Audit Keamanan Sistem Informasi Akademik Sekolah Tinggi Farmasi Bandung Berbasis Risiko dengan Menggunakan Standar ISO 27001

Security Audit of Academic Information System Bandung College of Pharmacy Based on Risk Using Standard ISO 27001

Muhammad Ikhsan[1], Eko Darwiyanto[2], Dawam Dwi Jatmiko Suwawi[3]

Prodi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom

Dewprism1@gmail.com[1] ekodarwiyanto@telkomuniversity.ac.id[2] dawamdjs@telkomuniversity.ac.id[3]

Pada tugas akhir ini akan dilakukan audit berbasis risiko dengan menggunakan standar ISO 27001di Sekolah Tinggi Farmasi Bandung (STFB). ISO 27001 adalah standar yang biasa digunakan untuk mengaudit keamanan sistem informasi sebuah perusahaan dan digunakan untuk menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil dari audit keamanan sistem informasi perusahaan tersebut. Selain itu hasil audit juga akanmenggambarkan tingkat kematangan (*Maturity Level*) , tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di Sekolah Tinggi Farmasi Bandung (STFB) dengan menggunakan *Capability Maturity Model for Integration* (CMMI).Berdasarkan hasil analisis risikodalam penelitian ini, ditentukan 16 kontrol objektif dan 57 kontrol keamanan yang tersebar dalam 4 klausal ISO 27001.Dari hasil audit dapat disimpulkan bahwa nilai tingkat kematangan tata kelola keamanan sistem informasi STFB adalah 2,5 yang berarti tingkat keamanan masih berada pada level 2 *planned and tracked* (sudah direncanakan dan dilacak secara aktif) namun telah mendekati level 3 *well defined* (telah didefinisikan dengan baik)

Kata kunci :SMKI, Teknologi informasi, ISO 27001, Risiko, CMMI, *Maturity Level*

In this minithesis, the risk-based audit using ISO 27001 standard was done in Sekolah Tinggi FarmasiBandung(STFB). ISO 27001 is a standard usually used for auditing information system safety in a company and is used to produce document (finding and recommendation), that was a result from safety audit in company information system. The audit result also describe the level of maturity, level of completeness of ISO/IEC 27001:2009 implementation, and area map of safety management information system in STFB, using Capability Maturity Model for Integration (CMMI). Based on risk analysis in this study, 16 objective controls and 57 safety controls that were spreaded in 4 clausul ISO 27001, were definited. The audit result concluded that the maturity level of information systems security managementin STFB is 2.5. It means that the security level is still at level 2 planned and tracked but nearly approachlevel 3 well defined.

Keywords : ISMS, information technology, ISO 27001, risk, CMMI, level of maturity

1. Pendahuluan

1.1. Latar Belakang

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di perusahaan mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola perusahaan yang baik. Dalam penyelenggaran tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). [5].Sepertinya halnya sebuah perusahaan yang menerapkan tata kelola Teknologi Informasi dan Komunikasi (TIK), perguruan tinggi di Bandung pun memerlukan Teknologi Informasi dalam rangka pengelolaan fasilitas penunjang kegiatan akademik mahasiswa. Salah satu fasilitas penunjang kegiatan akademik mahasiswa adalah layanan sistem informasi akademik (SIA). Salah satu perguruan tinggi yang menerapkan Sistem Informasi Akademik (SIA) adalah Sekolah Tinggi Farmasi Bandung (STFB).STFB dipilih sebagai tempat penelitian tugas akhir karena Layanan Sistem Informasi Akademik (SIA) adalah sistem yang baru dibuat 2 tahun terakhirdan belum pernah dilakukannya Audit keamanan terhadap sistem informasi tersebut dan setelah melakukan wawancara awal ke pihak STFB ternyata sistem informasi mereka sudah berhasil ditembus oleh mahasiswa yang ingin merekayasa nilai mata kuliah. Hal ini membuat pihak STFB ingin mendapatkan

masukan dari berbagai pihak soal bagaimana cara untuk menjaga keamanan sistem informasi mereka. Pada tugas akhir ini akan dilakukan audit Keamanan Sistem Informasi berbasisrisiko dengan menggunakan Standar ISO 27001. Standar ISO 27001 adalah standar yang biasa digunakan untuk mengaudit keamanan sistem informasi dan digunakan untuk menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil dari audit keamanan sistem informasi STFB .Selain itu juga hasil audit akan menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di STFB dengan menggunakan *Capability Maturity Model for Integration* (CMMI)

1.2 Rumusan Masalah

1. Bagaimana melakukan audit keamanan sistem informasi di STFB Bandung dengan menggunakan standar SNI ISO 27001:2009 terhadap faktor keamanan informasi CIA (*Confidentiality, Integrity* dan *Availability*)?
2. Bagaimana saran dan perbaikan yang mendukung pengelolaan sistem keamanan informasi di STFB?

1.3 Tujuan

1. Melakukan Audit terhadap keamanan sistem informasi STFB Bandung dengan menggunakan SNI ISO 27001:2009 berbasis risiko sebagai bahan referensi penentuan kebijakan pengelolaan keamanan informasi Sistem Informasi Akademik (SIA) STFB ke depannya
2. Menyusun hasil audit keamanan sistem informasi Akademik STFB dengan melakukan evaluasi terhadap kendala dan bukti yang ada, mendokumentasikan temuan audit dalam rangka pembuatan laporan audit.
3. Menggambarkan tingkat kematangan, tingkat kelengkapan penerapan ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di STFB dengan menggunakan Capability Maturity Model for Integration (CMMI)

1.4 Metodologi Penyelesaian Masalah

Metodologi yang digunakan untuk penyelesaian study kasus di atas adalah sebagai berikut :

1. Pencarian literatur berupa jurnal, paper dan makalah, baik secara online maupun offline.Literature yang di cari adalah yang berhubungan dengan SMKI, Teknologi informasi, ISO 27001, audit berbasis risiko
2. Penelitian dengan melakukan pemgumpulan data yang dibutuhkan berasal dari STFB Bandung melalui hasil wawancara, observasi dan questioner yang diberikan pada pegawai
3. Melakukan analisis dari data yang telah didapat untuk kemudian dilakukan pengukuran tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di STFB Bandung dengan menggunakan *Capability Maturity Model for Integration* (CMMI)
4. Mengambil kesimpulan dari hasil analisis dan menuliskan hasil penelitian ke dalam laporan tugas akhir.

2. Dasar Teori

2.1 Informasi

Informasi yang merupakan asset penting bagi perusahaan dapat dikelola dengan menggunakan teknologi informasi. Teknologi Informasi adalah suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan perusahaan. .Namun, semakin berkembangnya teknologi informasi akan semakin banyak ancaman-ancaman yang akan terjadi dari dalam maupun luar perusahaan.[2]

2.2 Keamanan Sistem Informasi

Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki..Keamanan Teknologi Informasi atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi darigangguan-gangguan berupa akses terlarang serta utilisasi jaringanyang tidak diizinkan.. Keamananan teknologi informasi merupakan bagian dari keseluruhan aspek keamananinformasi. Karena teknologi informasi merupakan salah satu alat atautool penting yang digunakan untuk mengamankan akses serta penggunaan dari data dan informasi perusahaan. Dari pemahaman ini pula, kita akan mengetahui bahwa teknologi informasi bukanlah satu-satunya aspek yang memungkinkan terwujudnya konsep keamananinformasi di perusahaan. Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut yaitu Confidentiality (kerahasiaan) , Integrity (integritas) dan Availability (ketersediaan) [3]

2.2 SNI ISO 27001:2009

SNI ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan [4].Standar menyatakan persyaratan utama yang harus dipenuhi menyangkut Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi), Tanggung jawab manajemen, Audit internal SMKI, Manajemen tinjau ulang SMKI dan Peningkatan berkelanjutan

2.3 Audit Berbasis Risiko

Auditor perlu memahami aspek-aspek yang perlu dalam melakukan pendekatan Audit Berbasis Risiko. Dalam menerapkan ABR, auditor perlu mengidentifikasi wilayah/area yang Memilikirisiko yang menghambat pencapaian tujuan manajemen. Wilayah/area yang memiliki tingkat risiko yang tinggi tersebut akan memerlukan pengujian yang lebih mendalam. Auditor dapat mengalokasikan sumber daya auditnya berdasarkan hasil identifikasi atas kemungkinan dan dampak terjadinya risiko.Wilayah berisiko rendah menjadi prioritas akhir alokasi sumber daya audit. Olehkarena itu, dalam ABR, auditor harus melakukan analisis dan penaksiran risiko yang dihadapi auditi. Audit dengan pendekatan berbasis risiko banyak dipakai oleh para praktisi audit di dunia. Mereka berpendapat bahwa makin besar suatu perusahaan berkembang maka lebih besar juga risiko yang akan datang. Risiko selalu ada pada tiap prosesyang dijalankan karena itu penting sekali pendekatan yang berbasiskan risiko dilakukan, jadi sudah biasa jika misalnya penilaian dan mitigasi risiko dilakukan sebagaibagian integral dari audit. [3]

2.4 Capability Maturity Model for Integration (CMMI)

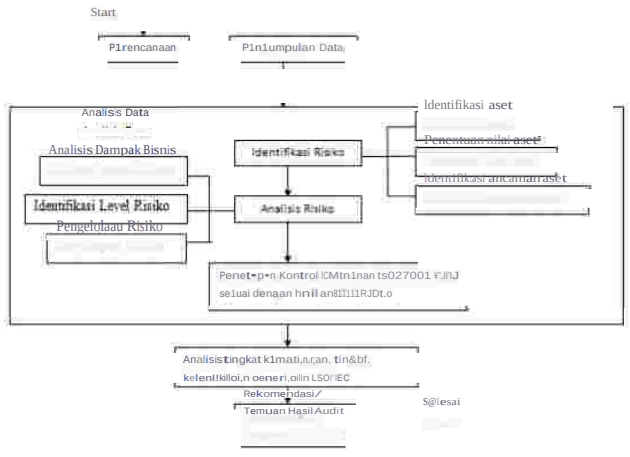
Capability Maturity Model for Integration **(**CMMI) adalah sebuah metode yang dikembangkan oleh *Carneige Mellon University* yang digunakan sebagai alat untuk melaporkan pemetaantata kelola keamanan sistem informasi danmengukur tingkat kematangan penerapan tata kelola keamanan informasi di lingkungan perusahaan tersebut. Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai berikut[4]:

1. Tingkat 0- Tidak Diketahui (PASIF)
2. Tingkat I- Kondisi Awal (REAKTIF)
3. Tingkat II- Penerapan Kerangka Kerja Dasar (AKTIF)
4. Tingkat III- Terdefinisi dan Konsisten (PRO AKTIF)
5. Tingkat IV- Terkelola dan Terukur (TERKENDALI)

3. METODOLOGI DAN IMPELEMENTASI PENELITIAN

3.1 Metodologi Penelitian

Audit Teknologi Informasi dilakukan dengan melalui berbagai tahap utama yang diantaranya adalah mengidentifikasi risiko-risiko yang mungkin terjadi kemudian dilanjutkan dengan analisis risiko yang hasilnya dapat digunakan untuk menetapkan kontrol keamanan ISO 27001 yang akan digunakan dalam audit. Setelah menetapkan kontrol keamanan ISO 27001 barulah Analisis tingkat kematangan dan tingkat kelengkapan penerapan ISO/IEC 27001:2009 di Sekolah Tinggi Farmasi Bandung dengan menggunakan CMMI dilakukan. Gambaran umum sistem audit adalah seperti berikut



Gambar 1 Jalannya Metodologi Penelitian

3.2 Impelementasi Penelitian

3.2.1 Perencanaan. Tahapan ini meliputi penyusunan daftar responden yang akan diwawancara dan membuat daftar pertanyaan awal untuk responden. Pertanyaan awal diajukan untuk mengetahui tentang bagaimana kondisi keamanan sistem informasidi Sekolah Tinggi Farmasi Bandung (STFB) secara kasar dan siapa saja personil yang berperan di dalam sistem tesebut

3.2.2 Pengumpulan Data. Tahapan pengumpulan data adalah tahapan untuk mengetahui proses bisnis yang terjadi di STFB dengan tujuan untuk memahami detail prosedur pengelolaan Sistem Informasi Akademik (SIA). Metode pengumpulan data sendiri dilakukan dengan menggunakan metode wawancara terhadap pihak-pihak di STFB seperti misalnya database administrator, operator dan Ketua STFB dan juga melalui observasi langsung di lapangan

3.2.3 Analisis Data. Tahapan ini meliputi tahapan identifikasi Risiko yang terdiri dari identifikasi nilai aset, penentuan nilai aset dan identifikasi ancaman aset dan tahapan analisis risiko yang terdiri dari analisis dampak bisnis, identifikasi level risiko dan pengelolaan risiko

3.2.4 Penetapan Kontrol Keamanan ISO 27001. Tahapan ini bertujuan untuk melakukan penentuan klausal kontrol keamanan yang akan digunakan dalam audit dari 11 klausal yang tersedia dalam SNI ISO 27001:2009. Penentuan klausal keamanan yang dipakai disesuaikan dengan dengan hasil analisis resiko yang terdiri dari hasil analisis nilai ancaman,kelemahan, nilai risiko dan dampak bisnis yang terdapat pada aset sistem informasi yang dimiliki STFB

3.2.5 Analisis Tingkat Kematangan dengan CMMI. Tahapan ini bertujuan untuk melakukan analisis dari data yang telah didapat untuk kemudian melakukan pengukuran tingkat kematangan sistem informasi di STFB dengan menggunakan *Capability Maturity Model for Integration* (CMMI). Hasil analisis akan menjelaskan detail penilaian tingkatan kematangan pada klausal keamanan yang telah dipilih sebelumnya.

3.2.6 Checklist Persyaratan Umum ISO 27001 terhadap Sistem Informasi Akademik STFB

Penerapan ISO 27001 dapat diimplementasikanpada Sistem Informasi Akademik STFB karena sudah memenuhi sebagian besar dari persyaratan umum penerapan ISO 27001 yaitu: Sistem manajemen keamanan informasi), Tanggung jawab manajemen, dan Manajemen tinjau ulang SMKI

4. Analisis Penelitian

4.1 Identifikasi Aset

Tahapan identifikasi aset pada dasarnya adalah mengkaji kondisi keamanan sistem informasi STFB dengan cara mengidentifikasi aset yang ada. Sebuah aset keamanan sistem informasi memiliki 3 nilai yang berbeda yaitu nilai Confidentiality, Integrity dan Availability. Berdasarkan Form questioner Penilaian Aset yang terdapat di lampiran A, berikut merupakan hasil questioner identifikasi aset

Tabel 1 hasil questioner identifikasi aset pada aset database kampus, murid dan dosen

No	N'''''''' ''''''	Nllal Confidentiality (LIM/HI	NIIII Inle9dty (Liii/Hi	Nllal Avallabilty (UIIIHI	Nil-6Aset
1	D•Ub•u K•mpus	3	3	2	8
2	D•t•b•— Mu•id	2	3	2	7
3	O8tabHe OO:HII	2	3	2	7

4.2 Identifikasi Ancaman dan kelemahan Aset

Berdasarkan hasil questioner identifikasi asset ,Sekolah Tinggi Farmasi Bandung memiliki 15 aset yang memiliki nilai-nilai tersendiri. Setelah mengetahui nilai aset maka langkah selanjutnya adalah mengindentifikasi Ancaman dan kelemahan Aset tersebut untuk kemudian menentukan nilai probabilitas kemunculan ancaman dan kelemahan yang dimiliki oleh aset tersebut dengan menggunakan rentang nilai sebagai berikut [1] :

a) Low : Nilai rerata probabilitas 0,0 – 0,3
b) Medium : Nilai rerata probabilitas 0,4 – 0,6
c) High : Nilai rerata probabilitas 0,7 – 1,0

Tabel 2 Nilai probabilitas ancaman dan nilai ancaman dari aset database kampus

Astl	Ke,adian	Jenis	Probablllt as	Ktladtan	Nllai Probablht as	Total Probabilhy '''	Nllai Anca,man
Database Kampus	Oata kampus diubah oleh pihak yang tidak btrwenang	Ancaman	low	0	0.0	0.2	0,06
	Kesalahan entry pada data kampus	Kelemahan	low	4	0.2		
	Tidak adanya proses dan kebl,akan back up dan atau recovery ''''	Kelemahan	low	0	0.0		

4.3 Analisis Dampak Bisnis

Setelah mengidentifikasi nilai , ancaman dan kelemahan aset maka langkah selanjutnya adalah menganalisis dampak bisnis. Analisis dampak bisnis digunakan untuk mengetahui sejauh mana dampak yang ditimbulkan aset yang terganggu oleh berbagai ancaman dan kelemahan terhadap kelangsungan proses bisnis yang berlangsung di STFB. Nilai dampak bisnis atau biasa disebut dengan Bussiness Impact Analysis (BIA) ini dapat digunakan untuk mengetahui batas toleransi dari 15 aset yang dimiliki oleh STFB terhadap kemungkinan munculnya gangguan yang diakibatkan oleh ancaman dan kelemahan aset tersebut. Dampak bisnis terhadap aset-aset yang dimiliki Sekolah Tinggi Farmasi Bandung dapat dilihat pada tabel berikut:

Tabel 3 Nilai BIA terhadap aset

Aset	Dampak	Nilai BIA
Database Kampus	Gangguan pada sistem	3
Database Murid	Gangguan pada sistem	3
Database Dosen	Gangguan pada sistem	3
Database User dan Password	User tidak bisa melakukan login pada aplikasi	4
Operator	Layanan terganggu karena tidak adanya operator	3
Sistem Administrator	Tidak ada yang memantau dan mengelola keamanan server	4
Database Laporan	Gangguan pada sistem	3
Server	Layanan terganggu karena tidak bisa diaksesnya server	4
Unit Komputer (Laptop/PC)	Terhambatnya kinerja operator	3
Sistem Operasi (OS)	Operator tidak bisa mengakses PC	2
Aplibsi sisfo siakad	Layanan SISFO terganggu sehingga tidak dapat melayani para user	3
Switch	Pendistribusian jaringan dalam ruangan menjadi terganggu	3
Modem	Terputusnya sinyal network yang mengakibatkan hilangnya akses internet	4
Jaringan	Komunikasi data/informasi antar receiver dan sender terganggu sehingga layanan terganggu	4
Router	Terputusnya komunikasi antar jaringan sehingga layanan terganggu	4

4.4 Respon Risiko

Setelah pembuatan matriks level risiko selanjutnya adalah menganalisis respon terhadap risiko yang ada tersebut. Respon risiko yang diaccept adalah risiko yang apabila terjadi pihak STFB dapat menerima dampak yang terjadi apabila risiko tersebut terjadi karena dampaknya kecil dan sangat jarang terjadi.. Untuk menentukan sebuah risiko diterima atau perlu dilakukan pengelolaan terhadap risiko tersebut, maka perlu diketahui nilai dari risiko. Nilai risiko dihitung dengan menggunakan rumus :

Risk Value = NA x BIA x NT [1]

Berikut adalah nilai risiko dari masing-masing aset berdasarkan perhitungan nilai aset, nilai ancaman, BIA dan nilai risiko :

Tabel 4 Nilai Risiko

Nomor	Aset	Nilai Aset	Nilai Ancaman	BIA	Nilai Risiko
1	Database Kampus	1	0,06	3	1,44
2	Database Murid	1	0,11	3	2,31
3	Database Dosen	1	0,03	3	0,63
4	Database Userdan Password	1	0,1	4	3,6
5	Operator	1	0,05	3	1,05
6	SistemAdministrator	1	0,00	4	0,00
7	Database Laporan	1	0,03	3	0,63
8	Server	1	0,1	4	3,6
9	Unit Komputer (Laptop/PC)	1	0,03	2	0,42
10	SistemOperasi(OS)	1	0,15	3	3,78
11	Aplikasi sisfo siakad	1	0,11	3	2,31
12	Switch	1	0,08	3	1,68
13	Modem	1	0,03	4	1,08
14	Jaringan	1	0,03	4	1,08
15	Router	1	0,00	4	0,00

Setelah didapatkan nilai risiko maka selanjutnya adalah menetapkan level risiko yang didapat dengan menyesuaikan nilai risiko ke dalam matriks level risiko sehingga diperoleh hasil level risiko untuk masing-masing aset.

Tabel 5 Level Risiko

Nomor	Aset	Nilai Risiko	Level Risiko
1	Database Kampus	1,44	Medium
2	Database Murid	2,31	Medium
3	Database Dosen	0,63	Medium
4	Database Userdan Password	3,6	High
5	Operator	1,05	Medium
6	SistemAdministrator	0,00	Low
7	Database Laporan	0,63	Medium
8	Server	3,6	High
9	Unit Komputer (Laptop/PC)	0,42	Low
10	SistemOperasi(OS)	3,78	High

11	Aplikasi sisfo		
stak.ad	2,97		
Medium			
12	Switch		
0,00		Low	
13	Modem		
1,08			
Medium			
14	Jsl'Ylgan		
1,08			
Medium			
15	Router		
0,00		Low	

Berdasarkan hasil perhitungan level risiko aset tersebut maka aset yang akan dilakukan pengelolaan risikonya adalah aset yang memiliki level risiko high yaitu database User dan Password, Server dan Sistem Operasi.

4.5 Penetapan Kontrol Keamanan ISO 27001

Berdasarkan dengan hasil analisis yang menyatakan bahwa aset Database User dan Password, Server dan Sistem Operasi memilki level risiko high maka diputuskan bahwa ruang lingkup audit keamanan sistem informasi yang menggunakan standar SNI ISO 27001:2009 akan menggunakan 4 buah klausal kontrol keamanan yaitu :

a. SNI-ISO 27001-A. 9 : Keamanan Fisik dan Lingkungan
b. SNI- ISO 27001-A.11 : Pengendalian Akses
c. SNI-ISO 27001-A.12 :Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
d. SNI-ISO 27001-A.13 : Pengelolaan insiden keamanan informasi

4.6 Menentukan Maturity Level

Setelah menentukan klausal kontrol keamanan yang akan digunakan dalam audit keamanan sistem informasi, selanjutnya adalah menentukan nilai *maturity level*.. *Maturity level* dapat digunakan sebagai parameter untuk mengetahui sejauh mana Sekolah Tinggi Farmasi Bandung dalam melakukan implementasi sistem keamanan informasi pada suatu area kontrol keamanan

Tabel 6 Tabel Hasil *Maturity Level* Klausal 9 Keamanan Fisik dan Lingkungan

Klausual	Obyektif kontrol	Kontrol Keamanan	Rata-Rata/Obyektif Kontrol
9. Keamanan Fisik dan Lingkungan	9.1 Keamanan Area	9.1.1 Perimeter Keamanan Fisik	2,5
		9.1.2 Pengendalian Entri yang Bersifat Fisik	
		9.1.3 Mengamankan Kantor, ruangan dan fasilitas.	
		9.1.4 Perlindungan terhadap Ancaman Eksternal Dan Lingkungan	
		9.1.5 Bekerja Pada Area Aman	
		9.1.6 Pengiriman Akses Publik dan Bongkar Muat	
	9.2 Keamanan Peralatan	9.2.1 Penempatan dan Perlindungan Peralatan	2,7
		9.2.2 Sarana Pendukung	
		9.2.3 Keamanan Kabel	
		9.2.4 Pemeliharaan Peralatan	
		9.2.5 Keamanan Peralatan di Luar Lokasi	
		9.2.6 Penggunaan Kembali Peralatan	
		9.2.7 Pemindahan Property	
Maturity Level Klausal 9			2,6

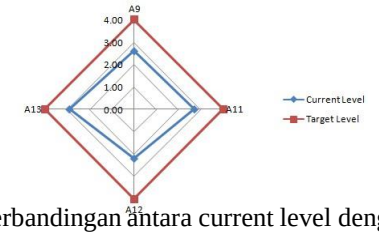
Setelah perhitungan *Maturity Level* dilakukan pada klausal 9,11, 12 dan 13 maka didapatkan nilai maturity level dari rata-rata semua nilai klausal. Hasil nilai maturity semua klausal dapat dilihat pada tabel berikut :

Tabel 7 Tabel nilai maturity semua klausal

Klausal	*Maturity level*
9	2,6
11	2,7
12	2,3
13	2,3
Nilai Maturity Level	2,5

4.7 Hasil Audit Keamanan Sistem Informasi

Dapat disimpulkan bahwa Berdasarkan audit keamanan sistem informasi dengan menggunakan SNI ISO/IEC 27001:2009 pada Sekolah Tinggi Farmasi Bandung sudah menerapkan kebijakan keamanan informasi dengan cukup baik. Hal ini ditunjukkan dari penilaian kematangan pada klausal keamanan yang bernilai 2,5yang berarti tingkat keamanan masih berada pada level 2 planned and tracked (sudah direncanakan dan dilacak secara aktif) namun telah mendekati level 3 well defined (telah didefinisikan dengan baik). Berikut adalah kondisi Gap antara *Maturity level* yang diharapkan pada 4 klausal kontrol keamanan yang dipilih yaitu klausa 9, 11, 12 dan 13. Seperti yang ditunjukan pada gambar bahwa kondisi saat ini *Maturity level* yang sedang terjadi (*current level*) digambarkan pada garis biru sedangkan *Maturity level* yang diharapkan (*Target level*) berada pada garis merah. Terlihat bahwa *maturity level* yang diharapkan yaitu empat yaitu terkelola dan terukur. Pemilihan level target ini berdasarkan pertimbangan hasil audit dimana nilai obyektif kontrol banyak tersebar di antara rentang nilai 2 dan 4. Berikut adalah grafik temuan audit yang membandingkan current level dengan target level



Gambar 2 Perbandingan antara current level dengan target level

Berikut adalah kesimpulan yang didapat berdasarkan temuan audit yang diperoleh :

1.Peraturan untuk menjaga kerahasiaan password masih kurang tegas dan kurang spesifik, belum adanya perjanjian atau pernyataan tertulis yang ditandatangani untuk benar-benar menjaga kerahasiaan password masing-masing, kurangnya kesadaran serta pengetahuan karyawan terhadap pentingnya merahasiakan password.

2.Masih adanya kebijakan dan prosedur yang belum terdokumentasi secara formal, tanpa ada aturan baku yang bersifat formal seperti misalnya kebijakan penggunaan aset di luar jam kerja.

3.Adanya kejadian penembusan sistem informasi akademik oleh mahasiswa yang ingin merekayasa nilai mata kuliah menandakan perlunya pembuatan sebuah sistem Manajemen insiden Keamanan Informasi agar ke depannya peristiwa tersebut bisa dicegah dan ditangani dengan lebih baik dari sebelumnya.

4.Server Siakad yang terkadang mati karena Gangguan listrik dari PLN perlu mendapat perhatian khusus dengan menyediakan UPS berbasis trafo atau genset dengan daya yang besar agar mampu mempertahankan computer server tetap menyala ketika pemadaman

5.Sudah adanya prosedur keamanan untuk melindungi akses ke ruangan pengolahan informasi

6.Sudah adanya prosedur untuk merespon kesalahan validasi, pendefinisian tanggung jawab semua personel yang terlibat dalam proses masukan data

4.8 Rekomendasi

Berdasarkan hasil audit yang telah dilakukan ditemukan beberapa hal yang harus diperhatikan oleh managemen Sekolah Tinggi Farmasi Bandung. Berikut adalah rekomendasi yang diberikan sebagai langkah perbaikan :

1. Berdasarkan hasil analisis data pada ISO 27001 klausa 9 Keamanan Fisik dan Lingkungan perlu dipasangnya CCTV dan Fingerprint door lock di ruangan server untuk mencegah pencurian, perusakan server dan akses oleh orang yang tidak berkepentingan

2. Berdasarkan hasil analisis data pada ISO27001 klausa 11 Manajemen Kontrol Akses pada klausal kontrol pengendalian akses perlu diberlakukan aturan tertulis tentang wajibnya semua karyawan yang mempunyai user id dan password harus mengganti password secara rutin misalnya 6 bulan sekali. Mengenai password sendiri disarankan memiliki kombinasi angka dan huruf dengan panjang tak kurang dari 8 character hal tersebut dimaksudkan agar password memiliki kualitas yang tinggi

3. Berdasarkan hasil analisis data pada ISO 27001 klausa 11 Manajemen Kontrol Akses pada klausal kontrol pengendalian akses pada Sesi Time Out, akan lebih baik apabila bagi sistem informasi SIAKAD agar memiliki batas akses bagi user yang sedang login dengan user id namun meninggalkan komputer tersebut dalam waktu yang lama misalnya 30 menit. Apabila telah lewat 30 menit, user id akan secara otomatis log out. Hal tersebut dimaksudkan agar data tidak dilihat pihak yang tidak berwenang.

4.Berdasaran hasil analisis data pada ISO 27001 klausa 12. Akusisi, Pengembangan dan Pemeliharaan Sistem Informasi perlu adanya prosedur pengecekan validasi yang dimasukkan secara langsung ke dalam aplikasi SIAKAD untuk mendeteksi kerusakan informasi melalui kesalahan pengolahan atau tindakan yang disengaja.

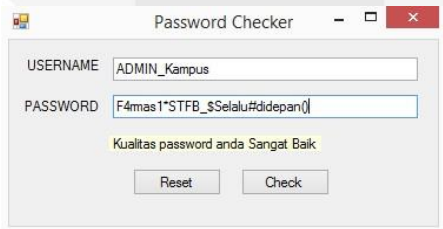
5.Berdasarkan hasil analisis data pada ISO 27001 klausa 13. Manajemen insiden Keamanan Informasiperlu adanya pembangunan sebuah sistem yang melakukan pemantauan, peringatan, dan kerentanan yang digunakan untuk mendeteksi insiden keamanan informasi sehingga manajemen bisa segera membereskan insiden tersebut dengan cepat dan efektif.

4.9 Implementasi Rekomendasi

Sesuai dengan rekomendasi pada penelitian ini akan dibuat contoh aplikasi pengecekan kualitas password dan design interface Sistem Deteksi Penyusup dalam Jaringan Komputer.:

a. Aplikasi Pengecekan Kualitas Password

Aplikasi pengecekan kualitas password bisa menjadi pedoman bagi pengguna Sistem Informasi Akademik STFB dalam memilih password yang aman untuk digunakan. Aplikasi ini dibangun dengan menggunakan Microsoft Visual Studio 2015 dengan bahasa pemrograman C.

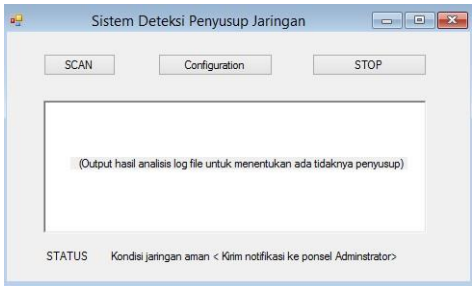


Gambar 3 Aplikasi Pengecekan kualitas password

b. Design interface Sistem Deteksi Penyusup dalam Jaringan Komputer

Design ini bisa menjadi pedoman bagi pihak management STFB dalam rangka pembangunan sebuah sistem yang melakukan pemantauan, peringatan, dan kerentanan yang digunakan untuk mendeteksi insiden keamanan informasi seperti misalnya insiden penyusupan jaringan komputer oleh pihak yang tidak berkepentingan.Sistem akan melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah jaringan. Jika ditemukan abnormality dalam traffic jaringan maka sistem akan memberikan

peringatan kepada administrator jaringan. Sistem deteksi penyusup memiliki 2 sub sistem yaitu sistem yang berfungsi untuk membaca log file apabila perintah scan dilakukan dan sistem yang menganalisis hasil log file dan memberikan output berupa notifikasi kepada administrator.



Gambar 4 Design interface Sistem Deteksi Penyusup

Setelah sistem menganalisis hasil log file maka selanjutnya sistem akan mengirimkan notifikasi ke ponsel Adminstrator.

Gambar 5 Contoh Notifikasi Hasil Deteksi Sistem di Ponsel Administrator

5. Kesimpulan

5.1 Kesimpulan

Berdasarkan hasil analisis risiko dalam penelitian ini, ditentukan 16 kontrol objektif dan 57 kontrol keamanan yang tersebar dalam 4 klausal ISO 27001 yang digunakan dalam proses audit keamanan sistem informasi. Dari hasil audit keamanan sistem informasi dengan menggunakan SNI ISO/IEC 27001:2009 pada Sekolah Tinggi Farmasi Bandung dapat disimpulkan bahwa Sekolah Tinggi Farmasi Bandung sudah menerapkan kebijakan keamanan informasi dengan cukup baik. Hal ini ditunjukkan dari penilaian tingkatan kematangan pada klausal keamanan yang bernilai 2,5 yang berarti kontrol keamanan masih berada pada level 2 *planned and tracked* (telah direncanakan dan dilacak secara aktif) namun telah mendekati level 3 *well defined* (sudah didefinisikan dengan baik). Dalam penelitian ini juga dibuat 2 contoh implementasi rekomendasi yaitu aplikasi pengecekan kualitas password dan Design Interface Sistem Deteksi Penyusup dalam Jaringan Komputer

5.2 Saran

1. Melakukan proses penjadwalan audit internal keamanan informasi (audit internal SMKI) secara berkala misalnya setiap 3 bulan sekali guna mengevaluasi perkembangan proses implementasi sistem keamanan informasi STFB agar sesuai dengan target yang diharapkan oleh pihak manajemen.

2. Karena sistem informasi akademik STFB yang baru berdiri selama 2 tahun ini belum pernah diaudit keamanannya, pihak manajemen STFB dapat melakukan audit keamanan sistem informasi dengan menggunakan standar lain sebagai perbandingan seperti misalnya dengan menggunakan standar COBIT 5.1

Daftar Pustaka :

[1] Utomo,Margo., Ahmad Holil Noor Ali & Irsal Affandi (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya

[2]_____.Pentingnya Audit Sistem Informasi bagi perusahaan, dikutip tanggal 19 Oktober 2015 [online]. Available: http://may9946.wordpress.com/2013/03/02/pentingnya-audit-sistem-informasi-bagi-perusahaan/

[3] Syafrizal, Melwin 2009. Informasi Security Management System (ISMS) Menggunakan Standar ISO 27001:2005

[4] Tim Direktorat Keamanan Informasi Depkominfo. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik.5Menteri Keuangan Republik Indonesia. 2010. KMK Nomor 479/KMK.01/2010 tanggal 13 Desember2010

[5] Ferdinand Aruan (2003), Tugas Keamanan Jaringan Informasi (Dosen. Dr. Budi Rahardjo) Tinjauan Terhadap ISO 17799 -Program Magister Teknik Elektro Bidang Khusus TeknologiInformasi ITB, dikutip tanggal 19 Oktober 2015, [online].Available:https://www.hitpages.com/doc/6191032416862208/1

[6] SNI ISO/IEC 27001 :2009 Information Tecnology-Security Techniques

[7]Bakuan Audit Keamanan Informasi Kemenpora. Agustus 2012.