PERANCANGAN ALAT UKUR TINGKAT KAPABILITAS MANAJEMEN RISIKO KEAMANAN INFORMASI BERDASARKAN COBIT 5

Carena Learns Prasetyo, Siti Mukaromah
Program Studi Sistem Informasi Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur
Email: carenalearns24@gmail.com

Abstrak. *Ada berbagai cara untuk meningkatkan kinerja organisasi dalam memenuhi kebutuhan dalam bisnisnya. Salah satu kebutuhan yang menjadi bagian yang sangat penting dalam organisasi adalah informasi. Perlu adanya teknologi informasi sebagai alat bantu meningkatkan efisiensi pengerjaan. Namun dalam penerapannya TI tidak selalu menjadi solusi yang baik, muncul berbagai risiko yang dapat menjadi hambatan dan kerugian bagi organisasi. Salah satu organisasi yang bertanggung jawab dalam pengelolaan informasi adalah Lembaga XYZ. Telah terdapat beberapa SOP atau kebijakan yang mengatur penggunaan, perawatan, dan keamanan TI pada Lembaga XYZ. Namun masih ditemukan beberapa aktivitas yang belum mencapai target perencanaan kinerja, khususnya dalam manajemen risiko keamanan informasi pada Sistem Informasi Pengelolaan Surat (SIPS). Maka dari itu untuk meminimalisir kerugian dan mencegah risiko yang akan terjadi, pengukuran tingkat kapabilitas manajemen risiko keamanan informasi harus dilakukan. Penelitian ini bertujuan untuk merancang alat ukur manajemen risiko keamanan informasi dari SIPS berdasarkan COBIT 5. Domain yang terpilih adalah EDM03 (Ensure Risk Optimisation) dan APO12 (Manage Risk). Hasil penelitian ini berupa alat ukur tingkat kapabilitas manajemen risiko keamanan informasi yang didasarkan pada metode Process Assessment Model (PAM) COBIT 5 yang dapat digunakan Lembaga XYZ atau peneliti lainnya untuk melakukan pengukuran secara mandiri. Hasil dari pengukuran dapat menjadi tolak ukur untuk meningkatkan manajemen risiko keamanan informasi.*

Kata Kunci: manajemen risiko, keamanan informasi, SIPS, tingkat kapabilitas, COBIT 5, process asessment model.

Perkembangan dunia teknologi informasi semakin pesat diiringi dengan tuntutan untuk pemenuhan kebutuhan yang tepat dan cepat. Organisasi menjadi salah satu pelaku pemanfaatan TI untuk menunjang kebutuhan bisnisnya. Ada berbagai proses bisnis yang terbantu berkat kehadiran teknologi informasi. Salah satu pemenuhan yang membutuhkan keakuratan dan kecepatan yang menjadi sangat penting untuk diperhatikan organisasi adalah informasi[1]. Lembaga XYZ merupakan salah satu organisasi yang berperan penting dalam pengolahan informasi. Dalam organisasinya mereka menyediakan Sistem Informasi Pengelolaan Surat (SIPS) untuk memudahkan setiap staf berkomunikasi utamanya dalam penyampaian hasil pertemuan, disposisi surat, dan lainnya. Hal tersebut membuktikan jika pemenuhan kebutuhan akan informasi Lembaga XYZ menghadirkan TI sebagai solusinya, namun risiko akibat TI juga dapat bermunculan. Kerusakan hingga kehilangan data dapat menjadi sebuah hambatan bahkan kerugian bagi organisasi [2]. Apabila hal tersebut terjadi, secara otomatis organisasi perlu menanganinya dengan mengorbankan aset tertentu dan menjadi kerugian. Maka dari itu perlu adanya manajemen risiko dalam keamanan informasi untuk menjamin informasi yang dibutuhkan dapat terjaga dengan baik dan meminimalisir kerugian dari risiko[3].

Lembaga XYZ telah menyediakan beberapa SOP dan menerapakan beberapa kebijakan dalam keamanan informasi. Namun masih ditemukan jika beberapa target dari perencanaan kinerja khususnya e-Gov yang didalamnya termasuk SIPS belum maksimal hingga tahun penelitian ini dilakukan. Pada periode sebelumnya dengan menggunakan kerangka kerja COBIT 5 masih ditemukan beberapa proses hanya mencapai *level* 0. Berdasarkan survei yang dilakukan, *outcomes* yang seharusnya dihasilkan dari hasil evaluasi yang dilakukan juga belum terwujud. Perlu dilakukan pengukuran tingkat kapabilitas sebagai pengetahuan organisasi apakah manajemen risiko keamanan informasi pada SIPS yang dilakukan telah maksimal[4].

Penelitian ini bertujuan untuk merancang alat ukur tingkat kapabilitas manajemen risiko keamanan informasi pada SIPS untuk mengoptimalkan mengetahui seberapa optimal manajemen yang telah diterapkan. Kerangka kerja yang digunakan sebagai pedoman perancangan alat ukur adalah COBIT 5 [5]. Metodologi yang penelitian dilakukan secara kualitatif dimana data yang

telah terkumpul akan dikelola dan dianalisis supaya dapat diselaraskan dengan pedoman yang ada pada COBIT 5 khususnya *Process Assessment Model* (PAM). Hasil dari penelitian ini dapat membantu penelitian dengan studi kasus yang sama untuk mencari tingkat kapabilitas manajemen risiko dalam keamanan informasi menggunakan alat ukur yang telah dirancang dalam penelitian ini.

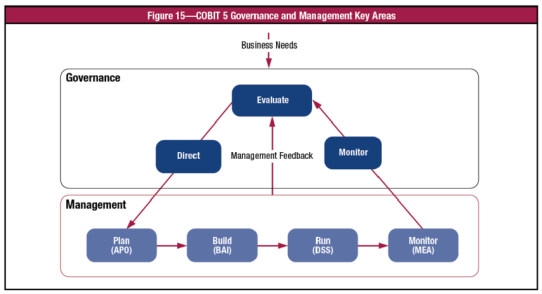
I. Metodologi

Studi Literatur

Salah satu kerangka kerja tata kelola TI yang hingga saat ini masih dikembangkan oleh *IT Governance Institute* (ITGI) dari *Information Systems Audit and Control Association* (ISACA) adalah COBIT [6]. *Control Objectives for Information and Related Technology* (COBIT) adalah seperangkat panduan yang berfokus pada tata kelola TI dan manajemen TI guna membantu auditor, manajemen, dan pengguna menjembatani resiko bisnis, kebutuhan kontrol, dan permasalahan- permasalahan teknis [7], [8]. Hingga saat ini COBIT melakukan penyempurnaan supaya sesuai dengan kondisi dan tantangan nyata yang terjadi[9].

Penelitian ini menggunakan COBIT 5 sebagai acuan dalam pembuatan alat ukur tingkat kapabilitas. COBIT 5 menyediakan *Process Assessment Model* (PAM) sebagai pedoman dalam menentukan tingkat kapabilitas yang telah terdefinisi dengan kriteria tertentu Jika dibandingkan dengan versi sebelumnya, COBIT 5 lebih berorientasi pada prinsip [10]. Prinsip ini digunakan untuk menyelaraskan sumber daya dengan kebutuhan pengguna untuk memanajemen berbagai risiko yang ada.

Dalam kerangka kerja COBIT 5 terbagi menjadi 2 area kunci yaitu manajemen dan tata kelola dari 37 proses dari 5 domain yang ada. Domain *Evaluate, Direct,* dan *Monitor* (EDM) dimana terdapat lima proses berada pada area kunci tata kelola. Pada area manajemen terdapat empat domain yang merupakan perkembangan dari versi sebelumnya diantaranya yaitu *Align, Plan, and Organize* (APO); *Build, Acquire, and Implement* (BAI); *Deliver, Service and Support* (DSS); dan *Monitor, Evaluate, and Assess* (MEA) [11].



Gambar 1. Area Kunci COBIT 5

COBIT 5 telah menyediakan panduan dalam menentukan domain dan proses yang digunakan untuk mengukur tingkat kapabilitas yang disesuaikan dengan kebutuhan penelitian serta mengacu pada tujuan strategis organisasi. Studi kasus penelitian ini berfokus pada manajemen risiko keamanan informasi dari Sistem Informasi Pengelolaan Surat pada Lembaga XYZ.

Pengumpulan Data

Penelitian ini menggunakan metode kualitatif, dimana pengumpulan data dilakukan melalui observasi, wawancara, dan melalui dokumentasi informasi yang mendukung penelitian. Acuan utama pada penelitian ini yaitu modul yang diterbitkan oleh ISACA dengan judul *Process Assessment Model* (PAM), COBIT 5 *Framework*, dan COBIT 5 *Enabling Process*.

Analisis

Setelah data berhasil terkumpul, dilakukan penyesuaian domain COBIT 5 dengan studi kasus yang diangkat dalam penelitian ini. Tahap ini diawali dengan menentukan tujuan bisnis dari perspektif internal[12]. Domain yang terpilih akan digunakan sebagai acuan dalam perancangan alat ukur tingkat kapabilitas SIPS berupa daftar pertanyaan wawancara. Pertanyaan dari setiap tingkatan kapabilitas didasarkan dari metode *Process Assessment Model* (PAM).

II. Hasil dan Pembahasan

Penentuan Domain

Pada penelitian ini berfokus pada tujuan perusahaan yang terkait dengan manajemen risiko, maka dari itu diputuskan pada EG03 yaitu *Managed Business Risk.* Pemetaan pertama dilakukan untuk mementukan tujuan TI yang sesuai dengan tujuan bisnis (khususnya pada studi kasus yang diangkat).

Pada tabel berikut merupakan temuan beberapa tujuan TI yang didefinikan menjadi ITRG.

Tabel 1. Hasil *IT-Related Goals* Terpilih dari Pemetaan Tujuan Bisnis pada Tujuan TI

No.	Kode	Tujuan TI
1.	ITRG04	*Managed IT-Related Business Risk*
2.	ITRG10	*Security of Information, processing infrastucture, and application.*
3.	ITRG16	*Competent and motivated business and IT personnel.*

Note : Berdasarkan BSC Figure 17 COBIT 5-Enabling Process.

Berdasarkan tujuan IT yang didapat kemudian diselaraskan kembali dengan lingkup dari pengukuran yang akan dilakukan yaitu pada keamanan informasi. Secara definisi maka ITRG04 dipilih untuk menentukan domain mana yang akan digunakan untuk mengukur tingkat kapabilitas manajemen risiko keamanan informasi.

Tabel 2. Hasil Proses Terpilih dari Pemetaan ITRG04 pada Domain COBIT 5

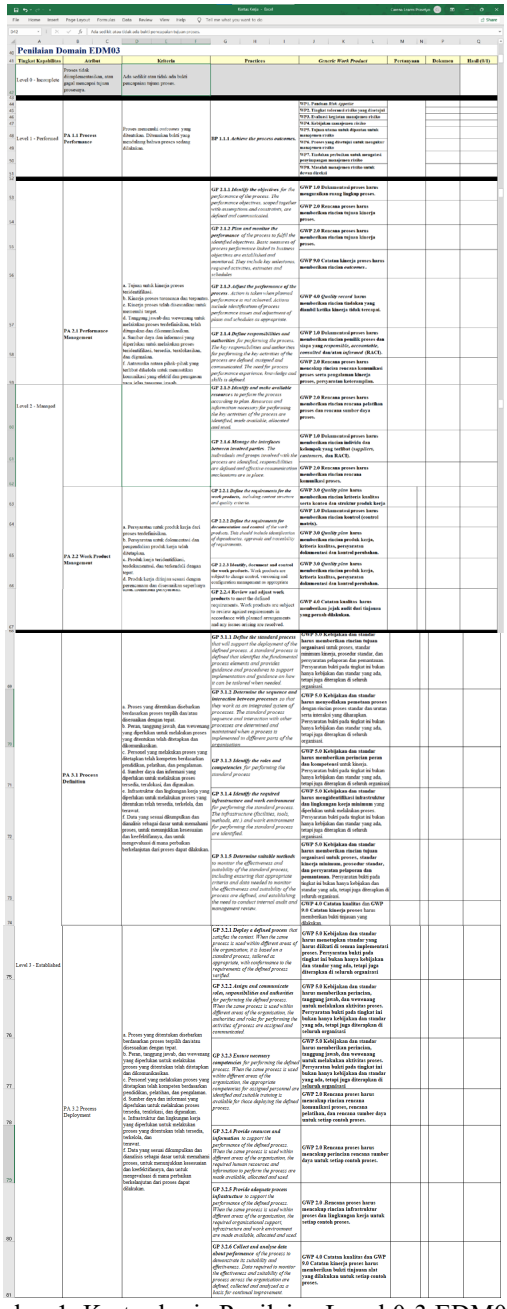
No.	Kode	Domain
1.	EDM03	*Ensure Risk Optimisation*
2.	APO12	*Manage Risk*
3.	APO13	*Manage Security*
4.	BAI06	*Manage Changes*

Note: Berdasarkan BSC Figure 18 COBIT 5-Enabling Process

Berdasarkan tabel di atas, diputuskan untuk memakai EDM03 dan APO12 sebagai fokus domain dalam pengukuran tingkat kapabilitas. Hal tersebut didasari dari beberapa penelitian terdahulu dan batasan dalam penelitian dimana hanya sampai pada memastikan bahwa risiko yang dimanajemen telah berjalan dengan optimal. Kertas kerja untuk mengukur tingkat kapabilitas dirancang menggunakan aplikasi Microsoft Excel tahun 2019. Penggunaan aplikasi ini guna memudahkan perhitungan presentase yang didapat setelah dilakukan penilaian. Tabel dibawah merupakan kerangka dari tabel penilaian. Kolom yang atribut untuk menghasilkan nilai dari pengukuran tingkat kapabilitas diantaranya :

1. Tingkat Kapabilitas
2. Atribut
3. Kriteria (Opsional)
4. *Practices*
5. *Generic Work Product*
6. Pertanyaan
7. Dokumen
8. Hasil (0/1)

Berdasarkan kolom tersebut, berikut ini tampilan kertas kerja dari rancangan alat ukur untuk domain EDM03 *Ensure Risk Management.*



Gambar 1. Kertas kerja Penilaian Level 0-3 EDM03

Seperti yang ada pada Gambar 1, kertas kerja disusun berdasarkan PAM yang dimana terdapat beberapa *work products* sesuai dengan

domain. Jika ditarik secara garis lurus maka hasil perhitungan akan seperti gambar berikut.

***Work Products* EDM03**

Work Product EDM03	Terpenuhi (0/1)	Keterangan
Panduan Risk Appetite		
Tingkat toleransi risiko yang disetujui		
Evaluasi kegiatan manajemen risiko		
Kebijakan manajemen risiko		
Tujuan utama untuk dipantau untuk manajemen risiko		
Proses yang disetujui untuk mengukur manajemen risiko		
Tindakan perbaikan untuk mengatasi penyimpangan manajemen risiko		
Masalah manajemen risiko untuk dewan direksi		

Gambar 2. Kertas kerja *work products* EDM03

Work Product APO12

Work Product APO12	Terpenuhi (0/1)	Keterangan
Data tentang lingkungan operasi yang berkaitan dengan risiko.		
Data tentang kejadian risiko dan faktor yang berkontribusi		
Masalah dan faktor risiko yang muncul		
Lingkup upaya analisis risiko		
Skenario risiko TI		
Hasil analisis risiko		
Skenario risiko yang terdokumentasi berdasarkan lini bisnis dan fungsi		
Aggregated risk profile, termasuk status tindakan manajemen risiko		
Analisis risiko dan laporan profil risiko untuk pemangku kepentingan		
Meninjau hasil penilaian risiko pihak ketiga		
Peluang untuk menerima risiko yang lebih besar		
Proposal proyek untuk mengurangi risiko		
Rencana respons insiden terkait risiko		
Komunikasi dampak risiko		
Akar penyebab terkait risiko		

Gambar 3. Kertas kerja *work products* APO12

Pada kolom ”Terpenuhi” akan diisi dengan nilai 1 apabila Lembaga XYZ telah memiliki dokumen tersebut. Hal tersebut akan disesuaikan dengan kriteria pada setiap level/ tingkat kapabilitas. Pada setiap tingkatan maka akan dilakukan perhitungan jumlah pertanyaan yang memenuhi dan *work products* yang terpenuhi. Secara garis besar, perhitungan dengan rumus ditampilkan pada gambar berikut.

Perhitungan Tingkat Kapabiltas EDM03

Best Practice EDM03	Pertanyaan		*Work Product*		Nilai yang dicapai
	Jumlah	Terpenuhi	Jumlah	Terpenuhi	
EDM03.01 *Evaluate Risk Management*					=(((C19/B19)*C24)+((E19/D19)*C24))/2
EDM03.02 *Direct Risk Management*					#DIV/0!
EDM03.03 *Monitor Risk Management*					#DIV/0!
				Total	#DIV/0!
Total BP adalah 3 maka nilai masing- masing BP adalah	33.33%				

Gambar 4. Kertas kerja Pehitungan Tiap *Level* pada EDM03

Perhitungan Tingkat Kapabiltas APO12

Best Practice APO12	Pertanyaan		*Work Product*		Nilai yang dicapai
	Jumlah	Terpenuhi	Jumlah	Terpenuhi	
APO12.01 *Collect Data*					=(((C19/B19)*C27)+((E19/D19)*C27))/2
APO12.02 *Analyse Risk*					#DIV/0!
APO12.03 *Maintain a risk profile*					#DIV/0!
APO12.04 *Articulate risk*					#DIV/0!
APO12.05 *Define a risk management action portofolio*					#DIV/0!
APO12.06 *Respond to risk*					#DIV/0!
				Total	#DIV/0!
Total BP adalah 6 maka nilai masing- masing BP adalah	16.67%				

Gambar 5. Kertas kerja Pehitungan Tiap *Level* pada APO 12

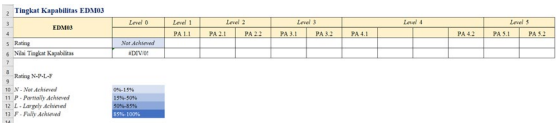
Rumus tersebut didapat dari akumulasi presentase dari pertanyaan yang terpenuhi dijumlahkan dengan *work products* yang terpenuhi. Setelah presentase didapatkan, kemudian dipetakan pada *Rating Levels* N-P-L-F. Jika nilai yang didapat termasuk pada tingkat F atau terpenuhi secara keseluruahan maka dapat melanjutkan penilaian pada tingkat/ *level* selanjutnya. Namun jika nilai tidak mencapai N maka Lembaga XYZ hanya dapat mencapai pada tingkat tertentu sesuai presentase terakhir yang dihasilkan. Hal tersebut dapat menjadi sebuah rekomendasi perbaikan untuk meningkatkan kinerja sesuai kriteria suatu tingkatan yang tidak dapat terpenuhi sesuai kondisi nyata.

Tabel 3. *Rating Levels COBIT 5*

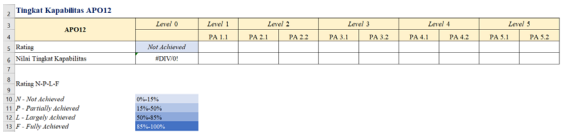
Kode	Keterangan	Presentase
N	*Not Achieved*	0 – 15%
P	*Partially Achieved*	16%-50%
L	*Largelly Achieved*	51%-85%
F	*Fully Achieved*	86%-100%

Note : Berdasarkan COBIT 5- Process Assessment Model

Pertanyaan akan disusun apabila telah melakukan observasi lebih lanjut terkait kondisi dari Lembaga XYZ. Kriteria yang ada kemudian akan dinilai sesuai dengan kondisi nyata yang ada pada Lembaga XYZ disertai dengan temuan bukti yang harus didokumentasikan sebagai laporan. Hasil tersebut kemudian ditampilkan pada tabel *summary* dalam kertas kerja.



Gambar 6. Kertas kerja *summary* EDM03



Gambar 7. Kertas kerja *summary* APO12

Pada *summary* akan ditampilkan hasil akhir sampai pada *Level* mana tingkat kapabilitas telah terwujud dimana N-P-L-F akan mendefinisikan suatu tingkatan sudah terpenuhi sampai pada titik tertentu. Dari hasil tersebut dapat digunakan sebagai tolak ukur Lembaga XYZ untuk meningkatkan kinerja bisnisnya terlebih pada Sistem Informasi Pengelolaan Surat (SIPS) dalam melakukan manajemen risiko keamanan informasinya.

III. Kesimpulan

Berdasarkan temuan yang ada, Lembaga XYZ perlu melakukan pengukuran untuk mengantisipasi risiko TI khususnya dalam kasus keamanan informasi yang dapat menjadi hambatan bisnis dalam Sistem Informasi Pengelolaan Surat. Pengukuran dapat dilakukan menggunakan kerangka kerja COBIT 5 dengan domain EDM03 *Ensure Risk Management* dan APO12 *Manage Risk*. Alat ukur tingkat kapabilitas yang dirancang dapat digunakan sebagai alternatif untuk melakukan penilaian secara mandiri pada Sistem Informasi Pengelolaan Surat Lembaga XYZ khususnya dalam manajemen risiko keamanan informasi untuk mempermudah organisasi mendapatkan parameter tingkatan yang perlu dilakukan untuk menghasilkan layanan yang maksimal.

IV. Daftar Pustaka

[1] Riadi, F. T., Manuputty, A. D., & Saputra, A. (2018). Evaluasi Manajemen Risiko Keamanan Informasi dengan Menggunakan COBIT 5 Subdomain EDM03 (Ensure Risk Optimisation). *JUTEI*, vol. 2, no. 1, pp. 1–10, 2018, doi: 10.21460/jutei.2018.12.53.

[2] Setyaningrum, N. D. & Kusyanti, A.,(2018). Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 (Studi Kasus : PT . Kimia Farma (Persero) Tbk – Plant Watudakon). vol. 2, no. 1, pp. 143–152.

[3] Thenu, P. P., Wijaya, A. F., Rudianto, C., Kristen, U., & Wacana, S.,(2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus : Pt Global Infotech). *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13.

[4] Aziz, R. A. Kusrini, & Sudarmawan. (2018). Evaluasi Manajemen Risiko Teknologi Informasi Pada Perusahaan BUMN Menggunakan Standar COBIT 5 (Studi Kasus : PT TASPEN PERSERO). *J. IT CIDA*, vol. 4, no. 2, pp. 1–11.

[5] Mukaromah, S. & Subriad, A. P. (2016). The Significant of Cobit Mapping Business Goal 12 and IT Goal 19 (Case Study: Stikom Surabaya). *IPTEK J. Proc. Ser.*, vol. 2, no. 1, pp. 117–118. doi: 10.12962/j23546026.y2015i1.1133.

[6] ISACA, *Enabling Processes*. ISACA, 2012.

[7] Mukaromah, S. & Putra, A. B. (2016). Maturity level at university academic information system linking it goals and business goal based on COBIT 4.1. *MATEC Web Conf.*, vol. 58, 2016, doi: 10.1051/matecconf/20165803009.

[8] Mukaromah, S. & Pribadi, A.. (2017). Information System Audit Based on Customer Perspective 4. *Adv. Sci. Lett.*, vol. 23, no. 12, pp. 12309–12312, 2017, doi: https://doi.org/10.1166/asl.2017.10627.

[9] Rochmania, N., Rozas, I. S., & Ilham. (2020). Tren Penggunaan Framework COBIT, ITIL, dan ISO 27001 pada Rentang Tahun 2014- 2018 di Indonesia. *EDUMATIC J. Pendidik. Inform.*, vol. 4, no. 2, pp. 10–19, 2020, doi: 10.29408/edumatic.v4i2.2249.

[10] Syuhada, A. M. (2021). Kajian Perbandingan COBIT 5 dengan COBIT 2019 sebagai Framework Audit Tata Kelola Teknologi Informasi. *J. Ilm. Indones.*, vol. 6, no. 1, p. 30.

[11] ISACA (2012). *COBIT Five: A Business Framework for the Governance and Manajement of Enterprise IT Using COBIT 5*.

[12] Mukaromah, S. & Subriadi, A. P. (2015). Tingkat Kematangan Tujuan IT 'Memastikan Informasi yang Penting dan Rahasia Disembunyikan dari Pihak-pihak yang Tidak Berkepentingan' Berdasar COBIT 4.1. *Pros. Semin. Nas. Manaj. Teknol. XXIII*, vol. 24, pp. C-24-1-C-24–8.