

# PEMETAAN PENURUNAN TUJUAN COBIT 5 UNTUK AUDIT KEAMANAN SISTEM INFORMASI (STUDI KASUS: SISTEM INFORMASI AKADEMIK SEKOLAH TINGGI XYZ)

Candra Santosa <sup>1</sup>, Widyawan <sup>2</sup>

Mahasiswa S2 Teknik Elektro, Universitas Gadjah Mada <sup>1</sup>

Dosen S2 Teknik Elektro, Universitas Gadjah Mada <sup>2</sup>

Email: [candra.santosa@gmail.com](mailto:candra.santosa@gmail.com) <sup>1</sup>, [widyawan@ugm.ac.id](mailto:widyawan@ugm.ac.id) <sup>2</sup>

## Abstrak

Saat ini, hampir semua perguruan tinggi, termasuk Sekolah Tinggi XYZ, menggunakan Sistem Informasi Akademik (SIA) untuk pengelolaan layanan administrasi akademik. SIA dapat mencerminkan kualitas pengelolaan sebuah perguruan tinggi. Salah satu yang menentukan kualitas layanan SIA adalah tingkat keamanannya. Audit perlu dilakukan untuk mengetahui tingkat keamanan Sistem Informasi (SI). Keamanan SI dapat dipandang dari sisi teknis dan sisi tata kelola. Penelitian akan difokuskan pada sisi tata kelola, karena sejauh ini belum ditemukan insiden keamanan di sisi teknis pada SIA Sekolah Tinggi XYZ. Kerangka kerja COBIT 5, khususnya COBIT 5 *for Information Security*, merupakan salah satu kerangka yang dapat digunakan untuk mengukur tingkat keamanan SI dari sisi tata kelola. COBIT 5 dipilih karena dapat menjangkau semua pemangku kepentingan dan dapat dengan mudah diintegrasikan ke proses bisnis. Penelitian ini akan menyusun kerangka pengukuran untuk mengetahui tingkat kapabilitas proses dalam hal keamanan SI, khususnya SIA pada Sekolah Tinggi XYZ.

Kata Kunci: Keamanan, Sistem Informasi, Cobit 5

## 1. Pendahuluan

Sejak tahun 2009, Sekolah Tinggi XYZ menerapkan Sistem Informasi Akademik (SIA) untuk mengelola layanan administrasi akademik. Proses yang dikelola oleh SIA antara lain adalah: pengisian Kartu Rencana Studi, penjadwalan kuliah, pengelolaan nilai, pengelolaan biodata mahasiswa, dan lain-lain.

Dari proses yang dikelola, terdapat data-data sensitif seperti nilai mahasiswa dan data-data yang bersifat pribadi seperti biodata mahasiswa. Karena SIA menyimpan data-data yang sifatnya sensitif, pribadi, atau rahasia, maka data tersebut perlu dijaga keamanannya. Selain itu, SIA juga mencerminkan kualitas pengelolaan sebuah perguruan tinggi. Salah satu yang menentukan kualitas layanan SIA adalah tingkat keamanannya. Karena itu, diperlukan audit keamanan pada SIA untuk mengetahui tingkat keamanannya.

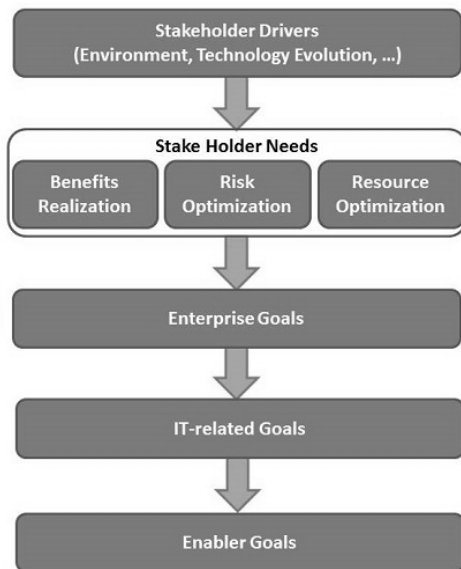
Audit keamanan dilakukan untuk mengetahui ada tidaknya pengamanan sistem informasi (SI) dan bagaimana proses pengamanan tersebut berjalan. Ukuran ini diperlukan untuk mengetahui apakah pengamanan yang ada sudah memenuhi standar

dan kriteria ideal yang ada. Di samping itu, audit dilakukan sebagai salah satu usaha untuk menilai resiko dan perlindungan terhadap aset organisasi. Dengan demikian dapat dipersiapkan keamanan yang lebih baik terhadap aset untuk mengurangi resiko yang mungkin muncul [1].

Audit sebagai bagian dari kendali internal harus dapat mengidentifikasi letak potensial resiko. Auditor harus menentukan area yang akan diaudit dengan memprioritaskan pada area dengan potensial resiko besar. Proses audit yang logis dan metodologis harus diformulasikan untuk memastikan sasaran telah tercakup [2]. Dalam audit juga diperlukan standar dan kriteria namun adakalanya standar yang tersedia masih berupa *best practices* dan aturan yang tidak formal [1].

Banyak penelitian mengenai kerangka kerja *Control Objectives for Information and Related Technology* (COBIT) 5 yang menyatakan bahwa COBIT 5 merupakan kerangka kerja untuk audit keamanan SI dan mampu menyediakan tata kelola keamanan informasi yang menyeluruh [3][4][5][6][7]. COBIT 5 merupakan kerangka kerja yang lengkap dan diterima secara

internasional untuk mengatur dan mengelola teknologi informasi (TI) organisasi yang mendukung eksekutif perusahaan dan manajemen dalam rangka pencapaian tujuan organisasi dan tujuan TI terkait. COBIT 5 yang merupakan integrasi dari RISK IT, VAL IT, BMIS, dan COBIT 4.1 dalam satu kerangka kerja. COBIT 5 menjelaskan 5 prinsip dan 7 pengungkit (*enabler*) yang mendukung organisasi dalam pengembangan, implementasi, dan perbaikan berkelanjutan dan pemantauan terkait tata kelola TI dan praktik manajemen yang baik. COBIT 5 mengidentifikasi proses yang tepat dengan menggunakan mekanisme penurunan tujuan (*Goal Cascade*). Penurunan tujuan pada COBIT 5 adalah mekanisme untuk menerjemahkan kebutuhan pemangku kepentingan menjadi Tujuan Organisasi (*Enterprise Goals*), Tujuan terkait TI (*IT-related Goals*), dan Tujuan Pengungkit (*Enabler Goals*) yang spesifik, nyata, dan sesuai. Penerjemahan ini memungkinkan untuk menetapkan tujuan yang spesifik pada setiap tingkatan dan pada setiap area institusi dalam mendukung tujuan dan permintaan pemangku kepentingan secara keseluruhan, dan dengan demikian secara efektif mendukung keselarasan antara kebutuhan institusi dengan solusi dan layanan TI [8].



Gambar 1. Penurunan Tujuan COBIT 5 (COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012)

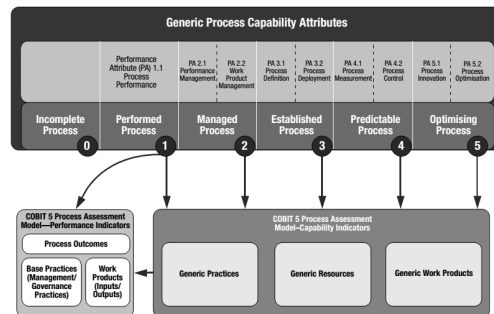
Pemahaman terhadap peran dan tanggung jawab manajemen dalam setiap proses merupakan kunci kesuksesan suatu tata kelola TI. Tabel RACI (Responsible, Accountable, Consulted and Informed) dalam COBIT menyediakan matriks untuk seluruh aktivitas dan otorisasi keputusan yang diambil dalam suatu organisasi yang dikaitkan dengan seluruh pihak atau posisi yang

terlibat. Responsible artinya orang yang melakukan suatu kegiatan atau pekerjaan. Accountable artinya orang yang memberikan arahan dan memiliki otoritas dalam suatu kegiatan. Sedangkan dua peran lainnya (Consulted and Informed) merupakan orang-orang yang terlibat dan memberi dukungan dalam suatu kegiatan.

Pada penelitian ini penulis menggunakan COBIT 5 khususnya COBIT 5 for Information Security sebagai kerangka dan standar untuk melakukan audit keamanan SI di Sekolah Tinggi XYZ. COBIT 5 dipilih karena COBIT dapat menjangkau semua pemangku kepentingan dan dapat dengan mudah diintegrasikan dengan proses bisnis [9].

Pemahaman terhadap peran dan tanggung jawab manajemen dalam setiap proses merupakan kunci kesuksesan suatu tata kelola TI, termasuk tata kelola keamanan TI. Tabel RACI (*Responsible, Accountable, Consulted and Informed*) dalam COBIT menyediakan matriks untuk seluruh aktivitas dan otorisasi keputusan yang diambil dalam suatu organisasi yang dikaitkan dengan seluruh pihak atau posisi yang terlibat. *Responsible* artinya orang yang melakukan suatu kegiatan atau pekerjaan. *Accountable* artinya orang yang memberikan arahan dan memiliki otoritas dalam suatu kegiatan. Sedangkan dua peran lainnya (*Consulted and Informed*) merupakan orang-orang yang terlibat dan memberi dukungan dalam suatu kegiatan.

Kapabilitas proses adalah alat bantu yang dapat digunakan untuk melakukan evaluasi pada organisasi untuk menilai pencapaian tiap proses TI. Dengan kapabilitas proses, organisasi bisa mengidentifikasi kondisi aktual dan yang diharapkan dari kinerja organisasi, mengetahui titik kelemahan, serta membuat rekomendasi. Kapabilitas proses dibagi menjadi 6 tingkat, mulai dari 0 (*Incomplete process*) sampai dengan 5 (*Optimising process*). Penilaian pencapaian tiap kapabilitas proses mengadopsi skala penilaian standar yang ditetapkan dalam standar ISO/IEC 15504 [10], seperti tampak pada Tabel 1.



Gambar 2. Model Kapabilitas Proses COBIT 5 (COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012)

Tabel 1: Tingkatan Peringkat

Tingkatan Peringkat		
	Keterangan	Pencapaian
N	Tidak tercapai	0% - 15%
P	Sebagian tercapai	>15% - 50%
L	Sebagian besar tercapai	>50% - 85%
F	Tercapai sepenuhnya	>85% - 100%

Sumber: *Process Assessment Model (PAM): Using COBIT 5*, 2013

Penelitian ini akan menyusun kerangka pengukuran untuk mengetahui tingkat kapabilitas proses dalam hal keamanan SI, khususnya SIA pada Sekolah Tinggi XYZ. Penelitian diawali dengan identifikasi terhadap tujuan organisasi pada Sekolah Tinggi XYZ yang erat kaitannya dengan SIA. Hasil identifikasi akan dipetakan ke dalam proses dalam COBIT 5. Pemetaan ini akan dipakai sebagai dasar menyusun kuesioner berdasarkan COBIT 5.

## 2. Metode

Metode penelitian yang dilakukan meliputi tahapan-tahapan berikut:

1. Pendahuluan. Dalam tahap ini dilakukan pendefinisian mengenai latar belakang, rumusan masalah, tujuan dan manfaat penelitian.
2. Tinjauan Pustaka. Dalam tahap ini dilakukan aktivitas penelaahan dokumen Renstra Sekolah Tinggi XYZ 2015-2019 dan dokumen resmi lainnya terkait struktur organisasi, tugas dan fungsi (tusi) Sekolah Tinggi XYZ. Selain itu, juga dilakukan studi literatur terkait COBIT 5.
3. Pengumpulan Data. Dalam tahap ini dilakukan wawancara untuk mendapatkan konfirmasi mengenai peran serta tanggung jawab para pemangku kepentingan yang terlibat dalam proses bisnis di Sekolah Tinggi XYZ. Tahap ini juga digunakan dasar pemetaan responden dan penyusunan kuesioner.

### 2.1 Metode Pengumpulan Data

Dalam penelitian ini, pengumpulan data dilakukan dengan observasi, kuesioner, dan wawancara terhadap pihak-pihak yang terkait dengan proses bisnis pengelolaan SIA di Sekolah Tinggi XYZ. Responden dipilih melalui pemetaan penurunan tujuan COBIT 5, sesuai dengan tugas dan fungsi masing-masing responden terkait SIA.

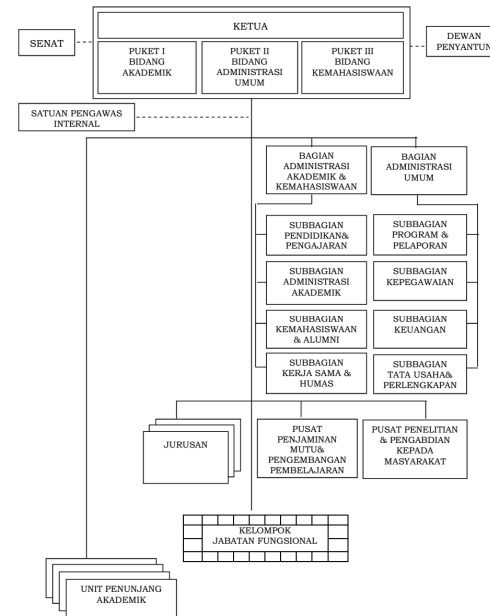
### 2.2 Metode Analisis Data

Teknik analisis data yang digunakan adalah teknik hitung analisis deskriptif untuk mendeskripsikan variabel penelitian dalam pengukuran. Analisis data tidak menggunakan *statistic inferential* karena tidak terdapat hipotesis dalam penelitian ini.

## 3. Hasil dan Pembahasan

### 3.1 Profil Organisasi

Sekolah Tinggi XYZ dipimpin seorang Ketua yang dibantu oleh 3 orang Pembantu Ketua. Untuk struktur organisasi Sekolah Tinggi XYZ bisa dilihat pada Gambar 3.



Gambar 3. Struktur Organisasi Sekolah Tinggi XYZ (Statuta Sekolah Tinggi XYZ, 2014)

Unit Penunjang Akademik bertanggung jawab kepada Ketua, dengan pembinaan dari Puket I. Setiap unit dipimpin oleh seorang Kepala. Unit Penunjang Akademik terdiri atas:

1. Unit Teknologi Informasi dan Komunikasi
2. Unit Perpustakaan dan Dokumentasi
3. Unit Laboratorium
4. Unit Studio dan Pemancar.

Pengelolaan SIA dilakukan oleh Unit Teknologi Informasi dan Komunikasi (TIK). Hal ini sesuai dengan tugas Unit TIK, yaitu: mengorganisasikan sekumpulan komponen yang terdiri atas *hardware*, *software*, *brainware*, prosedur, dan aturan untuk mengolah data menjadi informasi. Untuk fungsi pengamanan pada SIA, juga bertumpu pada Unit TIK. Ini tercermin pada salah satu fungsi Unit TIK, yaitu: mengelola sistem informasi yang ada, termasuk menganalisis dan mengidentifikasi kelemahan sistem dan penyalahgunaannya, menciptakan lingkungan pengendali, dan memastikan kualitas sistem.

Sedangkan operasional SIA dilakukan oleh Bagian Administrasi Akademik dan Kemahasiswaan. Hal ini sesuai dengan tugas Bagian Administrasi Akademik dan Kemahasiswaan, yaitu: memberikan layanan di bidang pendidikan dan pengajaran, administrasi

akademik, kemahasiswaan dan alumni, serta kerjasama dan hubungan masyarakat. [11]

### 3.2 Pemetaan Penurunan Tujuan

COBIT 5 menetapkan 17 tujuan organisasi yang terdiri dari dimensi Kartu Nilai Keseimbangan (*Balanced Scorecard*) yang membawahi tujuan organisasi yang sesuai, tujuan organisasi dan hubungan antara ketiga tujuan inti organisasi (realisasi keuntungan, optimasi risiko dan optimasi sumber daya) [8]. Dimensi Kartu Nilai Keseimbangan mengkategorikan 17 tujuan organisasi ke dalam 4 dimensi, yaitu dimensi Keuangan, Pelanggan, Proses Bisnis Internal, dan Belajar dan Bertumbuh.

Tujuan Organisasi dalam COBIT 5 akan diidentifikasi dari Tujuan Sekolah Tinggi XYZ yang tertuang dalam Rencana Strategis (Renstra) tahun 2015-2019. 4 tujuan Sekolah Tinggi XYZ dapat dipetakan ke 4 tujuan organisasi dalam COBIT 5. 4 tujuan organisasi tersebut adalah: Portofolio dari Produk dan Layanan yang Kompetitif; Kelangsungan dan Ketersediaan Layanan Bisnis; Produktivitas Operasional dan Staf; Karyawan yang Mempunyai Keahlian dan Motivasi. Tujuan organisasi tersebut akan dipetakan ke tujuan terkait TI dalam COBIT 5.

Tabel 2: Identifikasi Tujuan Organisasi dengan Tujuan Sekolah Tinggi XYZ

Dimensi	No	Tujuan Organisasi	Tujuan Sekolah Tinggi XYZ
Keuangan	2	Portofolio dari Produk dan Layanan yang Kompetitif	Mengembangkan sumber-sumber pendapatan yang berkelanjutan
Pelanggan	7	Kelangsungan dan Ketersediaan Layanan Bisnis	Meningkatkan Produktifitas dan Kualitas Tri Dharma Perguruan Tinggi
Proses Bisnis Internal	14	Produktivitas Operasional dan Staf	Mengembangkan sistem manajemen yang sehat dan harmonis
Belajar dan Bertumbuh	16	Karyawan yang Mempunyai Keahlian dan Motivasi	Melakukan Transformasi dan Pengembangan Kelembagaan

Dari 4 tujuan organisasi tersebut, penulis akan memfokuskan pada tujuan Kelangsungan dan Ketersediaan Layanan Bisnis. Tujuan tersebut dipilih karena tujuan tersebut lebih erat kaitannya dengan SIA dibandingkan dengan 3 tujuan lainnya. Tujuan organisasi tersebut dipetakan ke 17 Tujuan terkait TI dalam COBIT 5. Hasil pemetaan ini mendapatkan 3 Tujuan terkait TI dalam COBIT 5 dengan cara memilih proses

yang berkategori primer, seperti yang tercantum dalam Tabel 3.

3 Tujuan terkait TI dalam COBIT 5 yang sudah diperoleh dipetakan ke dalam 37 proses TI COBIT 5. Pemetaan ini juga hanya memilih proses yang berkategori primer. Hasil pemetaan ini mendapatkan 18 proses TI dalam COBIT 5, seperti yang tercantum pada Tabel 4.

Tabel 3: Pemetaan Tujuan Organisasi nomor 7 ke Tujuan terkait TI

		Tujuan Organisasi
		Kelangsungan dan Ketersediaan Layanan Bisnis
		7
Tujuan terkait TI		
4	Mengelola resiko bisnis terkait TI	P
10	Keamanan pada informasi, infrastruktur pengolah, dan aplikasi	P
14	Ketersediaan informasi yang dapat diandalkan dan digunakan untuk pengambilan keputusan	P

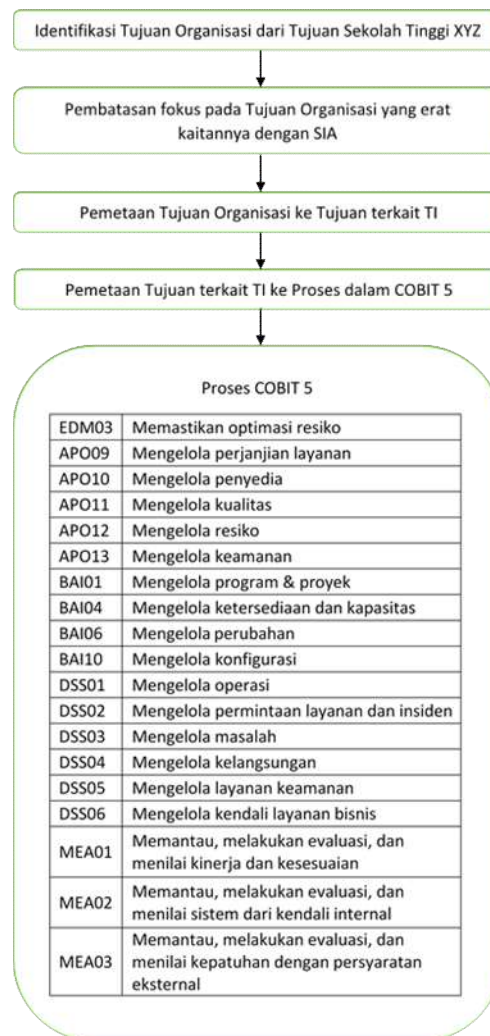
Tabel 4: Pemetaan Tujuan terkait TI ke Proses dalam COBIT 5

		Tujuan terkait TI		
		Mengelola resiko bisnis terkait TI	Keamanan pada informasi, infrastruktur pengolah, dan aplikasi	Ketersediaan informasi yang dapat diandalkan dan digunakan untuk pengambilan keputusan
		4	10	14
Proses COBIT 5				
EDM03	Memastikan optimasi resiko	P	P	S
APO09	Mengelola perjanjian layanan	S	S	P

AP010	Mengelola penyedia	P	S	S
AP012	Mengelola resiko	P	P	S
AP013	Mengelola keamanan	P	P	P
BAI01	Mengelola program & proyek	P		
BAI04	Mengelola ketersediaan dan kapasitas	S		P
BAI06	Mengelola perubahan	P	P	S
BAI10	Mengelola konfigurasi	S	S	P
DSS01	Mengelola operasi	P	S	S
DSS02	Mengelola permintaan layanan dan insiden	P	S	S
DSS03	Mengelola masalah	P		P
DSS04	Mengelola kelangsungan	P	S	P
DSS05	Mengelola layanan keamanan	P	P	S
DSS06	Mengelola kendali layanan bisnis	P	S	S
MEA01	Memantau, melakukan evaluasi, dan menilai kinerja dan kesesuaian	P	S	S
MEA02	Memantau, melakukan evaluasi, dan menilai sistem dari kendali internal	P	S	S
MEA03	Memantau, melakukan evaluasi, dan menilai kepatuhan dengan persyaratan eksternal	P	S	

Proses identifikasi dan pemetaan ini sesuai dengan penurunan tujuan dalam COBIT 5. Diawali dengan mengidentifikasi Tujuan Organisasi. Identifikasi tujuan organisasi ini untuk mencari kesesuaian antara tujuan organisasi terhadap 17 Tujuan Organisasi dalam COBIT 5. Tahap selanjutnya yaitu melakukan pemetaan Tujuan Organisasi dengan 17 Tujuan terkait TI dalam COBIT 5. Hasil pemetaan Tujuan terkait TI ini akan digunakan untuk pemetaan terhadap 37 proses TI 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 penurunan tujuan ini digambarkan pada Gambar 4.



Gambar 4. Penurunan Tujuan Penelitian

### 3.3 Pemetaan Responden dan Penyusunan Kuesioner

Setelah mendapatkan penurunan tujuan hingga ke proses COBIT 5, langkah selanjutnya adalah menentukan responden. Responden ditentukan menggunakan tabel RACI sesuai dengan rekomendasi dalam kerangka kerja COBIT 5. Penyusunan tabel RACI dilakukan pada tiap proses dalam COBIT 5, dengan mempertimbangkan proses bisnis terkait pengelolaan SIA dan tusi dari pihak yang terlibat dalam proses bisnis tersebut. Informasi mengenai proses bisnis dan tusi didapatkan melalui observasi, wawancara dengan pihak terkait di Sekolah Tinggi XYZ, dan studi literatur terkait tusi Sekolah Tinggi XYZ.

Tabel 5: Tabel RACI

TABEL RACI											
Proses	Kategori										
	Ketua	Puket I Bidang Akademik	Kepala Pusat Penjaminan Mutu	Staf PPM	Kabag Administrasi Umum	Kabag Administrasi Akademik & Kemahasiswaan	Kepala Unit TIK	PPK	Pejabat Pengadaan	Staf Unit TIK	Operator SIA
EDM03	A	R				R					
APO09	I				I	C	A	R			
APO10	I				I	C	A	R			
APO12	I	I			C	A		R			
APO13	I	I				A		R			
BAI01	I	I				A		R	R	R	
BAI04	I	I			C	A		R			
BAI06	C	C			C	A		R			
BAI10	I	I			C	A		R			
DSS01	I	I			A	C			C	R	
DSS02	I	I			C	A			R		
DSS03	C	A			R	R					
DSS04	I	I			C	A			R	R	
DSS05	I	I				A			R		
DSS06	I	C			A	C				R	
MEA01	I	I			C	C					
MEA02	I	I	A	R	C	C					
MEA03	I	I	A	R	C	C					

Pihak yang menjadi responden adalah pihak dengan peran R (*Responsible*) dan A (*Accountable*). Peran R dan A merupakan peran yang terlibat secara langsung di proses COBIT 5. Kuesioner Level 1 berpedoman pada aktivitas proses COBIT 5 dan COBIT 5 for Information Security. Penilaian disusun dengan pedoman pada Model Penilaian Proses (*Process Assessment Model*) pada COBIT 5. Responden cukup mengisi capaian dari tiap atribut dengan skala 0% - 100%. Kemudian hasilnya dirata-rata dan hasilnya menentukan tingkat kapabilitas tiap proses.

Tabel 6: Kuesioner Proses EDM03

Proses EDM03 Memastikan Optimalisasi Resiko		Capaian
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 Resiko	
Keluaran Produk Kerja		
EDM03-WP1	Menyelaraskan Indikator Risiko Utama organisasi dengan Indikator Risiko Utama keamanan SI	
EDM03-WP2	Keamanan SI pada tingkat yang dapat ditolerir	
EDM03-WP3	Memperbarui kebijakan manajemen risiko	
Praktik Dasar		
EDM03-BP2	Mengarahkan Manajemen Resiko	
Keluaran Produk Kerja		
EDM03-WP4	Tindakan perbaikan untuk mengatasi penyimpangan manajemen risiko	
EDM03-WP5	Sasaran utama dipantau untuk manajemen risiko	
EDM03-WP6	Langkah nyata untuk mengukur manajemen risiko	
Praktik Dasar		
EDM03-BP3	Memantau Manajemen Resiko	
Keluaran Produk Kerja		
EDM03-WP7	Langkah perbaikan dalam menangani penyimpangan manajemen risiko	
EDM03-WP8	Mengangkat masalah manajemen risiko ke pihak manajemen	

Contoh kuesioner pada Tabel 6 merupakan contoh kuesioner dari proses EDM03. Untuk proses yang lain, akan dilakukan hal yang sama

dengan poin-poin penilaian sesuai dengan pedoman pada COBIT 5.

#### 4. Kesimpulan

Dari Rencana Strategis Sekolah Tinggi XYZ dipetakan terhadap Tujuan Organisasi (*Enterprise Goals*) COBIT 5. Setelah didapatkan Tujuan Organisasi, kemudian dipetakan ke Tujuan Terkait TI (*IT-related Goals*) COBIT 5. Tujuan Terkait TI yang didapat juga dipetakan ke 37 proses dalam COBIT 5. 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 pada Sekolah Tinggi XYZ sesuai dengan tabel RACI.

#### Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang tak terhingga kepada Bapak Widyawan, Ph.D. dan Bapak Dr. Lukito Edi Nugroho atas bimbingannya. Terima kasih juga penulis ucapkan kepada Mas Gamal dan Mas Wisnu atas pencerahan dan masukannya.

#### Daftar Pustaka

- [1] Senft, S., and F. Gallegos. 2009. *Information Technology Control And Audit Third Edition*. 3 ed. Boca Raton: Taylor & Fancis Group
- [2] Davis, C., dan M. S. Wheler. 2007. *IT Auditing: Using Control to Protect Information Assets*. New York: MacGraw-Hill Companies.
- [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. Zavorsky, 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*. Illinois: ISACA, 2012.
- [9] Arora, V. "Comparing different information security standards: COBIT v s. ISO 27001," 2010. [Online]. Available: <http://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf> [Accessed: 1-Oct-2015]
- [10] ISACA, *Process Assessment Model (PAM): Using COBIT® 5*. Illinois: ISACA, 2013.
- [11] Sekolah Tinggi XYZ, *Statuta Sekolah Tinggi XYZ*. Jakarta, 2014.