PEMBUATAN PANDUAN TATA KELOLA PADA BIDANG KEAMANAN INFORMASI DAN PEMULIHAN BENCANA BERBASIS COBIT 4.1 DAN ISO 27002

Lailatul Fitriana R, Bambang Setiawan, Andre Parvian A.
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111 Indonesia
lailatul.fitriana@gmail.com, setiawan@is.its.ac.id, parvian.aristio@gmail.com

Abstrak

Pemanfaatan Teknologi Informasi (TI) dalam mendukung terselenggaranya pelayanan yang optimal menjadi kebutuhan utama organisasi saat ini, khususnya pada Kementerian Koordinator Politik, Hukum, dan Keamanan Jakarta. Akan tetapi, jaminan pengelolaan layanan yang baik dirasa belum maksimal tanpa adanya penggunaan sebuah standar. Dari sisi lain, pemerintah sebagai badan regulasi menetapkan peraturan akan terwujudnya Good Corporate Governance (GCG). Pengimplementasian GCG ini dititik beratkan pada pemamfaatan teknologi informasinya yang diharapkan tidak hanya kualitas layanannya saja yang meningkat tetapi juga adanya penjaminan keamanan yang sudah di standarkan. Akan tetapi, penggunaan sebuah standard dirasa belum maksimal melihat cakupan yang disediakan kurang luas sehingga diadakannya penggabungan beberapa standar dengan harapan standar-standar tersebut saling melengkapi. Pembuatan alat ukur sebagai penilaian implementasi manajemen keamanan dalam penelitian ini dimulai dari memetakan kebutuhan teknologi informasi berdasarkan indeks Keamanan Informasi (KAMI) yang mengarah pada ISO 27002, yang selanjutnya kebutuhan manajemennya dapat diukur menggunakan standar COBIT 4.1 dan disesuaikan dengan ISO 27001 dan ISO 27002 untuk memaksimalkan manajemen keamanan teknologi informasi di Divisi TI Kementerian XYZ. Dengan adanya tahapan proses tersebut dihasilkan Dokumen Tata Kelola TI pada bidang Keamanan dan Pemulihan Bencana TI dan Aplikasi monitoring untuk mengontrol kepatuhan pada dokumen tata kelola TI.

***Kata Kunci**: Tata Kelola IT, keamanan teknologi informasi, COBIT 4.1, ISO 27002, Good Corporate Governance.*

Abstract

Utilization of Information Technology (IT) services in support of the implementation of the optimal become the primary needs of today's organizations, especially at the Coordinating Ministry for Political, Legal and Security Affairs in Jakarta. However, collateral management services deemed not good without the use of a maximum of standard. On the other hand, as a government regulatory agency sets the rules will be the realization of Good Corporate Governance (GCG). GCG implementation of this emphasis on the utilization of information technology is expected to not only improve the quality of its service, but also the existence of a security guaranteeing that already standardize. However, the use of a standard deemed not see the maximum coverage provided less extensive so that the holding of merging some of the standards with the expectations of standards are complementary. Making a measuring tool as assessment of security management implementation in this research starts from the mapping needs of information technology based indexes Information Security (KAMI) which leads to ISO 27002, which further management needs can be measured using standard and customized COBIT 4.1 with ISO 27001 and ISO 27002 security management technology to maximize the information in the IT Division of the Ministry of XYZ. With the stages of the process of IT Governance Documents produced in the field of IT Security and Disaster Recovery and Application monitoring for compliance control in IT governance documents.

***Keywords**: IT governance, information technology security, COBIT 4.1, ISO 27002, Good Corporate Governance.*

1. PENDAHULUAN

Kementerian Koordinator Politik, Hukum, dan Keamanan Jakarta merupakan sebuah kementerian yang mengkoordinasi kementerian-kementerian yang lainnya [5]. Organisasi pada saat ini melakukan transformasi dan peningkatan pelayanan dengan pemanfaatan TI dalam proses bisnisnya [3]. Untuk memastikan penggunaan TI tersebut benar-benar mendukung tujuan penyelenggaraan pemerintahan, dengan memperhatikan efisiensi

penggunaan sumber daya dan pengelolaan risiko terkait dengannya, diperlukan *Good Corporate Governance (GCG)* terkait dengan TI, yang dalam dokumen ini disebut sebagai Tata Kelola TI.

Dalam upaya tersebut dirasa belum maksimal tanpa adanya pengimplementasian keamanan yang terencana dan terarah dengan beberapa standar keamanan. Pengimplementasian standar keamanan ini bertujuan untuk membantu manajemen mengetahui sejauh mana fungsi dan kinerja layanan keamanan dan pengelolaan jika terjadi bencana dapat ditangani, sehingga dapat mendukung proses bisnis dan strategi organisasi.Sejauh ini di Kedeputian VII yang menangani tentang Teknologi Informasi seluruh Divisi TI Kementerian XYZ penggunaan satu buah standar dirasa kurang luas cakupannya untuk memenuhi seluruh kebutuhan manajemen keamanan dan pengendalian bencana TI.

Berdasarkan hal tersebut, maka penelitian ini bertujuan menggabungkan beberapa standar pengelolaan dan keamanan serta pemulihan bencana yang berkaitan dengan TI dalam sebuah *panduan*tata kelola.Pembuatan *panduan*ini menggunakan standar ISO 27000 terutama ISO 27001 dan 27002 sebagai manajemen keamanan informasi. Konsep dan teknik pengelola serta operasi TI yang nantinya diukur berdasarkan COBIT 4.1.

Pelaksanaan penyusunan tata kelola ini adalah terkait dengan pelaksanaan penerapan Panduan Tata Kelola Keamanan dan Pemulihan Bencana TI berupa form *checklist* yang dilakukan dalam tahap preventif, detektif, dan korektif. Dari kajian lanjutan ini akan didapatkan informasi apakah Panduan tata kelola yang diterapkan berjalan baik atau tidak, dan apakah panduan tata kelola yang diterapkan dapat benar-benar membantu dalam proses monitoring penerapan tata kelola keamanan dan pemulihan bencana TI di Divisi TI Kementerian XYZ.

2. TINJAUAN PUSTAKA

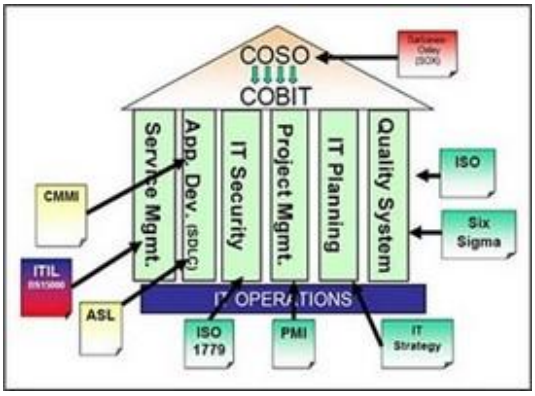
2.1. Keamanan Informasi

Keamanan informasi adalah bentuk usaha untuk melindungi segala aset informasi yang dimiliki baik itu berupa *hardware* ataupun *software*. Usaha perlindungan ini memiliki tujuan untuk memastikan keberlanjutan proses bisnis, meminimalkan ancaman ataupun resiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis [6].

Keamanan informasi terkait erat dengan fasilitas pemrosesan informasi (Fasilitas Informasi) yang meliputi dokumen, perangkat keras, perangkat lunak, infrastruktur dan bangunan yang melindunginnya [1][5][7]. Hal tersebut seharusnya direncanakan dan dikoordinasikan dengan baik agar dapat melindungi sumber daya (resource) dan investasi lainnya [2]. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi esensial bagia suatau organisasi, baik yang berupa organisasi komersial (instansi), perguruan tinggi, maupun lembaga pemerintahan maupun individual (pribadi).

2.2. Tata Kelola Teknologi Informasi

Tata Kelola Teknologi Informasi didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengontrol instansi agar tujuan bisnis dapat tercapai melalui penambahan nilai sekaligus terkait dengan pengelolaan proses TI [4]. Tidak hanya pengelolaan proses, tetapi juga memastikan bahwa proses tersebut telah dipenuhi oleh sumber daya TI yang memberikan dukungan secara optimal terhadap pemenuhan tujuan bisnis (IT Governance Institute, 2007). *Committee of Sponsoring Organizations of the Treadway Commission,* atau disingkat COSO, telah menyusun suatu definisi umum untuk pengendalian, standar, dan kriteria internal yang dapat digunakan instansi untuk menilai sistem pengendalian mereka. Sedangkan, di dunia informasi dan informasi, dibangunlah juga sebuah framework untuk mengontrol kegiatan internal dalam pengelolaannya bernama *Kontrol Objective for Information and related Technology,* disingkat COBIT yang di turunkan dari COSO.Adapun fokus utama pengerjaan penelitian ini adalah tata kelola teknologi informasi pada *IT Security*.



Gambar 11 Acuan tata kelola TI

2.3 Keterkaitan COBIT 4.1, ISO 27001, dan ISO 27002

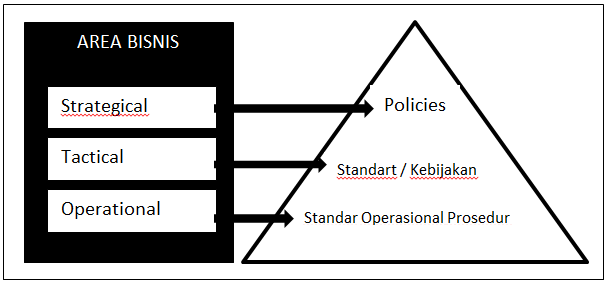
Pada ISO/IEC 27001 dan 27002 telah memiliki struktur dalam penerapan untuk menjamin keamanan organisasi secara keseluruhan di semua tingkat. Masalah administrasi dan manajemen yang tidak dibahas dalam standar ISO/IEC 27001 dan 27002 ditangani oleh COBIT. Hal tersebut dimungkinkan karena ISO/IEC 27001 dan 27002 memiliki fitur untuk menjaga kerahasiaan, integritas dan ketersediaan informasi dalam organisasi. Ketersediaan informasi ini ditangani dalam COBIT dengan aspek kualitas, keahlian dan pemeliharaan TI. COBIT digunakan untuk mengevaluasi faktor penentu keberhasilan, metrik, indikator dan audit. Selain itu, standar ISO/IEC 27001 - 27002 sebagai pedoman pengelolaan TI dalam hubungan dengan masalah keamanan.

2.4 Bentuk Kontrol Tata Kelola

Sesuai dengan definisi tata kelola TI yang terdiri dari seperangkat sistem dengan tujuan untuk mengarahkan, mengelola, serta mengontrol penggunaan TI, maka pada poin ini akan dijelaskan sekilas mengenai jenis-jenis bentuk kontrol yang digunakan pada pembuatan penelitian ini.

Bentuk kontrol tersebut adalah kebijakan, SOP (*Standard OperatingProcedure*) dan instrument prosedur seperti formulir dan checklist. Berikut ini adalah gambar hirarki level bentuk kontrol yang disebutkan dengan level area bisnis:

- Kebijakan (*Policies*) adalah rangkaian konsep dan asas yang menjadi garis besar dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak. Kebijakan berisikan pernyataan tujuan, prinsip,dan garis besar pedoman untuk manajemen dalam usaha mencapai sasaran.
- Standar (*Standard*) adalah suatu norma atau aturan yang biasanya berupa suatu dokumen formal untuk menciptakan kriteria, metode, proses,dan pelaksanaan teknis yang seragam.
- SOP adalah serangkaian instruksi tertulis atau metode langkah demi langkah yang didokumentasikan mengenai bagaimana suatu proses harus dilaksanakan dan diselesaikan secara terperinci sertaoleh siapa dilakukan.



Gambar 12 Level bentuk kontrol berdasarkan level bisnis

Selain didasarkan pada area bisnis diatas, bentuk kontrol tersebut akan dibedakan ke dalam kelompok kategori kontrol. Kategori kontrol yang dimaksudkan adalah kategori kontrol: *preventive, detective,* dan *corrective* [10].

Tabel 3 Kategori Kontrol

Kontrol Preventif	Kontrol Detektif	Kontrol Korektif
Kontrol yang diterapkan untuk mencegah hasil-hasil	Kontrol yang dirancang untuk menemukan hasil-hasil yang	Kontrol yang dirancang untuk memastikan bahwa tindakan korektif diambil untuk

yang diharapkan sebelum terjadi	tidak diharapkan pada saa terjadinya	memperbaiki hal-hal yang tidak diharapkan atau untuk memastikan bahwa hal-hal tersebut tidak terulang

2.5 Risiko Teknologi Informasi

Sebuah konsekuensi positif akan memberikan kesempatan dan peluang, sedangkan konsekuensi yang negatif dapat menimbulkan ancaman. Risiko adalah suatu peristiwa atau keadaan dimasa depan yang secara signifikan dapat meningkatkan atau bahkan menghambat kemampuan organisasi untuk mencapai tujuan bisnis. [8]. Adalah sebagai berikut : Bencana alam, (banjir, gempa bumi, dll), Kebakaran, Pemadaman listrik, *Hardware* failure, Software failure, Pencurian data: *unauthorized access*, Modifikasi data, Gangguan pada jaringan network, Backup data failure, Pelanggaran terhadap kebijakan dan peraturan, *Human Error*, seperti: inadvertent data entry, *Cybercrime* (computer *hacking*), Terorisme, Kerusuhan sosial [9] . Dari 14 macam risiko teknologi informasi tersebut yang didefinisikan oleh COBIT dan ISO 27002, beberapa diantaranya merupakan risiko yang memiliki potensi untuk terjadi dan sesuai dengan kondisidi Divisi TI Kementerian XYZ.

1. Verifikasi dan Validasi

Validasi dokumen dengan metode *acceptance testing* melalui form evaluator yang ditujukan kepada Asisten Divisi TI mengenai ketepatan, kelengkapan, dan kejelasan struktur dokumen. Form evaluator tersebut bertujuan menanyakan persetujuan *key user* terhadap hasil luaran dari setiap tahapan,apakah telah sesuai dengan yang diharapkan oleh perusahaan. Persetujuan tersebut dijabarkan melalui pertanyaan- pertanyaan form evaluator yang membantu mengukur kesesuaian dokumen dengan kondisi yang diharapkan oleh studi kasus. Kebijakan Keamanan TI dari segi ketepatan dokumen, kelengkapan dokumen, dan kejelasan struktur serta informasi konten. Hasil dari validasi ini adalah *feedback* dari korespondensi melalui email dan hasil form evaluator. Dari hasil validasi tersebut akan diketahui apakah dokumen luaran dapat diterima dan dipahami untuk kemudian dilakukan oleh perusahaan dari sudut pandang TI yang diwakilkan oleh Asisten Divisi TI tersebut diatas.

3. METODE PENELITIAN

3.1. Pengumpulan Data

Mengumpulkan data terkait profil serta data mengenai proses bisnis yang ada pada Divisi TI Kementerian XYZ. Studi mengenai kondisi yang ada pada keamanan informasi di Divisi TI Kementerian XYZ saat ini terkait penerapan tata kelola keamanan informasi. Sedangkan disini penulis menggunakan teknik pengumpulan data berdasarkan survey langsung ke tempat studi kasus dan wawancara dengan pihak Divisi TI.

3.2. Analisis Kondisi Kekinian

Dari observasi dan wawancara yang telah dilakukan untuk mengetahui kondisi eksisting dari Divisi TI Kementerian XYZ, maka diperoleh hasil dari analisis sebagai berikut: Profil singkat, Struktur Divisi TI, Kondisi Operasional, serta identifikasi peran SDM yang terlibat.

3.3. Proses Analisis

1. Kajian Awal	2. Penyimpulan Hasil	3. Identifikasi Kebutuhan	4. Pembuatan Perangkat Tata Kelola	5. Kajian Lanjutan Pelaksanaan Penerapan
Mengetahui sejauh mana peran TI, serta metode yang digunakan	Penyimpulan seluruh proses awal	Kebutuhan akan adanya form dan aplikasi agar bisa lebih membantu Divisi TI dalam proses monitoring penerapan tata kelola keamanan TI yang sebelumnya tidak ada.	Perangkat panduan tata kelola keamanan TI nantinya dapat digunakan untuk memudahkan divisi TI, serta menilai kelayakan dari penerapan.	Yang diterapkan berjalan baik atau tidak, dan apakah panduan tata kelola yang diterapkan dapat benar-benar membantu dalam proses monitoring penerapan tata kelola

4. ANALISIS DAN PEMBAHASAN

4.1. Penilaian Risiko

Identifikasi risiko yang dapat mengancam aset TI Kementerian XYZ. Risiko yang dimaksudkan adalah berupa kejadian yang memiliki probabilitas untuk terjadi bahkan sering terjadi baik disebabkan oleh faktor yang berasal dari kondisi eksternal maupun kondisi internal perusahaan, yaitu bencana alam, gangguan fasilitas umum, sosial, dan operasional. Berdasarkan observasi dan wawancara yang dilakukan maka dapat diidentifikasikan sebanyak

14 risiko yang memiliki potensi mengancam aset-aset TI Kementerian XYZ.

Keluaran yang akan dihasilkan adalah daftar risiko-risikoTI yang mungkin terjadi berdasarkan COBIT 4.1, serta aksi mitigasi untuk meminimalisir risiko keamanan divisi TI. Berdasarkan daftar risiko yang terjadi di Divisi TI Kementerian XYZ, pada Tabel 2 adalah daftar risiko yang langsung diperoleh dari proses wawancara oleh Asisten divisi TI. Sehingga diperoleh data berdasarkan level risiko tinggi, rendah, dan sedang.

Tabel 14 Pemetaan Risiko Berdasarkan Level

Low	Medium	High
• *Network failure* • *Cybercrime* • Backupdata *failure* • Kesalahan dalam memperkerjakan staff • *Human/technicianerror* • Pelanggaran terhadap peraturan atau regulasi yang berlaku • *Hardware failure* • *Software failure* • *Memory full*	• Banjir • Gempa Bumi • Terorisme • Kerusuhan (riots)	• Infrastruktur Fisik • Kebakaran • Modifikasi dan pencurian data • Pemadaman Listrik

4.2. Pembuatan Dokumen Kebijakan Tata Kelola

Dari hasil pendefinisian bentuk-bentuk kontrol diatas,berikut ini adalah kerangka pertanyaan atau persoalan yang menjadi acuan dalam pembuatan bentuk kontrol terutama bentuk kontrol prosedur. Tujuan dari kerangka pertanyaan atas persoalan dibawah ini adalah melihat keterkaitan antara pemanfaatan bentuk kontrol (prosedur) dalam menyelesaikan suatu permasalahan prosesTI.

Bentuk kontrol tersebut di atas akan digunakan sebagai tindakan strategi pada fase waktu yang berbeda, yaitu strategi pencegahan untuk fase sebelum insiden terjadi, strategi penanganan pada saat insiden terjadi, dan strategi pemulihan untuk fase setelah insiden terjadi. Hasil contoh dari Kebijakan, SOP, dan Form Checklist. Hasil Penilaian Terhadap Risiko-risiko TI pada divisi TI Kementerian XYZ Berdasarkan Framework COBIT. Penilaian dan analisis risiko mengacu kepada tahapan-tahapan yang ada pada standar COBIT4.1 khusunya didomain *plan and organize* 9 yaitu *assess and analyze risk*. Secara garis besar, tahapan-tahapan tersebut antara lain adalah: identifikasi risiko, penilaian risiko, dan identifikasi aksi atau tindakan untuk mitigasi risiko. Dari semua kemungkinan risikoyang terdapat didalam standar COBIT, dalam tahapan identifikasi risiko,telah dihasilkan yaitu 14 risiko potensial yang sesuai dengan kondisi data center. Setelah itu, akan dilakukan analisis pada 14 risiko tersebut penyebab risiko, dampak dari risiko, dan ketersediaan kontrol untuk risiko. Dari indentifikasi yang dilakukan, akan terlihat mana saja risiko yang termasuk dalam kategori risiko tinggi, sedang,dan rendah. Selanjutnya adalah menentukan tindakan seperti apa yang seharusnya dilakukan untuk mengelola risiko. Hasil dari keseluruhan proses penilaian risiko, didokumentasikan pada bentuk kontrol yaitu dokumen kebijakan tata kelola keamanan dan pemulihan bencana TI. Pada dokumen tersebut telah dibagi bentuk kontrol berdasarkan pembagian bentuk kontrol, yang nantinya digunakan dalam pembuatan kebijakan, standar operasional prosedur (SOP), dan form checklist.

Untuk memudahkan pemantauan digunakanlah aplikasi dashboard yang mengadopsi perangkat lunak indeks keamanan informasi berbasis web.Perangkat lunak yang digunakan menggunakan bahasa pemograman PHP dan manajemen basis data MySQL. Aplikasi dashboard hanyalah sebagai alat bantu untuk memudahkan pemantauan.

No	Risiko	Penyebab Risiko		Bentuk Kontrol (Prosedur)
1.	Keamanan Fisik Infrastruktur	- *Hardware* (Perangkat Keras) untuk menjalankan sistem informasi - Terjadi kecelakaan pada *Brainware* (Orang/Pelaku)	KDR001	Kebijakan Keamanan Fisik Infrastruktur
			SDR001	SOP Pengamanan Fisik Infrastruktur
			SDR002	SOP Pemasangan dan pengamanan sistem Kabel
			SDR003	SOP Pengamanan data center
2.	Modifikasi dan Pencurian Data	Belum ada pengaturan tentang hak akses dan pelanggaran hak akses Belum ada klasifikasi database	KDR002	Kebijakan Pengendalian Hak Akses
			SDR004	SOP Pengendalian Hak Akses
3.	Kebakaran	Kelebihan beban listrik	SDR005	SOP Monitoring Data Center dan Media Penyimpanan TI
			SDR006	SOP Monitoring Infrastruktur Listrik
			KDR003	Kebijakan Penanganan Kebakaran
			SDR007	SOP Penangaanan Kebakaran
			SDR008	SOP penilaian Kerusakan Aset TI
			SDR009	SOP Backup data
			SDR010	SOP Pemulihan Aset TI akibat Kebakaran
		Konsleting listrik	KDR004	Kebijakan Data Center dan Media Penyimpanan TI
			KDR005	Kebijakan Backup data
			SDR005	SOP Monitoring Data Center dan Media Penyimpanan TI
			SDR009	SOP Backup data
			SDR002	SOP Pemasangan dan pengamanan Sistem Kabel
			SDR007	SOP Penangaanan Kebakaran
			SDR008	SOP Penilaian Kerusakan Aset TI
			SDR010	SOP Pemulihan Aset TI akibat Kebakaran
		Terjadi kebakaran pada baterai UPS	KDR006	Kebijakan Monitoring UPS/Genset

Gambar 13 Acuan Pembuatan Bentuk Kontrol

5. KESIMPULAN DAN SARAN

5.1. Simpulan

Penelitian ini menghasilkan Panduan Tata Kelola Keamanan dan Aplikasi Audit. Panduan meliputi proses pemantauan dan penanganan menggunakan 3(tiga) kontrol internal, yaitu preventif, detektif, dan korektif.

Panduan tata kelola keamanan yang dibuat digunakan untuk mempercepat proses pemulihan kegiatan operasional yang diakibatkan dari insiden, serta untuk meminimalkan risiko dari insiden. Dan aplikasi audit digunakan untuk memantau gangguan yang harus ditangani sesuai prioritas.

5.2. Saran

1. Sebagai lanjutan penelitian seharusnya, penulis menyadari bahwa perlunya pembuatan suatu tolok ukur sebagai acuan dalam tingkat keberhasilan monitoring yang telah dibuat. Dalam pembuatan tolok ukur dirasa masih banyak proses dan tahapan yang cukup banyak, proses tolok ukur tersebut dapat berupa *KeyPerformance Indicator* (KPI).
2. Dalam penelitian selanjutnya, dimungkinkan adanya pengujian simulasi dalam proses monitoring yang dibuat untuk mengetahui apakah standard yang dibuat berhasil meminimalkan risiko, mudah digunakan, dan relevan dengan kondisi serta kebutuhan perusahaan.
3. Melakukan penelitian lebih lanjut yang memfokuskan penelitian kepada lingkup Dampak Analisis Bisnis secara spesifik dan terstruktur agar perusahaan memiliki pemahaman serta pengetahuan yang lebih luas lagi mengenai dampak risikoTI terhadap bisnis.

6. DAFTAR PUSTAKA

[1] Riyanto Sarno, I. I. (2009). *Sistem Manajemen Keamanan Informasi* . Surabaya: ITSPress.
[2] Mattord, M. W. (2010). *Management Of Information System.* Course Technology CENGAGE Learning.
[3] Kadir, A. (2003). *Pengenalan Sistem Informasi.* Yogyakarta: Penerbit ANDI.

[4] Panduan Penerapan Tata Kelola KIPPPi, 2. (2012, Februari 18).
[5] Departemen Komunikasi dan Informatika RI, Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional.: Detiknas, 2007.
[6] Tipton, Harold F. and Krause, Micki , Information Security Management Handbook.: CRC Press LLC, Fifth Edition, 2004.
[7] Tim Direktorat Keamanan Informasi, Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik., 2011.
[8] Andrew Graham.(2009). Integrated Risk Management: Implementation Guide. Canada.
[9] COSO.(2004,September). Enterprise Risk Management: Integrated Framework.
[10] John Kramer. (2003). *The CISA Prep Guide: Mastering the Certified Information System Auditor Exam.* Canada: Bob Ipsen.