p-ISSN : 2407 – 1846
e-ISSN : 2460 – 8416

Website : jurnal.umj.ac.id/index.php/semnastek

IMPLEMENTASI ISO/IEC 27001:2013 UNTUK SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) PADA FAKULTAS TEKNIK UIKA-BOGOR

Ritzkal[1*], Arief Goeritno[2], A. Hendri Hendrawan[3]
[*13]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ibn Khaldun Bogor
[2]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Ibn Khaldun Bogor
Jl. KH. Sholeh Iskandar KM.2, Kedung Badak, Tanah Sereal, Kota Bogor 16162 Jawa Barat
E-mail: ritzkal@ft.uika-bogor.ac.id

ABSTRAK

Telah dilakukan analisis terhadap sistem manajemen keamanan informasi pada lingkungan Fakultas Teknik Universitas Ibn Khaldun (UIKA) Bogor berdasarkan ISO/IEC 27001: 2013 Klausal 11 Kontrol Akses. Standardisasi ISO/IEC 27001:2013, adalah suatu standar berkenaan dengan Sistem Manajemen Keamanan Informasi (SMKI, *ISMS*: *Information Security Management System*) yang dipublikasikan pada 25 September 2013. Sistem Manajemen Keamanan Informasi (SMKI), adalah pendekatan sistematis untuk pengelolaan informasi sensitif institusi, agar tetap dalam kondisi aman. Di dalamnya termasuk orang, proses, dan sistem teknologi informasi melalui penerapan proses manajemen risiko. Analisis terhadap SMKI pada penelitian ini dimaksudkan untuk memperoleh tingkat keamanan pada jaringan *hotspot* Fakultas Teknik berdasarkan standar tersebut. Dilakukan pembuatan suatu kuesioner dengan pendekatan *Plan-Do-Check-Act* (*PDCA*). Pengisian kuesioner dikenakan terhadap 2 jenis responden, yaitu pengguna dan manajemen. Responden pengguna dibatasi pada 20 orang dengan sistem sampling dalam pengisian kuesioner, sedangkan manajemen menunjuk satu orang pengelola jaringan *hotspot*. Diperoleh hasil, yaitu (1) pengguna hanya mempercayai tingkat keamanan sebesar 49% dan (2) pihak manajemen hanya mempercayai tingkat keamanan sebesar 45%. Berdasarkan hal itu ditunjukkan, bahwa SMKI pada jaringan *hotspot* di Fakultas Teknik kurang aman menurut Standarisasi ISO/IEC 27001:2013.

Kata-kata Kunci: ISO/IEC 27001:2013, sistem manajemen keamanan informasi, FT-UIKA.

ABSTRACT

Analyzing the information security management system at the Faculty of Engineering, Bogor Ibn Khaldun University based on ISO/IEC 27001: 2013 clauses 11 Access Control have been done. ISO/IEC 27001:2013 is an information security standard that was published on the 25th September 2013. An ISMS is a systematic approach to managing sensitive company information so that it remains in secure condition. It includes people, processes, and IT systems by applying a risk management process. Analysis of the ISMS in this research is intended to obtain the level of security for hotspot network at the Faculty of Engineering is based on these standards. Preparation of a questionnaire carried out by the approach of Plan-Do-Check-Act (PDCA). Filling the questionnaire subjected to two types of respondents, namely users and management. Respondents of user were limited to 20 people to fill out a questionnaire with a sampling system, whereas the management appointed the someone as a responsible hotspot network. The results obtained, namely (1) the users trust that the level of security is only 49% and (2) the management trust that the level of security of only 45%. Accordingly, it was shown, that the ISMS on the hotspot network at the Faculty of Engineering is in less secure, if according to ISO/IEC 27001:2013.

Keywords: ISO/IEC 27001:2013, information security management system, FT-UIKA.

PENDAHULUAN

Informasi maupun data saat ini sudah menjadi hal yang sangat berharga, bahkan dapat dikatakan sangat vital, sehingga kerusakan atau kebocoran terhadap informasi suatu organisasi dapat berakibat organisasi tersebut berhenti atau tutup. Keberadaan suatu informasi atau data sangatlah berharga, maka tidaklah heran jika kemudian bermunculan beberapa pihak yang tidak bertanggung jawab, dimana pihak tersebut berusaha mencuri maupun merusak dan mengubah data atau informasi dari sistem komputer yang dimiliki oleh suatu organisasi tertentu(Bulu, Hariawan, Nur. 2013). Berdasarkan hal itu, dibutuhkan keamanan sistem informasi yang terjamin keamanan sistem secara menyeluruh.

p-ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Jaringan *hotspot* Fakultas Teknik merupakan salah satu jaringan komputer yang berada di lingkungan Fakultas Teknik Universitas Ibn Khaldun Bogor, dimana *hotspot* Fakultas Teknik dikelola secara independen oleh Fakultas Teknik. Keberadaan Fakultas Teknik yang memiliki 4 jurusan/program studi merupakan fakultas dengan jumlah mahasiswa terbanyak urutan kedua setiap tahunnya. Ancaman itu sendiri dapat berasal dari ancaman internal, eksternal, tak terstruktur, dan ancaman yang terstruktur. Pengamanan sistem informasi dapat dimulai dengan pencegahan serangan dari dalam, karenan serangan yang berasal dari dalam lebih sering terjadi dan lebih berbahaya.

Klausal 11 Kontrol Akses ISO/IEC 27001:2005 adalah standar *information security* yang diterbitkan pada Oktober 2005 oleh *International Organization for Standarization* (ISO) dan *International Electrotechnical Commission* (IEC). Standar ini menggantikan BS-77992:2002 (*British* Standard) dan membahas tentang pengamanan dari dalam, khususnya bagaimana pengamanan perangkat-perangkat jaringan dari individu-individu yang tidak berwenang dalam pengaksesannya (Kamat, M. 2012). Tujuan penelitian ini, yaitu memperoleh tingkat keamanan pada jaringan *hotspot* Fakultas Teknik berdasarkan standar ISO/IEC 27001:2005 klausal 11.2 dan 11.3.

METODE

Tempat penelitian di Fakultas Teknik, Universitas Ibn Khaldun Bogor dengan alamat Jalan K.H. Sholeh Iskandar. Bahan penelitian yang digunakan dalam penelitian ini berupa jaringan *hotspot* berdasarkan ISO 27001 Klausal 11 Kontrol Akses dilakukan dengan pengumpulan data, pembagian jenis-jenis data, dan analisis data yang diperlukan dengan tujuan kemudahan dalam pemecahan masalah.

Metode pengumpulan data untuk penelitian ini, yaitu observasi, penyebaran kuesioner, dan pengolahan data.

Observasi

Observasi yang dilakukan dalam melaksanakan penelitian ini, bertujuan untuk melihat kondisi dan keadaan yang berada di lingkungan Fakultas Teknik melalui *survey* langsung ke lapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya yang digunakan di lingkungan Fakultas Teknik. Gambaran yang didapat antara lain tentang keamanan jaringan *hotspot, software* dan *hardware* yang digunakan pada jaringan *hotspot.*

Kuesioner

Kuesioner merupakan daftar pertanyaan yang akan digunakan oleh periset untuk memperoleh data dari sumbernya secara langsung melalui proses komunikasi atau dengan mengajukan pertanyaan. Jenis kuesioner yang digunakan pada penelitian ini dengan menggunakan kuesioner terstruktur yang terbuka. Pada penelitian ini kuesioner dibuat untuk 2 jenis responden yaitu Kuesioner untuk Mahasiswa Fakultas Teknik Informatika dan Kuesioner untuk Unit Komputer Sistem Informasi (UKSI).

Pengolahan Data Kuesioner

Hasil data kuesioner diperoleh 20 contoh (*sample*) sejumlah mahasiswa setiap angkatan pada Fakultas Teknik dari jumlah yang ada. Metode penelitian ini disesuaikan ke ISO 27001 Klausal 11 Kontrol Akses dengan pendekatan proses *Plan, DO, Check, and Act* (*PDCA*) yang berada pada Standardisasi ISO 27001. Penjelasan metode pendekatan *PDCA,* yaitu:

a) ***Plan*****.** Tahapan ini merupakan kegiatan perencanaan dan perancangan SMKI. Tataran implementasinya adalah pembangunan komitmen, kebijakan, kontrol, prosedur, instruksi kerja, dan lainnya agar tercipta SMKI sesuai dengan keinginan, sehingga dilakukan analisis kebutuhan untuk penunjang kelengkapan dalam penelitian.

b) ***Do*****.** Kegiatan dalam tahapan ini, adalah implementasi dan operasi dari kebijakan, kontrol, proses, dan prosedur SMKI yang telah direncanakan pada tahapan *Plan*. Tahapan *do*, meliputi tentang pembuatan kuesioner yang diserahkan kepada Unit Komputer dan Sistem Informasi (UKSI) dan sejumlah mahasiswa Fakultas Teknik.

c) ***Check*****.** Bagian ini membahas tentang kegiatan pemonitoran pelaksanaan SMKI, termasuk pelaksanaan evaluasi dan audit terhadap SMKI. Proses dari kuesioner, tahapan ini dilakukan untuk pengolahan kuesioner yang dibuat sesuai dengan Standar ISO 27001.

d) ***Act*****.** *Act* adalah kegiatan *improvement*, yaitu kegiatan perbaikan dan pengembangan SMKI. Hal inilah yang

p-ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

diistilahkan dengan perbaikan yang terus-menerus, sehingga kegiatan perbaikan yang terus-menerus seharusnya dilakukan terhadap SMKI yang dibuat, karena hal itu merupakan bagian dari siklus hidup SMKI. Tahapan ini, adalah tahapan pemberian saran.

HASIL DAN PEMBAHASAN

Standarisasi ISO 27001 adalah suatu Standarisasi mengenai Sistem Manajemen Keamanan Informasi (SMKI), pada penelitian ini bermaksud untuk mengetahui Analisis Manajemen Keamanan Pada Jaringan *Hotspot* Berdasarkan ISO 27001 Klausal 11 Kontrol Akses pada Fakultas Teknik, diperoleh hasil berupa suatu kuesioner yang diisi oleh 2 jenis responden, yaitu pengguna dan pihak manajemen. Responden sebagai pengguna, digunakan sistem *sample*, dimana hanya diberikan kepada 20 orang dan 1 responden dari pihak manajemen. Diperoleh hasil 49% dari pengguna dan 45% dari manajemen. Hal itu berarti, Manajemen Keamanan Informasi pada jaringan *hotspot* di Fakultas Teknik kurang aman menurut Standar ISO 27001.

Berdasarkan hasil, maka dilakukan analisis berkenaan metode pendekatan *PDCA* sesuai standar ISO 27001(Herrmann, D.S. 2002).

Plan

Tahapan ini pembahasan tentang analisis kebutuhan yang digunakan yang meliputi: analisis data dan proses.

Analisis data

Analisis data dengan standar ISO 27001 Klausal 11 Kontrol Akses. Klausal 11.2 dan 11.3, seperti ditunjukkan pada Tabel 1.

Tabel 1 Klausal 11.2 dan 11.3

No.	Kriteria	Variabel (peubah)
1	Manajemen Akses *User*	Registrasi pengguna
		Manajemen istimewa atau khusus
		Manajemen *password*
		Tinjauan terhadap hak Akses *User*
2	Tanggung Jawab Pengguna	Pengguna *password*
		Peralatan pengguna yang tidak di jaga
		Kebijakan *clear desk* dan *clear screen*

Analisis proses

Analisis proses pada pada jaringan *hotspot* berdasarkan ISO 27001 Klausal 11 Kontrol Akses, dijelaskan tentang proses suatu sistem dan keluaran yang diharapkan. Analisis proses ini menggambarkan tentang proses perencanaan pembuatan kuesioner yang diberikan kepada responden dan diperoleh sejumlah criteria. nya. Kriteria hasil analisis proses sesuai standar ISO 27001, seperti ditunjukkan pada Tabel 1.

Tabel 2 Kriteria hasil analisis proses sesuai standar ISO 27001

Nilai Persentase	Kriteria
> 73	Aman
64-73	Cukup aman
53-63	Kurang aman
42-52	Tidak aman
< 42	Berisiko tinggi

p-ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Do

Tahapan ini berupa penjelasan tentang bagaimana cara pembuatan kuesioner yang sesuai dengan standar ISO 27001. Kuesioner ini dibuat menjadi 2 bagian, yaitu kuesioner untuk mahasiswa sebagai pengguna dan kuesioner untuk pihak manajemen yang diwakili oleh Unit Komputer dan Sistem Informasi (UKSI).

Check

Tahapan ini berupa pembahasan tentang evaluasi pada berkas dan bukti pengisian kuesioner yang dilakukan oleh sejumlah contoh mahasiswa dan salah satu pihak manajemen atau administrator pada Fakultas Teknik.

Kuesioner dari mahasiswa

Kuesioner ini sebagai *sample* yang hanya 20 orang pengisi kuesioner tersebut dengan 66 pertanyaan, Berdasarkan 66 pertanyaan dan 20 responden dengan 1320 butir pertanyaan yang dijawab, maka yang menjawab "ya" sebanyak 658 butir pertanyaan dan yang menjawab "tidak" sebanyak 662 butir pertanyaan. Untuk pembuatan persentase yang menjawab "ya" sebanyak (658/1320) x 100 = 49 %, sedangkan persetase yang menjawab "tidak" sebanyak 51%.

Kuesioner dari pihak manajemen atau *administrator*

Kuesioner yang diberikan kepada ihak manajemen sebanyak 148 butir pertanyaan, dimana pertanyaan yang diberikan kepada pengguna dengan pihak manajemen sangat berbeda. Berdasarkan dari 148 butir pertanyaan yang dijawab, maka yang dijawab "ya" sebanyak 67 butir pertanyaan dan yang dijawab "tidak" sebanyak 80 butir pertanyaan. Untuk pembuatan persentase yang dijawab "ya" sebanyak (67/148) x 100% = 45%, sedangkan yang dijawab "tidak" sebanyak 55%.

Act

Tahapan ini berupa pembahasan tentang perbaikan dan kelemahan yang ada pada jaringan *hotspot* di Fakultas Teknik, meliputi ketidakadaan prosedur tentang pengolahan jaringan *hotspot* seperti bagaimana cara pengubahan *password*, keberadaan seberapa level yang ada pada *hotspot* tersebut, dan lainnya. Prosedur tersebut sangat penting untuk pengolahan jaringan *hotspot* dengan standari ISO 27001. Disarankan untuk pembuatan prosedur terlebih dahulu dalam pengelolaan jaringan *hotspot*, agar lebih teratur dan dimengerti oleh semua pihak. Berdasarkan hasil pengolahan tersebut berupa pengolahan jaringan *hotspot* yang ada pada Fakultas Teknik dibawah 55%, sehingga sesuai standar ISO 27001, maka jaringan *hotspot* di Fakultas Teknik tergolong tidak aman sampai dengan kurang aman.

SIMPULAN DAN SARAN

Simpulan

Hasil analisis keamanan dengan ISO 27001 pada jaringan *hotspot* di Fakultas Teknik, adalah kuesioner yang diambil secara *sample* dari pengguna sebanyak 20 orang dengan 1320 butir soal yang menjawab "ya" sebesar 49%. Berdasarkan standar ISO 27001 dengan hasil 49% berarti masuk kategori "tidak aman". Analisis kuesioner dari pihak manajemen terdapat 147 butir pertanyaan dan yang dijawab "ya" sebanyak 45%, sehingga dengan nilai 45% yang idasarkan standar ISO 27001, masuk kategori "tidak aman". Berdasarkan kedua jenis kuesioner ditunjukkan, bahwa manajemen keamanan pada jaringan *hotspot* berdasarkan ISO 27001 Klausal 11 Kontrol Akses, terbukti "tidak aman".

Saran

Beberapa hal yang perlu diperbaiki, yaitu prosedur untuk manajemen keamanan tidak ada dan ketidakadaan sistem keamanan jaringan *Internet*. Hal itu berdampak kepada kerusakan terhadap sejumlah alat-alat jaringan *Internet.* Saran lebih lanjut, perlu pengembangan selanjutnya yang dapat dilakukan untuk pengoptimalan peranan sistem keamanan jaringan *hotspot*, diantaranya pengembangan selanjutnya sesuai Klausal 12 pada ISO 27001 dan pengembangan selanjutnya berupa dilakukan audit internal terhadap sistem keamanan *hotspot.*

DAFTAR PUSTAKA

Azuwa, et al. 2012. Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standart. Vol 1(4): 280-288. International Journal of Cyber-Security and Digital Forensics (IJCSDF).

Bulu, Hariawan, Nur. 2013. "Analisis Keamanan Jaringan STMIK AMIKOM

p-ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Yogyakarta Berdasarkan *ISO/IEC* 27001:2005 Standar A.11.4.4". Yogyakarta. STMIK AMIKOM Yogyakarta.

Herrmann, D.S. 2002. "*Security Engineering and Information Assurance"*. Auerbach

International Standart ISO/IEC 27001. (2013). Information Technology – Security Techniques – Information Security Management Systems – Requirement. ISO/IEC 2013.

Kamat, M. 2012. Dari ISO 27001 Security: http://www.ISO27001 security.com (Di unduh : Tanggal 3 Juni 2015)

Mataracioglu, Tolga & Ozkan, Sevgi. (2011). *Analysing of the User Acceptance for Implementing ISO/IEC 27001:2005 in Turkish Public Organizations.* Vol 3, No 1. International Journal of Managing Information Technology (IJMIT)