BAB II. LANDASAN TEORI

2.1 Audit Sistem Informasi

Audit sistem informasi merupakan proses pengumpulan dan pengevaluasian bukti-bukti untuk menentukan apakah suatu sistem aplikasi komputerisasi telah menetapkan dan menerapkan sistem pengendalian intern yang memadai, semua aktiva dilindungi dengan baik atau tidak disalahgunakan serta terjaminnya integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer tersebut. Audit sistem informasi juga memiliki tujuan sebagai berikut.

1. Pengamatan aset

   Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, *file /* data dan fasilitas lain harus dijaga dengan sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Efektifitas sistem

   Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut dirancang dengan benar (*doing the right thing*), telah sesuai dengan kebutuhan *user*. Informasi yang dibutuhkan oleh para manajer dapat dipenuhi dengan baik.

3. Efisiensi sistem

   Efisiensi menjadi sangat penting ketika sumber daya kapasitasnya terbatas. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya informasi yang minimal.

4. Ketersediaan

   Berhubungan dengan ketersediaan dukungan/layanan teknologi informasi (TI). TI hendaknya dapat mendukung secara kontinyu terhadap proses bisnis kegiatan perusahaan. Makin sering terjadi gangguan (*system down*) maka berarti tingkat ketersediaan sistem rendah.

5. Kerahasiaan

   Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindungi dari akses pihak-pihak yang tidak berwenang.

6. Kehandalan

   Berhubungan dengan kesesuaian dan keakuratan bagi manajemen dalam pengelolaan organisasi, pelaporan, dan pertanggungjawaban.

7. Menjaga integritas data

   Integritas data (*data integrity*) adalah salah satu konsep dasar sistem informasi. Data memilik atribut-atribut seperti: kelengkapan, kebenaran, dan keakuratan. Jika integritas data tidak terpelihara, maka suatu perusahaan tidak akan lagi memiliki informasi/laporan yang benar, bahkan perusahaan dapat menderita kerugian karena pengawasan tidak tepat atau keputusan-keputusan yang salah.

Faktor utama yang membuat data berharga bagi organisasi dan pentingnya untuk menjaga integritas data adalah :

a. Makna penting data/informasi bagi pengambilan keputusan. Peningkatan data sehingga dapat memberikan informasi bagi para pengambil keputusan.
b. Nilai data bagi pesaing, jika data tersebut berguna bagi pesaing maka kehilangan data akan memberikan dampak buruk bagi organisasi tersebut. Pesaing dapat menggunakan data tersebut untuk mengalahkan organisasi sehingga mengakibatkan organisasi menjadi kehilangan pasar (*market*), berkurangnya keuntungan, dan sebagainya (Sanyoto, 2015).

2.2 Keamanan Informasi

Keamanan informasi merupakan penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi resiko bisnis (*reduce business risk*), dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Pengamanan informasi juga merupakan suatu proses perlindungan terhadap informasi untuk memastikan beberapa hal berikut ini.

1. Kerahasiaan (*confidentiality*) : memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki wewenang.
2. Integritas (*integrity*) : memastikan bahwa informasi tetap akurat dan lengkap, serta informasi tersebut tidak dimodifikasi tanpa otorisasi yang jelas.
3. Ketersediaan (*availability*) : memastikan bahwa informasi dapat diakses oleh pihak yang memiliki wewenang ketika dibutuhkan.

Pengamanan informasi tersebut dapat dicapai dengan melakukan suatu kontrol yang terdiri dari kebijakan, proses, prosedur, struktur organisasi, serta fungsi-fungsi infrastruktur TI (Sarno, 2009).

2.3 *Framework COBIT*

Framework COBIT (*Control Objectives for Information and Related Technology*) adalah kerangka kerja tata kelola IT (*IT Governance Framework*) dan kumpulan perangkat yang mendukung dan memungkinkan para manager untuk menjembatani jarak (*gap*) yang ada antara kebutuhan yang dikendalikan (*control requirement*), masalah teknis (*technical issues*) dan resiko bisnis (*bussiness risk*). *COBIT* mempermudah perkembangan peraturan yang jelas (*clear policy development*) dan praktik baik (*good practice*) untuk mengendalikan IT dalam organisasi. *COBIT* menekankan keputusan terhadap peraturan, membantu organisasi untuk meningkatkan nilai yang ingin dicapai dengan penggunaan IT, memungkinkan untuk menyelaraskan dan menyederhanakan penerapan dari kerangka *COBIT*. *COBIT* muncul pertama kali pada tahun 1996, yaitu *COBIT* versi 1 yang menekankan pada bidang audit, *COBIT* versi 2 pada tahun 1998 yang menekankan pada tahap control, *COBIT* versi 3 pada tahun 2000 yang berorientasi kepada manajemen, *COBIT* versi 4 yang lebih mengarah pada IT *Governance*, dan terakhir dirilis adalah *COBIT* versi 5 pada tahun 2012 yang mengarah pada tata kelola dan menejemen untuk aset-aset perusahaan IT. Konsep dasar kerangka kerja *COBIT* adalah sebagai penentu kendali dalam TI berdasarkan informasi yang dibutuhkan untuk mendukung tujuan bisnis dan informasi yang dihasilkan dari gabungan penerapan proses TI dan sumber daya terkait. Dalam penerapan pengelolaan TI

terdapat dua jenis model kendali, yaitu model kendali bisnis (*business controls model*) dan model kendali TI (*IT focused control model*), *COBIT* mencoba untuk menjembatani kesenjangan dari kedua jenis kendali tersebut. *Framework COBIT* 5 terdiri atas 5 domain, yaitu :

1. EDM (*Evaluate, Direct and Monitor*)
2. APO (*Align, Plan and Organise*)
3. BAI (*Build, Acquire and Implement*)
4. DSS (*Deliver, Service, and Support*)
5. MEA (*Monitor, Evaluate and Assess*)

COBIT dirancang terdiri dari 37 proses bisnis yang menggambarkan proses TI yang terdiri dari 5 domain. Berikut ini adalah penjelasan proses bisnis dari masing-masing domain.

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

   Proses tata kelola ini berkaitan dengan tujuan tata kelola pemangku kepentingan dalam melakukan penilaian, optimasi risiko, dan sumber daya mencakup praktek dan kegiatan yang bertujuan untuk mengevaluasi pilihan strategis, memberikan arahan kepada TI dan pemantasan hasilnya. Proses bisnis yang terdapat pada domain EDM dijabarkan pada tabel 2.1.

Tabel 2.1 Proses Bisnis Pada Domain EDM

Kode Domain	Sub Domain
EDM01	*Ensure Governance Framework Setting and Maintenance*
EDM02	*Ensure Benefits Delivery*
EDM03	*Ensure Risk Optimisation*
EDM04	*Ensure Resource Optimisation*
EDM05	*Ensure Stakeholder Transparency*

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

   Memberikan arah untuk pengiriman solusi (BAI) dan penyediaan layanan dan dukungan (DSS). Domain ini mencakup strategi dan taktik, serta mengidentifikasi kekhawatiran cara terbaik TI agar dapat berkontribusi pada pencapaian tujuan bisnis. Realisasi visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perpektif yang berbeda. Sebuah organisasi yang tepat, serta infrastruktur teknologi harus dimasukkan kedalam tempatnya. Proses bisnis pada domain APO dapat dilihat pada tabel 2.2.

Tabel 2.2 Proses Bisnis Pada Domain APO

Kode Domain	Sub Domain
APO01	*Manage the IT Management Framework*
APO02	*Manage Strategy*
APO03	*Manage Enterprise Architecture*
APO04	*Manage Innovation*
APO05	*Manage Portfolio*

APO06	*Manage Budget and Costs*
APO07	*Manage Human Resources*
APO08	*Manage Relationships*
APO09	*Manage Service Agreements*
APO010	*Manage Suppliers*
APO011	*Manage Quality*
APO012	*Manage Risk*
APO013	*Manage Security*

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

   Memberikan solusi dan melewatinya sehingga akan berubah menjadi layanan. Untuk mewujudkan strategi TI, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan terintegrasi ke dalam proses bisnis. Perubahan dan pemeliharaan sistem yang ada juga dicakup oleh domain ini, untuk memastikan bahwa solusi terus memenuhi tujuan bisnis. Proses bisnis pada domain BAI dapat dilihat pada tabel 2.3.

Tabel 2.3 Proses Bisnis Pada Domain BAI

Kode Domain	**Sub Domain**
BAI01	*Manage Programmes and Projects*
BAI02	*Manage Requirements Definition*
BAI03	*Manage Solutions Identification and Build*

BAI04	*Manage Availability and Capacity*
BAI05	*Manage Organisational Change Enablement*
BAI06	*Manage Changes*
BAI07	*Manage Change Acceptance and Transitioning*
BAI08	*Manage Knowledge*
BAI09	*Manage Assets*
BAI010	*Manage Configuration*

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

   Meliputi mengirimkan, layanan, dan dukungan atau memberi pelayanan yang aktual bagi bisnis, termasuk manajemen data dan proteksi informasi yang berhubungan dengan proses bisnis. Proses bisnis pada domain DSS dapat dilihat pada tabel 2.4.

Tabel 2.4 Proses Bisnis Pada Domain DSS

Kode Domain	Sub Domain
DSS01	*Manage Operations*
DSS02	*Manage Service Requests and Incidents*
DSS03	*Manage Problems*
DSS04	*Manage Continuity*
DSS05	*Manage Security Service*
DSS06	*Manage Business Process Controls*

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

   Menerima solusi dan dapat digunakan bagi pengguna akhir. Domain ini berkaitan dengan pengiriman *actual* dan dukungan layanan yang dibutuhkan, yang meliputi pelayanan, pengelolaan keamanan dan kelangsungan, dukungan layanan bagi pengguna, dan manajemen data serta fasilitas operasional. Proses bisnis pada domain MEA dapat dilihat pada tabel 2.5.

Tabel 2.5 Proses Bisnis Pada Domain MEA

Kode Domain	Sub Domain
MEA01	*Monitor, Evaluate and Assess Performance and Conformance*
MEA02	*Monitor, Evaluate and Assess the System of Internal Control*
MEA03	*Monitor, Evaluate and Assess Compliance with External Requirements*

2.4 Pemetaan Proses Bisnis

Untuk menentukan proses bisnis yang akan digunakan peneliti, diperlukan pemetaan antara *enterprise goals*, IT *related goals*, dan proses bisnis. Contoh pemetaan *enterprise goals* dapat dilihat pada gambar 2.1.

Figure 5—COBIT 5 Enterprise Goals				
		Relation to Governance Objectives		
BSC Dimension	Enterprise Goal	Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Gambar 2.1 *Enterprise goals*

Berikut ini merupakan contoh pemetaan IT *related goals* dapat dilihat pada gambar 2.2.

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 2.2 *Mapping enterprise goals to IT related goals*

Berikut ini merupakan contoh pemetaan proses bisnis dapat dilihat pada gambar 2.3.

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	APO01	Manage the IT Management Framework	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Manage Strategy	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Manage Enterprise Architecture	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Manage Innovation	S			S	P			P	P		P	S		S			P
	APO05	Manage Portfolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Manage Budget and Costs	S		S	S	P	P	S	S			S		S				
	APO07	Manage Human Resources	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Manage Relationships	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Manage Service Agreements	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Manage Suppliers		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Manage Quality	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Manage Risk		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Manage Security		P		P		P	S	S		P				P			

Gambar 2.3 *Mapping IT related goals to processes*

(Sumber : ISACA, 2013)

2.5 Studi Literatur

Berikut adalah bahan studi literatur di dalam penelitian ini.

1. Audit Keamanan Sistem Informasi Pada Kantor Pemerintahan Kota Yogyakarta Menggunakan COBIT 5 (Ciptaningrum, Nugroho, & Adhipta, 2015).
   a. Masalah

      Permasalahan yang dikaji dalam penelitian ini adalah perlu adanya standar operasional dan prosedur manajemen pengamanan sistem informasi dan telekomunikasi dilingkungan pemerintahan Yogyakarta dengan menggunakan *Framework* COBIT 5 sebagai metode untuk mewujudkan standar pengamanan manajemen sistem informasi dan telekomunikasi di pemerintahan kota Yogyakarta.

   b. Hasil dan pembahasan

      Berdasarkan hasil penilaian tingkat kapabilitas keamanan Sistem Informasi (SI) tidak dapat ditargetkan dalam jangka pendek, yaitu level 3. Berdasarkan hasil penilaian tingkat kapabilitas keamanan Sistem Informasi (SI) pada Pemerintahan Kota Yogyakarta, hasil dari lima (5) proses tingkat kapabilitas keamanan SI, yaitu semua proses berada pada tingkat kapabilitas 1 (*performed process).*

2. Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan *Framework* COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk) (Mufti & Mursityo, 2017).

a. Masalah

PT Martina Berto Tbk adalah perusahaan manufaktur, pemasaran, penelitian dan pengembangan yang ada di Martha Tilaar Group. Saat ini perusahaan telah menerapkan sistem dan teknologi informasi dalam mendukung operasional perusahaan yang dilaksanakan oleh departemen *Corporate* IT. Tetapi, terdapat beberapa kekurangan dalam penerapan tersebut khususnya dalam hal keamanan seperti *security incident* yang kerap muncul serta serangan ke server perusahaan. Untuk mencegah hal-hal tersebut terjadi lagi, maka perlu diketahui sejauh mana tata kelola sistem keamanan teknologi informasi perusahaan dengan cara melakukan evaluasi, karena dengan adanya evaluasi dapat dihasilkan rekomendasi berupa tindakan-tindakan apa yang harus dilakukan agar hal-hal tersebut tidak terjadi lagi.

b. Hasil dan pembahasan

Hasil penelitian menunjukan *Capability Level* pada domain proses APO13 dan DSS05 *Framework* COBIT 5 berada pada level 1, sedangkan *capability level* yang diinginkan pada kedua domain proses adalah level 2, sehingga menyisakan *gap* sebesar 1. Setelah mengetahui *capability level* saat ini dan yang diinginkan, maka dibuatkan rekomendasi berdasarkan analisis SWOT. Rekomendasi yang diberikan seperti pembentukan unit khusus keamanan informasi, membuat dokumen terkait pengelolaan dan peningkatan keamanan informasi dan penaganan risiko keamanan informasi, membuat

dokumen standar operasional layanan keamanan serta melakukan pembaruan teknis teknologi informasi dan pemantauan secara rutin.

3. Audit Tata Kelola Teknologi Informasi Berbasis COBIT 5 (DSS05) Untuk Evaluasi Keamanan Sistem Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Kendal (Sari & Sari, 2016).

   a. Masalah

      Permasalahan yang dikaji dalam penelitian ini adalah pada Dinas Kominfo Kabupaten Kendal belum mendefinisikan secara jelas terkait *Standard Operasional Prosedur* (SOP) pada sistem informasi serta pada pengolahan/penyimpanan data, tidak rutin melakukan *monitoring back up* data, serta jaringan yang tidak stabil dan putusnya koneksi secara tiba-tiba juga menjadi permasalahan pada jaringan dan *server*. *Framework* yang digunakan dalam penelitian ini adalah COBIT 5 sebagai metode untuk mewujudkan standar pengamanan informasi di Dinas Kominfo Kabupaten Kendal.

   b. Hasil dan pembahasan

      Ditemukannya selisih *gap* sebesar 0,24 antara tingkat kapabilitas saat ini dan yang akan dicapai dengan target yang akan dicapai. Strategi perbaikan yang dapat dilakukan Dinas Kominfo Kabupaten Kendal untuk mencapai tingkat kapabilitas 3 adalah dengan memperbaiki kriteria pemenuhan dari setiap level 1 sampai 3 yang dapat dilakukan secara bertahap.

4. Audit Sistem Informasi Menggunakan Pendekatan Cobit 5.0dan Itil V3 Pada Sistem Informasi Akademik (Aziz & Nurlistiani, 2018)

   a. Masalah

      Mengevaluasi tata kelola sistem informasi akademik (siska) di institut informatika dan bisnis darmajaya untuk menghasilkan beberapa rekomendasi dengan menggunakan *framework* cobit 5 dan itil v3”

   b. pembahasan

      Hasil pengukuran tingkat kematangan SISKA IIB Darmajaya pada domain DSS-01, DSS-02, DSS-03, DSS-04, DSS-05, DSS-06, MEA-01, APO-12, dan APO-13 pada saat ini SISKA IIB Darmajaya adalah sebesar 2,48 dengan tingkat *capability Managed.* Sedangkan pengukuran untuk tingkat kematangan pada kondisi harapan adalah sebesar 4,44 dengan tingkat *capability Predictable.*