KOMBINASI STANDAR ISO17799, SSE-CMM UNTUK PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SISTEM INFORMASI PENJADWALAN

Ali Haidir[1], Mochamad Wahyudi[2]
AMIK BSI Jakarta[1], ali.alh@bsi.ac.id
STMIK Nusa Mandiri Jakarta[2], wahyudi@nusamandiri.ac.id

ABSTRACT

Bina Sarana Informatika is one of the largest educational institutions now have to process the data with a large number. The data were processed by the existing scheduling system scheduling information, is still very vulnerable to attack or destruction committed by people who are not responsible nor caused by system failures. This study examines the level of information security in the course scheduling Bina Sarana Informatika to get accurate measurement results, and to determine the level of system security scheduling information useful as input in improving the quality of information systems security. Using qualitative research methods, that is by distributing a questionnaire that contains a list of questions based on ISO 17799 on the implementation of information security management consisting of 11 clauses. The data is processed using the results of the questionnaire maturity level to get the level of maturity of information security. This research resulted in the existing clause of 11, the average was at the level of unity (Initial / ad hoc). The conclusion that can be is that the security of information systems at the BSI scheduling still needs improvement. But there are some clauses that already meet the standards of ISO 17799, the sixth clause of management and organizational communication and seventh clause of access control.

***Keyword**: ISO 17799, Security Of Informations System, SSE-CMM.*

ABSTRAK

Bina Sarana Informatika merupakan salah satu institusi pendidikan terbesar saat ini yang harus mengolah data dengan jumlah yang banyak. Data yang diolah oleh bagian penjadwalan yang ada pada sistem informasi penjadwalan, masih sangat rentan oleh penyerangan atau perusakan yang dilakukan oleh orang yang tidak bertanggung jawab maupun yang disebabkan oleh kegagalan sistem. Penelitian ini mengkaji tingkat keamanan informasi pada bagian penjadwalan perkuliahan Bina Sarana Informatika untuk mendapatkan hasil pengukuran yang akurat, dan untuk mengetahui tingkat keamanan sistem informasi penjadwalan yang berguna sebagai masukan dalam usaha peningkatan kualitas keamanan sistem informasi. Dengan menggunakan metode penelitian kualitatif, yaitu dengan cara penyebaran kuisioner yang berisi daftar pertanyaan berdasarkan ISO 17799 tentang pelaksanaan manajemen keamanan informasi yang terdiri dari 11 klausa. Data hasil kuesioner diolah menggunakan maturity level untuk mendapatkan tingkat kematangan keamanan informasi. Penelitian ini menghasilkan bahwa dari 11 klausa yang ada, rata-rata berada pada level kesatu (Initial/ad hoc). Kesimpulan yang di dapat adalah bahwa keamanan sistem informasi di bagian penjadwalan BSI masih perlu perbaikan. Namun ada beberapa klausa yang sudah memenuhi standar ISO 17799, yaitu klausa keenam tentang manajemen komunikasi dan organisasi serta klausa ketujuh tentang kontrol akses.

Kata Kunci: ISO 17799, Keamanan Sistem Informasi, SSE-CMM.

PENDAHULUAN

Perkembangan teknologi yang sangat cepat saat ini membuat perusahaan dan pelaku bisnis harus dapat beradaptasi dengan cepat, kebutuhan akan informasi dan koneksi data untuk update informasi tidak mengenal waktu dan tempat, kemungkinan terjadinya gangguan keamanan informasi semakin meningkat. Untuk itu perusahaan harus menerapkan kebijakan yang tepat untuk melindungi aset informasi yang dimiliki. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi.

ISO 17799 adalah standar internasional yang menyediakan petunjuk dan kontrol untuk mengatur keamanan sistem informasi. Keamanan informasi didefinisikan sebagai perlindungan kerahasiaan, integritas, dan ketersediaan. Ini dapat dicapai dengan menerapkan kontrol yang dapat berupa kebijakan, praktek, prosedur, struktur organisasi atau software yang berisi 133 kontrol dari 11 area yang dapat diterapkan di tingkat organisasi atau tingkat aplikasi. Kontrol tingkat organisasi berlaku pada batas dimana organisasi berada dan dibutuhkan agar aplikasi aman. ISO 17799 memberikan kontrol keamanan tetapi bukan kontrol itu dikembangkan atau diatur, ini disebabkan ISO bukan standar teknis juga bukan untuk teknologi tertentu. Oleh karena itu tidak ada mekanisme penilaian atau metoda evaluasi. ISO 17799 menyarankan bahwa pemilihan kontrol yang akan digunakan berdasarkan oleh resiko, peraturan, hukum dan undang-undang serta prinsip, tujuan dan kebutuhan informasi organisasi.

Penulisan ini akan menganalisis tingkat keamanan sistem informasi penjadwalan kuliah pada bagian penjadwalan Bina Sarana Informatika, karena saat ini data yang diolah oleh bagian penjadwalan Bina Sarana Informatika masih sangat rentan oleh penyerangan atau perusakan yang dilakukan oleh orang yang tidak bertanggung jawab maupun yang disebabkan oleh kegagalan sistem. Hasil studi yang dihasilkan diharapkan dapat digunakan sebagai pertimbangan dalam rangka menyusun langkah perbaikan sistem manajemen keamanan informasi di Bina Sarana Informatika.

Berdasarkan permasalahan tersebut penulis membuat rumusan masalah yang didapatkan pada penelitian ini, antara lain:

1. Bagaimanakah tingkat keamanan sistem informasi pengolahan data penjadwalan di Bina Sarana Informatika ?
2. Bagaimanakah tingkat kesiapan sistem informasi pengolahan data penjadwalan di Bina Sarana Informatika dalam penerapan keamanan sistem informasi ?
3. Bagaimanakah peranan standarisasi keamanan sistem informasi dalam menjaga informasi yang tersimpan dari berbagai ancaman yang ada ?

Tujuan dari penelitian ini adalah mendapatkan hasil pengukuran yang akurat dalam hal keamanan sistem informasi pada sistem informasi penjadwalan di Bina Sarana Informatika dan meningkatkan kualitas keamanan sistem informasi sesuai dengan standar yang diterapkan pada ISO 17799. Selain itu untuk mengetahui tingkat kematangan sistem keamanan informasi yang sudah diterapkan pada sistem informasi penjadwalan Bina Sarana Informatika.

KAJIAN LITERATUR

Keamanan Sistem Informasi.

Menurut Simanungkalit (2009) keamanan informasi adalah "perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan bisnis, mengurangi resiko bisnis, dan meningkatkan return of investment dan peluang bisnis".

Menurut HARR dalam Simanungkalit (2009) keamanan informasi meliputi perlindungan terhadap aspek-aspek berikut:

a. Confidentiality (Kerahasiaan).
b. Integrity (Integritas).
c. Availability (Ketersediaan).

Ketiga aspek tersebut dikenal dengan CIA Triad, dan menjadi prinsip dasar keamanan informasi.

Gambar 1
CIA Triad

Information Security Management System (ISMS).

Menurut BSI (2008), ISMS merupakan bagian dari sistem manajemen secara keseluruhan berdasarkan pendekatan resiko bisnis untuk membangun, melaksanakan, beroperasi, memantau, meninjau, mempertahankan dan meningkatkan keamanan informasi. ISMS merupakan sekumpulan kebijakan-kebijakan yang berhubungan dengan manajemen keamanan informasi. Konsep kunci dari ISMS adalah agar organisasi / perusahaan merancang, menerapkan dan memelihara rangkaian yang berkaitan dari proses dan sistem untuk secara efektif mengelola aksesibilitas informasi, kemudian memastikan confidentiality, integrity dan availability dari aset-aset informasi dan meminimalkan resiko-resiko keamanan informasi.

Standar ISO 17799

Latar belakang disusunnya ISO 17799 standar untuk manajemen keamanan sistem informasi adalah karena diperlukannya suatu cara bagaimana data atau informasi tersebut dikelola, dipelihara dan diekspos. Awalnya ISO 17799 adalah standar internasional yang menyediakan petunjuk dan kontrol untuk mengatur keamanan informasi. ISO 17799 berasal dari standar yang dikembangkan *Department of Trade and Industry* (DIT) tahun 1993. British Standards Institute (BSI) mengambil alih dan memperbaikinya kemudian disebut BS 7799 tahun 1995.

Menurut Ngqondi (2009) "ISO 17799 mendefinisikan 133 buah kontrol keamanan yang terstruktur dan dikelompokkan menjadi 11 clauses untuk memudahkan dalam mengidentifikasi hal-hal yang dibutuhkan untuk mengamankan aset informasi perusahaan." Berikut ini adalah 11 clauses yang terdapat dalam ISO 17799 :

a. *Security Policy.*
b. *Organization of Information Security.*
c. *Assets Management.*
d. *Human Resource Security.*
e. *Physical and Environment Security.*
f. *Communications and Operations Management.*
g. *Access Control.*
h. *Information Systems Acquisition, Development and Maintenance.*
i. *Incident Management.*
j. *Bussiness Continuity Management.*
k. *Compliance.*

Systems Security Engineering – Capabilty Maturity Model (SSE-CMM).

Menurut Hopkinson (1999) "SSE-CMM (Systems Security Engineering – Capability Maturity Model) menjelaskan karakteristik penting dari suatu proses rekayasa keamanan organisasi yang harus ada untuk memastikan teknik keamanan yang baik dengan tidak menganjurkan proses tertentu atau berurutan, namun mengambil praktek secara umum yang diamati dalam industri."

Model SSE-CMM memberikan gambaran menyeluruh tentang prinsip-prinsip dan arsitektur yang didasarkan SSE-CMM, gambaran eksekutif dari model, saran untuk pengggunaan model yang tepat, praktek-praktek yang termasuk dalam model, dan deskripsi atribut dari model. Metode penilaian SSE-CMM menjelaskan proses dan alat untuk mengevaluasi kemampuan teknik keamanan organisasi.

METODE PENELITIAN

Dalam penelitian ini penulis menggunakan metode penelitian kualitatif, data yang diperoleh berdasarkan hasil penyebaran kuesioner yang diberikan ke bagian penjadwalan. Populasi dalam penelitian ini yaitu karyawan pada Bagian Penjadwalan yang berada di Biro Administrasi Akademik Kemahasiswaan (BAAK) Bina Sarana Informatika yang berjumlah 7 orang. Penentuan jumlah sampel dari

populasi tertentu yang dikembangkan dari Isaac dan Michael, untuk jumlah populasi 7 jumlah anggota sampel sebenarnya hanya 9,56 tetapi dibulatkan menjadi 7 (Sugiyono, 2007). Responden yang dilibatkan berjumlah 7 orang yang terdiri dari satu orang koordinator bagian, enam orang anggota tim.

Teknik pengambilan sampel yang digunakan adalah purposive sampling, dimana sampel dipilih oleh peneliti dalam penelitian ini adalah orang yang ahli dalam bidang tersebut. Teknik ini digunakan karena responden yang dipilih merupakan orang yang memang bergelut di bidangnya, yaitu bagian penjadwalan kuliah di Bina Sarana Informatika. Data yang diperoleh dalam penelitian ini terbagi menjadi dua macam yaitu data primer yang merupakan data utama penelitian dan data sekunder yang merupakan data pendukung penelitian.

Data primer merupakan data utama yang digunakan dalam penelitian yang diperoleh melalui :

1. Observasi, yaitu pengamatan di lapangan terhadap penerapan dan penggunaan sistem informasi di bagian penjadwalan Akademi Bina Sarana Informatika.
2. Wawancara, yaitu dengan memberikan pertanyaan-pertanyaan kepada narasumber yang juga dijadikan sebagai responden.
3. Survei, yaitu dengan memberikan kuisioner yang dibagikan kepada responden yang dipilih sebagai sampel dalam penelitian.

Pada penyebaran kuesioner penulis membuat daftar pertanyaan berdasarkan standar yang terdapat pada ISO 17799 / BS 7799 tentang petunjuk pelaksanaan manajemen keamanan informasi yang terdiri dari 11 kriteria atau klausa. Data sekunder yang penulis gunakan dalam penelitian ini diperoleh melalui literature atau studi pustaka seperti buku, jurnal, prosiding dan laman. Selain itu penulis juga menggunakan dokumentasi data yang terdapat di bagian penjadwalan yang sesuai dengan topik penelitian.

PEMBAHASAN

Perhitungan Kuesioner.

Data yang diperoleh hasil dari penyebaran kuesioner pada bagian penjadwalan Bina Sarana Informatika sesuai dengan standar ISO 17799 kemudian diolah dengan menggunakan Maturity Level untuk mendapatkan hasil dari perhitungan tingkat kematangan keamanan informasi. Skala yang digunakan dalam kuesioner ini menggunakan skala Guttman, dimana dalam jawaban kuesioner disediakan dua pilihan yaitu pilihan jawaban Ya dan Pilihan jawaban Tidak. Dalam perhitungannya, jawaban Y (Ya) dikonversi menjadi nilai 1, dan jawaban T (Tidak) dikonversi menjadi nilai 0. Penelitian dengan menggunakan skala Guttman dilakukan bila ingin mendapatkan jawaban yang tegas teradap suatu permasalahan yang ditanyakan (Sugiyono, 2007).

Perangkat lunak yang digunakan dalam perhitungan maturity level ini adalah Microsoft Excel. Setelah semua hasil kuesioner dimasukkan dalam tabel, kemudian dihitung maturity level tiap proses dalam masing-masing klausa untuk setiap responden. Hasil maturity level tiap klausa dari 7 responden kemudian dicari rata-ratanya, dan hasil rata-rata tersebut akan menjadi nilai maturity level atau tingkat kematangan keamanan informasi pada bagian penjadwalan Bina Sarana Informatika.

Berdasarkan hasil rekapitulasi dari hasil penyebaran kuesioner kemudian dibuatkan rata-rata atas jawaban kuesioner yang dihitung berdasarkan klausa dan responden untuk mendapatkan maturity level-nya, hasilnya adalah sebagai berikut:

a. Kebijakan Keamanan.

Nilai yang diperoleh berada pada tingkat Initial/Ad Hoc yaitu pada posisi nilai 0.77 yang berarti belum ada proses standar. Berada pada level 1 dari level 3 yang diharapkan.

b. Mengorganisasi Keamanan Informasi.

Nilai yang diperoleh berada pada tingkat Initial/Ad Hoc pada posisi nilai 1.31 yang berarti belum ada proses standar. Berada pada level 1 dari level 3 yang diharapkan.

c. Klasifikasi Aset dan Kontrol.

Nilai yang diperoleh berada pada tingkat Initial/Ad Hoc pada posisi nilai 0.63 yang berarti belum ada proses standar. Berada pada level 1 dari level 3 yang diharapkan.

d. Keamanan Personil / Sumber Daya Manusia.

Nilai yang diperoleh berada pada tingkat Initial/Ad Hoc pada posisi nilai 1.21 yang berarti belum ada proses standar. Berada pada level 1 dari level 3 yang diharapkan.

e. Keamanan Fisik dan Lingkungan.

Nilai yang diperoleh berada pada tingkat Repeatable But Invinitive pada posisi nilai 1.61 yang berarti saat ini keamanan informasi harus dikembangkan kedalam tahapan yang lebih baik. Berada pada level 2 dari level 3 yang diharapkan.

f. Manajemen Operasi dan Komunikasi.

Nilai yang diperoleh berada pada tingkat Optimized pada posisi nilai 4.59 yang berarti saat ini keamanan informasi sudah berada pada tingkat praktek yang baik berdasarkan hasil dari perbaikan yang berkelanjutan. Berada pada level 5 diatas dari level standar yaitu level 3.

g. Kendali Akses.

Nilai yang diperoleh berada pada tingkat Managed and Measureable pada posisi nilai 3.59 yang berarti saat ini manajemen perlu mengawasi dan mengukur kepatuhan terhadap prosedur dan mengambil tindakan tegas jika proses tidak dijalankan secara efektif. Berada pada level 4 diatas dari level standar yaitu level 3.

h. Pengembangan Sistem dan Pemeliharaan.

Nilai yang diperoleh berada pada tingkat Defined Process pada posisi nilai 2.59 yang berarti keamanan informasi sudah berstandar dan harus didokumentasikan dan kemudian dipublikasikan melalui pelatihan.

i. Manajemen Insiden Keamanan Informasi.

Nilai yang diperoleh berada pada tingkat Initial/Ad Hoc pada posisi nilai 1.22 yang berarti saat ini keamanan informasi belum ada proses standar. Berada pada level 1 dari level 3 yang diharapkan.

j. Aspek Keamanan Informasi Keberlangsungan Bisnis.

Nilai yang diperoleh berada pada tingkat Initial/Ad Hoc pada posisi nilai 0.51 yang berarti saat ini keamanan informasi belum ada proses standar. Berada pada level 1 dari level 3 yang diharapkan.

k. Kepatuhan.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada klausa kesebelas tentang kepatuhan berada pada tingkat Repeatable but Intituitive pada posisi nilai 2.07 yang berarti saat ini keamanan informasi harus dikembangkan kedalam tahapan yang lebih baik. Berada pada level 2 dari level 3 yang diharapkan.

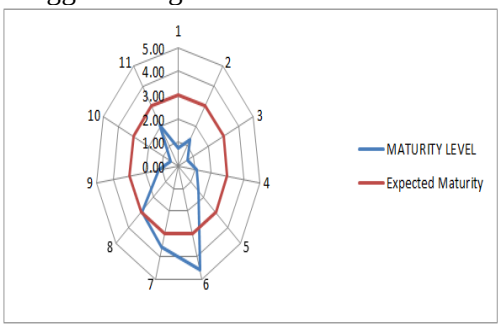
Perhitungan *Maturity Level.*

Nilai Maturity diperoleh dari hasil rata-rata jawaban responden terhadap masing-masing klausa yang terdapat pada standar ISO 17799 / BS 7799, sedangkan Expected Maturity menunjukkan tingkat standar maturity yang ada di Indonesia yaitu pada tingkat ketiga.

Tabel 1
Kriteria Index Nilai Maturity Level.

Range	Keterangan
0 – 0.50	*Non-Existent*
0.51 – 1.50	*Initial/Ad Hoc*
1.51 – 2.50	*Repeatable But Invinitive*
2.51 – 3.50	*Defined Process*
3.51 – 4.50	*Managed and Measurable*
4.51 – 5.00	*Optimized*

Gambar berikut ini menunjukkan hasil maturity yang digambarkan dengan menggunakan grafik radar.



Gambar 2
Current Maturity Level vs Expected Maturity.

Analisis hasil Maturity Level.

Berdasarkan hasil perhitungan tingkat keamanan informasi dengan menggunakan Maturity Level maka didapatkan penilaian terhadap tingkat keamanan informasi pada bagian penjadwalan Bina Sarana Informatika di setiap prosesnya. Berikut ini adalah hasil penilaian yang diperoleh pada

penelitian ini berdasarkan standar ISO 17799.

a. Kebijakan Keamanan.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 1 tentang kebijakan keamanan informasi berada pada tingkat Initial/Ad Hoc pada posisi nilai 0.77 yang berarti saat ini keamanan informasi dibagian penjadwalan BSI belum ada proses standar. Oleh karena itu diperlukan sebuah kebijakan yang dapat mengarahkan visi dan misi perusahaan agar kelangsungan usaha dapat dipertahankan dengan mengamankan dan menjaga integritas / keutuhan data dan informasi yang krusial. Selain itu kebijakan tersebut dibutuhkan mengingat banyak ditemuinya masalah-masalah non teknis salah satunya penggunaan password oleh lebih dari satu orang. Hal ini menunjukan tidak adanya kepatuhan dalam menerapkan sistem keamanan informasi serta harus dilakukan inventarisasi data-data perusahaan. Selanjutnya dibuat peraturan yang melibatkan semua biro sehingga peraturan yang dibuat dapat diterima oleh semua pihak, kemudian dirancang dan ajukan ke pihak direktur, setelah disetujui peraturan tersebut harus diterapkan.

b. Mengorganisasi Keamanan Informasi.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 2 tentang mengorganisasi keamanan informasi berada pada tingkat Initial/Ad Hoc pada posisi nilai 1.31 yang berarti saat ini keamanan informasi di bagian penjadwalan Bina Sarana Informatika belum ada proses standar. Tugas dan tanggung jawab keamanan informasi harus dilaksanakan oleh semua staf yang berada di bagian penjadwalan Bina Sarana Informatika. Pihak ketiga tidak diperkenankan untuk mengakses informasi yang bukan merupakan wewenangnya, pihak ketiga hanya boleh mengakses data yang bersifat umum. Oleh karena itu perusahaan perlu menetapkan dan menugaskan tanggung jawab keamanan informasi secara jelas, kemudian perlu adanya forum keamanan informasi dengan tujuan agar para staf dapat mengetahui dengan pasti kemana harus berkoordinasi jika terjadi pelanggaran terhadap keamanan sistem informasi.

c. Klasifikasi Aset dan Kontrol.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 3 tentang klasifikasi aset dan kontrol berada pada tingkat Initial/Ad Hoc pada posisi nilai 0.63 yang berarti saat ini keamanan informasi di bagian penjadwalan Bina Sarana Informatika belum ada proses standar. Aset perusahaan yang ada pada bagian penjadwalan Bina Sarana Informatika dicatat oleh masing-masing staf, namun proses pencatatannya dilakukan tanpa adanya panduan atau pedoman yang dikeluarkan oleh perusahaan, akibatnya tidak ada standar yang digunakan dalam pengelolaan aset perusahaan. Oleh karena itu perlu dibuatkan sebuah pedoman atau panduan dalam pengelolaan aset agar proses pengelolaan antara masing-masing staf memiliki standarisasi yang sama.

d. Keamanan Personil / Sumber Daya Manusia.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 4 tentang keamanan sumber daya manusia berada pada tingkat Initial/Ad Hoc pada posisi nilai 1.21 yang berarti saat ini keamanan informasi dibagian penjadwalan Bina Sarana Informatika belum ada proses standar. Saat ini pengelolaan hak akses sepenuhnya dilakukan oleh Biro Teknologi Informasi namun masih terdapat kekurangan misalnya untuk staf yang bukan bagian penjadwalan masih dapat mengakses data penjadwalan. Data pengguna masih tersimpan dalam basis data meskipun pengguna tersebut sudah tidak bekerja lagi pada bagian penjadwalan BSI. Selain itu tidak adanya prosedur mengenai pengelolaan hak akses pengguna sehingga siapa saja yang bisa masuk kedalam DBMS akan dengan mudah mengelola hak akses pengguna. Oleh karena itu dibutuhkan sebuah tim / perorangan yang bertugas dan bertanggung jawab mengatur atau mengelola hak akses user, kemudian pengelolaan tersebut harus berdasarkan pada prosedur dan kebijakan yang dikeluarkan perusahaan. Selain itu diperlukannya sumber daya manusia yang penuh tanggung jawab dan professional.

e. Keamanan Fisik dan Lingkungan.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 5 tentang keamanan fisik dan lingkungan berada pada tingkat Repeatable But Invinitive pada posisi nilai 1.61 yang berarti saat ini keamanan informasi di bagian penjadwalan Bina Sarana Informatika harus dikembangkan kedalam tahapan yang lebih baik. Akses terhadap lokasi fisik yang menyimpan pusat informasi harus dibatasi agar terhindar dari kemungkinan terjadinya bencana dan perusakkan yang dilakukan oleh pihak yang tidak bertanggung jawab. Pada saat ini lokasi penyimpanan server penjadwalan BSI sudah ditempatkan ditempat yang jauh dari keramaian dan akses orang banyak, ruangan server dikelola oleh Biro Teknologi informasi yang dilengkapi AC, kamera CCTV, kunci, dan pengamanan dari kebakaran. Terdapat pula larangan akses fisik terhadap server yang berupa larangan masuk selain orang yang berwenang. Namun saat ini tidak ada pencatatan tentang akses masuk ke ruang server sehingga tidak terekam siapa saja yang memasuki ruang server, selain itu manajemen pengkabelan masih belum terkelola dengan baik karena kabel yang ada pada ruang server terlihat berantakan, tidak tersusun rapih.

f. Manajemen Operasi dan Komunikasi.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 6 tentang manajemen operasi dan komunikasi berada pada tingkat Optimized pada posisi nilai 4.59 yang berarti saat ini keamanan informasi dibagian penjadwalan Bina Sarana Informatika sudah berada pada tingkat praktek yang baik berdasarkan hasil dari perbaikan yang berkelanjutan. Saat ini bagian penjadwalan Bina Sarana Informatika telah memiliki SOP sebagai landasan dalam pengoperasian sistem informasi, Back-Up dan pemeliharaan peralatan. Perencanaan sistem informasi baru, upgrade atau versi baru dilakukan berdasarkan permintaan dan kebutuhan. Terdapat kontrol pencegahan, deteksi dan respon terhadap software yang berbahaya dengan terpasangnya anti virus dai masing-masing unit komputer staf. Data yang terdapat pada server hanya bisa dilihat dengan menggunakan sistem informasi dan informasi yang tersimpan tidak bisa disalin. Sistem informasi penjadwalan sudah memiliki sistem keamanan berupa login untuk dapat mengolah data penjadwalan sehingga hanya orang-orang tertentu saja yang bisa melakukan pengolahan data penjadwalan dan transaksi yang dilakukan oleh pengguna akan direkam oleh sistem.

g. Kendali Akses.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 7 tentang kendali akses berada pada tingkat Managed and Measureable pada posisi nilai 3.59 yang berarti saat ini manajemen perlu mengawasi dan mengukur kepatuhan terhadap prosedur dan mengambil tindakan tegas jika proses tidak dijalankan secara efektif. Tidak ada kebijakan tentang pembuatan password untuk masuk kedalam sistem informasi dan tidak ada petunjuk dalam pembuatan password yang baik. Sistem informasi penjadwalan sudah menerapkan kegiatan autentikasi pengguna, yang berarti hanya pengguna yang sah saja yang bisa mengakses informasi dalam sistem informasi. Tidak ada registrasi formal untuk menjadi pengguna sistem informasi penjadwalan, semua diregistrasi oleh pimpinan berdasarkan ruang lingkup pekerjaannya. Tidak ada kebijakan dalam perubahan password secara berkala dan pengontrolan terhadap password dilakukan oleh masing-masing staf, jika staf lupa passwordnya, maka staf tersebut harus menghubungi pimpinannya untuk dilakukan reset password. Kerahasiaan password sistem informasi kurang baik karena data yang tersimpan ke dalam basis data bukanlah hasil enkripsi.

h. Pengembangan Sistem dan Pemeliharaan.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 8 tentang pengembangan sistem dan pemeliharaan berada pada tingkat Defined Process pada posisi nilai 2.59 yang berarti keamanan informasi sudah berstandar dan harus didokumentasikan dan kemudian dipublikasikan melalui pelatihan. Sistem informasi penjadwalan meliputi

pengolahan data dosen, ruangan, jadwal, mata kuliah, dan sebagainya. Saat ini data dosen yang tersimpan hanya bisa diidentifikasi oleh sistem berdasarkan kode dosen, NIP dan nama dosen, sistem informasi akan menolak jika ada penyimpanan dengan kode atau NIP yang sama, hal ini dilakukan agar tidak terjadinya duplikasi data yang tersimpan dalam basis data. Sistem informasi penjadwalan Bina Sarana Informatika merupakan sistem yang interaktif karena setiap validasi, sistem akan mengeluarkan pesan yang terkait dengan kegiatan yang dilakukan oleh pengguna. Semua sistem penjadwalan dirancang dan dibangun oleh Biro Teknologi informasi tanpa ada campur tangan dari pihak luar maupun out sourcing. Saat ini Bina Sarana Informatika sudah bekerja sama dengan salah satu provider software terbesar di dunia yaitu Microsoft.

i. Manajemen Insiden Keamanan Informasi.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 9 tentang manajamen insiden keamanan informasi berada pada tingkat Initial/Ad Hoc pada posisi nilai 1.22 yang berarti saat ini keamanan informasi dibagian penjadwalan Bina Sarana Informatika belum ada proses standar. Jika terjadi insiden terhadap keamanan informasi selalu dilaporkan kepada pihak Biro Teknologi Informasi (BTI) namun terkadang proses penanganannya yang masih kurang, hal ini dikarenakan staf yang bertanggung jawab menangani insiden tersebut hanya sedikit jumlahnya. Selain itu juga tidak ada prosedur atau kebijakan tentang pelaporan insiden yang terjadi, sehingga pada saat melaporkan insiden, pengguna melakukan sesuai dengan inisiatifnya sendiri. Tidak bekerjanya sistem yang dapat melakukan pemantauan terhadap ancaman keamanan informasi mengakibatkan seringnya pengrusakan data yang dilakukan oleh pihak yang tidak bertanggung jawab.

j. Aspek Keamanan Informasi Keberlangsungan Bisnis.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 10 tentang aspek keamanan informasi dan keberlangsungan bisnis berada pada tingkat Initial/Ad Hoc pada posisi nilai 0.51 yang berarti saat ini keamanan informasi dibagian penjadwalan Bina Sarana Informatika belum ada proses standar. Hal ini disebabkan tidak adanya kerangka kerja yang bisa digunakan untuk merencanakan keberlangsungan bisnis, perencanaan kelangsungan bisnis dilakukan dengan perencanaan yang tidak terstruktur dan tidak adanya kegiatan percobaan atas perencanaan yang telah disusun. Selain itu tidak adanya prosedur pengelolaan dalam pengembangan dan mempertahankan kelangsungan bisnis mengakibatkan terhambatnya proses perencanaan. Namun bagian penjadwalan sudah mempersiapkan kegiatan yang akan dilakukan pada masa yang akan datang.

k. Kepatuhan.

Berdasarkan hasil perhitungan Maturity Level nilai yang diperoleh pada proses 11 tentang kepatuhan berada pada tingkat Repeatable but Intituitive pada posisi nilai 2.07 yang berarti saat ini keamanan informasi di bagian penjadwalan Bina Sarana Informatika harus dikembangkan kedalam tahapan yang lebih baik. Sampai saat ini belum dilakukan proses audit terhadap keamanan informasi di bagian penjadwalan Bina Sarana Informatika, namun kebijakan-kebijakan yang dikeluarkan oleh manajemen disebar secara merata ke semua bagian yang ada pada Bina Sarana Informatika. Catatan penting ataupun informasi penting dilindungi oleh sistem agar terhindar dari kerusakan dan kehilangan.

PENUTUP

Berdasarkan hasil penelitian yang telah dilakukan, diperoleh kesimpulan sebagai berikut :

1. Tingkat kematangan keamanan sistem informasi yang ada di bagian penjadwalan perkuliahan Bina Sarana Informatika rata-rata masih berada di tingkat kesatu (Initial/ad hoc) yaitu pada klausa kebijakan keamanan, organisasi keamanan informasi, klasifikasi aset dan kontrol, keamanan personil, manajemen insiden keamanan informasi dan manajemen kontinuitas bisnis. Untuk klausa

keamanan fisik dan lingkungan, klausa kepatuhan berada pada tingkat kedua (Repeatable but invinite), Klausa pengembangan sistem dan pemeliharaan berada di tingkat ketiga (Defined process). Untuk klausa kontrol akses berada di tingkat keempat (Managed and measurable). Sedangkan klausa manajemen komunikasi dan operasi berada pada tingkat kelima (Optimized).

2. Pelaksanaan sistem informasi penjadwalan perkuliahan Bina Sarana Informatika dalam penerapan keamanan sistem informasi berdasarkan ISO 17799 masih belum siap karena dari 11 klausa yang ditetapkan, hanya tiga klausa saja yang baru memenuhi standar tingkat kematangan yaitu klausa pengembangan sistem dan pemeliharaan, klausa kontrol akses dan klausa manajemen komunikasi dan operasi.
3. Peranan ISO 17799 dalam menjaga informasi yang tersimpan adalah sebagai acuan dalam melakukan kontrol keamanan sistem informasi berdasarkan resiko, peraturan, hukum dan undang-undang serta prinsip, tujuan dan kebutuhan informasi pada sistem informasi penjadwalan Bina Sarana Informatika.

Berdasarkan hasil penelitian dan pengolahan data yang berkaitan dengan keamanan sistem informasi pada sistem informasi penjadwalan Bina Sarana Informatika, penulis dapat memberikan saran-saran sebagai berikut :

1. Perlu perbaikan dalam proses pengolahan informasi menjadi lebih baik terutama dalam sistem Informasi agar pengguna mendapatkan informasi yang dibutuhkan dengan lebih cepat dan akurat.
2. Diperlukan peningkatan Infrastruktur TIK mulai dari hardware, software, brainware
3. Diperlukan perbaikan kerangka kerja keamanan sistem informasi untuk menjaga aset informasi pada sistem informasi penjadwalan dari gangguan atau ancaman baik internal maupun eksternal.
4. Diperlukan pendokumentasian pemindahan perangkat lunak dari lingkungan testing ke lingkungan operasional.
5. Diperlukan pembuatan sistem keamanan yang lebih baik untuk menjaga informasi perusahaan dari berbagai macam ancaman.
6. Dilakukan penelitian lanjutan terhadap keamanan informasi pada sistem informasi penjadwalan Bina Sarana Informatika dengan cakupan yang lebih luas dengan menggunakan Standar keamanan sistem informasi yang terbaru misalnya ISO 27001:2005
7. Diperlukan penelitian lanjutan dengan di fasilitasi oleh instansi yang bersangkutan agar proses dan hasil penelitian lebih optimal.

REFERENSI

Bundesamt Fur Sicherheit in der Informationstechnik (BSI). (2008). BSI-Standard 100-1 Information Security Management Systems (ISMS). Bonn.

Hopkinson, Jhon P.(1999). The Relationship Between The SSE-CMM And IT Security Guidance Documentation. Canada. EWA-Canada Ltd.

Ngqondi, T.G. (2009). The ISO/IEC 27002 And ISO/IEC 27799 Information Security Management Standard: A Comparative Analysis From A Healthcare Perspective. Port Elizabeth: Nelson Mandela Metropolitan University.

Simanungkalit, S.Juliandry. (2009). Perancangan Manajemen Keamanan Sistem Informasi Studi Kasus Depkominfo. Tesis. Jakarta. Fakultas Ilmu Komputer Program Studi Magister Teknologi Informasi UI.

Sugiyono. (2007). Metode Penelitian Kuantitatif, Kualitatif dan R & D. Bandung. CV.Alfabeta.