AUDIT KEAMANAN SISTEM INFORMASI PADA KANTOR PEMERINTAH KOTA YOGYAKARTA MENGGUNAKAN COBIT 5

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

[1), 2), 3)] Teknik Elektro dan Teknik Informatika Universitas 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)]

ABSTRAKS
Sebagai institusi pemerintahan yang sudah memanfaatkan teknologi informasi dan komunikasi, Pemerintah Kota Yogyakarta mempunyai Peraturan Walikota Yogyakarta Nomor 78 Tahun 2007 tentang Standar Operasional dan Prosedur Manajemen Pengamanan Sistem Informasi dan Komunikasi pada Pemerintah Kota Yogyakarta. Selama ini Pemerintah Kota Yogyakarta belum pernah melaksanakan audit terhadap Keamanan Sistem Informasi. Penelitian ini akan melakukan audit keamanan sistem informasi pada Pemerintah Kota Yogyakarta menggunakan COBIT 5 untuk Keamanan Informasi. Pemilihan proses diukur melalui pemetaan tujuan kaskade menghasilkan lima (5) proses dalam COBIT 5. Responden berjumlah sembilan (9) orang pegawai yang berperan dan bertanggung jawab langsung terhadap pengelolaan sistem informasi. Hasil pengukuran nilai kapabilitas keamanan SI di Pemerintah Kota Yogyakarta dari lima (5) proses, semua proses berada pada tingkat kapabilitas 1 Performed Process.

Kata Kunci: audit, keamanan, sistem informasi, COBIT 5

1. PENDAHULUAN

1.1 Latar Belakang

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 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" (Pemerintah Kota Yogyakarta 2007a: 8).

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 serta sistem yang terkait dengan teknologi informasi dan komunikasi di lingkungan Pemerintah Kota Yogyakarta (Pemerintah Kota Yogyakarta, 2007b: 2).

Pada Laporan Ancaman Keamanan Internet (*Internet Security Threat Report*) yang disajikan oleh Symantec menunjukkan bahwa pada Tahun 2013, peretas (*hacker*) merupakan penyebab tertinggi dalam *data breach*, diikuti oleh pengungkapan tidak sengaja dan pencurian atau kehilangan perangkat elektronik seperti komputer jinjing (*laptop*), komputer, *flashdisk*, dan lain sebagainya (Symantec, 2014: 39). Symantec juga menyebutkan bahwa administrasi publik atau pemerintahan menjadi target utama dalam *data breach* pada Tahun 2013 dalam kategori *Spear-Phishing* (Symantec, 2014: 29). Tentunya hal ini meresahkan karena sektor administrasi publik atau pemerintahan merupakan lembaga yang seharusnya kredibel dan akuntabel dalam melayani, melindungi dan menjamin kepentingan rakyat.

Keamanan informasi pada era Teknologi Informasi dan Komunikasi (TIK) ini sangat penting. Kerentanan *Information Exchange Environment* (IEE) telah meningkat sebagai ancaman menjadi lebih luas dan rumit, maka dari itu, keamanan informasi telah menjadi masalah yang mendasar untuk bisnis, organisasi, dan pemerintahan (Hassanzadeh et al., 2014: 98). 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.

1.2 Tinjauan Pustaka

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 (Spremić, 2011: 5) (Spremic, 2011: 5) (Spremić et al., 2010: 3) (Huang et al., 2009: 2) (Morimoto, 2009: 1). 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*. Menjadikan COBIT 5 sebagai metode yang tepat untuk melakukan audit keamanan Sistem Informasi bagi Pemerintah Kota Yogyakarta.

Dari Tabel 1.1. dapat diketahui bahwa kelebihan ITIL adalah untuk mendefinisikan strategi, rencana dan proses. Kelebihan COBIT untuk metrik, tolok ukur dan audit, sedangkan kelebihan ISO/IEC 27001 dan 27002 untuk mengatasi masalah keamanan untuk mengurangi risiko (Sahibudin et al., 2008: 5) (Wallhoff, 2000: 6). Meski disebutkan bahwa kelebihan ISO/IEC 27001 dan 27002 adalah keamanan informasi, tetapi kelebihan dalam keamanan informasi tersebut hanya bersifat teknis saja (Spremić, 2011: 2). Pada praktiknya, keamanan SI tidak hanya menyangkut aspek teknis saja melainkan juga menyangkut aspek nonteknis. Kelebihan COBIT untuk metrik, tolok ukur dan melaksanakan audit (Sahibudin et al., 2008: 5) (Wallhoff, 2000: 6), serta menyediakan tata kelola dan manajemen menyeluruh yang mampu mencakup aspek teknis dan aspek non teknis yang melandasi pemilihan COBIT 5 untuk audit keamanan SI.

Tabel 1. 1 Perbandingan antara ITIL, COBIT dan ISO/IEC 27001 & 27002 (Sahibudin et al., 2008: 5) (Wallhoff, 2000: 6)

ITIL	COBIT	ISO/IEC 27001 dan 27002
Konsep/proses	*Critical Success Factors*	Keamanan Informasi (aspek teknis)
Aktivitas	Metrik (*Critical Success Factors and Key Performance Indicator*)	
Biaya/ keuntungan	*Benchmarking* (CMM)	
Merencanakan untuk penerapan	Kendali	
	Audit	

Sisi positif menggunakan COBIT 5 sebagai kerangka kerja tata kelola Keamanan Informasi adalah bahwa keamanan informasi 'terpadu' ke dalam kerangka tata kelola TI yang lebih besar atau lebih luas, yang disediakan oleh tiga puluh tujuh (37) proses COBIT 5 [12]. Kemudahan COBIT 5 untuk selaras dengan kerangka kerja audit dan standar keamanan lainnya seperti Bill 198, COSO, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC ISO / IEC 12207 dan ITIL ITIL (Spremić et al., 2010: 3) (Huang et al., 2009: 2-6) (Morimoto, 2009: 5) juga memberi nilai lebih pada COBIT 5.

COBIT berisi tentang tata kelola TI dan mengacu pada masalah-masalah lainnya, salah satu diantaranya memiliki komponen substansial yang terkait dengan Keamanan Informasi (von Solms, 2005: 2) (von Solms and von Solms, 2009: 41-43). Apabila seluruh proses dalam COBIT dikelola dengan baik, maka akan menghasilkan tata kelola TI yang tepat (von Solms, 2005: 2). Salah satu dari Tujuan Terkait TI pada COBIT 5 yaitu tujuan nomor sepuluh (10) adalah keamanan informasi, infrastruktur pengolahan dan aplikasi dan salah satu produk keluaran COBIT 5 yaitu COBIT 5 untuk Keamanan Informasi (*for Information Security*) (ISACA, 2012a: 52-53) (ISACA, 2012b: 67-159). Inilah yang melandasi penulis menggunakan COBIT 5 untuk Keamanan Informasi sebagai kerangka kerja untuk melakukan audit keamanan SI di Pemerintah Kota Yogyakarta.

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*. Memperkenankan penetapan tujuan yang spesifik pada setiap tingkatan dan di setiap wilayah dari perusahaan dalam mendukung tujuan keseluruhan dan kebutuhan para pemangku kepentingan (ISACA, 2012a: 18).

Gambar 1. 1 Tujuan Kaskade COBIT 5 (ISACA, 2012a: 18)

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 (*enterprise 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) (ISACA, 2012a: 19).

Pencapaian dari tujuan perusahaan membutuhkan serangkaian hasil terkait TI (*IT-related*), yang diwakili oleh tujuan terkait TI. *IT-related* merupakan singkatan dari informasi dan teknologi yang berhubungan, dan tujuan informasi dan teknologi yang berhubungan terstruktur bersama dimensi Kartu Nilai Keseimbangan (*Balanced Scorecard*) TI (ISACA, 2012a: 19).

1.3 Model Penilaian Proses (*Process Assessment Model*)

Model penilaian proses (*Process Assessment Model*) adalah model dua dimensi kemampuan proses. Salah satu dimensi adalah dimensi proses, proses didefinisikan dan diklasifikasikan dalam kategori proses. Dimensi yang kedua adalah dimensi kemampuan, satu set atribut proses dikelompokkan ke dalam tingkat kemampuan yang ditetapkan. Proses atribut memberikan karakteristik terukur kapabilitas proses.

Indikator penilaian digunakan untuk menilai apakah atribut proses telah dicapai. Ada dua jenis indikator penilaian (ISACA, 2012c: 14):

1. Indikator proses kemampuan atribut, yang berlaku untuk tingkat kemampuan 1 sampai 5
2. Indikator kinerja proses, yang berlaku secara eksklusif dengan kemampuan tingkat 1.

ISO/IEC 15504-2:2003 ini sengaja diadopsi oleh COBIT 5 untuk Model Penilaian Proses (*Process Assessment Model*). Seperangkat persyaratan minimum yang ditetapkan dalam ISO/IEC 15504-2:2003 memastikan bahwa hasil penilaian adalah objektif, berimbang, konsisten, berulang dan merupakan representatif dari proses yang dinilai (Piamonte, 2012: 27).

ISO/IEC 15504-2:2003 mengidentifikasi kerangka pengukuran untuk kemampuan proses dan persyaratan untuk:

1. melakukan penilaian;
2. model referensi proses;
3. model penilaian proses;
4. melakukan verifikasi kesesuaian penilaian proses.

Dimensi kemampuan memberikan ukuran kemampuan proses untuk memenuhi kebutuhan bisnis perusahaan saat ini atau proyeksi tujuan untuk proses itu. Kemampuan proses (*Process Capability*) dinyatakan dalam hal atribut proses dikelompokkan menjadi tingkat kemampuan, seperti ditunjukkan pada Tabel 1.2. Tingkat kemampuan proses ditentukan berdasarkan pencapaian proses tertentu atribut sesuai dengan ISO / IEC 15504-2: 2003.

Tabel 1. 2 Tingkatan Kapabilitas dan Atribut Proses (ISACA, 2012c: 13)

Atribut Proses	Tingkat Kemampuan dan Atribut Proses
	Level 0 : Proses tidak lengkap
	Level 1: Proses dilaksanakan
PA 1.1	Kinerja Proses
	Level 2: Proses dikelola
PA 2.1	Manajemen Kinerja
PA 2.2	Manajemen Produk Kerja
	Level 3: Proses didirikan
PA 3.1	Penetapan proses
PA 3.2	Penyebaran proses
	Level 4: Proses diprediksi
PA 4.1	Pengukuran proses
PA 4.2	Pengendalian proses
	Level 5: Proses mengoptimalkan
PA 5.1	Inovasi proses
PA 5.2	Optimasi proses

Sumber: Angka ini diadaptasi dari ISO / IEC 15504-2: 2003, dengan izin dari ISO / IEC di www.iso.org. Hak cipta tetap milik ISO / IEC.

Indikator kinerja proses (dasar praktik dan produk kerja) spesifik untuk setiap proses dan digunakan untuk menentukan apakah suatu proses berada pada kemampuan tingkat 1. Indikator kinerja ini terdiri dari praktik dasar dan produk kerja dan eksklusif untuk tingkat 1. Praktik-praktik dasar dan produk kerja untuk setiap COBIT 5 proses ditunjukkan didasarkan pada konten COBIT 5. Indikator kemampuan proses atribut generik untuk setiap atribut proses untuk tingkat kemampuan 1 sampai 5. Level 1 hanya memiliki indikator praktik generik tunggal untuk kemampuan yang sejalan langsung ke pencapaian indikator kinerja tertentu yang digariskan dalam model referensi proses.

Pada penelitian ini penulis akan 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 merupakan salah satu produk dari COBIT 5. Dalam COBIT 5 untuk Keamanan Informasi ini mengandung rekomendasi bagi praktisi keamanan informasi tentang bagaimana menerapkan keamanan informasi

dalam cakupan COBIT 5. COBIT 5 untuk Keamanan Informasi memberikan panduan spesifik yang berhubungan dengan semua *enabler*, yaitu pada prinsip dan kerangka kerja; proses; struktur organisasi; budaya, etika dan perilaku; informasi; kemampuan layanan; dan manusia, keahlian dan kompetisi (ISACA, 2012b: 26).

2. PEMBAHASAN

2.1 Jalannya Penelitian

Dimulai dengan melakukan studi literatur awal tentang keamanan sistem informasi. Studi literatur awal ini dilakukan dengan mengumpulkan infomasi, literatur baik itu berupa *paper*, jurnal, buku dan hasil-hasil penelitian terdahulu mengenai keamanan sistem informasi. Selain itu peneliti juga mengumpulkan data terkait permasalahan, kendala dan gangguan mengenai sistem keamanan informasi. Dari semua data dan informasi yang diperoleh itu kemudian dirumuskan apa yang menjadi permasalahannya. Berdasarkan dari rumusan masalah tersebut ditentukan batasan masalah, tempat yang akan menjadi tempat penelitian, metode yang akan digunakan dan menentukan tujuan yang akan dicapai melalui penelitian ini.

Rumusan masalah, batasan masalah, tempat penelitian dan tujuan penelitian telah ditetapkan. Langkah selanjutnya yang dilakukan adalah mencari dan memperdalam informasi mengenai metode yang akan digunakan dalam penelitian ini, yaitu kerangka kerja COBIT 5. Kemudian melakukan identifikasi tujuan perusahaan (*enterprise goals*) yang akan menjadi acuan untuk melakukan pemetaan terhadap tujuh belas (17) tujuan terkait TI (*IT-related Goals*). Hasil pemetaan ini juga dipetakan kembali terhadap tiga puluh tujuh (37) proses dalam COBIT 5. Setelah mendapatkan proses yang hendak diukur, kemudian merancang dan membuat kuesioner, melakukan identifikasi responden, pengumpulan data, pengolahan data. Data yang diperoleh kemudian dianalisis dan hasil analisis data ini dijadikan rekomendasi terhadap Pemerintah Kota Yogyakarta.

2.1.1 Identifikasi Tujuan perusahaan

Pertama kali yang harus dilakukan adalah menentukan Tujuan Perusahaan. COBIT 5 menyediakan Dimensi Kartu Nilai Keseimbangan yang mengkategorikan 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 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

2.1.2 Pemetaan Tujuan Bagian TIT dengan Tujuan terkait TI

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 terhadap tujuh belas (17) Tujuan Terkait TI 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 2.2.

Tabel 2. 2 Pemetaan Tujuan Bagian TIT dengan Tujuan Terkait Teknologi Informasi

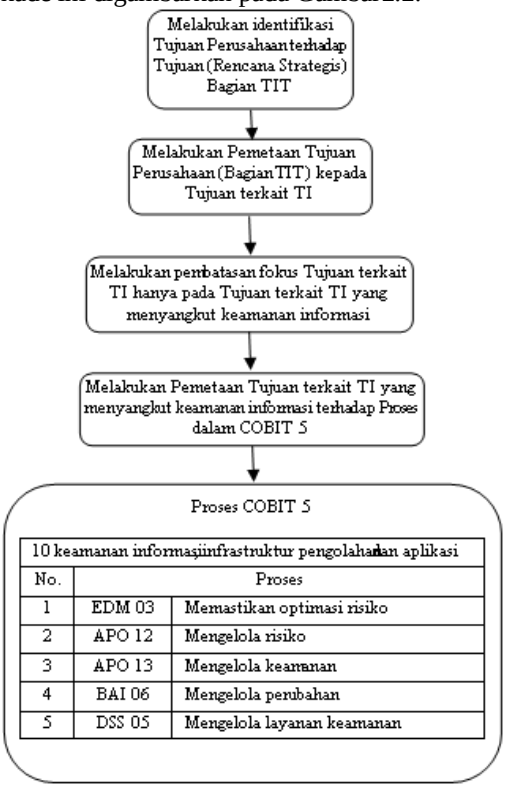
		Tujuan Perusahaan			
		Budaya Layanan yang Berorientasi pada Pelanggan	Kelangsungan dan Ketersediaan Layanan Bisnis	Optimasi Fungsionalitas Proses Bisnis	Produktivitas Operasional dan Staf
	Tujuan terkait Teknologi Informasi	**6**	**7**	**11**	**14**
1	Penyelarasan Strategi TI dan Bisnis	P	S	P	

		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**
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. 1 Tujuan Kaskade Penelitian

2.1.3 Identifikasi Responden

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 yang tugas pokok dan fungsinya menangani dan bertanggung jawab terhadap sistem informasi. Dalam penelitian ini penentuan contoh (*sample*) menggunakan metode *purposive sampling* karena tempat/lokasi penelitian kecil dan sudah dikenal dengan baik untuk bisa dipelajari secara intensif (Khotari, 2004: 15).

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.

Tabel 2. 4 Pemetaan Responden

No.	Proses dalam COBIT 5	Responden terkait	Jumlah
1	EDM03 Memastikan Optimasi Risiko	- Kepala Bagian TIT - Kepala Sub Bagian Aplikasi TIT - Kepala Sub Bagian Perangkat Keras dan Jaringan TI - Analis dan Perancang Sistem - Administrator Server	- 1 orang - 1 orang - 1 orang - 2 orang - 2 orang
2	APO12 Manajemen Risiko		
3	APO13 Manajemen Keamanan		
4	BAI06 Manajemen Perubahan		
5.	DSS05 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 - AdministratorJaringan	- 1 orang - 1 orang - 1 orang - 2 orang - 2 orang - 2 orang

2.1.4 Penetapan Level yang Ingin Dicapai

Pemerintah Kota Yogyakarta terutama Bagian TIT Setda Kota Yogyakarta belum menggunakan COBIT 5 untuk Keamanan Informasi sebagai kerangka kerja penyusunan Rencana Strategis (Renstra) Teknologi Informasi. Sehingga pada target yang ingin dicapai pada Renstra TI di Pemerintah Kota Yogyakarta tidak bisa untuk menentukan target kapabilitas proses yang ingin dicapai dalam COBIT 5 untuk Keamanan Informasi. Setelah Kepala Bagian TIT berdiskusi dengan Kepala Sub Bagian Aplikasi TIT dan Kepala Sub Bagian Perangkat Keras dan Jaringan TI, ketiganya sepakat untuk menetapkan target kapabilitas proses yang ingin dicapai dalam jangka pendek adalah level 3. Tapi dalam jangka panjangnya, Kepala Bagian TIT, Kepala Sub Bagian Aplikasi TIT dan Kepala Sub Bagian Perangkat Keras dan Jaringan TI menentukan level 5 sebagai target kapabilitas yang ingin dicapai.

2.1.5 Analisis Data

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).

Kuesioner lima (5) level ini tidak dibagikan secara bersamaan. Kuesioner untuk Level 1 penulis berikan kepada responden untuk mendapatkan tanggapan. Setelah pengolahan Level 1 dilakukan, bisa dilihat apakah hasil dari kuesioner Level 1 tersebut mampu melewati angka 85%-100% (*Largely Achieved* atau *Fully Achieved*). Jika mampu melewati angka 85%-100% baru akan dilanjutkan memberikan kuesioner untuk Level 2 dan seterusnya.

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.

Pada kuesioner, penulis 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. Peringkat ini terdiri dari:

Tabel 2. 5 Kategori Atribut Peringkat yang Digunakan dalam COBIT 5 (ISACA, 2012c: 14)

Singkatan	Keterangan	% Dicapai
N (*Not achieved*)	**Tidak dicapai** Ada sedikit bukti atau sama sekali tidak ada pencapaian atribut ditetapkan dalam proses yang dinilai.	0 sampai pencapaian 15%
P (*Partially Achieved*)	**Sebagian dicapai** Ada beberapa bukti dari pendekatan, beberapa pencapaian, dan atribut ditetapkan dalam proses yang dinilai. Beberapa aspek pencapaian atribut mungkin tidak terduga.	> 15% sampai pencapaian 50%

Singkatan	Keterangan	% Dicapai
L (*Largely Achieved*)	**Sebagian besar dicapai** Ada bukti dari pendekatan sistematis, pencapaian yang signifikan, atribut yang ditetapkan dalam proses yang dinilai.	> 50% sampai pencapaian 85%
F (*Fully Achieved*)	**Sepenuhnya dicapai** Ada bukti dari pendekatan yang lengkap dan sistematis, pencapaian penuh, atribut ditetapkan dalam proses yang dinilai.	> 85% sampai pencapaian 100%
Sumber: Angka ini direproduksi dari ISO/IEC 15504-2: 2003, dengan izin dari ISO/IEC di www.iso.org. Hak cipta tetap dengan ISO/IEC.		

Penilai/responden menggunakan peringkat ini untuk mengetahui tingkat kemampuan yang dicapai. Diterapkan secara konsisten, kriteria ini memungkinkan setiap penilaian harus didasarkan pada tingkat terstruktur dari formalitas dan memungkinkan perbandingan penilaian seluruh organisasi atau bahkan di perusahaan yang berbeda.

Pengolahan kuesioner lima (5) proses yang telah ditentukan untuk mendapatkan nilai kapabilitas. Pengolahan dilakukan dengan cara menghitung persentase dari setiap jawaban yang diperoleh dengan membagi jumlah persentase yang diperoleh dari setiap jawaban dengan jumlah pertanyaan, kemudian dikalikan 100%.

Pada level 1, menghitung rata-rata dari masing-masing praktik dasar dan produk kerja. Untuk mendapatkan nilai rata-rata dari praktik dasar dan nilai rata-rata produk kerja menggunakan *Mean* yang dikenal aritmetika rata-rata. *Mean* atau rata-rata ini merupakan aritmetika yang paling umum untuk mengukur kecenderungan sentral (*central tendency*) dan dapat didefinisikan sebagai nilai yang kita peroleh dengan membagi total nilai-nilai dari berbagai barang (*item*) yang diberikan dalam seri dengan jumlah total barang (*item*) (Khotari, 2004: 132).

$$\bar{X} = \frac{\sum Xi}{n}$$ (Khotari, 2004: 132)

Dimana

$\bar{X}$ = simbol untuk *mean* atau rata-rata hitung
Σ = simbol untuk penjumlahan keseluruhan
Xi = nilai berapa jumlah *X*, *I* = 1, 2, 3,..., n (nilai sampel ke-i)
n = jumlah sampel

Untuk mendapatkan penilaian proses (*process assessment*) maka akan menambahkan nilai praktik dasar dan nilai produk kerja kemudian dibagi dua (2).

$$\text{PA Level 1} = \frac{\bar{X}\ \text{BP} + \bar{X}\ \text{WP}}{2}$$

Dimana

PA = *Process Assessment* (Penilaian Proses)
$\bar{X}$ BP = *mean* atau rata-rata hitung Base *Practice* (Praktik Dasar)
$\bar{X}$ WP = *mean* atau rata-rata hitung *Work Product* (Produk Kerja)

Hasil persentase dari penghitungan ini juga akan menjadi pencapaian kategori dalam Level 1. Skala untuk menentukan kategori pencapaian ini sama dengan skala yang tercantum dalam Tabel 2.6.

Tabel 2. 6 Contoh tabel penilaian kapabilitas Level 1

Nama Proses	Nilai
Penilaian Proses (*Process Assessment*/PA)	
Praktik Dasar (*Base Practice*)	$\bar{X}$ BP
Produk Kerja (*Work Product*)	$\bar{X}$ WP

$$\text{PA Level 2 s.d. 5} = \frac{\bar{X}\ \text{GP} + \bar{X}\ \text{GWP}}{2}$$

Dimana

PA = *Process Assessment* (Penilaian Proses)
$\bar{X}$ GP = *mean* atau rata-rata hitung *Generic Practice* (Praktik Generik)
$\bar{X}$ GWP = *mean* atau rata-rata hitung *Generic Work Product* (Produk Kerja Generik)

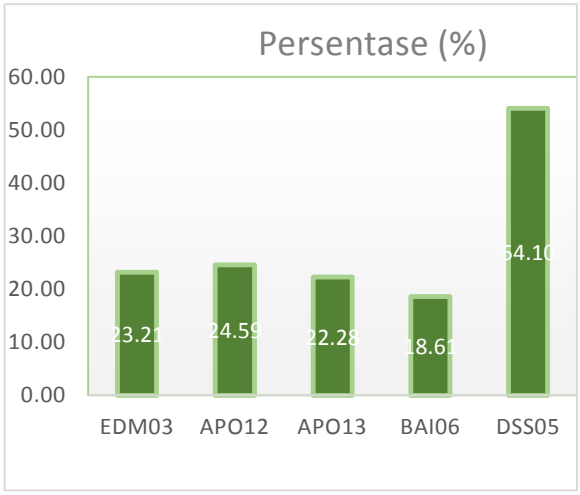
Tabel 2. 7 Contoh tabel penilaian kapabilitas Level 2 – 5

Nama Proses	Nilai
Penilaian Proses (*Process Assessment*/PA)	
Praktik Generik (*Generic Practice*)	$\bar{X}$ GP
Produk Kerja Generik (*Generic Work Product*)	$\bar{X}$ GWP

3. HASIL TINGKAT KAPABILITAS KEAMANAN SISTEM INFORMASI

Hasil nilai kapabilitas keamanan SI berada pada kisaran P (*Partially Achieved)* 15-50% dan ada satu proses yang berhasil mencapai kisaran L (*Largely Achieved*) 50-85%. Ini bisa dilihat pada Gambar 2.2.

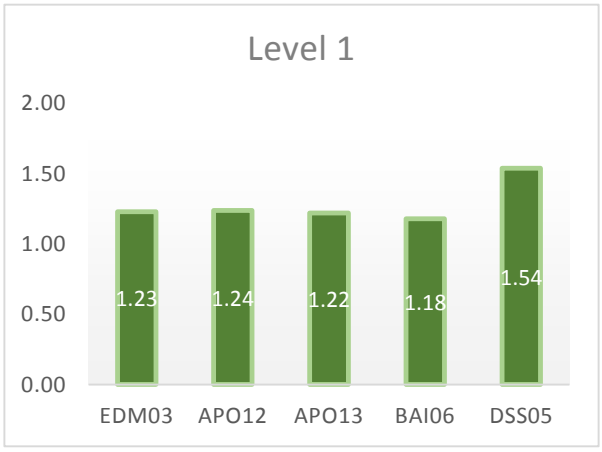
a. Proses EDM03 Mengelola Optimasi Risiko memperoleh predikat P (*Partially Achieved)* karena memperoleh nilai 23,21%.
b. Proses APO12 Mengelola Risiko memperoleh predikat P (*Partially Achieved)* karena memperoleh nilai 24,59%.
c. Proses APO13 Mengelola Keamanan memperoleh predikat P (*Partially Achieved)* karena memperoleh nilai 22,28%.
d. Proses BAI06 Mengelola Keamanan memperoleh predikat P (*Partially Achieved)* karena memperoleh nilai 18,61%.
e. Proses DSS05 Mengelola Layanan Keamanan memperoleh predikat L (*Largely Achieved*) karena memperoleh nilai 54,1%.



Gambar 3. 1 Hasil Persentase Pencapaian Level 1 Keamanan Sistem Informasi

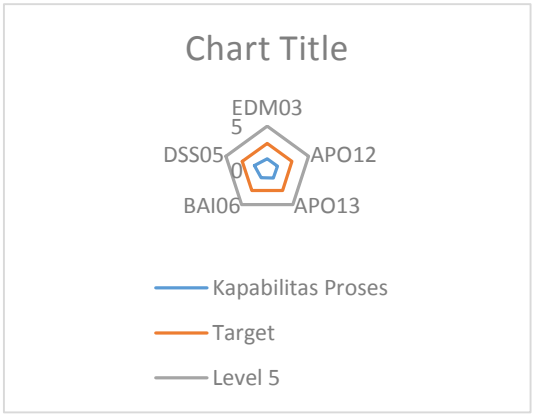
Hasil pengukuran kapabilitas keamanan SI menunjukkan bahwa dari kelima proses yang diukur tidak ada yang mampu mencapai level yang ditargetkan, yaitu level 3. Bahkan dari kelima proses itu hanya bisa mencapai level 1, seperti yang ditunjukkan pada Gambar 2.3.

a. Proses EDM03 Mengelola Optimasi Risiko mencapai level 1,23.
b. Proses APO12 Mengelola Risiko mencapai level 1,24.
c. Proses APO13 Mengelola Keamanan mencapai level 1,22.
d. Proses BAI06 Mengelola Keamanan mencapai level 1,18
e. Proses DSS05 Mengelola Layanan Keamanan mencapai level 1,54.



Gambar 3. 2 Hasil Tingkat Kapabilitas Keamanan Sistem Informasi

Pada Gambar 2.4 digambarkan bagaimana level yang dicapai saat ini dan level yang ditargetkan pada kapabilitas keamanan SI di Pemerintah Kota Yogyakarta. Level yang dicapai saat ini diwakili oleh warna biru. Sedangkan level yang menjadi target kapabilitas keamanan SI diwakili oleh warna merah.



Gambar 3. 3 Diagram Kesenjangan Level yang Dicapai Saat Ini dengan Target Level

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Berdasarkan hasil penilaian tingkat kapabilitas keamanan Sistem Informasi (SI) pada Pemerintah Kota Yogyakarta dapat disimpulkan sebagai berikut:

a. Hasil dari lima (5) proses tingkat kapabilitas keamanan SI, semua proses berada pada tingkat kapabilitas 1 *Performed Process* dengan rincian sebagai berikut:
   - Empat (4) proses berada pada level P (*Partially Achieved*), yaitu proses EDM03 Mengelola Optimasi Risiko, APO12 Mengelola Risiko, APO13 Mengelola Keamanan dan BAI06 Mengelola Perubahan.
   - Satu (1) proses berada pada level L (*Largely Achieved*), yaitu proses DSS05 Mengelola Layanan Keamanan.

b. Hasil penilaian tingkat kapabilitas keamanan SI tidak dapat mencapai level yang ditargetkan dalam jangka pendek yaitu level 3. Hal ini diakibatkan beberapa hal sebagai berikut:
   - Pemerintah Kota Yogyakarta memang belum menerapkan COBIT 5 untuk Keamanan Informasi sebagai kerangka kerja untuk keamanan SI di Pemerintah Kota Yogyakarta.
   - Masih kurangnya pendokumentasian laporan, pedoman dan atau SOP (Standar Operasional Prosedur) mengenai kebijakan terkait keamanan SI di Pemerintah Kota Yogyakarta. Sehingga meski sudah melakukan beberapa prosedur terkait keamanan SI, tidak mampu memperoleh nilai maksimal dalam penilaian tingkat kapabilitas keamanan SI.
   - Skala prioritas seringkali menyebabkan beberapa kegiatan terkait keamanan SI tidak dilakukan atau cenderung dinomorsekiankan. Sebagai contoh: cenderung mengabaikan membuat laporan atau dokumentasi sebuah proses karena ada prioritas melakukan pekerjaan lain yang saat itu lebih mendesak.

c. Untuk meningkatkan tingkat kapabilitas keamanan SI agar mencapai level yang ditargetkan, Bagian TIT Setda Kota Yogyakarta harus melakukan serangkaian praktik dasar perbaikan proses dan menghasilkan serangkaian produk kerja pada level 1 kinerja proses (*performed process*). Dilanjutkan dengan melakukan serangkaian praktik generik dan produk kerja generik pada level 2 proses dikelola (*managed process*).

4.2. Saran

Berdasarkan penelitian yang telah dilakukan, adapun saran-saran yang perlu dipertimbangkan Pemerintah Kota Yogyakarta khususnya Bagian TIT Setda Kota Yogyakarta untuk meningkatkan kapabilitas keamanan SI meliputi:

a. Melakukan rekomendasi yang diberikan agar minimal bisa mencapai nilai di atas 85% sampai dengan 100% pada level 1 sehingga bisa naik ke level 2. Sebab serangkaian praktik dasar dan produk kerja yang terdapat pada level 1 merupakan syarat minimal dalam kerangka kerja COBIT 5 untuk Keamanan Informasi dalam kapabilitas keamanan SI.
b. Merencanakan dan melaksanakan audit keamanan SI secara rutin yang dilakukan oleh auditor independen. Atau minimal melakukan uji penetrasi (*penetration test*) secara rutin. Mendokumentasikan audit dan uji penetrasi tersebut secara rutin agar bisa dievaluasi dan dianalisis untuk terus memperbaiki keamanan SI Pemerintah Kota Yogyakarta.
c. Mendokumentasikan kebijakan atau membuat SOP (Standar Operasional Prosedur) untuk proses keamanan SI yang mengacu pada kerangka kerja COBIT 5 untuk Keamanan Informasi.

Untuk melengkapi penelitian ini, beberapa saran berikut dapat dilakukan oleh peneliti berikutnya:

a. Melakukan penelitian tingkat kapabilitas hasil pemetaan dari tujuan perusahaan (*enterprise goals*) nomor 7 yaitu Kelangsungan dan Ketersediaan Layanan Bisnis (*Business Service Continuity and Availability*) sebab wilayah Pemerintah Daerah Istimewa Yogyakarta merupakan wilayah rawan bencana.
b. Melakukan pengukuran tingkat keamanan SI menggunakan metode atau kerangka kerja yang lain.
c. Melakukan penelitian tingkat kapabilitas manajemen risiko (*Risk Management*) menggunakan COBIT 5 atau kerangka kerja atau standar lain.
d. Melakukan penelitian tingkat kapabilitas tata kelola teknologi informasi (TI) menggunakan COBIT 5 atau kerangka kerja atau standar lain.

PUSTAKA

Hassanzadeh, M., Jahangiri, N. & Brewster, B., 2014. A Conceptual Framework for Information Security Awareness, Assessment, and Training. In B. Akhgar & H. R. Arabnia, eds. *Emerging Trends in ICT Security*. pp. 99 – 109.

Huang, Z., Zavarsky, P. & Ruhl, R., 2009. 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 International Conference on Computational Science and Engineering*, 198, pp.386–391. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5283287.

ISACA, 2012a. *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT*, Available at: http://www.isaca.org/COBIT/Pages/default.aspx?cid=1003566&Appeal=PR [Accessed April 13, 2014].

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

ISACA, 2012c. *Process Assessment Model (PAM): Using COBIT ® 5*, ISACA. Available at: www.isaca.org.

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

Morimoto, S., 2009. Application of COBIT to Security Management in Information Systems Development. *2009 Fourth International Conference on Frontier of Computer Science and Technology*, pp.625–630. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5392853 [Accessed September 15, 2014].

Pemerintah Kota Yogyakarta, 2007a. *Peraturan Walikota Yogyakarta*,

Pemerintah Kota Yogyakarta, 2007b. *Peraturan Walikota Yogyakarta Nomor 76 Tahun 2007*,

Piamonte, A., 2012. VALIT2.0 - COBIT 5 Unlocking the Value of Technology Investments. , pp.1–41.

Sahibudin, S., Sharifi, M. & Ayat, M., 2008. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, pp.749–753. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4530569 [Accessed May 4, 2014].

Von Solms, B., 2005. Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), pp.99–104. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404805000210 [Accessed March 26, 2014].

Solms, Basie von Solms; Solms, R. von, 2009. *Information Security Governance*,

Spremic, M., 2011. Standards and Frameworks for Information System Security Auditing and Assurance. *World Congress on Engineering*, I, p.6.

Spremić, M., 2011. Governing Information System Security: Review of Approaches to Information System Security Assurance and Auditing. *Latest Trends in Applied Informatics and Computing*, pp.42–48.

Spremić, M. et al., 2010. 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 Advances in Business Administration*, pp.45–50.

Symantec, 2014. INTERNET SECURITY THREAT REPORT. , 19(April), p.98. Available at: http://www.symantec.com/threatreport/.

Wallhoff, J., 2000. *Combining ITIL with COBIT and 17799*,