MENGUKUR INDEKS KEAMANAN INFORMASI DENGAN METODE *OCTAVE* BERSTANDAR ISO 27001 PADA UNIVERSITAS ALMUSLIM-BIREUEN

Zulkifli,M.Kom
Email : Zulladasicupak@gmail.com
Dosen Tetap Program studi Teknik Informatika Fakultas Ilmu Komputer Universitas Almuslim

ABSTRAK

Bagi sebuah Institusi Informasi merupakan aset yang maha penting,dan sangat diperlukan, keamanan dan perlindungan terhadap informasi merupakan hal yang mutlak yang harus diperhatikan secara sungguh-sungguh dan serius. Maka untuk mengantisipasi tingkat keamanan informasi, kami mencoba untuk mencari salah satu cara dalam rangka menggugah para pemakai informasi untuk dapat memperhatikan tingkat keamanan informasi pada sebuah institusi. Metode yang kami gunakan dalam penelitian ini adalah metode yang berstandar internasional yaitu OCTAVE berbasis ISO 27001. Sistem kerja yang dilakukan dengan metode ini, dimana dalam pengukuran tingkat keamanan informasi dengan menggunakan 6 variabel yaitu peran dan tingkat kepentingan TIK, tata kelola keamanan informasi, pengelolaan resiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan asset informasi dan teknologi keamanan informasi. Pengujian yang telah kami lakukan menunjukkan hasil bahwa tingkat kesiapan Universitas Almuslim dalam hal menjaga keamanan Informasi masih berada pada kondisi wilayah "Kerangka Kerja Dasar".

Kata kunci : Metode, *Dashboard Information System, keamanan informasi, Institusi Pendidikan Tinggi, Universitas Almuslim, OCTAVE, ISO 27001*

PENDAHULUAN

Informasi merupakan pengetahuan yang didapatkan dari pembelajaran, pengalaman atau instruksi.

Masalah keamanan sistem informasi tingkat kesadaran masih sangat rendah, padahal keamanan dan perlindungan terhadap berbagai hal tentang informasi merupakan hal yang mutlak yang diperlukan dan harus diperhatikan secara sungguh-sungguh dan serius bagi seluruh manajemen sebuah organisasi.

Saat ini Universitas Almuslim belum memberikan suatu perlindungan yang maksimal terhadap pengamanan informasinya, sehingga tingkat keamanan informasi pada Universitas Almuslim masih digolongkan dalam taraf biasa, belum dilakukan secara ketat dan permanen.

Metode *OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation)* adalah sebuah pendekatan terhadap evaluasi resiko keamanan informasi yang komprehensif, sistematik dan terarah.

Pada penelitian ini, penulis akan membuat *Dashboard Information System* untuk melakukan pengukuran indeks keamanan informasi pada institusi perguruan tinggi menggunakan metode *OCTAVE* berbasis ISO 27001. Untuk menampilkan hasil pengukuran digunakan model indeks keamanan informasi (KAMI) sesuai dengan Standar Nasional Indonesia (SNI) 27001 yang mengadopsi ISO 27001. Hasil dari evaluasi tersebut akan digunakan sebagai pertimbangan dalam membuat sistem kerangka kerja pengamanan informasi yang lebih baik.

Tujuan Penelitian

Untuk mengukur indeks keamanan informasi dan tingkat kesiapan suatu intitusi perguruan tinggi dalam menghadapi ancaman terhadap keamanan informasinya menggunakan metode OCTAVE berbasis ISO 27001.

Keamanan Informasi

Keamanan informasi bukan hanya berkaitan dengan aspek teknologi dan aspek sumber daya manusia saja tetapi juga terkait dengan berbagai aspek lain, seperti aspek manajemen termasuk kebijakan organisasi, sistem manajemen dan perilaku manusia.

Sebuah Universitas harus memperhatikan aspek-aspek keamanan informasi secara umum paling tidak memuat tiga unsur penting (sembiring & Lubis, 2012), yaitu: *Confidentiality (*kerahasiaan*), b. Integrity (*integrita*s, c. Availability (*ketersediaan*)*

Indeks keamanan informasi (KAMI)

Indeks Keamanan Informasi (KAMI) merupakan model pengukuran terhadap kesiapan atau kematangan suatu instansi dalam pengamanan informasi. KAMI juga dapat untuk mengidentifikasi kondisi saat ini, identifikasi keperluan pembenahan dan prioritasnya, pemetaan kesiapan atau kematangan instansi dalam pengamanan informasi.Indeks KAMI juga dapat dimanfaatkan untuk kelengkapan pengamanan informasi yang sesuai dengan kesiapan sertifikasi (ISO 27001 ISMS). Proses evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area sebagai berikut:

- Peran TIK dalam instansi
- Tata kelola keamanan informasi
- Pengelolaan risiko keamanan informasi
- Kerangka kerja keamanan informasi
- Pengelolaan aset informasi, dan

- Teknologi dan keamanan informasi

Adapun korelasi antara peran atau tingkat kepentingan TIK dalam instansi dapat dilihat pada Gambar berikut :

Peran TIK				
Rendah		Indeks (Skor Akhir)		Status Kelayan
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang		Skor Akhir		Status Kelayan
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		Skor Akhir		Status Kelayan
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik/Cukup
Kritis		Skor Akhir		Status Kelayan
37	48	0	333	Tidak Layak
		334	453	Perlu Perbaikan
		454	588	Baik/Cukup

Gambar 2. Skoring Peran dan Kepentingan TIK

Sumber: Sembiring& Lubis, 2014

OCTAVE *(The Operationally Critical Threat, Asset and Vulnerability Evaluation)*

The Operationally Critical Threat, Asset and Vulnerability Evaluation (*OCTAVE*) adalah metodologi mandiri yang memungkinkan pengguna untuk mendapatkan pengetahuan tentang masalah keamanan dan mengembangkan perbaikan posisi keamanan organisasi.Model ini menggabungkan sekelompok kriteria yang didalamnya terdapat prinsip-prinsip, atribut dan *output*.Yang dilakukan oleh karyawan di seluruh perusahaan dimana tingkat

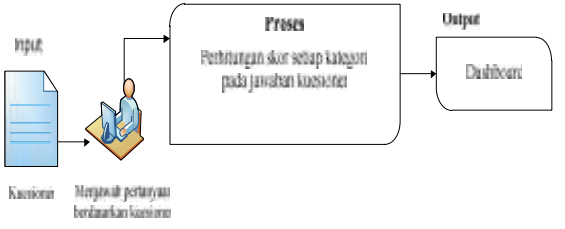
kepentingan untuk data perusahaan tertentu ditentukan dari ancaman terkait di dalamnya yang telah dinilai(Yadaf et al, 2013).

ANALISI DAN PERANCANGAN SISTEM

Arsitektur Umum

Ada beberapa tahapan metode penelitian yang digunakan dalam melakukan penelitian ini, antara lain : menjawab pertanyaan kuesioner, pertanyaan dibagi 6 bagian, dimana setiap bagian terdiri beberapa pertanyaan, dari jawaban pertanyaan tersebut, maka akan dihasilkan output berupa *dashboard*, skor, tingkat kematangan dan keterangan kelayakan sertifikasi.

Adapun arsitektur umum yang menggambarkan tahapan metode yang digunakan dalam penelitian ini dapat dilihat pada Gambar berikut :



Gambar 4. Arsitektur Umum

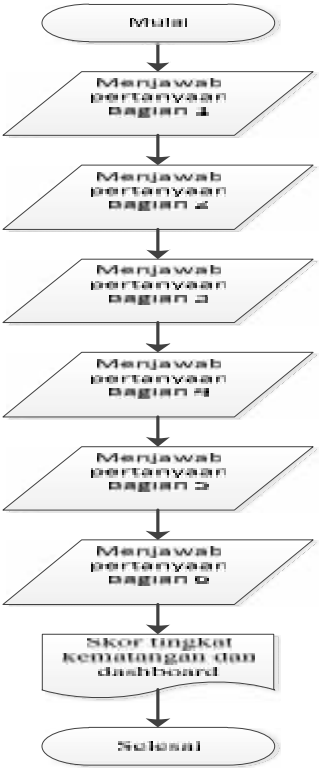
Analisis Masalah

Pengukuran indeks keamanan informasi diperlukan untuk mengetahui tingkat kematangan dan kesiapan suatu institusi pendidikan tinggi terhadap pengamanan informasi.

Oleh karena itu dibutuhkan aplikasi pengukuran indeks keamanan informasi yang dapat dijadikan sebagai *tools* untuk menilai tingkat kesiapan/kematangan Universitas Almuslim terhadap pengolahan pengamanan informasi.

Adapaun langkah-langkah yang dilakukan dalam aplikasi pengukuran indeks keamanan informasi ini adalah terlebih dahulu membuat akun, kemudian mengisi identitas *user* (responden) pada kolom-kolom yang terdapat pada halaman *sign up*.

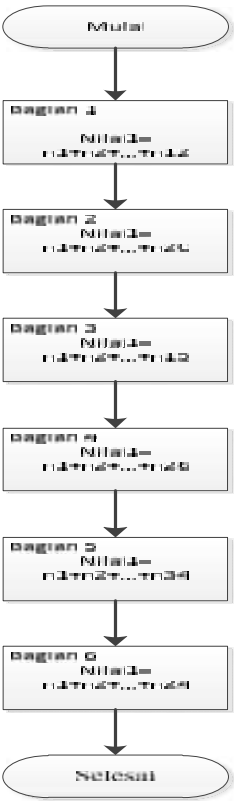
Proses sistem



Gambar 5. Proses Sistem

Setelah mempunyai akun maka lakukan *user login*. Jika *user* telah melakukan *login* maka *user* bisa menjawab pertanyaan-pertanyaan yang terdapat pada halaman *forms* yang terdiri dari 6 bagian.

Proses perhitungan skor



Gambar 6. Proses Perhitungan Skor

Pada proses perhitungan skor, dimana untuk mendapatkan nilai bagian 1, bagian 2, bagian 3, bagian 4, bagian 5 dan bagian 6, pertanyaan-pertanyaan yang telah dijawab oleh *user* memiliki bobot nilai yang berbeda berdasarkan kategori penerapan pertanyaannya yang akan dijumlahkan.

Penyusunan Instrumen

Berdasarkan hasil analisis tersebut Universitas Almuslim dalam mengukur resiko terhadap aset informasi menganalisis ancaman dan membangun strategi proteksi maka perlu dibentuk yang terdiri dari :

1. Dibentuk tim terdiri dari :

a. Dekan Fakultas di lingkup Universitas Almuslim

b. Bagian laboratorium Universitas Almuslim

c. Bagian server Universitas Almusim

2. Tim tersebut menganalisis terhadap :

a. Evaluasi resiko keamanan aset infromasi organisasi

b. Mengukur praktek organisasi

c. Menganalisis ancaman terhadap keamanan informasi

d. Membangun strategi proteksi

3. Berdasarkan hasil analisis itu maka digunakan seperangkat instrumen (kuesioner) untuk mendapatkan informasi yang berkaitan dengan hal tersebut.

Contoh Perhitungan Tingkat Kematangan

Tingkat kematangan hanya bernilai 1 sampai 9 dimana angka desimal dilambangkan seperti pada tabel 2.

Tabel 2. Tingkat kematangan

Nilai kematangan	Tingkat kematangan

1	I
2	I+
3	II
4	II+
5	III
6	III+
7	IV
8	IV+
9	V

Cara mendapatkan nilai kematangan ditentukan dari kategori tahap penerapan yang terkait. Setiap bagian pertanyaan memiliki kategori tahap penerapan yang berbeda. cara mendapatkan nilai kematangan ditentukan dari proses penjumlahan skor pertanyaan berdasarkan kategori penerapan dimulai dari kategori yang paling besar.

Kesimpulan

Kesimpulan yang dapat diambil dari sistem pengukuran keamanan informasi pada perguruan tinggi yang telah dibangun yaitu:

1 Pendekatan OCTAVE yang digunakan membangun instrumen untuk pengukuran indeks keamanan informasi pada perguruan tinggi dapat disesuaikan dengan instrument pada ISO 27001.

2 Dari hasil penelitian ini menunjukkan bahwa untuk melihat tingkat kematangan dan kesiapan institusi Universitas

Almuslim dalam proses ISO 27001, dapat digunakan sebagai *tools* (*self assessment*).

Saran

Adapun saran untuk penelitian selanjutnya antara lain:

Untuk lebih bagusnya sistem pengukuran keamanan Informasi dan kematangan institusi perlu dibuat sutu pengembangan sistem pengukuran secara *online.*

DAFTAR PUSTAKA

Few, S. 2005. Common PITFALLS in Dashboard Design.*Proclarity,* 2-4.

Fokuss.2013. Standarisasi Sistem Keamanan Manajemen Informasi. Jakarta.

Gui, A., Gondodiyoto, S. &Timotius,I. 2008. *Pengukuran Resiko Teknologi Informasi (TI) Dengan Metode OCTAVE-S*. Jurusan Komputerisasi Akuntansi, Fakultas Ilmu Komputer. Universitas Bina Nusantara.

Henderi, Rahayu S, &Prasetyo.B.M. 2012.*Dashboard Information System Berbasis Key Performance Indicator.*Seminar Nasional Informatika : 1-6.

Harahap, R.M. 2011. Information Technology Risk Measurment: Octave-S Method.*CommIT.* 1: 27-29.