Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5

Mei Lenawati [1)], Wing Wahyu Winarno [2)], *Armadyah Amborowati* [3)]
Magister Teknik Informatika STMIK AMIKOM Yogyakarta [1)2)3)]
meilenawati@gmail.com

Abstract - PDAM XYZ is a service company for public water providers around XYZ . As a company that is already using the information system security information must be maintained. Information security governance is a solution approach that can minimize attack on information security.
The aim of the research is to establish information security governance based on the requirements of information security with ISO/IEC 27001:2013 standard and COBIT 5 framework approaches. The research use mixed method with concurrent embedded strategy, which combine qualitativ and quantitative method. The conclusion of the research is improvement of the level of the level of maturity on the part of the subscription, and rekomondasi governance at the extreme-value variables.
Keywords: governance, information security, ISO / IEC 27001: 2013, COBIT 5

Abstrak – PDAM XYZ adalah perusahaan jasa penyedia air bersih untuk masyarakat sekitar XYZ . Sebagai perusahaan yang sudah menggunakan sistem informasi maka keamanan informasi harus terjaga. Tata kelola keamanan informasi adalah salah satu pendekatan yang dapat meminimalkan serangan terhadap keamanan informasi.
Penelitian ini bertujuan untuk membuat tata kelola keamanan informasi sesuai dengan persyaratan SMKI ISO 27001:2013 dan kerangka kerja keamanan informasi COBIT 5. Penelitian menggunakan metode mixed method dengan strategi concurrent embedded, yaitu menggabungkan metode penelitian kualitatif dan kuantitatif. Penelitian ini menghasilkan beberapa keluaran yaitu model referensi proses; rekomendasi proses bisnis dan struktur organisasi; dan langkah penerapan tata kelolanya. Kesimpulan yang diambil dari penelitian ini yaitu perbaikan level tingkat kematanngan pada bagian langganan, dan rekomondasi tata kelola pada variabel yang bernilai ekstrim.
Kata kunci: tata kelola, kemanan informasi, ISO/IEC 27001:2013, COBIT 5

1. Latar Belakang

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).
Pada Tahun 2012, Margo Utomo melakukan penelitian dengan judul "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses berbasis ISO/IEC 27001:27005 Pada Kantor Pelayanan Perbendaharaan Surabaya I" dengan hasil Langkah praktis penerapan SMKI di organisasi. Tahun 2009, Ita Ernala Kaban melakukan penelitian dengan judul "Tata Kelola Teknologi Informasi ", dengan hasil Perbandingan antara standar dan kerangka kerja TI, COBIT mempunyai sprektrum proses TI yang lebih luas.
Pada tahun 2012, tim Korea University melakukan riset keamanan informasi dan menyatakan bahwa pengendalian keamanan dilakukan berdasarkan identifikasi risiko. Riset yang dilakukan tim JianZhu University menyatakan bahwa permasalahan sistem keamanan informasi dapat diatasi dengan penerapan manajemen resiko keamanan teknologi informasi dan pengendalian sistem informasi.
Kelemahan sekecil apapun pada sistem keamanan informasi dapat memberikan dampak negatif terhadap pencapaian tujuan organisasi secara luas. Oleh karena itu, pembahasan keamanan informasi yang menyeluruh dan terintegrasi sangat diperlukan untuk mengamankan pencapaian tujuan tersebut. Tata kelola keamanan informasi yang menyeluruh

sangat bermanfaat untuk pimpinan dan manajemen tingkat atas sebagai panduan dan pedoman dalam menerapkan keamanan informasi untuk organisasi baik organisasi publik, *non-profit* ataupun swasta. Salah satu instansi penyelenggara pelayanan publik adalah PDAM XYZ .

PDAM XYZ merupakan perusahaan jasa yang bergerak dibidang pelayanan masyarakat dalam hal penyedia air bersih. Pada Tahun 2016 PDAM XYZ mempunyai 36.000 pelanggan, dengan jumlah pelanggan yang cukup banyak dan masing-masing pelanggan mempunyai data yang tersimpan dalam server PDAM. Data pelanggan adalah data yang perlu dilindungi, jika tidak dilindungi data tersebut bisa dimanfaatkan oleh orang-orang tertentu dan dapat dipergunakan untuk kejahatan. Oleh karena itu PDAM mempunyai kewajiban untuk melindungi data pelangganya. Berdasarkan Observasi dan wawancara pada beberapa karywan PDAM XYZ , penulis menemukan beberapa permasalahan yang berkaitan dengan kemanan informasi, yaitu pada tahun 2011 PDAM harus mengeluarkan dana yang cukup besar dikarenakan server PDAM mengalami kebakaran, dan kehilangan semua datanya, server terbakar dikarenakan server dan ruang tidak sesuai dengan stadart kemanan, ruang server yang tidak terjaga suhu dan kelembapanya, serta komputer yang digunakan bukanlah komputer server yang semestinya. PDAM XYZ menggunakan komputer biasa dengan menambahkan beberapa harddisk dan dijakan sebagai komputer server. Komputer server dan client yang ada di PDAM tidak dilindungi dengan anti virus yang berbayar, dan server juga tidak dilengkapi dengan Firewall. Jika keadaan seperti itu dibiarkan dan semakin bertambahnya data PDAM tidak menutup kemungkinan hardisk akan terbakar. Selain masalah server, alat baca meter yang digunakan pada PDAM masih menggunakan sistem manual, yaitu petugas baca meter melihat angka yang tertera pada meteran air pelanggan kemudian menginputkanya pada HP yang sudah dilengkapi aplikasi Android untuk baca meter. Penginputan secara manual bisa berdampak data tidak akurat. PDAM perlu mengembangkan Aplikasi dengan sistem bardcode sehingga data yang diinputkan akurat dan langsung terhubung ke server.

Selain masalah-masalah di atas, berdasarkan peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi dan observasi yang telah dilakukan pada instansi, ditemukan adanya rencana instansi tersebut untuk meningkatkan sistem keamanan informasi sesuai dengan Standar Nasional Indonesia. Adanya rencana untuk meningkatkan keamanan informasi sesuai dengan (SNI) dan kondisi saat ini, maka penulis melakukan suatu penelitian yang berfokus pada kemanan informasi yang sesuai dengan standar SNI ISO/EIC 27001:2013 dan COBIT 5. Dari uraian latar belakang yang telah dijelaskan dan kesesuaian dengan masalah yang pernah terjadi dan kondisi saat ini pada PDAM XYZ , maka penulis melakukan penelitian yang berjudul "**TATA KELOLA KEAMANAN INFORMASI PADA PDAM MENGGUNAKAN ISO/IEC 27001:2013 DAN COBIT 5**". Penelitian ini berfokus pada bagian baca meter dan penyimpanan data.

Untuk mendukung optimalisasi tata kelola keamanan informasi, perlu dibuat rancangan model tata kelola keamanan informasi. Tata kelola dibuat berdasarkan proses bisnis perusahaan yang dianalisis menggunakan standar manajemen keamanan informasi SNI ISO/IEC 27001 dan kerangka kerja COBIT 5. ISO/IEC 27001:2013 merupakan standar internasional dalam menetapkan persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan Sistem Manajemen Keamanan Informasi dalam konteks organisasi secara berkesinambungan. COBIT 5 merupakan IT *governance framework* yang membantu manager untuk menjembatani perbedaan antara *control requirement,* isu teknis dan resiko bisnis. *Framework* ini berfokus pada cara memberikan informasi yang sesuai dengan kebutuhan bisnis.

2.a. Kajian Pustaka

Penelitian ini dilakukan berdasarkan tinjauan penelitian sebelumnya, Berikut ini ikhtisar beberapa penelitian terkait tentang tata kelola keamanan informasi dan sistem manajemen keamanan informasi.

Penelitian dari Farroh Sakinah 2014 berjudul "Indeks Penilaian Kematangan (Maturity) Manajemen Keamanan Layanan TI". Penelitian menggabungkan beberapa standar pengelolaan dan keamanan layanan yang dapat diukur pencapaian dan kesiapannya dalam sebuah indeks penilaian untuk membantu organisasi. mengetahu tingkat kematangan (maturity) manajemen keamanan layanan di organisasinya. Pembuatan indeks penilaian ini menggunakan standar ISO 27000 terutama ISO 27001 dan 27002 sebagai information security management. Kerangka ITIL digunakan untuk konsep dan teknik pengelola serta operasi teknologi informasi (TI) yang berdasarkan control objective dan pengukuran maturity model COBIT 4.1. Kaitanya

dengan penelitian berikutnya adalah sama-sama menggunakan standar ISO 27001 perbedaanya penelitian ini tidak menghasilkan rekomondasi tata kelola keamanan informasi.

Penelitian dari Ciptaningrum Dewi 2015 berjudul "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5". Penelitian bertujuan untuk mengetahui tingkat kapabilitas kemanan Sistem Informasi pada pemerintah kota Yogyakarta. Peneliti menggunakan COBIT 5 khususnya COBIT 5 for Information Security (untuk Keamanan Informasi) sebagai kerangka dan standar untuk melakukan audit keamanan SI. Hasil dari penelitian menunjukkan proses tingkat kapabilitas keamanan SI berada pada tingkat kapabilitas 1 Performed Process.

Penelitian dari Margo Utomo Tahun 2012 berjudul "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I". Salah satu tugas pokok KPPN Surabaya I adalah menyalurkan pembiayaan yang dibebankan pada Anggaran Pendapatan Belanja Negara (APBN). Transaksi-transaksi yang terjadi merupakan aset informasi yang dimiliki KPPN Surabaya I. Data transaksi-transaksi yang terjadi nantinya akan dijadikan laporan yang mencerminkan tingkat penyerapan APBN. Kontrol akses terhadap transaksi yang terjadi merupakan hal penting agar informasi yang ada terjamin kerahasiaannya (confidentiality), keutuhannya (integrity) dan ketersediaannya (availibility). Sampai saat ini, KPPN Surabaya I belum memiliki tata kelola keamanan informasi lebih khusus lagi terhadap kontrol akses. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis resiko keamanan informasi yang berhubungan dengan akses kontrol, sedangkan hasil dari penelitian ini adalah dokumen tata kelola keamanan informasi berdasarkan ISO/IEC 27001:27005 yang berfokus pada kontrol akses di KKPN Surabaya 1. Sedangkan penelitian berikutnya menghasilkan dokumen tata kelola keamanan sistem informasi berdasarkan relasi dari dua framework yaitu COBIT 5 dan ISO/IEC 27001:2013.

2.b. Landasan Teori

2.b.1. Keamanan Informasi

Keamanan informasi didefinisikan secara singkat dan sederhana sebagai proses menjaga kerahasiaan, integritas dan ketersediaan informasi, tiga hal fundamental yang biasa dikenal sebagai C-I-A triad atau triad keamanan informasi.

2.b.2. Tata Kelola Keamanan Informasi

Tata kelola keamanan informasi didefinisikan sebagai sistem yang mengarahkan dan mengatur aktivitas keamanan informasi di sebuah organisasi.

Lima hasil utama dari tata kelola keamanan informasi meliputi.

1. Keselarasan strategi keamanan informasi dengan strategi bisnis untuk mendukung tujuan organisasi.
2. Manajemen risiko dengan menjalankan langkah-langkah yang tepat untuk mengelola dan mengurangi risiko serta mengurangi dampak potensial terhadap sumber daya informasi pada tingkat yang dapat diterima.
3. Pengelolaan sumber daya dengan memanfaatkan pengetahuan keamanan informasi dan infrastruktur secara efisien dan efektif.
4. Pengukuran kinerja dengan mengukur, memantau dan melaporkan metrik tata kelola keamanan informasi untuk memastikan bahwa tujuan-tujuan organisasi tercapai.

Menghasilkan nilai tambah dengan mengoptimalkan investasi keamanan informasi dalam mendukung tujuan organisasi.

2.b.3. ISO/IEC 27001

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

2.b.4. *COBIT 5 For Information Security*

COBIT 5 *for Information Security* dibangun berdasar kerangka kerja COBIT 5 yang berfokus pada keamanan informasi dan memberikan detail dan panduan praktis lebih banyak untuk keamanan informasi profeisonal dan bagian lain pada semua level di organisasi.

4. Implementasi Sistem dan Hasil

4.a. Pemetaan Tujuan Organisasi

Analisis pemetaan tujuan spesifik organisasi terhadap kerangka kerja COBIT 5 *Enterprise Goal* yang bersifat generik dapat dilihat pada **Error! Reference source not found.**.

Dari hasil pemetaan tujuan spesifik organisasi dengan tujuan generik didapatkan 10 tujuan generik organisasi yang terdapat pada COBIT 5.

4.b. Pemetaan Tujuan TI Organisasi

Pemetaan tujuan TI merupakan langkah selanjutnya setelah pemetaan tujuan organisasi. Proses ini menunjukkan bagaimana tiap tujuan organisasi didukung oleh tujuan TI.

Dari hasil pemetaan tujuan organisasi dengan tujuan terkait TI oganisasi, didapatkan 15 tujuan terkait TI organisasi. Tujuan terkait TI organisasi ini dilihat dari pentingnya penerapan TI di organisasi. TI dapat membantu proses bisnis organisasi menjadi lebih efisien.

4.c. Pemetaan Proses

Setelah proses pemetaan tujuan TI terkait organisasi, kemudian dipetakan ke dalam *cascade* proses.

Dari pemetaan TI terkait organisasi, didapatkan 37 proses tata kelola dan manajemen TI organisasi. Keseluruhan proses merupakan proses yang dibutuhkan oleh organisasi. Namun untuk penerapan tata kelola, diprioritaskan ke proses yang paling menguntungkan dan mudah untuk dilakukan perbaikan berdasarkan rencana strategi organisasi dan penilaian risiko organisasi.

4.d. Hasil Penilaian Resiko

Dari hasil penilaian risiko keamanan informasi, dapat disimpulkan prioritas risiko untuk organisasi. Prioritas risiko dipilih berdasarkan level risiko yang bernilai Tinggi dan Ekstrem. Prioritas risiko tersebut digunakan untuk menentukan kontrol akses yang harus dilakukan.

Kategori risiko	Risiko	Kemung-kinan	Dampak	Level risiko	Ket
Kerusakan, kehilangan aset informasi	Kehilangan integritas informasi	5	4	20	E
	Kehilangan peralatan, media dan dokumen	3	5	15	T
	Hancurnya rekaman data, peralatan dan media	3	5	15	T
Kekurangan sumber daya	Kekurangan internet	3	4	12	T
	Kekurangan jaringan	4	5	20	E
	Kekurangan dukungan layanan	3	4	12	T
	Kekurangan sumber daya manusia	3	5	15	T
Aktivitas berbahaya	Manipulasi informasi	3	4	12	T
Perusakan Data Tidak Disengaja	Kesalahan penggunaan atau administrasi perangkat, sistem	3	4	12	T
	Perencanaan dan adaptasi yang tidak memadai	3	4	12	T
Kegagalan dan malfungsi	Kegagalan perangkat dan layanan	4	4	16	E
	Kegagalan /gangguan komunikasi	4	5	20	E
	Kegagalan / gangguan fungsi pasokan utama	4	5	20	T
	Kegagalan gangguan penyedia layanan	4	3	15	T
	Kegagalan sistem / alat	4	5	20	E

Deskripsi Dampak Resiko

Dampak (Impact)	
Level	**Deskripsi**
Tidak signifikan	Sangat kecil
Minor	Kecil
Medium	Cukup besar
Mayor	Besar
Malapetaka	Sangat besar

Deskripsi kemungkinan terjadinya risiko

Kemungkinan Terjadi (Likelihood)	
Level	**Deskripsi**
Sangat kecil	Sangat tidak mungkin terjadi
Kecil	Kemungkinan kecil dapat terjadi
Sedang	Sama kemungkinannya antara terjadi atau tidak terjadi
Besar	Kemungkinan besar dapat terjadi
Sangat besar	Sangat mungkin terjadi

Matriks level resiko

Kemungkinan	Akibat				
	Tidak Signifikan 1	Minor 2	Medium 3	Mayor 4	Malapetaka 5
Sangat Besar	5	10	15	20	25
Besar	4	8	12	16	20
Sedang	3	6	9	12	15
Kecil	2	4	6	8	10
Sangat Kecil	1	2	3	4	5
Keterangan : Rendah = 1 - 4; Medium = 5 -10; Tinggi = 11 - 15; Ekstrim = 16 – 25					

4.e. Usulan Langkah Implementasi

Siklus implementasi menyajikan cara bagaimana organisasi memetakan kompleksitas dan perubahan selama penerapan keamanan informasi. Implementasi tata kelola keamanan informasi yang diusulkan berdasarkan siklus implementasi COBIT yang terdiri dari 7 fase, yang tiap fasenya terdiri dari 3 komponen. Untuk lebih jelasnya, diilustrasikan pada tabel di bawah ini

Siklus	Perbaikan berkelanjutan	Kemungkinan Perubahan	Manajemen Program
Fase 1: Mendapatkan pemahaman tentang latar belakang program, tujuan dan tata kelola yang ada saat ini			
1	Mengidentifikasi tata kelola yang ada saat ini	Menganalisis perubahan yang bisa dilakukan	Menyusun tujuan program kerja
Fase 2: Memastikan bahwa tim program yang menangani implementasi memahami tujuan organisasi, bisnis yang dilakukan dan fungsi TI sehingga dapat memberikan nilai di organisasi			
2	Menilai kondisi saat ini, bagaimana TI mendu- kung organisasi	Membentuk tim imple-mentasi yang kuat	Mendefinisikan masalah dan peluang (analisis SWOT)
Fase 3: Menentukan kemampuan target dari setiap proses yang terpilih			
3	Mendefinisikan status target dan analisis kesenjangan	Mengkomunikasikan hasil yang diharapkan	Membuat *road map*
Fase 4: Mengubah peluang menjadi proyek yang dapat dipertanggung jawabkan			
4	Merancang dan membangun perubahan	Memperkuat peran pihak-pihak yang terlibat dan mengidentifikasi *quick win*	Menyusun rencana program kerja
Fase 5: Mengimplementasikan proyek perbaikan, memanfaatkan program kerja dan kemampuan manajemen proyek, standar dan praktik. Mengevaluasi, menilai dan melaporkan kemajuan proyek			
5	Mengimplementasikan perbaikan	Memungkinkan operasi	Mengeksekusi rencana
Fase 6: Mengintegrasikan metrik untuk kinerja proyek dan merealisasikan manfaat program perbaikan tata kelola ke dalam sistem pengukuran kinerja dan pemantauan terus-menerus			
6	Mengoperasikan dan mengukur	Memasukkan pendekatan baru	Merealisasikan manfaat
Fase 7: Menilai hasil dan pengalaman yang didapat dari program yang telah dijalankan			
7	Memantau dan mengevaluasi	Mempertahankan program yang baik	Mengkaji efektivitas program yang telah berjalan

4.f. Usulan kontrol Akses

Dari usulan tata kelola di atas, dibuatkan pula usulan akses kontrol terhadap akses terkait dengan aset informasi operasi dan struktur organisasi yang menjadi fokus perbaikan proses bisnis. Berikut ini adalah kontrol akses terhadap aset informasi operasi.

1	2	3	4	5
Peran di Struktur Organisasi	**Hak masukan**	**Hak pemrosesan**	**Hak Keluaran**	**Hak akses**
Operator	✓	✓		✓
Ketua Litbang TI	✓	✓	✓	✓
Pemeliharaan				✓
Direktur Utama	✓	✓	✓	✓

Keterangan:

Hak masukan	mempunyai hak memasukkan data
Hak pemrosesan	mempunyai hak memproses data
Hak keluaran	mempunyai hak mengevaluasi dan menyetujui data untuk dikeluarkan
Hak akses	mempunyai hak melihat data

5. Penutup

a. Masih kurangnya kesadaran tentang keamanan informasi pada PDAM XYZ yang terlihat dari hasil identifikasi ancaman maupun kelemahan yang dilakukan.
b. Dari hasil penilaian resiko, didapat bahwa risiko bernilai ekstrim adalah kehilangan intgritas informasi, kegagalan perangkat dan layanan, gangguan komunikasi, dan kegagalan sistem/alat sehingga dibuatkan kotrol akses yang berkaitan dengan aset tersebut.
c. Pembuatan dokumen tata kelola ini menghasilkan dokumen manual keamanan informasi.

6. Pustaka

[1] ISACA, "COBIT 5 for Information Security", *ISACA,* 2012

[2] ISACA, "ISO/IEC 27001:2013 Information technology – Security techniques – Information Security Management systems – Requirements", 2013.

[3] ISO, "ISO/IEC 27002:2013 Information technology – Security techniques – Information Security Management systems – Code of Practice for Information Security Control", 2013.

[4] ISO, "ISO/IEC 27005:2008 Information technology – Security techniques – Information Security Risk Management", 2013.

[5] IT Governace Institute, "Information Security Governance: Guidance for Board of Directors and Executive Management, 2nd Edition, 2006.

[6] Hakim Abdul, "Evaluasi Tata Kelola Teknologi Informasi dengan Framework COBIT 5 di Kmenterian ESDM, Journal Of Information Systems, Volume 10, Issue 2, October 2014.

[7] Ciptaningrum Dewi, "Audit Keamanan Sistem Informasi pada Kantor Pemerintah Kota Yogyakarta menggunakan COBIT 5", Seminar Nasional Teknologi Informasi dan Komunikasi, 2015.

[8] Sakinah Farroh, "Indeks Penilaian Kematangan (Maturity) Manajemen Keamanan Layanan TI", Jurnal Teknik Pomits Vol. 3, No. 2, 2014.

[9] Kaban E., "Tata Kelola Teknologi Informasi", CommIT, Vol. 3 No. 1, hlm. 1 – 5, Mei, 2009.

[10] Kaban M. Utomo, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses berbasis ISO/IEC 27001:27005 Pada Kantor Pelayanan Perbendaharaan Surabaya", Jurnal Teknik ITS Vol. 1, No. 1, September, 2012.

[11] N. Waly, R. Tassabehji and M. Kamala, "Improving Organisational Information Security Management: The Impact of Trainig and Awareness", *IEEE 14th International Conference on High Performance Computing and Communication,* 2012.

[12] R. Al-Ali, R. Al-Dalky, M. Al-Mardini, W. El-Hajj, F. Aloul, "Smart Grid Security: Threats, Vulnerabilities and Solutions", *International Journal of Smart Grid and Clean Energy, vol. 1, no. 1, September.*2012.

[13] W. Najib, "Tata Kelola Keamanan Informasi pada Institusi Pendidikan Tinggi Berdasarkan COBIT 5 dan ISO/IEC 27001:2013, Studi Kasus : Universitas Padjajaran", 2013.

[14] Kruger, H., Flowerday, S., Drevin, L. dan Steyn, T. (2011), An assessment of the role of cultural factors in information security awareness, *Information Security South Africa (ISSA)*, pp. 1-7.

[15] Norman, A. dan Yasin, N. (2009), An analysis of Information Systems Security Management (ISSM): The hierarchical organizations vs. emergent organization, *ICITST International Conference on Internet Technology andSecured Transactions,* pp. 1-8.

[16] Siponen, M. dan Willison, R. (2009), Information security management standards: Problems and solutions, *Information Management*, vol. 46, no. 5, pp. 267-270

[17] Wang, C. H. dan Tsai, D. R. (2009), Integrated installing ISO 9000 and ISO 27000 management systems on an organization, *43rd Annual InternationalCarnahan Conference on Security Technology*, pp. 265-267.