Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013

Tuti Hartati[1]

Intisari—**Informasi merupakan salah satu aset dari perusahaan/institusi perguruan tinggi yang dapat mempertahankan kelangsungan hidup bagi organisasi tersebut. Sejalan dengan perkembangan jaringan komputer di dalam sharing informasi ternyata akan menimbulkan kerentanan terhadap keamanan informasi itu sendiri dengan risiko besar, karena informasi dapat diketahui atau terungkapoleh pihak lain yang tidak mempunyai hak akses sehingga bisa merugikan kesinambungan sistem kerja dalam suatu perguruan tinggi.**

Dengan memperhatikan permasalahan di atas maka diperlukan suatu perencanaan sistem manajemen keamanan informasi (SMKI) yang lebih baik untuk menjaga kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi pada suatu perguruan tinggi sehingga dapat memperkecil dampak sebuah risiko atau bahkan dapat menghilangkan risiko tersebut.

Dalam pembuatan rancangan perencanaan sistem manajemen keamanan informasi (SMKI) perguruan tinggi ini, diadopsi dari ISO 27001:2013, yang mempunyai tujuan pengendalian informasi dan teknologi serta sebagai standar untuk pengendalian terhadap teknologi informasi.

Sistem manajemen keamanan informasi merupakan hal yang penting dalam perguruan tinggi, hal ini berhubungan erat dengan keamanan informasi untuk menjaga aset baik itu informasi, prosedur, *hardware*, *software* dan sumber daya manusia serta menjaga kesinambungan sistem kerja perguruan tinggi agar tetap berjalan dengan baik.

Kata Kunci— **Sistem Manajemen Keamanan Informasi, ISO 27001:2013, Perencanaan**

Abstract— Information is one of the assets of college companies / institutions that can maintain survival for the organization. In line with the development of computer networks in the sharing of information it will lead to vulnerability to the security of information itself with great risks, because information can be known or exposed by other parties who do not have access rights that can harm the continuity of work systems within a college.

With regard to the above problems it is necessary to design a better information security management system (ISMS) to maintain confidentiality, integrity and availability of information in a university so as to minimize the impact of a risk or even eliminate the risk.

In the design of this information security management system (SMKI) planning system, adopted from ISO 27001: 2013, which has the purpose of controlling information and technology and as a standard for control of information technology.

Information security management system is an important thing in college, it is closely related to information security to maintain good assets information, procedures, hardware, software and human resources as well as maintaining the continuity of college working system to keep running well..

Keywords—Information Security Management System, ISO 27001:2003, Planning.

I. PENDAHULUAN

Informasi merupakan salah satu aset dari suatu perusahaan/ instansi/ perguruan tinggi baik itu swasta maupun pemerintahan, yang dapat mempertahankan kelangsungan hidup bagi organisasi tersebut.

Perkembangan manajemen dalam sistem informasi yang berbasis komputer telah menyebabkan terjadinya perubahan yang cukup signifikan dalam operasi organisasi. Dengan meningkatnya kebutuhan penggunaan teknologi informasi, telah merambah dalam kinerja pendidikan di setiap perguruan tinggi baik perguruan tinggi negeri maupun perguruan tinggi swasta dimana semua kegiatan sudah sangat bergantung pada sistem komputer berbasis jaringan.

Sejalan dengan perkembangan jaringan komputer didalam sharing informasi ternyata akan menimbulkan kerentanan terhadap keamanan informasi itu sendiri dengan risiko besar, karena informasi dapat di ketahui atau terungkap oleh pihak lain yang tidak mempunyai hak akses sehingga bisa merugikan kesinambungan sistem kerja dalam suatu perguruan tinggi.

Selain adanya ancaman dari luar (eksternal), ancaman datang dari dalam (internal) melalui personal yang melakukan kecurangan berdasarkan lemahnya pengawasan terhadap prosedur yang ada dalam keamanan informasi. Untuk itu manajemen keamanan informasi pada saat ini sangat penting diperhatikan, mengingat perkembangan teknologi di era modern ini begitu mudah dalam memperoleh sebuah informasi.

Berdasarkan penelitian [1], pentingnya sistem manajemen keamanan informasi dapat menjaga kesinambungan sistem kerja dan aset informasi suatu perusahaan. Berdasarkan [2] menerangkan bahwa perlu adanya keamanan informasi untuk menjaga aset perusahaan seperti aset *software*, *database* dan *file server*, *mediastore*, *server* dan *workstation*, *network hardware*, *communication network*, *auxiliary equipment* dan aset personal.

Dengan melihat latar belakang permasalahan diatas, maka dapat diidentifikasi masalah yang terjadi yaitu:

1) Masih minimnya kebijakan dari perguruan tinggi yang berhubungan dengan keamanan informasi di bidang akademik, hal ini akan menimbulkan peluang adanya ketidakamanan dalam keamanan informasi.

2) Perlu adanya perencanaan sistem manajemen keamanan informasi untuk menjaga keamanan informasi bidang akademik yang lebih baik.

[1]Program Studi Teknik Komputer, STMIK "AMIKBANDUNG", Jl. Jakarta No 28, Bandung, Jawa Barat, Indonesia
[#] E-mail: toohart2013@gmail.com

3) Masih minimnya dokumentasi standar operasional prosedur (SOP) yang berhubungan dengan keamanan informasi di bidang akademik.

Berdasarkan identifikasi masalah yang telah diterangkan diatas maka penulis dapat membuat suatu perumusan masalah yaitu:

1) Bagaimana membuat suatu kebijakan perguruan tinggi yang berhubungan dengan keamanan informasi di bidang akademik, sehingga memperkecil peluang ketidakamanan informasi.

2) Bagaimana membuat suatu perencanaan sistem manajemen keamanan informasi dengan baik sehingga dapat memperkecil peluang risiko kebocoran sebuah informasi atau memperkecil peluang terjadinya kecurangan dalam melakukan manipulasi sebuah data oleh pihak yang tidak mempunyai hak akses.

3) Bagaimana membuat standar operasional prosedur (SOP) sebagai implementasi dari perencanaan sistem manajemen keamanan informasi di bidang akademik untuk menjaga keamanan informasi yang lebih baik lagi dan terdokumentasikan dengan baik.

II. LANDASAN TEORI

A. *Informasi*

Secara Etimologi, Kata informasi ini berasal dari kata Bahasa Perancis kuno *informacion* (tahun 1387) mengambil istilah dari bahasa Latin yaitu *informationem* yang berarti "konsep, ide atau garis besar". Informasi ini merupakan kata benda dari *informare* yang berarti aktivitas. Aktifitas dalam "pengetahuan yang dikomunikasikan". Pengertian informasi menurut para ahli:

1) Abdul Kadir [3] dan McFadden dkk. (1999) mendefinisikan informasi sebagai data yang telah diproses sedemikian rupa sehingga meningkatkan pengetahuan seseorang yang menggunakan data tersebut.

2) Jogiyanto [4] dalam bukunya yang berjudul Analisis dan Desain Sistem Informasi, berpendapat bahwa informasi adalah data yang diolah menjadi bentuk yang lebih berguna bagi yang menerimanya.

Ciri-Ciri Informasi yang berkualitas, yaitu [3]:

1) Informasi harus Relevan, yang artinya informasi tersebut mempunyai manfaat oleh pemakainya.

2) Informasi harus Akurat, yang artinya informasi harus bebas dari kesalahan-kesalahan dan harus jelas mencerminkan maksudnya.

3) Tepat pada waktunya, yang artinya informasi yang diterima tidak boleh terlambat.

4) Konsisten, yang artinya informasi yang diterima sesuai dengan datanya tidak mengalami perubahan yang tidak benar.

B. *Keamanan Informasi*

Definisi Keamanan informasi :

1) Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. (G. J. Simons)

2) *"A computer is secure if you can depend on it and its software to behave as you expect."* (Garfinkel & Spafford)

Jadi keamanan informasi merupakan suatu usaha untuk melindungi informasi melalui beberapa jenis media seperti komputer, mesin fax dan juga fasilitas pendukung penyimpanan data dan informasi seperti media dokumen *hardcopy* dari penyalahgunaan oleh orang yang tidak mempunyai hak akses. Keamanan informasi dapat juga diartikan sebagai upaya melindungi, mengamankan aset informasi dari ancaman yang mungkin terjadi sehingga dapat membahayakan bagi aset informasi tersebut.

Tujuan keamanan informasi untuk mencapai tiga sasaran utama [5], yaitu:

1) Confidentiality {Kerahasiaan) : melindungi data dan informasi perusahaan dari penyingkapan orang –orang yang tidak berhak

2) Integrity (Integritas) : sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan

3) Availability (Ketersediaan) : meyakinkan bahwa data dan informasi perusahaan hanya dapat digunakan oleh orang yang berhak menggunakannya.

C. *Manajemen Keamanan Informasi*

Manajemen Keamanan Informasi mempunyai empat tahapan yaitu:

1) Identifikasi threats (ancaman). Menyerang sumber daya informasi perusahaan.Yang termasuk dalam ancaman keamanan informasi adalah organisasi, mekanisme, personal atau peristiwa yang dapat berpotensi menimbulkan kejahatan pada sumber daya informasi perusahaan. Ancaman dapat berasal dari internal atau external, baik itu disengaja atau tidak disengaja.

2) Mendefinisikan resiko dari ancaman. Tindakan tidak sah yang menyebabkan resiko dapat digolongkan ke dalam empat jenis: a. Pencurian dan Penyingkapan tidak sah; b. Penggunaan Tidak Sah; c. Pengrusakan dan Penolakan layanan yang tidak sah; d. Modifikasi yang tidak sah.

3) Penetapan kebijakan keamanan informasi. Tanpa melihat apakah perusahaan mengikuti manajemen resiko atau strategi pelaksanaan brenchmark, kebijakan keamanan harus diimplementasikan untuk mengarahkan keseluruhan program

4) Menerapkan kontrol yang tertuju pada resiko. Kontrol adalah mekanisme yang diimplementasikan baik untuk melindungi perusahaan dari resiko atau untuk memperkecil dampak resiko terhadap perusahaan.

D. *ISO 27001:2013*

ISO 27001 adalah suatu standar internasional untuk *Information Security Manajemen System* (ISMS). ISO 27001 berlaku untuk semua bisnis. Keamanan informasi yang dimiliki dalam bentuk apapun, bukan hanya berupa data elektronik.

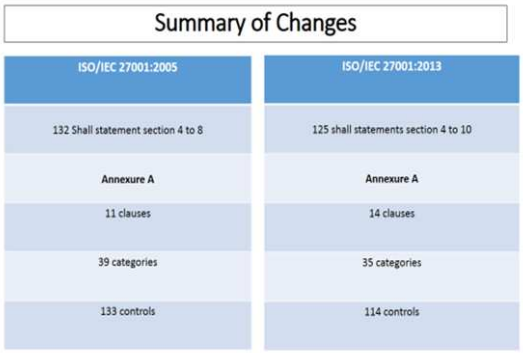
Di Uni Eropa diperkirakan kejahatan internet dan serangan cyber meningkat pesat dalam beberapa tahun terakhir. Yang jadi sasaran bukan hanya perusahaan swasta, melainkan juga lembaga pemerintahan.

Perbedaan atau Perubahan ISO 27001: 2013 dengan ISO 27001: 2005:

1) ISO 27001: 2013 memiliki 114 kendali (kontrol) dalam 14 kelompok domain,

2) ISO 27001: 2005 memiliki 133 kendali (kontrol) dalam 11 kelompok domain.

Adanya perubahan beberapa kontrol pada ISO 27001:2013 ini adalah salah satu dampak dari adanya perubahan/perkembangan teknologi. Untuk lebih jelasnya tentang ISO 27001: 2013.



Gbr. 1 Perbedaan ISO/IEC 27001: 2005 dengan ISO/IEC 27013

Adanya perubahan beberapa kontrol pada ISO 27001:2013 ini adalah salah satu dampak dari adanya perubahan/perkembangan teknologi. Untuk lebih jelasnya tentang ISO 27001: 2013 dapat dilihat sebagai berikut [6]:

1) Scope of the standard

2) How the document is referenced

3) Reuse of the terms and definitions in ISO/IEC 27000

4) Organizational context and stakeholders

5) Information security leadership and high-level support for policy

6) Planning an information security management system; risk assessment; risk treatment

7) Supporting an information security management system

8) Making an information security management system operational

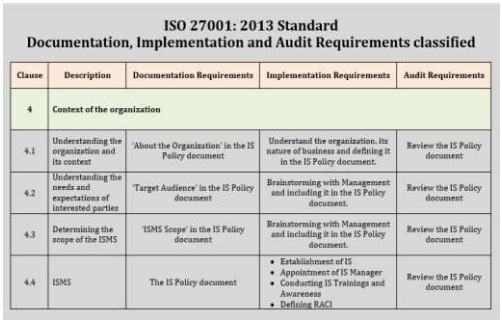
9) Reviewing the system's performance

10) Corrective action

Berdasarkan Establish ISMS 27001: 2013 di mana urutan ke 4 adalah *Contex of Organization* yang dapat di uraikan pada Gbr. 2.

E. Sistem Manajemen Keamanan Informasi

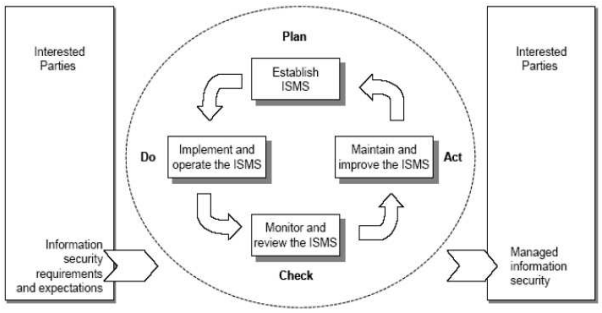
Sistem Manajemen Keamanan Informasi (SMKI) adalah suatu bentuk susunan proses yang dibuat berdasarkan pendekatan resiko bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitoring dan meninjau (*Check*), serta memelihara dan meningkatkan atau mengembangkan (*Act*) terhadap keamanan informasi perusahaan. Sistem Manajemen Keamanan Informasi (SMKI), biasanya dapat digunakan para manajer untuk mengukur, memonitor dan mengendalikan keamanan informasi.



ISO 27001: 2013 Standard
Documentation, Implementation and Audit Requirements classified

Clause	Description	Documentation Requirements	Implementation Requirements	Audit Requirements
4	Context of the organization			
4.1	Understanding the organization and its context	'About the Organization' in the IS Policy document	Understand the organization, its nature of business and defining it in the IS Policy document.	Review the IS Policy document
4.2	Understanding the needs and expectations of interested parties	'Target Audience' in the IS Policy document	Brainstorming with Management and including it in the IS Policy document.	Review the IS Policy document
4.3	Determining the scope of the ISMS	'ISMS Scope' in the IS Policy document	Brainstorming with Management and including it in the IS Policy document.	Review the IS Policy document
4.4	ISMS	The IS Policy document	• Establishment of IS • Appointment of IS Manager • Conducting IS Trainings and Awareness • Defining RACI	Review the IS Policy document

Gbr. 2 ISO 27001: 2013 *Standard Documentation, Implementation and Audit Requirment classified*



Gbr. 3 PDCA yang diterapkan untuk proses SMKI (Sistem Manajemen Keamanan Informasi) [7]

Sistem Manajemen Keamanan Informasi memberikan perlindungan informasi dan penghitungan aset yang ada. Terdapat tiga komponen kunci dalam menyediakan jaminan layanan keamanan informasi, diantaranya [5]:

1) Confidentiality/Kerahasiaan. Data hanya boleh diakses oleh yang berwenang.

2) Integrity/Integritas. Informasi tidak boleh berubah (*tampered, altered, modifield*) oleh pihak yang tidak berhak.

3) Availability/Ketersediaan. Informasi harus tersedia ketika dibutuhkan.

F. Perencanaan

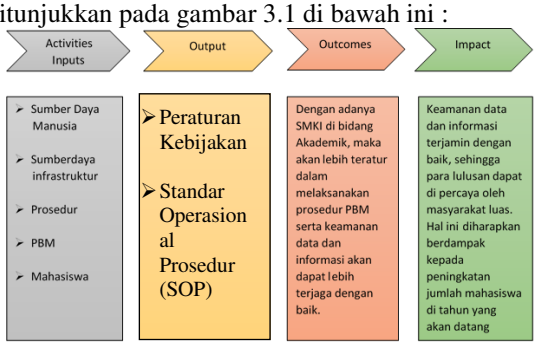
Dalam manajemen, perencanaan adalah proses mendefinisikan tujuan organisasi, membuat strategi untuk mencapai tujuan itu, dan mengembangkan rencana aktivitas kerja organisasi. Perencanaan merupakan proses terpenting dari semua fungsi manajemen karena tanpa perencanaan fungsi - fungsi lain — pengorganisasian, pengarahan, dan pengontrolan — tak akan dapat berjalan.

Rencana dapat berupa rencana informal atau rencana formal. Rencana informal adalah rencana yang tidak tertulis dan bukan merupakan tujuan bersama anggota suatu organisasi. Sedangkan rencana formal adalah rencana tertulis yang harus dilaksanakan suatu organisasi dalam jangka waktu tertentu. Rencana formal merupakan rencana bersama anggota korporasi, artinya, setiap anggota harus mengetahui dan menjalankan rencana itu. Rencana formal dibuat untuk mengurangi ambiguitas dan menciptakan kesepahaman tentang apa yang harus dilakukan.

III. PEMBAHASAN

A. *Logical Framework SMKI*

Adapun *Logical Framework* SMKI di bidang Akademik ini dapat ditunjukkan pada gambar 3.1 di bawah ini :

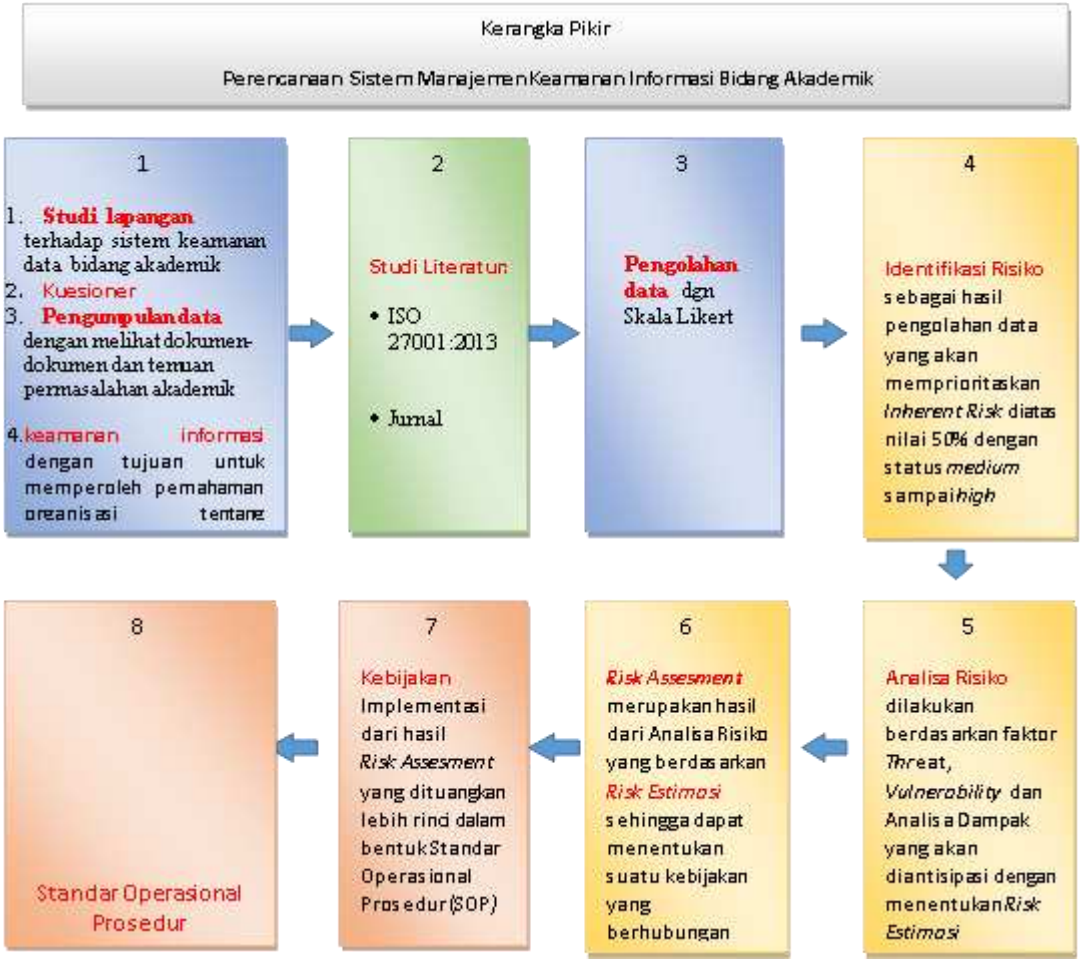


Gbr. 4 *Logical Framework* SMKI bidang Akademik

B. *Kerangka Pikir*

Kerangka penelitian ini dapat digambarkan pada Gbr. 5sebagai gambaran langkah-langkah strategis dan operasional dalam melakukan penelitian ini.

Penelitian ini dilakukan secara bertahap dan berkesinambungan antara satu tahap dengan tahap berikutnya sampai mencapai tujuan yang diharapkan yaitu sistem manajemen keamanan informasi yang baik yang dapat diimplementasikan dengan memperoleh *outcome standar operational procedure* (SOP).



Gbr. 5 Kerangka Pikir Perencanaan SMKI Bidang Akademik menggunakan

C. *Ruang Lingkup*

Lingkup penelitian yang penulis lakukan hanya berhubungan dengan permasalahan keamanan informasi pada bidang akademik, dimana rancangan perencanaan sistem manajemen keamanan informasi yang diadopsi dari ISO 27001: 2013. Beberapa faktor yang mempengaruhi sistem manajemen keamanan informasi adalah:

1) Sumber Daya Manusia.

2) Desain ruang kerja harus aman dari faktor lingkungan.

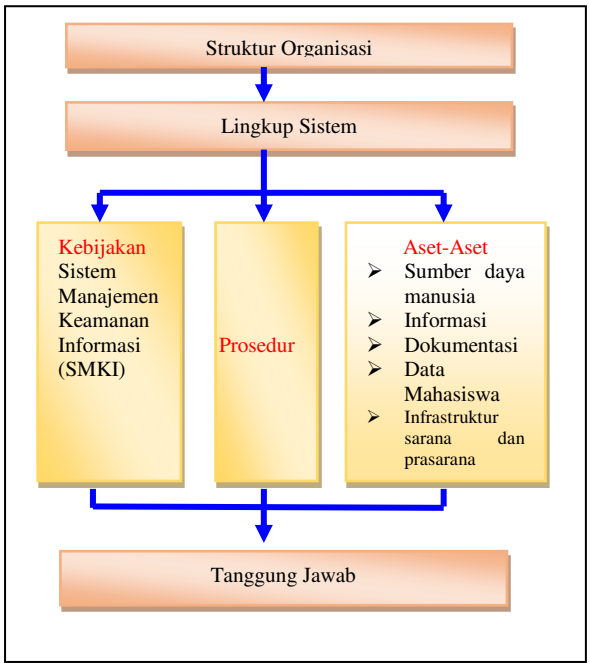
3) Kedisiplinan para pegawai dapat menjalankan tugas sesuai dengan prosedur kerja yang telah ditetapkan oleh institusi.

Sedangkan dalam menentukan pencapaian sistem manajemen keamanan informasi pada bidang akademik, penulis melakukan beberapa hal seperti di bawah ini:

1) Menentukan tujuan dari sistem manajemen keamanan informasi.

2) Mendefinisikan setiap tahapan dari kerangka kerja yang akan digunakan.

Pada Gbr. 6 dibawah ini menerangkan Struktur Sistem Manajemen Keamanan Informasi.



Gbr. 6 Struktur Sistem Manajemen Keamanan Informasi

Struktur Organisasi sangat penting untuk membuat prosedur kerja dari sebuah alur sistem kerja yang akan dibuat dimana diperlukan adanya penanggung jawab masing-masing lini / bagian dari struktur organisasi tersebut. Dengan demikian akan terkendali dan termonitor semua bagian dalam menjalankan tugasnya masing-masing.

Pada penelitian ini dimana lingkup sistem manajemen keamanan informasi yang akan dibahas panya pada bidang akademik. Adapun komponen-komponen yang terlibat meliputi prosedur, personal perguruan tinggi, data mahasiswa dan infrastruktur. Mengingat begitu pentingnya komponen-kompnen tersebut sebagai bagian dari asset-aset perguruan tinggi, maka perlu adanya pengamanan terhadap sistem informasinya sehingga semua itu dapat terjaga dengan baik. Apabila hal tersebut diabaikan keamanannya, maka hal ini bisa mempengaruhi bagi sistem kerja lainnya seperti data nilai yang berubah, pengambilan jumlah sks pada saat perwalian tidak sesuai dengan aturan yang berlaku serta penyalahgunaan data mahasiswa oleh orang yang tidak bertanggung jawab.

1) Kebijakan SMKI. Perlu adanya sebuah kebijakan dalam menghadapi permasalahan-permasalahan yang mungkin timbul, karena suatu alasan yang dapat dipahami seperti pada proses perwalian masih seringnya mahasiswa terlambat dalam melakukan perwalian, masih seringnya keterlambatan pengumpulan nilai dari dosen yang mengakibatkan terlambatnya entri nilai bagi mahasiswa.

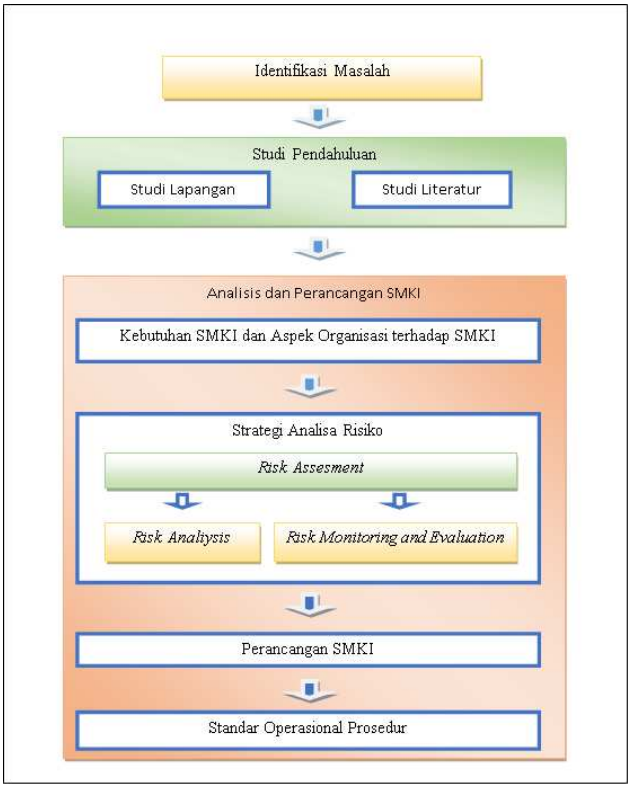
2) Prosedur. Untuk menjaga keamanan sistem informasi maka perlu adanya pengendalian dan monitoring dari prosedur-prosedur yang telah dibuat supaya setiap bagian dapat menjalankan tugas dan tanggung jawabnya masing-masing sesuai dengan struktur organisasi.

3) Aset. Bagian terpenting yang harus diperhatikan pengamanan adalah aset seperti: 1) Sumber daya manusia; 2) Data Mahasiswa; 3) Dokumentasi; 4) Infrastruktur sarana dan prasarana; 5) Aplikasi. Jika perguruan tinggi dapat menjaga aset-aset tersebut maka sistem keamanan yang diharapkan dapat terlaksana dengan baik.

Pada tahapan Tanggung Jawab, merupakan tahapan yang mempunyai pengendali tanggung jawab atas semua kegiatan dari sistem manajemen keamanan informasi. Jika pada tahapan ini diabaikan maka kemungkinan adanya kelonggaran terhadap keamanan informasi bisa terjadi, dan hal ini bisa membahayakan keamanan informasi dimana sistem informasi dapat diakses oleh orang lain.

D. Analisis dan Perencanaan Sistem Manajemen Keamanan Informasi (SMKI)

Alur analisis dan perencanaan Sistem Manajemen Keamanan Informasi diterangkan pada gambar 3.4. di bawah ini:



Gbr. 7 Alur Analisis dan Perencanaan Sistem Manajemen Keamanan Informasi

E. Perencanaan Sistem Manajemen Keamanan Informasi

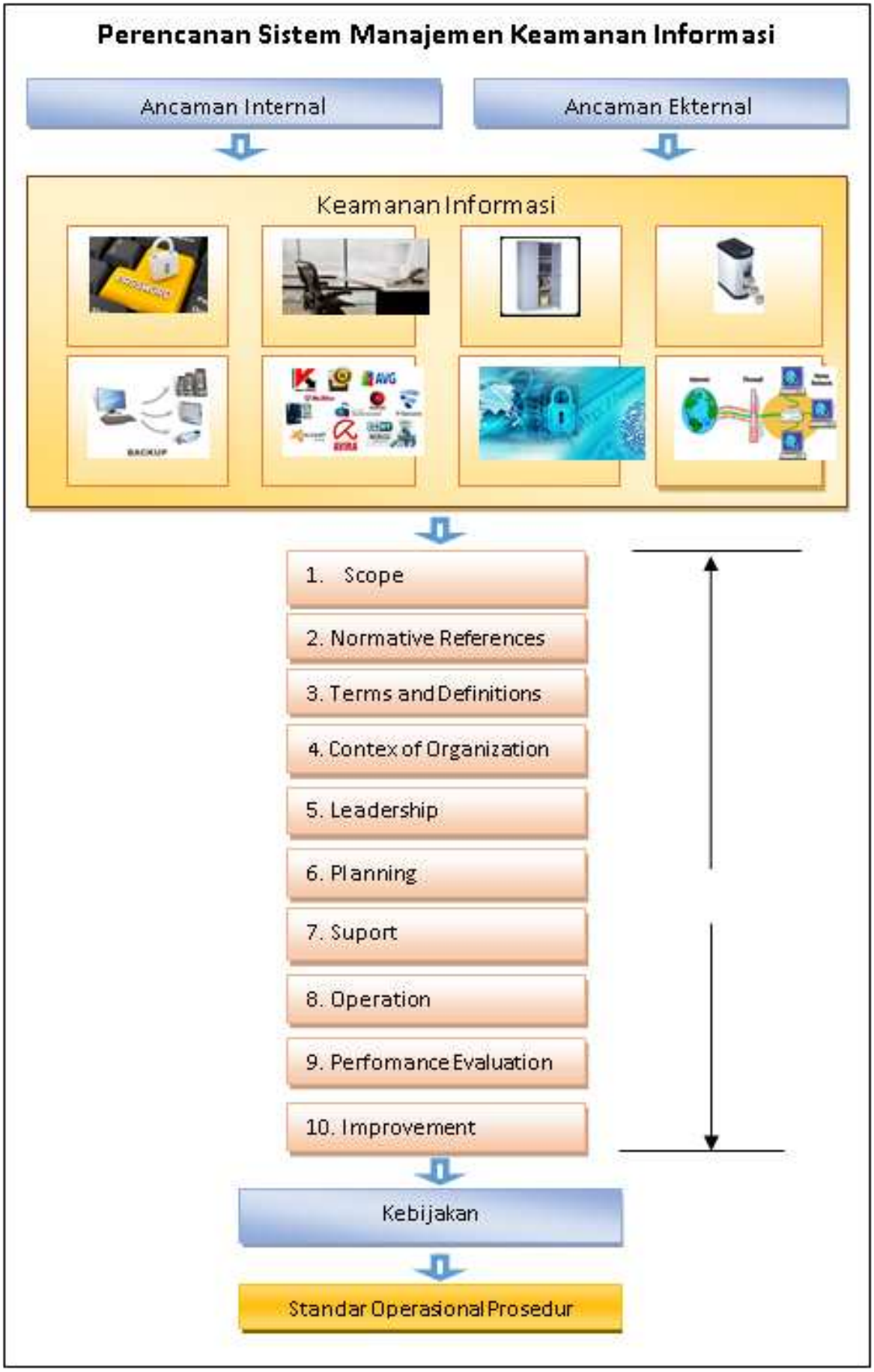
1) Ancaman Internal. Ancaman yang berasal dari dalam perguruan tinggi itu sendiri seperti, a. Personal; b. Prosedur yang salah; c. Lemahnya pengawasan terhadap keamanan informasi.

2) Ancaman Ekternal. Ancaman yang berasal dari luar seperti: a. *Internet of Things*; b. Serangan DDoS; c. Serangan Media Sosial; d. *Malware Celuler*; e. Serangan Pihak Ketiga; f. *IP Spoofing Hacker*; g. *Sniffing*; h. *Remote attack*.

3) Keamanan Informasi. Bagian dari perguruan tinggi yang melakukan upaya untuk melindungi, mengamankan aset informasi dari ancaman yang mungkin terjadi sehingga dapat membahayakan aset informasi tersebut.

4) ISO 27001:2013. Standar Internasional ISO IEC 27001 adalah standar yang memberikan persyaratan untuk

 ISSN: 2549-9351



Gbr. 8 Kerangka Kerja Perencanaan Sistem manajemen Keamanan Informasi

penetapan, penerapan, operasi, pemantauan, peninjauan, pemeliharaan dan peningkatan suatu Sistem Manajemen Keamanan Informasi (SMKI) yang terdokumentasi dalam konteks risiko organisasi bisnis secara keseluruhan. Standar ini menentukan persyaratan pelaksanaan kontrol keamanan yang disesuaikan dengan kebutuhan organisasi. SMKI dirancang untuk menjamin pemilihan kontrol keamanan yang memadai dan proporsional untuk melindungi aset informasi dan memberikan kepercayaan kepada para pihak yang berkepentingan.

5) Kebijakan. Peraturan yang dibuat oleh institusi pada level pimpinan secara tertulis untuk memberikan petunjuk dan arahan secara umum dalam mengatur dan melaksanakan sistem kerja, baik untuk personal sebagai pelaksana maupun berupa prosedur sebagai alur sistem kerja yang harus dikerjakan agar dapat berjalan dengan baik sehingga memperoleh tujuan akhir yang harapkan sesuai dengan visi dan misi yang sudah ditetapkan institusi. Atau peraturan yang dibuat sebagai konsep/ asas yang menjadi garis pelaksanaan suatu pekerjaan, kepemimpinan dalam menjalankan alur kerja yang sesuai prosedur sehingga dapat mencapai tujuan sesuai dengan visi dan misi yang ditetapkan.

6) Standar Operasional Prosedur (SOP). Pedoman atau acuan untuk melaksanakan pekerjaan yang sesuai dengan tugas dan fungsi dalam organisasi dengan menggunakan alat penilaian kinerja berdasarkan indikator-indikator teknis, administrasif dan prosedural yang sesuai dengan tata kerja pada unit yang bersangkutan. Berdasarkan hasil penelitian maka penulis membuat standar operasional prosedur (SOP) dengan melihat penilaian tingkat risiko dan tingkat *impact* hanya pada status *high* yaitu berada pada klausul dibawah ini: 1) Kebijakan Keamanan Informasi - Kebijakan untuk keamanan informasi (*Clause* A.5.1.1); 2) Keamanan Sumber Daya Manusia- Proses Disiplin (*Clause* A.7.2.3); 3) Manajamen Aset - Inventarisasi aset (*Clause* A.8.1.1); 4) Keamanan Operasional - Dokumen prosedur operasional (*Clause* A.12.1.1).

IV. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan oleh penulis maka dapat disimpulkan:

1) Dengan adanya penerapan kebijakan keamanan informasi dibidang akademik dalam perguruan tinggi, maka dapat memperkecil peluang ketidakamanan informasi atau bahkan dapat menghilangkan peluang ketidakamanan informasi tersebut dalam bentuk setiap karyawan disiplin menjalankan pekerjaan berdasarkan standar operasional prosedur yang sudah ditetapkan institusi perguruan tinggi. Dengan pendisiplinan karyawan dalam menjalankan tugasnya masing-masing maka akan memperoleh sistem manajamen keamanan informasi yang lebih baik lagi dan terjaga tetap terjaga keamanan informasinya.

2) Dengan membuat perencanaan sistem manajemen keamanan informasi yang berlandaskan ISO 27001: 2013, kita dapat mengetahui faktor-faktor dari ketidakamanan informasi tersebut dan dengan cepat dapat menanggulangi akar permasalahan sehingga dapat memperkecil peluang adanya risiko kebocoran informasi.

3) Setelah dibuat standar operasional prosedur (SOP) keamanan informasi, maka sebaiknya institusi selalu mensosialisasikan SOP kepada seluruh karyawan agar setiap karyawan dapat menjankannya dengan baik dan selalu mendokumentasikan setiap berkas dokumen penting lainnya dalam kegiatan akademik. Dengan demikian sistem dokumentasi institusi perguruan tinggi akan semakin baik, hal ini akan berdampak kepada kinerja karyawan dalam menjaga keamanan informasi di bidang akademik

REFERENSI

[1] M. Syafrizal, "Information Security Management System (ISMS) MenggunakanStandar ISO/IEC 27001: 2005," *Jurnal DASI,* vol. 10, no. 1, pp. 92--117, 2009.

[2] R. S. Rozas and R. Sarrno, "SiPKoKI ISO 27001: Sistem Pemilihan Kontrol Keamanan Informasi Berbasis ISO 27001," in *Seminar Nasional Pascasarjana XI*, Surabaya, 2011.

[3] A. Kadir, Pengenalan Sistem Informasi, Yogyakarta: Andi Offset, 2003.

[4] H. M. Jogiyanto, Analisis dan desain sistem informasi, Yogyakarta: Andi Offset, 2005.

[5] A. Kristanto, Komputer dan Teknologi Informasi, Yogyakarta: Graha Ilmu, 2003.

[6] Catur Daya Solusi, "Upgrading ISO 27001:2005 ke ISO 27001:2013," 9 Maret 2015. [Online]. Available: http://caturdayasolusi.com/upgrading-iso-270012005-ke-iso-270012013/.

[7] A. M. Wibowo, *ISO 27001 Informations Security Management Systems,* 2005.

[8] H. Ryana and B. Rahardjo, "Kajian ISO/IEC 17799: 2005 Sebagai Kerangka Dasar Pengendalian Keamanan Informasi," Institut Teknologi Bandung, Bandung, 2009.

[9] H. Susanto, M. N. Almunawar and Y. C. Tuan, "Information security management system standards: A comparative study of the big five," *International Journal of Electrical Computer Sciences IJECSIJENS,* vol. 11, no. 5, pp. 23--29, 2011.

[10] I. Tashi and S. Ghernouti-Helie, "Information security management is not only risk management," in *Internet Monitoring and Protection, 2009. ICIMP'09. Fourth International Conference on*, 2009.

[11] I. Sudanawati and R. Rozas, "SiPKoKI ISO 27001: Sistem Pemilihan Kontrol Keamanan Informasi Berbasis ISO 27001," in *Seminar Nasional Pasca Sarjana XI*, Surabaya, 2011.

[12] E. Kosasih, Cerdas Berbahasa Indonesia, Jakarta: Erlangga, 2006.

[13] F. M. Natsir, *Cara Menghitung Skala Likert,* 2013.

[14] Sugiyono, Metode penelitian bisnis, Bandung: Alfabeta, 2004.

[15] Z. Cosic and M. Boban, "Information security management—Defining approaches to Information Security policies in ISMS," in *Intelligent Systems and Informatics (SISY), 2010 8th International Symposium on*, 2010.

(Halaman ini sengaja dikosongkan)