Jurnal Informatika – COMPUTING Volume 06 Nomor 02, Desember 2019: 37-41
ISSN: 2656 – 3861

PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN STANDAR SNI ISO/IEC 27001: 2013

Dadan Rahmat, ST., MT[1]

1. Dosen Pendidikan Teknologi Informasi, FKIP Universitas Muhammadiyah Sukabumi

ABSTRACT

This study discusses the planning of the Information Security Management System (ISMS) using SNI ISO / IEC 27001: 2013 standards at Muhammadiyah University, Sukabumi. Using descriptive qualitative research methods, and data collected through survey and interview methods. The results obtained are the planning of the ISMS using the ISO / IEC 27001: 2013 standard at the Muhammadiyah University of Sukabumi, as follows: Designing document 1 that contains the policy, published, scope, and Statement of Applicability (SOA) to cope with reports on external expenditure; and provide document 2 that contains information security procedures using the Plan-Do-Check-Act (PDCA) model.

Key Word: *Information Security Management System, SNI ISO / IEC 27001: 2013 standards.*

ABSTRAK

Penelitian ini bertujuan untuk mengetahui Perencanaan Sistem Manajemen Keamanan Informasi (SMKI) menggunakan Standar SNI ISO/IEC 27001:2013 di Universitas Muhammadiyah Sukabumi. Menggunakan metode penelitian deskriptif kualitatif, dan data dikumpulkan melalui metode survey dan wawancara. Hasil yang diperoleh yaitu perencanaan SMKI menggunakan standar SNI ISO/IEC 27001:2013 di Universitas Muhammadiyah Sukabumi, sebagai berikut: Merancang dokumen 1 yang meliputi kebijakan, penilaian risiko, ruang lingkup, dan *Statement Of Applicability* (SOA) untuk menanggulangi insiden pihak luar; dan merancang dokumen 2 yang berisi prosedur keamanan informasi dengan menggunakan model *Plan-Do-Check-Act* (PDCA).

Kata Kunci: Sistem Manajemen Keamanan Informasi, Standar SNI ISO/IEC 27001:2013

I. PENDAHULUAN

Latar Belakang

Universitas Muhammadiyah Sukabumi (UMMI) merupakan salah satu Perguruan Tinggi Swasta (PTS) yang berada di Kota Sukabumi, menyediakan pelayanan ke masyarakat khususnya mahasiswa menggunakan pelayanan berupa fasilitas Teknologi Informasi dan Komunikasi untuk pelayanan akademik dengan menggunakan Sistem Informasi Akademik (SIAK), *Electronic Library* (*E-Library*), *Open Journal System* (OJS) dan Open Public Acces Catalog (OPAC) katalog yang dapat diakses oleh mahasiswa dan dosen (di perpustakaan). Seluruh sistem informasi tersebut berbasis *website* yang dapat diakses dimana saja, kapan saja secara *realtime*, dan dapat digunakan bersama-sama. Sebagai sebuah sistem informasi SIAK, *E-library*, OJS, dan OPAC dapat melakukan proses pengelolaan, pengendalian, pengolahan, pencarian, penyimpanan, pemeliharaan, penghapusan, dan pembagian data serta informasi.

Penggunaan teknologi informasi tersebut tentunya haruslah didukung oleh keamanan informasi yang baik sehingga aspek *confidentiality*, *integrity*, dan *availability* bisa terjaga. Untuk menjaga hal-hal tersebut diperlukan sebuah prosedur yang mengaturnya. SMKI merupakan proses yang disusun berdasarkan *plan* (perencanaan), *do* (implementasi), *check* (evaluasi), dan *act* (meningkatkan) terhadap keamanan informasi perusahaan. Dengan dibangunnya SMKI, diharapkan UMMI dapat mengurangi dampak insiden TI, melindungi proses bisnis, menghindari kegagalan serius, serta dapat mengelola dan meminimalkan risiko keamanan informasi.

SMKI digunakan untuk meminimalisir ancaman terhadap keamanan informasi. Pentingnya implementasi SMKI dalam suatu institusi untuk dipahami, diupayakan, dan dicoba supaya pengelolaan informasi dilaksanakan dengan benar, sehingga lebih fokus mencapai visi yang telah ditetapkan dan dalam memberikan layanan terbaik bagi penggunanya. Tahapan dalam merencanakan SMKI yaitu menentukan: ruang lingkup, kebijakan, cara penilaian risiko, identifikasi risiko, analisa risiko, evaluasi risiko, evaluasi

pilihan penanganan risiko, dan memilih objek kontrol.

Pada dasarnya, suatu instansi dapat memilih standar yang akan digunakan dalam rangka menunjang SMKI, salah satunya mengadopsi standar dari *International Organization for Standardization* (ISO) / *International Electrotechnical Commission* (IEC) 27001: 2013 yang memiliki sifat kontrol secara spesifik. Perancangan SMKI pada penelitian ini mengacu kepada standar SNI ISO/IEC 27001:2013, menggunakan dokumen tingkat 1 kebijakan, penilaian risiko, ruang lingkup, dan *Statement Of Applicability* (SOA) dan dokumen tingkat 2 yang berisi prosedur keamanan informasi.

Menurut Sarno dan Iffano (2009), SNI ISO/IEC 27001 merupakan standar internasional yang fleksibel karena pengembangannya tergantung pada kebutuhan, tujuan, dan persyaratan keamanan organisasi, serta menyediakan sertifikat implementasi SMKI yang diakui secara nasional dan internasional yang disebut *Information Security Management System* (ISMS). Tiga unsur utama dalam konteks keamanan informasi yang harus dilindungi menurut SNI ISO/IEC 27001:2013 yaitu, kerahasiaan (menjamin kerahasiaan data dan informasi), keutuhan (menjamin data dan informasi utuh), dan ketersediaan (menjamin data dan informasi selalu tersedia). SMKI yang menggunakan standar SNI ISO/IEC 27001: 2013 dapat diterapkan pada sebuah organisasi, perusahaan, instansi pemerintahan, dan institusi pendidikan yang menyelenggarakan TIK. Demikian pentingnya SMKI ini sehingga Kominfo menerbitkan Peraturan Menteri Kominfo No. 4 Tahun 2016. Bab III tentang SMKI Pasal 7. Berdasarkan hasil wawancara awal dengan Kepala Sistem Informasi Manajemen UMMI didapatkan informasi, sebagai berikut:

1. *E-Library* dan OJS yang berbasis web memiliki celah kebocoran yang menyebabkan sering terjadinya *deface web* terhadap kedua sistem informasi tersebut.
2. UMMI belum menggunakan standardisasi SNI ISO/IEC 27001:2013.
3. UMMI belum memiliki dokumen *blueprint* manajemen keamanan informasi serta tata kelola teknologi informasi, sehingga perencanaan keamanan dan tata kelola informasi tidak terarah.

Dari hasil wawancara diatas, bahwa UMMI belum memiliki blueprint manajemen keamanan informasi yang berbasis standar SNI ISO/IEC 27001:2013, selain itu didapatkan juga informasi bahwa telah terjadi beberapa kali insiden *deface web* dan berhasil menembus keamanan *E-Library* dan OJS yang dimiliki UMMI. Hal ini tentu saja menimbulkan kerugian bagi UMMI dan dikhawatirkan akan mengganggu kerahasiaan *(confidentiality)*, keutuhan *(integrity)*, dan ketersediaannya *(availability)* data dan informasi.

Berdasarkan kondisi real permasalahan TIK di UMMI langkah pertama adalah merancang perencanaan SMKI SNI ISO/IEC 27001:2013, mengimplementasikan dan mengukur keefektifan implementasi SNI ISO/IEC 27001:2013 di UMMI. Sesuai dengan hasil observasi dan wawancara dengan Kepala Sistem Informasi Manajemen, UMMI memiliki rencana di tahun 2017 untuk membuat *blueprint* SMKI yang menggunakan standar SNI ISO/IEC 27001:2013, maka dari itu demi berjalannya rencana tersebut perlu dilakukan sebuah penelitian tentang perencanaan SMKI menggunakan SNI ISO/IEC 27001:2013 yang bertujuan untuk menghasilkan *blueprint*, prosedur, dan kebijakan yang berkaitan dengan SMKI, dalam mencegah dan menanggulangi ancaman, risiko, dan serangan yang akan mengganggu kerahasiaan, merusak keutuhan, dan mengganggu ketersediaan data dan informasi yang dimiliki UMMI.

Tujuan dari penelitian ini yaitu untuk mengetahui perencanaan SMKI menggunakan standar SNI ISO/IEC 27001:2013 di UMMI.

II. METODOLOGI

Penelitian ini deskriptif kualitatif. Pengumpulan data melalui observasi dan wawancara.

III. HASIL DAN PEMBAHASAN

a. Bagian Sistem Informasi Manajemen (SIM)

SIM adalah bagian pelaksana teknis di bidang pengolahan data, berada di bawah tanggung jawab biro administrasi umum, keuangan dan SDM. SIM dipimpin oleh seorang kepala yang diangkat diantara tenaga akademik atau tenaga ahli komputer ataupun ahli teknologi informasi yang ada di lingkungan UMMI. SIM mempunyai tugas mengumpulkan, mengolah, menyajikan, dan menyimpan data informasi serta memberikan pelayanan dalam bidang pendidikan, penelitian, pengabdian kepada masyarakat, pelatihan dan kerjasama.

b. Penentuan Ruang Lingkup

Universitas Muhammadiyah berkomitmen untuk mengelola, menjaga dan melindungi aset perangkat TI yang merupakan bagian dari proses sistem informasi dari berbagai insiden maupun ancaman yang mungkin terjadi. Universitas Muhammadiyah menyetujui untuk membangun SMKI berbasis Manajemen Risiko dengan mengacu kepada standar S N I ISO/IEC 27001 dan S N I ISO/IEC 27005. Adapun ruang lingkup perancangan SMKI mencakup pengelolaan keamanan aset dan Infrastruktur Teknologi Informasi yang terdiri dari :

a. Data dan Dokumen
   Meliputi data atau file penting yang tersimpan di komputer dan basis data, maupun berkas fisik lainnya yang terdokumentasi secara *real*.
b. Perangkat keras (*Hardware*) dan Jaringan
   Meliputi perangkat komputer, perangkat jaringan dan komunikasi, dan perangkat pendukung lainnya.
c. Perangkat lunak (*Software*)
   Meliputi perangkat sistem operasi, perangkat lunak sistem aplikasi dan basis data serta perangkat bantu pengembangan sistem.
d. Sumber daya manusia
   Meliputi personil (karyawan) perusahaan, pihak mitra ketiga dan pihak umum yang menjadi user pengguna aplikasi.

Aset informasi pada Universitas Muhammadiyah Sukabumi meliputi: Organisasi dan lokasi, Asset (data dan informasi, *software*, *hardware*, perangkat jaringan dan komunikasi, fasilitas pendukung, dan sumber daya manusia).

Kebijakan pengendalian hak akses meliputi: akses *logic* dan fisik terhadap informasi dan fasilitas sistem informasi yang dikelola UMMI dalam menyelenggarakan pendidikan dan pengaksesan melalui media teknologi informasi dan sistem informasi.

Proses manajemen risiko yang akan diberlakukan secara berkelanjutan menggunakan siklus *Plan-Do-Check-Act* (PDCA) pada SNI ISO/IEC 27001, yaitu: .
***Plan** (Establish the Management System), **Do** (Implement and Operate the Management System), **Check** (Monitor and Review the Manajemen System),* dan ***Act** (Maintain and Improve the Management System).*

c. Penilaian Risiko

Penilaian risiko *(risk assesment)* merupakan langkah dari proses manajemen risiko dengan bertujuan untuk mengetahui ancaman *(threat)* dari luar yang berpotensi mengganggu keamanan informasi pada Universitas dan potensial kelemahan *(vulnerability)*.

Nilai dari masing-masing aset yang diperoleh dari hasil wawancara dan observasi, disajikan pada tabel berikut.

Tabel 1. Kategori Aset

No.	Kategori Aset	Nama Aset
1	Informasi	• Data akademik • Topologi jaringan • Platform *hardware* & *software* • Aplikasi • Data karyawan & dosen • SDM
2	Layanan dan aplikasi	• *Internet* (Asti Net) • Sistem informasi akademik • Server *(Mail, Web, Elearning, Database*, DNS, *Proxy*, *Firewall*, *RADIUS*, FTP, *Repository*) • PHP, Mysql • Sistem Operasi (*Linux*, *Free* BSD, *Windows*)
3	Sumber Daya Manusia (SDM)	• Rektor • Dekan • Direktur • Kepala Program Studi • Kepala Bagian • Dosen • Karyawan • *Programmer* • *Network Administrator* • Pengembang • *Maintenance*

Tabel 2. Nilai Aset

No	Aset	Kriteria			Nilai Aset $\frac{(NC+NI+NV)}{3}$
		NC	NI	NV	
1	*Server*	1	3	3	2,3
2	*Software*	1	1	1	1
3	*Hardware*	1	1	1	1
4	Jaringan	1	1	1	1
5	Data Akademik	2		1	1,3
6	Sistem Informasi Akademik	1	1	1	1
7	SDM	2	1	1	1,3
8	Aplikasi	1	3	3	2,3
9	Data Karyawan dan Dosen	2	1	1	1,3

Berdasarkan dari tabel diatas dapat disimpulkan bahwa semua aset memerlukan perlindungan menyeluruh. Akan tetapi, kebutuhan keamanan yang paling dominan terdapat pada aset *server*, aset jaringan, dan sistem akademik dengan skor nilai aset (NA) 3 paling tinggi, sehingga harus dijamin aspek keamanan informasi yang meliputi kerahasiaan, keutuhan, dan ketersediaan.

d. Identifikasi Risiko

Tabel 3. Identifikasi Risiko

No.	Kejadian	Jenis	Probabilitas	Rata-rata Probabilitas
1	Gangguan Sumber Daya	*Vulnerable*	*Low*	0,1
2	Gangguan *Hardware*	*Vulnerable*	*Medium*	0,4
3	Gangguan *Software*	*Vulnerable*	*Medium*	0,4
4	*Virus Attack*	*Threat*	*High*	0,7
5	*Hacker*	*Threat*	*Medium*	0,4
6	Akses illegal	*Threat*	*Medium*	0,4
7	*Fault logging*	*Threat*	*Medium*	0,4
Jumlah Ancaman		7	Jumlah Rata-rata Probabilitas	2,8

Berdasarkan hasil dari perhitungan nilai ancaman diperoleh nilai rerata probabilitas yaitu 0,4 yang diklasifikasikan dengan nilai Medium.

Universitas Muhammadiyah Sukabumi belum menyusun kebijakan keamanan informasi sehingga diperlukannya perencanaan *security policy*. Selain itu, pada *organizational security* belum ada kerjasama terhadap pihak ketiga. Pada *Physical Environmental Security* belum diterapkan otorisasi manajemen tertulis untuk membawa peralatan, data, atau *software* ke luar lokasi. Sedangkan pada *Communication* and *Operations Management* belum menerapkan prosedur untuk merekam *Logging Fault* yang dilaporkan oleh *user* tentang masalah yang mereka temukan pada komputer atau sistem komunikasi. Pada *access control* belum ada *manajemen password* resmi untuk mengontrol *password* yang bisa mengancam kerahasiaan informasi. Selain itu belum disusun kebijakan mengenai *mobile computing* dan *teleworking*. Pada *system development* dan *maintenance* belum tersedia kontrol modifikasi *software* dari pihak *vendor* dan terbukanya jalur gelap *(convert channel)*. Dari masing-masing *assessment checklist* yang diperoleh maka diperlukan manajemen keamanan informasi dan penentuan kontrol akses yang tepat guna menunjang pencapaian tujuan yang telah ditetapkan oleh Universitas Muhammadiyah Sukabumi.

Berdasarkan hasil observasi didapat bahwa semua aset memerlukan perlindungan menyeluruh. Akan tetapi, kebutuhan keamanan yang paling dominan terdapat pada aset *server*, aset jaringan, dan sistem akademik yang mengharuskan adanya jaminan untuk aspek keamanan informasi.

IV. KESIMPULAN DAN SARAN

KESIMPULAN

Berdasarkan hasil penelitian, maka dapat ditarik kesimpulan sebagai berikut:

1. Universitas Muhammadiyah telah melakukan dokumentasi terhadap kebijakan dan keamanan informasi untuk menanggulangi insiden pihak luar, tetapi pencatatan tersebut belum mencakup penerapan Kontrol Keamanan Informasi organisasi.
2. Pembuatan SMKI menghasilkan 2 (dua) dokumen, yaitu dokumen yang meliputi kebijakan, penilaian risiko, ruang lingkup, dan *Statement Of Applicability* (SOA) serta dokumen 2 (dua) yang berisi prosedur keamanan informasi.

SARAN

Berdasarkan kesimpulan, maka saran yang dapat diberikan untuk penelitian ini adalah sebagai berikut:

1. Universitas Muhammadiyah hendaknya memelihara dan tetap melakukan evaluasi terhadap kontrol keamanan informasi yang sudah ada.
2. Harus ada operator khusus untuk di perpustakaan, untuk menginput Jurnal.
3. Klausul yang digunakan dalam penelitian ini adalah klausul kelompok teknikal yang ditentukan berdasarkan abstraksi permasalahan yang ditemukan di lingkungan perusahaan, oleh karena itu diharapkan pada pengembangan penelitian selanjutnya dapat lebih dilengkapi dengan menggunakan Klausul lainnya yang mencakup pembahasan yang lengkap.

.

DAFTAR PUSTAKA

Andi Rafiandi, M. Hadi Cahyono. 2010. Jurus Sukses Sertifikasi ISO 27001, Andita Publishing.

Aprian, Rosmiani, Syahril Rizal, Muhammad Sobri. 2015. Perencanaan Sistem

Manajemen Keamanan Informasi Menggunakan Standar ISO 27001:2013 Studi Kasus: Universitas Bina Darma Palembang. Palembang: Jurnal Informatika, Universitas Bina Darma Palembang.

Badan Standarisasi Nasional Indonesia. Teknologi Informasi - Teknik Keamanan - Sistem Manajemen Keamanan Informasi - Persyaratan. (SNI ISO/IEC 27001:2013. IDT).

Badan Standarisasi Nasional Indonesia. Teknologi Informasi - Teknik Keamanan - Manajemen Risiko Keamanan Informasi. (SNI ISO/IEC 27005:2011. IDT).

Direktorat Keamanan Informasi. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik : Edisi 2.0, Direktorat Keamanan Informasi Kementrian Komunikasi dan Informatika Republik Indonesia.

Elia Setiana. 2015. Perancangan Keamanan Sistem Jaringan Pada Perusahaan Efek (Studi Kasus: PT. Reliance Securities)

http://perpustakaan.ummi.ac.id Downloaded at Februari, 7 2017, 20:20 AM.

http://perpustakaan.ummi.ac.id/layanan/detail/6-ejournal Downloaded at Februari, 7 2017, 20:30 AM.

https://www.edrawsoft.com/template-pdca-cycle-model.php Downloaded at Januari, 24 2017, 9:30 AM.

Hutahaean Jeperson. 2014. Konsep Sistem Informasi. Penerbit Deepublish. Yogyakarta.

Jayawardhana, R., & Tamura, M., *Substellar Objects in Nearby Young Clusters* (SONYC). V. New Brown Dwarfs in Ophiuchi, ApJ, 744, 134 (01/2012).

Kominfo (2016). Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Keamanan Informasi. Jakarta: Tim Direktorat Keamanan Informasi.

Ratna, Nyoman Kutha. 2010. Metodologi Penelitian: Kajian Budaya dan Ilmu Sosial Humaniora Pada Umumnya. Pustaka Pelajar : Yogyakarta.

Richardus Eko Indrajit, Kerangka Standar Keamanan Infomasi [online]. Available:http://www.idsirtii.or.id/doc/IDSIRTII-Artikel-pengantar_ISO.pdf

Sarno, R. dan Irsyat Iffano. 2009. Sistem Manajemen Keamanan Informasi Berbasis ISO 27001. Surabaya: ITS Press.

Sugiyono. Edisi 16. 2013. Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Jo Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

Utomo, Ali, dan Affandi 2012. Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis SNI ISO/IEC 27001:2005.

Wheeler, E., 2011. Security Risk Mangement, Elsevier, Inc.

Widodo, Isnanto, dan Rochim. 2013. Perencanaan dan Implementasi Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2005.