Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000

Mona Permatasari Mokodompit[a*], Nurlaela[b]

[a]Program Studi Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Papua
[b]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Papua

Naskah Diterima : 22 April 2016; Diterima Publikasi : 20 Juli 2016

DOI: 10.21456/vol6iss2pp97-104

Abstract

The security of an information system in a college is important since the strength of the security system will have a direct impact on the sustainability of the college. Academic information system in college is used in order to meet academic need, and therefore it's security must be maintained in order to provide useful information for its users. Assessment standard for management information system information security that is internationally recognized is ISO 17799:2000. The research aims to evaluate the security academic information system of University X based on ISO 17799:2000 and to give recommendations to improve the security. This study was conducted using interview techniques, observation and giving questionnaires to managers and users of academic information system of university X. The questionnaire used is a closed questionnaire, which is a broke-down result of ten control clauses of ISO 17799:2000. Answers gathered were then assessed based on established criteria. The results showed that the academic information system security of University X included in the category of less secure, where the result presentation obtained was 59%. In order to increase the security, University X must give special attention to work on the security policy, security organization, personnel security, physical and environmental security, communication and operation management, access control and compliance.

***Keywords*: A**academic information systems; Security system evaluation; ISO 17799:2000

Abstrak

Keamanan suatu sistem informasi dalam suatu perguruan tinggi sangatlah penting, karena kuat lemahnya sistem keamanan akan berdampak langsung pada keberlangsungan perguruan tinggi tersebut. Sistem informasi akademik pada perguruan tinggi digunakan sebagai sarana untuk memenuhi kebutuhan akademik, maka keamanannya harus dijaga agar dapat menghasilkan informasi yang bermanfaat bagi para penggunanya. Standar penilaian untuk sistem informasi manajemen keamanan informasi yang telah diakui secara internasional adalah ISO 17799:2000. Tujuan penelitian ini adalah untuk mengevaluasi keamanan sistem informasi akademik perguruan tinggi X berdasarkan standar keamanan ISO 17799:2000 dan memberikan rekomendasi untuk meningkatkan keamanannya. Penelitian ini dilakukan dengan menggunakan teknik wawancara, observasi dan pemberian kuesioner kepada pengelola dan pengguna sistem informasi akademik. Kuesioner yang digunakan adalah kuesioner tertutup yang merupakan hasil *break-down* dari sepuluh klausul kontrol ISO 17799:2000. Jawaban dari kuesioner kemudian dipersentase dan dinilai berdasarkan kriteria yang telah ditetapkan. Hasil penelitian menunjukkan bahwa keamanan sistem informasi akademik perguruan tinggi X termasuk dalam kategori kurang aman, dimana hasil persentasi yang diperoleh adalah sebesar 59%. Untuk meningkatkan keamanan masih perlu adanya perhatian khusus pada klausula kebijakan keamanan, pengorganisasian keamanan, keamanan personil, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, pengontrolan akses, dan kepatuhan.

Kata kunci : Sistem informasi akademik; Evaluasi keamanan sistem; ISO 17799:2000

1. Pendahuluan

Dalam dunia bisnis, penggunaan Sistem Informasi sangatlah penting. Menurut Anwar & Warnars (2009), sistem informasi berfungsi untuk mengumpulkan dan mengelola data atau menghasilkan informasi yang berguna dan efektif untuk mendukung kegiatan organisasi dan seluruh level manajemen yang menggunakan. Sistem informasi yang terkendali, efisien dan kompetitif dalam suatu perusahaan atau organisasi dapat

*) Penulis korespondensi: mmokodompit@gmail.com

diciptakan dengan adanya dukungan teknologi informasi.

Dewasa ini dengan makin pesatnya perkembangan teknologi, banyak organisasi dan perusahaan, termasuk Perguruan Tinggi, berusaha mengadopsi teknologi informasi terbaru untuk membantu kelancaran bisnis. Dalam Perguruan Tinggi banyak informasi yang disimpan, dikelola dan di*sharing*, sehingga besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan. Pentingnya keamanan informasi kadang terabaikan dan baru disadari setelah terjadi bencana. Mengingat kerugian sebagai akibat dari sebuah serangan terhadap sistem informasi sangat besar, maka sistem manajemen informasi harus dapat melindungi kerahasiaan, integritas dan ketersediaan informasi. Salah satu standar penilaian untuk sistem informasi manajemen keamanan informasi yang telah diakui secara internasional adalah ISO 17799:2000.

Standar ISO 17799:2000 memiliki 10 klausul kontrol keamanan untuk meminimalkan resiko ke level yang dapat diterima, yaitu: kebijakan kemanan, pengorganisasian keamanan, klasifikasi dan kontrol aset, keamanan personil, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, pengontrolan akses, pengembangan dan pemeliharaan sistem, manajemen kelangsungan bisnis serta kepatuhan.

Hasil evaluasi dengan menggunakan ISO 17799:2000 dapat menunjukkan seberapa baik (atau seberapa buruk) keamanan informasi yang diterapkan oleh suatu organisasi atau perusahaan, sehingga standar ini dapat digunakan sebagai suatu alat untuk organisasi atau perusahaan, termasuk Perguruan Tinggi, dalam membangun atau memperbaiki keamanan informasi dalam organisasi mereka. Adapun kriteria penilaian digunakan kriteria penilaian Peltier (2002) dimana hasilnya akan menunjukkan tingkat keamanan sistem informasi yang diteliti.

Berdasarkan perumusan masalah diatas, tujuan penelitian ini adalah untuk mengevaluasi apakah keamanan Sistem Informasi Akademik (SIA) PT. X telah memenuhi standar keamanan berdasarkan ISO 17799:2000 dengan menggunakan kriteria penilaian menurut Peltier (2002), dan untuk memberikan informasi dan/atau rekomendasi kepada PT. X atas hasil evaluasi keamanan SIA yang dilaksanakan.

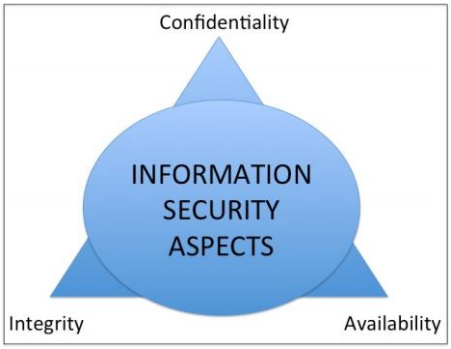
2. Kerangka Teori

2.1. Pengertian Sistem Informasi

Sistem informasi adalah sekumpulan komponen yang saling berhubungan, mengumpulkan atau mendapatkan, memproses, menyimpan, dan mendistribusikan informasi untuk menunjang pengambilan keputusan dan pengawasan dalam suatu organisasi (Kenneth dan Jane, 2007). Informasi sendiri berarti data yang telah diolah menjadi sesuatu yang memiliki arti dan berguna bagi yang menerimanya (Afrianto et al., 2015). Sebaliknya, data merupakan sekumpulan fakta mentah yang belum dikelola ke dalam bentuk yang dapat secara efektif dipahami oleh manusia.

2.2. Keamanan Sistem Informasi

Informasi pada sistem informasi merupakan salah satu aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu informasi seharusnya dilindungi agar aman dan terbebas dari ancaman atau bahaya. Keamanan sistem informasi bertujuan untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat segala kerusakan sistem. Keamanan informasi memiliki beberapa aspek yang harus dipahami dan dilindungi. Menurut Sarno dan Iffano (2009), ada tiga aspek yang paling umum atau disebut dengan C.I.A *triangle model*, seperti tampak pada Gambar 1.



Gambar 1. Aspek Keamanan Informasi (Sarno & Iffano, 2009)

Aspek keamanan sistem informasi dapat dijelaskan: 1) Kerahasiaan (*confidentiality*): informasi dipastikan hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan; 2) Intergritas (*integrity*): akurasi dan kelengkapan informasi dilindungi melalui sejumlah metodologi pengolahan yang efektif; 3) Ketersediaan (*availability*): memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

2.3. Ancaman Keamanan Sistem Informasi

Menurut Hendradhy (2009), masalah keamanan sistem informasi ada 2 yaitu: "*threat*" (ancaman) dan "*vulnerability*" (kelemahan). Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman terhadap sistem informasi dapat dibagi menjadi 2 macam yaitu ancaman aktif dan ancaman pasif (Bodnar dan Hopwood, 2006). Yang termasuk dalam ancaman aktif yaitu kecurangan dan kejahatan terhadap komputer, sedangkan yang

termasuk dalam ancaman pasif adalah bencana alam, kesalahan manusia, dan kegagalan sistem/lingkungan (Bodnar dan Hopwood, 2006).

Dengan adanya ancaman-ancaman tersebut, maka harus dilakukan usaha untuk melindungi keamanan sistem informasi yang dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang dimaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, dan fungsi-fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruh sasaran keamanan yang dimaksud dapat tercapai.

2.4. Standarisasi Keamanan Sistem Informasi

Ancaman dan resiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data atau informasi menjadi alasan disusunnya standar manajemen keamanan sistem informasi yang salah satunya adalah ISO (*the International Organization for Standardization*) 17799. Penyusunan standar ini dipersiapkan oleh Institut Standar Inggris (dikenal sebagai BS 7799) pada tahun 1995. BS 7799 terdiri dari 2 bagian, yaitu: *Part 1, The Code of Practice for Information Security Management. Part 2, The Specification for Information Security Management Systems.* Pada tahun 2000, *International Organization for Standardization* (ISO) dan *International Electro-Technical Commission* (IEC) mengadopsi BS 7799 *Part 1* dan menerbitkannya sebagai standar ISO 17799:2000 yang telah diakui secara internasional sebagai standar sistem manajemen keamanan informasi.

BS 7799 *Part 1* atau ISO 17799:2000 meliputi 10 klausul control keamanan (*security control clauses*), yaitu: kebijakan keamanan (*security policy*), pengorganisasian keamanan (*security organization*), klasifikasi dan kontrol aset (*asset clasification and control*), keamanan personil (*personnel security*), keamanan fisik dan lingkungan (*physical and environmental security*), manjemen Komunikasi dan Operasi (*communication and operations management*), pengontrolan akses (*access control*), Pengembangan dan pemeliharaan sistem (*system development and maintenance*), manajemen kelangsungan bisnis (*business continuity management*), dan kepatuhan (*compliance*).

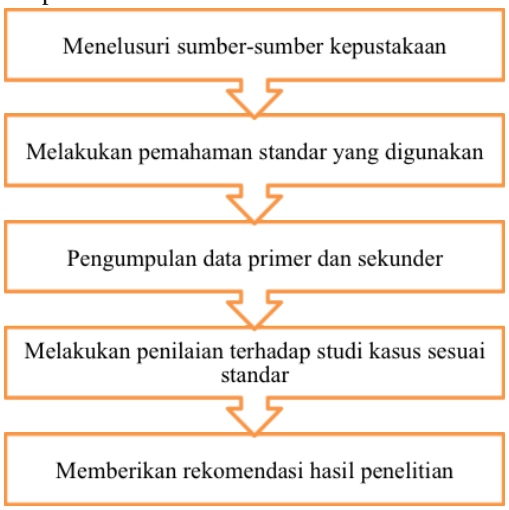
Keuntungan utama dari ISO 17799 berhubungan dengan kepercayaan publik adalah standar ini merupakan tanda kepercayaan dalam seluruh keamanan perusahaan. Suatu organisasi yang menerapkan ISO 17799 akan mempunyai suatu alat untuk mengukur, mengatur dan mengendalikan informasi yang penting bagi operasional sistem mereka. Hal ini tentunya dapat mendorong kearah kepercayaan pelanggan, efisiensi dan efektifitas.

2.5. Evaluasi Keamanan Sistem Informasi

Hal yang penting dalam pelaksanaan sistem manajemen keamanan informasi adalah melakukan evaluasi. Evaluasi diadakan dengan tujuan untuk menjaga kesesuaian antara sistem manajemen keamanan informasi dengan kebutuhan organisasi. Untuk itu sistem manajemen keamanan informasi perlu selalu ditinjau, dikoreksi dan diperbaiki sesuai dengan kebutuhan organisasi. Menurut Rahardjo (2005), evaluasi terhadap keamanan sistem informasi harus selalu dilakukan walaupun sudah ada perangkat pengamanan karena timbulnya lubang keamanan yang baru.

3. Metodologi

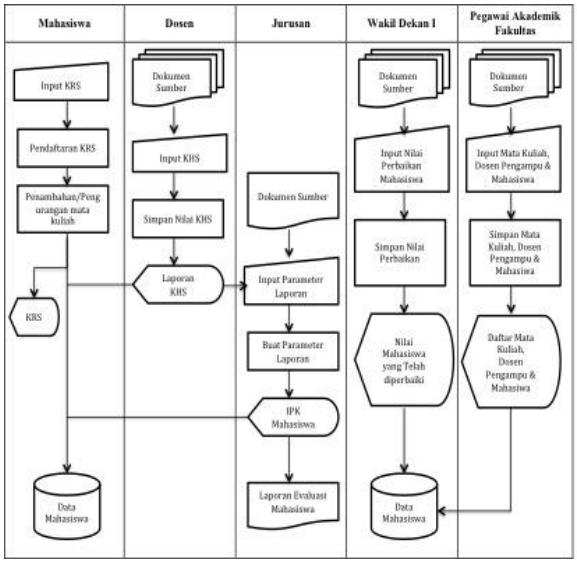
Tujuan penelitian ini adalah untuk mengevaluasi apakah keamanan Sistem Informasi Akademik (SIA) PT. X telah memenuhi standar keamanan berdasarkan ISO 17799:2000 dengan menggunakan kriteria penilaian menurut Peltier (2002), dan untuk memberikan informasi dan/atau rekomendasi kepada PT. X atas hasil evaluasi keamanan SIA yang dilaksanakan. Sementara metode penelitiannya dapat dilihat pada Gambar 2.



Gambar 2. Metode Penelitian

3.1. Obyek Penelitian

Perguruan tinggi (PT) X memiliki SIA yang berfungsi untuk melayani seluruh proses akademik dan memberikan laporan yang berkaitan dengan bidang akademik. SIA tersebut dikelola oleh Bagian Akademik PT. X dan UPT Teknologi Informasi Komputer PT. X dengan menggunakan program Grama Tekno. SIA PT. X berkaitan dengan pengembangan sistem, pemeliharaan data, *back up and recovery*, dan *networking system.* Untuk setiap fakultas dikontrol dari satu pusat, yang mana dari segi struktur data di database untuk tiap fakultas sama, sedangkan dari segi kurikulum dan mahasiswa berbeda. Proses SIA diawali dengan pendaftaran mahasiswa, lalu kemudian transaksi akademik per semester. Bagan alir data SIA dapat dilihat pada Gambar 3.



Gambar 3. Bagan Alir Data SIA PT. X

3.2. Jenis dan Sumber Data

Data yang digunakan dalam penelitian ini adalah data primer dan sekunder. Data primer diperoleh langsung dari responden, yaitu para pengelola dan pengguna SIA PT.X. Sedangkan data sekunder berupa data yang diperoleh dari buku, literatur atau artikel yang berhubungan dengan data mengenai SIA perguruan tinggi secara umum dan standar keamanan yang digunakan untuk mengevaluasi kemanan sistem informasi.

3.3. Mekanisme Pengumpulan Data

Pengumpulan data primer untuk melakukan evaluasi keamanan SIA PT. X adalah dengan melakukan wawancara, observasi (pengamatan) dan pemberian kuesioner kepada responden. Penggunaan instrumen kuesioner dan wawancara dilakukan untuk memperoleh gambaran tentang status keamanan sistem informasinya, sedangkan observasi lapangan dilakukan untuk mendapatkan informasi dan data-data secara langsung dari obyek penelitian. Pemberian kuesioner dan wawancara kepada pengguna dikhususkan untuk sub kendali klausula Pelatihan Pengguna dan sub kendali klausula Menanggapi Kejadian dan Salah Fungsi Keamanan pada klausula Keamanan Informasi. Adapun pengumpulan data sekunder dilakukan dengan cara studi dokumen baik dari buku, literatur atau artikel.

3.4. Teknik Pengolahan Data

Data pada penelitian ini dikumpulkan menggunakan kuesioner tertutup yang diadaptasi langsung dari Peltier (2002). Peltier (2002) mem-*breakdown* sepuluh klausul kontrol keamanan ISO 17799:2000 yang terdiri dari beberapa sub kontrol menjadi 128 kuesioner/pertanyaan. Skala yang digunakan dalam kuesioner penelitian ini adalah skala Guttman, dimana masing-masing pertanyaan pada kuesioner mempunyai pilihan jawaban ya atau tidak. Jumlah jawaban "ya" yang akan menentukan tingkat keamanan dari sistem informasi yang diteliti. Untuk jawaban "tidak" untuk sebuah *control* dari responden akan dianalisis dan dilihat peranan *control*-nya serta potensi bahaya yang dapat ditimbulkan didalam sistem. Kemudian akan diberikan rekomendasi mengenai bagaimana seharusnya *control* tersebut diberlakukan agar keamanan sistem informasi didalamnya menjadi lebih terjamin. Standar penilaian dan penyebaran kuesioner Peltier (2002) pada klausul sub kontrol ISO 17799:2000 dapat dilihat pada Lampiran 1. Sedangkan untuk kriteria penilaian keamanan sistem informasi menurut Peltier (2002) dapat dilihat pada Tabel 1.

Tabel 1. Kriteria Penilaian Keamanan Sistem Informasi

Kategori	Skor/Persentase Keamanan
Baik sekali/aman	> 95 jawaban "ya" (≥74%)
Baik/cukup aman	> 82 – 95 jawaban "ya" (64-73%)
Cukup/kurang aman	> 68 – 81 jawaban "ya" (53-63%)
Kurang/tidak aman	> 54 – 67 jawaban "ya" (42-52%)
Beresiko/beresiko tinggi	< 54 jawaban "ya" (≤41%)

4. Hasil dan Pembahasan

Pada bagian ini diberikan hasil evaluasi kemanan sistem informasi akademik Universitas X yang diperoleh. Dari data penilaian yang telah dilakukan diperoleh tingkat keamanan untuk masing-masing klausul ISO 17799:2000 di PT. X.

4.1. Hasil Penilaian Keamanan SIA PT.X

Untuk Klausul I pada Tabel 3, yaitu Kebijakan Keamanan menunjukkan bahwa kebijakan keamanan SIA PT. X berdasarkan kriteria penilaian Peltier (2002) termasuk dalam kategori **beresiko tinggi** dengan persentase keamanan 0%. Sementara pada klausul II Pengorganisasian Keamanan termasuk dalam kategori **kurang aman** dengan persentase keamanan 54%. Sedangkan untuk klausul III terkait klasifikasi dan control asset memperoleh persentase keamanan sebesar 100% sehingga berdasarkan kriteria penilaian Peltier (2000) klausul ini termasuk dalam kategori **aman**. Klausul IV, keamanan personil, termasuk dalam kategori **tidak aman** dengan nilai persentase keamanan 50%. Untuk klausul V (keamanan fisik dan lingkungan) tingkat keamanannya masuk dalam kategori **tidak aman** dengan persentase keamanan 42%.

Tabel 2. Hasil Penilaian Tingkat Keamanan SIA PT.X

Klausul	Kontrol Klausul	Jumlah Jawaban Ya/Total Pertanyaan	Persentase Keamanan	Tingkat Keamanan
I	Kebijakan Keamanan	0/2	0%	Beresiko Tinggi
II	Pengorganisasian Keamanan	6/11	54%	Kurang Aman
III	Klasifikasi & Kontrol Aset	3/3	100%	Aman
IV	Keamanan Personil	5/10	50%	Tidak Aman
V	Keamanan Fisik & Lingkungan	5/12	42%	Tidak Aman
VI	Manajemen Komunikasi & Operasi	13/23	57%	Kurang Aman
VII	Pengontrolan Akses	20/33	61%	Kurang Aman
VIII	Pengembangan & Pemeliharaan Sistem	14/18	78%	Aman
IX	Manajemen Kelangsungan Bisnis	4/5	80%	Aman
X	Kepatuhan	5/11	45%	Tidak Aman
Tingkat Keamanan Menyeluruh		75/128	59%	Kurang Aman

Pada Tabel 2 juga menunjukkan bahwa tingkat keamanan pada klausul VI (manajemen komunikasi dan operasi) dan VII (pengontrolan akses) masuk dalam kategori **kurang aman**. Sedangkan untuk klausul VIII (pengembangan dan pemeliharaan sistem) dan IX (manajemen kelangsungan bisnis) masuk dalam kategori **aman**. Sementara untuk klausul X, kepatuhan, tingkat keamanannya masuk dalam kategori **tidak aman.**

Dengan demikian hasil evaluasi keamanan SIA PT. X secara keseluruhan dilihat dari jumlah hasil nilai "ya" dari kesepuluh klausul memperoleh total nilai sebanyak 75 dari 128 atau 59%. Berdasarkan kriteria penilaian Peltier (2002) maka dapat disimpulkan bahwa keamanan SIA PT. X masuk dalam kategori **kurang aman**.

4.2. Rekomendasi Keamanan SIA untuk PT.X

Dari hasil persentase yang diperoleh ini dapat disimpulkan bahwa tingkat keamanan SIA PT.X termasuk dalam kategori kurang aman. Adapun hal-hal yang dapat direkomendasikan untuk meningkatkan tingkat keamanan SIA PT.X adalah sebagai berikut:

1. Klausul I Kebijakan Keamanan [Beresiko Tinggi]: Menetapkan langkah untuk menyusun dan memublikasikan kebijakan keamanan informasi kepada pengguna di seluruh tataran organisasi.
2. Klausul II Pengorganisasian Keamanan [Kurang Aman]: Membentuk forum yang tugasnya mengawasi dan mendukung pelaksanaan keamanan informasi dan menetapkan persyaratan keamanan jika melibatkan pihak ketiga untuk mengakses SIA.
3. Kalusul III Klasifikasi dan Kontrol Aset [Aman]: Mempertahankan perlindungan yang telah diberikan kepada aset perguruan tinggi dan aset informasi.
4. Klausul IV Keamanan Personil [Cukup Aman]: Menetapkan prosedur pelaporan secara resmi terkait keamanan SI, mewajibkan pengguna untuk melaporkan setiap kelemahan sistem informasi dan menetapkan sangsi untuk menindak para pegawai yang melanggar kebijakan dan prosedur keamanan.
5. Klausul V Keamanan Fisik dan Lingkungan [Tidak Aman]: Memastikan untuk memeriksa ruangan yang digunakan secara berkala, melindungi peralatan secara fisik dari ancaman keamanan, mengadakan pengawasan dan pemantauan kepada pihak ketiga yang bekerja di dalam ruangan dan memberikan otorisasi dan perijinan bagi penggunaan peralatan diluar ruangan.
6. Kalusul VI Manajemen Komunikasi dan Operasi [Kurang Aman]: Mendokumentasikan dan memelihara prosedur operasi yang ditetapkan dalam kebijakan pengamanan dengan jelas, memantau kapasitas penyimpanan informasi, memproyeksikan kebutuhan kapasitas di masa depan, menetapkan prosedur formal untuk pembuangan media secara aman dan menetapkan pengaturan pertukaran informasi dan piranti lunak.
7. Kalusul VII Pengontrolan Akses [Kurang Aman]: Menetapkan peraturan dan hak kontrol akses untuk setiap pengguna, menetapkan proses manajemen kata sandi yang formal dimana pengguna dipersyaratkan untuk memelihara kata sandinya, menggunakan identifikasi terminal otomatis, akses oleh pengguna remote harus diotentikasi, dan mengembangkan kebijakan formal yang dapat memengaruhi resiko bekerja dengan fasilitas komputasi bergerak, khususnya dilingkungan yang tidak terlindungi.
8. Klausul VIII Pengembangan dan Pemeliharaan Sistem [Aman]: Mempertimbangkan otentikasi

pesan dan mengembangkan kebijakan tentang penggunaan kendali kriptografi untuk kebutuhan perlindungan informasi.

9. Klausul IX Manajemen Kelangsungan Bisnis [Aman]: Melakukan sosialisasi terkait proses manajemen kelangsungan usaha ke seluruh tataran organisasi.
10. Klausula X Kepatuhan [Tidak Aman]: Mendefinisikan dan mendokumentasikan hukum terkait peraturan dan persyaratan kontrak secara khusus untuk setiap informasi, meminta nasehat mengenai kepatuhan organisasi pada hukum, dan memberi perlindungan untuk akses terhadap perangkat audit sistem.

5. Kesimpulan

Setelah melakukan evaluasi terhadap keamanan SIA PT.X dengan menggunakan kuesioner yang di*breakdown* dari sepuluh klausula ISO 17799, maka diperoleh nilai 75 (dari maksimal 128) atau 59%. Dari hasil presentase yang diperoleh ini dapat disimpulkan bahwa tingkat keamanan SIA PT.X termasuk dalam kategori kurang aman. Untuk meningkatkan keamanan SIA PT.X perlu adanya perhatian khusus kepada klausula kebijakan keamanan, pengorganisasian keamanan, keamanan personil, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, pengontrolan akses, dan kepatuhan. Selain itu perlu adanya peningkatan pemahaman standar keamanan informasi menurut ISO.

Ucapan Terima Kasih

Ucapan terima kasih sebesar-besarnya disampaikan kepada pihak pengelola dan pengguna SIA PT. X yang telah memberikan kontribusi sehingga penelitian ini berhasil diselesaikan dengan baik.

Daftar Pustaka

Afrianto, I., Suryana, T., & Sufa'atin. 2015. Pengukuran dan Evaluasi Keamanan Sistem Informasi Menggunakan Indeks KAMI-SNI

ISO/IEC 27001:2009. ULTIMA InfoSys, Vol. VI, No.1, 43.

Anwar, C. & Warnars H.L.H.S. 2009. Sistem Informasi Akademik Online Sebagai Penunjang Sistem Perkuliahan. Fakultas Teknologi Informasi Universitas Budi Luhur. Website: http://arxiv.org/pdf/1006.2082, (diunggah 13 April 2015).

Bodnar G.H. & Hopwood W.S., 2006. Sistem Informasi Akuntansi Edisi 9. ANDI. Yogyakarta.

Hendradhy, O. 2009. Keamanan sistem informasi apa dan bagaimana?. Website: http://mugi.or.id/blogs/oke/archive/2008/12/16/keamanan-sistem-informasi-apa-dan-bagaimana.aspx, (diunggah 13 April 2015)

Kenneth C. L. & Jane P. L., 2007 . Sistem Informasi Manjemen, Buku I, Edisi ke-10. Penerbit Salemba Empat: Jakarta.

Peltier, T.K., 2002. ISO 17799 Self Assessment Checklist. Website: http://www.cccure.org, (diunggah 13 April 2015).

Rahardjo, B. 2005. Keamanan Sistem Informasi Berbasis Internet.PT Insan Indonesia, Bandung dan PT INDOCISC, Jakarta.

Sarno, R. & Iffano, I., 2009. Sistem Manajemen Keamanan Informasi berbasis ISO 27001. ITS Press. Surabaya.

Lampiran 1. Standar Penilaian dan Penyebaran Kuesioner Peltier (2002) padal ISO 17799:2000

No.	Kontrol Klausul	Standar Penilaian	Total Pertanyaan
1	Kebijakan Keamanan		
	Kebijakan Keamanan Informasi	Adanya arahan kepada manajemen dan dukungan untuk keamanan informasiyang tersusun secara jelas.	2
2	Pengorganisasian keamanan		
	Infrastruktur Keamanan Informasi	Tersusunnya kerangka kerja manajemen.	7
	Keamanan Akses Pihak Ketiga	Terjaganya fasilitas-fasilitas TI organisasi dan aset-aset informasi yang mengendaliakan akses pihak ketiga yang non-organisasi.	3
	Mengalihdayakan (*Outsourcing*)	Dipertahankannya keamanan informasi bahkan ketika tanggung jawab pemrosesan dialihdayakan kepada organisasi lain	1
3	Klasifikasi dan Kontrol Aset		
	Akuntansi Aset	Tersusunnya akuntansi yang memadai atas akses organisasi.	1
	Klasifikasi Informasi	Digunakannya klasifikasi keamanan untuk menunjukkan keperluan akan, dan prioritas untuk, perlindungan keamanan aset informasi.	2
4	Keamanan Personil		
	Keamanan dalam Definisi Kerja dan Pensumberdayaan	Keamanan telah ditangani sejak tahapan perekrutan, termasuk yang menyangkut deskripsi tugas dan kontrak, dan dipantau selama seseorang dipekerjakan.	4
	Pelatihan Pengguna	Adanya pelatihan bagi para pengguna dalam hal prosedur keamanan dan penggunaan fasilitas TI yang benar.	1
	Menanggapi Kejadian dan Salah Fungsi Keamanan	Pelaporan terkait kejadian-kejadian yang mempengaruhi keamanan dilakukan secepat mungkin melalui jalur manajemen.	5
5	Keamanan Fisik dan Lingkungan		
	Wilayah yang Diamankan	Pengamanan fasilitas TI yang mendukung kegiatan.	5
	Keamanan Peralatan	Perlindungan peralatan secara fisik.	5
	Kendali Umum	Terlindunginya informasi dan fasilitas pemrosesan informasi.	2
6	Manajemen Komunikasi dan Operasi		
	Prosedur dan Tanggung Jawab Operasional	Ditetapkannya tanggung jawab dan prosedur untuk manajemen dan operasi semua komputer dan jaringan.	5
	Perencanaan dan Penerimaan Sistem	Perencanaan dan persiapan sebelumnya dapat memastikan ketersediaan kemampuan dan sumber daya yang memadai.	2
	Perlindungan dari Peranti Lunak yang Berbahaya	Menerapkan prinsip kehati-hatian untuk mencegah dan mendeteksi peranti lunak yang berbahaya.	1
	Pemeliharaan	Tersusunnya prosedur rutin untuk membuat salinan data cadangan, mencatat peristiwa-peristiwa dan kesalahan-kesalahan, dan jika sesuai, memantau lingkungan peralatan.	3
	Manajemen Jaringan	Diaturnya keamanan jaringan komputer yang dapat menjangkau batas-batas organisasi untuk mengamankan informasi dan untuk melindungi infrastruktur pendukung.	1
	Penanganan dan Keamanan Media	Media komputer dikendalikan dan secara fisik dilindungi.	4
	Pertukaran Informasi dan Peranti Lunak	Pertukaran Informasi maupun data dan Peranti Lunak antarorganisasi dikendalikan untuk mencegah penghilangan, perubahan, atau penyalahgunaan data.	7
7	Pengontrolan Akses		
	Persyaratan Bisnis untuk Akses Sistem	Kebijakan untuk penyebarluasan dan pemilikan hak atas informasi harus mengendalikan akses terhadap layanan komputer dan data berdasarkan persyaratan bisnis.	1

No.	Kontrol Klausul	Standar Penilaian	Total Pertanyaan
	Manajemen Akses Pengguna	Prosedur resmi diperlukan untuk mengendalikan alokasi hak-hak akses terhadap layanan TI.	4
	Tanggung Jawab Pengguna	Pengguna disadarkan atas tanggung jawab mempertahankan kendali akses yang efektif..	3
	Kendali Akses Jaringan	Koneksi pada layanan-layanan jaringan dikendalikan untuk memastikan bahwa para pengguna atau layanan komputer yang terhubung tidak /berkompromi dalam soal keamanan dengan layanan jaringan lainnya.	9
	Kendali Akses Sistem Operasi	Akses terhadap komputer harus sangat terbatas melalui penggunaan: ● Identifikasi terminal otomatis; ● Prosedur log masuk terminal;; ● Identitas pengguna: ● Manajemen kata sandi; ● Tanda bahaya yang mengancam; ● Jeda terminal; dan ● Waktu koneksi terbatas.	9
	Kendali Akses Aplikasi	Mendukung kendali akses logis untuk melindungi sistem-sistem aplikasi dan data dari akses tanpa izin.	2
	Akses dan Penggunaan Sistem Pemantauan (*Monitoring*)	Dipantaunya sistem-sistem.	3
	Beraktivitas secara M*obile* dan Bekerja Jarak Jauh dengan bantuan alat komunikasi	Ketika menggunakan komputer mobil dan bekerja jarak jauh, organisasi memeriksa resiko dan menerapkan perlindungan yang sesuai dengan peralatan atau lokasinya.	2
8	Pengembangan dan Pemeliharaan Sistem		
	Persyaratan Keamanan Sistem-sistem	Persyaratan keamanan harus diidentifikasi, dibenarkan, disetujui, dan didokumentasi sebagai bagian dari tahapan definisi persyaratan dari semua proyek pengembangan sistem TI.	1
	Keamanan dalam Sistem Aplikasi	Kendali keamanan yang mematuhi standar industri praktik keamanan yang baik.	4
	Kendali Kriptografis	Digunakannya sistem kriptografis dan teknik.	5
	Keamanan Arsip-arsip Sistem	Pengendalian akses terhadap arsip-arsip sistem aplikasi diberikan pada dan dilakukan oleh fungsi pengguna pemilik atau kelompok pengembang.	3
	Keamanan dalam Lingkungan Pengembangan & Dukungan	Lingkungan proyek dan dukungan secara ketat dikendalikan.	5
9	Manajemen Kelangsungan Bisnis (*Business Continuity Management)*		
	Aspek-aspek Perencanaan Keberlanjutan Bisnis	Adanya rencana-rencana keberlanjutan bisnis untuk menghadapi gangguan terhadap aktivitas bisnis.	5
10	Kepatuhan		
	Kepatuhan pada Persyaratan Hukum	Semua persyaratan terkait untuk setiap sistem TI didefinisikan dan didokumentasikan.	7
	Tinjauan Kebijakan Keamanan dan Kepatuhan Teknis	Tinjauan terhadap kepatuhan dilakukan secara teratur.	2
	Pertimbangan Audit Sistem	Adanya kendali atas sistem operasional dan perangkat audit.	2
	Total Pertanyaan		128