PENILAIAN KEAMANAN SISTEM INFORMASI AKADEMIK UNIVERISITAS MUHAMMADIYAH SUKABUMI DENGAN MENGGUNAKAN ISO 27001

Asriyanik[1]
[1]*Program Studi Teknik Informatika UMMI*
asriyanik@gmail.com

PENDAHULUAN

Latar Belakang Masalah

Sistem informasi akademik adalah bagian yang penting dalam perguruan tinggi. Proses pengolahan data dalam sistem informasi akademik meliputi data akademik yang terdiri dari data mahasiswa, dosen, perkuliahan dan berbagai data lainnya yang terkait dengan data akademik. Proses pengolahan data akademik harus berjalan dengan baik, terintegrasi, cepat, akurat dan aman karena data dan proses dalam bidang akademik merupakan data yang penting dan diakses oleh berbagai pengguna. Universitas Muhammadiyah Sukabumi (UMMI) berdiri pada tahun 2003, dengan jumlah awal mahasiswa sebanyak 350 orang dari 11 program studi. Sejak awal berdiri UMMI telah mulai membangun sistem informasi akademik, pada waktu itu UMMI membuat sistem informasi akademik baru pada tahap pengolahan data perkuliahan yaitu proses pengolahan data nilai dan pembayaran mahasiswa yang menggunakan Ms Access.

Seiring dengan berjalannya waktu, jumlah mahasiswa UMMI semakin bertambah, sehingga proses pengolahan data melalui Ms. Access banyak mengalami kendala, terutama karena sistem yang tidak *online*. Oleh karena itu pada tahun 2012, UMMI mulai membangun sistem informasi akademik yang berbasis web sehingga sistem informasi akademik berjalan secara online. Pada awal tahun 2013 UMMI telah mulai mensosialisasikan sistem informasi akademik online. Komponen sistem informasi akademik yang dibangun meliputi sistem pengisian KRS, pembimbingan mahasiswa, pengisian nilai, sistem keuangan mahasiswa, sistem penerimaan mahasiswa baru dan sistem administrasi fakultas.
Dengan adanya sistem informasi akademik yang berbasis online, maka sistem terbuka ke semua pihak. Hal ini membuat sistem akan lebih rentan, karena peluang terjadinya serangan lebih besar, oleh karena itu diperlukan adanya sebuah sistem keamanan yang baik. Konsep keamanan harus memenuhi minimalnya tiga aspek yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Untuk membangun sistem keamanan pada sistem informasi akademik maka perlu dilakukan sistem manajemen keamanan agar sistem keamanan yang terbentuk sesuai dengan kebutuhan. Salah satu standar yang digunakan untuk membangun sistem manajemen keamanan informasi adalah menggunakan standar seri ISO 27000, yang memiliki beberapa standar yang berkaitan dengan keamanan informasi. Selain standar ISO, terdapat juga standar lain yang dikeluarkan oleh beberapa organisasi seperti NIST dan COBIT. Namun standar ISO ini adalah salah satu standar yang telah diakui oleh pemerintah Indonesia dan juga sebagian telah masuk pada peraturan pemerintah dalam tata kelola keamanan informasi untuk organisasi publik.

Untuk membangun manajemen keamanan informasi yang baik pada sistem informasi akademik, maka terlebih dahulu perlu dilakukan penilaian keamanan terhadap sistem informasi akademik yang ada sekarang, sehingga dapat dibangun sebuah sistem keamanan yang baru yang lebih sesuai. Oleh karena itu maka dibuat penelitian yang berjudul penilaian keamanan sistem informasi akademik dengan mengggunakan ISO 27001 (Studi Kasus pada Universitas Muhammadiyah Sukabumi).

Rumusan Masalah

Berdasar pada uraian di atas, maka dirumuskan sebuah masalah yaitu bagaimana melakukan proses penilaian keamanan sistem informasi akademik sehingga dapat menjadi tolok ukur dalam menentukan model keamanan sistem informasi yang harus diterapkan.

Batasan Penelitian

Penelitian ini akan dibatasi pada penilaian keamanan sistem informasi akademik berdasarkan aset perangkat lunak pada sistem informasi akademik UMMI.

TINJAUAN PUSTAKA

Sistem Informasi

Beberapa pengertian sistem informasi menurut para pakar adalah:

1. Tata Sutabri (2012) dalam bukunya yang berjudul Konsep Sistem Informasi mengungkapkan bahwa sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang bersifat manajerial dengan kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan-laporan yang ditentukan.

2. Menurut Laudon (2012:16) sistem informasi adalah komponen-komponen yang saling berkaitan yang bekerja bersama-sama untuk mengumpulkan, mengolah, menyimpan, dan menampilkan informasi untuk mendukung pengambilan keputusan, koordinasi, pengaturan, analisa, dan visualisasi pada sebuah organisasi.
3. Menurut Whitten, Bentley, dan Ditman (2009:10) sistem informasi adalah pengaturan orang, data, proses, dan informasi (TI) atau teknologi informasi yang berinteraksi untuk mengumpulkan, memproses, menyimpan, dan menyediakan sebagai output informasi yang diperlukan untuk mendukung sebuah intansi atau organisasi.
4. Menurut O'Brien (2014:34) mengatakan bahwa komponen Sistem Informasi terbagi atas beberapa hal, yaitu:
   a. Sumber daya data (sebagai data dan pengetahuan).
   b. Sumber daya Manusia (sebagai pemakai akhir dan ahli SI).
   c. Sumber daya software (sebagai program dan prosedur).
   d. Sumber daya hardware (mesin dan media).
   e. Sumber daya jaringan (sebagai media komunikasi dan dukungan jaringan).
5. Menurut Ladjamudin (2013), sistem Informasi dapat didefinisikan sebagai berikut :
   a. Suatu sistem yang dibuat oleh manusia yang terdiri dari komponen-komponen dalam organisasi untuk mencapai suatu tujuan yaitu menyajikan informasi.
   b. Sekumpulan prosedur organisasi yang pada saat dilakasanakan akan memberikan informasi bagi pengambilan keputusan dan/atau untuk mengendalikan organisasi.
   c. Suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi, mendukung operasi, bersifat manajerial, dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan.

Berdasarkan latar belakang di atas, maka dapat disimpulkan sistem informasi adalah kumpulan dari perangkat keras, perangkat lunak, sumber daya manusia, dan komponen lainnya yang saling bekerjasama untuk melakukan tujuan organisasi dengan menggunakan bantuan teknologi komputer.

Sistem Informasi Akademik

Sistem informasi akademik merupakan sistem informasi yang mengolah data akademik. Biasanya modul sistem informasi akademik disesuaikan dengan kebutuhan pengolahan data dari Direktoral Jendral Pendidikan Tinggi (DIKTI). Beberapa modul yang biasa ada dalam sistem informasi akademik adalah:

1. Modul administrasi akademik
   - Manajemen data master seperti data dosen, jurusan, fakultas, mata kuliah, jadwal kuliah, dll
   - Menajemen pelaporan, seperti pelaporan data mahasiswa, data dosen, data kurikulum data alumni, daftar hadir, dll
   - Menajemen konversi/ import data
   - Manajemen pengguna
2. Modul penerimaan mahasiswa baru
   Meliputi informasi pendaftaran, data pendaftar, cara mendaftar, dan pendaftaran online
3. Modul mahasiswa
   Meliputi pengisian KRS online, pengecekan nilai dan proses pembimbingan akademik
4. Modul Dosen
   Meliputi data mahasiswa bimbingan, penilaian, daftar hadir, dll
5. Modul keuangan mahasiswa
   Meliputi informasi data keuangan SPP, DPP, praktikum, dll
   (Sutabri, 2012)

Keamanan Informasi

Berdasar pada ISO/IEC 17799:2005 tentang *information security management system*, keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis. Keamanan Informasi memiliki 3 aspek, diantaranya adalah:

1. Kerahasiaan (*Confidentiality)*

Dengan adanyan keamanan informasi maka harus dapat menjamin bahwa data bersifat rahasia, maksudnya hanya dapat diakses oleh pihak yang berhak.

2. Keutuhan (*Integrity)*

Maksudnya, dengan adanya keamanan informasi dapat menjamin bahwa data tetap utuh dan lengkap, menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya.

3. Ketersediaan (*Availability)*

Maksudnya adalah dengan adanya keamanan informasi menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan.

Tiga aspek keamanan informasi tersebut biasa disingkat dengan istilah CIA (*Confidentiality*, *Integrity*, *Availability*) yang merupakan aspek dasar yang harus dipenuhi dari konsep keamanan informasi. Dalam membuat sistem keamanan informasi.

Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (*plan*), mengimplementasi (do), memonitor dan meninjau ulang (check) serta memelihara dan meningkatkan atau mengembangkan (*act*) terhadap Keamanan Informasi perusahaan [ISO/IEC 27001, 2005]. Tujuan dibangun dan diterapkannya SMKI adalah untuk menjaga aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) dari informasi.

International Standard Organization (ISO) mengelompokkan standar Keamanan Informasi ke dalam serial ISO/IEC 27000, yaitu:

1. ISO 27000: Dokumen yang berisi definisi-definisi Keamanan Informasi yang digunakan sebagai istilah dasar dalam serial ISO/IEC 27000.
2. ISO 27001: Dokumen yang menjelaskan persyaratan standar yang harus dipenuhi untuk membangun SMKI.
3. ISO 27002: Dokumen yang berisi panduan praktis (*code of practice*) teknik Keamanan Informasi.
4. ISO 27003: Dokumen yang berisi panduan implementasi SMKI
5. ISO 27004: Dokumen yang berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.
6. ISO 27005: Dokumen panduan pelaksanaan manajemen risiko.
7. ISO 27006 : Dokumen panduan untuk sertifikasi SMKI perusahaan.
8. ISO 27007: dokumen panduan audit SMKI perusahaan

(Sarno dan Isyat Iffano, 2009)

Manajemen Risiko

Risiko adalah peluang terjadinya sesuatu yang dapat mengakibatkan terganggunya proses bisnis atau memberikan dampak sehingga tujuan organisasi terganggu. Manajemen risiko adalah proses untuk mengidentifikasi risiko, menganalisis risiko serta melakukan penanganan untuk mengurangi risiko sampai dampaknya dapat diterima terhadap keberlangsungan proses bisnis. Kegiatan manajemen risiko meliputi:

1. Mengidentifikasi informasi/ aset, yaitu melakukan pengelompokkan aset ke dalam beberapa kategori atau golongan.
2. Mengidentifikasi ancaman (*threat*)
   Ancaman (*threat*) adalah suatu potensi yang disebabkan oleh insiden yang mungkin membahayakan jalannya proses bisnis organisasi. Tujuan melakukan identifikasi ancaman adalah agar diketahui ancaman yang mungkin terjadi.
3. Mengidentifikasi kelemahan (*vulnerability*)
   Kerentanan/ kelemahan (*vulnerability*) adalah kekurangan yang ada pada sistem yang dapat menjadi celah terjadinya ancaman. Tujuan melakukan identifikasi kelemahan adalah agar dapat memahami kelemahan yang dimiliki oleh sistem/ organisasi.
4. Menentukan kemungkinan ancaman (*probability*)
   Tahapan ini bertujuan untuk mengetahui kemungkinan ancaman yang terjadi sesuai dengan identifikasi ancaman yang telah didefinisikan.
5. Analisis Dampak (*Impact Analysis*)
   Tahapan ini adalah kegiatan untuk mementukan sebesara besar pengaruh suatu risiko yang diakibatkan oleh kelemahan atau ancaman terhadap proses bisnis suatu organisasi.
6. Penilaian risiko (*risk assessment*)
   Penilaian risiko dilakukan untuk memberikan gambaran dari seberapa besar akibat yang akan diterima organisasi jika ancaman yang menyebabkan kegagalan bisnis terjadi. Cara melakukan penilaian risiko terdapat dua metode, yaitu:
   a. Metode kualitatif
      Dilakukan dengan melakukan perkiraan terhadap biaya yang akan ditanggung oleh suatu organisasi akibat dari risiko yang diterima. Biasanya dibuat terlebih dahulu patokannya. Nilai risiko biasanya berupa pilihan: risiko rendah, risiko medium, risiko tinggi
   b. Metode kuantitatif
      Untuk metode kuantitatif dilakukan penilaian dengan rumus matematis yaitu:
      Nilai risiko = Nilai aset x analisis dampak bisnis x nilai ancaman

METODE PENELITIAN

Tahapan – tahapan penelitian

Tahapan penelitian yang dilakukan pada penelitian ini yaitu:

1. Studi pendahuluan
   Pada tahap studi pendahuluan dilakukan pengenalan terhadap lingkungan organisasi dan sistem informasi akademik yang ada di UMMI untuk dapat menentukan dengan lebih baik tentang permasalahan dan solusi yang dibutuhkan.
2. Melakukan penilaian risiko dengan tahapan berikut:
   a. Mengidentifikasi aset pada sistem informasi akademik UMMI
   b. Mengidentifikasi ancaman yang mungkin terjadi pada sistem informasi akademik UMMI

c. Mengidentifikasi *exsisting control*
d. Mengidentifikasi kelemahan pada sistem informasi akademik UMMI
e. Mengindentifikasi dampak yang terjadi saat ancaman terjadi
f. Melakukan penilaian risiko

3. Membuat keluaran dari proses penilaian risiko yaitu berupa: inventarisasi aset, daftar ancaman, daftar kelemahan, nilai kemungkinan ancaman, nilai dampak, risiko dan level risiko
4. Membuat pelaporan

Lokasi Penelitian

Lokasi penelitian ini dilakukan di Universitas Muhammadiya Sukabumi (UMMI) yang terletak di Jl. R. Syamsudin, S.H. No. 50 Kota Sukabumi – Jawa Barat. Objek penelitian yang diteliti adalah perangkat lunak yang terlibat dalam sistem informasi akademik UMMI.

Data yang diamati

Pada penelitian ini objek penelitian dibatasi pada perangkat lunak pada sistem informasi akademik, adapun data yang diamati adalah:

1. Basis Data yang ada pada sistem informasi akademik
2. Aplikasi/ bagian sistem informasi akademik
3. Sistem operasi
4. Dan perangkat lunak lainnya yang terlibat

Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan metode berikut:

1. Wawancara
   Wawancara dilakukan untuk mengetahui secara langsung tentang sistem informasi akademik dari pengelola sistem dan pengguna sistem. Dalam hal ini pengelola sistem yang diwawancarai adalah kepala bagian SIM beserta dua stafnya dan perwakilan pengguna dari mahasiswa, dosen dan staf.
2. Observasi
   Observasi dilakukan dengan melihat secara detail isi dari sistem informasi akademik di UMMI dan mencoba secara langsung setiap proses bisnis yang ada.

PEMBAHASAN

Untuk penilaian risiko yang ada pada sistem informasi akademik dilakukan dengan matriks penilaian risiko yaitu sebagai berikut:

		Likelyhood Of Incident Scenario/Threat				
		Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Business Impact	Severe (5)	5	10	15	20	25
	Major (4)	4	8	12	16	20
	Moderate (3)	3	6	9	12	15
	Minor (2)	2	4	6	8	10
	Insignificant (1)	1	2	3	4	5

Keterangan Warna :

: Risiko Ekstrim (*Critical / Very High*)
: Risiko Tinggi (*High*)
: Risiko Moderat (*Medium / Moderate*)
: Risiko Rendah (*Very Low*)

Gambar 1. Matriks Penilaian Risiko

Berdasar pada nilai aset, ancaman dan kerentanan, maka nilai risiko dari aset perangkat lunak SIAK UMMI adalah:

Tabel 1. Penilaian risiko

No	Aset	Jenis Ancaman	Kelemahan (Vulnerability)	LOIS	BIA	RV	Risk Level
	Aplikasi SIAK			2	3	6	Moderate
1		Site Scraping (Site Reconnaissance)	Tidak adanya perlindungan terhadap file atau data pada suatu halaman web, mengakibatkan user yang tidak berwenang dapat mendownload beberapa atau keseluruhan source, konten atau data-data yang terkandung di situs secara langsung di internet.				
2		Brute Force Login	Tidak adanya batasan ketika user gagal melakukan login	2	4	8	High
3		Cross Site Scripting (XSS)	Kurangnya pemeriksaan atau pengujian (testing) terhadap aplikasi ketika selesai dibangun	2	4	8	High
4		Dictionary Password Attack	Tidak adanya batasan ketika user gagal melakukan login	2	4	8	High
5		Guessing Password Attack	Password yang digunakan oleh user terlalu mudah untuk ditebak	2	4	8	High
6		Kesalahan penggunaan perangkat Lunak	Antar muka perangkat lunak yang rumit. Kurangnya dokumentasi mengenai penggunaan perangkat lunak Spesifikasi pengembangan perangkat lunak yang tidak jelas atau tidak lengkap	3	4	12	High
7		Pelanggaran pemeliharaan sistem informasi	Tidak adanya pengawasan terhadap user yang menggunakan komputer	3	3	9	High
8		Penyalahgunaan hak akses	Tidak adanya pencatatan log aktivitas administrator atau operator	4	4	16	Critical
9		SQL Injection	Aplikasi menerima seluruh karakter yang diinputkan oleh user	2	4	8	High
10		Penyalahgunaan Fungsi Aplikasi	Tidak adanya pencatatan log aktivitas administrator atau operator	4	4	16	Critical
11		Software error	Tidak ada atau tidak cukupnya pengujian perangkat lunak	2	5	10	Critical

Keterangan:
LOIS = Likely of Insiden
BIA = Bussiness Impact Analysis
RV = Risk Value

KESIMPULAN DAN SARAN

KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa pada sistem informasi akademik UMMI jika dilihat dari aplikasinya, maka terdapat 11 jenis ancaman yang mungkin terjadi dengan berbagai nilai risiko terhadap sistem. Nilai risiko paling tinggi disebabkan oleh penyalagunaan hak akses, penyalahgunaan fungsi aplikasi dan aplikasi yang error.

SARAN

Berdasarkan hasil penelitian ini dapat dilanjutkan untuk penganalisisan nilai risiko dari jenis aset yang lainnya sehingga didapatkan penilaian yang lebih lengkap mengenai keamanan sistem informasi pada Sistem Informasi Akademik (SIAK) UMMI

DAFTAR PUSTAKA

ISO/ IEC. (2008). *Information Security Risk Management.* USA: ISO.

James A. OBrien, G. M. (2014). *Sistem Informasi Manajemen (Management Information Systems) 2, E9.* Jakarta: Salemba Empat.

Jeffrey L. Whitten, L. D. (2007). *Systems analysis & design methodsJeffrey L. Whitten, Lonnie D. Bentley.* NewYork: McGraw-Hill/Irwin.

Ladjamudin, A.-B. B. (2013). *Analisis dan Desain Sistem Informasi.* Yogyakarta: Graha Ilmu.

Laudon, K. C. (2012). *sistem informasi manajemen mengelola perusahaan digital edisi 13.* Jakarta: Salemba Empat.

Sarno, R., & Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi.* Surabaya: ITS Press.

Sutabri, T. (2012). *Analisis Sistem Informasi.* Yogyakarta: Andi.

UMMI, T. S. (2012). *Manual Mutu SIAK UMMI.* Sukabumi: UMMI Press.