

AUDIT KEAMANAN INFORMASI BERDASARKAN TRIANGLE CIA MENGUNAKAN FRAMEWORK COBIT® 4.1

Agung Pambudi¹⁾

¹⁾Informatika Universitas AMIKOM Yogyakarta
email : pambudia@amikom.ac.id¹⁾

Abstraksi

Tata kelola Teknologi Informasi merupakan kumpulan proses yang memastikan sesuai dengan implementasi teknologi informasi dalam mendukung tujuan dari organisasi. Tata kelola Teknologi Informasi (IT Governance) yang efektif, akan sangat berperan membantu dan mendukung sukses organisasi dalam mencapai tujuannya, meyakinkan untuk menginvestasikan Teknologi Informasi dan mengelola Teknologi Informasi dengan tepat berkaitan dengan resiko dan peluang, COBIT4.1. Terjadi peningkatan pelanggaran keamanan di organisasi / perusahaan, sebesar 90% PWC & Infosecurity[15], berdasarkan data ini perlu diadakan audit dan untuk mengetahui sejauh mana tata kelola Teknologi Informasi diterapkan. Tujuan dari penelitian ini adalah melakukan audit terhadap tata kelola Teknologi Informasi yang telah di implementasikan, audit keamanan informasi berdasarkan Triangle CIA (Confidentiality, Integrity, Availability),[16], menggunakan framework COBIT® 4.1. Berdasarkan Triangle CIA, maka diperoleh 4 domain, Plan and Organize, Acquire and Implement, Deliver and Support dan Monitor and Evaluate dengan 13 proses, terdiri dari PO2, PO9, AI2, AI3, AI6, DS4, DS5, DS10, DS11, DS12, DS13, ME1, ME2. Dalam penentuan responden berdasarkan tabel RACI (Responsible, Accountable, Consulted and Informed), diharapkan mewakili jabatan dan sesuai dengan tanggung jawabnya. Hasil akhir rata-rata Maturity Level 2 : Repeatable but Intuitive atau proses ini secara umum telah dimengerti oleh pihak manajemen tetapi belum didokumentasikan secara pasti.

Kata Kunci :

Audit keamanan informasi, Triangle CIA, Framework, Cobit 4.1

Abstract

IT governance is process which ensures IT implementation in supporting the organization goals. Effective IT governance would perform important roles in the effort of achieving organization objectives, in ensuring effective IT investment, and in governing effective IT properly in related to threats and opportunities. Threats to organizations or companies have reached 90 % based on PWC and info security therefore some audits should be initiated to observe the effectiveness of implementation of IT governance. The objective of the research is to audit an implemented IT governance, to audit the information security as it is based on CIA (Confidentiality, Integrity, and Availability) which uses COBIT® 4.1. The triangle CIA concludes 4 domains of Planning and Organizing, Acquiring and Implementing, Delivering, Supporting, Monitoring, and Evaluating using 13 processes of PO2, PO9, AI2, AI3, AI6, DS4, DS5, DS10, DS11, DS12, DS13, ME1, and ME2. The respondents are classified based on the table of RACI (Responsible, Accountable, Consulted, and Informed). The respondents represent the position and the responsibility in the company. The final result shows average Maturity Level 2: Repeatable but Intuitive, which concludes that, in general, the management is already aware of the processes but the processes are not yet surely documented.

Keywords :

Audit an implemented IT governance, framework, COBIT 4.1®.

Pendahuluan

Laudon[9] mendefinisikan infrastruktur Teknologi Informasi adalah sebagai sumber daya teknologi bersama dan sebagai platform sistem aplikasi khusus untuk perusahaan. Teknologi informasi merupakan investasi berupa perangkat keras, perangkat lunak dan layanan yang digunakan secara bersama sama di seluruh perusahaan atau di seluruh unit bisnis di perusahaan. Infrastruktur Teknologi Informasi melengkapi perusahaan dalam melayani dengan vendor dan dalam proses internal manajemen proses. Di era digital saat ini, informasi adalah aset

yang sangat berharga bagi kelangsungan suatu lembaga atau organisasi, pertahanan keamanan serta keutuhan negara, kepercayaan publik, konsumen dan reputasi atau kredibilitas, sehingga harus dijaga ketersediaan, ketepatan dan keutuhan informasinya, Karsten [10]. Informasi itu bisa berupa dalam berbagai bentuk format, seperti teks, audio, visual atau video. Berkaitan dengan hal tersebut diatas maka diperlukan suatu manajemen pengelolaan informasi yang bertujuan untuk melindungi kerahasiaan, integritas dan ketersediaan informasi tersebut. Pada tahun 2017 serangan keamanan

informasi / dunia maya merupakan ancaman yang terus menerus, sekitar sepertiga (32%) bisnis dan dua dari sepuluh badan amal (22%) melaporkan mengalami pelanggaran atau serangan keamanan, Cyber Security [4]. Berdasarkan data serangan keamanan ini, maka perlu diadakan audit dan untuk mengetahui sejauh mana tata kelola Teknologi Informasi diterapkan.

Dengan demikian penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi, organisasi dan layanan umum seperti di Perpustakaan dalam rangka peningkatan kualitas layanan. Dalam penyelenggaraan tata kelola Teknologi Informasi dan Komunikasi (TIK), faktor keamanan informasi merupakan bagian yang sangat penting diperhatikan, Pedoman Sekjen [14], dalam rangka kinerja tata kelola Teknologi Informasi dan Komunikasi (TIK) akan terganggu jika informasi salah, obyek utama tata kelola Teknologi Informasi dan Komunikasi (TIK) mengalami masalah keamanan informasi yang menyangkut kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) (Introduction to Information Security) [10] [16].

Sejarah tentang keamanan informasi berawal dari keamanan komputer, dimana yang diperlukan dalam keamanan komputer berupa keamanan lokasi fisik, perangkat keras dan perangkat lunak dari ancaman luar, Grampp and Morris [5]. Setelah perang dunia ke II, komputer main frame pertama kalinya dikembangkan untuk membantu memecahkan kode-kode rahasia dalam komunikasi. Berlapis-lapisnya tingkatan keamanan diterapkan untuk melindungi komputer main frame dan integritas datanya. Pada awalnya untuk akses lokasi yang peka harus menggunakan tanda pengenalan atau lencana, kunci dan pengenalan wajah oleh penjaga. Seiring dengan kebutuhan dalam menjaga keamanan informasi selanjutnya semakin lebih rumit dan dibutuhkan teknologi.

Audit Keamanan Informasi di Perpustakaan AMIKOM YOGYAKARTA ini dipilih COBIT® versi 4.1 dengan pertimbangan lebih mudah diterapkan dibandingkan dengan Audit Keamanan Informasi seperti BS7799, COBIT 5 dan COBIT 2019. COBIT adalah sekumpulan dokumentasi best practices untuk IT governance yang dapat membantu auditor, pengguna (user), dan manajemen, untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI, Sasongko [17]. Dari penelitian ini, bagaimana melakukan audit keamanan informasi berdasarkan triangle CIA menggunakan Framework COBIT® 4.1?

Tinjauan Pustaka

Didalam penelitian ini, penulis menggunakan beberapa referensi dari hasil penelitian yang pernah dilakukan, antara lain : Hasil penelitian, Lucia Meita Rosalika, dkk, Audit Sistem Informasi

Perpustakaan Universitas Kristen Petra Berdasarkan Standar Control Objectives for Information and Related Technology (COBIT 4.0). Pada penelitian ini, dilakukan proses audit operasional untuk mengumpulkan data guna menunjang penilaian audit. Pedoman yang digunakan dalam mengukur aspek – aspek tingkat kedewasaan TI ialah COBIT 4.0 pada bagian delivery and support 4, 5, 10, 11, dan 12 yang terdiri dari pemastian kelangsungan layanan TI, pengelolaan sistem keamanan, pengelolaan masalah, pengelolaan data, dan pengelolaan lingkungan fisik di perpustakaan. Penelitian ini menghasilkan temuan dan nilai tingkat kematangan TI di perpustakaan. Proses audit membantu perpustakaan dalam mengevaluasi kinerja layanan TI dan memberi masukan untuk perbaikan, Lucia [11], penelitian ini tidak mengacu berdasarkan triangle CIA dan menggunakan COBIT 4.0.

Hasil penelitian Paradise, Kusri, Asro Nasiri tentang Audit Keamanan Aplikasi E-Cash Menggunakan ISO 27001, melakukan audit menggunakan ISO 27001 untuk memastikan Bank Mandiri bekerja sesuai dengan prosedur yang ada. ISO/IEC 27001:2005 adalah standar keamanan sistem informasi yang mempunyai 27 klausul untuk mengukur tingkat keamanan bank, penelitian ini tidak mengacu berdasarkan triangle CIA dan menggunakan ISO 27001 [13].

Hasil penelitian Audit Sistem Informasi Perpustakaan FMIP UNS, Yudho Yudhanto, Ema Utami, Andi Sunyoto, melakukan penelitian aktifitas-aktifitas pada Domain Deliver and Support sudah, penelitian ini tidak mengacu berdasarkan triangle CIA.

COBIT 4.1 terbit pada tahun 2007, menggambarkan Framework COBIT dalam bentuk kubus dengan 3 (tiga) dimensi, dimensi pertama berupa proses TI yang terdiri dari 3 (tiga) bagian yaitu activities, processes dan domains. Dimensi kedua berupa Business Requirements terdiri dari 7 (tujuh), Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance dan Reliability. Penelitian ini berdasarkan Business Requirements dengan Confidentiality, Integrity dan Availability. Dimensi ketiga kubus COBIT adalah IT Resources, yang terdiri dari sejumlah komponen sumber daya, berupa : aplikasi, informasi, infrastruktur, dan manusia.

Untuk memenuhi tujuan dari bisnis, informasi harus sesuai dengan kriteria kontrol tertentu, COBIT menyebutkan sebagai bisnis persyaratan informasi, berdasarkan kualitas, fidusia dan keamanan yang lebih luas, kriteria informasi didefinisikan sebagai berikut :

1. Effectiveness (efektivitas). Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, konsisten dapat dipercaya dan tepat waktu
2. Efficiency (efisiensi). Penyediaan informasi yang optimal melalui penggunaan sumber daya (yang paling produktif dan ekonomis)

3. Confidentially (kerahasiaan). Berkaitan dengan perlindungan informasi penting dari pihak-pihak yang tidak memiliki hak otorisasi / tidak berwenang
4. Integrity (keutuhan). Berkaitan dengan keakuratan, kelengkapan data / informasi, tingkat validitas yang sesuai dengan harapan dan nilai bisnis
5. Availability (ketersediaan). Fokus terhadap ketersediaan data / informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun dimasa yang akan datang, juga terkait dengan pengamanan atas sumber daya yang diperlukan
6. Compliance (kepatuhan). Pemenuhan data / informasi yang sesuai dengan ketentuan hukum, peraturan, dan rencana perjanjian / kontrak untuk proses bisnis
7. Reliability (kehandalan). Fokus pada penyampaian informasi yang tepat bagi manajemen untuk menjalankan perusahaan dan pemenuhan kewajiban mereka untuk membuat laporan yang berkaitan dengan keuangan.

Organisasi TI memenuhi tujuan dengan serangkaian proses yang didefinisikan dengan jelas, menggunakan keterampilan orang dan teknologi infrastruktur untuk menjalankan aplikasi bisnis, sambil memanfaatkan informasi bisnis, berikut ini penjelasan sumber daya TI berdasarkan kubus COBIT :

1. Aplikasi : Berupa sistem otomatis dan prosedur manual yang memproses informasi.
2. Informasi : Berupa data dengan beragam macamnya, masukan, olahan dan keluaran oleh sistem informasi dalam bentuk apapun yang digunakan bisnis.
3. Infrastruktur : adalah teknologi dan fasilitas (bisa dalam bentuk perangkat keras, sistem operasi, sistem manajemen basis data, jaringan , multimedia dan lingkungan yang menampung dan mendukungnya) memungkinkan pemrosesan aplikasi.)
4. Orang : adalah personel yang diperlukan untuk merencanakan, mengatur, memperoleh, melaksanakan, menyampaikan, mendukung, memantau, dan mengevaluasi informasi sistem dan layanan.

COBIT Framework mencakup tujuan pengendalian yang terdiri dari 4 domain yaitu :

1. Plan and Organise (PO)

Domain ini menitik beratkan pada proses perencanaan dan penyesuaian strategi TI, dengan strategi perusahaan, mencakup masalah strategi, taktik dan identifikasi tentang bagaimana TI dapat memberikan kontribusi maksimal terhadap

pencapaian tujuan bisnis organisasi sehingga terbentuk sebuah organisasi yang baik dengan infrastruktur teknologi yang baik pula, COBIT4.1[3]. Domain ini mencakup 10 proses :

- PO1 – Menentukan rencana strategis
- PO2 – Menentukan arsitektur informasi
- PO3 – Menentukan arah teknologi
- PO4 – Menentukan proses TI, organisasi dan hubungannya
- PO5 – Mengelola investasi TI
- PO6 – Mengkomunikasikan tujuan dan arahan manajemen
- PO7 – Mengelola sumber daya manusia
- PO8 – Mengelola kualitas
- PO9 – Menilai dan mengelola resiko TI
- PO10 – Mengelola proyek

2.Acquire & Implementation (AI).

Domain ini berkaitan dengan implementasi solusi TI dan integrasinya dalam proses bisnis organisasi untuk mewujudkan strategi TI, juga meliputi perubahan dan maintenance yang dibutuhkan sistem yang sedang berjalan untuk memastikan daur hidup sistem tersebut tetap terjaga, COBIT4.1 [3]. Domain ini meliputi:

- AI1 – Mengidentifikasi solusi yang dapat diotomatisasi,
- AI2 – Mendapatkan dan maintenance software aplikasi.
- AI3 – Mendapatkan dan maintenance infrastuktur teknologi
- AI4 – Mengaktifkan operasi dan penggunaan
- AI5 – Pengadaan sumber daya IT.
- AI6 – Mengelola perubahan
- AI7 – Instalasi dan akreditasi solusi dan perubahan

3. Delivery and Support (DS)

Domain ini mencakup proses pemenuhan layanan IT, keamanan sistem, kontinuitas layanan, pelatihan dan pendidikan untuk pengguna, dan pemenuhan proses data yang sedang berjalan. COBIT4.1 [3], Domain ini meliputi :

- DS1 – Menentukan dan mengelola tingkat layanan.
- DS2 – Mengelola layanan dari pihak ketiga
- DS3 – Mengelola performa dan kapasitas.
- DS4 – Menjamin layanan yang berkelanjutan
- DS5 – Menjamin keamanan sistem.
- DS6 – Mengidentifikasi dan mengalokasikan dana.
- DS7 – Mendidik dan melatih pengguna
- DS8 – Mengelola service desk dan insiden.
- DS9 – Mengelola konfigurasi.
- DS10 – Mengelola permasalahan.
- DS11 – Mengelola data
- DS12 – Mengelola lingkungan fisik
- DS13 – Mengelola operasi.

4. Monitoring and Evaluation (ME)

Domain ini berfokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan

internal dan eksternal dan jaminan independent dari proses pemeriksaan yang dilakukan, COBIT4.1 [3].

Domain ini meliputi:

ME1 – Mengawasi dan mengevaluasi performansi TI.

ME2 – Mengevaluasi dan mengawasi kontrol internal

ME3 – Menjamin kesesuaian dengan kebutuhan eksternal.

ME4 – Menyediakan IT Governance.

COBIT menyediakan kerangka identifikasi sejauh mana perusahaan telah memenuhi standar pengelolaan proses TI yang baik yang direpresentasikan dalam sebuah model maturity yang memiliki level pengelompokan kemampuan organisasi dalam pengelolaan proses TI dari level nol (non existent) hingga level lima (optimized), dengan penjelasannya sebagai berikut:

0 Non Existent (tidak ada), merupakan posisi kematangan terendah, kondisi di mana organisasi merasa tidak membutuhkan adanya mekanisme proses tata kelola TI yang baku.

1 initial (inisialisasi), inisiatif mekanisme perencanaan, tata kelola dan pengawasan sudah ada, namun sifatnya masih adhoc, sporadis, dan reaktif.

2 Repeatable (dapat diulang), organisasi telah memiliki perencanaan dan pengelolaan TI secara berulang namun belum melibatkan prosedur dan dokumen formal.

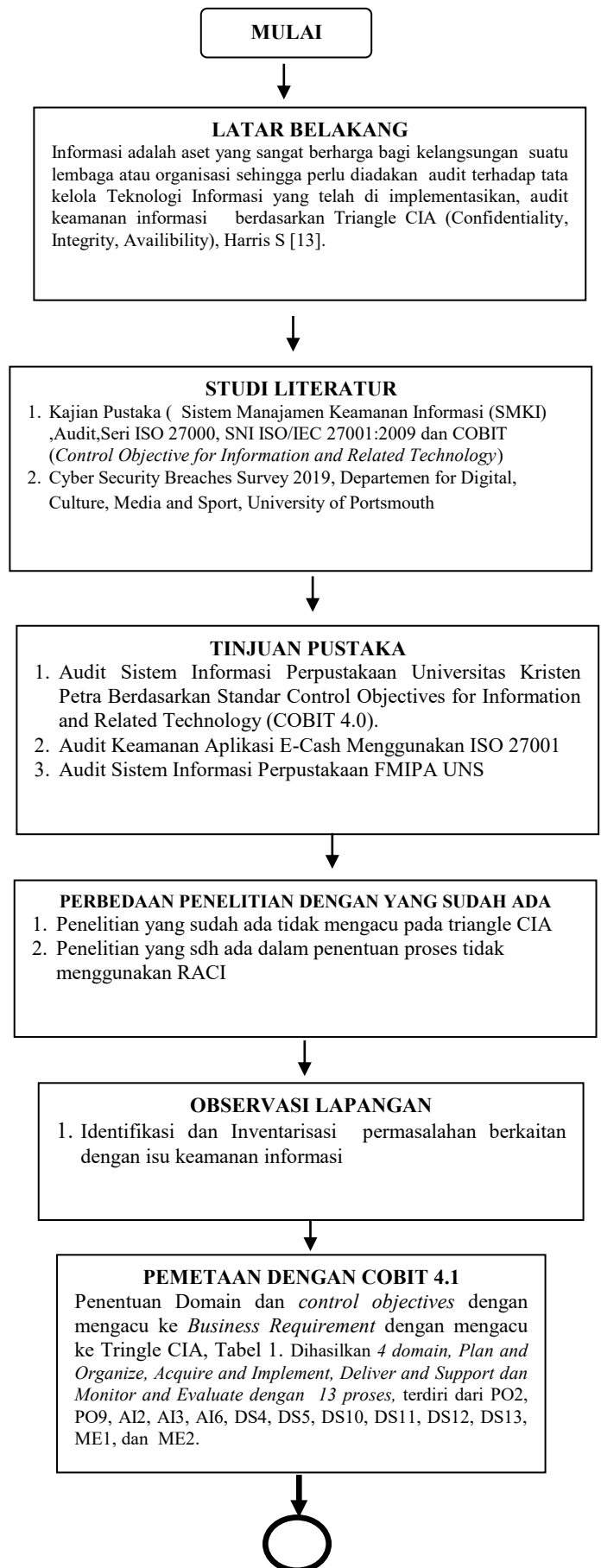
3 Defined (ditetapkan), mekanisme dan prosedur yang jelas mengenai tata cara dan manajemen tata kelola IT telah dikomunikasikan dan disosialisasikan dengan baik di seluruh jajaran manajemen.

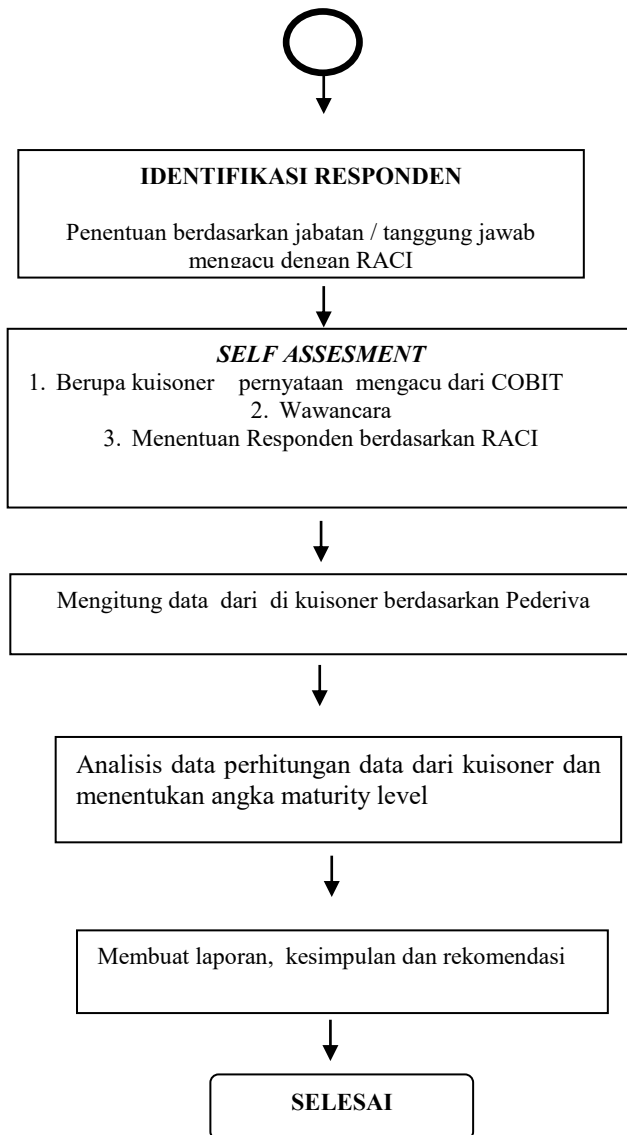
4 Managed (diatur), manajemen telah menerapkan indikator pengukuran kinerja kuantitatif untuk memonitor efektivitas pelaksanaan manajemen tata kelola IT.

5.Optimised, adalah kondisi dimana perusahaan dianggap telah mengimplementasikan manajemen tata kelola TI yang mengacu pada “best practices” dan sepenuhnya otomatis.

Metode Penelitian

Metoda penelitian yang digunakan dalam Audit Keamanan Informasi di Perpustakaan Universitas AMIKOM YOGYAKARTA terdiri dari penelaahan dokumen yang berkaitan dengan Sistem Informasi Perpustakaan yang bernama Smart Library, infra struktur yang mendukungnya dan self Assessment berupa kuisioner, dengan tahapannya di Gambar 1.





Gambar 1 Tahapan Metoda Penelitian

DOMAIN	PROCESS	Information Criteria					IT Resources			
		Efficacy	Efficiency	Confidentiality	Integrity	Availability	People	Applications	Technology	Facilities
Plan and Organise	PO1 Define a strategic IT plan	P	S				✓	✓	✓	✓
	PO2 Define the information architecture ✓	P	S	S	S		✓		✓	
	PO3 Determine technological direction	P	S						✓	✓
	PO4 Define the IT organisation and relationships	P	S				✓			
	PO5 Manage the IT investment	P	P			S	✓	✓	✓	✓
	PO6 Communicate management aims and direction	P				S	✓			
	PO7 Manage human resources	P	P				✓			
	PO8 Ensure compliance with external requirements	P				P	S	✓	✓	✓
	PO9 Assess risks ✓	P	S	P	P	S	S	✓	✓	✓
	PO10 Manage projects	P	P				✓	✓	✓	✓
Acquire and Implement	AI1 Identify automated solutions	P	S				✓	✓	✓	
	AI2 Acquire and maintain application software ✓	P	P	S	S	S	✓			
	AI3 Acquire and maintain technology infrastructure ✓	P	P	S					✓	
	AI4 Develop and maintain procedures	P	P	S	S	S	✓	✓	✓	✓
	AI5 Install and accredit systems	P		S	S	S	✓	✓	✓	✓
	AI6 Manage changes ✓	P	P	P	P	S	✓	✓	✓	✓
Deliver and Support	DS1 Define and manage service levels	P	P	S	S	S	S	✓	✓	✓
	DS2 Manage third-party services	P	P	S	S	S	S	✓	✓	✓
	DS3 Manage performance and capacity	P	P	S				✓	✓	✓
	DS4 Ensure continuous service ✓	P	S	P				✓	✓	✓
	DS5 Ensure systems security ✓		P	P	S	S	S	✓	✓	✓
	DS6 Identify and allocate costs		P				P	✓	✓	✓
	DS7 Educate and train users	P	S					✓		
	DS8 Assist and advise customers	P	P					✓		
	DS9 Manage the configuration	P				S	S	✓	✓	✓
	DS10 Manage problems and incidents ✓	P	P	S				✓	✓	✓
	DS11 Manage data ✓			P			P			✓
	DS12 Manage facilities ✓			P	P					✓
	DS13 Manage operations ✓	P	P	S	S			✓	✓	✓
Monitor and Evaluate	M1 Monitor the processes ✓	P	P	S	S	S	S	✓	✓	✓
	M2 Assess internal control adequacy ✓	P	P	S	S	S	P	S	✓	✓
	M3 Obtain independent assurance	P	P	S	S	S	P	S	✓	✓
	M4 Provide for independent audit	P	P	S	S	S	P	S	✓	✓

Gambar 1. Penentuan Domain dan kriteria informasi berdasarkan Triangle CIA

Hasil dan Pembahasan

Dari Gambar 1 maka didapatkan 4 domain yang terdiri dari *Plan and Organise*, *Acquire and Implement*, *Delivery Support* dan *Monitor and Evaluate* dengan 13 Proses TI.

Tabel 1. Penentuan Domain dan kriteria informasi berdasarkan Triangle CIA

No	Struktur RACI	Struktur Organisasi	High Control Objectives													
			PO 2	PO 9	AI 2	AI 3	AI 6	DS 4	DS 5	DS1 0	DS1 1	DS1 2	DS1 3	ME 1	ME 2	
1	CEO (Chief of executive Officer)	Rektor													✓	
2	CFO (Chief Financial Officer)	Warek II		✓												
3	Business Executive															
4	CIO (Chief of Information Officer)	Wadir , Innovation Centre		✓		✓										
5	Business Process Owner	Resource Centre/Pe rpus		✓	✓										✓	
6	Head Operations	Wadir , Innovation Centre		✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Chief Architect	Manager Software	✓	✓					✓	✓	✓					
8	Head Development	Manager Software		✓	✓			✓	✓	✓	✓				✓	✓
9	Head IT Administration	Manager Content+infra struk		✓		✓		✓		✓						✓
10	PMO (Project Manager Officer)	Manager Software			✓		✓									
11	Compliance,Audit, Risk and Security.	Bagian Penjaminan mutu	✓	✓	✓			✓	✓	✓						✓

No	Struktur RACI	Struktur Organisasi	High Control Objectives													
			PO 2	PO 9	AI 2	AI 3	AI 6	DS 4	DS 5	DS1 0	DS1 1	DS1 2	DS1 3	ME 1	ME 2	
1	CEO (Chief of executive Officer)	Rektor													✓	
2	CFO (Chief Financial Officer)	Warek II		✓												
3	Business Executive															
4	CIO (Chief of Information Officer)	Wadir , Innovation Centre		✓		✓										
5	Business Process Owner	Resource Centre/Pe rpus		✓	✓										✓	
6	Head Operations	Wadir , Innovation Centre		✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Chief Architect	Manager Software	✓	✓					✓	✓	✓					
8	Head Development	Manager Software		✓	✓			✓	✓	✓	✓				✓	✓
9	Head IT Administration	Manager Content+infra struk		✓		✓		✓		✓						✓
10	PMO (Project Manager Officer)	Manager Software			✓		✓									
11	Compliance,Audit, Risk and Security.	Bagian Penjaminan mutu	✓	✓	✓			✓	✓	✓						✓

Berdasarkan dari RACI (*Responsibility, Accountable, Consulted, Informed*) chart dalam Tabel 2. Dalam melakukan penelitian ini, ada sejumlah 13 responden, terdiri 5 unsur pimpinan, 2 manajer dan 5 staf. Dengan rincian masing-masing untuk kriteria untuk pernyataan, yang didapatkan dari RACI *chart*. Tabel 2, penentuan kuisoner untuk unsur pimpinan, manajer dan staf.

No	Struktur Organisasi	High Control Objectives													
		PO 2	PO 9	AI 2	AI 3	AI 6	DS 4	DS 5	DS 10	DS 11	DS 12	DS 13	ME 1	ME 2	
1	Rektor													✓	
2	Warek II		✓												
3															
4	Wadir , Innovation Centre		✓		✓										
5	Perpustakaan		✓	✓										✓	
6	Wadir , Innovation Centre		✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Manajer Software	✓	✓					✓	✓	✓					
8	Manajer Software		✓	✓		✓	✓	✓	✓					✓	✓
9	Manajer Content-infrastruktur		✓		✓		✓	✓	✓						✓
10	Manajer Software			✓		✓									
11	Bagian Penjaminan mutu	✓	✓	✓			✓	✓	✓						✓

Gambar 2. Tabel penentuan kriteria kuisoner berdasarkan jabatan

Tabel 2. Latar belakang pendidikan responden.

No	Pendidikan	Jumlah	Prosentase (%)
1	S3	1	7.69
2	S2	6	46.15
3	S1	5	38.46
4	D3	1	7.69

Dalam melakukan penelitian ini, tingkat kematangan dari keamanan Sistem Informasi Perpustakaan *Smart Library* yang diharapkan dapat ditentukan melalui pengkajian dokumen-dokumen yang berkaitan, wawancara dan kuisoner berupa *self assessment* dengan mengacu dari pertanyaan berdasarkan COBIT4.1. Berikut ini hasil dari wawancara dan kesimpulan rencana strategi Institusi Universitas AMIKOM YOGYAKARTA 2016-2020, dalam rangka mewujudkan Visi Misi dari Institusi menjadi *Entrepreneur University* dan Universitas berbasis Teknologi Informasi Komputer:

- a. Mewujudkan *Integrated University*, diantaranya termasuk Sistem Informasi Perpustakaan *Smart Library*.

- b. Mewujudkan tata kelola Teknologi Informasi institusi yang secara menyeluruh dan efektif.

Atas tujuan strategis TI tersebut selanjutnya dijabarkan sebagai berikut:

- a. Terpenuhinya akan kebutuhan dan kepentingan akan Teknologi Informasi Komunikasi.
- b. Meningkatkan penggunaan dan pemanfaatan Teknologi Informasi dan Komunikasi secara menyeluruh di segala lini.
- c. Meningkatkan mutu pengelola sumber daya Teknologi Informasi dan Komunikasi.
- d. Meningkatkan mutu layanan berbasis Teknologi Informasi dan Komunikasi.

Dari asas tujuan strategis TI dan dikaitkan dengan fokus IT *Resources* dari COBIT® 4.1, yaitu *Application, Information, Infrastructure* dan *People* maka diharapkan dari Universitas AMIKOM YOGYAKARTA adalah sebagai berikut :

- a. *Application* : Penggunaan Teknologi Informasi di organisasi dikembangkan secara bertahap dan diterapkan di segala lini layanan dan bagian.
- b. *Information* : Organisasi sudah seharusnya mengelola dan menggunakan informasi sebaik-baiknya dan menjauhkan informasi dari akses yang tidak berkepentingan.
- c. *Infrastructure* : Organisasi sudah seharusnya mengelola infrastruktur yang meliputi perangkat keras komputer, perangkat lunak *platform* atau Sistem Operasi, basis data, jaringan LAN ataupun WAN / Internet mengandung aspek efisien, efektif dan fleksibel.
- d. *People* : Organisasi sudah seharusnya bahwa Sumber Daya Manusia atau *Human Capital* meningkatkan keahlian dan kompetensi melalui berbagai pelatihan dan *workshop*.

Didalam penelitian ini, teknik perhitungan untuk mengetahui *maturity level* COBIT® dengan mengacu dari Pederiva (*The COBIT Maturity Model in a Vendor Evaluation Case*). Ada dua hal penting yang perlu dilakukan dalam tahap evaluasi yaitu kriteria untuk memilih proses-proses yang dievaluasi dan metoda untuk mengukur tingkat kedewasaan organisasi berdasarkan pedoman model kedewasaan COBIT® [Pederiva, 2003]. Pederiva mengemukakan bahwa skenario tingkat kematangan mencakup deskripsi dari organisasi dan pengontrolan internal perusahaan yang memenuhi persyaratan tingkat kematangan tertentu. Pembuatan kuesioner mengacu dari COBIT® berdasar *maturity level* yang terbagi menjadi 6 (enam) tingkatan, dimulai dari tingkatan 0 (*non-existent*), tingkatan 1 (*initial /adhoc*), tingkatan 2 (*Repeatable but intuitive*), tingkatan 3 (*Defined*), tingkatan 4 (*Managed and Measureble*) dan tingkatan 5 (*Optimised*).

Dari setiap pernyataan diatas ada 4 (empat) pilihan yang berupa :

1. Tidak benar sama sekali

2. Ada benarnya
3. Sebagian besar benar
4. Sepenuhnya benar

Setiap jawaban diatas selanjutnya diberikan bobot penilaian seperti pada Tabel 3.

Tabel 3. Contoh Kuisioner Maturity level 3, Andrea [2]

Compliance Level Numeric Values	
Agreement with Statement	Compliance Value
Not at all	0
A little	0.33
Quite a lot	0.66
Completeness	1

Tabel 4. Maturity model

Questionnaire for the Level 3 Maturity Model of Process PO10					
Level	Statements	How much do you agree?			Statements compliance values
		Not at all	A little	Completely	
1	The IT project management process and methodology have been formally established and communicated.				0.66
2	IT projects are defined with appropriate business and technical objectives.				0.66
3	Stakeholders are involved in the management of IT projects.			x	1
4	The IT project organization and some roles and responsibilities are defined.			x	1
5	IT projects have defined and updated schedule milestones.				0.66
6	IT projects have defined and managed budgets.			x	1
7	IT projects monitoring relies on clearly defined performance measurement techniques.	x			0.33
8	IT projects have formal post-system implementation procedures.				0.66
9	Informal project management training is provided.			x	1
10	Quality assurance procedures and post-system implementation activities have been defined, but are not broadly applied by IT managers.				0.66
11	Policies for using a balance of internal and external resources are being defined.			x	1
Total level: 8.63					

Tabel 5. Contoh Perhitungan Pencapaian tiap maturity level (Pederiva, 2003)

Computation of the Maturity Level Compliance Values			
Maturity level	Sum of statements compliance values (A)	Number of maturity level statements (B)	Maturity level compliance value (A/B)
0	0.00	2.00	0.00
1	0.00	9.00	0.00
2	3.00	6.00	0.50
3	8.63	11.00	0.78
4	6.97	9.00	0.77
5	6.31	8.00	0.79

Dari hasil nilai capaian setiap maturity level seperti di Tabel 3, maka langkah selanjutnya melakukan normalisasi seperti pada Tabel 4.

Tabel 5. Contoh Perhitungan normalisasi tiap maturity level, Andrea [2]

Computation of the Normalized Compliance Vector		
Level	Not normalized compliance values (A)	Normalized compliance values [A/Sum(A)]
0	0.00	0.000
1	0.00	0.000
2	0.50	0.176
3	0.78	0.275
4	0.77	0.272
5	0.79	0.277
Total:	2.84	1

Dibawah contoh ini proses perhitungan maturity level setiap proses dimulai dengan proses PO2, PO9, AI2, AI3, AI6, DS4, DS5, DS10, DS11, DS12, DS13, ME1 dan ME2.

Tujuan dari PO2 ini adalah pengukuran Maturity Level dalam mendefinisikan arsitektur informasi di Sistem Informasi Perpustakaan Smart Library, berikut ini ada hasil perhitungan untuk proses PO2.

Tabel 9. Nilai Perhitungan rata-rata Maturity Level dari PO2

NO	RACI Roles	Organization Roles	PO2 Maturity Level					
			0	1	2	3	4	5
1	CEO	Rektor	0.67	2.67	2	3	4	3
2	CFO	Warek II						
3	Business Executive							
4	CIO	Wadir IC						
5	BP Owner	Perpus						
6	Head Operations	Wadir IC						
7	Chief Architect	Manajer SW	0.33	2	1.67	2.67	3.34	2.65
8	Head Development	Manajer SW						
9	Head IT Admin	Content+infra struktur						
10	PMO	Manajer SW						
11	Compliance, Audit, Risk & Security	Bagian Penjaminan Mutu	0.67	2.01	1.67	1.67	0.33	1
Nilai rata-rata =			0.56	2.23	1.78	2.45	2.56	2.22
A=(Nilai rata-rata /Jumlah Pernyataan)			0.28	0.56	0.593	0.41	0.37	0.32

Tabel 10, Jumlah pernyataan tiap maturity level PO2

	PO2					
	Maturity Level					
Jumlah Pernyataan	0	1	2	3	4	5
	2	4	3	6	7	7

Tabel 11. Hasil perhitungan normalisasi tiap Maturity Level PO2

Perhitungan normalisasi		
Level	A	$B=(A/\Sigma A)$
0	0.28	0.11
1	0.56	0.22
2	0.59	0.24
3	0.41	0.16
4	0.37	0.15
5	0.32	0.13
Total	2.52	1.00

Tabel 12. Hasil akhir perhitungan tiap Maturity Level PO2

Perhitungan Maturity		
Level	B	$B*Level$
0	0.11	0.00
1	0.22	0.22
2	0.24	0.47
3	0.16	0.49
4	0.15	0.58
5	0.13	0.63
Maturity Level		2.39

Contoh perhitungan tabel 12 perhitungan tiap maturity level nilai kematangan untuk PO2 *Define the Information Architecture* berada di maturity level 2- *Repeatable but intuitive*, COBIT4.1 [3]. Hasil dari perhitungan dari masing-masing domain dan proses didapatkan hasil dalam Tabel 13.

Tabel 13, hasil perhitungan dari 4 domain dan 13 proses

No	Proses	Hasil perhitungan Maturity level
1	PO2 , <i>Define the Information Architecture</i>	2,39
2	PO9, <i>Assess and Manage IT Risks</i>	1,89
3	AI2, <i>Acquire and Maintain Application</i>	2,55

	<i>Software</i>	
4	AI3, <i>Acquire and Maintain Technology Infrastructure</i>	3,11
5	AI6, <i>Manage Changes</i>	2,44
6	DS4, <i>Ensure Continuous Service</i>	2,40
7	DS5, <i>Ensure Systems Security</i>	1,78
8	DS10, <i>Manage Problemstems Security</i>	2,32
9	DS11, <i>Manage Data</i>	2,65
10	DS12, <i>Manage the Physical Environment</i>	2,57
11	DS13, <i>Manage Operations</i>	2,88
12	ME1, <i>Monitor and Evaluate IT Performance</i>	2,16
13	ME2, <i>Monitor and Evaluate Internal Control</i>	1,55
	Rata-rata	2,36

Kesimpulan dan Saran

Kesimpulan

Hasil audit berdasarkan Proses TI hasil kesimpulannya adalah sebagai berikut :

1. Dari 4 domain dan 13 proses dihasilkan dengan nilai rata-rata sebesar 2.36, artinya berada pada posisi Maturity Level ke2- Repeatable but intuitive.
2. Proses yang mirip dan umum sudah mulai dilaksanakan namun sebagian besar bersifat intuitif yang muncul dari keahlian individu.
3. Beberapa aspek proses bersifat repeatable karena keahlian individu, serta beberapa dokumentasi dan pemahaman informal terhadap kebijakan dan prosedur sudah ada.
4. Responsibility & Accountability sebagai berikut: Individu mengasumsikan tanggung jawab masing-masing dan biasanya accountable walaupun tidak disepakati secara formal.
5. Kebingungan terkait tanggungjawab kadang terjadi ketika masalah muncul dan budaya saling menyalahkan biasanya terjadi.
6. Goal setting mulai muncul, disertai dengan pengukuran financial terkait, namun hanya diketahui oleh level manajemen senior.
7. Monitoring dilakukan secara inkonsisten pada area-area tertentu saja.
8. testing untuk memastikan bahwa sistem dapat berjalan sesuai kebutuhan fungsionalitas dan untuk menemukan

kesalahan-kesalahan yang mungkin masih terdapat dalam sistem.

Saran

Berdasarkan analisis perhitungan maturity level 2 - Repeatable but intuitive, saran-saran yang diberikan adalah sebagai berikut:

1. Penilai tingkat maturity level Sistem Informasi Perpustakaan, bahwa proses tata kelola melalui 4 domain masih banyak terdapat kekurangan di hampir semua Proses TI kecuali di AI3 Acquire and Maintain Technology Infrastructure, dengan nilai mencapai 3.11.
2. Sumber daya manusia: perlu ada peningkatan pelatihan atau workshop yang dibuat dalam rencana, adanya sharing session supaya setiap ada permasalahan tidak saling menyalahkan dan budaya manajemen untuk mengkomunikasikan permasalahan yang ada.
3. Didalam penelitian ini belum semua dari Triangle CIA bagian Sekunder untuk semua domain digunakan dan memungkinkan peneliti lain untuk melakukan proses ini.

Daftar Pustaka

- [1] Andrea Pederiva, "The COBIT Maturity Model ini Vendor Evaluton Case"
- [2] Yudho Yudhanto, Ema Utami, Andi Sunyoto, Audit Sistem Informasi Perpustakaan FMIP UNS, Prosiding: Seminar Nasional Teknologi Informasi dan Multimedia 2018, 2018
- [3] COBIT4.1, Frame work Control Objectives Management Guidelines Maturity Models
- [4] Cyber Security Breaches Survey 2019, Departemen for Digital, Culture, Media and Sport, University of Portsmouth
- [5] F. T. GRAMPP and R. H. MORRIS, UNIX Operating System Security (Manuscript received February 7, 1984)
- [6] Harris S. CISSP Certification Exam Guide. McGraw-Hill/Osbourne, 2002
- [7] Implementation of modified maturity level measurement model for All COBIT framework (case study: IT Management audit of PT.POS Indonesia) belum masuk
- [8] ISO/IEC 27001 , Information technology Security techniques Information security management systems Requirements
- [9] K. Laudon, Management Information System: Managing the Digital Firm. England: Pearson Education Limited, 2014, p. 195.,
- [10] Karsten Brauer, AUTHENTICATION AND SECURITY ASPECTS in an international multi-user network
- [11] Lucia Meita Rosalika, Adi Wibowo, Ibnu Gunawan, Audit Sistem Informasi Perpustakaan Universitas Kristen Petra Berdasarkan Standar Control Objectives For Information and Related Technology (COBIT 4.0).
- [12] Oscarson, Information Security Fundamental, 2003
- [13] Paradise , Kusrini , Asro Nasiri, Audit Keamanan Aplikasi E-Cash Menggunakan ISO 27001, creative information technology journal (citec journal), 2018
- [14] Pedoman Sekjen No.1 Tahun 2018 tentang Tata Kelola Teknologi Informasi di lingkungan Kemkominfo
- [15] PWC& Infosecurity Europe , 2015 Information Security Breaches Survey
- [16] Saman Shojae Chaeikar, Mohammadreza Jafari, Hamed Taherdoost, Nakisa Shojae Chaei kar, Definitions and Criteria of CIA Security, Triangle in Electronic Voting System, International Journal of Advanced Computer Science and, Information Technology (IJACSIT), Vol. 1, No.1, October 2012, Page: 14-24, ISSN: 2296-1739, © Helvetic Editions LTD, Switzerland
- [17] Sasongko, Pengukuran Kinerja Teknologi Informasi dengan Menggunakan Framework COBIT Versi 4.0, Ping Test dan CAAT pada PT. Bank X Tbk di Bandung. Seminar Nasional Aplikasi Teknologi Informasi 2009 (SNATI 2009), Yogyakarta
- [18] Shengnan (Sophie) Zhang, An Exploratory Examination of the Practicability of COBIT framework