Audit Sistem Keamanan TI Menggunakan Domain DSS05 Pada *Framework* COBIT 5

(Studi Kasus: Diskominfo Kabupaten Karawang)

D.V.Gusman[1], F.H.Prasetyo[2] dan K.Adi[3]
[1,2,3]*Jurusan Sistem Informasi, Sekolah Pascasarjana, Universitas Diponegoro*
Jl. Imam Bardjo SH No.5, Semarang
E-mail : deavalenska28@gmail.com[1], fhary15@gmail.com[2], kusworoadi@lecturer.undip.ac.id[3]

Abstract—Information security in the digital era is very important, so it becomes a critical problem for enterprise, organizations and governments. The Communication and Informatics Office of Karawang Regency was formed based on Peraturan Daerah No. 14 of 2016 concerning the Formation and Composition of the Karawang Regency Regional Apparatus. Information technology is already implememted in the information security system of the Karawang Regency government. However, in realizing this, the value and benefits have not been fully succeeded. This study aims to evaluate the security of information systems that have been implemented in institutions to assess Capability Level using the DSS05 domain at COBIT 5. The method used is the Assessment Process Activities of COBIT 5, including Initiation Program, Define Problems and Opportunities, Data Collection, Data Validation and Process Attribute Level. The results of this study obtained the capability value of 3,4 (as is) and 4.1 (to be) of the two values, so the process that has been implemented in outline is achieved. In the DSS05 domain, the achievement was 92%, meaning that the 3.1 process definition attribute process was fully achieved, so that the assessment could be continued to the next level, namely (PA) 3.2 Process Deployment.

Abstrak—Keamanan informasi pada era digital sangat penting, sehingga menjadi masalah penting bagi perusahaan, organisasi, serta lembaga pemerintahan. Dinas Komunikasi serta Informatika Kabupaten Karawang didirikan berdasarkan Peraturan Daerah No.14 pada Tahun 2016 mengenai Pembentukan serta Susunan Perangkat Daerah Kabupaten Karawang. Pemanfaatan teknologi informasi sudah diterapkan dalam sistem keamanan informasi pemerintah Kabupaten Karawang. namun dalam mewujudkan hal itu, belum sepenuhnya berhasil dalam pengambilan nilai serta manfaatnya. Riset ini mempunyai tujuan untuk melakukan evaluasi keamanan sistem informasi yang telah diimplementasikan pada institusi untuk menilai level kapabilitas menggunakan *domain* DSS05 pada COBIT 5. Metode yang dipakai yaitu *Assesment Process Activities* COBIT 5 antara lain *Initiation Programme, Define Problems and Opportunities, Data Collection, Data Validation* serta *Process Atribut Level*. Hasil riset ini didapatkan nilai kapabilitas 3,4 *(as is)* serta 4.1 *(to be)* maka proses yang telah diimplementasikan secara garis besar tercapai. Pada *domain* DSS05 mendapatkan capaian sebesar 92% berarti pada proses atribut 3.1 *process definition* tercapai penuh, sehingga penilaian dapat dilanjutkan ke level berikutnya yaitu (PA) 3.2 *Process Deployment*.

Kata Kunci—DSS05, COBIT 5, Diskominfo, Level Kapabilitas

I. PENDAHULUAN

Teknologi informasi saat ini merupakan bagian utama dalam perusahaan atau organisasi. Penerapan sistem informasi diharapkan mampu memberikan dampak positif untuk institusi. Namun seiring dengan berkembangnya teknologi, muncul penyalahgunaan oleh oknum yang tidak bertanggungjawab dan bisa menimbulkan terjadinya permasalahan dari penerapan teknologi. Penerapan keamanan sistem informasi menjadi sangat penting dari sebuah institusi untuk menjaga informasi secara optimal dan aman. Adanya masalah keamanan memicu prosedur untuk mengendalikan hak akses pada sebuah sistem informasi [1].

Tata kelola TI yang baik secara langsung mengarah pada peningkatan produktivitas, kualitas yang lebih tinggi, serta hasil keuangan yang lebih baik. Tata kelola TI yang buruk, di sisi lain, sering menyebabkan pemborosan programatik, birokrasi, moral yang lebih rendah, serta kinerja keuangan yang berkurang secara keseluruhan [2]. Tata pengaturan serta manajemen TI yang efisien serta sejajar dengan kebutuhan bisnis serta didukung oleh kemitraan bisnis yang kuat sangat penting bagi keberhasilan fungsi penerapan TI [3]. Aset TI yang berinteraksi dengan tata pengaturan TI yang bagus diyakini bisa memengaruhi kinerja sebuah organisasi secara keseluruhan [4].

Keamanan data dan informasi saat ini sangat penting serta menjadi perhatian utama dalam bisnis, organisasi, serta pemerintah, karena Lingkungan Keamanan Informasi (IEE) telah menjadi ancaman utama yang kompleks. Sistem informasi yang tepat adalah sistem informasi yang dapat dinilai tingkat keamananya, sehingga mampu memberikan

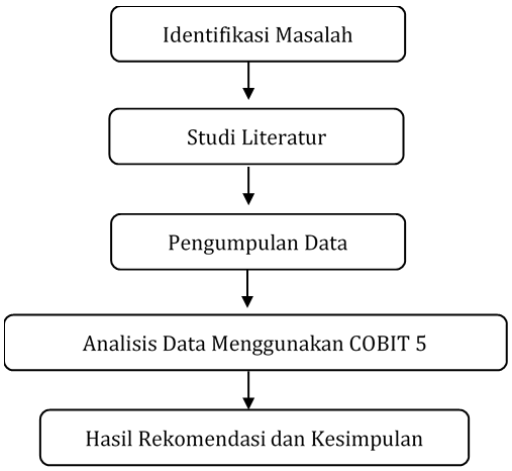
kenyamanan bagi pengguna [5]. Laporan ancaman keamanan internet (*Internet Security Threat Report*) yang dikemukakan oleh Symantec membuktikan bahwa pemerintahan adalah sasaran utama pembobolan data pada tahun 2013 dengan jenis *Spear-Phishing*. Hal ini tidak dapat dianggap remeh karena pemerintahan adalah lembaga yang seharusnya bersifat kredibel serta akuntabel dalam memberikan pelayanan, perlindungan, serta menjamin kemanan serta kepentingan rakyatnya [6].

COBIT (*Control Objectives for Information and related Technology*) adalah suatu pedoman dalam manajemen teknologi informasi aturan mengatur TI yang dapat mempermudah pengaudit, manajemen, serta konsumen buat memisahkan antara risiko bidang usaha, keahlian pengaturan, serta kasus teknis tercantum keamanan sistem informasi [7]. Daerah yang berkaitan dengan keamanan teknologi informasi merupakan *domain* DSS. *Domain* DSS (*Deliver, Service and Support*) adalah *domain* yang diperlukan untuk menganalisa teknologi informasi dalam zona menajemen yang di dalamnya ada sebagian cara. Dalam daerah DSS ada *sub-domain* DSS05 yang ialah metode yang lebih detail kepada sistem keamanan informasi. *Sub-domain* yang diartikan merupakan *manage security services* dimana *sub-domain* ini melakukan sekian banyak aktivitas [8].

Dinas Komunikasi serta Informatika (Diskominfo) merupakan organisasi yang bertanggung jawab terhadap pelaksanaan tugas di bidang komunikasi serta informatika. Diskominfo Kabupaten Karawang dibangun beralaskan pada Peraturan Daerah No.14 pada Tahun 2016 mengenai Pembentukan serta Susunan Perangkat Daerah Kabupaten Karawang kemudian petunjuk pelaksanaan tugasnya diatur dengan Peraturan Bupati Karawang No.56 Tahun 2016 mengenai Rincian Tugas, Fungsi serta Tata Kerja Diskominfo Kabupaten Karawang. Di Kabupaten Karawang pemanfaatan teknologi informasi sebenarnya sudah diterapkan dalam sistem keamanan informasi pemerintahannya. namun keberhasilan belum sepenuhnya dapat diimbangi dengan perolehan nilai gunanya [9].

II. METODE PENELITIAN

Pada riset ini perencanaan kegiatan audit sistem keamanan pada Diskominfo Kabupaten Karawang disusun seperti pada gambar 1.



Gambar. 1. Rancangan Kegiatan Audit Sistem Keamanan

A. Identifikasi Masalah

Langkah awal di riset ini merupakan melaksanakan identifikasi masalah yang ada pada Diskominfo Kabupaten Karawang pada bagian kemanan yang selanjutnya akan dievaluasi menggunakan COBIT 5 untuk memberikan rekomendasi perbaikan.

B. Studi Literatur

Pada tahap ini dilaksanakan pencarian serta pengumpulan informasi dari literasi-literasi terdahulu. Pada riset ini pengumpulan informasi didapatkan dari sumber jurnal serta dokumen yang membahas mengenai implementasi *framework* COBIT 5. Selain itu, dilakukan juga studi pada dokumen Rencana Strategis Diskominfo Kabupaten Karawang bertujuan untuk mengumpulkan informasi serta data-data mengenai organisasi. Adapun informasi-informasi yang dibutuhkan ialah meliputi visi serta misi, profil departemen yang ada, rencana strategis organisasi, *Standard Operating Procedure* (SOP), serta struktur organisasi.

C. Pengumpulan Data

Riset ini dilakukan di Diskominfo Kabupaten Karawang. Data primer diperoleh dari wawancara, kuisioner, serta observasi pada sistem keamanan di Diskominfo Kabupaten Karawang.

D. Analisis Data

Metode yang digunakan pada tahapan analisa data riset ini menyesuaikan dengan Assesment Process Activities COBIT 5 [7], sebagai berikut:

1. *Initiation Programme*

Melakukan identifikasi permasalahan yang terdapat di Diskominfo Kabupaten Karawang yang bermaksud untuk mempelajari keadaan yang sebenarnya.

2. *Define Problems and Opportunities*

Pada bagian ini dilaksanakan pemetaan bagian-bagian yang termasuk di pengukuran level kapabilitas sesuai dengan diagram RACI yang disusun menyesuaikan jabatan serta fungsi yang terdapat di Diskominfo Kabupaten Karawang.

3. *Data Collection*

Tahap ini dilakukan identifikasi dari kebutuhan dari output untuk berbagai tahapan yang akan dilakukan instansi berdasarkan COBIT 5 dengan tujuan melihat terpenuhinya angka *Capability Level* yang sanggup digapai pada cara *domain* yang sudah didetetapkan maka tahapan- tahapan yang dinilai menurut bukti jadi objektif.

4. *Data Validation*

Langkah ini dicoba validasi hasil penemuan dokumen cocok RACI *Chart process*, *domain* yang sudah ditetapkan dengan menentukan data yang didapat dari responden merupakan data yang cermat serta sesuai dengan lingkup penilaian.

5. *Process Atribut Level*

Pada langkah ini dicoba rekapitulasi dari totalitas cara yang terdapat pada cara *domain* yang sudah didetetapkan, serta melaksanakan cara pengecekan *Generic Work Product* (GWP) dengan cara berangsur-angsur pada cara *domain* yang sudah didetetapkan, memperhitungkan apakah cara itu sudah penuhi standar yang wajib dipadati pada tiap-tiap tingkat, penilaian dicoba menurut data yang sudah divalidasi pada sebelumnya.

E. Hasil Rekomendasi serta Kesimpulan

Hasil penentuan *capability level* dilaporkan sehingga dapat memberikan rekomendasi pada organisasi serta menentukan kesimpulan dari riset.

III. HASIL DAN PEMBAHASAN

A. Gambaran Umum Organisasi

Diskominfo Kabupaten Karawang berkewajiban dalam aktualisasi tugas serta fungsi dalam bidang teknologi informasi di wilayah Kabupaten Karawang. Dalam rangka merealisasikan visi pemerintah Kabupaten Karawang yaitu: “Karawang yang Mandiri, Maju, Adil, serta Makmur”. Selanjutnya Diskominfo Kabupaten Karawang dalam upaya mewujudkan visi serta misi mereka membentuk struktur organisasi. Berikut adalah visi dan misi serta struktur organisasi Diskominfo Kabupaten Karawang [9]:

1. Visi

Terwujudnya pelayanan teknologi informasi serta komunikasi yang efektif serta efisien menuju Karawang maju serta mandiri.

2. Misi
   a. Meningkatkan perkembangan prasarana teknologi informasi serta komunikasi (TIK) lewat perancangan aplikasi, kualitas fasilitas informasi publik, penyeragaman serta penggunaan jaringan teknologi informasi serta komunikasi (TIK) serta keamanaan informasi serta data untuk mengoptimalisasi jasa publik.
   b. Menambah mutu serta kuantitas pengarsipan serta informasi lewat pengembangan serta pemberdayaan pers serta media massa.
   c. Menambah mutu layanan informasi publik, distribusi informasi serta pemberdayaan golongan publik.
   d. Tingkatkan pengetahuan serta keterampilan aparatur di aspek teknologi informasi serta komunikasi serta di dukung oleh prasarana serta infrastruktur yang mencukupi, serta layanan logistik dengan cara elektronik (LPSE).
3. Struktur Organisasi Dinas Komunikasi serta Informatika Kabupaten Karawang

Gambar. 2. Struktur Organisasi Diskominfo Kabupaten Karawang

B. Initiation Programme

Di bagian ini dilakukan penentuan *domain* di COBIT 5 yang berikutnya akan dievaluasi di Diskominfo Kabupaten Karawang. Berdasarkan data hasil observasi dapat diketahui bahwa misi dari Diskominfo Kabupaten Karawang antara lain adalah:

1. Meningkatkan perkembangan infrastruktur teknologi informasi serta komunikasi (TIK).
2. Standarisasi serta pemanfaatan teknologi informasi serta komunikasi (TIK).
3. Keamanaan informasi serta data untuk mengoptimalisasi pelayanan publik.
4. Meningkatkan pengetahuan serta keterampilan perangkat daerah di bagian teknologi informasi serta komunikasi serta dibantu oleh sarana serta prasarana pendukung yang layak, serta layanan pengadaan secara elektronik (LPSE).

Dari visi serta misi tersebut maka pada riset ini penulis ingin memfokuskan pada audit keamanan sistem informasi atau berfokus pada *domain* DSS05 pada Diskominfo Kabupaten Karawang. Proses DSS05 (Kelola Layanan Keamanan) menjaga informasi perusahaan buat menjaga level dari keamanan Informasi yang dapat diperoleh oleh perusahaan cocok dengan kebijaksanaan keamanan. Memutuskan serta menjaga kedudukan keamanan informasi serta hak akses serta melaksanakan pengawasan keamanan. Sub cara pada DSS05 sebagai selanjutnya:

1. DSS05.01
(Menjaga Sistem dari Perangkat Lunak Berbahaya)
2. DSS05.02
(Mengatur Jaringan serta Keamanan Konektivitas)
3. DSS05.03
(Mengatur Keamanan Titik Akhir)
4. DSS05.04
(Mengatur Bukti Diri Pemakai serta Akses Lojik)
5. DSS05.05
(Mengatur Akses Fisik ke Kekayaan TI)
6. DSS05.06
(Mengatur Arsip Penting serta Perangkat *Output*)
7. DSS05.07
(Memonitor Prasarana buat Peristiwa Terkait Keamanan)

C. Define Problems and Opportunities

1. Pemetaan Struktur Organisasi terhadap RACI *Chart process* (DSS05)

Tabel 1.
Matrik RACI Chart DSS05

Key Governance Practice	*Kepala Pejabat Informasi*	*Kepala Operasi TI*	*Manajer Keamanan Informasi*
DSS05.01 Menjaga Sistem dari Perangkat Lunak Berbahaya	C	R	R
DSS05.02 Mengatur Jaringan serta Keamanan Konektivitas	C	R	R
DSS05.03 Mengatur Keamanan Titik Akhir	C	R	R
DSS05.04 Mengatur Bukti Diri Pemakai serta Akses Lojik	C	R	R
DSS05.05 Mengatur Akses Fisik ke Kekayaan TI	C	R	R
DSS05.06 Mengatur Arsip Penting serta Perangkat *Output*	A	R	R
DSS05.07 Memonitor Prasarana buat Peristiwa Terkait Keamanan	C	R	R

Menurut RACI *Chart process* DSS05, periset mendapatkan 3 (tiga) narasumber yang sesuai dengan aturan serta struktur organisasi di COBIT 5, ketiga responden itu tercatat di tabel 2 berikut.

Tabel 2.
Pemetaan RACI Chart DSS05

RACI Chart	***Struktur Organisasi Diskominfo***
Kepala Pejabat Informasi	Kepala bidang penyelenggara *e-Government*
Kepala Operasi TI	Kepala Seksi insfrastruktur serta teknologi
Manajer Keamanan Informasi	Kepala Seksi persandian serta keamanan informasi

D. Data Collection

Tahap ini dilakukan pemahaman pada kebutuhan *output* pada setiap proses yang akan dijalankan instansi. Output proses DSS05 dapat dilihat pada tabel 3.

Tabel 3.
Ouput Proses DSS05 (*Manage Security)*

Key Management Practice	***Outputs***
DSS05.1 Menjaga Sistem dari Perangkat Lunak Berbahaya	Kebijakan pencegahan perangkat lunak berbahaya
DSS05.2 Mengatur Jaringan serta Keamanan Konektivitas	Kebijakan keamanan konektivitas
DSS05.3 Mengatur Keamanan Titik Akhir	Kebijakan keamanan untuk perangkat titik akhir
DSS05.4 Mengatur Bukti Diri Pemakai serta Akses Lojik	Hak akses pengguna yang disetujui Hasil ulasan akun pengguna serta hak istimewa
DSS05.5 Mengatur Akses Fisik ke Kekayaan TI	Permintaan akses yang disetujui Kunci akses
DSS05.6 Mengatur Arsip Penting serta Perangkat *Output*	Inventarisasi dokumen serta perangkat sensitif Hak akses istimewa
DSS05.7 Memonitor Prasarana buat Peristiwa Terkait Keamanan	Kunci peristiwa kemanan Karakteristik insiden keamanan Tiket insiden keamanan

E. Data Validation

Proses DSS05 yaitu menjaga informasi perusahaan buat menjaga jenjang keamanan informasi yang dapat diperoleh oleh perusahaan pantas dengan kebijaksanaan keamanan. Memutuskan serta mempertahankan peran keamanan informasi serta hak akses serta melaksanakan pengawasan keamanan. Sub proses DSS05 dapat dilihat pada tabel 4.

Tabel 4.
Hasil Rekapitulasi Jawaban Kuesioner DSS05

DSS05 (Kelola Layanan Keamanan)	*Nilai Capaian*					*Nilai Harapan*				
	P1	P2	P3	P4	P5	P1	P2	P3	P4	P5
DSS05.1 (Menjaga Sistem dari Perangkat Lunak Berbahaya)	0	0	0	3	0	0	0	0	2	1
DSS05.2 (Mengatur Jaringan serta Keamanan	0	0	2	1	0	0	0	0	3	0

Konektivitas)										
DSS05.3 (Mengatur Keamanan Titik Akhir)	0	0	1	2	0	0	0	0	3	0
DSS05.4 (Mengatur Bukti Diri Pemakai serta Akses Lojik)	0	0	2	1	0	1	0	0	3	0
DSS05.5 (Mengatur Akses Fisik ke Kekayaan TI)	0	0	2	1	0	0	0	0	3	0
DSS05.6 (Mengatur Arsip Penting serta Perangkat *Output*)	0	0	1	2	0	0	0	0	2	1
DSS05.7 (Memonitor Prasarana buat Peristiwa Terkait Keamanan)	0	0	3	0	0	0	0	0	3	0
Level Precentage	0%	0%	367%	333%	0%	33%	0%	0%	633%	67%
Maturity Level (as is)	24,33									
Maturity Level (to be)	29									

F. *Process Atribut Level*

Dalam langkah *process attribute* tingkat ini dilaksanakan pelevelan pada *domain* yang sudah ditetapkan. Cara ini bermaksud supaya membuktikan hasil dari nilai serta *capability level* dari kuisioner dari para responden. Sehabis melaksanakan process *attribute level*, tahap selanjutnya merupakan membagikan saran, *capability*, serta penemuan buat Diskominfo Kab. Karawang. Pengukuran *capability level* pada cara ini ialah memakai Skala Likert. Skala Likert digunakan buat mengukur opini serta tindakan dari tiap responden.

G. *Penentuan Nilai serta Capability Level DSS05*

Menurut kalkulasi di dasar ini bisa disimpulkan kalau pada cara evaluasi manajemen sumber daya pada dikala ini mempunyai angka kapabilitas 3,4 ialah terletak pada tingkatan daya 3, sebaliknya buat situasi yang diharapkan mempunyai angka kapabilitas 4,1 ialah terletak pada tingkatan kapabilitas 4.

Capaian DSS05

$$NK = \frac{(0\% \times 1) + (0\% \times 2) + (367\% \times 3) + (333\% \times 4) + (0\% \times 5)}{3} \times 100\%$$
$$= 3{,}4$$

Harapan DSS05

$$NK = \frac{(33\% \times 1) + (0\% \times 2) + (0\% \times 3) + (633\% \times 4) + (67\% \times 5)}{3} \times 100\%$$
$$= 4{,}1$$

H. *Temuan, Capability, serta Rekomendasi DSS05*

Menurut penilaian yang sudah dilaksanakan pada bagian *data validation* diperoleh nilai 3,3 untuk kondisi capaian sekarang, hal ini berarti pada proses DSS05 saat ini ada di *level* 3, tabel dibawah ini akan menjelaskan temuan, *capability*, serta rekomendasi DSS05.

Tabel 5.
Temuan, *Capability Level*, serta Rekomendasi DSS05

Temuan	***Capability Level***	**Rekomendasi**
Kebijakan keamanan konektivitas hasil tes penetrasi	Kurangnya kesadaran pegawai terhadap hak akses yang mereka miliki Penetrasi untuk mengidentifikasi keamanan sistem informasi belum diperhatikan	Berikan pemahaman lebih terkait hak akses serta pembatasan aturan penggunaan terhadap aset yang dimiliki setiap pegawai Lakukan penetrasi testing disetiap jalur konektivitas serta perangkat lunak yang dipakai untuk mencegah terjadinya kehilangan data

IV. KESIMPULAN

Menurut proses analisa serta evaluasi tingkatan kapabilitas tata kelola teknologi informasi pada *domain* DSS (*Deliver, Service, and Support*) cara DSS05.01 (Menjaga Sistem dari Perangkat Lunak Berbahaya), DSS05.02 (Mengatur Jaringan serta Keamanan Konektivitas), DSS05.03 (Mengatur Keamanan Titik Akhir), DSS05.04 (Mengatur Bukti Diri Pemakai serta Akses Lojik), DSS05.05 (Mengatur Akses Fisik ke Kekayaan TI), DSS05.06 (Mengatur Arsip Penting serta Perangkat *Output*), DSS05.07 (Memonitor Prasarana buat Peristiwa Terkait Keamanan) pada Diskominfo Kabupaten Karawang maka dapat disimpulkan :

1. Pada *domain* DSS05, didapatkan angka kapabilitas sebesar 3,4 untuk kondisi sekarang (*as is*), hal ini berarti pada *domain* tersebut berada pada level 3 yang pada umumnya proses yang telah diimplementasikan secara garis besar tercapai. Sedangkan untuk keadaan yang diharapkan (*to be*) didapatkan angka kapabilitas sebesar 4,1 hal ini dapat diartikan Diskominfo Kab. Karawang mengharapkan level kapabilitas berada di tingkat 4 yaitu proses yang sudah didirikan selanjutnya di operasikan dengan batasan-batasan supaya bisa menggapai harapan dari proses itu.
2. Pada *domain* DSS05 mendapatkan capaian sebesar 92%, hal ini menunjukkan bahwa proses atribut 3.1 *process definition* termasuk dalam kriteria *fully*

achieved (tercapai optimal) sehingga penilaian dapat dilanjutkan ke level berikutnya yaitu (PA) 3.2 *Process Deployment*.

DAFTAR PUSTAKA

[1] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan *Capability* Maturity Model Integration (CMMI)," J Sistem Informasi Bisnis., vol. 01, 2019.

[2] R. Moeller," Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL," Canada: John Wiley & Sons Inc, 2013.

[3] J. Selig," Implementing Effective IT Governance and IT Management," Amersfoort: Van Haren Publishing, 2015.

[4] Yi Wang, Si Shi, Saggi Nevo, Shaorui Li, and Yang Chen," The interaction effect of IT assets and IT management on firmperformance: A systems perspective," International Journal of Information Management, pp. 580-593, 2015.

[5] M. Hassanzadeh, N. Jahangiri, and B. Brewster, "A Conceptual Framework for Information Security Awareness, Assessment, and Training," in Emerging Trends in ICT Security, 2014, pp. 99 – 109.

[6] Symantec, "Internet Security Threat Report," vol. 19, p. 98, 2014.

[7] ISACA," A Business Framework for the Governance and Management of Enterprise IT," USA: IT Governance Institute, 2012.

[8] D. Firmansyah, "Pengukuran kapabilitas pengelolaan sistem informasi sub *domain* deliver, service, support 01 menggunakan framework Cobit 5 Studi Kasus : Politeknik Komputer Niaga LPKIA Bandung," in Konferensi Nasional Sistem & Informatika, pp. 689–695, 2015.

[9] *http://diskominfo.karawangkab.go.id/artikel/selayang-pandang*