

Evaluasi *Security Management* Pada Arsitektur Berorientasi Layanan

Indra Ranggadara*, Muhibbudin Suretno

Fakultas Ilmu Komputer, Universitas Mercu Buana, Jakarta
Jl. Meruya Selatan No. 1, Kembangan, Jakarta Barat

*indra.ranggadara@mercubuana.ac.id, 41817120105@student.mercubuana.ac.id

ABSTRACT

Teknologi berkembang dari waktu ke waktu. Perkembangan teknologi ini membawa banyak manfaat bagi manusia. Misalnya dapat membantu mempercepat pekerjaan manusia, meningkatkan kualitas dan kuantitas pelayanan, serta mempermudah proses transaksi keuangan. Tidak hanya manfaat, tetapi juga keamanan dari teknologi itu sendiri harus diperhitungkan. Tentunya tujuannya untuk memprediksi risiko ancaman berupa kerusakan bagian fisik komputer atau pencurian data. Meraki Digital Indonesia ingin meningkatkan manajemen keamanannya, yang menjadi agenda setiap tahun, setelah memutakhirkan sistemnya ke arsitektur berorientasi layanan (SOA) untuk meningkatkan keamanan. Tujuan dari penelitian ini adalah untuk mengevaluasi peningkatan manajemen keamanan, terutama pada arsitektur berorientasi layanan (SOA) yang diimplementasikan, dan untuk membuat rekomendasi yang sesuai. Metode penelitian yang digunakan untuk mengevaluasi manajemen keamanan arsitektur berorientasi layanan (SOA) dan proses hierarki analitik (AHP) menggunakan kerangka kerja COBIT 4.1 dan untuk menjelaskan persyaratan manajemen secara lebih rinci. Hasil evaluasi yang diperoleh ada beberapa kesimpulan yang diperoleh, yaitu hasil evaluasi menggunakan COBIT 4.1, terdapat penilaian yang diperoleh untuk People, Technology, dan Facilities, perlu untuk ditingkatkan maturity levelnya. Sedangkan untuk rekomendasi yang dibutuhkan dengan menggunakan proses AHP, ada tiga hal yang perlu ditingkatkan: yaitu kriteria Technology, Facilities, dan People.

Kata Kunci: AHP, COBIT 4.1, Evaluasi Manajemen, Manajemen Keamanan TI

PENDAHULUAN

Di era teknologi yang berkembang pesat hingga saat ini dibutuhkan pengawasan operasional dalam bisnis untuk mendukung kelangsungan bisnis suatu perusahaan sesuai dengan aturan perusahaan. Saat ini, Meraki Digital Indonesia, salah satu konsultan IT di Indonesia, telah menerapkan arsitektur berorientasi layanan untuk mendukung pertukaran data antar aplikasi, meningkatkan keandalan, berpartisipasi dalam proses bisnis, dan membakukan dan mengkonsolidasikan aplikasi yang dimiliki oleh perusahaan. Gagasan lain tentang arsitektur berorientasi layanan (SOA) (MacLennan & Van Belle, 2013). Mengambil pendekatan arsitektur untuk merancang dan menerapkan solusi TI. Saat ini implementasi arsitektur berorientasi layanan (SOA) yang dikembangkan memiliki 7 aplikasi yang terintegrasi dan terstandarisasi sehingga proses pembangunan ke depan dapat dengan mudah dilakukan. Aplikasi yang dikembangkan termasuk aplikasi *HRIS, CRM, Incident Services, Payroll, Big Data, Corporate social media*, dan

Project Management. Untuk meningkatkan manajemen keamanan aplikasi yang dikembangkan, diperlukan evaluasi untuk menyusun dan memelihara program keamanan informasi untuk memastikan pemenuhan 3 persyaratan dasar sumber daya informasi organisasi, yaitu kerahasiaan integritas dan ketersediaan data atau informasi. Seiring dengan perkembangan teknologi komputer dan komunikasi, mengelola program keamanan komputer dan jaringan akan menjadi semakin kompleks dan menantang, hal ini untuk melindungi data atau informasi dalam sistem sehingga hanya dapat diakses oleh mereka yang memiliki akses yang sesuai, dapat dilihat pada gambar 1.

Gambar 1 menjelaskan arsitektur aplikasi pada perusahaan Meraki Digital Indonesia, yang mana perusahaan ini merupakan perusahaan IT solusi. Saat ini perusahaan menginginkan peningkatan *security management* yang merupakan agenda tahunan setelah meningkatkan sistem nya menjadi arsitektur berorientasi layanan (SOA) untuk meningkatkan keamanannya, hal ini dimulai berdasarkan hasil evaluasi dari kerangka kerja IT

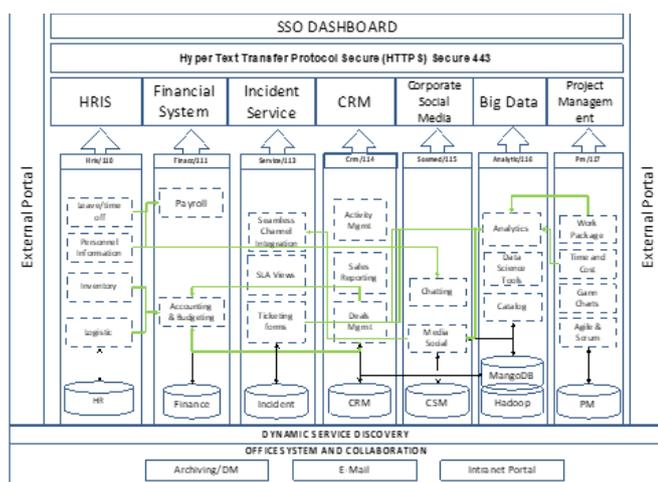
STUDI LITERATUR

yang umum. Evaluasi dilakukan dengan menggunakan salah satu dari beberapa kerangka kerja yang ada, termasuk COBIT, ISO 7799 dan ITIL V3. Di sini penulis menggunakan kerangka COBIT 4.1 (Tujuan Kontrol untuk Informasi dan Teknologi Terkait). COBIT adalah model yang dirancang untuk mengendalikan fungsi TI dan COBIT menyediakan instrumen Tata Kelola TI yang memungkinkan manajer untuk menjembatani kesenjangan sehubungan dengan persyaratan kontrol, sistem informasi (IS) dan masalah teknologi informasi (TI) dan risiko bisnis, untuk mengkomunikasikan tingkat kontrol pemangku kepentingan, memungkinkan pengembangan kebijakan yang jelas dan praktik yang baik untuk kontrol TI di seluruh organisasi (Brand & Boonen, 2007). Kerangka COBIT 4.1 sebagai acuan dalam melakukan audit sistem informasi, dalam konteks ini Arsitektur berorientasi layanan (SOA). Proses audit dimaksudkan untuk mendeteksi ketidakcocokan produk dengan standar, prosedur atau persyaratan eksternal (Cotfas & Palaghița, 2010) dan evaluasi ini untuk menilai situasi 'apa adanya' dari fungsi TI dan menggunakan hasil yang diperoleh untuk memberikan rekomendasi ke fungsi TI (Latif & Hanifi, 2013). Sementara itu, selain evaluasi yang dilakukan, diperlukan rekomendasi oleh pemangku kepentingan untuk menyelesaikan situasi yang kompleks. Dalam penelitian ini metode yang digunakan untuk memberikan rekomendasi menggunakan metode pengambilan keputusan (Saaty, 1996) dengan menggunakan Analytical Hierarchy Process (AHP) menurutnya untuk memecah situasi menjadi bagian komponennya dan mengatur bagian atau variabel ini menjadi pengaturan hierarkis. Dalam memecahkan masalah dengan analisis logis eksplisit, ada tiga prinsip yang mendasari pemikiran AHP, yaitu prinsip menyusun hierarki, prinsip menetapkan prioritas, dan prinsip konsistensi logis. Jadi, dalam penelitian ini bertujuan untuk melakukan evaluasi sekaligus memberikan rekomendasi yang tepat untuk mendukung perbaikan manajemen keamanan khususnya pada arsitektur berorientasi layanan (SOA) yang telah dilaksanakan.

Berdasarkan latar belakang dijelaskan ada beberapa penelitian sebelumnya yang telah berhasil menerapkan konsep COBIT 4.1 dan AHP. Dalam penelitian pertama (Asyari dan Triana, 2018) menjelaskan evaluasi Aplikasi Sistem Alat Analisis Kredit menggunakan COBIT 4.1 dengan hasil proses telah dipantau dan dievaluasi secara ketat mengenai sejauh kepatuhan terhadap prosedur yang ditetapkan dan mampu mengambil tindakan yang diperlukan jika proses yang ada tidak berjalan dengan baik. Aplikasi SABAK secara optimal mendapatkan level empat, tetapi ada domain yang lemah di antara domain lainnya, yaitu PO2 Mendefinisikan Arsitektur Informasi. Evaluasi domain diperlukan. Penelitian kedua (Harwikarya, et al, 2015) menggunakan COBIT 4.1 di pendidikan tinggi, penelitian ini menunjukkan bagaimana modifikasi kerangka kerja yang akrab dari rencana strategis IS dan kerangka Tata Kelola TI mampu memandu arah dan manajemen IS / IT Universitas. Penelitian ketiga (Fitriah & Sucahyo, 2008) dari hasil pengujian terhadap efektivitas pengendalian ada kontrol yang sedang berjalan, yaitu PO8.1. Sistem Manajemen Mutu, PO8.4. Fokus Pelanggan, Peningkatan Berkelanjutan PO8.5 dan Pengukuran Kualitas PO8.6, Pemantauan dan Peninjauan, bahkan kemudian karena ada penerapan standardisasi ISO. Kontrol lainnya adalah DS5.9. Pencegahan, Deteksi, dan Koreksi Perangkat Lunak Berbahaya. Penelitian keempat (Koç & Burhan, 2015) model hierarkis hasil yang ditetapkan untuk masalah ini dapat memberikan wawasan mengenai masalah pemilihan lokasi. Juga sebagai contoh solusi yang layak untuk masalah pemilihan lokasi dunia nyata. Penelitian lain dari (Li, et al, 2018) faktor penilaian hasil pendidikan jaringan dianalisis, faktor penilaian pendidikan jaringan memiliki dua faktor penilaian kelas satu dan enam faktor penilaian kelas dua untuk evaluasi pendidikan jaringan yang diusulkan dan diterapkan untuk evaluasi pendidikan jaringan universitas Tianjin. Dari penelitian sebelumnya kontribusi dalam penelitian ini adalah menggabungkan metode evaluasi menggunakan COBIT 4.1 dan *Analytical Hierarchy Process* (AHP) untuk menentukan peringkat rekomendasi yang diperlukan untuk meningkatkan arsitektur berorientasi layanan (SOA) yang telah dilakukan sesuai dengan keinginan perusahaan sebagai pemangku kepentingan..

METODOLOGI

Metode penelitian yang digunakan dengan menggunakan kerangka COBIT 4.1 dan *Analytical Hierarchy Process* (AHP). Pada metode pertama untuk evaluasi menggunakan COBIT 4.1, kerangka kerja ini memungkinkan pembuatan kebijakan kontrol TI dan praktik terbaik di seluruh tingkat bisnis (Khther &



Gambar 1 Corporate Application Architecture

Othman, 2013) Sesuai dengan aturan dalam kerangka kerja COBIT 4.1 terdapat tahapan-tahapan yang digunakan untuk melakukan evaluasi, evaluasi ini akan menjawab manajer yang bertanggung jawab terhadap departemen teknologi informasi sebagai reviewer. Seperti yang dijelaskan (Krisanthi, et al, 2014) tahap proses audit menggunakan kerangka COBIT 4.1 terdiri dari beberapa tahap:

1. Mengidentifikasi Tujuan Bisnis, Tahap ini akan dilakukan dengan analisis SOA sebagai deskripsi ke mana arah aplikasi. Kemudian tujuan bisnis disesuaikan sesuai dengan pandangan mereka dalam domain yang ada di COBIT 4.1.
2. Mengidentifikasi Tujuan TI, tahap ini akan mengidentifikasi tujuan berdasarkan aplikasi SOA, pada tahap ini tujuan Tujuan TI akan diperoleh dengan menghubungkan tujuan bisnis dengan Tujuan TI berdasarkan COBIT 4.1.
3. Mengidentifikasi Proses TI, pada tahap ini, proses teknologi informasi yang telah ditentukan akan diidentifikasi. Pada tahap ini proses teknologi informasi akan diperoleh dari keterkaitan antara proses teknologi informasi yang berjalan dalam proses proses teknologi informasi berdasarkan kerangka COBIT 4.1.
4. Tujuan Kontrol, tahap ini dilanjutkan dari proses IT. Setelah mengidentifikasi, tujuan kontrol digunakan sebagai bahan kuesioner untuk memenuhi persyaratan data yang diperlukan dalam menentukan objektivitas.
5. Perhitungan Tingkat Kematangan, pada tahap kelima penelitian ini adalah perhitungan tingkat kematangan, sesuai dengan model kematangan berdasarkan kerangka COBIT 4.1.

Kemudian Tahapan yang dilakukan meliputi proses pemilihan COBIT 4.1, serta pendataan yang dilakukan terdiri dari wawancara, observasi dan kuesioner, dan pengolahan questioner. Analisis data meliputi *maturity level* saat ini yang diharapkan, perbaikan strategi berdasarkan COBIT 4.1 [11]. Kemudian Secara umum, rentang penilaian tingkat kematangan digambarkan sebagai berikut:

1. Level 0 (tidak ada), perusahaan tidak memiliki manajemen dalam suatu proses, bahkan tidak dapat menilai masalah apa yang perlu dipertimbangkan. Pada skala ini, penting untuk mengevaluasi kontrol dan membuat temuan penting.
2. Level 1 (level awal), perusahaan telah menyadari masalah yang perlu dipertimbangkan. Perusahaan tidak memiliki proses standar, tetapi proses informal yang cenderung diterapkan secara individual jika terjadi kasus dan secara umum (masih reaktif atau sesuai dengan kebutuhan mendadak), pendekatan

yang digunakan tidak terorganisir dengan baik. Dalam skala ini, probabilitas risiko yang terjadi tidak sebesar skala 0 (nol).

3. Level 2 (tingkat berulang), perusahaan memiliki pola untuk mengelola proses berdasarkan pengalaman berulang yang telah dilakukan sebelumnya. Namun, pola ini belum terstandarisasi dan dikomunikasikan, dan belum ada pelatihan formal yang diberikan kepada setiap karyawan mengenai prosedur sehingga kemampuan staf ahli terbatas, selain itu tanggung jawab diberikan sepenuhnya kepada individu sehingga kemungkinan penyimpangan dapat terjadi.
4. Level 3 (Tingkat yang ditentukan), manajemen telah berhasil menciptakan standar untuk mengelola proses terkait, dan telah dikomunikasikan, tetapi belum dilaksanakan secara terpadu, tetapi telah diperlukan dalam implementasinya. Prosedurnya masih sederhana dan tidak memadai, belum menerima proses evaluasi, sehingga masih ada kemungkinan terjadi penyimpangan.
5. Level 4 (Tingkat terkelola), proses ini telah dipantau dan dievaluasi dengan benar mengenai sejauh mana kepatuhan terhadap prosedur yang ditetapkan, dan mampu mengambil tindakan yang diperlukan jika proses yang ada tampaknya tidak bekerja dengan baik. Alat dan sistem otomatis sedang digunakan meskipun masih terbatas.
6. Level 5 (Tingkat yang dioptimalkan), proses ini telah mencapai tingkat Praktik Terbaik karena peningkatan dan perbandingan yang berkelanjutan dengan perusahaan lain. Teknologi informasi digunakan untuk menjalankan alur kerja. Menyediakan alat pendukung untuk efektivitas dan kualitas proses yang mendorong adaptasi perusahaan terhadap perubahan.

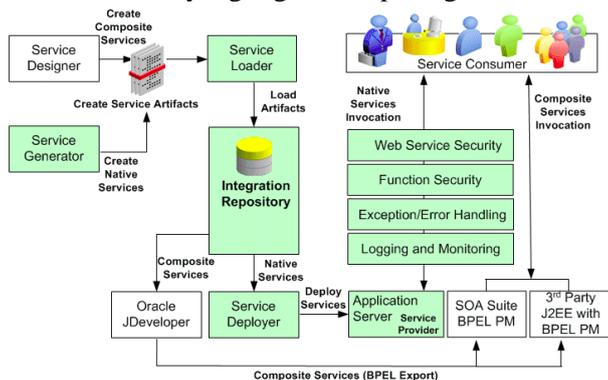
Metode kedua untuk rekomendasi menggunakan AHP, fungsi AHP adalah proses menekankan pentingnya penilaian intuitif dari pembuat keputusan dan konsistensi dalam perbandingan alternatif dalam proses pengambilan keputusan (Balubaid & Alamoudi, 2015). Pada dasarnya, AHP adalah teori umum pengukuran yang digunakan untuk menemukan skala rasio perbandingan berpasangan diskrit dan kontinu. Perbandingan ini dapat diambil dari ukuran aktual atau skala dasar yang mencerminkan kekuatan perasaan dan preferensi relatif (Sulistiyono, 2016). Metode ini akan mendapatkan nilai untuk mendapatkan peringkat sebagai keinginan pemangku kepentingan, kuesioner hanya akan dijawab oleh *stakeholder* dan metode ini memiliki beberapa prinsip dalam memecahkan masalah dengan Analytical Hierarchy Process (AHP):

1. Menentukan hierarki

2. Menentukan prioritas elemen dengan membuat perbandingan berpasangan
3. Sintesis
4. Mengukur konsistensi
5. Menghitung konsistensi indeks
6. Menghitung rasio indeks.

HASIL DAN PEMBAHASAN

Dalam kajian ini, membahas evaluasi implementasi SOA yang dilakukan, saat ini SOA dilaksanakan menggunakan *Oracle E-Business Suite* yang diimplementasikan di Meraki Digital Indonesia. Terlihat arsitektur SOA yang digunakan pada gambar 2.



Gambar 2. *Oracle E-Business Suite Integrated SOA Gateway Architecture* (Weld & Yang, 2018)

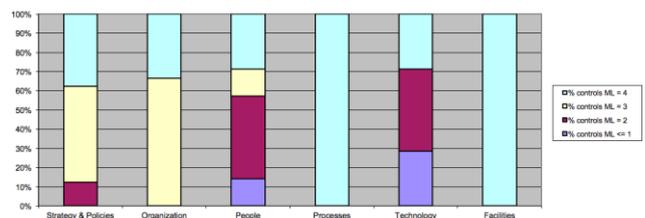
Sebelum mendapatkan hasil evaluasi, perlu ditentukan domain dan pengukuran kontrol dalam penelitian ini, berdasarkan COBIT 4.1 terdapat domain yang berperan dalam melakukan evaluasi, yaitu *plan and organize* (PO), *acquire and implement* (AI), *deliver and support* (DS), dan *monitoring and evaluate* (ME). Domain yang telah ditentukan sebagai dasar evaluasi dan dalam penelitian ini rekapitulasi pertanyaan sesuai dengan domain yang digunakan dapat dilihat pada tabel 1.

Tabel 1. Domain dan Ukuran Kontrol

Domain	Ukuran Kontrol	COBIT 4.1
Strategy & Policies	Define an information security plan	DS5.2, PO6.3
	Define the information architecture	PO2.1, PO2.3
	Determine technological direction	PO3.3, PO3.4
	Assess and manage (IT) risks	PO9.1, PO9.4, PO9.6
Organization	Information Security Organization	PO4.8, DS5.1
	Data and system ownership	PO4.9
	Manage segregation of duties	PO4.11

People	Manage IT human resources	PO7.1, PO7.2, PO7.5, PO7.6, PO7.8	
	Ensure operations and use	AI4.3, AI4.4	
Processes	Change Management	AI6.1, AI6.2, AI7.4, AI7.6, AI7.8	
	Continuity Management	DS4.2, DS4.5, DS4.9, DS11.5	
	Manage data	DS11.2, DS11.4, DS11.6	
	Configuration Management	DS9.1, DS9.2	
	Manage third party and supplier services	DS1.5, DS2.3	
	Incident Management	DS5.6, DS8.3	
	Monitoring	DS5.5, ME2.1, ME2.6, ME3.3, ME4.7	
	User Account Management	DS5.3, DS5.4	
	Technology	Secure infrastructure	AI3.2, AI3.3, DS5.8, DS5.10, DS5.11
		Manage malware attacks	DS5.9
Protect infrastructure component		DS5.7	
Facilities	Physical security	DS12.2, DS12.3	

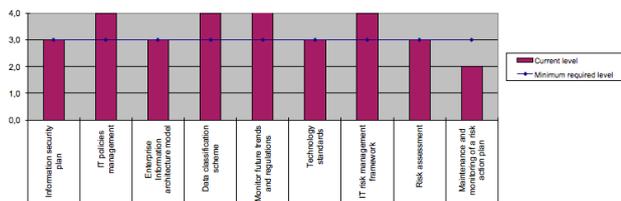
Setelah mendapatkan domain yang diinginkan untuk evaluasi, dan penilaian dapat dilakukan pada gambar 3 hasil maturity yang perlu dievaluasi per setiap domain dapat dilihat pada gambar 3, untuk mendapatkan nilai pada level setiap domain.



Gambar 3 *Security Management - spread of operational maturity level*

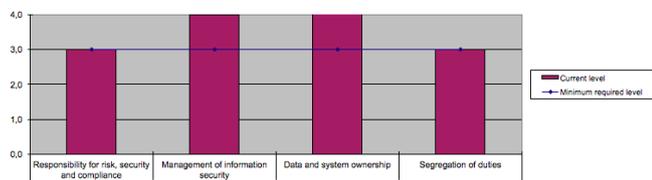
Saat ini ada 6 domain yang telah dievaluasi, termasuk strategi & kebijakan, organisasi, orang, proses, teknologi, dan fasilitas. Rincian evaluasi yang dilakukan per setiap domain dijelaskan di pada gambar 4-9. Berikut gambar 4

menjelaskan hasil *maturity level* domain *strategy and policy*.



Gambar 4. Hasil *maturity level* domain *strategy and policy*

Gambar 4 menjelaskan bahwa strategi domain *strategy and policy* memiliki tingkat *maturity* yang tinggi, kecuali untuk *maintenance and monitoring of a risk action plan* dengan *maturity level* 2 (berulang). Karena penerapan layanan berorientasi baru dilakukan selama 1 tahun dan Di bidang keamanan, muncul kemampuan SOA untuk hal-hal seperti jasa otentikasi dan *audit trail collection* (Karimi, 2011) maka perlu dibiasakan dalam menjalankan strategi yang dilakukan untuk melakukan pemeliharaan dan pemantauan di sisi *Security Management*.



Gambar 5. Hasil *maturity level* domain *Organization*

Gambar 5 menjelaskan domain *Organization*, dalam kontrol domain *responsibility for risk, security and compliance* dan *segregation of duties* perlu ditingkatkan untuk dioptimalkan sampai *maturity level* 4. Namun secara keseluruhan domain ini sudah terbilang baik karena pengelolaan keamanan informasi dan kepemilikan data dan sistem telah dioptimalkan. Selanjutnya menjelaskan domain *people* pada gambar 6.



Gambar 1. Hasil *maturity level* domain *people*

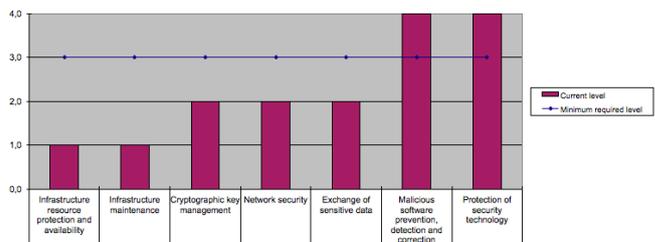
Gambar 6 menjelaskan domain *people*, dalam domain ini masih banyak hal yang perlu ditingkatkan, termasuk recruitment and retention of personnel, *kompetensi personel*, *personnel competencies*, *knowledge transfer to end users*, dan *knowledge transfer to operations and support staff*. Terutama bidang pemahaman keahlian tentang *security management*. Dengan keahlian, dapat mempermudah untuk melindungi aplikasi yang

diimplementasikan. Selain itu, banyak diperlukan penyesuaian keamanan untuk setiap layanan pada aplikasi. dan konsultan sangat diperlukan untuk memberikan pengetahuan dan pelatihan tentang *standard IT services* untuk menjalankan *IT Services* pada organisasi dengan aman dan konsultan perlu memberikan pelatihan orientasi keamanan kepada *enduser* dengan tingkat pelatihan yang berbeda, karena pemahaman *enduser* sangat berbeda. Hal ini diperlukan untuk menciptakan kesadaran keamanan di semua elemen perusahaan. sementara untuk tenaga *clearance*, prosedur dan pemutusan hubungan kerja sudah sangat baik dan telah dioptimalkan. Karena hal ini juga akan berdampak pada domain proses yang dibutuhkan oleh seluruh personel untuk mematuhi standar operasional prosedur perusahaan, terutama pada keamanan dan rahasia perusahaan. Selanjutnya menjelaskan domain proses pada gambar 7.



Gambar 2. Hasil *maturity level* domain *Process*

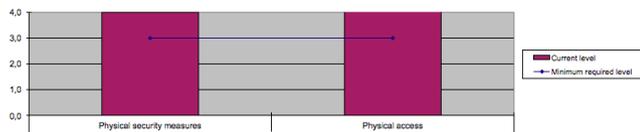
Gambar 7 pada domain, *process* secara keseluruhan telah sangat baik. Standar operasional yang telah diterapkan sebelumnya telah dioptimalkan. Dengan proses berjalan itu telah berkonsultasi dengan konsultan yang tepat untuk menangani proses. Namun meski dapat dioptimalkan secara keseluruhan, prosesnya perlu dipertahankan dan meningkatkan tingkat kematangan saat ini untuk periode berikutnya. Selanjutnya menjelaskan domain *Technology* pada gambar 8.



Gambar 3. Hasil *maturity level* domain *Technology*

Gambar 8 menjelaskan domain *Technology*, domain ini perlu ditingkatkan, terutama dalam *infrastructure resource protection and availability*, serta *maintenance infrastructure* yang masih pada level satu. Untuk saat ini, sumber daya tidak maksimal dalam memantau infrastruktur yang dibangun sehingga tim yang bergiliran membutuhkan waktu 8 jam untuk melaksanakan tugas ini.

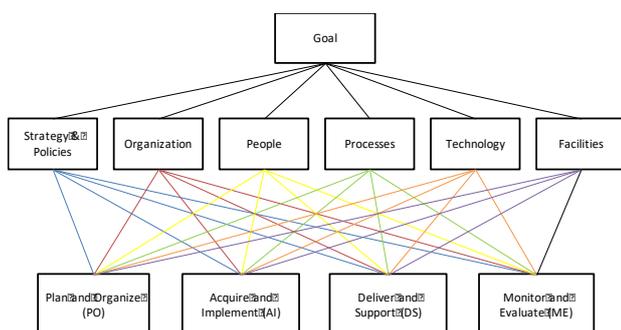
Selain untuk menjaga infrastruktur, lebih baik tidak menunggu vendor melakukan perawatan preventif atau korektif, namun perlu rutin menjadwalkan tim yang memiliki tanggung jawab dalam melakukan perawatan secara bulanan atau triwulanan. Serta *cryptographic key management*, *network security*, dan *exchange of sensitive data* masih perlu ditingkatkan, dan spesialis pada bidang teknologi tertentu diperlukan untuk terus mengupdate teknologi yang digunakan. Selanjutnya domain *facility* pada gambar 9.



Gambar 4. Hasil maturity level domain Facility

Gambar 9 menjelaskan domain *Facility*, dalam domain ini optimisasi of *physical security* dan *physical access* telah dilakukan. Namun, perbaikan sarana penyimpanan infrastruktur fisik perlu dilakukan karena tempat yang cukup lengkap dengan infrastruktur data center, dan untuk keesokan harinya untuk mengembangkan skalabilitas data center, akan sulit dilakukan, bukan untuk memulihkan sarana infrastruktur data center.

Setelah mendapatkan evaluasi dasar berbasis COBIT, maka diperlukan dukungan keputusan oleh *stakeholder* yang sesuai dengan keinginan dan pemantauan *security management* dalam berorientasi pelayanan yang telah dilaksanakan, maka selanjutnya dengan pendekatan AHP untuk menjelaskan lebih dalam keinginan dari manajemen. Sesuai dengan aturan AHP, hierarki diperlukan untuk mencapai keinginan *stakeholder* seperti yang terlihat pada Gambar 9 yang menjelaskan untuk mencapai tujuan pada tingkat satu dan di mana ada kriteria di level 2 yang berisi *strategies & policies*, *organizations*, *people*, *processes*, *technology*, dan *facilities*. Untuk level 3 adalah alternatif yang disediakan dan disesuaikan dengan domain COBIT yaitu, *Plan and Organizes (PO)*, *Acquire and Implement (AI)*, *Deliver and Support (DS)*, and *Monitor and Evaluate (ME)*. Informasi ini kemudian diatur dalam pohon bertingkat.



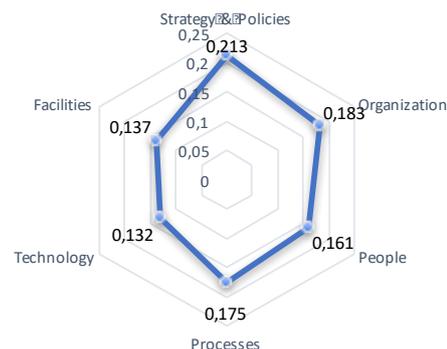
Gambar 5. Hirarki AHP

Setelah membuat kriteria dan alternatif yang diinginkan oleh para pemangku kepentingan, kriteria tersebut kemudian ditimbang sesuai dengan aturan proses hierarki analitis secara konsisten, setelah itu nilai-nilai dari yang terbesar hingga yang terkecil terlihat dan diberi peringkat prioritas untuk menentukan kriteria mana yang perlu ditingkatkan. Hasil yang diperoleh dapat dilihat pada tabel 2.

Tabel 2 Domain dan ukuran kontrol

Kriteria Security Management	Hasil Akhir	Peringkat prioritas	Perlu Ditingkatkan? (Ya/Tidak)
Strategy & Policies	0,213	6	Tidak
Organization	0,183	5	Tidak
People	0,161	3	Ya
Processes	0,175	4	Tidak
Technology	0,132	1	Ya
Facilities	0,137	2	Ya

Tabel 2 menjelaskan bahwa dari hasil perhitungan menggunakan AHP berdasarkan kriteria *Security Management*, pada kriteria *Strategy & Policies*, *Organization*, dan *Processes* memiliki nilai masing-masing 0,213 pada peringkat ke 6, 0,183 pada peringkat ke 5, 0,175 pada peringkat ke 6. Ketiga kriteria ini dirasa tidak perlu diperbaiki tetapi manajemen beranggapan perlu dipertahankan pencapaian yang sudah ada berdasarkan hasil analisa COBIT. Selanjutnya kriteria *People*, *Technology*, dan *Facilities* memiliki masing-masing nilai 0,161 peringkat ke-3, 0,132 peringkat ke-1, 0,137 peringkat ke-2. Kesimpulan dari tabel 2 menjelaskan bahwa ada tiga kriteria yang perlu ditingkatkan, yaitu *People*, *Technology*, dan *Facilities*. Ketiga kriteria ini perlu ditingkatkan untuk meningkatkan *Security Management* pada arsitektur berorientasi layanan berdasarkan keinginan pemangku kepentingan dan untuk memfasilitasi penjelasan yang didapatkan maka dapat diinterpretasikan dengan menggunakan *radar chart* pada gambar 11.



Gambar 11. Hasil penilaian berdasarkan AHP dengan radar chart

KESIMPULAN

Berdasarkan hasil evaluasi yang diperoleh ada beberapa kesimpulan yang diperoleh, yaitu hasil evaluasi menggunakan COBIT 4.1, terdapat 6 kriteria *Security Management* yang dijadikan dasar untuk mengevaluasi, antara lain *Strategy & Policies, Organization, dan Processes* serta domain yang digunakan adalah *Plan and Organizes (PO), Acquire and Implement (AI), Deliver and Support (DS), Monitor and Evaluation (ME)*. Sebagai hasil dari penilaian yang diperoleh untuk *People, Technology, dan Facilities*, perlu untuk ditingkatkan *maturity* levelnya. Sedangkan untuk rekomendasi yang dibutuhkan dengan menggunakan proses AHP, ada tiga hal yang perlu ditingkatkan sesuai keinginan pemangku kepentingan, yaitu perlunya meningkatkan kriteria *Technology* dengan nilai 0,132, *Facilities* dengan nilai 0,137, dan *People* dengan nilai 0,161 ketiga kriteria ini merupakan peringkat terendah pada kriteria yang diuji. Ketiga kriteria ini perlu ditingkatkan untuk meningkatkan *Security Management* pada arsitektur berorientasi layanan dan kedua metode ini dapat meyakinkan para pemangku kepentingan dalam mengevaluasi tidak hanya teori yang digunakan tetapi juga untuk mengukur evaluasi berdasarkan keinginan yang diinginkan oleh para pemangku kepentingan.

Penelitian ini memiliki kekurangan untuk menguji layanan berbasis kualitas, dalam penelitian ini hanya melihat dari perlu atau tidak nya domain yang diuji untuk ditingkatkan, tetapi tidak melihat kualitas yang dijalani pada organisasi, oleh karena itu diharapkan penelitian selanjutnya dapat meningkatkan pengujian pada domain cobit yang digunakan dipadukan dengan Teknik manajemen kualitas lain seperti *Quality Function Deployment (QFD), Six Sigma*, atau process mining berdasarkan *event log*.

DAFTAR PUSTAKA

- Balubaid, M., & Alamoudi, R. (2015). Application of the analytical hierarchy process (AHP) to multi-criteria analysis for contractor selection. *American Journal of Industrial and Business Management*, 5(09), 581.
- Brand, K. & Boonen, H. (2007). IT governance based on CobiT® 4.1-A management guide. *Van Haren*.
- Cotfas, L., & Palaghiță, D. (2010). Audit Techniques for Service Oriented Architecture Applications. *Informatica Economica*, 14(1).
- Fitrianah, D., & Sucahyo, Y. G. (2008). Audit Sistem Informasi/Teknologi Informasi dengan kerangka kerja COBIT untuk evaluasi manajemen teknologi informasi di Universitas XYZ. *Jurnal Sistem Informasi*, 4(1), 37-46.
- Harwikarya, M. S., Fitrianah, D., Sarinanto, M. M., Nurhaida, I., & Dwiyanto, A. R. (2015). IS Strategic Plan for Higher Education Based on COBIT Assessment: A Case Study. *International Journal of Information and Education Technology*, 5(8), 629-633.
- Karimi, O. (2011). Security model for service-oriented architecture. *arXiv preprint arXiv:1108.1314*
- Khther, R. A., & Othman, M. (2013). Cobit framework as a guideline of effective it governance in higher education: a review. *International Journal of Information Technology Convergence and Services*, 3(1), 21.
- Koç, E., & Burhan, H. A. (2015). An application of analytic hierarchy process (AHP) in a real world problem of store location selection. *Advances in Management and Applied Economics*, 5(1), 41.
- Krisanthi, G. A. T., Sukarsa, I. M., & Bayupati, I. P. A. (2014). Governance audit of application procurement using COBIT framework. *Journal of Theoretical and Applied Information Technology*, 59(2), 342-351.
- Latif, A. A., & Hanifi, N. (2013). Analyzing IT Function Using COBIT 4.1—A Case Study of Malaysian Private University. *Journal of Economics, Business and Management*, 1(4), 406-408.
- Li, H., Ni, F., Dong, Q., & Zhu, Y. (2018). Application of analytic hierarchy process in network level pavement maintenance decision-making. *International Journal of Pavement Research and Technology*, 11(4), 345-354.
- MacLennan, E., & Van Belle, J.-P. (2013). Factors affecting the organizational adoption of service-oriented architecture (SOA). *Information Systems and E-Business Management*, 12(1), 71-100. <https://doi.org/10.1007/s10257-012-0212-x>
- Saaty, T. L. (1996). Decision making with dependence and feedback. *The analytic network process*.
- Sulistiyono, M. (2016). Sistem Penunjang Keputusan Untuk Seleksi Calon Guru Menggunakan Analytical Hierarchy Process (Ahp). *Data Manajemen dan Teknologi Informasi (DASI)*, 17(2), 62-66.
- Weld, D., & Yang, M. (2018). Oracle® E-Business Suite Integrated SOA Gateway User's Guide, Release 12. United States of America.