	Manage Organisational Change Enablement	S		S		S		S	P	S		S	S	P				P
	BAI06	Manage Changes			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Manage Change Acceptance and Transitioning				S	S		S	P	S			P	S	S	S		S
	BAI08	Manage Knowledge	S				S		S	S	P	S	S			S		S	P
	BAI09	Manage Assets		S		S		P	S		S	S	P			S	S		
	BAI10	Manage Configuration		P		S		S		S	S	S	P			P	S		
Deliver, Service and Support	DSS01	Manage Operations		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Manage Service Requests and Incidents				P			P	S		S				S	S		S
	DSS03	Manage Problems		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Manage Continuity	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Manage Security Services	S	P		P			S	S		P	S	S		S	S		
	DSS06	Manage Business Process Controls		S		P			P	S		S	S	S		S	S	S	S

Gambar 2.8 Mapping IT-related Goals dengan COBIT 5 Process [12]

2.7 Process Capability Model

Process capability model digunakan untuk mengukur kematangan IT enterprise, diadopsi dari ISO/IEC 15504 sebagai standar proses penilaian. Model ini menyediakan pengukuran performansi dari proses-proses pada area governance maupun manajemen, dan melakukan peningkatan pada area-area yang telah diidentifikasi [13].

Terdapat 6 Level kapabilitas proses yang bisa dicapai termasuk incomplete process jika prakteknya tidak tercapai sesuai dengan tujuan.

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work product management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimizing process
PA 5.1	Process innovation
PA 5.2	Process optimization

Gambar 2.9 Process Capability Model [13]

Berikut adalah penjelasan level dari process capability :

a. Level 0 (Incomplete)

   Proses tidak melaksanakan atau gagal untuk mencapai tujuan proses. Pada tingkat ini, ada sedikit atau tidak sama sekali bukti (evidence) dari setiap pencapaian tujuan proses.

b. Level 1 (Perfomed)

   Proses diimplementasikan untuk mencapai tujuan bisnisnya.

c. Level 2 (Managed)

   Proses yang diimplementasikan dikelola (plan, monitor, and adjusted) dan hasilnya ditetapkan dan dikontrol.

d. Level 3 (Established)

   Proses didokumentasikan dan dikomunikasikan (untuk efisiensi organisasi).

e. Level 4 (Predictable)

Proses dimonitor, diukur, dan diprediksi untuk mencapai hasil.

f. Level 5 (Optimizing)

Sebelumnya proses telah di prediksikan kemudian ditingkatkan untuk memenuhi tujuan bisnis yang relevan dan tujuan yang akan dating.

Setiap proses yang dinilai akan menghasilkan 4 level rating point, yaitu :

a) Not achieved, apabila hasil penilaian antara 0% - 15%
b) Partially achieved, apabila hasil penilaian >15% - 50%
c) Largely achieved, apabilahasil penilaian >50% - 85%
d) Fully achieved, apabila hasil penilaian >85% - 100%

2.8 Perbedaan Framework COBIT 4.0/2.1 dan COBIT 5

COBIT 4.0/4.1

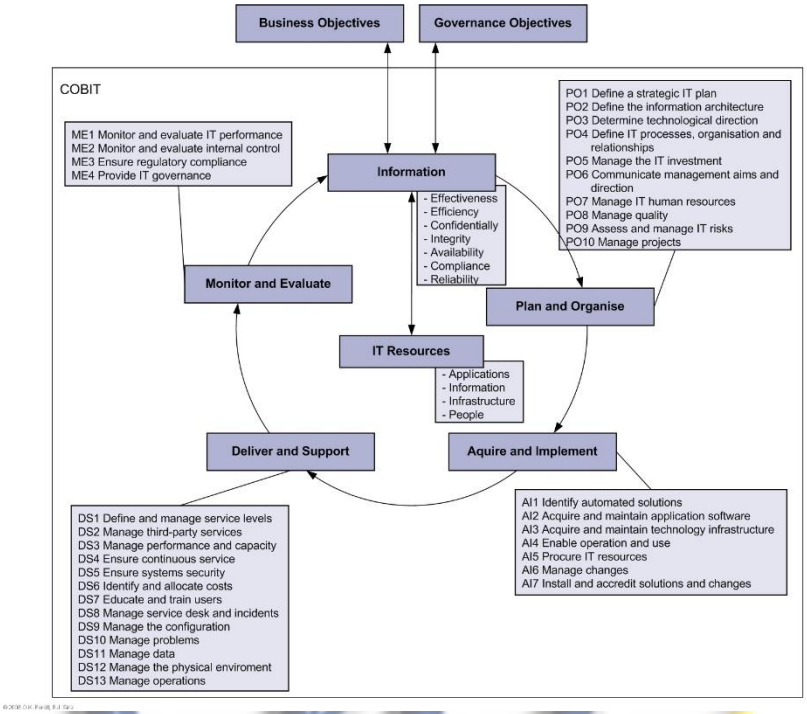
COBIT versi 4.0 diterbitkan pada tahun 2005 dan COBIT 4.1 diterbitkan pada tahun 2007, memiliki penambahan dari versi sebelumnya yaitu pada tata kelola (governance) dan kepatuhan (compliance). COBIT 4.0/4.1, selanjutnya dalam tulisan ini disebut COBIT 4 meiliki prinsip yaitu sebagai penyedia informasi bagi organisasi dengan cara mengelola dan mengendalikan sumberdaya TI (aplikasi, informasi, infrastruktur dan orang) dengan menggunakan sekumpulan proses – proses yang terstruktur. Agar tujuan manajemen dalam mengelola dan mengendalikan sumberdaya TI dapat dilakukan maka diperlukan “kebijakan, perencanaan dan prosedur, dan ada struktur organisasi” yang dirancang dengan baik [14].

Untuk mewujudkan tujuan manajemen tersebut, COBIT memberikan kerangka kerja tata kelola TI dan panduan secara detail (DCO – detailed control objective). Panduan ini terdiri atas empat domain utama dengan 34 proses pengendalian TI. Domain tersebut terdiri dari :

1. *Pland and Organize (PO)*
2. *Acquire and Implement (AI)*
3. *Deliver and Support (DS)*
4. *Monitor and Evaluate (ME)*

Setiap proses memiliki keterkaitan dengan domain untuk mendapatkan hasil pengolahan TI yang baik. Adapun kriteria control pada pengelolaan TI dalam COBIT terdiri atas (1)

Efektivitas, (2) Efisiensi, (3) Kerahasiaan, (4) Integritas, (5) Ketersediaan, (6) Kepatuhan, (7) Keandalan. Selengkapnya domain dan proses dalam COBIT 4 terlihat pada gambar dibawah.



Gambar 2.10 Framework COBIT 4 [14]

COBIT 5

Penggunaan panduan berstandar internasional, tanpa kecuali COBIT dalam organisasi bertujuan untuk mengurangi resiko dan meningkatkan kepercayaan yang terkait dengan pemanfaatan TI yang dihasilkan. Namun berdasarkan hasil survey, pengguna COBIT mengalami peningkatan yang cukup tinggi. Hal ini karena penggunaan COBIT dalam sebuah organisasi memiliki peran antara lain :

1) Penciptaan nilai melalui penggunaan IT yang efektif dan inovatif dalam organisasi
2) Kepuasan pengguna IT dalam bisnis dan jasa
3) Kepatuhan terhadap hokum, peraturan kontrak perjanjian dan kebijakan internal
4) Peningkatan hubungan antara kebutuhan bisnis dan tujuan IT

Meningkatnya penggunaan COBIT, membuat ISACA selaku pembuat terus melakukan penyempurnaa. Bahkan COBIT 5 diterbitkan pada bulan April 2012 merupakan versi terbaru sebagai wujud kepercayaan para organisasi pengguna dalam kurun waktu 16 tahun. Dimana COBIT 5 ini bersifat generik dan dapat digunakan oleh semua jenis organisasi baik yang

bersifat komersial, maupun nirlaba atau sektor publik. COBIT 5 memiliki dua fokus yaitu tata kelola (*governance*) dan manajemen (*management*) yang dikenal dengan istilah EDM (*evaluating, direction, monitoring*) untuk tata kelola dan PBRM (*plans, builds, runs, monitors*) untuk manajemen. Dapat dikatakan bahwa COBIT 5 merupakan bentuk restrukturisasi untuk memastikan cakupan yang lengkap pada semua aspek utama yang berhubungan dengan tata kelola dan manajemen organisasi TI[16].

Setiap versi COBIT memiliki kekuatan dan fokus tertentu untuk menyelesaikan permasalahan yang terkait TI. COBIT 5 memiliki lima prinsip baru, terdiri dari:

(1) *Meeting stakeholder needs* (mempertemukan kebutuhan stakeholder)
(2) *Covering the enterprise end-to-end* (melingkupi kegiatan organisasi hingga akhir)
(3) *Applying a single integrated framework* (menerapkan kerangka terpadu)
(4) *Enabling a holistic approach* (menerapkan pendekatan yang bersifat holistik)
(5) *Separating governance from management* (pemisahan jelas antara tata kelola dan manajemen).

Selain itu COBIT 5 menerapkan secara spesifik tujuh *enabler* terdiri dari :

1) *Principles, policies and frameworks* (prinsip-prinsip, kebijakan-kebijakan dan kerangka kerja)
2) *Processes* (proses-proses)
3) *Organizational structures* (struktur organisasi)
4) *Culture, ethics and behavior* (budaya, etika dan prilaku)
5) *Information* (informasi)
6) *Services, infrastructure and application* (layanan, infrastruktur dan aplikasi)
7) *People, skills and competencies* (orang, keterampilan dan kompetensi)

COBIT 5 membagi proses ke dalam dua, bagian pertama dinamakan governance terdiri dari 5 proses (EDM-Evaluate, Direct & Monitor) dan 15 kunci praktis tata kelola (key governance practices), bagian kedua dinamakan management terdiri dari 32 proses (APO-Align, Plan & Organize, BAI-Build, Acquire & Implement, DSS-Deliver, Service & Support dan MAE Monitor, Evaluate & Assess) dan 195 kunci praktis manajemen (key management practices).

2.9 Kombinasi Framework COBIT, ITIL dan ISO/IEC 27002

Perbedaan mendasar yang terdapat pada metodologi ITIL adalah bagaimana proses – proses dijelaskan dan ditangani pada setiap aktifitas dan dijelaskan dan ditangani pada setiap aktifitas dan flowchart yang berbeda yang nantinya diharapkan akan memberikan IT dengan efektif dan efisien. Namun, dari sisi *Critical Success Factor*, sementara Cobit menjelaskan dengan lebih detail dan lebih tepat sasaran.

COBIT memiliki struktur yang lebih baik dalam hal mengalamatkan masalah – masalah yang berkaitan dengan *IT Auditing*, dalam hal *IT Auditing* pada COBIT mencakup area yang lebiha luas dan lebih cocok digunakan untuk menilai dan mengevaluasi sebuah IT *Governance*. Fitur – fitur yang dimiliki COBIT dalam penanganan terhadap masalah yang berkaitan dengan manajemen adalah COBIT mampu mereferensikan *Critical Success Factor* yang dibarengi dengan indicator kinerja dan model kapabilitas sebuah IT Governance [17].

ITIL tidak mendukung minat dalam IT (*Strategic Interest of IT*). Dalam hal ini COBIT diakui memiliki struktur IT *Governance* yang lebih baik [15]. Dapat dilihat dalam melakukan komparasi antara COBIT ITIL, keduanya memiliki kesamaan dalam model dan terstruktur dalam kesamaan yang tinggi di bidang IT management, terlebih lagi COBIT di bidang dan terstruktur dalam kesamaan yang tinggi di bidang IT *management*, terlebih lagi COBIT menggunakan metodologi ITIL dalam merombak strukturnya di versi yang terbaru. Ada beberapa masalah yang ditunjukan oleh metodologi ini dan terdapat sedikit perbedaan konotasi yang dapat dilihat dalam tabel berikut :

Table 1.2 Kesamaan Antara Proses ITIL dan COBIT

ITIL	COBIT
Incident Management	*Administrate the problems and incidents*
Problem Management	*Administrate the problems and incidents*
Configuration Management	*Administrate and Configure*
Change Management	*Administrate Change*
IT Services Financial Management	*Identifity and carry out Apropriation Costs*
Capacity Management	*Administrate Performance and Capacity*
Continuity of Service Management	*Ensure Continuity of Services*
Avalaibility Management	*Administrate Performance and Capacity*

Version Management	*Administrate Change and Configuration*
Service Level Management	*Define and Manage Service Level*

Metodologi ITIL memiliki perbedaan pada strukturnya, dapat dilihat sebagai contoh dalam penanganan Incident Management bahwa ITIL memiliki pendekatan yang spesifik dan tidak memiliki bagian yang ekuivalen di dalam kerangka kerja COBIT. Namun, walaupun tidak adanya bagian yang ekuivalen, metodologi COBIT tidak mengalamatkan masalah ini ke bagian lain dalam strukturnya atau COBIT melakukan pendekatan berbeda ITIL menangani masalah ini dengan cara yang sangat detail pada level pemeliharaan jasa dan level *oprating agreements*.

2.10 ITIL dan COBIT dalam Realisasinya dengan ISO/IEC 27002

ISO/IEC 27002 standar banyak digunakan untuk mengatasi masalah yang berkaitan dengan keamanan informasi dan tidak hanya masalah yang terkait dengan manajemen TI. Dengan tujuan umum, jelas bahwa standar ISO/IEC 27002 tidak sesuai dengan yang setara dengan metodologi ITIL seperti yang dapat kita bandingan metodologi ITIL dengan metodologi COBIT. Dalam pelaksanaannya bahwa keamanan dan control dari standar ISO/IEC 27002 dikombinasikan dengan ITIL atau COBIT mengurangi ancaman kritis yang dapat mengganggu hasil proyek.

ISO/IEC 27002 memiliki struktur utamanya untuk diterapkan berdasarkan suatu organisasi dan manajemen keseluruhan keselamatan di semua tingkat keamanan informasi dari suatu organisasi. Masalah administrasi dan manajemen ditangani oleh ITIL dan COBIT, metodologi tidak memiliki standar struktur setara yang dibahas dalam ISO/IEC 27002. Manajemen konfigurasi memiliki dampak yang besar pada lingkungan TI yang harus ditangani. ISO/IEC 27002 memiliki fitur untuk menjaga kerahasiaan, integritas dan ketersediaan informasi dalam organisasi. Ketersediaan informasi ini ditangani dalam ITIL dan COBIT dengan aspek kualitas, keandalan dan pemeliharaan IT yang menekankan bahwa ISO/IEC 27002 bersama – sama dengan ITIL dapat membantu penciptaan proses yang berkaitan dengan pengiriman dan dukungan dari IT. Hal lain yang dapat dibandingkan dengan metodologi ini adalah terkait dengan masalah keuangan, sebagian ISO/IEC 27002 tidak membahas masalah ini secara komprehensif. Hanya berkaita dengan manajeman resiko, meninggalkannya sampai pelaksana untuk mengontrol dan mengurangi risiko untuk

menghindari meningkatnya biaya. Pendekatannya diperlakukan berbeda oleh ITIL dan COBIT, memberikan biaya manajemen resiko yang efektif dan aspek keuangan yang berkaitan dengan IT.

Table 2.3 Metodologi Kombinasi

ITIL	COBIT	ISO/IEC 27002
Konsep/ Proses	Critical Success Factors (CSF)	Information Security
Aktivitas	Metrik (CSF/KPI)	
Biaya / Keuntungan	Good Partice (CMM)	
Perencanaan dan Eksekusi	Audit	

Berdasarkan karakteristik dari masing – masing metodologi ini, kelebihan dan kelemahan framework struktur evaluasi dapat disimpulkan bahwa penggunaan kombinasi metodologi ITL, COBIT dan ISO/IEC 27002 harus dilakukan seperti yang ditunjukkan pada table 2.3 di atas. Tabel 2.3 dibuat dengan membandingkan tujuan pengendalian yang sama antara metodologi ITIL, COBIT dan ISO/IEC 27002. Identifikasi praktik yang baik diantara metode yang terdaftar pada (Tabel 2.3) yaitu penanganan pendekatan ditangani oleh masing – masing tujuan. CSF dalam metodologi COBIT mengatasi sejumlah besar aspek dibandingkan dengan ITIL dan ISO/IEC 27002. Sebagai hasil dari pekerjaan ini saran yang diajukan adalah bahwa metodologi ITIL harus digunakan untuk mendefinisikan strategi, konsep dan proses yang terkait dengan manajemen TI. COBIT harus digunakan untuk mengevaluasi kritis keberhasilan factor, materik, indicator dan audit. Selain itu, standar ISO/IEC 27002 harus memandu pengelolaan TI dalam kaitannya dengan masalah keamanan IT [17].