

ANALISIS SISTEM KEAMANAN SUMBERDAYA MANUSIA DENGAN PENERAPAN ISO 27001 KLAUSAL 9 DI UNIVERSITAS IBN KHALDUN BOGOR

Andri Rinaldi¹⁾, Ritzkal²⁾, Bayu Adhi Prakosa²⁾, Arief Goeritno³⁾

^{1),2)}Program Studi Teknik Informatika, Fakultas Tekni, Universitas Ibn Khaldun Bogor
³⁾Program Studi Teknik Elektro, Fakultas Teknik, Universitas Ibn Khaldun Bogor
Jl. Sholeh Iskandar km.2, Kedung Badak, Tanah Sareal, Kota Bogor 16162 Jawa Barat
Email: andri_rinaldi60@yahoo.com

Abstrak. Telah dilakukan analisis terhadap sistem keamanan sumberdaya manusia pada lingkungan Universitas Ibn Khaldun (UIKA) Bogor berdasarkan ISO/IEC 27001: 2013 Klausul 9 Sumberdaya Manusia. 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 yang berada di lingkungan Universitas Ibn Khaldun (UIKA) Bogor 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 200 orang dengan sistem sampling dalam pengisian kuesioner, sedangkan manajemen menunjuk satu orang pengelola keamanan jaringan. Diperoleh hasil, yaitu (1) pengguna hanya mempercayai tingkat keamanan sebesar 49,96% dan (2) pihak manajemen hanya mempercayai tingkat keamanan sebesar 66%. Berdasarkan hal itu ditunjukkan, bahwa SMKI pada jaringan hotspot di Universitas Ibn Khaldun (UIKA) Bogor kurang aman menurut Standardisasi ISO/IEC 27001:2013.

Kata kunci: ISO/IEC 27001:2013, sistem manajemen keamanan informasi, FT-UIKA

1. Pendahuluan

Kejahatan dalam penggunaan Teknologi Informasi (TI) sangat erat dengan kejahatan dalam penggunaan komputer dan *Internet*, karena keduanya memegang peranan penting di dunia TI. Kejahatan dalam penggunaan TI, kemudian lebih sering dikenal dikalangan masyarakat luas sebagai kejahatan komputer. Kejahatan komputer pada dasarnya dilakukan pada aset dimaksud, antara lain berupa informasi, aset fisik, aset peranti lunak, pelayanan, orang, maupun aset yang tidak terukur (*intangible*), misal reputasi dan *image* perusahaan[1].

Setiap perusahaan, instansi, dan institusi memiliki beberapa sumberdaya yang harus dijaga. Sumberdaya menurut para ahli merupakan kemampuan terpadu dari daya pikir dan daya fisik yang dimiliki individu. Kemampuan sumberdaya manusia tidak dapat dilihat dari satu sisi saja, namun harus mencakup keseluruhan dari daya pikir dan juga daya fisik. Dalam sumberdaya yang dimiliki tersebut, maka setiap perusahaan ataupun institut wajib dipelihara dan dijaga, agar tidak dimiliki oleh orang lain[2].

Jaringan *hotspot* yang berada di lingkungan Universitas Ibn Khaldun Bogor adalah salah satu sumberdaya yang harus dijaga dari sebuah ancaman yang ada. Ancaman yang 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.

Standardisasi ISO 27001 memiliki 15 Klausul yaitu terdiri dari, Klausul 1 sampai 3 mengenai organisasi, Klausul 4 mengenai sistem manajemen kemanan informasi, Klausul 5 mengenai kebijakan keamanan, Klausul 6 mengenai organisasi keamanan informasi, Klausul 7 mengenai manajemen aset, Klausul 8 mengenai keamanan sumberdaya manusia, Klausul 9 mengenai keamanan sumberdaya

manusia, Klausal 10 mengenai manajemen komunikasi dan operasi, Klausal 11 mengenai control akses, Klausal 12 mengenai akuisisi sistem informasi, pembangunan dan pemeliharaan, Klausal 13 mengenai manajemen kejadian keamanan informasi, Klausal 14 mengenai manajemen kelangsungan bisnis dan Klausal 15 mengenai kepatutan[4].

Penelitian ini merupakan analisis standardisasi ISO 27001 Klausal 9 yang membahas mengenai keamanan sumberdaya manusia, khususnya menerangkan pembatas keamanan fisik, kontrol masuk fisik, keamanan kantor, perlindungan terhadap ancaman, bekerja di wilayah aman, akses publik, letak peralatan, keamanan peralatan di luar tempat yang tidak disyaratkan, keamanan untuk pembuangan atau pemanfaatan kembali peralatan, dan hak pemanfaatan[7,8]. Penekanan pada penelitian ini diambil dari klausal 9 tentang Sumberdaya Manusia yang berada di Universitas Ibn Khaldun Bogor yang berdasarkan pada ISO 27001.

Berdasarkan penelitian pada Universitas Ibn Khaldun Bogor dalam melakukan Keamanan Sumberdaya Manusia yang ada tentang penerapan dengan ISO 27001 ini ada, terdapat beberapa masalah yang dihadapi, yaitu bagaimana analisis sistem keamanan Sumberdaya Manusia dengan ISO 27001 Klausal 9 di Universitas Ibn Khaldun Bogor dan apa rekomendasi yang diberikan dari hasil analisis terhadap penelitian tersebut. Berdasarkan kepada rumusan masalah yang ada, maka tujuan penelitian ini, yaitu memperoleh data hasil analisis sistem keamanan Sumberdaya Manusia dengan ISO 27001 Klausal 9 di Universitas Ibn Khaldun Bogor dan memperoleh hasil akhir sebagai rekomendasi kepada manajemen Universitas Ibn Khaldun Bogor berdasarkan Standardisasi ISO 27001 Klausal 9.

Berdasarkan latar belakang tersebut, maka dilakukan analisis sistem keamanan sumberdaya manusia dengan penerapan ISO 27001 Klausal 9 di Universitas Ibn Khaldun Bogor melalui 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 yang dilakukan dalam pelaksanaan penelitian ini, bertujuan untuk tinjauan terhadap kondisi dan keadaan yang terdapat di lingkungan Universitas Ibn Khaldun Bogor melalui *survey* langsung ke lapangan untuk perolehan hasil sesungguhnya dan gambaran seutuhnya yang digunakan di lingkungan Universitas Ibn Khaldun Bogor. Kuesioner merupakan daftar pertanyaan yang digunakan oleh peneliti untuk perolehan data dari sumber secara langsung melalui proses komunikasi atau dengan pengajuan pertanyaan. Jenis kuesioner yang digunakan pada penelitian ini berupa kuesioner terstruktur yang terbuka. Kuisener pada penelitian ini dibuat untuk 2 jenis responden, yaitu kuesioner untuk para mahasiswa dari setiap fakultas dan kuesioner untuk Unit Komputer Sistem Informasi (UKSI). Metode penelitian ini secara umum disesuaikan ke ISO 27001 Klausal 9 Sumberdaya manusia dengan pendekatan proses *Plan, DO, Check, and Act (PDCA)* yang berada pada Standardisasi ISO 27001[1,3,4].

2. Pembahasan

ISO (*International Organization for Standarization*) adalah pengembang terbesar di dunia standar internasional secara sukarela. Standar Internasional memberikan sentuhan seni untuk spesifikikasi produk, layanan dan praktik yang baik, membantu industri lebih efisien dan efektif. Dikembangkan melalui kesepakatan global, mereka membantu untuk mengatasi hambatan perdagangan internasional (ISO)[9].

ISO mengembangkan standar internasional. ISO didirikan pada tahun 1947, dan sejak itu telah menerbitkan lebih dari 19.500 standar internasional mencakup hampir semua aspek teknologi dan bisnis. Dari keamanan pangan ke komputer, dan pertanian untuk kesehatan, ISO standar internasional berdampak pada semua aspek kehidupan kita (ISO)[10].

Standardisasi ISO 27001 adalah suatu Standardisasi mengenal Sistem Manajemen Keamanan Informasi (SMKI), pada penelitian ini bermaksud mengetahui Analisis keamanan sumberdaya manusia dengan ISO 27001 Klausal 9 di Universitas Ibn Khaldun Bogor. Dimana dalam memperoleh hasil peneliti membuat suatu kuesioner yang akan diisi oleh 2 jenis responden yaitu pengguna dan manajemen. Responden sebagai pengguna, digunakan sistem sample, dimana hanya diberikan kepada

200 orang dan 1 responden dari pihak manajemen. Diperoleh hasil 49,91% dari pengguna dan 66% dari manajemen. Hal itu berarti, Manajemen Keamanan Sumberdaya manusia pada Universitas Ibn Khaldun Bogor kurang aman menurut Standar ISO 27001. Berdasarkan hasil, maka dilakukan analisis berkenaan metode pendekatan *PDCA* sesuai standar ISO 27001 [5].

2.1. Analisis sistem keamanan sumberdaya manusia dengan ISO 27001 Klausal 9

Tahapan ini membahas tentang *plan*, *do*, dan *check*.

Plan

Tahapan *plan* berupa analisis kebutuhan yang meliputi analisis data dan proses.

a. Analisa data

Analisa data pada penelitian ini berdasarkan ISO 27001 Klausal 9. Klausal 9 tentang Sumberdaya Manusia, seperti ditunjukkan pada Tabel 1.

Tabel 1 Klausal 9 tentang Sumberdaya Manusia

No.	Kriteria	Variabel
1	Wilayah Aman	Pembatasan keamanan fisik
		Kontrol masuk fisik
		Keamanan kantor dan fasilitasnya
		Perlindungan terhadap ancaman dari luar dan lingkungan sekitar
		Bekerja di wilayah aman
		Akses publik, tempat pengiriman dan penurunan barang
2	Keamanan Peralatan	Letak Peralatan dan pengamanannya
		Utilitas pendukung
		Keamanan pengkabelan
		Pemeliharaan peralatan
		Keamanan peralatan diluar tempat yang tidak disyaratkan
		Keamanan untuk pembuangan atau pemanfaatan kembali peralatan
		Hak pemanfaatan

b. Analisis proses

Analisis proses pada Analisis Manajemen Keamanan Pada Jaringan *Hotspot* berdasarkan ISO 27001 Klausal 9 tentang Sumberdaya Manusia, menjelaskan tentang proses suatu sistem dan keluaran yang diharapkan sesuai dengan ISO 27001. Analisis proses ini menggambarkan tentang proses perancangan pembuatan kuesioner yang akan diberikan kepada responden dan mendapatkan kriterianya. Kriteria perhitungan ISO 27001 Klausal 9, seperti ditunjukkan pada Tabel 2.

Tabel 2 Kriteria perhitungan Klausal 9 tentang Sumberdaya Manusia

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

Do

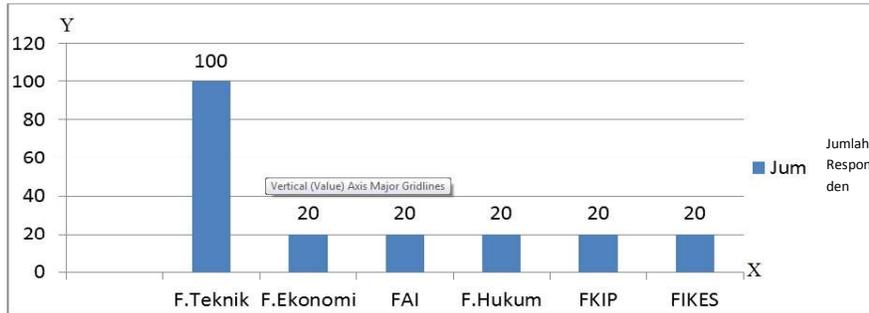
Tahapan ini menjelaskan tentang bagaimana cara membuat Kuesioner yang sesuai dengan Standardisasi ISO 27001. Kuesioner ini dibuat menjadi 2 bagian yaitu Kuesioner untuk Mahasiswa dan Kuesioner untuk Manajemen yaitu diwakili oleh Unit Komputer dan Sistem informasi (UKSI).

Check

Tahapan ini membahas mengenai evaluasi di dalam berkas dan bukti pengisian kuesioner yang dilakukan oleh perwakilan mahasiswa dan salah satu pihak Manajemen Unit Komputer dan Sistem Informasi (UKSI).

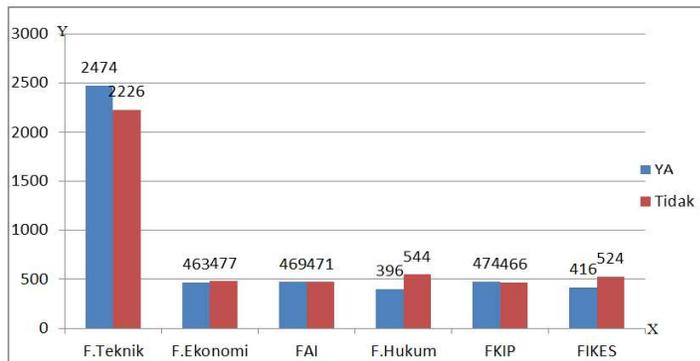
Kuesioner dari mahasiswa

Kuesioner ini sebagai sample (contoh) dari 200 orang pengisi kuesioner tersebut dengan 47 pertanyaan. Jumlah responden mahasiswa setiap fakultas, seperti ditunjukkan pada Gambar 1.



Gambar 1 Jumlah responden mahasiswa setiap fakultas

Berdasarkan 47 pertanyaan dan 200 responden dengan 9400 butir pertanyaan yang dijawab, maka yang menjawab “Ya” sebanyak 4692 butir pertanyaan dan yang menjawab “tidak” sebanyak 4708 butir pertanyaan. Persentase yang menjawab “Ya” $(4692/9400) \times 100 = 49,91\%$, sedangkan yang menjawab “tidak” sebanyak 50,09%. Jawaban responden mahasiswa, seperti ditunjukkan pada Gambar 2.



Gambar 2 Jawaban responden mahasiswa

Berikut contoh kuesioner yg sudah diisi, seperti ditunjukkan pada Gambar .



Gambar 3 Contoh kuesioner yang sudah diisi

Kuesioner dari pihak manajemen atau administrator

Kuesioner yang diberikan kepada pihak manajemen sebanyak 200 butir pertanyaan, dimana pertanyaan yang diberikan kepada pengguna dengan pihak manajemen sangat berbeda. Berdasarkan dari 200 butir pertanyaan yang dijawab, maka yang dijawab “ya” sebanyak 131 butir pertanyaan dan yang dijawab “tidak” sebanyak 68 butir pertanyaan. Untuk pembuatan persentase yang dijawab “ya” sebanyak $(132/200) \times 100 = 66\%$, sedangkan yang dijawab “tidak” sebanyak 44%.

2.2 Rekomendasi pada manajemen Universitas Ibn Khaldun Bogor berdasarkan Standardisasi ISO 27001 Klausal 9

Act

Tahapan ini berupa pembahasan tentang perbaikan dan kelemahan yang ada pada keamanan sumberdaya manusia di Universitas Ibn Khaldun Bogor, meliputi ketidak adaan prosedur tentang wilayah aman dan keamanan peralatan seperti pembatasan keamanan fisik, letak peralatan dan pengamanannya. Prosedur tersebut sangat penting untuk pengolahan Sumberdaya manusia dengan standar ISO 27001. Disarankan untuk membuat prosedur terlebih dahulu dalam menglola keamanan sumberdaya manusia dengan ISO 27001 Klausal 9 di Universitas Ibn Khaldun Bogor agar lebih teratur dan di mengerti oleh semua pihak. Dari hasil pengolahan tersebut dibawah 47,606% jika menurut Standardisasi ISO 27001 maka keamanan sumberdaya manusia dengan ISO 27001 maka keamanan sumberdaya manusia dengan ISO 27001 Klausal 9 di Universitas Ibn Khaldun Bogor tergolong Tidak Aman sampai dengan Kurang Aman.

Simpulan

Berdasarkan pembahasan, maka ditarik simpulan sesuai tujuan penelitian.

1. Berkenaan dengan analisis sistem keamanan sumberdaya manusia maka hasil analisis keamanan dengan ISO di Universitas Ibn Khaldun Bogor sebagai berikut : kuesioner yang di ambil secara sample dari pengguna 200 orang dan 9400 butir pertanyaan yang menjawab Ya sebesar 49,91%. Menurut Standardisasi ISO 27001 dengan hasil 49,91% berarti masuk kategori Tidak Aman. Analisis kuesioner selanjutnya dari manajemen dimana ada 200 butir pertanyaan dan yang menjawab Ya sebesar 66%. Menurut Standarisasi ISO 27001 dengan hasil 66% masuk Cukup Aman. Dari 2 jenis kuesioner tersebut maka analisis sistem keamanan sumberdaya manusiadengan penerapan ISO 27001 Klausal 9 sumber daya manusia dinyatakan Cukup Aman.
2. Rekomendasi pada analisis sistem keamanan sumber daya manusia menurut ISO 27001 klausal 9 adalah tidak adanya procedure pengelolaan sumber daya manusia seperti pengelolaan peralatan, wilayah aman dan lain lain, sehingga tidak ada lagi kehilangan alat, gangguan terhadap informasi, pencurian hak akses dan lain-lain yang sesuai dengan standardisasi ISO 27001 Klausal 9.

Untuk melengkapi simpulan, disampaikan saran guna pengembangan selanjutnya yang dapat dilakukan untuk mengoptimalkan peranan keamanan sumberdaya manusia diantaranya adalah :

1. Pengembangan selanjutnya dengan Klausal 12 pada ISO 27001.
2. Pengembangan selanjutnya dengan Klausal 9 pada ISO 27002.
3. Pengembangan selanjutnya diadakan audit internal pada sistem keamanan *hotspot*.

Daftar Pustaka

- [1] Sarno, Rianarto, 2009, *Sistem Manajemen Keamanan Informasi*, Media Nusantara, Surabaya.
- [2] Hasibuan, 2003, *Pengertian-Sumber-Daya-Manusia-Menurut*, (hlm 244) tersedia di <http://www.kumpulan.net/2016/12/pengertian-sumber-daya-manusia-menurut.html> (diunduh 22 September 2016)
- [3] Herrmann, D.S., 2002. “*Security Engineering and Information Assurance*”. Auerbach.
- [4] Kamat, M., 2012, ISO 27001 Security tersedia di: <http://www.ISO27001security.com> (diunduh 3 Juni 2015).
- [5] Wahidin. 2007, *Jaringan Komputer Untuk Orang Awam*,. Maxicom, Palembang.
- [6] Sofana, Iwan, 2011, *Teori & Modul Praktikum Jaringan Komputer*, Modula, Bandung.
- [7] Kusuma, Arbi, Riawan. 2014, *ISO 27001 Sistem Informasi Akademi*. Yogyakarta

- [8] Bulu, Hariawan, Nur, 2013, *Analisis Keamanan Jaringan STMIK AMIKOM Yogyakarta Berdasarkan ISO/IEC 27001:2005 Standar A.11.4.4*. STMIK AMIKOM Yogyakarta.
- [9] Ermana. Fine., et al. 2012. *Audit Keamanan Sistem Informasi Berdasarkan ISO 27001 pada BPR Jatim. Skripsi S1* pada STIKOM Surabaya;
- [10] Kamat, M., 2012, ISO 27001 Security tersedia di: <http://www.ISO27001 security.com> (diunduh 3 Juni 2015).