Indeks Penilaian Kematangan (*Maturity)* Manajemen Keamanan Layanan TI

Farroh Sakinah, Bambang Setiawan
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, ITS Sukolilo, Surabaya, 60111
E-mail : setiawan@is.its.ac.id

***Abstrak*—Pemanfaatan Teknologi Informasi (TI) dalam mendukung terselenggaranya pelayanan yang optimal menjadi kebutuhan utama organisasi saat ini. Jaminan pengelolaan layanan dan keamanan yang baik menjadi salah satu tolok ukurnya. Pengimplementasian sebuah standar menjadi salah satu solusinya meskipun penggunaan satu buah standar dirasa belum maksimal melihat cakupan yang disediakan kurang luas sehingga diadakannya upaya penggabungan beberapa standar dengan harapan standar-standar tersebut dapat saling melengkapi. Pengimplementasian beberapa standar ini dapat dimonitoring tingkat kematangannya (*maturity*) dengan menggunakan alat ukur penilaian kematangan (*maturity*). Alat ukur kematangan (*maturity*) manajemen keamanan layanan ini merupakan gabungan pemetaan dari *control objective IT Governance* COBIT 4.1 yang dipenuhi kebutuhan manajemen layanannya sesuai dengan *Service Management* di dalam ITIL v3 *(Information Technology Infrastructure Library*). Selanjutnya kebutuhan manajemen layanan ini diukur dengan *maturity level* COBIT 4.1 dan disesuaikan dengan *framework* ISO 27000 untuk memaksimalkan manajemen keamanan informasi.**

Kata Kunci : COBIT 4.1, ISO 27000, ITIL v3, Keamanan Teknologi Informasi, Manajemen Layanan, Maturity

I. PENDAHULUAN

Peran teknologi bagi komunikasi dalam proses bisnis oleh perusahaan atau organisasi dalam bentuk layanan semakin dirasakan manfaatnya yang akhirnya mendorong pemanfaatan teknologi informasi dengan jaminan pengelolaan layanan yang baik menjadi kebutuhan yang mendasar. Di sisi lain, pemerintah sebagai pihak *regulator* memberikan tolok ukur akan kebijakan pelaksanaan perusahaan yang berhubungan dengan manajemen layanan dan keamanan [1] terutama bagi organisasi penyelenggara pelayanan publik.

Penggunaan standar pelayanan dan keamanan dalam memandu proses bisnis menjadi salah satu solusinya akan tetapi organisasi memiliki kesulitan tersendiri untuk memahami sejauh mana standar tersebut telah terimplementasikan terlebih ketika organisasi mengimplemetasikan lebih dari satu buah standar. Hal ini dimungkinkan terjadi karena ruang lingkup atau fokusan sebuah standar dirasa kurang luas cakupannya untuk memenuhi seluruh kebutuhan manajemen TI [2].

Berdasarkan hal tersebut, penelitian ini akan menggabungkan beberapa standar pengelolaan dan keamanan layanan yang dapat diukur pencapaian dan kesiapannya dalam sebuah indeks penilaian untuk membantu organisasi mengetahu tingkat kematangan (*maturity*) manajemen keamanan layanan di organisasinya.

Pembuatan indeks penilaian ini menggunakan standar ISO 27000 terutama ISO 27001 dan 27002 sebagai *information security management*. Kerangka ITIL digunakan untuk konsep dan teknik pengelola serta operasi teknologi informasi (TI) yang berdasarkan *control objective* dan pengukuran *maturity model* oleh COBIT 4.1 [2].

II. METODE PEMETAAN INDEKS

Meskipun manajemen layanan dan manajemen keamanan merupakan dua buah prespektif yang berbeda, tetapi keduanya memiliki satu kesamaan dalam proses yaitu, sebuah organisasi harus mampu merencanakan (*plan*) , melakukan (*do*), memantau (*check*) dan memelihara (*act*) setiap strategi dalam proses bisnisnya [3] sehingga dimungkinkan beberapa standar dipetakan dan digunakan secara bersamaan.

Metode yang digunakan dalam penelitian ini dijelaskan dalam bagan berikut :

Gambar 1 Metodologi Penelitian

Langkah pertama yang dilakukan adalah melakukan studi literatur terkait dengan manajemen layanan dan keamanan serta melakukan wawancara dan pengambilan data. Studi kasus yang digunakan dalam penelitian ini mengambil data dari sebuah badan penyedia layanan TI di sebuah perguruan tinggi di kota Surabaya.

Langkah selanjutnya adalah proses perancangan dan uji coba indeks yang kemudian akan dilakukan kajian lanjutan pelaksanaan penerapan indeks pada sebuah organisasi.

III. TINJAUAN PUSTAKA

3.1 Tata kelola Teknologi Informasi

Tata Kelola Teknologi Informasi didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis dapat tercapai melalui penambahan nilai sekaligus terkait dengan pengelolaan proses TI. Tidak hanya pengelolaan proses, tetapi juga memastikan bahwa proses tersebut telah dipenuhi oleh sumber daya TI yang memberikan dukungan secara optimal terhadap pemenuhan tujuan bisnis [4].

Committee of Sponsoring Organizations of the Treadway Commission, atau disingkat COSO, telah menyusun suatu definisi umum untuk pengendalian, standar, dan kriteria internal yang dapat digunakan perusahaan menilai sistem pengendalian TI internalnya dalam pengelolaannya bernama *Control Objective for Information and related Technology*, disingkat COBIT.

Dalam praktik penggunaannya di dalam *IT Operation*, terdapat beberapa tiang penyangga atau rujukan agar terciptanya bangunan TI yang kokoh yaitu, *Service Management*, *App. Development (SDLC)*, *IT Security*, *Project Management*, *IT Planning* dan *Quality System* [4]. Adapun fokus utama pengerjaan penelitian ini adalah tata kelola teknologi informasi pada *IT Security.*

3.2 ITIL v3

Information Technology Infrastructure Library (ITIL) adalah standar praktik yang terkait dengan layanan teknologi informasi. ITIL menyediakan *framework*/ kerangka praktik yang baik dalam memandu pengelolaan manajemen layanan TI [2].

Service atau layanan adalah tentang menyampaikan *value* (nilai) kepada konsumen. ITIL mendefinisikan layanan sebagai sarana penyampaian *value* kepada pelanggan guna menfasilitasi hasil yang pelanggan inginkan tanpa adanya penambahan biaya atau resiko yang spesifik [5].

ITIL mendefinisikan *service management* sebagai sebuah seperangkat kemampuan organisasi yang terspesialisasi untuk memberikan nilai kepada pelanggan dalam bentuk jasa atau layanan. *Tedapat lima buah tahap* di dalam ITIL yaitu, *Service Strategy, Service Design, Service Transition, Service Operation* dan *Continual Service Improvement* [5].

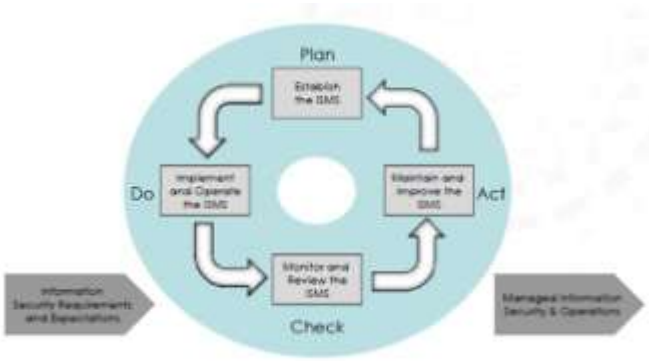
3.3 ISO 27000: 2005

Tujuan dari keamanan informasi adalah untuk melindungi aset guna memastikan kelangsungan bisnis tetap berjalan, meminimalkan risiko bisnis dan memaksimalkan keuntungan perusahaan [6].

ISO/IEC 27000:2005 *series* adalah sebuah standar untuk manajemen keamanan informasi yang diakui secara internasional. ISO yang akan digunakan pada pengerjaan penelitian ini adalah ISO 27001:2005 dan 27002:2005.

1) *3.3.1 ISO/IEC 27001:2005*

ISO/IEC 27001:2005 merupakan sebuah standar untuk membangun sistem manajemen keamanan informasi (ISMS). Di dalamnya terdapat empat buah langkah proses untuk menerapkan ISO/IEC 17799 dan bagaimanakah cara untuk menetapkan, menerapkan, memantau dan memelihara ISMS [7].



Gambar 2 ISO 27001:2005

2) *3.3.2 ISO/IEC 27002:2005*

ISO/IEC 27002 pada awalnya diterbitkan untuk mengganti standar sebelumnya yaitu ISO 17799:2005 yang digunakan sebagai *best practice* manajemen keamanan informasi. Pada dasarnya, ISO 27002 menguraikan ratusan kontrol potensial dan mekanisme kontrolnya, yang akan di implementasikan, dan mengikuti teori yang di pandukan dalam ISO 27001 [8].

Di dalam ISO/IEC 27002 ditetapkan pedoman yang digunakan sebagai prinsip umum untuk memulai, melaksanakan, memelihara dan meningkatkan keamanan informasi dalam sebuah organisasi. ISO/IEC 27002 memiliki 14 rincian area yang sebelumnya hanya dijelaskan dalam 11 area dalam ISO/IEC 17799.

Area dalam ISO/IEC 27002 :

1. *Framework - Acceptable Use of Information Technology Resources*
2. *Information Security Definition & Terms*
3. *Risk Assessment*
4. *Security Policy*
5. *Organization of Information Security*
6. *Asset Management*
7. *Human Resources Security*
8. *Physical and Environmental Security*
9. *Communication and Operations Management*
10. *Access Control*
11. *Information System Acquisition, Development and Maintenance*
12. *Information Security Incident Management*
13. *Business Continuity Management*
14. *Compliance*

3.4 Framework COBIT 4.1

Control Objectives for Information and related Technology (COBIT) adalah sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, manajemen dan pengguna *(user)* untuk menjembatani *gap* antara risiko bisnis, melaksanakan kontrol serta permasalahan-permasalahan teknis [4].

Di dalam *practice* yang diberikan oleh COBIT, diberikan langkah-langkah untuk menjamin pelayanan dan pemberian standar pengukuran untuk menilai ketika terdapat kesalahan dalam penggunaannya.

Terdapat 13 *control objective* dalam memastikan penyampaian dan dukungan terhadap layanan yang baik, mulai dari *Define and Manage Service Levels, Manage Performance and Capacity, Manage Performance and Capacity, Ensure Continuous Service, Ensure Systems Security, Identify and Allocate Costs, Educate and Train Users, Manage Service Desk and Incidents, Manage the Configuration, Manage Problem, Manage Data, Manage the Physical Environment* dan *Manage Operations*[4].

COBIT juga menyediakan parameter untuk penilaian pengelolaan TI pada suatu organisasi dengan menggunakan *maturity models* yang bisa digunakan untuk penilaian kesadaran pihak pengelola (*management awareness*) dan tingkat kematangan (*maturity level*) menggunakan metode penilaian (*scoring*).

Gambar 3 Maturity Model COBIT 4.1

3.5 ITIL dan COBIT Terkait dengan ISO 27000

Saint - Jerman [2] menyoroti bahwa pelaksanaan keamanan dan kontrol ISO/IEC 27000 yang dikombinasikan dengan standar ITIL atau COBIT mampu mengurangi ancaman kritis yang dapat mengganggu hasil proyek.

ISO/IEC 27000 memiliki struktur utama untuk diterapkan dalam menjamin keamanan organisasi secara keseluruhan di semua tingkat. Masalah administrasi dan manajemen yang tidak dibahas dalam standar ISO/IEC 27000 ditangani oleh ITIL dan COBIT. Hal ini dimungkinkan karena ISO/IEC 27000 memiliki fitur untuk menjaga kerahasiaan, integritas dan ketersediaan informasi dalam organisasi. Ketersediaan informasi ini ditangani dalam ITIL dan COBIT dengan aspek kualitas, kehandalan dan pemeliharaan TI .

Metode yang akan digunakan adalah, ITIL digunakan untuk menentukan strategi, konsep, dan proses yang terkait dengan manajemen TI. COBIT digunakan untuk mengevaluasi faktor penentu keberhasilan, metrik, indikator dan audit, standar ISO/IEC 27000 untuk memandu pengelolaan TI dalam kaitannya dengan masalah keamanan.

3.6 STUDI KASUS

Studi kasus pembuatan indeks penilaian kematangan (maturity) manajemen keamanan layanan dilakukan pada sebuah organisasi penyelenggara layanan TI di salah satu perguruan tinggi di kota Surabaya yang memiliki fungsi sebagai unit pelaksana teknis di bidang pengelolahan data.

Dalam proses bisnis keseharian, organisasi ini memiliki tugas mengumpulkan, mengolah, menyajikan, dan menyimpan data dan informasi serta memberikan layanan untuk program-program pendidikan, penelitian, dan pengabdian kepada masyarakat.

Untuk menyelenggarakan tugas tersebut organisasi ini telah membagi tugas dan fungsinya dalam struktur organisasi yang baik dengan dilengkapi beberapa *Standard Operasional Procedure* (SOP).

Untuk menemukan fokusan dalam kondisi eksisting organisasi, maka disebarkan kuisioner untuk pengumpulan data. Kuisioner diberikan kepada pihak manajemen utama organisasi.

Berdasarkan pengumpulan data, diketahui bahwa :

Tabel 1 Hasil Pengambilan Data

Proses Manajemen	Kondisi Eksisting	Kondisi Ideal	Keterangan
Kesiapan Organisasi	2.87	4	Tidak Sesuai
Manajemen Aset	2.96	4	Tidak Sesuai
Penyusunan TI	2.25	4	Tidak Sesuai
Pelaksanaan TI	2.34	4	Tidak Sesuai
Perencanaan Pengembangan	1.59	4	Sangat Tidak Sesuai

* Kuisioner menggunakan skala likert

Didapati bahwa organisasi belum memiliki standar atau manajemen keamanan layanan yang baik. Hal ini tercerminkan dari kelengkapan SOP yang dimiliki dan kepatuhan organisasi terhadap setiap SOP yang dimiliki.

IV. PERANCANGAN INDEKS DAN *ASSESSMENT*

Pada bab ini akan dijelaskan mengenai rancangan indeks yang akan dibangun pada penelitian. Rancangan tersebut merupakan penggabungan dari beberapa standar yang telah dijabarkan pada bab sebelumnya.

4.1 Konsep / Proses

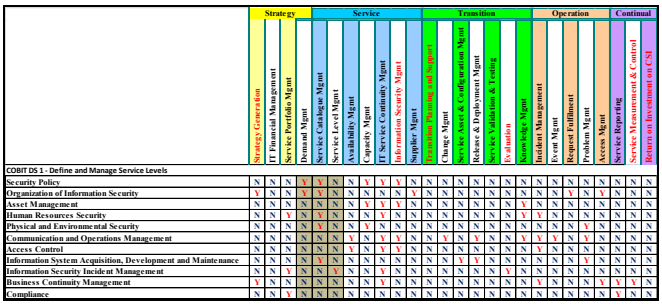
Di dalam Konsep/Proses dibahas prespektif kemanan dari lima siklus ITIL. Hal ini didasari pada kemampuan ITIL untuk mendeskripsikan proses, fungsi dan struktur organisasi guna mendukung area-area utama dalam manajemen layanan TI. Dari sisi keamanan, ITIL juga membahas dari sisi *Information Security Management* (ISM) di masing-masing tahapan layanan [9].

4.2 Area

Di dalam Area dibahas prespektif dari sisi manajemen keamanan layanan . Hal ini didasari oleh tujuan penggabungan ITIL V3, ISO 27000 dan COBIT 4.1 untuk keamanan layanan teknologi informasi yang diharapkan mampu dilakukan secara efisien, risiko keamanan yang minim dan sesuai dengan persyaratan hukum yang berlaku [2].

4.3 Pemetaan Komponen Indeks

Pemetaan indeks penilaian kesiapan manajemen keamanan layanan ini menggunakan konsep hibridasi yang didasari pada kebutuhan organisasi, yaitu tidak hanya memastikan layanannya dapat berjalan dengan baik sesuai dengan kualitas yang direncanakan, tetapi juga mampu memastikan bahwa layanan berjalan dengan aman.



Gambar 4 Pemetaan Komponen Indeks

Proses hibridasi ini menghasilkan pemetaan indeks yang lebih terarah dengan mencocokkan fase manajemen keamanan layanan dengan manajemen keamanan yang dibutuhkan di masing-masing fase dengan *control objective* strategi TI yang kesemuanya menggunakan *best practice*.

4.4 Penetapan Skoring dan Status Penilaian

Penetapan skoring dan status penilaian menggunakan parameter penilaian COBIT 4.1, yaitu model kematangan (*maturity models*) berdasarkan tingkat kematangan manajemen keamanan layanan di organisasi yang sudah dijabarkan dalam sub-bab 3.4 *Framework* COBIT 4.1

Di dalam indeks penilaian, terdapat enam buah tingkatan penilaian, yaitu :

Tabel 2 Penentuan Nilai

Skor	Status	Keterangan
0	*Non-existient*	*Management Processes are not applied at all*
1	*Initial*	*Processes are ad hoc and disorganized*
2	*Repeatable*	*Processes follow a regular pattern*
3	*Defined*	*Processes are documented and communicated*
4	*Managed*	*Processes are monitored and measured*
5	*Optimised*	*Good practices are followed and automated*

4.5 Pemetaan Indeks Penilaian

Pemetaan indeks didasari pada kebutuhan organisasi, yaitu tidak hanya memastikan layanannya dapat berjalan dengan baik sesuai dengan kualitas yang direncanakan, tetapi juga mampu memastikan bahwa layanan yang ada berjalan dengan aman yang didapatkan dari proses hibridasi pemetaan komponen indeks.

Didapati beberapa kesimpulan dari proses hibridasi pemetaan :

1. Seluruh *Control Objective* dalam *Delivery and Support* COBIT terimplementasi kecuali *COBIT DS 6- Identify and Allocate Costs* yang diharapkan mampu diimplentasikan menggunakan manajemen terpisah dalam *Financial Management* dalam ITIL.
2. Seluruh *Lifecycle* ITIL V3 terimplementasi kecuali *Continous Service Improvement* yang hanya mampu diimplementasikan oleh ISO 27002 dalam sisi Reporting, tetapi tidak dalam sisi *Service Measurement & Control* dan *Return on Investment on CSI.*
3. Proses manajemen keamanan layanan dapat dimaksimalkan pada saat *Service Design*, terbukti dengan mampu terpenuhinya kebutuhan keamanan manajemen layanan di seluruh proses *Service Design* baik oleh ISO 27002 maupun COBIT 4.1
4. Seluruh proses dari manajemen keamanan layanan memiliki korelasi yang baik antara standar dengan standar lainnya kecuali tentang penekanan akan kewajiban bagi organisasi dalam memenuhi seluruh kebutuhan persyaratan keamanan yang dapat di *cover* dalam ISO 27002– *Compliance.*
5. Dalam menetapkan manajemen keamanan layanan di fase *Service Strategy*, organisasi berfokus pada *COBIT DS 1- Define and Manage Service Levels* dengan mempertimbangkan *Services Security Policy* and Organization of Information dalam *Demand Management*, serta *COBIT DS 2 - Manage Third-Party Services* dalam menentukan *positioning* pihak ketiga di dalam *Organization of Information and Business Continuity Management* dalam *Service Generation*.
6. Dalam menetapkan manajemen keamanan layanan di fase *Service Design*, organisasi berfokus pada *COBIT DS 1- Define and Manage Service Levels* dengan memastikan bahwa organisasi memiliki *Service Catalogue Management*, *Service Level Management* yang mempertimbangkan *level* kemungkinan terjadi dan pengelompokan dari macam-macam insiden dalam *Information Security Incident Management Information*. Pada *COBIT DS2 - Manage Third-Party Services* dengan melakukan manajemen di *Supplier Management*. Pada COBIT *DS3 - Manage Performance and Capacity* dan *COBIT DS11- Manage Data* dengan memastikan *Availability Management*. Pada *COBIT DS4-Ensure Continous Service* dengan memastikan *IT Service Continuity Management*. Pada *COBIT DS5 - Ensure System Securities* dengan memastikan *Information Security Management*.
7. Dalam menjalakan manajemen keamanan layanan di fase *Service Transition*, organisasi berfokus pada *DS7-Educate and Train Users* dalam proses *Release & Deployment Management*. Pada *DS 9-Manage the Configuration dalam Service Asset & Configuration Management* yang mempertimbangkan keamanan dalam proses *Information System Acquisition, Development and Maintenance.* Pada

DS12-Manage Physical Environment dan *DS 13- Manage Operations* di dalam proses *Change Management*.

8. Dalam menjalakan manajemen keamanan layanan di fase *Service Operation*, organisasi berfokus pada *DS8-Manage Service Desk and Incident* dalam proses *Incident Management* dan Pada *DS10-Manage Problems* dalam proses *Problem Management* serta Pada *DS13-Manage Operation* dalam proses *Event Management*.

Dari ke-delapan kesimpulan di atas, dibuatlah struktur pembuatan Indeks Penilaian Kesiapan Manajemen Keamanan yang ditunjukkan dalam Tabel 3 Pemetaan Indeks Penilaian.

Tabel 3 Pemetaan Indeks Penilaian

ITIL	ISO	COBIT	
Service Strategy	Kebijakan Keamanan	**DS1 DS2**	***Maturity Model***
	Struktur Organisasi		
Service Design	Manajemen Aset	**DS1 DS2 DS3 DS4 DS5 DS11**	
	Keamanan Sumber Daya Manusia		
	Keamanan Fisik dan Lingkungan		
Service Transition	Penambahan, Pengembangan dan Pemeliharaan Sistem Informasi	**DS7 DS9 DS12 DS13**	
Service Operation	Manajemen Komunikasi dan Operasional	**DS8 DS10 DS13**	
	Kontrol Akses		
	Manajemen Insiden Keamanan		
Continual Service Improvement	*Business Continuity Management*	-	
	Pemenuhan Persyaratan		

4.6 Dashboard

Business Intelligence (BIS) Dashboard adalah sebuah alat visualisasi data yang menampilkan status terkini dari sebuah metrik dan *Key Performance Indicator* (KPI) untuk sebuah organisasi. *Dashboard* mengkonsolidasikan dan menyusun angka-angka, metrik dan juga performa *scorecard* dalam satu layar.

Dashboard dapat disesuaikan untuk peran tertentu dan metrik tampilan ditargetkan untuk satu titik pandang atau departemen.Fitur penting dari produk dashboard termasuk antarmuka yang dapat disesuaikan dan kemampuan untuk menarik data secara real-time dari berbagai sumber [10].

4.6.1 Dashboard Indikator Kinerja

Sumber data yang digunakan dalam pembuatan *dashboard* indikator kinerja adalah rata-rata capaian dari masing-masing proses manajemen keamanan teknologi informasi.

Terdapat tiga indikator capaian, yaitu :

1. Merah : Pelaksanaan manajemen keamanan informasi masih dalam proses inisiasi atau belum menjadi fokusan utama dari organisasi
2. Kuning : Pelaksanaan manajemen keamanan informasi sudah menjadi fokusan utama dari organisasi akan tetapi pelaksanaannya belum optimal.
3. Hijau : Pelaksanaan manajemen keamanan informasi sudah optimal baik dari sisi manajemen hingga pelaksanaannya di tingkat operasional.

Gambar 5 Dashboard Indikator Kinerja

Gambar di atas merupakan gambar *dashboard* indikator manajemen keamanan layanan. Sebagai contoh penghitungan capaian, masing-masing konsep atau tahapan manajemen layanan dapat dilihat. Dari dashboard diatas, dapat dilihat satu buah tahapan manajemen layanan masuk ke dalam indikator merah, tiga tahapan manajemen layanan masuk ke dalam indikator kuning dan satu tahapan manajemen layanan telah mencapai indikator hijau.

Dengan melihat dashboard ini, diharapkan organisasi dapat melihat dengan lebih menyeluruh akan tahapan manajemen keamanan layanan manakah yang harus mendapatkan fokusan lebih dan perbaikan.

4.5.2 Dashboard Kesiapan Keamanan

Sumber data yang digunakan dalam pembuatan *dashboard* kesiapan keamanan adalah rata-rata capaian dari seluruh proses manajemen keamanan teknologi informasi.

Indikator capaian sama dengan indikator pada *dashboard* indikator kinerja, hanya saja prespektif yang dilihat dari dashboard ini bukan kesiapan dari masing-masing area/tahapan, tetapi dari kesiapan organisasi secara menyeluruh.

Gambar 6 Tingkat Kesiapan Keamanan

Gambar di atas merupakan gambar *dashboard* tingkat kesiapan keamanan layanan. Sebagai contoh penghitungan capaian, kesiapan organisasi masuk ke dalam indikator hijau dimana secara keseluruhan kesiapanan manajemen keamanan sudah optimal.

4.7 Assessment

Dari proses *assessment* awal didapatkan bahwa kondisi *existing* yang didapatkan masih belum sesuai dengan kondisi ideal berdasarkan standar keamanan layanan, karena masih terdapat beberapa ketidaksesuaian ketersediaan tata kelola TI. Masalah keamanan dalam pelaksanaan layanannya belum menjadi fokusan, organisasi studi kasus masih mencari sebuah pola yang cocok digunakan dalam pengukuran tingkat *maturity* dari manajemen keamanan layanan TI. Dengan menggabungkan beberapa *framework* dan beberapa *best practice* ini, diharapkan mampu menjawab kebutuhan tersebut.

V. KESIMPULAN DAN SARAN

Berdasarkan hasil uji studi kasus dan analisis yang telah dilakukan dalam penelitian ini, maka dapat diambil kesimpulan sebagai berikut:

1. Pembuatan indeks penilaian manajemen keamanan layanan dengan menggabungkan standar berbasis *Service Delivery* COBIT 4.1, ITIL V3, ISO 27000 dan penilaian kesiapan berdasarkan *maturity model* COBIT 4.1, **relevan**. Hal tersebut ditunjukkan dengan dapat diperolehnya sebuah indeks penilaian yang saling mendukung antara satu standar dengan standar lainnya.
2. Kombinasi antara metodologi manajemen TI menggunakan ITIL, COBIT dan ISO / IEC 27002 akan memberikan hasil yang lebih komprehensif dan efisien baik dari sisi persiapan hingga pengimplementasian fitur-fitur yang sebelumnya tidak dipertimbangkan oleh organisasi yang hanya menggunakan satu buah metodologi.
3. Indeks penilaian yang dibuat memiliki fitur yang dikhususkan untuk organisasi penyelenggara layanan publik, terutama di perguruan tinggi sehingga fitur/pertanyaan yang ada di dalam indeks lebih bersifat khusus.

Saran untuk pengembangan indeks penilaian kesiapan manajemen keamanan layanan selanjutnya adalah:

1. Perlunya pengembangan indeks ke dalam bentuk aplikasi, yang diharapkan aplikasi tersebut dapat terhubung langsung dengan dengan laporan kinerja proses bisnis organisasi secara otomatis.
2. Terkait dengan manajemen keamanan layanan, aplikasi belum meng-*cover* manajemen keamanan terkait proses *Transition Planning and Support* dan *Continual Service Improvement* ITIL, diharapkan terdapat pengembangan indeks lebih lanjut agar dapat meng-*cover* hal tersebut.
3. Dalam melakukan manajemen layanan di organisasi, kami merekomendasikan untuk organisasi tersebut mengimplementasikan dan melakukan pengontrolan pelaksanaan manajemen layanan menggunakan dokumen *Service Level Agreement* (SLA), sehingga nantinya manajemen layanan yang ada tidak bersifat statis dan dapat melakukan penambahan atau pengubahan SLA, jika suatu waktu terjadi perubahan proses bisnis maupun jenis layanan yang ada.

DAFTAR PUSTAKA

[1] Tim Direktorat Keamanan Informasi, Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, Jakarta: Kominfo, 2011.

[2] M. Gehrmann, *Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organization,* 2012.

[3] J. Clinch, ITIL V3 and Information Security, OGC, 2009.

[4] IT Governance Institute, COBIT 4.1, USA: IT Governance Institute, 2007.

[5] itSMF International, Foundation of IT Service Management based on ITIL V3, Van Haren, 2007.

[6] A. Calder and S. Watkins, IT Governance A Manager's Guide to Data Security and ISO 27001/27002, London: Kogan Page Limited, 2007.

[7] S. Architecture, Security Management Framework, Security Architecture, 2009.

[8] ISO/IEC, Information Technology - Security techniques - Code of Practice for Information Security Management, Switzerland: ISO/IEC 2005, 2005.

[9] P. Lijnse, "Service Management Art," 2006. [Online].

[10] Williams, S., & Williams, N. (2007). The Profit Impact of Business Intelligence. San Fransisco, US: Morgan Kaufmann Publishers.