AUDIT SISTEM INFORMASI AKADEMIK BERBASIS *WEB* MENGGUNAKAN FRAMEWORK COBIT 5.0 PADA DOMAIN APO13 DAN DSS05 (Studi Kasus: SIAT STMIK ROSMA KARAWANG)

[1]Rahmat Gunawan, [2] Djajasukma Tjahjadi
E-mail: [1]gunawanr46@gmail.com, [2]djaja@likmi.ac.id

Abstrak

STMIK Rosma adalah perguruan tinggi swasta yang berdiri didalam naungan Yayasan Pendidikan Rosma yang berdomisili di Kabupaten Karawang. Saat ini perguruan telah menerapkan sistem dan teknologi informasi dalam mendukung operasional akademik yang dilaksanakan oleh Divisi IT. Tetapi, terdapat beberapa kekurangan dalam penerapan tersebut khususnya dalam hal keamanan seperti security incident. Untuk mencegah hal-hal tersebut terjadi lagi, maka perlu diketahui sejauh mana tata kelola sistem keamanan teknologi informasi perguruan tinggi dengan cara melakukan perbaikan, karena dengan adanya perbaikan dapat dihasilkan rekomendasi berupa tindakan-tindakan apa yang harus dilakukan agar hal-hal tersebut tidak terjadi lagi. Sehingga penelitian dilakukan untuk mengetahui Capability Level pada tata kelola sistem keamanan teknologi informasi STMIK Rosma dengan menggunakan framework COBIT 5.0 domain proses APO13 dan DSS05. Hasil penelitian menunjukan Capability Level pada domain proses APO13.01,02,03 dan DSS05.01,02,03,04,05,06,07, berada pada level 1, sedangkan Capability Level yang diinginkan pada kedua domain proses adalah level 2, sehingga terdapat gap sebesar 1. Setelah mengetahui Capability Level saat ini dan yang diinginkan dapat diberikan rekomendasi untuk perbaikan suatu system.

Kata kunci: keamanan, *framework* COBIT 5, evaluasi tata kelola, STMIK Rosma

Abstract

STMIK Rosma is a private tertiary institution that is established under the auspices of the Rosma Education Foundation domiciled in Karawang Regency. Currently the college has implemented information systems and technology to support the academic operations carried out by the IT Division. However, there are some deficiencies in the application, especially in terms of security such as security incidents. To prevent these things from happening again, it is necessary to know the extent of the governance of the university's information technology security system by evaluating, because with the evaluation recommendations can be generated in the form of what actions must be taken so that these things do not happen again . So the research was conducted to find out the Capability Level in the governance of the STMIK Rosma information technology security system using the COBIT 5 domain process APO13 and DSS05 domains. The results show that the Capability Level in the APO13.01, 02, 03 dan DSS05.01, 02, 03, 04, 05, 06, 07 process domains is at level 1, while the desired Capability Level in both process domains is level 2, leaving a gap of 1. After knowing the current Capability Level and the desired can be given recommendations for an improvement system.

Keywords*: security, COBIT 5 framework, governance evaluation, STMIK Rosma*

Pendahuluan

Teknologi Informasi (TI) menjadi salah satu kebutuhan yang sangat penting bagi suatu organisasi saat ini, karena dengan adanya teknologi informasi dapat membantu perusahaan dalam meningkatkan efisiensi dan efektifitas dari proses bisnis perusahaan itu sendiri, penerapan teknologi informasi diperlukan juga sebagai alat bantu dalam upaya memenangkan persaingan, tidak hanya dalam dunia bisnis, tetapi juga dalam dunia pendidikan perguruan tinggi.

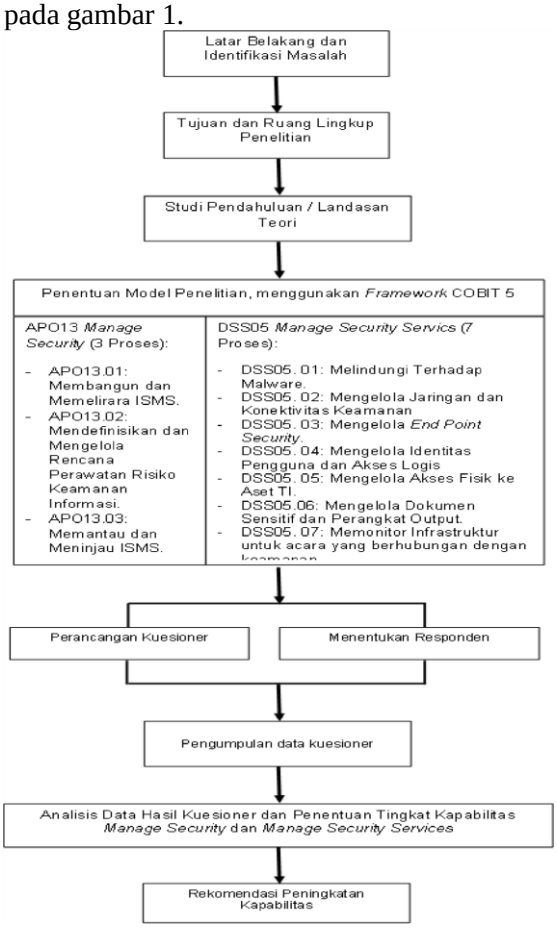
Perkembangannya, teknologi informasi yang dibangun dan dikelola masih dioperasikan secara terpisah oleh masing-masing unit fungsi organisasi. Salah satu tata kelola teknologi informasi yang dapat dilakukan adalah dengan pengelolaan keamanan informasi yang terbaik. Evaluasi bertujuan untuk mengatur penggunaan TI, dan memastikan kinerja TI sesuai dengan tujuan/fokus utama area tata kelola TI, dimana teknologi informasi perusahaan berkaitan dengan para *stakeholder* yang berharap perusahaan dapat memberikan solusi TI dengan kualitas yang bagus, tepat waktu, dan sesuai dengan anggaran, menguasai dan menggunakan TI untuk mendatangkan *value* serta menerapkan TI untuk meningkatkan keamanan dan produktifitas sambil menangani risiko TI. Sehingga penerapan TI di perguruan tinggi akan dapat dilakukan dengan baik dengan suatu pengelolaan TI (IT *Governance*) dari mulai perencanaan sampai dengan pengelolaan implementasinya.

Peneliti dalam kaitannya sebagai pihak yang meneliti di STMIK Rosma Karawang, melihat kebutuhan tersebut perlu dilakukan evaluasi terhadap pengelolaan keamanan informasi akademik dikarenakan terutama belum pernah dilakukan pengukuran keamanan informasi akademik menggunakan standar kerangka kerja (*framework*) COBIT 5.

Diharapkan kerangka kerja (*framework*) COBIT 5 ini dapat digunakan untuk membantu dalam tata kelola Teknologi Informasi yang sesuai standar, kebijakan dalam menjalankan operasi bisnis yang efektif dan efisien, serta memenuhi kebutuhan proses bisnis, maka dilakukanlah analisis dan evaluasi terhadap pengelolaan keamanan informasi akademik di lingkungan STMIK Rosma Karawang dengan menggunakan standar kerangka kerja (*framework*) COBIT 5.

Metodologi Penelitian

Berdasarkan masalah yang sedang diteliti dan tujuan yang hendak dicapai pada penelitian ini maka ditentukan tahapan-tahapan penelitian yang secara garis besar dapat dilihat pada gambar 1.



Gambar 1. Tahapan-Tahapan Penelitian

Keterangan gambar:

1. Latar Belakang dan Identifikasi Masalah, Tujuan Penelitian dan Ruang Lingkup Penelitian yang teridentifikasi.
2. Studi Pendahuluan/Landasan Teori dilakukan untuk mengumpulkan semua data dan informasi dari berbagai jurnal, buku, laporan, artikel, dan data internet

yang berhubungan dengan obyek penelitian.

3. Penentuan Model Penelitian ditentukan dengan menggunakan kerangka kerja COBIT 5 yang dikeluarkan oleh IT *Governance Institute and* ISACA.
4. Metode Penelitian dengan melakukan survey pada STMIK Rosma Karawang dengan menggunakan metode kueisoner. Perancangan kuesioner dilakukan dengan berpedoman pada Proses *Assessment* Model dan Capability Model COBIT 5.
5. Kueisoner berupa kueisoner untuk mengetahui tingkat kapabilitas tata kelola sistem informasi yaitu berupa pertanyaan dengan jawaban Ya dan Tidak dan akan dibagaikan kepada pihak-pihak yang terkait.
6. Pemilihan Responden dilakukan pada seluruh bagian yang terdapat didalam struktur organisasi. Responden yang dipilih dalam penelitian ini adalah orang-orang yang dianggap mengetahui dan memahami sistem informasi yang sedang dijalankan oleh perusahaan tersebut sesuai arahan RACI (*Resposible, Accountable, Consulted, Informed) chart*.
7. Pengumpulan Data yaitu berupa data kuesioner yang telah diisi oleh responden.
8. Selanjutnya data kuesioner diolah dengan menggunakan perangkat lunak *spreadsheet microsoft excel*, kemudian dibuat grafik pencapaian tingkat *capability* (kapabilitas).
9. Dari hasil olah data kuesioner kemudian dianalisis penyajian analisis data akan dilengkapi dengan tabel sebagai pendukung analisis data kuantitatif.
10. Dibuat laporan berupa laporan *assessment*, yang digunakan untuk melaporkan temuan dan rekomendasi usulan perancangan peningkatan tingkat kapabilitas pada manajemen.
11. Kesimpulan hasil penelitian dan saran.

Tinjauan Pustaka

Beberapa teori atau definisi yang berhubungan dengan penelitian ini diuraikan sesuai dengan metoda yang digunakan.

Sistem Informasi

Telah diketahui bahwa informasi merupakan hal yang sangat penting bagi manajemen organisasi di dalam pengambilan keputusan dan suatu Informasi dapat diperoleh dari sistem informasi (*Information Systems*), dan Pengambilan keputusan yang baik sangat ditentukan oleh digunakannya informasi yang baik. Informasi yang baik adalah informasi yang sesuai dengan kebutuhan untuk pengambilan keputusan tersebut, akurat, dan tersedia atau siap pada saat dibutuhkan.

Menurut Reynold and Stair (2010, 4) menjelaskan, bahwa "Sistem informasi adalah sekumpulan komponen yang saling berhubungan dimana komponen tersebut mengumpulkan, memanipulasi, menyimpan, dan menyebarkan data dan informasi serta menyediakan mekanisme timbal balik sedemikian rupa untuk memenuhi suatu tujuan".

Dari pendapat di atas maka dapat diambil kesimpulan bahwa, sistem informasi adalah sistem buatan manusia yang terdiri dari kombinasi teratur dari orangorang, hardware, software, jaringan komunikasi, prosedur dan sumber daya data secara teratur yang terintegrasi melakukan kegiatan mengumpulkan, memproses, menyimpan, menganalisa dan mendistribusikan informasi untuk menunjang dalam pengambilan keputusan, koordinasi dan pengawasan demi memenuhi tujuan organisasi.

Audit Sistem Informasi

Menurut pendapat Ron Weber (1999:10) dalam Evi Maria, 2011:

"*Information systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently*".

(Audit sistem informasi adalah proses mengumpulkan dan mengevalusi bukti untuk menentukan kemampuan sistem komputer dalam melindungi aset, merawat integritas data, mencapai tujuan organisasi dan menggunakan

sumber daya dengan efisien").

Tahapan Audit Sistem Informasi

Menurut Gllegos, dalam bukunya *Audit and Control of Information System (chapter* 10), tahapan audit sistem informasi yaitu:

1. Perencanaan (*Planning*)
2. Pemeriksaan Lapangan (*Fieldwork*)
3. Pelaporan (*Reporting*)
4. Tindak Lanjut (*Follow Up*)

Sedangkan menurut Menurut Ron Weber dalam bukunya "*Information System Control and Audit*" (1999:47-55), yang dikutip oleh Sanyoto Gondodiyoto dalam bukunya audit sistem informasi (2006:425-428), terdapat 5 (lima) langkah atau tahapan audit sistem informasi, yaitu:

1. Merencanakan Audit (*Planning the Audit*)
2. Menguji Pengendalian (*Test of Controls*)
3. Menguji Transaksi (*Test of Transactions*)
4. Menguji Keseimbangan atau Hasil
5. Mengakhiri (penyelesaian) Audit (*Completion of the Audit*)

   Pada fase akhir ini auditor akan menjalankan beberapa pengujian tambahan terhadap bukti autentik. Ada empat opini yang diberikan terhadap hasil audit oleh eksternal auditor yaitu:

   a) *Disclaimer of Opinion*: auditor tidak dapat memberikan opini.
   b) *Adverse Opinion*: auditor berpendapat bahawa banyak kesalahan.
   c) *Qualified Opinion*: auditor berpendapat terjadi beberapa kesalahan tetapi nilainya tidak material.
   d) *Unquaified Opinion*: auditor berpendapat tidak terjadi kesalahan atau misstatement.

Audit Keamanan Sistem Informasi

Di sisi lain kita juga mengenal istilah audit keamanan, adapun yang dimaksud dengan audit keamanan menurut Ahmad (2012:27), "audit keamanan adalah suatu proses atau kejadian "yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan semua keadaan dari perlindungan yang ada, dan untuk memverifikasi apakah perlindungan yang ada berjalan dengan baik".

Dari pengertian diatas dapat di garis bawahi bahwa audit keamanan tujuan utamanya adalah memberikan perlindungan sesuai dengan kebijakan dan standar keamanan yang ada serta memverifikasi apakah perlindungan sudah berjalan dengan baik. Oleh karena itu, suatu hal yang penting untuk memahami dan mengimplementasikan audit keamanan pada sistem informasi yang digunakan.

COBIT (Control Objective for Information and Related Technology)

COBIT adalah kerangka IT *governance* yang ditujukan kepada manajemen, staf pelayanan TI, *control departement*, fungsi audit dan lebih penting lagi bagi pemilik proses bisnis (*business process owners*), untuk memastikan *confidentiality, integrity* dan *availability* data serta informasi sensitif dan kritikal (Fransisikus). COBIT telah berkembang menjadi IT *Governance framework* yang paling signifikan dan juga cocok digunakan untuk audit karena COBIT menyediakan pedoman komprehensif di lingkungan proses-proses TI dan hubungannya dengan tujuan bisnis (Omari, 2012).

COBIT merupakan suatu cara untuk menerapkan IT Governance secara terstruktur, COBIT terdiri dari seperangkat *control objective* untuk bidang teknologi informasi (Campbell 2005). COBIT dikembangkan oleh IT Governance Institute (ITGI) yang merupakan bagian dari *Information Systems Audit and Control Association* (ISACA).

COBIT 5

COBIT 5 adalah kerangka bisnis untuk tata kelola dan manajemen perusahaan IT (IT governance framework), dan juga kumpulan alat yang mendukung para manajer untuk menjembatani jarak (gap) antara kebutuhan yang dikendalikan (*control requirements*), masalah teknis (*technical issues*) dan resiko bisnis (*business risk*). Menurut ISACA (2012:51), "COBIT 5 adalah sebuah kerangka kerja untuk tata kelola dan manajemen

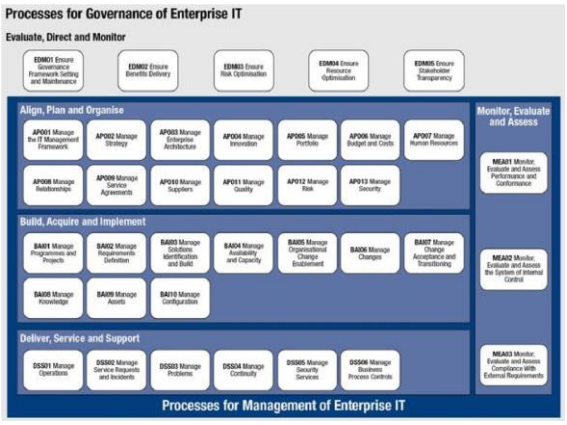
teknologi informasi dan semua yang berhubungan, yang dimulai dari memenuhi kebutuhan *stakeholder* akan informasi dan teknologi".

COBIT 5 memiliki 5 domain yang terbagi dalam domain *governance* dan *management*, masing- masing domain memiliki proses yang memungkinkan untuk mencapai tujuannya (ISACA, 2012). Satu domain berasal dari *governance* dan empat lainnya berasal dari management. Domain pada COBIT 5 yang terdiri dari 5 (lima) domain dan 37 proses tata kelola IT adalah evolusi dari struktur proses COBIT 4.1. Nama domain dipilih sejalan dengan penandaaan area utama, tetapi lebih menggambarkan kata kerja seperti tergambar pada gambar 1 untuk tata kelola *governence* dan *managemen*t.

COBIT 5 memiliki 5 (lima) domain untuk manajemen dan tata kelola IT yaitu:

a) EDM (*Evaluate, Direct and Monitor*) terdiri dari 5 proses.
b) APO (*Align, Plan and Organize*) terdiri dari 13 proses.
c) BAI (*Build, Aquire and Implement*) terdiri dari 10 proses.
d) DSS (*Deliver, Service and Support*) terdiri dari 6 proses.
e) MEA (*Monitor, Evaluate adn Access*) terdiri dari 3.

COBIT 5 terdiri dari 5 domain dan 37 proses tatakelola dan proses manajemen.



Gambar 1. Proses Tata Kelola dalam Cobit 5.0

Hasil dan Pembahasan

Analisis APO13 (Manage Security)

COBIT 5 mendefinisikan APO13 memiliki 3 proses, antara lain: APO13.01 Membangun dan Memelihara ISMS, APO13.02 Mendefinisikan dan Mengelola Rencana Perawatan Risiko Keamanan Informasi dan APO13.03 Memantau dan Meninjau ISMS. Pengukuran dari APO13 dihasilkan dari pengisian kuesioner yang disebarkan kepada responden berdasarkan *Base Practice* (BPs) dan *Work Products* (WPs) dari masing-masing proses tersebut.

Analisis APO13.01 Membangun dan Memelihara ISMS

Untuk aktifitas Membangun dan Memelihara ISMS (APO13.01):

1. Menentukan ruang lingkup dan batasan ISMS dalam hal karakteristik perusahaan, organisasi, lokasi, aset dan teknologi.
2. Mendefinisikan ISMS yang sesuai dengan kebijakan enterprise dan sejalan dengan enterprise, organisasi, lokasi, aset dan teknologi.
3. Menyelaraskan ISMS dengan pendekatan enterprise secara keseluruhan terhadap manajemen keamanan
4. Memperoleh autorisasi manajemen untuk mengimplementasikan dan mengoperasikan serta mengubah ISMS.
5. Menyiapkan dan memelihara penerapan pernyataan yang menggambarkan ruang lingkup ISMS.
6. Mendefinisikan dan mengkomunikasikan peran serta tanggung jawab manajemen keamanan informasi
7. Mengkomunikasikan pendekatan ISMS

Analisis DSS05 (Manage Security Services)

COBIT 5 mendefinisikan DSS05 memiliki 7 proses, antara lain : DSS05.01 Melindungi terhadap *malware*, DSS05.02 Mengelola jaringan dan keamanan konektivitas, DSS05.03 Mengelola keamanan endpoint, DSS05.04 Mengelola identitas pengguna dan akses logis, DSS05.05 Mengelola akses fisik ke aset TI, DSS05.06 Mengelola perangkat sensitif dan output, dan DSS05.07 Memonitor infrastruktur untuk acara yang berhubungan dengan keamanan.

Pengukuran dari DSS05 dihasilkan dari pengisian kuesioner yang disebarkan kepada responden berdasarkan *Base Practice* (BPs) dan Work Products (WPs) dari masing-masing proses tersebut.

Analisis DSS05.01 Melindungi Terhadap Malware

Aktifitas Memantau dan Meninjau ISMS (DSS05.01)

1. Sadar berkomunikasi dengan perangkat lunak berbahaya dan menegakkan prosedur dan tanggung jawab pencegahan.
2. Menginstal dan alat perlindungan aktif perangkat lunak berbahaya di semua fasilitas pengolahan, dengan berbahaya file definisi perangkat lunak yang diperbarui seperti yang diperlukan (otomatis atau semi-otomatis).
3. Mendistribusikan semua perangkat lunak perlindungan terpusat (versi dan patchlevel) menggunakan konfigurasi terpusat dan manajemen perubahan.
4. Secara teratur meninjau dan mengevaluasi informasi ancaman baru yang berpotensi menyerang sistem (misalnya, meninjau produk vendor dan petunjuk keamanan layanan).
5. Filter lalu lintas masuk, seperti email dan download, untuk melindungi informasi yang tidak diminta (misalnya, spyware, phishing email).
6. Melakukan pelatihan berkala tentang malware di email dan internet penggunaan. pengguna untuk tidak menginstal bersama atau software yang tidak disetujui.

Analisis DSS05.02 Mengelola Jaringan Dan Keamanan Konektivitas Aktifitas Memantau dan Meninjau ISMS (DSS05.02)

1. Membangun dan mempertahankan kebijakan untuk keamanan konektivitas. Berdasarkan penilaian risiko dan kebutuhan bisnis.
2. Memungkinkan hanya yang berwenang perangkat untuk memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasi perangkat ini mengharuskan masuk menggunakan password.
3. Menerapkan mekanisme penyaringan jaringan, seperti *firewall* dan perangkat lunak intrusion detection, dengan kebijakan yang tepat untuk mengendalikan lalu lintas inbound dan outbound.
4. Mengenkripsi transit Informasi menurut klasifikasinya.
5. Menerapkan protokol keamanan disetujui pada konektivitas jaringan.
6. Mengkonfigurasi peralatan jaringan dengan cara yang aman
7. Membangun mekanisme terpercaya untuk mendukung transmisi penerimaan informasi yang aman.
8. Melaksanakan pengujian penetrasi secara periodik untuk menentukan kecukupan perlindungan jaringan.
9. Melaksanakan pengujian berkala dari sistem keamanan untuk menentukan kecukupan perlindungan sistem.

Hasil Pengukuran Tingkat Capability Level 1

Hasil Pengukuran Tingkat Capability Pada APO13 (Manage Security)

Hasil penelitian didapatkan dari pemberian kuesioner terhadap 11 (Orang) responden yang kemudian dilakukan analisis dan perhitungan sebagai dasar untuk pembuatan rekomendasi. Untuk kepentingan pemetaan tingkat Kapabilitas *Manage Security* (APO13) jumlah responden yang diminta pendapatnya mengenai hal-hal yang berkaitan dengan Tata Kelola IT khususnya Proses IT APO13 (Manage Security) sebanyak 11 orang responden, dimana selama pengisian kuesioner tersebut peneliti mendampingi responden, untuk menjawab pertanyaan yang mungkin muncul dari para responden yang diberikan kuesioner dan diberikan juga penjelasan dengan tujuan untuk menjamin keakuratan pengisian terutama pada perbedaan persepsi responden terhadap keadaan yang sesungguhnya dengan yang diinginkan. Berdasarkan hasil isian kuesioner tersebut kemudian dapat dihitung tingkat kapabilitas untuk setiap sub domain berdasarkan *governance/management practice* dan output yang dihasilkan. Isian Y bernilai 1 dan T bernilai 0. Untuk memudahkan perhitungan maka isian dari masing-masing responden dimasukan ke dalam *template* yang telah disediakan berikut ini:

Tabel 1. *Template* Kuesioner APO13 *Manage Security*

Kode	Proses	Base Practices				Work Products			
		Dilakukan	Tidak	Jumlah	%	Dihasilkan	Tidak	Jumlah	%
APO13.01	Membangun dan Memelihara ISMS								
APO13.02	Mendefinisikan dan Mengelola Rencana Perawatan Risiko Keamanan Informasi.								
APO13.03	Memantau dan Meninjau ISMS								
	Total								

Rekapitulasi dari keseluruhan responden kemudian dimasukan dalam tabel 2.

Tabel 2. *Template* Rekapitulasi Data Kuesioner

Kode	Proses	Base Practices				Work Products				Skala (%)	Pencapaian
		Dilakukan	Tidak	Jumlah	%	Dihasilkan	Tidak	Jumlah	%		
APO13.01	Membangun dan Memelihara ISMS										
APO13.02	Mendefinisikan dan Mengelola Rencana Perawatan Risiko Keamanan Informasi.										
APO13.03	Memantau dan Meninjau ISMS										
	Total										

Hasil Pengukuran Tingkat Capability Level 1 Pada DSS05 (Manage Security Services)

Hasil penelitian didapatkan dari pemberian kuesioner terhadap 11 (Orang) responden yang kemudian dilakukan analisis dan perhitungan sebagai dasar untuk pembuatan rekomendasi. Untuk kepentingan pemetaan tingkat Kapabilitas Manage Security Services (DSS05) jumlah responden yang diminta pendapatnya mengenai halhal yang berkaitan dengan Tata Kelola IT khususnya Proses IT DSS05 (Manage Security Services) sebanyak 11 orang responden, dimana selama pengisian kuesioner tersebut peneliti mendampingi responden, untuk menjawab pertanyaan yang mungkin muncul dari para responden yang diberikan kuesioner dan diberikan juga penjelasan dengan tujuan untuk menjamin keakuratan pengisian terutama pada perbedaan persepsi responden terhadap keadaan yang sesungguhnya dengan yang diinginkan. Berdasarkan hasil isian kuesioner tersebut kemudian dapat dihitung tingkat kapabilitas untuk setiap sub domain berdasarkan governance/management practice dan output yang dihasilkan. Isian Y bernilai 1 dan T bernilai 0. Untuk memudahkan perhitungan maka isian dari masing-masing responden dimasukan ke dalam template yang telah disediakan berikut ini:

Tabel 3. Template Kuesioner DSS05 *Manage SecurityServices*

Kode	Proses	Base Practices				Work Products			
		Dilakukan	Tidak	Jumlah	%	Dihasilkan	Tidak	Jumlah	%
DSS05.01	Melindungi terhadap *malware*.								
DSS05.02	Mengelola jaringan dan keamanan konektivitas.								
DSS05.03	Mengelola keamanan *endpoint*.								
DSS05.04	Mengelola identitas pengguna dan akses logis.								
DSS05.05	Mengelola akses fisik ke aset TI.								
DSS05.06	Mengelola perangkat sensitif dan *output*								
DSS05.07	Memonitor infrastruktur untuk acara yang berhubungan dengan keamanan								
	Total								

Rekapitulasi dari keseluruhan responden kemudian dimasukan dalam tabel 4.

Tabel 4. Template Rekapitulasi Data Kuesioner

Kode	Proses	Base Practices				Work Products				Skala (%)	Pencapaian
		Dilakukan	Tidak	Jumlah	%	Dihasilkan	Tidak	Jumlah	%		
DSS05.01	Melindungi terhadap *malware*.										
DSS05.02	Mengelola jaringan dan keamanan konektivitas.										
DSS05.03	Mengelola keamanan *endpoint*.										
DSS05.04	Mengelola identitas pengguna dan akses logis.										
DSS05.05	Mengelola akses fisik ke aset TI.										
DSS05.06	Mengelola perangkat sensitif dan *output*										
DSS05.07	Memonitor infrastruktur untuk acara yang berhubungan dengan keamanan										
	Total										

Tabel Skala (%) diperoleh dari rata-rata prosentase Base Practices dan Work Products untuk masing-masing proses. Tabel 5 menunjukan tingkat pencapaian level atau tingkat kapabilitas dari setiap proses yang diperoleh.

Tabel 5. Tabel Pencapaian Tingkat Kapabilitas

Kode	Level	Pencapaian
N	*Not Achieved*	0 % - 15 %
P	*Partially Achieved*	16 % - 50 %
L	*Largely Achieved*	51 % - 85 %
F	*Fully Achieved*	86 - 100 %

Hasil Pengukuran APO13.01 Membangun dan Memelihara ISMS

Hasil pengolahan kuisioner APO 13.01 Membangun dan Memelihara ISMS di STMIK Rosma Karawang dari 11 responden seperti pada tabel 6.

Tabel 6. Hasil Pengukuran APO 13.01 Membangun dan Memelihara ISMS

Administrasi APO13.01 : Membangun dan Memelirara ISMS																
Base Practies (*BPs*)																
Pertanyaan	Divisi IT											Dilakukan	Tidak	Prosentase	Rata Rata	Skala %
	1	2	3	4	5	6	7	8	9	10	11					
1	1	0	1	1	1	0	1	1	0	0	1	7	4	64%	62%	72%
2	1	0	0	1	1	0	1	1	0	0	1	6	5	55%		
3	1	0	0	1	1	0	0	1	0	0	1	5	6	45%		
4	1	0	1	1	0	1	1	1	1	0	1	8	3	73%		
5	1	0	0	1	0	0	1	1	0	1	1	6	5	55%		
6	1	0	1	1	1	1	1	1	1	1	1	10	1	91%		
7	1	0	0	1	1	0	1	1	0	0	1	6	5	55%		
Jumlah	7	0	3	7	5	2	6	7	2	2	7	48	29	62%		
Work Products (*WPs*)																
1	1	1	1	1	1	1	1	1	1	0	1	10	1	91%	82%	
2	1	1	0	1	0	0	1	1	1	1	1	8	3	73%		
Jumlah	2	2	1	2	1	1	2	2	2	1	2	18	4	82%		

Banyaknya *Base Practices* pada Proses APO13.01 Membangun dan memelihara ISMS adalah sebesar 62% sedangkan banyaknya Work Products pada proses APO13.01 Membangun dan memelihara ISMS adalah sebesar 82%, sehingga rata-ratanya adalah sebesar 72%. Hal ini menunjukkan bahwa proses APO13.01 menunjukkan hasil pencapaian pada rating L (Largely Achieved) yang artinya Ada bukti dari pendekatan sistematis, dan pencapaian signifikan, atribut didefinisikan dalam penilaian proses.

Tabel 7 menunjukan pengolahan kuesioner APO13 dalam bentuk prosentase:

Tabel 7. Hasil Pengolahan Quesioner Capability APO13.01 Membangun dan memelihara ISMS

APO13.01 : Membangun dan memelihara ISMS		Nilai
Base Practices (BPs): Deskripsi Aktivitas		%
1	Menentukan ruang lingkup dan batasan ISMS dalam hal karakteristik perusahaan, organisasi, lokasi, aset dan teknologi.	64%
2	Mendefinisikan ISMS yang sesuai dengan kebijakan enterprise dan sejalan dengan enterprise, organisasi, lokasi, aset dan teknologi.	55%
3	Menyelaraskan ISMS dengan pendekatan enterprise secara keseluruhan terhadap manajemen keamanan	45%
4	Memperoleh autorisasi manajemen untuk mengimplementasikan dan mengoperasikan serta mengubah ISMS.	73%
5	Menyiapkan dan memelihara penerapan pernyataan yang menggambarkan ruang lingkup ISMS.	55%
6	Mendefinisikan dan mengkomunikasikan peran serta tanggung jawab manajemen keamanan informasi	91%
7	Mengkomunikasikan pendekatan ISMS	55%
Work Products (*WPs*)		Nilai
1	Kebijakan ISMS (Information Security Management System)	91%
2	Scope / ruang lingkup ISMS	73%

Hasil Pengukuran DSS05.01 Melindungi Terhadap Malware

Tabel 7 menunjukan hasil kuisioner DSS05.01 Melindungi Terhadap *Malware* di STMIK Rosma Karawang dari 11 responden pada tabel 8 menunjukan perolehan hasil pencapaian level.

Tabel 8. Hasil Pengukuran DSS05.01 Melindungi Terhadap Malware

Administrasi DSS05.01 Melindungi Terhadap Malware																
Base Practies (*BPs*)																
Pertanyaan	Divisi IT											Dilakukan	Tidak	Prosentase	Rata Rata	Skala %
	1	2	3	4	5	6	7	8	9	10	11					
1	1	1	1	1	1	1	1	1	1	1	1	11	0	100%	55%	59%
2	1	1	0	1	0	1	1	1	1	1	1	9	2	82%		
3	1	0	0	0	0	0	1	0	0	0	0	2	9	18%		
4	1	0	0	1	0	1	1	0	1	0	1	6	5	55%		
5	1	0	0	0	0	1	1	1	1	0	1	6	5	55%		
6	0	0	0	0	0	0	1	1	0	0	0	2	9	18%		
Jumlah	5	2	1	3	1	4	6	4	4	2	4	36	30	55%		
Work Products (*WPs*)																
1	1	0	0	1	1	1	0	0	0	1	1	6	5	55%	64%	
2	1	1	0	1	1	1	0	1	1	0	1	8	3	73%		
Jumlah	2	1	0	2	2	2	0	1	1	1	2	14	8	64%		

Banyaknya *Base Practices* pada Proses DSS05.01 Melindungi Terhadap Malware adalah sebesar 55% sedangkan banyaknya *Work Products* pada proses DSS05.01 Melindungi Terhadap Malware adalah sebesar 64%, sehingga rata-ratanya adalah sebesar 59%. Hal ini menunjukkan bahwa proses DSS05.01 menunjukkan hasil pencapaian pada rating L (*Largely Achieved*) yang artinya Ada bukti dari pendekatan sistematis, dan pencapaian signifikan, atribut didefinisikan dalam penilaian proses. Beberapa kelemahan yang berkaitan dengan atribut ini mungkin ada dalam penilaian proses (pencapaian 51-85 persen). Tabel 8 menunjukan pengolahan kuesioner DSS05.01 dalam bentuk prosentase:

Tabel 8. Hasil Pengolahan Quesioner Capability DSS05.01 Melindungi Terhadap Malware

DSS05.01 Melindungi Terhadap Malware		Nilai
Base Practices (*BPs*): Deskripsi Aktivitas		%
1	Sadar berkomunikasi dengan perangkat lunak berbahaya dan menegakkan prosedur dan tanggung jawab pencegahan.	100%
2	Menginstal dan alat perlindungan aktif perangkat lunak berbahaya di semua fasilitas pengolahan, dengan berbahaya file definisi perangkat lunak yang diperbarui seperti yang diperlukan (otomatis atau semiotomatis).	82%
3	Mendistribusikan semua perangkat lunak perlindungan terpusat (versi dan patch-level) menggunakan konfigurasi terpusat dan manajemen perubahan.	18%
4	Secara teratur meninjau dan mengevaluasi informasi ancaman baru yang berpotensi menyerang sistem (misalnya, meninjau produk vendor dan petunjuk keamanan layanan).	55%
DSS05.01 Melindungi Terhadap Malware		Nilai
Base Practices (*BPs*): Deskripsi Aktivitas		%
5	Filter lalu lintas masuk, seperti email dan download, untuk melindungi informasi yang tidak diminta (misalnya, spyware, phishing email).	55%
6	Melakukan pelatihan berkala tentang malware di email dan internet penggunaan. pengguna untuk tidak menginstal bersama atau software yang tidak disetujui.	18%
Work Products (*WPs*)		Nilai
1	Kebijakan pencegahan perangkat lunak berbahaya	55%
2	Evaluasi potensi ancaman	73%

Hasil Pengukuran DSS05.02 Mengelola Jaringan dan Keamanan Konektivitas

Tabel 9 menunjukan hasil kuisioner DSS05.02 Mengelola Jaringan dan Keamanan Konektivitas di STMIK Rosma Karawang dari 11 responden pada tabel 9. menunjukan perolehan hasil pencapaian level.

Tabel 9. Hasil Pengukuran DSS05.02 Mengelola Jaringan dan Keamanan Konektivitas.

Administrasi DSS05.02 Mengelola Jaringan Dan Keamanan Konektivitas																
***Base Practies* (*BPs*)**																
Pertanyaan	**Divisi IT**											Dilakukan	Tidak	Prosentase	Rata-Rata	Skala %
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**					
1	1	1	1	1	0	1	0	1	1	1	1	9	2	82%	71%	67%
2	1	1	1	1	0	1	1	1	1	1	1	10	1	91%		
3	1	1	0	1	0	1	1	1	1	1	1	9	2	82%		
4	0	1	0	0	0	0	1	1	0	0	1	4	7	36%		
5	1	1	0	0	0	1	1	1	1	0	1	7	4	64%		
6	1	1	1	1	0	0	1	1	1	0	1	8	3	73%		
7	1	1	0	1	1	1	1	1	1	0	1	9	2	82%		
8	1	0	1	0	1	0	0	0	0	1	1	5	6	45%		
9	1	0	1	1	1	0	1	1	1	1	1	9	2	82%		
Jumlah	8	7	5	6	3	5	7	8	7	5	9	70	29	71%		
***Work Products* (*WPs*)**																
1	1	1	1	0	1	0	0	1	1	1	1	8	3	73%	64%	
2	1	0	1	0	1	0	0	1	0	1	1	6	5	55%		
Jumlah	2	1	2	0	2	0	0	2	1	2	2	14	8	64%		

Banyaknya Base Practices pada Proses DSS05.02 Mengelola Jaringan Dan Keamanan Konektivitas adalah sebesar 71% sedangkan banyaknya *Work Products* pada proses DSS05.02 Mengelola Jaringan Dan Keamanan Konektivitas adalah sebesar 64%, sehingga rata-ratanya adalah sebesar 67%. Hal ini menunjukkan bahwa proses DSS05.02 menunjukkan hasil pencapaian pada rating L (*Largely Achieved*) yang artinya Ada bukti dari pendekatan sistematis, dan pencapaian signifikan, atribut didefinisikan dalam penilaian proses.

Beberapa kelemahan yang berkaitan dengan atribut ini mungkin ada dalam penilaian proses (pencapaian 51-85 persen). Tabel 10 menunjukan pengolahan kuesioner DSS05.02 dalam bentuk prosentase:

Tabel 10 Hasil Pengolahan *Quesioner Capability* DSS05.02 Mengelola Jaringan Dan Keamanan Konektivitas

DSS05.02 Mengelola Jaringan Dan Keamanan Konektivitas		**Nilai**
***Base Practices* (*BPs*): Deskripsi Aktivitas**		**%**
1	Membangun dan mempertahankan kebijakan untuk keamanan konektivitas. Berdasarkan penilaian risiko dan kebutuhan bisnis.	82%
2	Memungkinkan hanya yang berwenang perangkat untuk memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasi perangkat ini mengharuskan masuk menggunakan password.	91%
3	Menerapkan mekanisme penyaringan jaringan, seperti firewall dan perangkat lunak intrusion detection, dengan kebijakan yang tepat untuk mengendalikan lalu lintas inbound dan outbound.	82%
4	Mengenkripsi transit Informasi menurut klasifikasinya.	36%
5	Menerapkan protokol keamanan disetujui pada konektivitas jaringan.	64%
6	Mengkonfigurasi peralatan jaringan dengan cara yang aman	73%
7	Membangun mekanisme terpercaya untuk mendukung transmisi penerimaan informasi yang aman.	82%
8	Melaksanakan pengujian penetrasi secara periodik untuk menentukan kecukupan perlindungan jaringan.	45%
9	Melaksanakan pengujian berkala dari sistem keamanan untuk menentukan kecukupan perlindungan sistem.	82%
***Work Products* (*WPs*)**		**Nilai**
1	Kebijakan keamanan konektivitas	73%
2	Hasil uji penetrasi	55%

Hasil Rekapitulasi Pengolahan Quesioner Capability Level 1 APO13 Manage Security

Berikut hasil olah data dari kuesioner berdasarkan hasil isian kuesioner berdasarkan Best Practice dan Work Product yang dihasilkan. Isian Ya bernilai 1 dan Tidak bernilai 0.

Skala *Best Practice* dan *Work Product* dihitung dengan rumus berikut:

Berikut hasil olah data dari kuesioner dari 11 (Sebelas) responden, yang ditampikan dalam bentuk tabel berikut ini:

Tabel 11. Hasil rekapitulasi pengolahan Quesioner Capability APO 13 Manage Security

Kode	Proses	Base Practices				Work Products			
		Dilakukan	Tidak Dilakukan	Jumlah	%	Ada	Tidak Ada	Jumlah	%
APO13.01	Membangun dan Memelihara ISMS	48	29	77	62%	18	4	22	82%
APO13.02	Mendefinisikan dan Mengelola Rencana Perawatan Risiko Keamanan Informasi.	44	33	77	57%	14	8	22	64%
APO13.03	Memantau dan Meninjau ISMS	28	27	55	51%	17	17	34	50%
	Total	120	89	209	57%	49	29	78	63%

Prosentase didapat dari hitungan sebagai berikut:

(Aktivitas bernilai 1 / jumlah aktivitas)*100%, dari nilai yang dihasilkan ada pembulatan. Selanjutya dari rekapitulasi dari keseluruhan responden yang mengisi kuesioner kemudian dimasukan dalam tabel rekapitulasi berikut ini,

untuk dapat menentukan nilai skala yang ada, skala diperoleh dari rata-rata persentase aktivitas dan output.

Tabel 12. Rekapitulasi Hasil Kuesioner

Kode	Proses	Base Practices				Work Products				Skala(%)	Pencapaian
		Dilakukan	Tidak	Jumlah	%	Ada	Tidak	Jumlah	%		
APO13.01	Membangun dan Memelihara ISMS	48	29	77	62%	18	4	22	82%	72%	*Largely Achieved*
APO13.02	Mendefinisikan dan Mengelola Rencana Perawatan Risiko Keamanan Informasi.	44	33	77	57%	14	8	22	64%	60%	*Largely Achieved*
APO13.03	Memantau dan Meninjau ISMS	28	27	55	51%	17	17	34	50%	37%	*Partially Achieved*
Total		120	89	209	57%	49	29	78	63%	56%	*Largely Achieved*

Dari rekapitulasi APO 13.1 terlihat bahwa pencapaian pada level L (Largely achieved) yang artinya proses audit berada pada level 1 dan tidak dapat dilanjutkan ke tahap level 2, Ada bukti dari pendekatan yang sistematis, pencapaian signifikan, atribut yang didefinisikan dalam proses dinilai.

Beberapa kelemahan yang berkaitan dengan atribut ini mungkin ada dalam proses yang dinilai.

Hasil Rekapitulasi Pengolahan Quesioner Capability Level 1 DSS05 Manage Security Services

Berikut hasil olah data dari kuesioner berdasarkan hasil isian kuesioner berdasarkan *Best Practice* dan *Work Product* yang dihasilkan. Isian Ya bernilai 1 dan Tidak bernilai 0.

Skala *Best Practice* dan *Work Product* dihitung dengan rumus berikut:

Berikut hasil olah data dari kuesioner dari 11 (Sebelas) responden, yang ditampikan dalam bentuk tabel 13 berikut ini.

Tabel 13. Hasil rekapitulasi pengolahan Quesioner Capability DSS05 Manage Security Services

Kode	Proses	Base Practices				Work Products			
		Dilakukan	Tidak	Jumlah	%	Ada	Tidak	Jumlah	%
DSS05.01	Melindungi Terhadap Malware	36	30	66	55%	14	8	22	64%
DSS05.02	Mengelola Jaringan Dan Keamanan Konektivitas	70	29	99	71%	14	8	22	64%
DSS05.03	Mengelola Keamanan Endpoint	64	35	99	65%	7	4	11	64%
DSS05.04	Mengelola Identitas Pengguna dan Akses Logis	60	28	88	68%	14	8	22	64%
DSS05.05	Mengelola Akses Fisik ke Aset TI	38	39	77	49%	17	5	22	77%
DSS05.06	Mengelola Perangkat Sensitif dan Output	27	28	55	49%	12	10	22	55%
DSS05.07	Memonitor Infrastruktur Untuk Acara yang Berhubungan Dengan Keamanan	26	29	55	47%	19	14	33	58%
Total		321	218	539	60%	97	57	154	63%

Prosentase didapat dari hitungan sebagai berikut:

= (Aktivitas bernilai 1 / jumlah aktivitas)*100%, dari nilai yang dihasilkan ada pembulatan. Selanjutya hasil rekapitulasi dari keseluruhan responden yang mengisi kuesioner kemudian dimasukan dalam tabel rekapitulasi berikut ini, untuk dapat menentukan nilai skala yang ada, skala diperoleh dari rata-rata persentase aktivitas dan output.

Tabel 14. Rekapitulasi Hasil Kuesioner

Kode	Proses	Base Practices				Work Products				Skala	Pencapaian
		Dilakukan	Tidak Dilakukan	Jumlah	%	Ada	Tidak	Jumlah	%		
DSS05.01	Melindungi Terhadap Malware	36	30	66	55%	14	8	22	64%	59%	*Largely Achieved*
DSS05.02	Mengelola Jaringan Dan Keamanan Konektivitas	70	29	99	71%	14	8	22	64%	67%	*Largely Achieved*
DSS05.03	Mengelola Keamanan Endpoint	64	35	99	65%	7	4	11	64%	64%	*Largely Achieved*
DSS05.04	Mengelola Identitas Pengguna dan Akses Logis	60	28	88	68%	14	8	22	64%	66%	*Largely Achieved*
DSS05.05	Mengelola Akses Fisik ke Aset TI	38	39	77	49%	17	5	22	77%	63%	*Largely Achieved*
DSS05.06	Mengelola Perangkat Sensitif dan Output	27	28	55	49%	12	10	22	55%	52%	*Largely Achieved*
DSS05.07	Memonitor Infrastruktur Untuk Acara yang Berhubungan Dengan Keamanan	26	29	55	47%	19	14	33	58%	52%	*Largely Achieved*
Total		321	218	539	60%	97	57	154	63%	61%	*Largely Achieved*

Dari rekapitulasi DSS05.01, DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06, DSS05.07 terlihat bahwa pencapaian pada level L (*Largely achieved*) yang artinya proses audit

berada pada level 1 dan tidak dapat dilanjutkan ke tahap level 2, Ada bukti dari pendekatan yang sistematis, pencapaian signifikan, atribut yang didefinisikan dalam proses dinilai. Beberapa kelemahan yang berkaitan dengan atribut ini mungkin ada dalam proses yang dinilai.

Kesimpulan Dan Saran

Kesimpulan

Beberapa hal dapat disimpulkan sebagai hasil dari penelitian yang dilakukan pada Yayasan Pendidikan Rosma (Yaperos) berdasarkan audit sistem informasi berbasis web menggunakan COBIT 5.0 :

1. Hasil penilaian terhadap capability di STMIK Rosma Karawang untuk APO13.01 Membangun dan Memelihara ISMS, adalah sebesar 72% atau L (Largely Achieved) artinya ada bukti dari pendekatan yang sistematis, pencapaian signifikan, atribut yang didefinisikan dalam proses dinilai.
2. Hasil penilaian terhadap capability di STMIK Rosma Karawang untuk DSS05.01 Melindungi Terhadap Malware, adalah sebesar 59% atau L (Largely Achieved) artinya ada bukti dari pendekatan yang sistematis, pencapaian signifikan, atribut yang didefinisikan dalam proses dinilai.

Saran

Dari penelitian yang dilakukan di STMIK Rosma Karawang maka saran dari hasil kajian dapat dikemukakan sebagai berikut:

a. Mempertahankan dan menegakkan pendekatan standar Cobit APO13 *Manage Security* dan DSS05 *Manage Security Services* untuk program dan manajemen project disesuaikan dengan lingkungan spesifik perusahaan dan dengan praktek yang baik berdasarkan pada proses yang telah didefinisikan dan penggunaan teknologi yang tepat guna.
b. Rekomendasi perbaikan tata kelola sebelum diarahkan menuju tingkat kapabilitas F (*Fully Achieved*), sebaiknya maksimalkan terlebih dahulu untuk menuju tingkat kapabilitas L (*Largely Achieved*) yang dilakukan pada proses-proses yang mempunyai nilai tingkat kapabiltas saat ini yang kecil dengan membuat prosedur standar, mendokumentasikan dan mengkomunikasikan melalui pelatihan. Tetapi pelaksanaannya diserahkan pada individu untuk mengikuti proses tersebut, sehingga tidak akan ada penyimpangan pada pelaksanaannya.

Daftar Pustaka

Abdul Hakim, Hoga Saragih, Agus Suharto, 2014. "Evaluasi Tata Kelola Teknologi Informasi Dengan *Framework* Cobit. 5 Di Kementerian ESDM", *Journal of Information Systems*, Volume 10, Issue 2

Ana Ranitania, 2015. "Analisis Tata Kelola Proses Layanan Keamanan Informasi Penyedia Barang/Jasa (DSS05) Dalam Kegiatan *E-Procurement* Pada LPSE Provinsi Jawa Tengah Berdasarkan Kerangka Kerja COBIT 5"

Christina Juliane, dkk, 2014. "Pengukuran Kinerja Sistem Informasi Di PT. Rancek Sukses Bandung Dengan Menggunakan Framework COBIT 5.0 (Studi Kasus Sios-Sistem Informasi Kios)"

Desepta Isna Ulumi, dkk, 2015. "Audit TeNOSS Menggunakan COBIT 5 pada *Domain Deliver, Service and Support* (DSS)"

Evi Maria and Endang Haryani, 2011. "Audit Model Development Of Academic Information System: Case Study On Academic Information System Of Satya Wacana", *Journal of Arts, Science & Commerce*, E- Vol.– II, Issue –2,April 2011, ISSN 2229-4686, ISSN 2231-4172.

Gelinas, Jr., Ulric J., Dull, Richard B., 2012. "*Accounting Information System*", 9th Edition. Canada: South Western Cengage Learning. Gondodiyoto, Sanyoto. & Hendarti, Henny., 2006. "Audit Sistem Informasi". Mitra Wacana Media, Jakarta. Laudon, Kenneth C. dan Laudon, Jane P, 2008. "Sistem Informasi Manajemen". Terjemahan Chriswan Sungkono dan Machmudin Eka P. Edisi 10. Jakarta: Salemba Empat.

ISACA (*Information System Audit and Control Association)*, 2012. "COBIT 5 A *Business Framework for the Governance and Management of Enterprise*".

ISACA (*Information System Audit and Control Association), 2012. "COBIT 5 Enabling Processes*".

ISACA (*Information System Audit and Control Association), 2012. "COBIT 5 Framework*".

ITGI, 2012. "Cobit 5 : *Enabling Process". United States America Omari, Al, dkk, 2012. "Optimising COBIT 5 for IT Governance". Queensland University of Technology.*

Rahmat, 2105. "*Audit Control Capability Level* Tata Kelola Sistem Informasi Menggunakan COBIT 5", Jurnal Informasi, Volume VII No.2.