ISO 27001 Sebagai Metode Alternatif Bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan Untuk Diterapkan di Arsip Nasional RI)

Dicky Rutanaji [1], Sri Suning Kusumawardani [2], Wing Wahyu Winarno [3]

[1.]Mahasiswa, Jurusan Teknik Elektro dan Teknologi Informasi
[2,3] Dosen, Jurusan Teknik Elektro dan Teknologi Informasi
Universitas Gadjah mada
Jl. Grafika no.2 Kampus UGM 55281, Yogyakarta, Indonesia
[1)]dicky.rutanaji@mail.ugm.ac.id, [2)]suning@ugm.ac.id [3)]wing@mail.ugm.ac.id

Abstrak

Seri ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu confidentiality, integrity dan availability. Adanya tata kelola data pemerintahan yang efisien, transparan, inovatif dan patisipatif dalam hal ini keamanan data dan informasi akan memiliki peran penting dalam mewujudkan penyelenggaraan pemerintahan yang baik dan bersih. Oleh karena itu kemampuan untuk menyediakan informasi secara cepat dan akurat merupakan hal yang esensial. Salah satu bentuk dukungan dan penyelenggaraan keamanan informasi adalah dengan adanya tata kelola keamanan informasi (Information Security Governance) bagi pemerintahan. Paper ini dimaksudkan untuk menunjukkan kelebihan ISO 27001 sebagai sebuah metode yang paling cocok (fit) untuk digunakan dalam perancangan tata kelola keamanan informasi arsip digital berbasis komputasi awan di lingkungan Arsip Nasional RI.

Kata Kunci: tata kelola, keamanan informasi, ISO 27001, komputasi awan

1. Pendahuluan

Isu keamanan data dan informasi pada era Teknologi Informasi dan Komunikasi (TIK) ini sangat penting. Adapun kerentanan dalam hal pertukaran informasi telah meningkat menjadi ancaman yang lebih luas, sehingga keamanan informasi kini menjadi masalah yang mendasar untuk pemerintahan. [1]

Berdasarkan data dari Government Computer Security Incident Response Team (Govt – CSIRT), terjadi tren peningkatan ancaman terhadap keamanan informasi di pemerintahan yang paling sering terjadi yaitu antara lain web defacement, disusul dengan malware, spam,ip brute force, phising dan lain-lain.[2]

Hal ini sangat membahayakan bagi pemerintah yang seharusnya menjadi lembaga yang terpercaya khususnya dalam hal ini Arsip Nasional RI dalam melakukan tugasnya yaitu menyampaikan informasi pemerintah yang autentik dan utuh kepada masyarakat. [3]

Keamanan informasi merupakan tindakan melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, teliti, inspeksi, rekaman atau kehancuran[4]

Di lingkungan Arsip Nasional sendiri saat ini terdapat sistem informasi yang digunakan, baik itu yang sudah digunakan maupun masih tahap pengembangan ke arah komputasi awan yang di dalamnya berisi arsip digital baik itu bersifat rahasia dan terbuka untuk masyarakat. Dan semua sistem informasi yang ada tidak luput dari berbagai risiko dan ancaman yang ada terkait dengan keamanan informasinya.

Akan tetapi sampai dengan saat ini di lingkungan Arsip Nasional RI masih belum ada kebijakan secara spesifik mengatur berkaitan dengan keamanan informasi arsip digital tersebut. Sehingga resiko terjadinya kehilangan integritas, kerahasiaan, dan ketersediaan dari sebuah informasi dari asip digital itu sendiri akan sangat berpengaruh ke dalam pelaksanaan tugas dan fungsi Arsip Nasional RI sebagai Lembaga Kearsipan Nasional.

Salah satu bentuk dukungan dan penyelenggaraan keamanan informasi adalah dengan adanya tata kelola keamanan informasi (Information Security Governance) agar risiko keamanan informasi dapat dihindari atau dikurangi.

Dewasa ini terdapat beberapa metode dan standar yang bisa digunakan untuk membuat tata kelola

keamanan informasi. Paper ini dimaksudkan untuk menunjukkan kelebihan ISO 27001 sebagai sebuah metode yang paling sesuai digunakan dalam perancangan tata kelola keamanan informasi arsip digital berbasis komputasi awan di lingkungan Arsip Nasional RI.

2. Metode

Metode dalam penelitian ilmiah harus dilakukan teknik penyusunan yang sistematis untuk memudahkan langkah-langkah yang akan diambil. Begitu pula yang dilakukan penulis dalam penelitian ini, langkah pertama yaitu dengan melakukan studi literatur pada jurnal ilmiah, thesis, artikel laporan penelitian, dan situs-situs di internet yang membahas tentang ISO 27001 dan keamanan informasi. Adapun tujuan dari metode penelitian studi literatur ini akan digunakan untuk memperkuat permasalahan serta sebagai dasar teori dalam melakukan studi dan juga menjadi dasar untuk melakukan perancangan tata kelola keamanan informasi berbasis komputasi awan.

2.1 Metode Pengumpulan Data

Adapun data sekunder yang dibutuhkan untuk dapat menyelesaikan penelitian ini adalah:

- ISO 27001
- Jurnal terkait dengan tata kelola keamanan informasi, ISO 27001 dan komputasi awan

2.2 Metode Analisis Data

Data-data yang sudah diperoleh kemudian dianalisis dengan metode analisis deskriptif. Metode analisis deskriptif dilakukan dengan cara mendeskripsikan fakta-fakta yang kemudian disusul dengan analisis, tidak semata-mata menguraikan, melainkan juga memberikan pemahaman dan penjelasan secukupnya.

3. Hasil dan Pembahasan

3.1. Pengertian Tata Kelola

Pengertian Tata Kelola telah dikemukakan oleh beberapa ahli, dan dirangkum oleh Paim dan Flexa dalam *Process Governance: Definition and* Framework[5] adalah sebagai berikut:

a. Tata kelola sebagai instrument untuk menjamin bahwa proses, desain dan strategi bekerja dengan baik serta digunakan untuk memastikan adanya keselarasan antara ketiganya.
b. Tata kelola sebagai kebutuhan untuk memastikan koordinasi antara proses inisiatif oleh unit-unit fungsional uyang berbeda dan untuk menghilangkan ketidakselarasan antara strategi organisasi dan proses.
c. Tata kelola digunakan untuk mendefinisikan seperangkat aturan yang mengatur bagaimana sebuah organisasi harus melakukan fungsi bisnis yang spesifik.

Dari 3 (tiga) definisi di atas dapat disimpulkan bahwa tata kelola mempunyai tugas memberikan panduan dalam proses manajemen dengan tujuan secara menyeluruh oleh peraturan dan instrumen yang selaras dengan tujuan organisasi.

3.2. Keamanan Informasi

Keamanan informasi merupakan suatu usaha pencegahan atas serangan untuk mendapatkan sesuatu dari sistem informasi baik melalui akses yang tidak semestinya maupun penggunaan yang tidak semestinya[6]. Dalam keamanan informasi terdapat empat aspek utama[4], yaitu:

a. ***Confidentiality*:** merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses informasi tersebut.
b. ***Integrity*:** keaslian informasi yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
c. ***Authentication*:** agar penerima informasi dapat memastikan keaslian informasi tersebut datang dari orang yang dimintai informasi.
d. ***Avability*:** Informasi yang berada pada sistem jaringan dapat tersedia pada waktu kapanpun ketika dibutuhkan.

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang berupa kebijakan (*policy*), pedoman kerja (*guidance work* atau SOP), struktur organisasi hingga perangkat lunak

Didalam keamanan informasi terdapat berbagai macam risiko yang akan dihadapi baik itu dari berbagai sisi yaitu internal, eksternal, alamiah dan alam seperti bencana alam seperti banjir, kebakaran, dan lain-lain.

Salah satu contoh skandal adanya kebocoran informasi yang sudah pernah ada yaitu adanya skandal panama paper. Panama paper merupakan salah satu kebocoran dokumen finansial terbesar dalam sejarah mengguncang perhatian global. Kebocoran itu berasal dari dokumen firma hukum Mossack Fonseca yang berbasis di Panama sehingga disebut sebagai "Panama Papers". Sedikitnya 140 politisi, termasuk 12 pemimpin dan mantan pemimpin negara, selebritas, dan bintang olahraga serta pengusaha di Indonesia disebut dalam dokumen yang mengungkap aneka dugaan praktik skandal keuangan rahasia.

3.3. Tata Kelola Keamanan Informasi

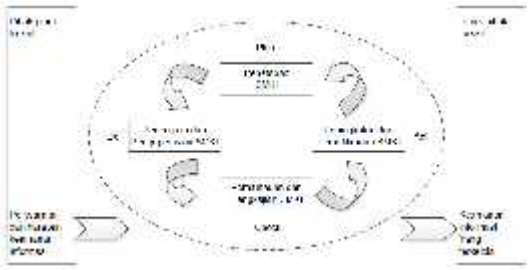
Dalam sebuah tata kelola TI, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TI akan terganggu jika informasi sebagai salah satu objek utama tata kelola TI mengalami masalah keamanan informasi yang menyangkut kerahasiaan

(*confidentality*), keutuhan (*integrity*), autetik (*Authentication*), dan ketersediaan (*availability*). [7].

3.4. Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) adalah cara untuk melindungi dan mengelola informasi berdasarkan pendekatan risiko bisnis yang sistematis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara, dan meningkatkan keamanan informasi. SMKI adalah sebuah pendekatan organisasi untuk keamanan informasi. SMKI menyediakan pendekatan sistematik dalam mengatur informasi yang sensitif agar dapat memproteksinya, dimana SMKI ini meliputi pegawai, proses-proses dan sistem informasi itu sendiri [8].

SMKI digunakan untuk memastikan bahwa semua daya upaya terkoordinasi untuk mencapai keamanan yang maksimal. SMKI mengadopsi siklus model PDCA sebagai metode evaluasi, perlindungan dan dokumentasi serta revisi, dengan prinsip pentingnya yaitu *Plan* (Perencanaan) – *Do* (Mengerjakan) – *Check* (Pemeriksaan) – *Act* (Pelaksanaan). Proses dalam SMKI disusun berdasarkan resiko pendekatan bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitor dan meninjau ulang (*Check*) serta memelihara dan meningkatkan atau mengembangkan (*Act*) [9].



Gambar 1. Model PDCA yang diterapkan untuk proses SMKI
(International Organization for Standardization 27001)

3.5. ISO/IEC 27001:2013

SNI ISO/IEC 27001 yang diterbitkan tahun 2013 dan merupakan revisi dari SNI ISO/IEC 27001:2009, Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan.

Dalam SNI ISO/IEC 27001:2013 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan [10].

Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (*review*), pemeliharaan dan peningkatan suatu SMKI. Pendekatan proses mendorong pengguna menekankan pentingnya:

a) Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi
b) Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan
c) Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
d) Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.

Didalam ISO 27001:2013 terdapat 14 (empat belas) area pengamanan informasi [11] yaitu:

a. Kebijakan keamanan informasi, mengarahkan visi dan misi manajemen agar kelangsungan organisasi dipertahankan dengan mengamankan dan menjaga integritas data dan informasi penting dari organisasi
b. Keamanan sumber daya manusia, upaya pengurangan resiko dari penyalahgunaan fungsi dan wewenang akibat kesalahan manusia, manipulasi data dalam pengoperasian aplikasi atau sistem.
c. Manajemen aset, memberikan perlindungan terhadap aset organisasi berupa aset informasi berdasarkan tingkat perlindungan yang berbeda
d. Mengakses kontrol dan mengelola akses pengguna, mengendalikan /membatasi akses user terhadap informasi dengan cara mengatur kewenangannya, termasuk pengendalian secara *mobile-computing* atau *tele-networking*
e. Teknologi kriptografi, melindungi kerahasiaan, keaslian atau integritas informasi dengan cara kriptografi
f. Keamanan fisik, mencegah kehilangan dari/atau kerusakan data yang diakibatkan oleh lingkungan secara fisik, termasuk bencana alam dan pencurian data yang tersimpan dalam media penyimpanan atau fasilitas penyimpanan informasi yang lain.
g. Keamanan operasional, memelihara keamanan informasi secara global, memelihara dan menjaga keutuhan sistem informasi terhadap ancaman pihak eksternal dan pihak ketiga.
h. Mengamankan komunikasi dan transfer data, memastikan bahwa keamanan media komunikasi, teknologi komunikasi beserta

isinya, serta kemampuan untuk memanfaatkan untuk mencapai tujuan organisasi.

i. **Akuisisi, pengembangan, dan dukungan sistem informasi yang aman**, memastikan bahwa sistem informasi maupun aplikasi yang baru saja diimplementasikan mampu bersinergi melalui verifikasi dan validasi.
j. **Keamanan untuk pemasok dan pihak ketiga**, menerapkan dan memelihara tingkat keamanan informasi dan pelayanan jasa yang sesuai dengan perjanjian pelayanan jasa pihak ketiga.
k. **Manajemen Insiden**, menyangkut ketersediaan layanan atau gangguan karena penyusupan dan pengubahan informasi dari yang tidak berwenang.
l. **Kesinambungan bisnis / pemulihan bencana**, untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagagalan utama sistem informasi atau bencana alam dan untuk menjamin keberlanjutannya secara tepat waktu.
m. **Kepatuhan,** memastikan implementasi kebijakan keamanan selaras dengan peraturan perundang-undangan yang berlaku.

3.6. Keamanan Data di Komputasi Awan

Pemanfaatan penyimpanan data secara *cloud* memberikan media penyimpanan yang cukup luas, disini anda bisa menggunakannya untuk menyimpan berbagai keperluan seperti dokumen, presentasi, foto, atau video. Tidak hanya dari piranti yang dipakai, kita bisa bebas mengakses data yang ada pada penyimpanan *cloud* melalui perangkat lain karena kini aplikasi *cloud* sudah menyebar diberbagai sistem operasi dari windows, linux, ios, hingga mobile.

Beberapa poin penting dalam proses pengamanan data di komputasi awan [12] antara lain:

a. Proteksi Data
   Ketika kita sudah memutuskan untuk adopsi atau migrasi data ke *cloud*, yang yang diperhatikan adalah bagaimana penyedia layanan *cloud* memberikan proteksi terhadap data kita. Dengan metode apa mereka melakukan proteksi sehingga kita yakin data aman, selain itu lokasi penyimpanan data juga adalah pertimbangan penting dimana ini hubungannya dengan Data Center. Dipastikan data center yang mereka buat sudah tersertifikasi/teraudit, misalnya lokasi bebas gempa, standar sumber daya listrik 3 lapis dll.
b. Kontrol Keamanan
   Setelah data kita betul-betul terproteksi, selanjutnya adalah bagaimana keamanan dari akses terhadap data kita (role), bagaimana prosedurnya sehingga hanya orang-orang yang berhak saja yang bisa akses data kita. Disini termasuk akses para pekerja/karyawan di penyedia layanan terhadap data kita.
c. Kepatuhan
   Standar yang diterapkan pada penyedia layanan komputasi awan, misalnya untuk keamanan data menggunakan ISO/IEC 27001:2013, untuk penyediaan layanan memakai ITIL, COBIT, Cloud Security Alliance, termasuk regulasi internasioanl dan pemerintah. Sehingga jika ada pelanggaran akan mudah dalam penyelesaian
d. Multi tenant
   Salah satu sifat komputasi awan adalah *resource sharing*, nah bagaimana ketika ada penyewa lain terdapat melakukan kecurangan atau bocor, apa imbasnya terhadap data kita disana, ini harus dipertimbangkan. Karena secara fisikal, data kita bisa jadi ada dalam satu media fisik yang sama dengan yang lain.
e. Tata Kelola Keamanan
   Ini lebih kepada tata kelola kebijakan dari penyedia layanan atau kita sebagai pemakai layanan, harus dijabarkan dan tata kelola-nya memakai apa harus didefinisikan disini.

3.7. Perbandingan COBIT, ITIL, dan ISO 27001

COBIT, ITIL, dan ISO 27001 sering sekali digunakan dalam pembuatan model tata kelola TI dalam sebuah organisasi.

a. COBIT

COBIT adalah kerangka kerja manajemen risiko teknologi informasi yang dibuat oleh Sistem Informasi Audit dan Control Association & Foundation (ISACA) dan IT Governance Institute (ITGI). COBIT menyediakan teknologi informasi yang diterima mengontrol sasaran set dalam rangka meningkatkan manfaat menggunakan teknologi informasi serta mengembangkan dan mengendalikan tata kelola yang sesuai untuk teknologi informasi bagi manajer teknologi informasi, auditor dan pengguna [13]. COBIT terdiri dari empat domain utama:

- Perencanaan dan Organisasi
- Akuisisi dan Implementasi
- Pengiriman dan Dukungan
- Pemantauan dan evaluasi

COBIT mengasosiasikan dengan 34 proses teknologi informasi dengan kriteria dan sumber informasi berikut:

- Kriteria Informasi: Khasiat, efisiensi, kerahasiaan, integritas, kontinuitas, kompatibilitas, dan kehandalan.
- Sumber informasi: Sumber daya manusia, sistem implementasi, teknologi, lingkungan fisik, dan data.

b. ITIL

Di dalam ITIL tersedia secara rinci dan struktural contoh praktek terbaik dalam mengelola layanan

teknologi informasi. ITIL adalah proses dan metode perpustakaan di mana proses infrastruktur TI dan layanan dijelaskan dan standar yang ditetapkan mengingat contoh praktek terbaik yang tersedia. ITIL mengedepankan proses dan metode yang tepat dalam rangka memberikan layanan TI secara keseluruhan pada kualitas yang maksimal, ketertiban dan kontinuitas, untuk memastikan harmonisasi maksimum antara layanan TI dan target bisnis lembaga dan untuk memenuhi harapan pelanggan pada tingkat tertinggi. Kami bisa daftar alasan untuk penerimaan di seluruh dunia dari ITIL sebagai standar sebagai berikut [13]:

- Ini tersedia untuk penggunaan umum
- Ini terdiri dari praktek-praktek terbaik
- Ini adalah standar de facto
- Hal ini menyajikan pendekatan kualitas

c. ISO 27001

Standar ISO 27001 adalah sebuah standar keamanan seri ISO 27000 merupakan panduan referensi mendasar dalam meningkatkan kesadaran pengguna, mengurangi risiko keamanan dan menentukan langkah-langkah yang harus diambil ketika celah keamanan yang ditemukan [13].

ISO 27001 adalah standar yang menjelaskan konsep yang berkaitan dengan informasi dasar mengenai manajemen keamanan informasi.

Tabel 1: Perbandingan COBIT, ITIL dan ISO 27001.

Area	COBIT	ITIL	ISO27001
Function	Mapping IT Process	Mapping IT Service Level Management	Information Security Framework
Area	34 Processes and 4 Domains	9 Processes	14 Domains
Issuer	ISACA	OGC	ISO Board
Implementation	Information System Audit	Manage Service Level	Compliance with security standards
Consultant	Accounting Company, IT Consulting Company	IT Consulting Company	IT Consulting Company, Security Company, Network Consultant

Sumber: Radovanovic, Dalibor, et al. "Analysis of methodology for it governance and information systems audit." 6th International Scientific Conference, ISSN. 2010)

Di tabel atas di jelaskan bahwa COBIT menyediakan praktik dan alat terbaik untuk pemantauan dan memetakan proses TI sementara ITIL bertujuan memetakan manajemen tingkat layanan TI dan ISO27001 memberikan panduan untuk penerapan sebuah kerangka keamanan informasi standar.

COBIT terdiri dari 4 domain dan 34 proses yang diperlukan untuk pelaksanaan audit sistem informasi sedangkan ITIL mencakup total 9 proses dan memungkinkan pelaksanaan manajemen tingkat layanan TI dengan fokus pada pencapaian efektivitas bisnis dan efisiensi dalam pengelolaan layanan TI. Untuk ISO 27001 sendiri terdiri dari 14 domain dan sejak awal dibuat standar ini mempunyai fokus lebih kearah framework keamanan informasi secara lebih mendalam dari sudut pandang pandang sempit.

4. Kesimpulan

Dengan adanya tata kelola keamanan informasi yang baik, maka diharapkan organisasi dapat memprediksi resiko-resiko yang muncul akibat penyalahgunaan data dan informasi sehingga dapat menghindari atau mengurangi resiko yang ungkin dapat terjadi seperti kebocoran/hilangnya integritas, kerahasiaan, dan ketersediaan dari sebuah informasi itu sendiri. Standar ISO/IEC 27001 adalah sebuah standar yang sangat ideal untuk melakukan pembuatan tata kelola keamanan informasi di sebuah organisasi. ISO/IEC 27000 dapat disesuaikan dengan kebutuhan yang diperlukan untuk mencapai sasaran keamanan informasi organisasi. Dan Apabila seluruh proses dalam COBITISO 27001 dikelola dengan baik, maka akan menghasilkan tata kelola keamanan informasi yang tepat.. Dalam lingkungan suatu organisasi pemerintahan seperti Arsip Nasional RI, ISO/IEC 27001 layak dijadikan sebagai metode yang paling cocok untuk perancangan tata kelola keamanan informasi berbasis komputasi awan.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada keluarga yang tidak henti-hentinya memberikan dukungan dan doa, pada dosen pembimbing serta dosen pengajar, para pegawai dan staff Departemen teknik elektro dan teknik Informatika universitas Gadjah Mada, teman-teman pasca sarjana *Chief Information Officer* tahun angkatan 2016, rekan-rekan pegawai Arsip Nasional RI serta para pihak yang tidak dapat disebutkan satu persatu.

Daftar Pustaka

[1] M. Hassanzadeh, N. Jahangiri, and B. Brewster, "A Conceptual Framework for Information Security Awareness, Assessment, and Training," in *Emerging Trends in ICT Security*, 1st ed., B. Akhgar and H. R. Arabnia, Eds. 2014, pp. 99 – 109.

[2] Kominfo.go.id, "Ancaman Cyber Attack dan Urgensi Keamanan Informasi Nasional",https://kominfo.go.id/index.php/content/detail/3479/Siaran+Pers+No_+83_PIH_KOMINFO_11_2013+tentang+Ancaman+Cyber+Attack+dan+Urgensi+Keamanan+Infor

masi+Nasional/0/siaran_pers (diakses 16 November 2017).
[3] "Undang-Undang Nomor 43 Tahun 2009 Tentang Kearsipan," 2009
[4] Simson Garfinkel, "*PGP: Pretty Good Privacy*," O'Reilly & Associates, Inc., 1995
[5] Paim, Rafael, and Raquel Flexa. "*Process Governance: Definitions and Framework, Part 1*." BPTrends, November (2011).
[6] Rahardjo, Budi. "Keamanan Sistem Informasi Berbasis Internet." PT Insan Komunikasi Indonesia, Bandung (2002).
[7]
[8] Triantono, H, Kebijakan keamanan dengan Standar BS 779/ISO 17799 pada Sistem Manajemen Keamanan Informasi Organisasi. Paper Seminar Nasional Aplikasi Teknologi Informasi, Yogyakarta, Universitas Islam Indonesia, 2007
[9] Sarno, R & Iffano, Sistem Manajemen Keamanan Informasi, Surabaya, Percetakan ITS Press,2009
[10] Kementerian Komunikasi dan Informatika Republik Indonesia, Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, 2011
[11] SN ISO 27001:2013
[12]
[13] Ozdemir, Yavuz, et al. "EVALUATION AND COMPARISON OF COBIT, ITIL AND ISO27K1/2 STANDARDS WITHIN THE FRAMEWORK OF INFORMATION SECURITY."