Jurnal Ilmu Komputer Revolusioner

Vol.8 No.1, Januari 2024
ISSN: 24430355

EVALUASI TINGKAT KEMATANGAN TATA KELOLA TEKNOLOGI INFORMASI TERHADAP KEAMANAN SISTEM DENGAN MENGGUNAKAN FRAMEWORK COBIT 5 (SUB DOMAIN DS5): STUDI KASUS SATUAN KERJA DI BADAN RISET DAN INOVASI NASIONAL

Brilyan Hendra Suryawan
Universitas Sebelas Maret
E-mail: brilyan.hendra@gmail.com

Abstrak

Sebagai institusi pemerintahan yang sudah memanfaatkan teknologi informasi dan komunikasi, Salah Satu Satuan Kerja di Badan Riset dan Inovasi Nasional menyadari perlunya ada standar operasional dan prosedur manajemen pengamanan sistem informasi dan telekomunikasi. Penelitian ini bertujuan untuk menilai sejauh mana tingkat kematangan atau *maturity level* teknologi informasi fokus keamanan informasi dengan mengevaluasi Tata Kelola Sistem Keamanan Teknologi Informasi menggunakan Framework COBIT 5. Penelitian ini menggunakan tipe deskriptif kualitatif. Berdasarkan analisis dan evaluasi tingkat kematangan dapat di simpulkan bahwa tingkat kematangan *(maturity level)* pengelolaan proses untuk memastikan keamanan sistem yang ada di salah satu Satuan Kerja BRIN menurut domain DS5 berada di level 3,72 yang termasuk dalam skala *Managed and Measurable* atau tingkat kematangan. Setelah tercapai tingkat kematangan level 4 untuk semua atribut, maka dilakukan langkah perbaikan yang berkelanjutan pada semua atribut secara bersama-sama untuk mencapai tingkat kematangan tata kelola teknologi informasi yang diharapkan yakni tingkat kematangan level 5 (*optimized*).

Kata Kunci — Cobit 5, *Maturity Level*, Tata Kelola, Sistem Keamanan.

1. PENDAHULUAN

Berhasilnya tata kelola organisasi/instansi saat ini sangat bergantung pada sejauh mana tata kelola dari teknologi informasi yang dilakukan. Layanan Teknologi Informasi (TI) setiap organisasi berbeda tingkatannya. Untuk mengidentifikasi sejauh mana perusahaan/organisasi telah memenuhi standar pengelolaan proses teknologi informasi yang baik, COBIT menyediakan kerangka identifikasi yang direpresentasikan dalam sebuah model kedewasaan (*maturity level*) yang mengindikasikan tingkat reliabilitas TI organisasi/instansi.

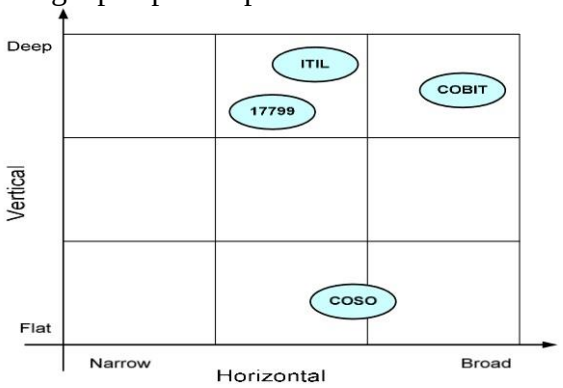
Terdapat bebarapa framework yang sering digunakan dalam Tata Kelola TI yang telah mendapat pengakuan secara luas antara lain COBIT, COSO, ITIL, dan ISO/IEC 17799. Dengan menggunakan framework tersebut, maka tujuan penerapan TI di sebuah perusahaan/organisasi akan sesuai dengan tujuan yang diharapkan dan menghindarkan dari terjadinya kerugian akibat risiko-risiko penerapan yang tidak terpetakan.

Tabel 1. Matriks Domain COBIT vs ITIL, ISO/IEC 17799, dan COSO
(COBIT Mapping, Overview of International IT Guidance, 2008)

Standar	Domain COBIT			
	PO	AI	DS	M
ITIL	○	+	+	-
ISO/IEC 17799	○	+	+	○
COSO	+	+	○	-
+ Frequently addressed ○ Moderately addressed - Not or rarely addressed				

Gambar 1 memetakan standar COBIT dengan standar lainnya dalam hal kelengkapan proses-proses TI yang dilihat dalam dua dimensi:

1. Vertical: melihat kedetailan atau kedalaman standar dalam hal teknis dan operasional.
2. Horizonal: melihat kelengkapan proses-proses TI



Gambar 1. Pemetaan COBIT terhadap ITIL, ISO/IEC 17799, dan COSO
(COBIT Mapping, Overview of International IT Guidance, 2008)

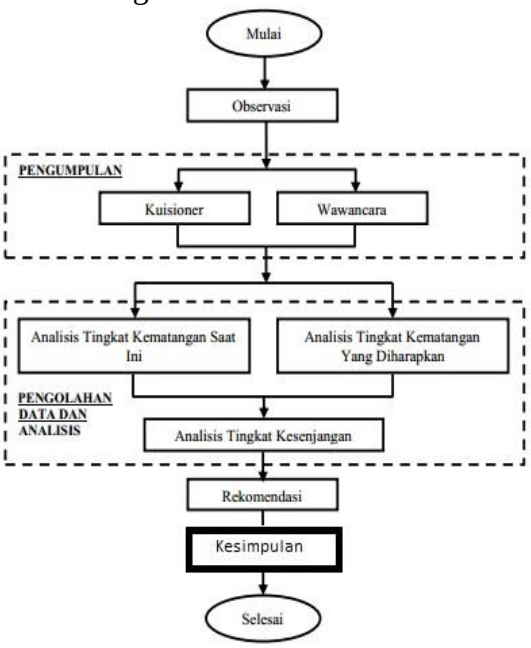
Dari Gambar 1, dapat dilihat bahwa COBIT mempunyai kompromi antara dimensi horisontal dan vertikal yang lebih baik dari standar-standar lainnya. COBIT mempunyai spektrum proses TI yang lebih luas dan lebih mendetail. ITIL merupakan standar yang paling mendetail dan mendalam dalam mendefinisikan proses-proses TI yang bersifat teknis dan operasional. Sedangkan COSO mempunyai detail yang dangkal, walaupun spektrum proses teknis dan operasionalnya cukup luas.

Selanjutnya, untuk mengetahui tingkat keamanan dalam Tata Kelola Teknologi Informasi yang ada, maka dalam penelitian ini digunakanlah framework COBIT 5 yang memberikan layanan kerangka kerja secara komprehensif untuk membantu manajemen TI dalam sebuah perusahaan dan instansi mencapai tujuan yang di harapkan. Dalam Jurnalnya (Habsoro, 2009) mengenai "*Aplikasi Tata Kelola dan Audit Informasi Menggunakan Framework COBIT pada domain DS dan ME"* dapat disimpulkan bahwa Teknologi Informasi sudah merupakan hal yang penting dalam sebuah perusahaan.

Tujuan dari penelitian ini adalah untuk menilai sejauh mana tingkat kemampuan atau *Capability Level* teknologi informasi fokus keamanan informasi di Satker BRIN dengan mengevaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5. Diharapkan dengan penerapan evaluasi keamanan teknologi informasi tersebut dapat mengukur *Capability Level* dan memberikan rekomendasi untuk perbaikan teknologi informasi dari analisis kesenjangan atau *gap analysis* dari hasil evaluasi tersebut.

2. METODE PENELITIAN

Dalam Metode Penelitian ini terdapat urutan langkah-langkah penelitian dalam penyelesaikan masalah adalah sebagai berikut:



Gambar 2. Langkah-langkah Penelitian

A. Prosedur Pengumpulan data

Penelitian ini menggunakan tipe deskriptif kualitatif. Dimana pengumpulan data dilakukan dengan kuisioner dan wawancara. Penentuan responden dibuat berdasarkan tabel RACI (*Responsible, Accountable, Consulted, and Informed*) pada kerangka kerja COBIT 5 dan disesuaikan dengan struktur organisasi di Satker BRIN. Daftar pertanyaan-pernyataan pada kuisioner dibuat mengacu pada kerangka kerja COBIT 5 berdasarkan variabel-variabel yang terdapat pada *process attributes* dan indikator-indikator kegiatan yang terdapat pada *control objectives* proses memastikan keamanan sistem (DS5).

Tabel 2. Struktur RACI Pada Proses DS5

Struktur RACI	**Struktur Satker Pusyantek BRIN**
Business Manager (Accountable)	Kepala Pusyantek BRIN
Head of IT (Consulted)	Koordinator Bidang
IT Operation Manager (Responsible)	SubKoordinator Bidang

B. Pengolahan Data dan Analisis

Teknik untuk menganalisa data yaitu Melakukan studi literatur tentang COBIT 5, kemudian menentukan subjek dan objek penelitian, melakukan wawancara, observasi dan pengambilan data dengan menggunakan kuesioner kepada responden yang sudah

ditentukan. Kemudian mengevaluasi dan menganalisis data dari kuesioner yang delah diisi. Selanjutnya membuat analis gap dari hasil kuesioner yang telah diisi.

Pengumpulan data dilakukan dengan melakukan observasi secara langsung, penyebaran kuesioner dan wawancara untuk melakukan klarifikasi data kuesioner dan pengumpulan dokumen sebagai bukti tertulis. Kuesioner yang penulis buat terdiri dari lima (5) level disesuaikan dengan tingkatan pada COBIT 5. Dalam COBIT 5 memang ada enam (6) level yaitu Level 0 Tidak Lengkap *(Incomplete)*, Level 1 Dilaksanakan *(Performed)*, Level 2 Dikelola *(Managed)*, Level 3 Didirikan *(Established)*, Level 4 Diprediksi *(Predictable)* dan Level 5 Optimasi *(Optimizing)*. Tetapi hanya Level 1 sampai dengan Level 5 saja yang ditetapkan dalam Model Penilaian Proses *(Process Assessment Model/PAM*). Level 0 tidak termasuk jenis indikator. Level 0 mencerminkan proses yang tidak dilaksanakan atau proses yang gagal untuk mencapai hasil tersebut (ISACA, 2012c: 115).

Melakukan pengumpulan dan pengolahan terhadap hasil kuesioner, kemudian mengkaji hasil *(outcome)* dan praktik dasar *(base practice)* COBIT 5 dengan hasil kuesioner. Menentukan tingkat kapabilitas tata kelola TI pada aspek keamanan sistem informasi. Data yang diperoleh dari kuesioner merupakan data mentah yang berisi jawaban dari responden. Tujuan analisis data yang dilakukan adalah untuk menyederhanakan seluruh data dan kemudian disajikan dalam susunan yang sistematis.

Indeks kematangan atribut diperoleh dari perhitungan total pilihan jawaban kuesioner dan pembobotan dengan rumus pilihan jawaban sebagai berikut:

$$\text{Indek Kematangan Atribut} = \frac{\sum (\text{Total Jawaban x Bobot})}{\text{Jumlah Responden}}$$

Tabel 3. Indek Kematangan

Indek Kematangan	Level Kematangan
0 – 0,50	0-Non- existent
0,51 – 1,50	1-Initial/ ad hoc
1,51 – 2,50	2-Repetable But intuitive
2,51 – 3,50	3-Defined Process
3,51 – 4,50	4-Managed and Measurable
4,51 – 5,00	5-Optimized

3. HASIL DAN PEMBAHASAN

Hasil dari kuesioner untuk domain DS5 *(ensure system sequrity)* yang disebarkan pada pegawai berjumlah 20 orang pada Satker Pusyantek BRIN, yang terdiri dari Kepala Satker, Koordinator Bidang, dan juga para pegawai yang sudah ditentukan sebelumnya.

Tabel 4. Hasil Kuesioner Domain DS5

Pertanyaan DS5	Responden																				Rata-rata	Rata-rata per proses
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20		
DS5 1	5	4	4	4	5	5	5	4	3	5	4	4	4	5	4	4	5	4	5	5	4.54	
DS5 2	5	5	4	5	2	5	5	5	4	4	1	4	4	5	4	5	4	5	5	4	3.82	
DS5 3	4	3	3	4	4	5	4	5	5	4	4	5	5	4	3	4	5	4	4	4	4.38	
	4	2	3	5	5	4	4	3	4	5	5	4	5	4	5	4	4	5	4	4	4.21	
	5	4	4	4	5	3	5	4	1	3	4	5	3	3	5	4	4	4	3	5	3.70	
	2	5	5	4	4	5	4	3	5	4	5	3	4	5	5	5	4	5	4	4	4.27	
	4	4	4	5	3	4	3	3	5	4	4	4	5	4	5	5	5	5	5	5	4.51	
DS5 4	3	4	4	0	0	2	5	0	1	4	3	5	5	5	4	5	5	5	4	4	3.31	3.72
	4	2	1	5	0	4	4	3	5	4	3	4	4	4	4	4	5	4	4	5	4.18	
DS5 5	3	4	5	5	5	5	5	4	5	4	3	5	4	5	4	2	3	3	4	4	3.68	
DS5 6	5	5	4	5	5	4	5	5	4	4	1	4	5	4	3	4	4	5	4	5	4.39	
DS5 7	4	3	2	4	3	4	5	2	5	5	5	5	3	5	4	5	5	4	5	4	3.65	
DS5 8	5	5	4	5	5	5	5	5	4	4	3	4	2	4	5	4	4	5	4	3	3.07	
DS5 9	5	0	1	3	4	5	2	2	5	4	4	3	4	3	4	5	4	4	4	4	4.27	
DS5 10	2	2	4	2	5	5	3	4	5	2	0	2	4	5	5	4	5	4	5	5	3.21	
DS5 11	4	4	4	5	5	4	3	5	5	1	2	2	5	4	4	4	5	5	5	4	4.22	

Bisa dilihat dari tabel diatas, proses pengawasan dan evaluasi terhadap tata kelola teknologi informasi berdasarkan *maturity model* sudah berjalan baik yaitu berada pada sekala 4 yaitu 3.72 menurut responden keamanan sistem komputer sudah berfungsi dengan baik dan penempatannya sudah sesuai dengan aturan, penggunaan internet selalu mendapat pengawasan dari pimpinan sehingga tugas dapat diselesaikan tepat waktu. Namun kegiatan *training* teknologi informasi untuk pegawai belum secara keseluruhan.

Hasil Pengukuran Tingkat Kematangan Setiap Proses TI pada Domain DS5 *(Ensure System Sequrity)* bisa dilhat pada tabel berikut:

Tabel 5. Pengukuran Tingkat Kematangan Proses TI

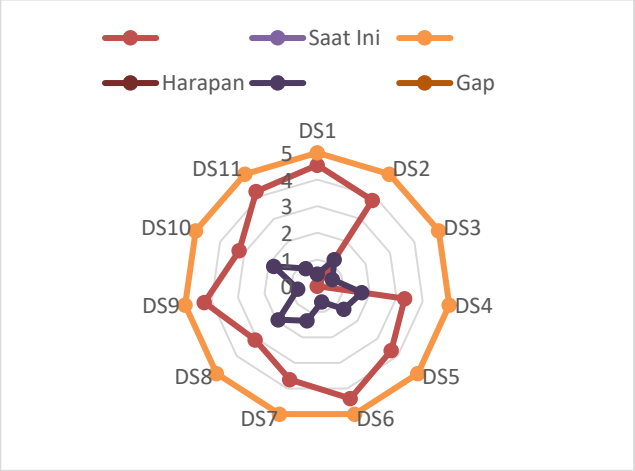
Control proses TI	Kondisi TI saat ini Rata-rata per proses TI	Tingkat *Model Maturity*
DS5.1 : Manajemen Keamanan TI *(Managementof IT Security)*	4.54	*managed and measurable*
DS5.2: Rencana Keamanan TI *(IT Security Plan)*	3.82	*managed and measurable*
DS5.3 : Manajemen Identitas *(Identity Management)*	4,38	*managed and measurable*
DS4: Manajemen akun pengguna *(User Acount management)*	3.31	*Defined process*
DS5: Uji Coba Keamanan, Penjagaan dan Pemantauan *(Security Testing, Surveillance and monitoring*	3.68	*managed and measurable*
DS5.6: Definisi Insiden Keamanan (Security Incident Definition)	4.39	*managed and measurable*
DS5.7: Proteksi Teknologi Keamanan *(Protection of Security Technology)*	3,65	*managed and measurable*
DS5.8: Manajemen Kunci Kriptografi *(Cryptographic Key Management)*	3.07	*managed and measurable*
DS5.9: Pencegahan Software Berbahaya, Deteksi dan Perbaikan *(Software Prevention, Detection and Correction)*	4.27	*managed and measurable*
DS10: keamanan jaringan *(network security)*	3.21	*Defined proses*
DS5.11: Pertukaran Data Sensitif *(Exchange of Sensitive Data)*	4.22	*managed and measurable*

Pada tingkat *maturity* skala 4 yaitu *managed and measurable*, pada tingkat ini, antara lain:

a. Kondisi dimana perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun objektif terhadap kinerja proses teknologi informasi.
b. Terdapat fasilitas untuk memonitor dan mengukur prosedur yang sudah berjalan, dapat mengambil tindakan jika terdapat proses yang diindikasikan tidak efektif.
c. Proses diperbaiki terus menerus dan dibandingkan dengan praktik-praktik terbaik.
d. Terdapat perangkat bantu dan otomatisasi untuk pengawasan proses.
e. Adapun grafik hasil pengukuran tingkat kematangan bisa dilihat dibawah ini:

Tabel 6. *Maturity level* skala 4

	DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9	DS10	DS11
Saat Ini	4.54	3.82	4,38	3.31	3.68	4.39	3.65	3.07	4.27	3.21	4.22
Harapan	5	5	5	5	5	5	5	5	5	5	5
Gap	0.46	1.18	0.62	1.69	1.32	0.61	1.35	1.93	0.73	1.79	0.78



Gambar 3. model *maturity level* skala 4

Berdasarkan data diatas hasil tingkat model *maturity level* penelitian berada di skala 4 *(Managed and Measurable)*, artinya Satker Pusyantek BRIN sudah menerapkan keamanan sistem teknologi informasi yang ada. Prosedur telah distandarisasi dan didokumentasikan, serta dikomunikasikan melalui pelatihan. Hal ini diamanatkan bahwa proses harus diikuti, namun tidak mungkin bahwa penyimpangan akan terdeteksi. Prosedur sendiri belum canggih tetapi hanya formalisasi praktek yang ada.

Temuan dari sistem informasi Saker Pusyantek BRIN sudah distandarisasi, terdokumentasi, dan dikomunikasikan melalui pelatihan tetapi implementasi masih tergantung pada pegawai apakah mau mengikuti prosedur tersebut atau tidak. Prosedur yang dibuat tersebut tidak rumit, hanya merupakan formalitas yang suda ada.

KESIMPULAN

Berdasarkan analisis dan evaluasi tingkat kematangan dapat di simpulkan bahwa tingkat kematangan (maturity level) pengelolaan proses untuk memastikan keamanan sistem yang ada Satuan Kerja Pusyantek BRIN menurut domain DS 5 ada di level 3,72 yang termasuk dalam skala Managed and Measurable atau tingkat kematangan. Setelah tercapai tingkat kematangan level 4 untuk semua atribut, maka dilakukan langkah perbaikan yang berkelanjutan pada semua atribut secara bersama-sama untuk mencapai tingkat kematangan

tata kelola teknologi informasi yang diharapkan yakni tingkat kematangan level 5 (optimized).

DAFTAR PUSTAKA

ISACA, 2006, Integrating COBIT into the IT Audit Process, IT Governance Institute

ISACA, 2012a. COBIT 5 A Business Framework for the Governance and Management of Enterprise IT, Available at: www.isaca.org

ISACA, 2012b. COBIT 5 for Information Security, ISACA. Available at: www.isaca.org.

Fajar Tri Prabowo dkk. 2017. Jurnal Teknologi Elektro Vol.16. p-ISSN:1693 – 2951; e-ISSN: 2503-2372

Habsoro, A. (2009). Aplikasi Tata Kelola dan Audit Informasi Menggunakan. EEPIS Repository , Vol 1, 10.

Iik Muhamad Malik dkk, 2017. Jurnal Teknik Informatika Vol.10 No.02. p-ISSN 1979-9160; e-ISSN 2549-7901

Isa, Irawan. 2012. "Evaluasi Pengontrolan Sistem Informasi". Yogyakarta: Graha Ilmu

Khotari, C.R., 2004. Research Methodology Methods and Techniques Second., New Delhi: New Age Publisher. Available at: www.newagepublishers.com.

Sarna, Riyanarto. 2009. Audit Sistem dan Teknologi Informasi. Edisi Pertama. Surabaya. ITS Press

Spremic, M., 2011. Standards and Frameworks for Information System Security Auditing and Assurance. World Congress on Engineering