

IMPLEMENTASI DOMAIN *DELIVER, SERVICE AND SUPPORT* (DSS05) BERDASARKAN COBIT 5 SEBAGAI UPAYA PROTEKSI ASET INFORMASI PADA PT ASTRAGRAPHIA TBK

Aida Miladina Mayasari¹, Yupie Kusumawati²

Mahasiswa Universitas Dian Nuswantoro Semarang¹, Dosen Universitas Dian Nuswantoro Semarang²

^{1,2}Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang

Jl. Nakula I, No. 5-11, Semarang, Kode Pos 50131, Telp. (024) 3515261, 3520165 Fax: 3569684

E-mail : 112201104289@mhs.dinus.ac.id¹, yupie@dsn.dinus.ac.id²

Abstrak

Sistem informasi dapat diakses dimanapun, kapanpun dan terkadang suatu instansi atau organisasi mempunyai sistem informasi sendiri (*office automation*). Pada penelitian ini bentuk *office automation* pada PT. Astragraphia Tbk yaitu Docushare. Docushare memiliki tingkat keamanan sistem yang masih kurang, hal ini memungkinkan terjadinya penyalahgunaan. Docushare merupakan sistem yang terintegrasi, berfungsi untuk mengakses informasi yang berkaitan dengan fasilitas kompensasi karyawan bisa dilakukan diberbagai cabang maupun depo PT. Astragraphia Tbk. Terdapat permasalahan yang terjadi pada sistem Docushare yaitu sistem tidak menutup secara otomatis ketika user lupa logout, pada saat login terjadi kesalahan berulang sistem tidak menutup secara otomatis, dan tidak tersedia informasi tentang umur password. Dari permasalahan tersebut, maka akan dilakukan analisa berdasarkan domain *deliver, service and support (DSS05)* yang mengacu pada COBIT 5 dengan mengumpulkan informasi pendukung melalui studi dokumen, wawancara, dan kuesioner. Proses selanjutnya akan diolah untuk mengetahui hasil penelitian yang diperoleh dari analisis tingkat kapabilitas dan analisis kesenjangan. Setelah dilakukannya analisa tingkat kapabilitas maka diperoleh hasil sebesar 82.19% atau sebanding dengan 3,25 dengan status *Larger Achieved* dimana dalam proses yang berkaitan dengan keamanan sistem masih terdapat kelemahan. Dari hasil analisa tingkat kapabilitas yang mengacu pada level 4, dapat disimpulkan bahwa terdapat kesenjangan (*gap*) selisih nilai untuk dapat mencapai hasil maksimal. Dengan begitu PT Astragraphia Tbk dapat melakukan strategi perbaikan yang dilakukan secara bertahap pada proses atribut level 1 hingga level 4.

Kata Kunci: Keamanan Sistem, *Deliver, Service and Support (DSS05)*, COBIT 5, Tingkat Kapabilitas, Kesenjangan (*gap*).

Abstract

Information system can be accessed everywhere ,everytime, and sometimes an institution or an organization has their own information system. The kind of automation that used in PT Astragraphia Tbk is Docushare system. Docushare have a minim security system that may caused the abuse to this system. It can be abuse in this system. Docushare is a intergrated system, that used to access the system information that can conducted in every branch of PT Astragraphia Tbk. interconnected with compensation of employee facilities that will doing in every branch and also depot PT. Astragraphia Tbk. Where the problem in user login in many time, the system doesn't do automatically, and when the user login the problem was happened in many times, and not to closed automatically, and there is no information about the password. From this problem,the system will be analysed based on domain *deliver, service and support (DSS05)* that refer to COBIT 5 with collecting informations that supported trough by the literature review, interview and questionnaire. The data analyze condused to know about the research result that obtained from the grade of capability analyse and discrepancy analyse. After the grade of capability analyse, and researcher can got the result 82.19% or comparable with 3.25 with the status *Larger Achieved* where in process that relate to security system still have the weakness. From the the grade of capability analyse that refers to the level 4, can be concluded there are still have the deviation *Gap* results to achieved the maximum result. So, PT

Astragraphia Tbk need revinment strategy step by step on the attribute process level 1 until level 4.

Keywords: *Security System, Deliver, Service and Support (DSS05), COBIT 5, Capability Level, Gaps.*

1. PENDAHULUAN

1.1 Latar Belakang

Sistem otomatisasi kantor (*Office Automation*) merupakan sistem informasi yang berbasis telekomunikasi yang mengumpulkan, memproses, menyimpan dan mendistribusikan pesan, dokumen dan komunikasi elektronik lainnya antar individu, kelompok kerja dan organisasi. Otomatisasi kantor dimanapun selalu bersangkutan dengan aktifitas informasi, dari data yang masuk kemudian dilanjutkan pada proses data hingga menjadi informasi. Setelah data diolah, selanjutnya informasi bisa digunakan langsung oleh personil saat beraktifitas didalam kantor, berupa informasi yang sifatnya hanya dapat digunakan pada cabang lokal maupun interlokal. Pemanfaatan sistem otomatisasi kantor akan lebih efisien dan relevan sebagai sarana berkomunikasi antar bagian [1].

PT. Astragraphia Tbk memiliki sistem otomatisasi yang dikenal dengan nama Docushare. Docushare merupakan salah satu perangkat lunak yang dibeli dari Fuji Xerox, Jepang. Docushare berperan sebagai media penyampaian informasi khususnya yang berhubungan dengan karyawan antara lain: *medical online, solution online*, absensi, lembur, pemberitahuan mutasi, gaji, dan prestasi karyawan. Pemanfaatan sistem informasi Docushare ini menggunakan fasilitas intranet dan jaringan LAN (*Local Area Network*). Untuk mengakses sistem Docushare, harus melalui proses *login* dengan mengisi *username* dan *password*. Namun, pihak Astragraphia tidak memberikan hak akses bagi seluruh karyawan, hanya

karyawan tetap yang memperoleh hak tersebut.

Docushare dapat diakses diberbagai cabang dan depo Astragraphia. Meskipun *user* bekerja di cabang Semarang, tetapi ketika melakukan kunjungan di cabang Bandung *user* ingin mengakses infomasi melalui Docushare, maka proses login tetap bisa dilakukan. Proses tersebut memang dirasa lebih fleksibel, jika pihak Astragraphia lebih optimal dalam meningkatkan kualitas dan peran keamanan sistemnya. Sebab, segala proses yang sudah terintegrasi dengan bantuan sistem, tidak terlepas dengan berbagai macam gangguan dan resiko penyalahgunaan, antara lain: Pertama, tidak adanya respon sistem untuk menutup secara otomatis jika *user* menggunakan komputer lain saat ingin mengakses informasi dari Docushare dan lupa *logout* (keluar) maka memungkinkan orang lain bisa melihat segala informasi milik *user*. Kedua, apabila *user* melakukan kesalahan secara berulang saat proses *login*, seharusnya sistem menutup secara otomatis untuk meminimalisir jika hal tersebut dilakukan pada pihak yang tidak terotorisasi. Ketiga, tidak tersedianya informasi tentang pembatasan umur *password*.

Untuk meminimalisir permasalahan tersebut, maka pihak Astragraphia harus menjamin keamanan sistem Docushare. Langkah ini dilakukan sebagai upaya untuk memonitor aktifitas yang mencurigakan serta melindungi segala aset perusahaan yang berkaitan dengan *database*, jaringan, sistem komputer, dan sistem informasi. Namun, keamanan sistem juga harus memperhatikan beberapa prinsip seperti

kerahasiaan, integritas, ketersediaan, dan akses kontrol.

Sistem informasi yang sudah tersedia dan terintegrasi perlu dilakukan proses pemeriksaan untuk mengetahui bagaimana pelaksanaan dan kualitas yang diterapkan.

Proses pemeriksaan akan dilakukan menggunakan COBIT 5. COBIT 5 adalah salah satu kerangka bisnis untuk tata kelola dan manajemen perusahaan berbasis teknologi informasi. Kerangka kerja ini membantu perusahaan menciptakan nilai yang optimal dari IT dengan menjaga keseimbangan antara menyadari manfaatnya dan meminimalisir tingkat resiko serta penggunaan sumber daya [2].

1.2 Rumusan Masalah

1. Bagaimana kualitas keamanan sistem Docushare yang diterapkan PT Astragraphia Tbk menggunakan domain *deliver, service and support* (DSS05) sebagai upaya proteksi aset informasi yang dilihat dari analisis tingkat kapabilitas berdasarkan COBIT 5?
2. Apa saja yang harus diperbaiki untuk meminimalisir resiko yang mungkin terjadi pada sistem informasi Docushare, dari hasil analisis kesenjangan?

1.3 Batasan Masalah

1. Pembahasan hanya berkisar tentang peran dan kualitas keamanan sistem informasi Docushare menggunakan domain *deliver, service and support* (DSS05).
2. Hanya melihat apakah tingkat keamanan sistem informasi Docushare cukup potensial yang di tentukan melalui domain *deliver, service and support* (DSS05), sebagai upaya proteksi aset informasi PT. Astragraphia Tbk berdasarkan COBIT 5.

3. Melihat pengolahan sistem informasi Docushare sebagai tolak ukur pemanfaatan teknologi informasi yang tersedia, dan memberikan saran terkait dengan perbaikan sistem yang terjamin keamanannya.

1.4 Tujuan Penelitian

1. Mengidentifikasi kualitas keamanan sistem Docushare saat ini dan yang akan diharapkan, dengan mengukur tingkat kapabilitas sistem guna mendukung media penyampaian informasi sebagai fasilitas kompensasi karyawan PT. Astragraphia Tbk yang relevan menggunakan domain *deliver, service and support* (DSS05) berdasarkan COBIT 5.
2. Dari hasil analisis kesenjangan (gap) dapat membuat rencana strategis untuk meningkatkan kualitas keamanan sistem sesuai yang diharapkan PT. Astragraphia Tbk berdasarkan COBIT 5.

2. LANDASAN TEORI

2.1 Tinjauan Pustaka

Dalam penelitian ini, mengacu dengan beberapa penelitian yang dilakukan seseorang sebelumnya terkait dengan tata kelola IT berdasarkan COBIT 5 dan keamanan sistem.

Tabel 1: Penelitian Terkait

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1	Alvin, Wongso Soekamto, dan Riny Harsono, 2013 [3].	Analisis dan evaluasi tata kelola IT pada PT. FIF dengan standart COBIT 5.	Mengukur tingkat kapabilitas menggunakan standart COBIT 5.	Tingkat kapabilitas yang diperoleh yaitu 2,38.
2	Abdul Hakim, Hoga Saragih, dan Agus Suharto,	Evaluasi tata kelola teknologi informasi dengan framework	Analisis kapabilitas menggunakan framework COBIT 5	Hasil penelitian evaluasi pada domain (BAI)

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
	2014 [4].	cobit 5 di Kementrian ESDM.	dan analisis gab.	dengan target capaian 3.
3	Dimas Aryo Anggoro, 2013 [5].	Analisis kepatuhan karyawan terhadap kebijakan pengamanan data pada PT. XYZ dengan standart COBIT 5.	Menggunakan uji statistik dan analisis gap.	Tingkat kepatuhan karyawan terhadap kebijakan pengamanan data sebesar 3.83.

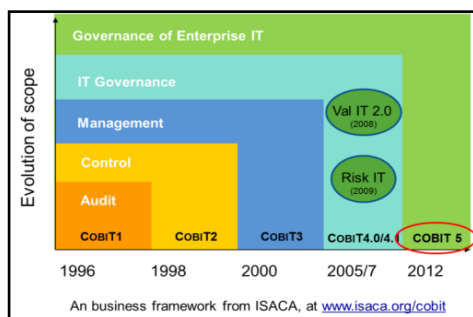
2.2 PROTEKSI ASET INFORMASI

Proteksi aset informasi dibagi menjadi 4 macam [7].

1. Proteksi pada sistem operasi
2. Proteksi pada basis data
3. Proteksi pada sistem informasi
4. Proteksi pada jaringan komputer

2.3 COBIT 5

COBIT 5 merupakan salah satu kerangka bisnis dalam tata kelola manajemen perusahaan yang berbasis IT, dengan mengkombinasikan tata kelola perusahaan dan teknik manajemen. Pada COBIT 5 juga menyediakan prinsip, analisis serta model yang berfungsi untuk membantu dalam meningkatkan kepercayaan dan nilai dari sistem informasi. [4].

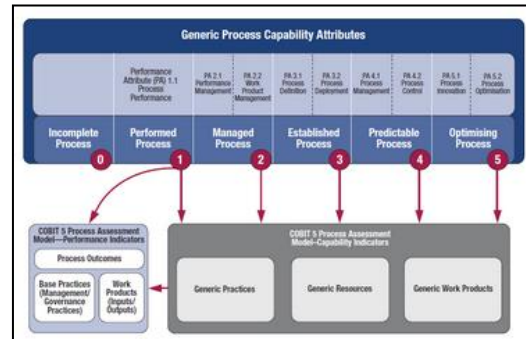


Gambar 1. COBIT 5 [8]

2.4 Tingkat Kapabilitas

Tingkat kapabilitas memberikan penilaian dimana proses penilaian

tersebut bertujuan untuk mengukur pencapaian proses bisnis dengan didukung pemanfaatan teknologi informasi yang telah saat ini diterapkan perusahaan dan yang akan diharapkan [4].



Gambar 2. Kapabilitas Atribut Proses [2]

2.5 Skala Penilaian

Skala penilaian digunakan setelah memperoleh hasil dari analisa tingkat kapabilitas.

Tabel 1: Skala Penilaian

Abbreviation	Description	% Achieved
N	Not achieved	0 to 15% achievement
P	Partially achieved	>15% to 50% achievement
L	Largely achieved	>50% to 85% achievement
F	Fully achieved	>85% to 100% achievement

2.6 Diagram RACI deliver, service and support (DSS05)

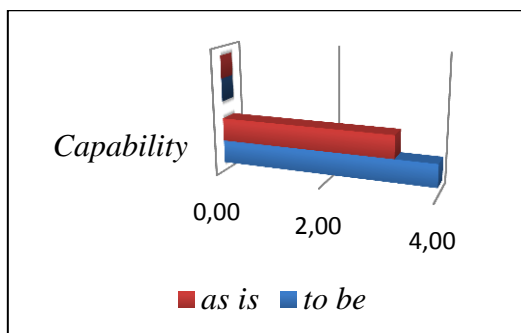
Diagram RACI berfungsi untuk mengelompokkan tanggung jawab dan peran sesuai struktur organisasi yang ada pada suatu perusahaan. Dengan adanya diagram RACI maka akan diketahui bahwa peran seseorang tersebut penting dalam mengelola perusahaan yang berbasis IT.

4. HASIL DAN PEMBAHASAN

Tabel 2: Hasil Kuesioner

Process Name	DSS 05 Manage Security Service									
Description	Fokus sebagai upaya melindungi informasi organisasi untuk meningkatkan kualitas keamanan suatu sistem agar dapat diterima oleh organisasi sesuai dengan kebijakan keamanan.									
Purpose	Meminimalisir dampak operasional bisnis dari kerentanan layanan keamanan informasi dan insiden.									
Level	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
Process Atribut		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Percentage	81.88%	89.38%	62.50%	82.50%	79.38%	85.00%	86.88%	71.25%	59.38%	64.38%
Rating by Criteria	L	F	L	L	L	L	F	L	L	L
Capability Level Achieved					82.19%		Target			
					3.25					

Dari hasil perhitungan kuesioner maka diperoleh tingkat kapabilitas PT Astragraphia Tbk yaitu 3,25 (82,29%) dengan target yang terdapat pada level 4. Dengan prosentase kurang dari 85,00% sehingga perusahaan memperoleh kriteria *Larger Achieved* dimana pada setiap prosesnya masih membutuhkan perbaikan guna meningkatkan performa perusahaan. Setelah melakukan analisis tingkat kapabilitas, tahap berikutnya yaitu analisis kesenjangan. Analisis kesenjangan diperoleh dari selisih antara level saat ini (level 3) dan yang diharapkan (level 4).



Gambar 5. Grafik Kesenjangan Pada Tingkat Kapabilitas

Dari diagram diatas terlihat bahwa terjadi kesenjangan sebesar 0,75. Hasil tersebut merupakan nilai gap yang berasal dari selisih antara nilai pencapaian level saat ini (3.25) dengan target level yang diinginkan. Penentuan target level tidak mengarah pada perolehan hasil tertinggi ataupun terendah, namun disesuaikan dengan status level yang dimiliki oleh kedua level tersebut.

Dengan nilai dan status yang dimiliki oleh kedua level tersebut, maka pada level 4 yang merupakan target (yang diinginkan) harus memperoleh status *Fully Achieved*. Sesuai dengan ketentuan bahwa untuk memperoleh status F harus memenuhi kriteria penilaian yaitu (lebih dari 85.00% hingga 100.00%). Proses penilaian yang dilakukan yaitu perbandingan selisih nilai dengan menggunakan acuan prosentase nilai 85.01% sebagai syarat pemenuhan status *Fully Achieved*.

Dari nilai kesenjangan tersebut dapat dilakukan strategi perbaikan guna meningkatkan kualitas keamanan pada sistem Docushare serta sebagai upaya proteksi aset informasi. Berikut strategi perbaikan dari setiap proses atribut, antara lain:

1. PA 1.1 *Process Performance*

Terdapat 2 startegi perbaikan pada proses ini, diantaranya sebagai berikut:

- Proses *error recovery* seharusnya dilakukan perbaikan sistem yang baik, atau dengan cara menyiapkan tenaga ahli yang bertugas untuk memantau secara rutin. Ini merupakan upaya agar sistem tersebut dapat merespon secara cepat apabila terjadi gangguan.
- Meskipun sistem Docushare hanya dapat diakses oleh karyawan saja. Namun pihak PT Astragraphia Tbk harus menyiapkan sumber daya manusia yang dipercaya untuk

memberikan informasi kepada karyawan tidak tetap melalui email ataupun SMS. Informasi yang diberikan berupa informasi yang layak untuk semua karyawan. Sehingga tidak terjadi kesalahpahaman ataupun ketidaktahuan tentang informasi yang up to date saat ini.

2. PA 2.1 *Performance Management*

Proses *login* memang sudah diterapkan, tetapi ada beberapa proses yang sampai sekarang masih belum di realisasikan. Pihak PT Astragraphia Tbk harus segera merealisasikan proses tersebut, karena proses yang berkaitan dengan respon menutup otomatis dan informasi umur *password* sangat penting. Sebab, dengan diterapkannya proses ini nantinya dapat meminimalisir penyalahgunaan oleh pihak yang tidak bertanggung jawab untuk berusaha mengakses informasi pribadi karyawan maupun perusahaan.

3. PA 2.2 *Work Product Management*

Apabila terjadi permasalahan pada sistem Docushare, akan tetapi dari pihak PT Astragraphia Tbk mengalami kendala dalam proses perbaikannya. Sebaiknya segera melaporkan permasalahan ini pada PT AGIT (*Astragraphia Information Technology*), karena sistem Docushare menampung segala hal yang dapat mendukung aktivitas kerja.

4. PA 3.1 *Process Definition*

Seharusnya PT Astragraphia Tbk menambahkan kuota internet, agar lebih cepat. Sehingga tidak berdampak pada penurunan respon sistem saat bandwidth over limit. Dengan peningkatan layanan khususnya terkait dengan akses internet, karyawan tidak akan panik jika terjadi hal tersebut. Karena kemungkinannya sangat kecil apabila terjadi gangguan respon sistem.

5. PA 3.2 *Process Deployment*

Kebijakan mengenai batasan untuk masuk ke ruang server, perlu diingatkan kembali kepada karyawan dan diberikan sanksi tegas jika diketahui ada karyawan yang masuk dengan merusak komponen didalamnya. Sebaiknya, diruang server disediakan kamera CCTV guna memantau kondisi ruangan tersebut.

6. PA 4.1 *Process Measurement*

Setiap karyawan yang memiliki wewenang untuk mengakses sistem Docushare harus melindungi akun pribadinya. Bentuk perlindungan akun dapat dilakukan dengan cara sebagai berikut:

- a. Tidak menulis *password* pada kertas maupun menyimpannya dalam komputer.
- b. Tidak memberitahukan *password* kepada karyawan lain.
- c. Rutin mengganti *password* setiap 3 bulan sekali dengan mengkombinasikan angka dan huruf.
- d. Usahakan tidak membuat *password* berdasarkan tanggal lahir ataupun nomor *handphone*.

7. PA 4.2 *Process Control*

Informasi terkait dengan *password expired* (sudah kadaluarsa), harus diterapkan. Apabila batasan umur *password* diterapkan dan di sesuaikan seperti yang sudah dijelaskan sebelumnya pada strategi perbaikan PA 4.1. Dengan begitu maka privasi *user* keamanannya terjamin.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Perolehan nilai tingkat kapabilitas yang dicapai pada level 3, sebesar 3.25 atau sebanding dengan 82.19% dengan status *Larger Achieved*. Pada proses tersebut masih perlu

- peningkatan agar dapat mendukung kinerja PT Astragraphia Tbk.
2. Terdapat kelemahan pada kualitas keamanan sistem Docushare. Sehingga dibutuhkan strategi perbaikan pada setiap prosesnya yang dilakukan secara bertahap pada level 2 hingga level 4.

5.2 Saran

1. Peningkatan kualitas keamanan sistem dapat dilakukan dengan cara melaksanakan proses audit secara lebih intens khususnya terkait pada tata kelola IT. Sebab, keamanan sistem merupakan hal utama untuk mendukung performa perusahaan.
2. Saran untuk penelitian selanjutnya, yaitu dapat menggunakan google form sebagai sarana pengumpulan data secara *online* yang mampu menghasilkan laporan dan lebih fleksibel. Pengumpulan data kuesioner dengan memanfaatkan fasilitas ini, cukup akurat sebab jika kuesioner belum diisi lengkap, maka sistem akan memberikan peringatan.

- [5] D. A. Anggoro, "Analisis Kepatuhan Karyawan Terhadap Kebijakan Pengamanan Data Pada PT. XYZ Dengan Standart Cobit 5," *Skripsi*, Juli 2013.
- [6] dr. ahmad sudiro SE, ME ,Perdana Rahadian SE, ME , Ir. Nur prima MM, Sistem Informasi Manajemen, Universitas Brawijaya Press, 2011.
- [7] R. T. Asmono, "Proteksi Aset Informasi," Semarang, 2014.
- [8] T. Sutabri, Konsep Sistem Informasi, I. Nastiti, Penyunt., Yogyakarta: CV Andi Offset, 2012.
- [9] ISACA, "Process Reference Guide Cobit 5," 2011.
- [10] ISACA, "Process Assesment Method," 2011.
- [11] F. Xerox, "User Guide Docushare," 2011.

6. DAFTAR PUSTAKA

- [1] R. Mc.Leod, "Sistem Otomatisasi Kantor," Jakarta, 2014.
- [2] ISACA, "A Bussiness Framework for the Governance and Management of Enteprise IT," 2012.
- [3] A. dkk, "Analisis dan evaluasi tata kelola IT pada PT. FIF dengan standart Cobit 5," *Skripsi*, 2013.
- [4] H. S. a. A. S. Abdul Hakim, "Evaluasi Tata Kelola Teknologi Informasi Dengan Framework Cobit 5 Di Kementrian ESDM," *Tesis Jurusan Teknik Informatika*, p. 13, Oktober 2014.