PEMETAAN TUJUAN KASKADE COBIT 5 DALAM PERUMUSAN PROSES AUDIT KEAMANAN SISTEM INFORMASI DI PEMERINTAH KOTA YOGYAKARTA

Dewi Ciptaningrum[1)], Eko Nugroho[2)], Dani Adhipta[3)]

[1), 2), 3)] Teknik Elektro dan Teknik Informatika Uviversitas Gadjah Mada Yogyakarta
Jl Grafika, Condongcatur, Sleman, Yogyakarta 55281
Email : dewi.cio13@mail.ugm.ac.id[1)], nugroho@ugm.ac.id[2)], dani@ugm.ac.id[3)]

Abstrak

Sistem informasi dan telekomunikasi yang terjamin keamanannya diharapkan dapat meningkatkan pelayanan kepada masyarakat umum di lingkungan Pemerintah Kota Yogyakarta. Selama ini, Pemerintah Kota Yogyakarta belum pernah melaksanakan audit terhadap Keamanan Sistem Informasi. COBIT 5 merupakan kerangka kerja yang lengkap dan diterima secara internasional untuk mengatur dan mengelola informasi perusahaan dan teknologi (TI) dalam rangka pencapaian tujuan bisnis dan tujuan TI terkait. COBIT 5 for Information Security layak diajukan sebagai metode yang tepat untuk audit keamanan sistem informasi. Beberapa fitur seperti mekanisme dan alat ukur yang sederhana, menjangkau keseluruhan komponen organisasi, serta tingkat validitas menjadikan metode ini sesuai untuk melaksanakan audit keamanan Sistem Informasi bagi Pemerintah Kota Yogyakarta.

Kata kunci: *Keamanan, Sistem Informasi, COBIT 5, Pemerintah Kota Yogyakarta*

1. Pendahuluan

Pemerintah Kota Yogyakarta sudah memanfaatkan teknologi informasi dan komunikasi melalui pembangunan aplikasi-aplikasi yang mendukung pelayanan masyarakat. Aplikasi-aplikasi ini berupa situs resmi Pemerintah Kota Yogyakarta *http://jogjakota.go.id*, Penerimaan Peserta Didik Baru (PPDB) *Online*, Unit Pelayanan Informasi dan Keluhan (UPIK), Layanan Pengadaan Secara Elektronik (LPSE), Bursa Kerja *online*, *CCTV* (*Closed-Circuit Television*) *online* yang bisa dimanfaatkan masyarakat untuk memantau tiga belas (13) tempat strategis di Kota Yogyakarta dan masih banyak lagi. Ini merupakan perwujudan dari salah satu misi Rencana Induk *e-government* Pemerintah Kota Yogyakarta, yaitu "Mewujudkan *e-government* dalam lingkup pelayanan kepada masyarakat" [1].

Sejak 15 Desember 2007, Pemerintah Kota Yogyakarta telah memiliki Dokumen Perencanaan Pembangunan *e-government* yang mengacu pada *Master Plan* (Rencana Induk) *e-government* [1]. Rencana Induk *e-government* memuat pernyataan visi dan misi, strategi pengembangan, cetak biru pengembangan, tahapan pengelolaan dan implementasi. Melalui dokumen tersebut Pemerintah Kota Yogyakarta merencanakan pembangunan *e-government* melalui empat (4) tahap yang masing-masing tahap terbagi menjadi jangka waktu lima (5) tahun. Rencana Induk *e-government* ini disusun sesuai dengan kondisi, keinginan dan kebutuhan Pemerintah Kota Yogyakarta dalam membangun *e-government* Pemerintah Kota Yogyakarta untuk mewujudkan *good governance* [1].

Sebagai institusi pemerintahan yang sudah memanfaatkan teknologi informasi dan komunikasi, Pemerintah Kota Yogyakarta menyadari perlunya ada standar operasional dan prosedur manajemen pengamanan sistem informasi dan telekomunikasi di lingkungan Pemerintah Kota Yogyakarta. Peraturan Walikota Yogyakarta Nomor 78 Tahun 2007 tentang Standar Operasional dan Prosedur Manajemen Pengamanan Sistem Informasi dan Komunikasi pada Pemerintah Kota Yogyakarta ditetapkan untuk dijadikan pedoman dan acuan dalam mengelola dan menggunakan perangkat dan sistem yang terkait dengan teknologi informasi dan komunikasi di lingkungan Pemerintah Kota Yogyakarta [2]. Dengan sistem informasi dan telekomunikasi yang terjamin keamanannya diharapkan Pemerintah Kota Yogyakarta dapat meningkatkan pelayanan kepada masyarakat umum seiring dengan tambahnya kepercayaan pemanfaatan infrastruktur teknologi yang tersedia.

Sudah tujuh (7) tahun berlalu sejak ditetapkannya Peraturan Walikota tentang Standar Operasional dan Prosedur Manajemen Pengamanan Sistem Informasi dan Komunikasi pada Pemerintah Kota Yogyakarta. Selama kurun waktu ini, Pemerintah Kota Yogyakarta belum pernah melaksanakan audit terhadap Keamanan Sistem Informasi. Melalui audit keamanan sistem informasi pada Pemerintah Kota Yogyakarta ini diharapkan mampu mengetahui tingkat kapabilitas keamanan sistem informasi pada Pemerintah Kota Yogyakarta.

Banyak penelitian mengenai COBIT 5 yang membuktikan bahwa COBIT 5 merupakan kerangka kerja untuk audit keamanan SI dan mampu menyediakan tata kelola keamanan informasi yang menyeluruh [3][4][5][6][7]. Bahkan dalam COBIT 5 juga ada tujuan terkait TI tentang keamanan dan ada salah satu produk dari COBIT 5 yang khusus fokus pada keamanan

informasi, yaitu COBIT 5 *for Information Security*. Fokus spesifik COBIT 5 ini sebagai metode yang tepat untuk melakukan audit keamanan Sistem Informasi bagi Pemerintah Kota Yogyakarta.

COBIT 5 merupakan kerangka kerja yang lengkap dan diterima secara internasional untuk mengatur dan mengelola informasi perusahaan dan teknologi (TI) yang mendukung eksekutif perusahaan dan manajemen dalam rangka pencapaian tujuan bisnis dan tujuan TI terkait. COBIT 5 menjelaskan lima (5) prinsip dan tujuh (7) *enabler* yang mendukung perusahaan dalam pengembangan, implementasi, dan perbaikan terus-menerus dan pemantauan terkait tata kelola TI dan praktik manajemen yang baik [8]. Pada penelitian ini penulis menggunakan COBIT 5 khususnya COBIT 5 *for Information Security* (untuk Keamanan Informasi) sebagai kerangka dan standar untuk melakukan audit keamanan SI di Pemerintah Kota Yogyakarta. COBIT 5 untuk Keamanan Informasi ini mengandung rekomendasi bagi praktisi keamanan informasi tentang bagaimana menerapkan keamanan informasi dalam cakupannya.

2. Pembahasan

Tujuan kaskade COBIT 5 adalah mekanisme untuk menerjemahkan kebutuhan para pemangku kepentingan menjadi tujuan perusahaan yang spesifik, bisa dilaksanakan dan disesuaikan, tujuan terkait TI dan tujuan *enabler*. Sehingga dapat dirumuskan penetapan tujuan yang spesifik pada setiap tingkatan dan di setiap wilayah dari perusahaan dalam mendukung tujuan keseluruhan dan kebutuhan para pemangku kepentingan [8].

Gambar 2.1. Tujuan Kaskade COBIT 5 [8]

Kebutuhan para pemangku kepentingan dipengaruhi oleh beberapa pemicu seperti perubahan strategi, perubahan bisnis dan perubahan peraturan. Kebutuhan para pemangku kepentingan juga bisa dihubungkan kepada serangkaian tujuan perusahaan umum/generik. COBIT 5 menetapkan tujuh belas (17) tujuan perusahaan (*Enterprises Goal*) yang terdiri dari dimensi Kartu Nilai Keseimbangan (*Balanced Scorecard*) yang membawahi tujuan perusahaan yang sesuai, tujuan perusahaan dan hubungan antara ketiga tujuan inti perusahaan (realisasi keuntungan, optimasi risiko dan optimasi sumber daya) [8].

Untuk mendapatkan proses-proses apa yang akan diaudit dalam Keamanan Sistem Informasi Pemerintah Kota Yogyakarta ini, yang pertama kali yang harus dilakukan adalah menentukan Tujuan Perusahaan. COBIT 5 menyediakan Dimensi Kartu Nilai Keseimbangan yang mengategorikan 17 Tujuan Perusahaan ke dalam empat (4) dimensi, yaitu dimensi Keuangan, Pelanggan, Proses Bisnis Internal dan yang terakhir adalah Belajar dan Bertumbuh. Tujuan (Rencana Strategis/Renstra) Bagian Teknologi Informasi dan Telematika (TIT) Setda Kota Yogyakarta akan diidentifikasi ke dalam Tujuan Perusahaan yang telah ditetapkan COBIT 5. Lima (5) Renstra Bagian TIT Setda Kota Yogyakarta diidentifikasi menjadi empat (4) Tujuan Perusahaan yang ditetapkan COBIT 5. Empat (4) Tujuan Perusahaan tersebut adalah Budaya Layanan yang Berorientasi pada Pelanggan, Kelangsungan dan Ketersediaan Layanan Bisnis, Optimasi Fungsionalitas Proses Bisnis, dan Produktivitas Operasional dan Staf.

Dari empat (4) Tujuan Perusahaan yang sudah diidentifikasi akan dipetakan terhadap Tujuan terkait TI dalam COBIT 5.

Tabel 2.1. Identifikasi Tujuan Perusahaan dengan Tujuan Bagian TIT

Dimensi Kartu Nilai Keseimbang-an	No.	Tujuan Perusahaan	Tujuan Bagian TIT (Renstra)
Pelanggan	6	Budaya Layanan yang Berorientasi pada Pelanggan	Pengembangan dan Pengelolaan *e-government*
			Pembinaan dan Pengembangan Teknologi Informasi
	7	Kelangsungan dan Ketersediaan Layanan Bisnis	Peningkatan Sistem Pengamanan Jaringan
Proses Bisnis Internal	11	Optimasi Fungsionalitas Proses Bisnis	Peningkatan dan Pengelolaan Sistem Telekomunikasi
			Pengelolaan Perangkat Keras dan Jaringan Informasi
			Peningkatan Sistem Pengamanan Jaringan
	14	Produktivitas Operasional dan Staf	Peningkatan dan Pengelolaan Sistem Telekomunikasi
			Pengelolaan Perangkat Keras dan Jaringan Informasi

Empat (4) Tujuan Perusahaan yang telah diidentifikasi (Budaya Layanan yang Berorientasi pada Pelanggan, Kelangsungan dan Ketersediaan Layanan Bisnis, Optimasi Fungsionalitas Proses Bisnis, dan Produktivitas

Operasional dan Staf) dipetakan dari tujuh belas (17) Tujuan terkait TI (*IT Related Goal*) dalam COBIT 5. Hasil pemetaan ini mendapatkan sembilan (9) Tujuan terkait TI dalam COBIT 5 dengan cara memilih proses yang berkategori primer, seperti yang terlampir dalam Tabel 2.3.

Sembilan (9) Tujuan terkait TI dalam COBIT 5 yang sudah diperoleh dipetakan ke dalam tiga puluh tujuh (37) proses COBIT 5. Pemetaan ini juga hanya memilih proses yang berkategori primer. Hasil pemetaan ini mendapatkan enam belas (16) proses dalam COBIT 5. Untuk lebih lanjut penelitian ini memfokuskan pada audit keamanan SI, sehingga penulis memilih Tujuan terkait TI yang berhubungan dengan keamanan informasi. Dengan memilih Tujuan terkait TI nomor 10 keamanan informasi, infrastruktur pengolahan dan aplikasi penulis membatasi ruang lingkup penelitian agar lebih fokus. Pemetaan Tujuan terkait TI nomor 10 keamanan informasi, infrastruktur pengolahan dan aplikasi mendapatkan lima (5) proses dalam COBIT 5 yang berkategori primer.

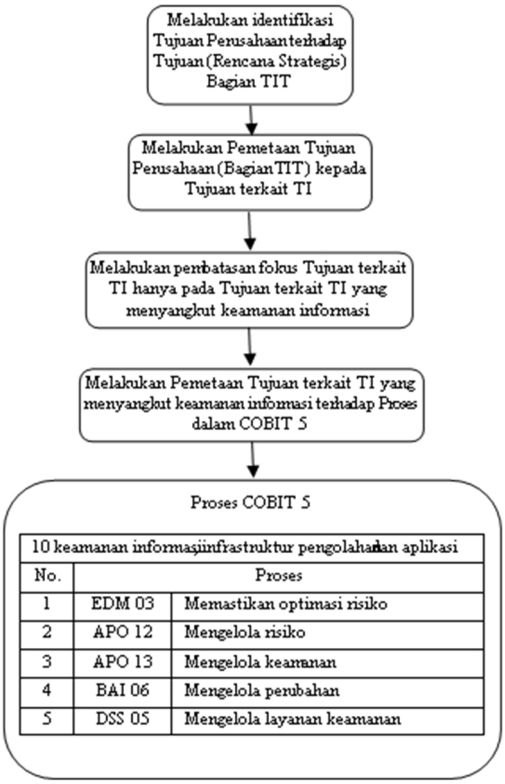
Tabel 2.2. Pemetaan Tujuan Bagian TIT dengan Tujuan Terkait Teknologi Informasi

		Tujuan Perusahaan			
		Budaya Layanan yang Berorientasi pada Pelanggan	Kelangsungan dan Ketersediaan Layanan Bisnis	Optimasi Fungsionalitas Proses Bisnis	Produktivitas Operasional dan Staf
	Tujuan terkait Teknologi Informasi	**6**	**7**	**11**	**14**
1	Penyelarasan Strategi TI dan Bisnis	P	S	P	
4	Mengelola Risiko Bisnis Terkait TI		P		
7	Penyampaian Layanan TI sejalan dengan Persyaratan Bisnis	P	S	P	
8	Penggunaan Aplikasi, Informasi dan Solusi Teknologi yang Mencukupi	S	S	P	P
9	Ketangkasan TI	S		P	S
10	Keamanan Informasi, Infrastruktur Pengolahan dan Aplikasi		P		
12	Memungkinkan dan Mendukung Proses Bisnis dengan Menggabungkan Aplikasi dan Teknologi dalam Proses Bisnis	S		P	S
14	Ketersediaan Informasi yang Bisa Diandalkan dan Digunakan untuk Pengambilan Keputusan		P	S	
16	Karyawan yang Kompeten dan Termotivasi Bisnis dan TI	S			P

Tabel 2.3. Pemetaan Tujuan terkait TI nomor 10 dengan Proses dalam COBIT 5

		Tujuan terkait TI
		Keamanan Informasi, Infrastruktur Pengolahan dan Aplikasi
		10
Kode	**Proses dalam COBIT 5**	
EDM03	Memastikan Optimasi Risiko	P
APO12	Mengelola Risiko	P
APO13	Mengelola Keamanan	P
BAI06	Mengelola Perubahan	P
DSS05	Mengelola Layanan Keamanan	P

Proses pengidentifikasian dan pemetaan ini sesuai dengan tujuan kaskade yang terdapat dalam COBIT 5. Diawali dengan mengidentifikasi Tujuan Perusahaan (*Enterprise Goals*). Identifikasi tujuan perusahaan ini untuk mencari kesesuaian antara tujuan organisasi/perusahaan/instansi terhadap tujuh belas (17) Tujuan Perusahaan yang ditetapkan oleh COBIT 5. Kemudian beranjak ke tahap selanjutnya yaitu melakukan pemetaan Tujuan Perusahaan dengan tujuh belas (17) Tujuan terkait TI COBIT 5. Hasil pemetaan Tujuan terkait TI ini akan digunakan untuk pemetaan terhadap tiga puluh tujuh (37) proses dalam COBIT 5. Ada dua kategori, yaitu primer dan sekunder yang bisa dipilih. Pada penelitian ini, penulis memfokuskan diri pada yang berkategori primer saja. Proses dalam tujuan kaskade ini digambarkan pada Gambar2.2.



Gambar 2.2. Tujuan Kaskade Penelitian

Dalam Rencana Induk *e-government* disebutkan bahwa penanggung jawab penyelenggaraan pengembangan *e-government* Pemerintah Daerah adalah instansi yang membidangi pengembangan teknologi informasi [1]. Di Pemerintah Kota Yogyakarta, instansi yang membidangi pengembangan teknologi informasi adalah Bagian Teknologi Informasi dan Telematika (TIT) Setda Kota Yogyakarta. Jadi yang akan menjadi responden sasaran penelitian adalah para pegawai di Bagian Teknologi Informasi dan Telematika Setda Kota Yogyakarta.

Bagian TIT Setda Kota Yogyakarta merupakan satu dari sembilan bagian Sekretariat Daerah di Pemerintah Kota Yogyakarta. Berada di bawah Asisten Perekonomian dan Pembangunan Setda Kota Yogyakarta. Semua hal yang berkaitan dengan aplikasi teknologi informasi, telematika, perangkat keras dan jaringan teknologi informasi menjadi tanggung jawab Bagian TIT Setda Kota Yogyakarta. Bagian TIT ini terdiri dari dua sub bagian, yaitu Sub Bagian Aplikasi Teknologi Informasi dan Telematika dan Sub Bagian Perangkat Keras dan Jaringan Teknologi Informasi.

Pada penentuan responden ini penulis tidak menggunakan *RACI Chart* (*Responsible, Accountable, Informed and Consulted*) seperti yang disarankan oleh COBIT 5 untuk Keamanan Informasi. Struktur organisasi Bagian TIT Setda Yogyakarta yang hanya merupakan unit kerja tidak memungkinkan untuk menerapkan *RACI Chart* tersebut. Penulis menetapkan responden ini dengan menitikberatkan pada pegawai yang berperan dan bertanggung jawab langsung terhadap pengelolaan sistem informasi. Adapun pemetaan responden ini digambarkan pada Tabel 2.4.

Tabel 2.4. Pemetaan Responden

No.	Proses dalam COBIT 5	Responden terkait
1.	EDM 03 Memastikan Pengoptimalan Risiko	- Kepala Bagian TIT - Kepala Sub Bagian Aplikasi TIT - Kepala Sub Bagian Perangkat Keras dan Jaringan TI - Analis dan Perancang Sistem - *Administrator Server*
2.	APO 12 Manajemen Risiko	
3.	APO 13 Manajemen Keamanan	
4.	BAI 06 Manajemen Perubahan	
5.	DSS 05 Manajemen Layanan Keamanan	- Kepala Bagian TIT - Kepala Sub Bagian Aplikasi TIT - Kepala Sub Bagian Perangkat Keras dan Jaringan TI - Analis dan Perancang Sistem - *Administrator Server* - *Administrator*Jaringan

Kuesioner Level 1 untuk Audit Keamanan Sistem Informasi ini berpedoman pada aktivitas Proses COBIT 5 untuk Keamanan Informasi.

Tabel 2.5. Contoh Kuesioner Proses EDM03 Memastikan Optimasi Risiko

Proses Evaluasi, Mengarahkan dan Memantau (EDM03) Memastikan Optimasi Risiko			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
EDM03	Manajemen Risiko Sistem Informasi adalah bagian dari keseluruhan manajemen risiko perusahaan (ERM).					
	Praktik Dasar					
	EDM03-BP1	Mengevaluasi Manajemen Risiko				
	EDM03-BP2	Mengarahkan Manajemen Risiko				
	EDM03-BP3	Memantau Manajemen Risiko				
	Keluaran Produk Kerja					
	EDM03-WP1	Menyelaraskan Indikator Risiko Utama (KRIs) perusahaan dengan Indikator Risiko (KRIs)Utama keamanan SI				
	EDM03-WP2	Keamanan SI pada tingkat yang dapat ditolerir				
	EDM03-WP3	Memperbarui kebijakan manajemen risiko				
	EDM03-WP4	Tindakan perbaikan untuk mengatasi penyimpangan manajemen risiko				

Tabel 2.6. Contoh Kuesioner Proses APO12 Mengelola Risiko

Proses Menyelaraskan, Merencanakan dan Mengatur (APO12) Mengelola Risiko			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
APO12-01	Sebuah profil risiko informasi yang terkini dan lengkap ada untuk teknologi, aplikasi dan infrastruktur dalam perusahaan.					
	Praktik Dasar					
	APO12-BP1	Mengumpulkan data				
	APO12-BP2	Menganalisa Risiko				
	APO12-BP3	Mempertahankan profil risiko				
	APO12-BP4	Menjelaskan risiko				
	Keluaran Produk Kerja					
	APO12-WP1	Data pada risiko keamanan SI				
	APO12-WP2	Hasil analisis risiko keamanan SI				
	APO12-WP3	Skenario risiko keamanan SI				
	APO12-WP4	Profil risiko keamanan SI				
	APO12-WP5	Strategi respon risiko keamanan SI				
APO12-02	Informasi penanganan insiden keamanan terintegrasi dengan proses manajemen risiko secara keseluruhan demi menyediakan kemampuan untuk memperbarui portofolio manajemen risiko.					
	Praktik Dasar					
	APO12-BP1	Mendefinisikan portofolio tindakan manajemen risiko				

Proses Menyelaraskan, Merencanakan dan Mengatur (APO12) Mengelola Risiko			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
	APO12-BP2	Menanggapi risiko				
	Keluaran Produk Kerja					
	APO12-WP1	Proposal proyek untuk mengurangi risiko keamanan SI				
	APO12-WP2	Proposal proyek untuk mengurangi risiko				
	APO12-WP3	Praktik mitigasi risiko keamanan SI				

Tabel 2.7. Contoh Kuesioner Proses APO13 Mengelola Keamanan

Proses Menyelaraskan, Merencanakan dan Mengatur (APO13) Mengelola Keamanan			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
APO13-01	Sebuah sistem di tempat yang mempertimbangkan dan efektif menangani persyaratan keamanan informasi perusahaan.					
	Praktik Dasar					
	APO13-BP1	Membangun dan memelihara sistem manajemen keamanan informasi (SMKI).				
	Keluaran Produk Kerja					
	APO13-WP1	Pernyataan lingkup SMKI				
	APO13-WP2	Kebijakan SMKI				
APO13-02	Rencana keamanan telah dibentuk, diterima dan dikomunikasikan ke seluruh perusahaan.					
	Praktik Dasar					
	APO13-BP1	Mendefinisikan dan mengelola rencana perlakuan risiko keamanan informasi.				
	Keluaran Produk Kerja					
	APO13-WP1	Kasus Bisnis keamanan SI				
APO13-03	Solusi keamanan SI diimplementasikan dan dioperasikan secara konsisten di seluruh perusahaan.					
	Praktik Dasar					
	APO13-BP1	Memantau dan meninjau SMKI.				
	Keluaran Produk Kerja					
	APO13-WP1	Rekomendasi untuk meningkatkan SMKI				
	APO13-WP2	Laporan audit SMKI				

Tabel 2.8. Contoh Kuesioner Proses BAI06 Mengelola Perubahan

Proses Membangun, Memperoleh dan Menerapkan (BAI06) Mengelola Perubahan			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
BAI06-01	Persyaratan keamanan informasi yang dimasukkan selama penilaian dampak dari proses, aplikasi dan perubahan infrastruktur.					
	Praktik Dasar					

Proses Membangun, Memperoleh dan Menerapkan (BAI06) Mengelola Perubahan			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
	BAI06-BP1	Mengevaluasi, membuat prioritas dan memberikan kewenangan permintaan perubahan				
	BAI06-BP2	Mengelola perubahan darurat				
	Keluaran Produk Kerja					
	BAI06-WP1	Penilaian dampak				
	BAI06-WP2	Ulasan pascapelaksanaan perubahan darurat				
BAI06-02	Perubahan Darurat memperhitungkan persyaratan keamanan SI yang diperlukan.					
	Praktik Dasar					
	BAI06-BP1	Rekam jejak dan laporan status perubahan				
	BAI06-BP2	Teliti dan dokumentasikan perubahan				
	Keluaran Produk Kerja					
	BAI06-WP1	Perbarui laporan status permintaan perubahan				

Tabel 2.9. Contoh Kuesioner Proses DSS05 Mengelola Layanan Keamanan

Proses Menyampaikan, Layanan dan Dukungan (DSS05) Mengelola Layanan Keamanan			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
DSS05001	Jaringan dan keamanan komunikasi memenuhi kebutuhan bisnis.					
	Praktik Dasar					
	DSS05-BP1	Memberikan perlindungan dalam menghadapi *malware*				
	Keluaran Produk Kerja					
	DSS05-WP1	Kebijakan pencegahan perangkat lunak berbahaya				
	DSS05-WP2	Evaluasi potensi ancaman				
DSS05-02	Informasi diproses pada, disimpan dan ditransmisikan oleh perangkat *endpoint* dilindungi.					
	Praktik Dasar					
	DSS05-BP1	Mengelola keamanan jaringan dan konektivitas				
	Keluaran Produk Kerja					
	DSS05-WP1	Kebijakan keamanan konektivitas				
	DSS05-WP2	Hasil uji penetrasi				
DSS05-03	Semua pengguna secara unik diidentifikasi dan memiliki hak akses sesuai dengan peran bisnis mereka.					
	Praktik Dasar					
	DSS05-BP1	Mengelola keamanan *endpoint*				
	Keluaran Produk Kerja					
	DSS05-WP1	Kebijakan keamanan untuk perangkat *endpoint*				

Proses Menyampaikan, Layanan dan Dukungan (DSS05) Mengelola Layanan Keamanan			N	P	L	F
PA 1.1 Proses yang dilaksanakan mencapai tujuan prosesnya.						
DSS05-04	Tindakan fisik telah dilaksanakan untuk melindungi informasi dari akses yang tidak sah, kerusakan dan gangguan sedang diproses, disimpan atau dikirimkan.					
	Praktik Dasar					
	DSS05-BP1	Mengelola pengidentifikasian pengguna dan akses logis				
	Keluaran Produk Kerja					
	DSS05-WP1	Hasil tinjauan dari pengguna akun dan hak istimewa				
	DSS05-WP2	Hak akses pengguna disetujui				
DSS05-05	Mengamankan informasi elektronik dengan baik ketika disimpan, ditransmisikan atau dihancurkan.					
	Praktik Dasar					
	DSS05-BP1	Mengelola akses fisik ke aset SI				
	Keluaran Produk Kerja					
	DSS05-WP1	log akses				
	DSS05-WP2	Permintaan akses disetujui				

Pada kuesioner ini, peneliti menggunakan skala peringkat dalam standar ISO/IEC 15504 karena pada Model Penilaian Proses (*Process Assessment Model*) dalam COBIT 5 ini mengadopsi standar tersebut. Setiap atribut dibuat peringkat menggunakan skala penilaian standar yang ditetapkan dalam standar ISO/IEC 15504 [9].

Tabel 2.10. Tingkatan Peringkat

Tingkatan Peringkat		
	Keterangan	Pencapaian
N	Tidak dicapai	0 – 15% pencapaian
P	Sebagian dicapai	> 15% sampai 50% pencapaian
L	Sebagian besar dicapai	> 50% sampai 85% pencapaian
F	Dicapai sepenuhnya	> 85% sampai 100% pencapaian
Source: This figure is reproduced from ISO/IEC 15504-2:2003, with the permission of ISO/IEC at*www.iso.org*. Copyright remains with ISO/IEC.		

3. Kesimpulan

Dari Rencana Strategis (Renstra) Bagian TIT Setda Kota Yogyakarta dipetakan terhadap Tujuan Perusahaan (*Enterprise Goal*) COBIT 5. Setelah didapatkan Tujuan Perusahaan, maka Tujuan Perusahaan tersebut dipetakan terhadap Tujuan Terkait TI (*IT Related Goal*) COBIT 5. Tujuan Terkait TI hasil pemetaan ini juga akan dipetakan terhadap tiga puluh tujuh (37) proses yang terdapat di COBIT 5 untuk Keamanan Informasi (*for Information Security*). Ada dua kategori, yaitu primer dan sekunder yang bisa dipilih. Pada penelitian yang sedang berjalan ini, penulis memfokuskan diri pada yang berkategori primer saja. Proses hasil pemetaan inilah yang nantinya akan dijadikan acuan untuk membuat kuesioner. Kuesioner diberikan kepada responden terpilih, yaitu pegawai Bagian TIT Setda Kota Yogyakarta yang berperan dan bertanggung jawab langsung terhadap pengelolaan sistem informasi.

Daftar Pustaka

[1] P. K. Yogyakarta, *Peraturan Walikota Yogyakarta*. 2007, p. 36.
[2] K. Yogyakarta, P. D. Kota, B. Dalam, L. Propinsi, J. Timur, J. Tengah, P. Daerah, and O. P. Daerah, "Walikota yogyakarta," 2007.
[3] M. Spremić, "Governing Information System Security: Review of Approaches to Information System Security Assurance and Auditing," *Latest Trends Appl. Informatics Comput.*, pp. 42–48, 2011.
[4] M. Spremic, "Standards and Frameworks for Information System Security Auditing and Assurance," *World Congr. Eng.*, vol. I, p. 6, 2011.
[5] M. Spremić, D. Ph, M. Ivanov, and P. D. Full, "Using CobiT Methodology in Information System Auditing : Evidences from measuring the level of Operational Risks in Credit Institutions 2 . Managing Risks in Credit Institutions System Auditing and Assessing The," *Recent Adv. Bus. Adm.*, pp. 45–50, 2010.
[6] Z. Huang, P. Zavarsky, and R. Ruhl, "An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002," *2009 Int. Conf. Comput. Sci. Eng.*, vol. 198, pp. 386–391, 2009.
[7] S. Morimoto, "Application of COBIT to Security Management in Information Systems Development," *2009 Fourth Int. Conf. Front. Comput. Sci. Technol.*, pp. 625–630, Dec. 2009.
[8] ISACA, "COBIT 5 A Business Framework for the Governance and Management of Enterprise IT," 2012. [Online]. Available: http://www.isaca.org/COBIT/Pages/default.aspx?cid=1003566&Appeal=PR. [Accessed: 13-Apr-2014].
[9] ISACA, *Process Assessment Model (PAM): Using COBIT ® 5*. ISACA.

Biodata Penulis

Dewi Ciptaningrum,memperoleh gelar Sarjana Sosial (S.Sos), Jurusan Ilmu Komunikasi MassaUniversitas Negeri Sebelas Maret Surakarta, lulus Tahun 2005.Saat ini menjadi PNS di Pemerintah Kota Yogyakarta.
Dr. Ir. Eko Nugroho, M.Si.,memperoleh gelar Insinyur (Ir.), Jurusan Teknik ElektroUniversitas Gadjah Mada Yogyakarta, lulus Tahun 1978. Memperoleh gelar Magister Sains (M.Si.) Jurusan Akuntasi Manajemen Universitas Gajah Mada Yogyakarta, lulus Tahun 1992.Memperoleh gelar Doktor (Dr.) Jurusan *Cognitive Psychology* Universitas Gajah Mada Yogyakarta, lulus Tahun 2004. Saat ini menjadi Dosen di Universitas Gadjah Mada Yogyakarta.
Dani Adhipta, S.Si., M.T., memperoleh gelar Sarjana Sains (S.Si.), Jurusan Fisika Universitas Gadjah Mada Yogyakarta pada Tahun 1994. Memperoleh gelar Magister Teknik (M.T.) dari Jurusan Teknik Elektro Universitas Gadjah Mada Yogyakarta pada Tahun 1998. Saat ini menjadi Dosen di Universitas Gadjah Mada Yogyakarta.