BAB 2

TINJAUAN PUSTAKA

2.1 Sistem Informasi

Sistem informasi adalah integrasi yang terorganisasi dari teknologi *hardware* dan *software*, data, proses, dan sumber daya manusia yang didesain untuk menghasilkan informasi yang tepat waktu, terintegrasi, relevan, akurat, dan berguna dalam proses pengambilan keputusan dalam perusahaan [5]. Dalam sistem informasi, ada dua jenis komponen, yaitu *Resources* dan *Activities*. *Information System Resources* terdiri atas *people resources* yang merupakan *end users* dan *IS specialist*, *software resources* yang terdiri atas program dan sumber daya yang digunakan, *hardware resources* yang adalah mesin-mesin dan media yang digunakan, *network resources* yang merupakan media komunikasi dan *network support*, dan *data resources* yang terdiri dari basis-basis data dan pengetahuan. Sedangkan *Information System Activities* terdiri dari *input, processing, output, storage,* dan *control* dari *data resources*. *Input* merupakan proses memasukkan data, *processing* berfungsi mengolah data menjadi informasi, *output* merupakan disemasi informasi pada *end users*, *storage* berfungsi sebagai tempat penyimpanan data, dan control merupakan pengawasan umpan balik untuk memastikan sistem dapat memenuhi standar performanya [6].

2.2 *Information Security (InfoSec)*

Information security (InfoSec) atau keamanan informasi merupakan perlindungan aset-aset informasi yang menggunakan, menyimpan, atau

mentransmisikan informasi dari resiko melalui aplikasi kebijakan, pendidikan, dan teknologi [7].

Definisi lain dari *Information security* adalah perlindungan aset organisasi dari penyingkapan atau modifikasi yang tidak sah, baik disengaja atau tidak dan memastikan informasi itu siap saat diperlukan [8]. *Information security* memiliki tiga komponen sentral yang membentuk pilar sebuah keamanan informasi, yaitu *confidentiality, integrity, dan availability*. Ketiga komponen ini membentuk sebuah model keamanan yang disebut *CIA Triangle* [7].

1. *Confidentiality* berarti memastikan bahwa hanya orang-orang yang memiliki *privilege* tertentu yang dapat mengakses informasi tertentu.
2. *Integrity* merupakan jaminan bahwa data masih tetap asli dan belum diubah oleh pihak-pihak yang tidak memiliki izin.
3. *Availibility* adalah membuat informasi dapat diakses oleh user tanpa interferensi atau gangguan dalam format yang dibutuhkan

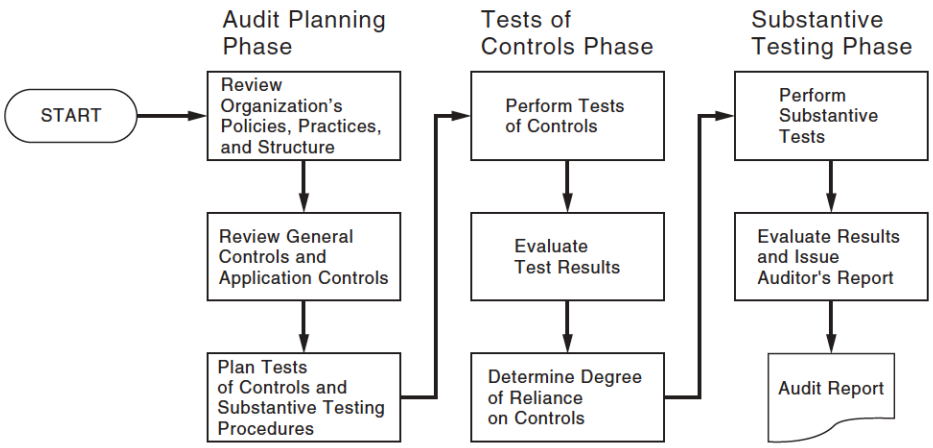
Selain dari tiga komponen pilar diatas, komponen-komponen kunci lain yang juga membentuk *Information Security* adalah *privacy, identification, authentication, authorization*, dan *accountability*.

2.3 Audit Sistem Informasi

Pengertian audit secara umum adalah sebuah proses terpadu mengumpulkan dan melakukan penilaian pada informasi sebagai bagian dari organisasi yang dilakukan oleh seorang ahli [9]. Audit sistem informasi merupakan audit yang terfokus pada aspek-aspek sistem informasi organisasi yang berbasis komputer yang didalamnya sudah termasuk keamanan informasi [10]. Dari kedua penjabaran tersebut dapat disimpulkan bahwa audit keamanan informasi merupakan proses

pengumpulan dan evaluasi pada keamanan sistem informasi berbasis komputer milik organisasi. Secara umum struktur dari audit TI terdiri dari tiga tahap diantaranya,

1. *Audit Planning* – Merupakan langkah pertama dari proses audit. Perencanaan audit meliputi peninjauan pada kebijakan, praktek, dan struktur organisasi; me-*review General Control* dan *Application Control*; dan merencanakan *testing* pada fungsi kontrol dan menyediakan prosedur *testing* yang substansif [10].
2. *Test of Controls* – Bertujuan untuk menentukan apakah kontrol internal yang layak sudah diterapkan dan berfungsi seperti seharusnya. *Test of Controls* dilakukan dengan melakukan beberapa uji kontrol, hasil testing kemudian dievaluasi untuk menentukan tingkat ketergantungan pada kontrol [10].
3. *Substantive Testing Phase* – Melakukan investigasi secara rinci pada transaksi dan *account balance* yang spesifik. Hasil kemudian dievaluasi dan dimasukkan ke dalam laporan auditor yang akan dikeluarkan [10].

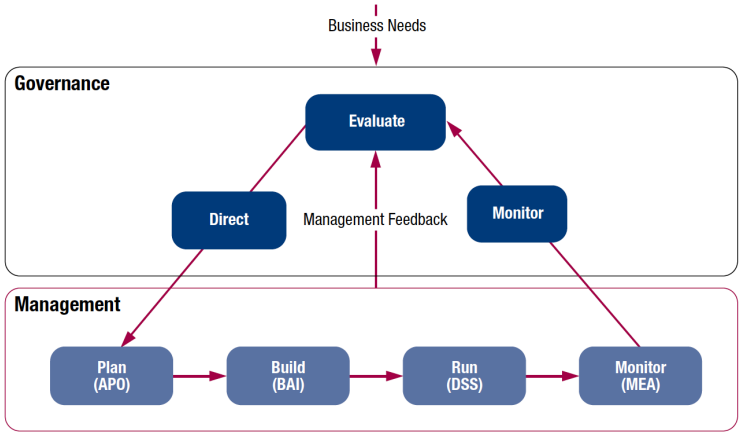


Gambar 2.1 Tahapan Audit TI

2.4 COBIT 5

2.4.1 Definisi Proses COBIT 5

Control Objective for Information and Related Technologies (COBIT) adalah *framework* yang dibuat oleh ISACA untuk mendefinisikan seperangkat proses-proses generik untuk manajemen IT [11]. Keunggulan penggunaan COBIT sebagai *framework information security governance* adalah fungsinya tidak terbatas hanya pada *information security*, tetapi meliputi tata kelola IT secara keseluruhan, sehingga keamanan informasi dapat diintegrasikan kedalam *framework IT Governance* yang lebih luas [2]. COBIT membagi tata kelola IT menjadi 37 proses dan menyediakan *Control Objective* (CO) pada setiap proses. Setiap CO kemudian terbagi menjadi *serangkaian Direct Control Objective* (DCO) yang menspesifikasi bagaimana CO harus dijalankan. Secara total ada 316 DCO untuk 37 proses COBIT [12]. Sedangkan kelemahan COBIT sebagai *framework InfoSec Governance* adalah COBIT tidak memberi petunjuk yang lebih rinci tentang "bagaimana" melakukan hal—hal tertentu. Setiap DCO lebih mengarahkan ke "apa" yang harus dilakukan, padahal di sebagian besar kasus diperlukan tuntunan yang lebih rinci mengenai "bagaimana" sesuatu harus diselesaikan [2].

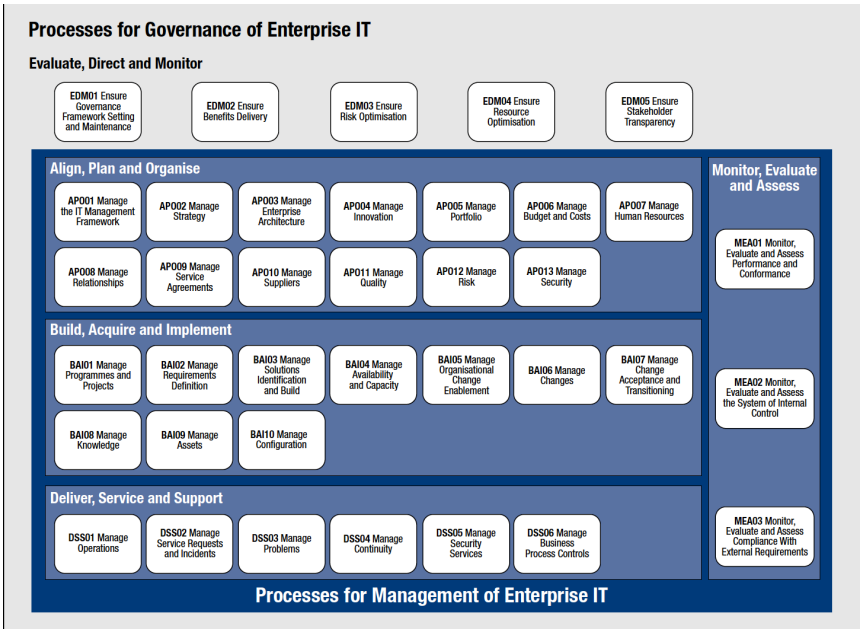


Gambar 2.2 Tata Kelola COBIT 5 dan Manajemen Area Kunci

Saat ini COBIT 5 merupakan versi terbaru dari COBIT yang dikembangkan untuk menyediakan *framework* yang komprehensif untuk membantu perusahaan dalam mencapai tujuan dalam tata kelola dan manajemen IT perusahaan. COBIT 5 dibuat berdasarkan pada lima prinsip kunci, yaitu memenuhi kebutuhan *stakeholder*, meng-*cover* perusahaan *end-to-end*, mengaplikasikan *framework* tunggal yang terintegrasi, memungkinkan pendekatan holistik, dan memisahkan tata kelola dari manajemen [12].

2.4.2 *Domain* COBIT 5.0

COBIT 5 terdiri dari 37 proses tata kelola dan manajemen yang dikelompokkan kedalam area tata kelola dan manajemen. Area tata kelola terdiri dari satu *domain*, yaitu *Evaluate, Direct, and Monitor* (EDM), sedangkan area manajemen terdapat empat *domain*, *yaitu Align, Plan, and Organize* (APO), *Build, Acquire, and Implement* (BAI), *Deliver, Service, and Support* (DSS), dan *Monitor, Evaluate, and Assess* (MEA).



Gambar 2.3 Proses dan *Domain* COBIT 5

Diagram pada Gambar 2.3 menunjukkan pengelompokan *domain-domain* yang terdapat pada COBIT 5. Penjabaran lebih lanjut pada masing-masing *domain* adalah sebagai berikut.

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

Proses ini dapat digunakan oleh perusahaan untuk melakukan evaluasi serta optimasi resiko dan sumber daya dengan tujuan melakukan evaluasi keputusan strategis dan memberi arahan dan melakukan pengawasan pada bagian IT [13]. *Domain* dari proses EDM terdiri atas:

a. EDM01 Memastikan pengaturan dan pemeliharaan *framework IT Governance*

b. EDM02 Menjamin *delivery* manfaat

c. EDM03 Memastikan adanya optimisasi resiko

d. EDM04 Menjamin optimisasi sumber daya

e. EDM05 Memastikan transparansi stakeholder

2 *Align, Plan, and Organize* (APO)

Merupakan proses manajemen untuk memberi arah untuk penyampaian solusi dan ketersediaan layanan [13] . *Domain* APO mencakup strategi, taktik, dan proses untuk mengidentifikasi metode terbaik IT untuk mencapai tujuan perusahaan. *Domain* proses APO terdiri atas

a. APO01 Mengelola *framework* manajemen IT

b. APO02 Mengelola strategi

c. APO03 Mengelola Arsitektur Enterprise

d. APO04 Mengelola inovasi

e. APO05 Mengelola portfolio

f. APO06 Mengelola biaya dan dana

g. APO07 Mengelola SDM

h. APO08 Mengelola relasi

i. APO09 Mengelola persetujuan layanan

j. APO10 Mengelola supplier

k. APO11 Pengelolaan kualitas

l. APO12 Mengelola resiko

m. APO13 Mengelola keamanan

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

Berfungsi memberi solusi dan cara mengimplementasikannya agar dapat menjadi layanan [13]. *Domain* BAI terdiri atas

a. BAI01 Mengelola program dan proyek

b. BAI02 Mengelola definisi syarat

c. BAI03 Mengelola indentifikasi dan pembangunan solusi

d. BAI04 Mengelola ketersediaan dan kapasitas

e. BAI05 Mengelola enabler perubahan organisasi

f. BAI06 Mengelola perubahan

g. BAI07 Mengelola penerimaan perubahan dan proses transisi

h. BAI08 Mengelola knowledge

i. BAI09 Mengelola aset perusahaan

j. BAI10 Mengelola konfigurasi system

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

Berfungsi menyampaikan solusi yang dapat digunakan oleh *end user*. Meliputi layanan dan pengelolaan keamanan dan kelangsungan dukungan *service* bagi *user*, manajemen data, dan operasional [13]. *Domain* DSS meliputi,

a. DSS01 Mengelola operasi
b. DSS02 Mengelola permintaan layanan dan insiden
c. DSS03 Mengelola masalah
d. DSS04 Mengelola keberlangsungan sistem
e. DSS05 Mengelola layanan keamanan
f. DSS06 Mengelola kontrol proses bisnis

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

Berfungsi memonitor seluruh proses untuk memastikan arahan-arahan yang ada pada *domain* sebelumnya diikuti. *Domain* MEA meliputi manajemen kinerja, *internal control*, dan kepatuhan pada regulasi dan tata kelola [13]. *Domain* proses MEA terdiri atas,

a. MEA01 Memonitor, mengevaluasi, dan memeriksa performance dan conformance
b. MEA02 Memonitor, mengevaluasi, dan memeriksa sistem kontrol internal
c. MEA03 Memonitor, mengevaluasi, dan memeriksa kepatuhan dengan pesyaratan external.

Dari 37 proses pada *framework* COBIT 5, ada dua proses yang berhubungan langsung dengan keamanan informasi pada perusahaan, yaitu APO13 dan DSS05.

2.4.3 Fokus Area Penelitian Tata Kelola Keamanan Informasi

Dari 37 proses pada kerangka kerja COBIT 5, ada 2 proses yang menjadi fokus area penelitian dan evaluasi tata kelola keamanan informasi PT XYZ, yaitu APO13 dan DSS05.

2.4.3.1 APO13 – *Manage Security*

Deskripsi proses APO13 adalah untuk mendefinisikan, mengoperasikan, dan memonitor sistem untuk manajemen keamanan informasi. Tujuan dari proses ini adalah untuk menjaga agar dampak dan kejadian insiden keamanan informasi tetap berada pada *level* yang masih dapat diterima [13]. APO13 memiliki tiga *Key Management Practice* diantaranya

1. APO13.01 – *Establish and maintain an information security management system* (ISMS), yaitu untuk membangun dan memelihara ISMS yang menyediakan pendekatan yang standar, formal, dan berkelanjutan pada manajemen keamanan informasi, sehingga memungkinkan adanya teknologi dan proses bisnis yang aman dan sesuai dengan kebutuhan bisnis dan keamanan perusahaan
2. APO13.02 – *Define and manage an information security risk treatment plan*, yaitu memiliki sebuah rencana keamanan informasi yang menggambarkan bagaimana resiko keamanan informasi harus dikelola dan sesuai dengan strategi dan arsitektur perusahaan.
3. APO13.03 – *Monitor and review the ISMS*, yaitu mengkomunikasikan kebutuhan dan keuntungan dari kemajuan dari keamanan informasi secara teratur. Mengumpulkan dan menganalisa data mengenai ISMS, serta memperbaiki ketidaksesuaian untuk mencegah terulangnya insiden.

2.4.3.2 DSS05 – *Manage Security Services*

Proses DSS05 bertujuan untuk melindungi informasi perusahaan untuk menjaga agar *level* resiko keamanan informasi masih dapat diterima perusahaan berdasarkan kebijakan keamanannya. Proses ini bertujuan meminimalisasi dampak bisnis dari *vulnerabilities* dan insiden pada operasional keamanan informasi [13]. Proses ini memiliki tujuh *Key Management Practice*, yaitu

1. DSS05.01 – *Protect against malware*, mengimplementasikan dan memelihara langkah-langkah preventif, detektif, dan korektif di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari malware.
2. DSS05.02 – *Manage network and connectivity security* – Menggunakan langkah-langkah keamanan dan prosedur manajemen lainnya untuk melindungi informasi pada seluruh jaringan *network.*
3. DSS05.03 – *Manage endpoint security*, yaitu memastikan setiap *endpoint* aman pada *level* yang sama atau lebih tinggi dari kebutuhan keamanan yang didefinisikan
4. DSS05.04 – *Manage user identity and logical access*, memastikan semua pengguna memiliki hak akses informasi berdasarkan kebutuhan bisnis setiap *user*.
5. DSS05.05 – *Manage physical access to IT access*, yaitu mendefinisikan dan mengimplementasikan prosedur untuk memberi, membatasi, dan menyangkal akses pada situs, bangunan, dan area berdasarkan kebutuhan bisnis.

6. DSS05.06 – *Manage sensitive document and output devices*, yaitu membuat sistem keamanan fisik, praktek akuntansi, dan manajemen *inventory* yang layak pada aset-aset IT yang sensitif.
7. DSS05.07 – *Monitor the infrastructure for security-related events*, menggunakan *tools-tools* pendeteksi penyusupan, mengawasi infrastruktur dari akses tidak berizin, dan memastikan setiap kejadian diintegrasikan dengan *general event monitoring* dan manajemen insiden.

2.4.2. Pemetaan COBIT 5

Pemetaan COBIT 5 terdiri dari 2 tahap. Tahap pertama adalah memetakan tujuan perusahaan ke dalam *IT-related goals* dan tahap kedua adalah menerjemahkan *IT-related goals* ke dalam *domain-domain* proses COBIT 5.

2.4.2.1. Pemetaan Tujuan Perusahaan Kedalam *IT-Related Goals*

Tujuan tahap ini adalah untuk menunjukkan bagaimana tujuan perusahaan dapat diterjemahkan kedalam *IT-related goals*. Secara keseluruhan COBIT 5 memiliki 17 *IT-related goals*. Dibawah ini merupakan gambaran matriks pemetaan *Enterprise Goals* kedalam *IT-related goals.*

Figure 22—Mapping COBIT 5 Enterprise Goals to IT-related Goals

		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 2.4 Pemetaan Enterprise Goals ke IT-related Goals

2.4.2.2. Pemetaan IT-related Goals Kedalam Proses COBIT 5

Tahap kedua pemetaan COBIT 5 adalah pemtaan *IT-related goals* terhadap proses COBIT5. Dibawah ini adalah gambar matriks pemetaan *IT-related goals* dengan proses COBIT 5.

Figure 23—Mapping COBIT 5 IT-related Goals to Processes

			IT-related Goal																
			Alignment of IT and business strategy	IT compliance and support for business compliance with external laws and regulations	Commitment of executive management for making IT-related decisions	Managed IT-related business risk	Realised benefits from IT-enabled investments and services portfolio	Transparency of IT costs, benefits and risk	Delivery of IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information, processing infrastructure and applications	Optimisation of IT assets, resources and capabilities	Enablement and support of business processes by integrating applications and technology into business processes	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	Availability of reliable and useful information for decision making	IT compliance with internal policies	Competent and motivated business and IT personnel	Knowledge, expertise and initiatives for business innovation
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		COBIT 5 Process	Financial						Customer		Internal							Learning and Growth	
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Ensure Benefits Delivery	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S		S
Align, Plan and Organise	AP001	Manage the IT Management Framework	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	AP002	Manage Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	AP003	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S
	AP004	Manage Innovation	S			S	P			P	P		P	S		S			P
	AP005	Manage Portfolio	P		S	S	P	S	S	S	S		S		P				S
	AP006	Manage Budget and Costs	S		S	S	P	P	S	S			S		S				
	AP007	Manage Human Resources	P	S	S	S			S		S	S	P		P		S	P	P
	AP008	Manage Relationships	P		S	S	S	S	P	S			S	P	S		S	S	P
	AP009	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	P	S		
	AP010	Manage Suppliers		S		P	S	S	P	S	P	S	S		S	S	S		S
	AP011	Manage Quality	S	S		S	P		P	S	S		S		P	S	S	S	S
	AP012	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S
	AP013	Manage Security		P		P		P	S	S		P				P			
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
Monitor, Evaluate and Assess	MEA01	Monitor, Evaluate and Assess Performance and Conformance	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Monitor, Evaluate and Assess the System of Internal Control		P		P		S	S	S		S				S	P		S
	MEA03	Monitor, Evaluate and Assess Compliance With External Requirements		P		P	S		S			S					S		S

Gambar 2.5 Pemetaan IT-related Goals ke COBIT 5 Processes

Dari kedua gambar matriks pemetaan COBIT 5 diatas, dapat dilihat adanya hubungan *primary* (P) dan *secondary* (S) diantara proses-proses COBIT yang ada.

Primary menandakan bahwa hubungan tujuan perusahaan dengan tujuan TI atau hubungan tujuan TI dengan *domain-domain* COBIT 5 adalah penting dan merupakan dukungan utama untuk mencapai tujuan TI perusahaan. *Secondary* menandakan hubungan diantara proses-proses kuat tetapi kurang penting.

2.4.3. COBIT 5 Process Assessment Model (PAM)

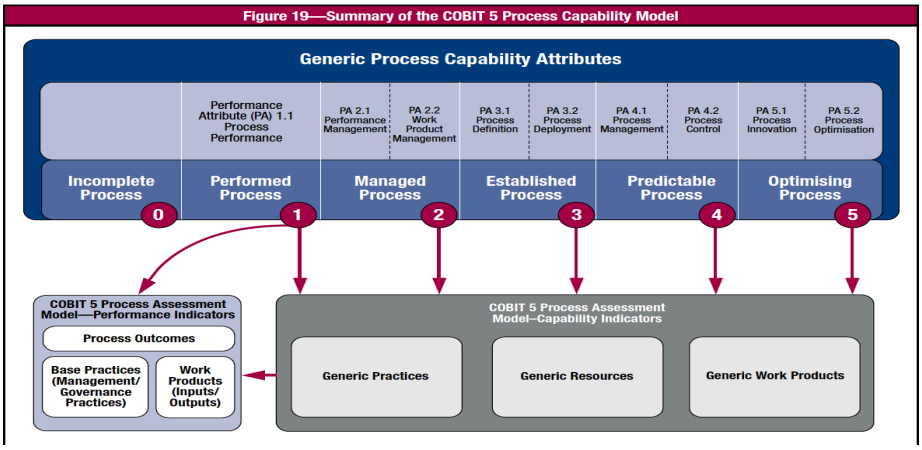
Process Assessment Model atau model penilaian proses merupakan dasar atau panduan untuk melakukan evaluasi pada kemampuan proses TI suatu perusahaan terhadap COBIT 5 [12]. Dalam *framework* COBIT 5, model ini juga *disebut Process Capability Model (PAM)*. Penilaian pada kapabilitas proses dalam COBIT 5 didasarkan pada standar ISO/IEC 15504. Penilaian ini bertujuan untuk menemukan tingkatan atau derajat kematangan/kapabilitas tata kelola TI suatu organisasi [14]. COBIT 5 PAM terdiri atas satu set indikator kinerja dan kemampuan proses yang dapat digunakan sebagai pedoman untuk mengumpulkan informasi-informasi serta bukti objektif yang mendukung proses evaluasi [12].

Dalam COBIT 5 PAM, ada 6 tingkat atau derajat kematangan atau kapabilitas yang dapat dicapai sebuah proses, mulai dari 0 (proses tidak selesai) sampai 5 (proses teroptimisasi).

- 0 (*Incomplete process*) – Proses tidak diimplementasikan atau gagal mencapai tujuan
- 1 (Performed process) – Proses yang diterapkan berhasil mencapai tujuan dari proses tersebut.
- 2 (*Managed process*) – Proses telah diimplementasikan dengan cara yang lebih teratur dan produk-produk kerjanya telah dibangun, dikendalikan, dan dirawat dengan baik.

- 3 (*Established process*) – Proses pada *level* sebelumnya diimplementasikan dengan mengikuti proses yang telah didefinisikan sehingga memungkinkan untuk mencapai tujuan dari proses itu sendiri.
- 4 (*Predictable process*) – Proses pada *level* sebelumnya telah beroperasi didalam batasan-batasan yang sudah terdefinisikan untuk mencapai hasil dari proses.
- 5 (*Optimizing process*) – Proses sudah dapat berkembang (improve) secara terus menerus untuk memenuhi sasaran bisnis masa kini yang relevan dan sasaran yang sudah diproyeksikan.

Keseluruhan model penilaian proses COBIT 5 dapat dijabarkan seperti pada Gambar 2.6.



Gambar 2.6 *COBIT 5 Process Capability Model*

2.5 *Information Security Culture*

Setiap organisasi atau perusahaan masing-masing memiliki kebiasaan dan kode etik tertentu yang beragam yang disebut sebagai budaya perusahaan atau *corporate culture*. Definisi *corporate culture* adalah nilai-nilai atau keyakinan yang dimiliki bersama oleh orang-orang dalam perusahaan serta berfungsi mengarahkan semua aktivitas dalam perusahaan tersebut. Nilai-nilai serta kebiasaan yang ada dalam

perusahaan memiliki pengaruh pada bagaimana setiap individu menjalankan tugas sehari-harinya dan juga bagaimana setiap individu menafsirkan kebijakan perusahaan serta bagaimana cara mengimplementasikan prosedur [15].

Dari penjabaran diatas, dapat ditarik kesimpulan *information security culture* atau budaya keamanan informasi adalah nilai-nilai, kebiasaan, dan etik dalam perusahaan yang mengarahkan aktivitas-aktivitas yang berkaitan dengan implementasi tata kelola keamanan informasi perusahaan, termasuk pendekatan keamanan yang diterapkan perusahaan.

2.6 Penelitian Terdahulu

Tabel 2.1 Referensi Penelitian Sejenis

Judul Jurnal	Penulis/Tahun	Hasil	Kesimpulan
Information Security Governance: When Compliance Becomes More Important than Security	Terence C.C. Tan, Anthonie B. Ruighaver, and Atif Ahmad (2010). *IFIP Advances in Information and Communication Technology.*	Penelitian dan pengumpulan data dilakukan secara kualitatif dengan interview pada beberapa personel IT perusahaan. Hasil dari interview menunjukkan bahwa ITUM menggunakan pendekatan *InfoSec* yang sentralistik dan cenderung mengedepankan compliance, sehingga menyebabkan staff IT memiliki keterlibatan yang terbatas dalam pembuatan strategi dan kebijakan keamanan tingkat tinggi	Analisis dari studi kasus perusahaan ITUM menyimpulkan bahwa pendekatan keamanan yang sentralistik menyebabkan terjadinya beberapa efek negatif dalam perusahaan, yaitu kurangnya diversity in decision making, mission statement level eksekutif yang kabur, serta security governance dan *IT governance* yang tidak terintegrasi.
Evaluation of Information Technology Governance using COBIT 5 *Framework* Focus APO13 and	Suryo Suminar, Fitroh, dan Suci Ratnawati (2014). *2014 International Conference on Cyber and IT*	Hasil penelitian secara kualitatif dan kuantitatif pada kapabilitas *IT governance* dari PPIKSN secara keseluruhan	Bagian *computer network* and data communication dari PPIKSN disarankan untuk memiliki dokumentasi RACI

DSS05 in PPIKSN-BATAN	*Service Management.*	menggunakan Process Assessment Model menunjukkan value kapabilitas 1,96 di APO13 dan 1,71 pada DSS05 atau kapabilitas *level* 2 (Managed Process). Sedangkan penelitian khusus pada bagian Computer Network and Data Communication menunjukkan nilai APO13=2.96 dan DSS05=2.71 atau berada pada *level* 3.	*chart* dalam membangun dan mengelola ISMS dan untuk memlihara keamanan operasional. Selain itu PPIKSN juga dianjurkan agar kebijakan dan standar dari tujuan organisasi diselaraskan, serta memiliki minimum labor *standard*, dan standar dalam implementasi prosedur untuk membangun dan mengelola ISMS.
The Effectiveness of COBIT 5 Information Security *Framework* for reducing Cyber Attacks on Supply Chain Management System	Mark Wolden, Raul Valverde, dan Malleswara Talla (2015). *IFAC-PapersOnLine*	Penelitian ini menemukan bahwa manajemen memiliki pengaruh pada sistem keamanan dari SCMS. Selain itu, penelitian juga mendemonstrasikan bahwa kemauan admin untuk mem-back up program keamanan informasi melalui penegakan aturan dan konsistensi memiliki pengaruh langsung pada efektivitas dari implementasi *framework* SI dalam mencegah serangan siber pada SCMS.	Terdapat beberapa hal yang mempengaruhi efektifitas penerapan *framework* COBIT 5, yaitu masalah manajemen aturan, tanggung jawab, dan kebijakan serta struktur hiearki dalam organisasi. Para manajer juga memiliki peran krusial dalam keamanan SI karena mereka dapat mempengaruhi pendekatan yang diambil oleh karyawan lain.
Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5	Dewi Ciptaningrum, Eko Nugroho, dan Dani Adhipta (2015). *Sentika*	Hasil pengukuran kapabilitas keamanan SI menunjukkan dari kelima proses yang diukur tidak ada yang mencapai target, yaitu *level* 3. Bahkan kelima proses hanya dapat mencapai *level* 1.	Hasil dari 5 proses tingkat kapabilitas SI semua berada pada *level* kapabilitas 1 (*Performed Process*) dengan 4 proses berada pada *level* P (*Partially Achieved*), yaitu

			EDM03, APO12, APO13, dan BAI06 serta 1 proses ada pada *level* L (*Largely Achieved*), yaitu DSS05
Audit Sistem Informasi *Front Office* Pada World Hotel Menggunakan Kerangka Kerja COBIT 4.1	Tika Pradini, Johanes Fernandes Andry (2018). *Ikraith-Informatika*	Hasil penelitian menemukan bahwa maturity *level* DS5, DS11, dan DS13 berada pada *level* 2 sedangkan DS7 dan DS12 ada pada *level* 1 (masih dibawah expected *level*).	Penelitian ini menyimpulkan bahwa ada kesenjangan antara maturity *level* SI saat ini dengan expected *level* yang diinginkan. Nilai tertinggi masih berada di *level* 2, sedangkan expected *level* yang diharapkan pada *level* 3
Evaluasi Kapabilitas Keamanan Teknologi Informasi pada Proses APO13 dan DSS05 berdasarkan *Framework* Cobit 5 (Studi pada Dinas Komunikasi dan Informatika Kota Malang)	Muhammad Fariz Arizali Effendi, Andi Reza Perdanakusuma, dan Buce Trias Hanggara (2020). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer.*	Penelitian menunjukkan tingkat kapabilitas APO13 *level* 1 sebesar 64% (*largely achieved*) dan DSS05 *level* 1 sebesar 32% (*partially achieved*) sehingga evaluasi tidak dapat dilanjutkan pada level berikutnya (berhenti di *level* 1)	Hasil dari observasi dan wawancara menunjukkan proses APO13 berada pada *level* 1, sedangkan DSS05 berada di *level* 0, sehingga keduanya berada dibawah *expected level* yang diharapkan DISKOMINFO (*level* 2).

Beberapa jurnal yang terdapat pada tabel tersebut memiliki judul dan tujuan yang berbeda, tetapi lima dari enam jurnal tersebut memiliki banyak kesamaan dalam hal pembahasan, referensi, dan metode penelitian sehingga dapat digunakan sebagai acuan dalam penelitian ini.

Jurnal berjudul "*Information Security Governance: When Compliance Becomes More Important than Security*" yang ditulis oleh Terrence Tan, Anthoine B. Ruighaver, dan Atif Ahmad menggunakan metodologi penelitian kualitatif

dengan mewawancarai beberapa anggota staff TI perusahaan ITUM. Hasil wawancara kemudian dianalisa untuk menemukan hubungan antara pendekatan keamanan informasi yang diterapkan perusahaan dengan performa dari para staff IT perusahaan. Kesimpulan penelitian ini adalah bahwa pendekatan keamanan informasi yang sentralistik perusahaan ITUM menyebabkan munculnya beberapa dampak negatif, seperti kurangnya keragaman dalam pengambilan keputusan, *mission statement* eksekutif yang kurang jelas, serta tata kelola keamanan dan TI yang tidak terintegrasi.

Penelitian lain yang dilakukan Suryo Suminar, Fitoh, dan Suci Ratnawati menggunakan metode wawancara dan observasi untuk mendapat hasil penelitian untuk dianalisa dengan *COBIT Process Assessment Model* untuk mengevaluasi tingkat kepabilitas *domain-domain* yang menjadi fokus proses (DSS05 dan APO13) pada PPIKSN-BATAN. Kesimpulan dari penelitian ini adalah bahwa PPIKSN-BATAN disarankan untuk memiliki dokumentasi *RACI chart* dalam mengelola ISMS serta melakukan penyelarasan pada kebijakan dan standar dari tujuan organisasi [16].

Studi yang hampir sama juga dilakukan oleh Muhammad Fariz Arizali Effendi, Andi Reza Perdanakusuma, dan Buce Trias Hanggara pada tahun 2020. Penelitian tersebut menggunakan domain yang sama, yaitu APO13 dan DSS05 dengan objek DISKOMINFO Malang. Penelitian ini menyimpulkan bahwa DISKOMINFO Malang masih belum mencapai tingkat kapabilitas keamanan informasi yang diharapkan (*level* 2) dan peneliti memberi 13 butir rekomendasi perbaikan pada APO13 dan 15 butir pada DSS05 [17].

Mark Wolden, Raul Valverde, dan Malleswara Talla melakukan penelitian yang bertujuan untuk menganalisa efektivitas *framework* keamanan informasi COBIT5 dalam mengurangi *cyber attack* pada sistem *supply chain management (SCM)* dengan menggunakan metode kuesioner yang kemudian dianalisis untuk mendapat hasil. Kesimpulan penelitian tersebut adalah manajemen perusahaan memiliki pengaruh yang krusial dalam meningkatkan efektivitas dari sistem keamanan pada sistem SCM perusahaan, terutama dalam mencegah serangan siber [18].

Pada jurnal "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5" yang disusun Dewi Ciptaningrum, Eko Nguroho, dan Dani Adhipta, penelitian dilakukan dengan metode pengisian kuesioner yang kemudian dianalisa menggunakan *Process Assessment Model* untuk mendapatkan tingkat kapabilitas keamanan SI pada *domain* EDM03, APO12, APO13, BAI06, dan DSS05. Kesimpulan yang ditarik dari penelitian ini menemukan bahwa tingkat kapabilitas keamanan SI pada kantor pemerintah kota Yogyakarta masih belum mencapai tingkatan target yang diinginkan.

Penelitian lain yang hampir serupa juga dilakukan oleh Tika Pradini dan Johanes Fernandes Andry dalam mengaudit sistem informasi pada *front office* World Hotel yang juga dilakukan dengan pengisian kuesioner dan dianalisa dengan Process Assessment Model untuk mencari tingkat kapabilitas SI [19]. Namun kerangka yang digunakan pada penelitian ini adalah COBIT 4.1. Penelitian ini menyimpulkan bahwa ada kesenjangan antara tingkat kematangan SI saat ini dengan target yang ingin dicapai.

Berdasarkan jurnal-jurnal penelitian terdahulu, ada 4 penelitian yang memiliki kriteria yang paling sesuai dan berhubungan dengan penelitian ini. Jurnal yang pertama adalah penelitian yang dilakukan oleh Tan, Ruighaver, dan Ahmad mengenai pendekatan keamanan yang diterapkan perusahaan ITUM serta hubungannya dengan performa staff IT perusahaan. Tiga jurnal lain yang juga memiliki keterkaitan langsung pada penelitian yang dilakukan pada PT XYZ adalah jurnal tentang penelitian yang dilakukan terhadap PPIKSN-BATAN, pengukuran keamanan informasi pada DISKOMINFO Malang, dan jurnal mengenai audit keamanan informasi pada kantor pemerintah kota Yogyakarta. Ketiga penelitian yang terdapat pada ketiga jurnal ini dilakukan secara kuantitatif dengan metode observasi dan kuesioner yang dokumentasinya dilakukan dengan menggunakan *Process Assessment Model,* dengan dua jurnal yang pertama melakukan pengukuran pada proses APO13 dan DSS05 atau sama dengan yang dilakukan penelitian in