PENILAIAN TINGKAT EFEKTIVITAS PENERAPAN KEAMANAN SISTEM INFORMASI MENGGUNAKAN ISO/IEC 27004:2009 DAN ISO/SNI 27001:2009 (STUDI KASUS DI STTI TANJUNGPINANG)

Linda Apriyanti
linda@sttindonesia.ac.id

Abstrak

Sejak tahun 2014 STT Indonesia Tanjungpinang sudah menerapkan kebijakan SMKI, hal ini guna menunjang oprasional penerapan sistem informasi khususnya sistem informasi akademik dan keuangan (SIMAK), namun sampai saat ini belum dilakukan evaluasi terhadap penerapan SMKI tersebut.
Maka dari itu penelitian ini berfokus pada penilaian tingkat efektivitas penerapan keamanan sistem informasi menggunakan ISO/IEC 27004. Untuk memastikan bahwa kebijakan SMKI yang sudah diterapkan saat ini berjalan dengan baik. Tahap yang dilakukan dimulai dari pengukuran tingkat efektivitas penerapan keamanan sistem informasi, dari hasil pengukuran dilakukan penilaian tingkat efektivitas.
Jika dalam proses penelitian didapat kebijakan yang lemah, maka akan diberikan rekomendasi saran perbaikan baik berupa prosedur maupun standar oprating prosedur (SOP) guna meningkatkan keamanan informasi. Metodologi yang digunakan adalah fremework ISO/SNI 27001. Dalam penelitian ini peneliti mengharapkan adanya perbaikan kebijakan dan prosedur yang lemah guna meningkatkan keamanan informasi yang dapat menunjang oprasional dan proses bisnis.

Kata Kunci : SMKI, penilaian, pengukuran, efektivitas, ISO/IEC 27004, ISO/SNI 27001

1. Pendahuluan

Seiring dengan perkembangan teknologi dan informasi yang pesat dalam bidang pendidikan juga mempunyai persaingan yang semakin ketat demi mendukungnya proses bisnis yang berjalan, sehingga menuntut perguruan tinggi untuk melakukan terobosan dan perubahan agar dapat mengoptimalkan penggunaan Teknologi Informasi.STT Indonesia adalah perguruan tinggi yang telah memanfaatkan Teknologi Informasi, pengembangan pengelolaan dan pemanfaatan Sistem Informasi Terintegrasi. Sistem Informasi akademik (SIMAK) sebagai sistem utama yang terintegrasi dengan Sistem informasi Kerja Praktek dan Skripsi, Sistem Absensi, Ujian Saringan Mahasiswa Baru, Ujian Akhir Semester Online, E-library dan e-learning. Sehingga dengan adanya layanan ini terselenggaranya pelayanan mahasiswa yang optimal dan tersedianya data dan informasi yang akurat melalui implementasi sistem informasi.

Sistem Informasi Terintegrasi di STT Indonesia mulai diimplementasikan pada tahun 2011. Hasil wawancara dengan staf Pusat Pengolahan Data (PUSLAHTA) terdapat insiden dalam keamanan database yang pernah terjadi, diantaranya banyak pengguna yang mengakses terhadap sistem mengakibatkan banyak masalah yang timbul, terutama yang berkaitan dengan keamanan data yang mengakibatkan kehilangan dan kerusakan data.

Sehingga pada akhir tahun 2013, Ketua STT Indonesia menerbitkan Surat Keputusan tentang Kebijakan Keamanan Sistem Informasi. Namun sampai saat ini belum ada pengukuran tingkat efektivitas penerapan keamanan sistem informasi yang bisa menjamin bahwa kebijakan keamanan sistem informasi yang berjalan selama ini sudah mampu menangani masalah keamanan sistem informasi khususnya SIMAK di STT Indonesia Tanjungpinang.

2. Keamanan Sistem Informasi

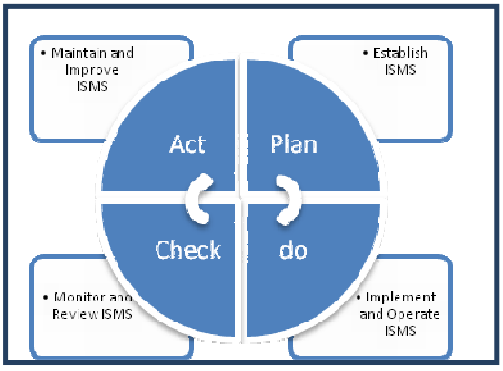
Menurut SNI ISO/IEC 27001 : 2009 dikutif dari Iqbal (2013 :21) keamanan sistem informasi adalah penjagaaan kerahasiaan, integeritas dan ketersediaan informasi. Keamanan sistem informasi merupakan salah satu hal yang harus diperhatikan oleh perusahaan, kebocoran data dan informasi dan kegagalan sistem dapat menyebabkan kerugian baik di sisi finansial maupun produktifitas perusahaan. Keamanan informasi meliputi suatu mekanisme untuk mengontrol akses dan penggunaan database pada level obyek, keamanan informasi pada pengguna, dimana pengguna tersebut memiliki akses tertentu. Pengaturan mengenai keamanan informasi terutaman akan ditentukan berdasarkan seberapa jauh tingkat keamanan yang akan dibangun untuk informasi database. Tingkat keamanan informasi yang bergantung pada tingkat sensitifitas informasi dalam database, biasanya informasi yang tidak terlalu sensitif perlu pengaturan keamanan yang ketat untuk akses ke informai tersebut (mufadhol, 2009).

Seiring dengan perkembangan teknologi, pengelolaan keamanan database semakin lama menjadi pekerjaan yang semakin sulit dan menantang. Pihak yang bertanggung jawab terhadap sistem keamanan database harus dapat memastikan tiga hal utama dalam keamanan database yaitu kerahasiaan (*confidentiality*), integritas (*Integrity*) dan ketersediaan (*availability*).

3. SistemManajemenKeamananInformasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) merupakan bagian dari manajemen secara keseluruhan. Informasi dipandang sebagai aset penting sama seperti aset perusahaan lainnya, karena itu bagi perusahaan adalah hal yang penting untuk menggunakan pendekatan risiko dalam mengelola aset tersebut (ISO 27001: 2005).

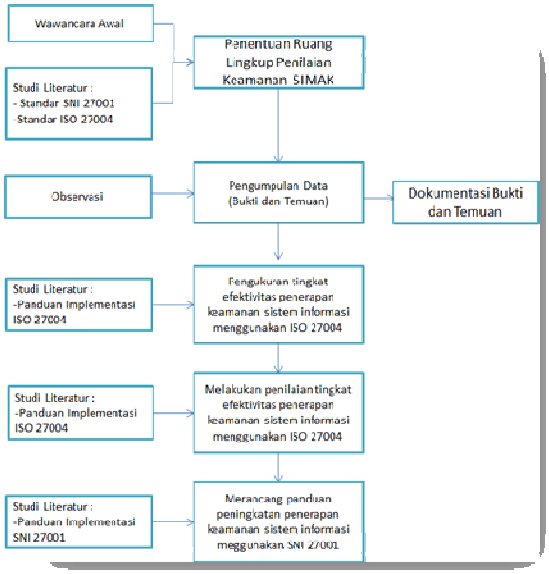
Model *PLAN – DO – CHECK – ACT (PDCA)* diterapkan terhadap struktur keseluruhan proses information security management system ISMS/SMKI. Berikut adalah tahapan-tahapan PDCA:



Gambar 1. Proses SMKI/ ISMS

4. KerangkaPenelitian

Kerangka penelitian adalah langkah-langkah sistematis atau sekumpulan metode yang digunakan untuk menyelesaikan suatu permasalahan. Tahapan yang dilakuakan dimulai dengan melakukan wawancara dengan unit bagian yang terkait yaitu denagn ketua STT Indonesia Tanjungpinang, ketua pusat pengolahan data (PUSLAHTA) dan pusat pengelolaan komputer (PUSKOM) dan melakukan studi pustaka terkait keamanan sistem informasi, dari sini kemudian ditentukan ruang lingkup yang akan dijadikan topik penelitian yaitu keamanan sistem informasipada SIMAK lebih sepesifiknya adalah penilaian tingkat efektivitas penerapan SMKI. Langkah selanjutnya adalah mengumpulkan data berupa bukti dan temuan yang berkaitan dengan topik penelitian, dari data yang diperoleh dilkuakan pengukuran tingkat efektivitas penerapan SMKI dengan menggunakan ISO 27004 dan dari hasil pengukuran dilakukan penilaian tingkat efektivitas dengan menggunakna fremwork ISO 27004. Dari hasil penilaian yang dilkukan dibuatkan saran perbaikan terutama untuk point yang dianggap rawan yaitu dengan penilaian paling rendah. Perancangan panduan peningkatan penerapan SMKI pada tahap ini menggunakan ISO / SNI 27001. Berikut adalah gambar dari kerangka penelitia :



Gambar 2. Kerangka Penelitian

5. Pengukurantingkatefektivitas

Berdasarkan penerapan SMKI di STT Indonesia Tanjungpinang, maka peneliti melakukan pengukuran tingkat efektivitas dengan menggunakan ISO/IEC 27004 klausul B8yaitu pengukuran operasi. Pengukuran oprasi keamanan informasi melibatkan kegiatan yang penting untuk memastikan bahwa hasil pengukuran dikembangkan memberikan informasi yang akurat berkaitan dengan efektivitas sebuah diimplementasikan SMKI.

Berdasarkan hasil kuesioner yang disebarkan kepada responden, maka dapat diketahui pernyataan responden mengenai tingkat efektivitas penerapan SMKI.Adapun kriteria penilaian sebagai berikut:

Tabel 1 : Kriteria Penilaian

Kriteria penilaian	Skor
Sangat Efektif	5
Efektif	4
Cukup Efektif	3
Kurang Efektif	2
Tidak Efektif	1

6. Penilaian Tingkat Efektivitas

Penilaian tingkat efektivitas terhadap penerapan SMKImerupakan salah satu indikator kinerja bagi pelaksanaan suatu kegiatan yang telah ditetapkan untuk menyajikan informasi tentang seberapa besar pencapaian sasaran atas target. Penilaian efektivitas penerapan SMKI dikategorikan efektif atau tidak apabila interval nilai dimulai dari angka 1.00 – 5.00. Untuk penilaian tingkat efektivitas keamanan sistem informasi manajemen akademik dan keuangan (SIMAK) STT indonesia Tanjungpinang, apabila hasilnya menunjukan nilai dengan interval yang semakin besar dapat dikatakan bahwa semakin efektif, demikian sebaliknya semakin kecil nilai interval hasilnya maka menunjukan semakin tidak efektif.Berikut adalah kriteria penilaian tingkat efektivitas berdasarkan hasil pengukuran tingkat efektivitas :

Tabel 2 : Penilaian tingkat efektivitas

Dampak	**Keterangan**
Sangat Efektif (5)	Dampak tidak berpengaruh pada operasional dan bisnis
Efektif (4)	Dampak tidak terlalu berpengaruh pada operasional dan bisnis
Cukup Efektif (3)	Dampak berpengaruh pada operasional
Kurang Efektif (2)	Dampak berpengaruh pada operasional dan bisnis
Tidak Efektif (1)	Dapat mematikan bisnis

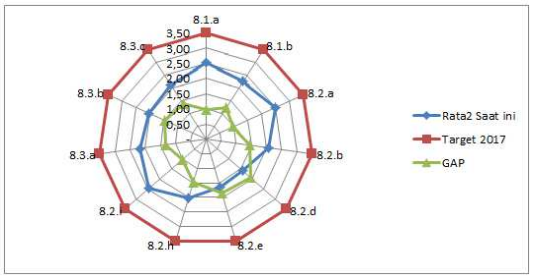
7. Hasil Pengukuran Efektivitas SMKI

Hasil pengukuran tingkat efektivitas SMKI yang dilakukan di STT Indonesia Tanjungpinang berada pada nilai**2,13** yaitu pada tingkat Kurang Efektif. sesuai dengan interval nilai yang digunakan oleh peneliti pada bab 3(tiga) Metodelogi Penelitian.

Tabel 3 : Interval Penilaian Jawaban Responden

Interval	Kriteria
4,20 - 5,00	Sangat Efektif
3,40 -4,19	Efektif
2,60-3,39	Cukup Efektif
1,80-2,59	Kurang Efektif
1,00 - 1,79	Tidak Efektif

Setelah mengetahui hasil pengukuran yang berada pada nilai 2,13 selanjutnya adalah melakukan perhituanga gap terhadap masing-masing point pertanyaan sesuai dengan target organisasi yaitu pada nilai 3,5 (Efektif) pada tahun 2017.



Gambar 3. Diagram radar perhitungan gap terhadap target

8. Penilaian Tingkat Efektivitas

Penilaian tingkat efektivitas penerapan SMKI berdasarkan hasil pengukuran pada point (4.4), adalah dengan melakukan analisis data dari identifikasi kesenjangan antra hasil pengukuran yang diharapkan dan aktual dari hasil implementasi SMKI.Setelah dilakukan pengukuran tingkat efektivitas penerapan SMKI di STT Indonesia Tanjungpinang berada pada nilai 2,13 dimana itu adalah posisi "Kurang Efektif", sedangkan target yang ingin di capai adalah pada nilai 3,5 yaitu "Efektif", agar proses operasional dapat terus berjalan dan bisnis dapat terus berkembang. Untuk merealisasikan hal tersebut perlu dibuatkan alisis hasil pengukuran tingkat efektivitas SMKI dengan membuat dokumen kontrol dapat digunakan disetiap insiden yang terjadi dalam implementasi SMKI. Dokumen kontrol dipergunakan untuk menindak lanjuti ketika ada insiden terjadi, hasil dari analisis dikomunikasikan dengan pimpinan. Berikut adalah analisis hasil pengukuran efektivitas SMKI :

Tabel 5 : Pengukuran efektivitas SMKI

Skala	Dampak	Indikator		
		Uraian	Identifikasi	Kontrol
5	Sangat Efektif	Terjadi peningkatan terhadap implemnetasi SMKI secara signifikan	Insiden jarang sekali terjadi, masalah dapat diselesaikan dengan mudah dan cepat	a. Tidak menjadi fokus pemeriksaan b. Tetap melakukan pendokumentasian secara berkala
4	Efektif	Terjadi peningkatan terhadap implemnetasi SMKI, namun tidak signifikan	Insiden sesekali terjadi dan ada usaha perbaikan, tetapi ada kemungkinan akan mengalaminya di masa depan. Sehingga strategi saat ini harus mengatasi insiden yang terjadi	a. Tetap menjadi fokus pemeriksaan b. Tetap melakukan pendokumentasian secara berkala
3	Cukup Efektif	Terjadi peningkatan terhadap implemnetasi SMKI, namun hanya di bagian tertentu	Insiden berlangsung terus menerus namun sudah ada kesadaran untuk melakukan usaha perbaikan. Alternatif mungkin diperlukan dan harus mempertimbangkan tindakan mitigasi	a. Walaupun tidak menjadi fokus, tetapi harus ada perhatian yang cukup b. Menjadi fokus pemeriksaan walaupun tidak terlalu mendalam c. Tindakan mitigasi berpedoman pada prosedur
2	Kurang Efektif	Tidak ada peningkatan terhadap implemnetasi SMKI yang signifikan	Insiden terus menerus dan sedikit ada usaha perbaikan. Alternatif akan diperlukan dan menentukan tindakan mitigasi yang dibutuhkan	a. Menjadi fokus pemeriksaan b. Melakukan perbaikan sesuai dengan prosedur untuk mengurangi insiden
1	Tidak Efektif	Tidak ada peningkatan terhadap implementasi SMKI	Insiden berlangsung terus menerus dan tidak ada usaha perbaikan sama sekali. Alternatif sangat diperlukan dan tindakan mitigasi harus segera dilakukan	c. Prioritas utama adalah untuk melakukan tindakan d. Menjadi fokus pemeriksaan secara mendalam e. Melakuakn perbaikan sesuai dengan prosedur

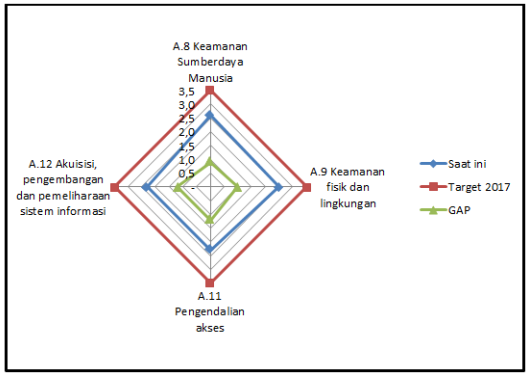
9. RekapAnalisistingkatkematangan berdasarkan ISO /SNI 27001 klausul A.8, A.9, A.11 dan A.12

Setelah melakukan analisis dari setiap klausul yang digunakan yaitu klausul A.8 Keamanan Sumber daya Manusia, A.9 Keamanan fisik dan lingkungan, A.11 Pengendalian akses, A.12 Akuisisi, pengembangan dan pemeliharaan sistem informasi. Didapat bahwa tingkat kematangan saat ini rata-rata adalah 2,4 dimana masih dibawah tingkat kematangan yang diharapkan yaitu 3,5 kesenjangan tersebut digunakan sebagai dasar dalam mengembangkan strategi pengembangan penerapan keamanan sistem informasi selanjutnya. Hasil dan laporan temuan digunakan sebagai rekomendasi saran untuk perbaikan kontrol keamanan sistem informasi berikutnya.

Tabel 4 : Tabel Analisis tingkat kematangan berdasarkan klausul A.8, A.9, A.11 dan A.12

No	Kontrol	Saat ini	Target 2017	GAP
1	A.8 Keamanan Sumber daya Manusia	2,6	3,5	0,9
2	A.9 Keamanan fisik dan lingkungan	2,5	3,5	1,0
3	A.11 Pengendalian akses	2,3	3,5	1,2
4	A.12 Akuisisi, pengembangan dan pemeliharaan sistem informasi	2,3	3,5	1,2
	RATA-RATA	2,4	3,5	1,1

Berikut adalah diagram radar berdasarkan tabel 4.16analisis tingkat kematangan berdasarkan klausul A.8, A.9, A.11 dan A.12



Gambar 4 : Tingkat kematangan berdasarkan klausul A.8, A.9, A.11 dan A.12

10. Rekomendasi Perbaikan

Rekomendasi terhadap tingkat kematangan yang diperoleh mengimplementasikan kontrol-kontrol keamanan sesuai dengan pencapaian nilai rata-rata untuk diberikan saran perbaikan yang dirancang untuk menjamin bahwa tujuan dan target dapat tercapai, sedangkan insiden yang merugikan dapat dicegah, dideteksi dan dievaluasi secara berkala.

1. A.8 Keamanan Sumberdaya Manusia

Rekomendasi :

a. Melakukanpemeriksaanlatarbelakangdaricalonkaryawan TI
b. Melakukanpenyesuaiankontrakperjanjiankerjaberdasarkankebijakankeamananinformasi
c. Melakukanpembinaandenganmelaksanakanpelatihantentangkepedulianmenjagakeamananinformasi
d. Memberikanpenugasandanmemperhatikan shering responsibilitas, berdasarkan bebankerja, sehinggakaryawandapatbekerjadenganpenuhtanggungjawab

2. A.9 Keamananfisikdanlingkungan

Rekomendasi :

a. Memilihtempatlokasipenyimpanan dan backup yang terpisah dari ruang server.
b. Membuatdokumentasikaryawan yang diperbolehkanmasukkeruang server untukmemastikanhanyakaryawan yang berwenang yang mempunyaihakaksesmasuk.
c. Mengkomunikasikanmengenaistandardan prosedur mengenai keamanan sistem informasi yang diterapkansehinggabisamemberikansolusiuntukpengadaandanpemeliharaanperalatan.

3. A.11 Pengendalianakses

Rekomendasi :

a. Membuatprosedurpendaftarandanpembatalandalampemberiandalampemberiandanpencabutanaksesterhadaps eluruhlayanandansisteminformasi.
b. Membuatprosedurpenggantian password secararegulер.
c. Menambahkanpasilitastingkatkerumitandari password, (Tingkat rendah, sedang, rumit)
d. Memberikanpelatihandansosialisai agar setiapkaryawanmenyadaripentingnyapengendalianakses

4. A.12 Akuisisi, pengembangandanpemeliharaansisteminformasi

Rekomendasi :

a. Membuatprosedurpemantauanpenggunaanfasilitaspengolahansisteminformasi
b. Membuatdokumentasihasilpemantauandanpengawasan yang diperlukanberdasarkantingkatinsiden.
c. Menggunakanenkripsipadainformasi yang dianggapsangatrahasia
d. Melakukan monitoring, evaluasidanperbaikansecaraberkalauntuktercapainya target keamanansisteminformasi
e. Memberikanpelatihandansosialisai agar setiap karyawan menyadari pentingnya keamanan sistem informasi

11. Simpulan dan Saran

Kesimpulan :

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan beberapa hal, yaitu:

1. Pengukuran tingkat efektivitas penerapan SMKI di STT Indonesia Tanjungpinang menghasilkan saran perbaikan untuk peningkatan tingkat efektivitas SMKIterhadap SIMAK, dalam melakukan pengukuran dimulai dengan melakukan wawancara untuk menentukan dokumen-dokumen yang diperlukan. Langkah pengukuran dilakukan dengan melakukan kuisioner, pengukuran dan penilain tingkat efektivitas.
2. Framework ISO 27004 dan ISO 2700 dipilih karena Indonesia meupakan member ISO melalui BSN. ISO 27004 dan ISO 27001 merupakan metoda pengukuran tingkat efektivitas penerapan SMKI yang dapat diterapkan pada perguruan tinggi. Pengukuran tingkat efektivitas penerapan SMKI memberikan gambaran mengenai hasil penilaian yang dianggap krusial dan memerlukan penanganan secara khusus dan prioritas. Dimana pembuat kebijakan dapat membuat perencanaan strategis untuk menjagakepercayaan, operasional dan proses bisnis tetap berlangsung.
3. Berdasarkan hasil pengukuran tingkat efektivitas, saat ini berada pada nilai 2,13 (Kurang Efektif) dengan nilai gap 1,37 dari target organisasi pada tahun 2017 yaitu 3,5 (Efektif).
4. Analisis hasil pengukuran tingkat efektivitas pada tingkat Kurang Efektif yaitu terjadi peningkatan terhadap implemnetasi SMKI, namun hanya di bagian tertentu. Dimana insiden berlangsung terus menerus namun sudah ada kesadaran untuk melakukan usaha perbaikan. Alternatif mungkin diperlukan dan harus mempertimbangkan tindakan mitigasi.

Saran :

Berdasarkan hasil penelitian yang dilakukan, dapat dikemukakan beberapa saran yang dapat dipertimbangkan untuk ditindak lanjuti, yaitu:

1. Tingkat keamanan sistem masih pada tingkat cukup efektif sehingga harus ditingkatkan sesuai dengan target organisasi yaitu tingkat efektif.
2. Menyempurnakan SOP untuk meningkatkan keamanan sistem informasi yang dapat mendukung kelancaran pelayanan SIMAK di STT Indonesia Tanjungpinang sehingga bisa meningkatkan proses bisnis.
3. Rekomendasi saran perbaikan dan prosedur sehingga dapat meningkatkan keamanan informasi. Yaitu keamanan sumberdaya manusia, keamanan fisik dan lingkungan, pengendalian akses, akuisisi, pengembangan dan pemeliharaan system informasi, terutama yang memiliki hasil penilaian yang dianggap krusial yaitu pengendalianakses , akuisisi, pengembangandanpemeliharaansisteminformasi

I. DaftarPustaka

[1]Ahmad, Deni, Dirgahayu, Teduh & Hendrik, 2013. "Manajemen Risiko Sistem Informasi Akademik pada Pergutuan Tinggi Menggunakan Actave Allegro" Yogyakarta : SNATI (Seminar Nasional Aplikasi Teknologi Informasi).

[2] Azwar, Saifuddin.(2000). Reliabilitas dan Validitas. Yogyakarta : Pustaka Belajar

[3] Djojosoedarso, Soeisno, 2000. "Prinsip-prinsip Manajemen Resiko dan Asuransi". Jakarta : Salemba 4

[4] Hidayat, M. N, 2011. "Kajian Tata Kelola Keamanan Informasi Berdasarkan Information Scurity (ISMS) ISO 27001:2005 Untuk Outsourting Teknologi Informasi Pada PT Kereta Api Indonesia (Persero)". Jakarta : Program Studi Magister Teknologi Informasi Fasikom UI.

[5] ISO/SNI 27001:2009(E)

[6] ISO/IEC 27004:2009(E)

[7] Jogiyanto, Hartono, 2005. "Analisis & Desain Sistem Informasi Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis. Andi Yogyakarta.

[8] Maryuni, Bekti, 2013. "Mengukur Keamanan Informasi : Studi Komparasi ISO 27002 dan NIST 800-55" Yogyakarta : SENTIKA2013.

[9] M, Andre & Wajong R, 2012. "Information security managemen system using ISO 27000" Jakarta : Universitas Keristen Indonesia.

[10] Rahardjo, Budi, 2005, "Keamanan Sistem Informasi Berbasis Internet"Jakarta : PT Insan Infonesia - Bandung & PT INDOCISC .

[11] Richardus Eko Indrajit.2000. "Konsep Dasar Manajemen Sistem Informasi dan Teknologi Informasi". Jakarta : Elex Media Komputindo

[12] Syafrizal, M, 2007 ISO 17799. "Standar Sistem Manajemen Keamanan Informasi" Seminar Nasional Teknologi 2700 (SNT 2007)

[13] Soenardi, Idbal & Ichsan, M, 2013. "Analisis Kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan dan Pelatihan Keuangan Diukur Menggunakan Indeks Keamanan Informasi" Jakarta : Kementrian Keuangan RI.

[14] Sugiyono, 2006, Statistika Untuk Penelitian, Cetakan Ketujuh, Bandung: CV. Alfabeta.

[15] Sugiyono (2004), *Metode Penelitian Bisnis*, CV. Alfabeta, Bandung.

[16] Zulfikar, Reza, 2013. "Audit Kepatuhan Keamanan Informasi [Karya Akhir]" Jakarta : Program Studi Magister Teknologi Informasi UI.