DoubleClick: Journal of Computer and Information Technology E-ISSN: 2579-5317
P-ISSN: 2685-2152
Vol. 3, No. 2, February 2020, Pages 67-74 http://e-journal.unipma.ac.id/index.php/doubleclick

Kebijakan-Kebijakan Iso 17799 Pada Organisasi Sebagai Manajemen Sistem Keamanan Informasi

Hendy Maulana Jaya Saputra, Bestin Septia Sinambela, Renaldi Johar Awal, dan Tegar Palyus Fiqar
Program Studi S1 Sistem Informasi Institut Teknologi Kalimantan
10171034@student.itk.ac.id

Abstrak. Informasi merupakan suatu aset penting dalam organisasi. Informasi pada suatu organisasi menjadi salah satu hal penting yang memengaruhi keberlangsungan usaha, peluang usaha, maupun ancaman bagi organisasi. Oleh karena itu, sangat diperlukan upaya dalam memanajemen keamanan suatu informasi pada sebuah organisasi, baik dari perangkat keras yang dimiliki, perangkat lunak, maupun sumber daya dan aset, termasuk orang dan karyawan, kemampuan dan keahlian, serta budaya dari organisasi. Dalam memanajemen suatu keamanan informasi, telah diterbitkan beberapa standar untuk memanajemen keamanan informasi agar proses keamanan dapat dilakukan dengan baik dan optimal. Salah satu standar yang terlah ada untuk memanajemen sebuah sistem keamanan informasi adalah ISO:17799. Oleh karena itu, pada paper ini akan membahas mengenai bagaimana kebijakan ISO:17799 dapat digunakan dan diterapkan oleh organisasi. seperti diantaranya adalah kontrol dan proteksi, pemantauan dan audit, serta mengetahui apa saja ancaman dalam memanajemen sistem keamanan informasi.

Kata kunci : manajemen, keamanan informasi, audit

Abstract. Information is an important asset in an organization. Information on an organization becomes one of the important things that affects business continuity, business opportunities, and threats to the organization. Therefore, efforts are needed in managing the security of information in an organization, both from the hardware that is owned, software, and resources and assets, including people and employees, capabilities and expertise, as well as the culture of the organization. In managing an information security, several standards have been issued to manage information security so that the security process can be carried out properly and optimally. One standard that has existed for managing an information security system is ISO: 17799. Therefore, this paper will discuss how ISO: 17799 policies can be used and implemented by organizations. such as control and protection, monitoring and auditing, and knowing what are the threats in managing an information security system.

Keywords: management, information security, audit

Pendahuluan

Permasalahan keamanan informasi pada suatu perangkat lunak komputer akan selalu menarik untuk dibahas, hal ini dikarenakan perkembangan teknologi informasi yang semakin mengalami peningkatan dan semakin canggih serta meluas. Akan tetapi, kecanggihan teknologi informasi teidak selalu diikuti dengan penerapan keamanan yang memadai, sehingga ancaman keamanan akan selalu menjadi masalah pada penerapan sistem komputer dan teknologi infor-masi pada suatu perusahaan. Salah satu kunci keberhasilan sistem informasi adalah adanya visi dan komitmen dari pimpinan. Apabila tidak ada komitmen dari pimpinan, maka akan berdampak pada investasi pengamanan data, sebab pengamanan data tidak dapat berkembang tanpa adanya usaha dan biaya, termasuk

investasi untuk pengamanan data elektronik.

Selain memerlukan adanya komitmen perlindungan data, masih dapat berbagai permasalahan dalam pengamanan sistem informasi, diantaranya bisa berupa kesalahan desain, kesalahan desain dapat terjadi dimana keamanan sering diabaikan. Kesalahan implementasi, kesalahan ini sering terjadi pada saat diimplementasikannya suatu desain menjadi sebuah sistem informasi, sebagai contoh adalah pembuatan aplikasi yang pengembang aplikasi tidak memahami betul mengenai keamanan pada aplikasi. Kesalahan konfigurasi, kesalahan ini terjadi pada tahap operasional, sistem yang dijalankan tidak sesuai dengan prosedur dari pemilik sistem. Kesalahan penggunaan, juga terjadi pada saat mengoperasikan sistem, umunya disebabkan karena sistem yang terlalu kompleks, sementara sumber daya terbatas [1].

Masalah keamanan informasi juga ditinjau dari beberapa aspek. Diantaranya aspek-aspek dari tinjauan keamanan informasi adalah *Physical Security*, yang memfokuskan strategi untuk mengamankan anggota organisasi, keamanan fisik, lokasi, tempat kerja, serta meliputi berbagai macam ancaman fisik, seperti misalnya kebakaran, akses tanpa otorisasi, dan bencana alam. *Personal Security* yang memfokuskan mengenai perlindungan orang-orang dalam organisasi. *Operation Security* yang memfokuskan pengamanan kemampuan prganisasi terhadap keberlangsungan bisnis yang sedang berjalan. *Communications Security* yang bertujuan sebagai pengamanan media informasi dan komunikasi. *Network Security* yang memfokuskan pada keamanan jaringan teknologi informasi pada suatu organisasi [2].

Solusi masalah keamanan informasi kini telah diterbitkan oleh Organisasi Internasional untuk Standarisasi (ISO). Standar Manajemen Keamanan Informasi ini telah diakui secara internasional. Standar Manajemen Keamanan Informasi ini dilabeli ISO 17799. ISO 17799 diterbitkan pada bulan Desember 2000. ISO 17799. ISO 17799 mendefinisikan informasi sebagai aset yang mungkin ada dalam berbagai bentuk dan nilai bagi organisasi. Tujuan dari keamanan informasi sendiri adalah untuk melindungi aset ini guna memastikan keberlangsungan bisnis, meminimal-kan kerusakan bisnis, dan memaksi-malkan laba atas investasi.

Pada karya tulis ini akan membahas mengenai isi dan ketentuan dari ISO 17799 yang merupakan standar untuk manajemen keamanan sistem informasi. ISO 17799 juga menawarkan berbagai spesifikasi untuk memastikan manajemen layanan TI (Teknologi Informasi). ISO 17799 merupakan standar yang sering digunakan untuk mengetahui kebutuhan dan menerapkan kamanan sistem informasi.

Metodologi

Metodologi penelitian yang digunakan dalam pembuatan paper ini adalah deskriptif kualitatif, yakni dengan mengumpulkan data-data yang berupa kata-kata, gambar, dan bukan angka-angka. Namun, apabila ditemukan data yang beruka angka, maka akan diolah dan dideskripsikan serta dijelaskan dengan menggunakan kalimat penjelas. Sehingga hasil dari paper ini adalah naskar yang berasal dari rangkuman naskah-naskah dengan pembahasan yang serupa.

Pembahasan

Sistem Manajemen Keamanan Informasi

Sistem manajemen keamanan informasi adalah bagian dari integrasi dengan proses organisasi serta struktur manajemen secara menyeluruh. Pada ISO/IEC 27001 (2013) Sistem manajemen keamanan informasi menjaga integritas, kerahasiaan serta ketersediaan informasi melalui proses resiko dan meyakinkan pihak yang berkepentingan bahwa resiko dapat

dikelola dengan baik [3]. Keamanan informasi terdiri dari perlindungan 3 aspek yaitu *Confidentiality (kerahasiaan)* merupakan aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi tersebut hanya dapat diakses oleh orang yang berwenang serta menjamin kerahasiaan data yang diterima , dikirim, ataupun yang disimpan. *Integrity (integritas)* merupakan aspek yang menjamin bahwa data tidak bisa diubah tanpa ijin pihak yang berwenang, menjaga keutuhan dan keakuratan keutuhan informasi serta metode prosesnya dalam menjamin aspek *integrity* ini. Dan terakhir yaitu *Availability (ketersediaan)* merupakan aspek yang menjamin bahwa data akan tersedia ketika dibutuhkan, memastikan user yang memiliki hak dapat menggunakan informasi dan perangkat yang terkait seperti aset yang berhubungan ketika diperlukan [4].

Keamanan dapat tercapai dengan berbagai cara ataupun strategi yang biasa dilakukan dengan cara stimultan atau dilakukan dalam kombinasi satu dengan lainnya. Masing-masing strategi dari keamanan informasi memiliki fokus dan dibangun dengan tujuan tertentu sesuai kebutuhan. Contoh keamanan informasi yaitu *Physical security, Personal security, Operation security, Communication security*, *Network security* [5].

Alasan Keamanan Informasi Dibutuhkan

Keamanan sebuah informasi melindungi suatu informasi dari ancaman ancaman yang datang untuk memastikan kelancaran usaha, memperkecil kerugian dari perusahaan atau organisasi dan memaksimalkan keuntungan dari investasi dan kesempatan usaha. Manajemen dari suatu sistem informasi memungkinkan data untuk terbagi secara elektronis, sehingga memerlukan sebuah sistem untuk memastikan data terkirim dan diterima oleh tujuan yang benar. hasil dari survey ISBS (Information Security Breaches Survey) pada tahun 2000 menunjukan bahwa sebagian besar dari suatu data atau informasi tidak hanya cukup aman sehingga beralasan kerawanan. Langkah untuk memastikan bahwa suatu sistem memang mampu menjamin keamanan suatu data dan informasi telah dilakukan dengan benar menerapkan kunci kunci pengendalian dari standar yang telah teridentifikasi [5].

Komponen, Aplikasi, dan Implikasi ISO 17799

ISO 17799 menyediakan kerangka kerja untuk menetapkan meode penilaian risiko, kebijakan kontrol dan perulangan, dan dokumentasi program. Standar adalah model yang sangat baik untuk organisasi adalah perlu untuk membuat keamanan informasi dan prosedur, menetapkan peran dan tanggung jawab, memberikan manajemen aset yang konsisten, membangun keamanan manusia dan fisik, Komunikasi dokumen dan prosedur operasional, menentukan kontrol akses dan sistem terkait, bersiap untuk insiden dan manajemen kontinuitas bisnis, serta mematuhi persyaratan hukum dan kontrol audit [6].

Keamanan informasi dapat didefinisikan sebagai program yang memungkinkan suatu organisasi untuk melindungi lingkungan yang saling terhubung secara terus-menerus dari kelemahan, kerentanan, serangan, ancaman, dan insiden yang muncul. Program ini harus membahas masalah fisik dan tidak berwujud. Aset informasi ditangkap dalam berbagai format dan beragam, dan kebijakan, proses, dan prosedur harus dibuat sesuai dengan itu [7].

Organisasi dapat menggunakan standar ini tidak hanya untuk membuat program keamanan informasi tetapi juga untuk membuat pedoman yang berbeda untuk tujuan sertifikasi, kepatuhan, dan audit. Standar ini menyediakan berbagai istilah dan definisi yang dapat diadopsi serta alasan, pentingnya, dan alasan untuk

membangun program untuk melindungi informasi organisasi [8].

Langkah untuk Membangun dan Mengimplementasikan Program Keamanan Informasi

Deskripsi kontrol memiliki definisi, panduan implementasi, dan informasi lain untuk memungkinkan organisasi menetapkan tujuan programnya sesuai dengan metodologi standar. Adapun tahapan dalam membangun dan mengimplementasikan program keamanan sistem informasi adalah sebagai berikut :

Langkah 1 : Mengadakan Analisis atau Penilaian Risiko

Risiko didefinisikan sebagai segala sesuatu yang menyebabkan paparan kemungkinan kerugian atau cedera. Analisis risiko ditetapkan sebagai proses mengidentifikasi risiko pada suatu organisasi dan sering melibatkan evaluasi probabilitas dari suatu peristiwa atau suatu penilaian potensi bahaya. Kerugian potensi harus dipahami menentukan kemampuan organisasi untuk potensi kerugian seperti itu. Kategori risiko keduanya internal dan eksternal dan dapat mencakup [6]:

1. Alami: Peristiwa cuaca signifikan seperti badai, banjir, dan badai salju
2. Manusia: Kebakaran, tumpahan bahan kimia, vandalisme, pemadaman listrik, dan virus / peretas
3. Politik: serangan teroris, bom ancaman, pemogokan, dan kerusuhan

Lakukan penilaian risiko untuk memahami, menganalisis, menge-valuasi, dan menentukan apa risiko organisasi membayar kemungkinan besar terjadi di lingkungan mereka. Risiko kegiatan penilaian melibatkan informasi teknologi (TI) dan informasi
fasilitas pengolahan, manajemen fasilitas dan membangun keamanan, manusia sumber daya (SDM), manajemen catatan (RM) dan perlindungan catatan vital, dan kepatuhan dan manajemen risiko kelompok.

Analisis risiko dilakukan untuk mengisolasi peristiwa spesifik dan tipikal yang wouid kemungkinan mempengaruhi organisasi; mengingat
geografi dan sifatnya kegiatan bisnis akan membantu mengidentifikasi risiko. Kehilangan potensi dari semua ini acara dapat mengakibatkan akses terlarang, pasokan listrik terganggu, kebakaran dari gas atau gangguan listrik, kerusakan air, jamur atau cetakan untuk koleksi kertas, kerusakan asap, bahan kimia kerusakan, dan total kerugian (dengan kehancuran seluruh bangunan) [6].

Langkah 2 : Menetapkan Kebijakan Keamanan

Komponen standar ini menyediakan konten yang harus dimasukkan serta panduan implementasi untuk menetapkan fondasi dan otorisasi program. Untuk mengatur prioritasnya, sebuah informasi kebijakan keamanan harus dikembangkan, disahkan oleh manajemen, diterbitkan, dan dikomunikasikan. Itu harus berlaku untuk semua aset informasi dan harus menunjukkan komitmen manajemen ke program. Jelaskan implikasinya pada proses kerja dan terkait tanggung jawab dan garis besar di dalamnya deskripsi pekerjaan karyawan. Kebijakan keamanan seharusnya dikelola, didokumentasikan, dan secara berkala dievaluasi dan diperbarui untuk mencerminkan tujuan organisasi dan arah bisnis [6].

Langkah 3 : Menyusun Inventarisasi Aset

Komponen standar ini membahas manajemen aset, kontrol, dan perlindungannya. Ini berlaku untuk alt aset dalam bentuk berwujud dan tidak berwujud. Identifikasi intelektual organisasi properti (IP), toot untuk membuat dan mengelola IP, dan aset fisik dengan persediaan terperinci sehingga organisasi tahu jenis sumber daya apa yang dimilikinya, di mana mereka berada, dan siapa yang memiliki tanggung jawab untuk mereka. Identifikasi caranya aset

harus digunakan, diklasifikasikan, perlu diberi label, dan ditangani untuk membangun aset inventaris manajemen. Persediaan ini juga harus membedakan jenis, format, dan masalah kontrol kepemilikan [6].

Langkah 4 : Tentukan Akuntabilitas

Program keamanan informasi tidak akan diimplementasikan kecuali peran dan tanggung jawab diartikulasikan dengan jelas dan dipahami oleh mereka yang memiliki peran dalam program. Idealnya, peran dan tanggung jawab ini harus diuraikan dalam uraian tugas dan didokumentasikan dalam suatu hal dan ketentuan kerja [6].

Karyawan adalah bagian dari keseluruhan lanskap keamanan informasi dan seringkali merekalah yang paling ber-peran dan mampu mencegah terjadinya insiden tertentu. SDM biasanya bertanggung jawab atas hal ini masalah, tetapi mereka harus berkolaborasi dengan IT dan RM untuk memastikan bahwa semua informasi aset ditangani sesuai. Tentukan peran dan tanggung jawab selama pra-employnient dan skrining proses, dan melakukan peninjauan latar belakang untuk mendukung proses perekrutan [6].

Ketika karyawan pergi atau berubah pekerjaan, penting bahwa SDM, dalam kolaborasi dengan pemangku kepentingan lainnya, ikuti melalui pengembalian proses aset dan penghapusan hak akses, yang bisa ditangkap dalam proses keluarnya SDM dan Prosedur. Proses ini sering tidak terkoordinasi, yang memung-kinkan karyawan pergi dengan informasi atau pergi balik pada server dan dalam pekerjaan fisik ruang massa yatim dan tidak dikenal informasi [6].

Langkah 5 : Alamat Keamanan Fisik

Komponen standar ini menguraikan semua persyaratan fisik batas keamanan dan entri resmi kontrol; langkah-langkah untuk melindungi ancaman eksternal dan lingkungan; keamanan peralatan, utilitas, dan pemasangan kabel pertimbangan; dan pembuangan aman atau penghapusan media peralatan penyimpanan. Bangunan organisasi dan bangunan, peralatan, dan pemrosesan informasi fasilitas harus menjadi bukti kegagalan mencegah intrusi yang tidak sah dan akses, dan kemungkinan masalah pencurian [6].

Langkah 6 : Operasi Dokumen Prosedur

Prosedur untuk aktivitas sistem, ubah kontrol manajemen, dan segregasi tugas termasuk dalam komponen ini. Program organisasi apa pun akan lebih mapan ketika administrasi program, kebijakan, prosedur, dan segala terkait proses didokumentasikan secara formal. Komponen ini menetapkan untuk mendefinisikan operasi prosedur, instruksi untuk eksekusi rinci daripadanya, dan manajemen jejak dan sistem audit informasi. Hal ini berlaku untuk semua segi keamanan informasi program [6].

Langkah 7 : Menentukan Kontrol Akses

Komponen standar ini termasuk pedoman untuk menetapkan kebijakan dan aturan untuk informasi dan sistem mengakses. Tindakan kontrol akses harus termasuk:

1. Menyiapkan pendaftaran pengguna dan prosedur deregistrasi
2. Mengalokasikan hak istimewa dan kata sandi
3. Menerapkan "meja kerja yang jelas dan hapus kebijakan layar "
4. Mengelola;
   - Peralatan tanpa pengawasan
   - Solusi jaringan pribadi virtual
   - Jaringan nirkabel dan otentikasi
   - Masalah layanan jaringan seperti perutean dan koneksi
   - Telecommuting ruang virtual dan hak kekayaan intelektual
   - Kunci dan prosedur kriptografis
   - Pengembangan perangkat lunak, pengujian, dan lingkungan produksi
   - Kode sumber program dan perpustakaan

- Ubah prosedur kontrol dan dokumentasi
- Tambalan, pembaruan, dan layanan paket [6]

Langkah 8 : Mengoordinasikan Kontinuitas Bisnis

Komponen standar ini termasuk persyaratan pelaporan, respons dan prosedur eskalasi, dan bisnis manajemen kontinuitas. Sebagai organisasi semakin datang diserang dan menderita pelanggaran keamanan, mereka harus memiliki beberapa formal cara menanggapi peristiwa ini. Manajemen kesinambungan bisnis mengatasi gangguan tak terduga di kegiatan bisnis atau counter mereka peristiwa yang menghambat organisasi fungsi bisnis penting. Proses ini harus mencakup:

1. Mengidentifikasi risiko dan kemungkinan kejadian
2. Melakukan analisis dampak bisnis
3. Memprioritaskan fungsi bisnis penting
4. Mengembangkan tindakan pencegahan untuk mengurangi dan meminimalkan dampaknya kejadian [6].

Langkah 9 : Menunjukkan Kepatuhan Hukum

Komponen standar ini menyediakan standar untuk kekayaan intelektual hak, persyaratan RM, dan kepatuhan tindakan. Ini berlaku untuk semuanya dari pemrosesan informasi suatu organisasi sistem data granular dan transaksional catatan yang terkandung di dalamnya sistem. Ada peningkatan pengawasan pada organisasi untuk menunjukkan kepatuhan dengan hukum, peraturan yang berlaku, dan persyaratan legislatif untuk semua aspek transaksi bisnis mereka. Kepatuhan terhadap aturan dan peraturan bagian integral dari keamanan informasi program dan akan berkontribusi menunjukkan akunta-bilitas perusahaan [6].

10 Klausa Kontrol dari ISO 17799

Salah satu isi dari ISO 17799 meliputi 10 klausa kontrol (10 pasal pengamatan). Adapun 10 klausa kontrol adalah sebagai berikut :

Security Policy (kebijakan keamanan), yakni mengarahkan visi dan misi manajemen agar kontinuitas bisnis dapat berlangsung san mampu untuk menjaga keutuhan informasi penting yang dimiliki oleh perusahaan [7].

System Access Control **(**sistem kontrol akse), yakni bagaimana mengendalikan akses pada setiap pengguna terhadap informasi-informasi yang telah diatur kewenangannya, termasuk juga pengendalian penggunaan TI [7].

Communication and Operations Management (manajemen komunikasi dan operasi), yakni penyediaan suatu perlindungan terhadap infrastruktur sistem informasi dan teknologi informasi melalui perawatan, pemeriksaan berkala, serta memastikan kesediaan panduan sistem [7].

System Development and Maintenance (pengembangan sistem dan pemeliharaan), yakni klausa yang dilakukan setelah dilakukan pemeriksaaan berkala terkait sistem informasi dan teknologi informasi. Pada tahapan ini adalah memastikan bahwa sistem operasi maupun aplikasi mampu untuk bersinergi melalui proses verifikasi [7].

Physical and Environment Security (keamanan fisik dan lingkungan), yakni keamanan sistem informasi dan teknologi informasi dari segi fisik, lingkungan, dan jaringan untuk mencegah adalah kerusakan atau kehilangan data yang diakibatakn oleh factor lingkungan, bisa berupa bencana alam maupun pencurian (Carlson, 2001).

Compliance (penyesuaian), yakni memastikan implementasi kebijakan keamanan telah seuai dengan peraturan perundang-undangan yang berlaku, termasuk didalamnya adalah pernyaratan kontrakturan melalui audit sistem [7].

Personel Security (keamanan perorangan), yakni mengatur tentang pengurangan risiko dari penyalahgunaan fungsi penggunaan atau wewenang akibat kesalahan pengguna. Oleh karenanya, penting mengadakan pelatihan-pelatihhan mengenai *security awareness* agar setiap pengguna mampu menjaga keamanan dan kerahasiaan informasi atau data pada lingkup kerjanya masing-masing [7].

Security Organization (keamanan organisasi), mengatur tentang keamanan secara untuh suatu organisasi atau perusahaan, yakni mengendalikan keutuhan sistem informasi dalam organisasi tersebut terhadap keperluan pihak luar [7].

Asset Classification and Control (klasifikasi dan kontrol aset), yakni memberikan perlindungan terhadap aset perusahaan dan aset informasi berdasarkan tingkat perlindungan yang telah ditetapkan (Carlson, 2001).

Business Countinuity Management (manajemen kelanjutan usaha), yakni kesiapan dalam menghadapi risiko yang akan ditemui selama aktivitas bisnis berlangsung yang mampu mengakibaykan '*major failure´* atau risiko kegagalan yang utama ataupun bencana dan kejadian buruk yang tidak terduga [7].

Simpulan

Adapun simpulan yang dapat diperoleh dari paper ini diantaranya adalah sebagai berikut :

1. Sistem manajemen keamanan informasi merupakan integrasi antar proses organsisasi serta struktur untuk menjaga kerahasiaan dan ketersediaan informasi.
2. Sistem manajemen keamanan informasi yang telah tersertifikasi dan diakui secara internasional adalah ISO 17799.
3. Penting bagi suatu organisasi untuk memanajemen keamanan informasi guna melindungi informasi dari ancaman terhadap informasi atau data tersebut.
4. ISO 17799 meliputi kerangka kerja, kebijakan kontrol, serta dokumentasi program.
5. Terdapat delapan ahapan yang dapat dilakukan untuk membangun dan mengimplementasikan dan menjalankan program keamanan informasi.
6. ISO 17799 meliputi 10 klausa kontrol untuk memastikan berjalannya layanan sistem informasi dan teknologi informasi

Daftar Pustaka

[1] Februariyanti, H. (2006). Standar dan Manajemen Keamanan Komputer. *Jurnal Teknologi Informasi DINAMIK Volume XI, No. 2* , 134-142.

[2] Trisantono, H. B. (2007). Kebijakan Keamanan dengan Standar BS 7799/ISO 17799 Pada Sistem Manajemen Keamanan Informasi Organisasi. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)* , C75 - C76.

[3] Yuze, Y. C. (2006). *Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC27001 : 2013 Serta Rekomendasi Model Sistem Menggunakan Data Flew Diagram pada Direktorat Sistem Informasi Perguruan Tinggi.* Bandung: Jurnal Sistem Informasi Bisnis.

[4] Utomo, M. d. (2012). *Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I.* Surabaya: Jurnal Teknik ITS.

[5] Syafrizal, M. (2007). *ISO 17799: Standar Sistem Manajemen Keamanan Informasi*. Yogyakarta: STMIK AMIKOM Yogyakarta.

[6] Myler, E. C. (2006). ISO 17799 Standard for Security. *The Information Management Journal* , 43-52.

[7] Carlson, T. (2001). *Information Security Management: Understanding ISO 17799.* United States: International Network Services Inc.