ITS
Institut
Teknologi
Sepuluh Nopember

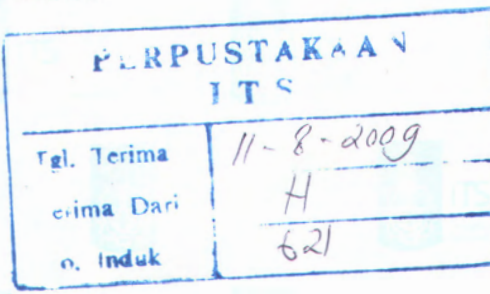
TUGAS AKHIR - CF 1380

PEMBUATAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) DI BIRO ADMINISTRASI & AKADEMIK KEMAHASISWAAN (BAAK) INSTITUT TEKNOLOGI SEPULUH NOPEMBER BERDASARKAN ISO 27001:2005

KARTIKA SARI
NRP 5205 100 063

Dosen Pembimbing
Ir. Aris Tjahyanto, M.Kom

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
2009



ITS
Institut
Teknologi
Sepuluh Nopember

FINAL PROJECT - CF 1380

DEVELOPING INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) OF STUDENT ADMINISTRATION & ACADEMIC BEAROU INSTITUT TEKNOLOGI SEPULUH NOPEMBER BASED ON ISO 27001:2005

KARTIKA SARI
NRP 5205 100 063

Supervisor
Ir. Aris Tjahyanto, M.Kom

DEPARTMENT OF INFORMATION SYSTEM
Faculty of Information Technology
Institut Teknologi Sepuluh Nopember
2009

PEMBUATAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) DI BIRO ADMINISTRASI & AKADEMIK KEMAHASISWAAN (BAAK) INSTITUT TEKNOLOGI SEPULUH NOPEMBER BERDASARKAN ISO 27001:2005

TUGAS AKHIR
Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Pada
Bidang Studi Perencanaan dan Pengembangan Sistem Informasi
(PPSI)
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

KARTIKA SARI
NRP 5205 100 063

Surabaya, 23 Juli 2009

KETUA
JURUSAN SISTEM INFORMASI

Ir. A. Holil Noor Ali M.Kom
NIP 131 996 150

PEMBUATAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) DI BIRO ADMINISTRASI & AKADEMIK KEMAHASISWAAN (BAAK) INSTITUT TEKNOLOGI SEPULUH NOPEMBER BERDASARKAN ISO 27001:2005

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
Pada
Bidang Studi Perencanaan dan Pengembangan Sistem Informasi (PPSI)
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

KARTIKA SARI
NRP 5205 100 063

Disetujui Tim Penguji: Tanggal Ujian : 21 Juli 2009
Periode Wisuda : Oktober 2009

Ir. Aris Tjahyanto, M.Kom **(Pembimbing)**

Bekti Cahyo Hidayanto, S.si, M.Kom **(Penguji 1)**

Ahmad Mukhlason, S.Kom, M.Sc. **(Penguji 2)**

PEMBUATAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) DI BIRO ADMINISTRASI & AKADEMIK KEMAHASISWAAN (BAAK) INSTITUT TEKNOLOGI SEPULUH NOPEMBER BERDASARKAN ISO 27001:2005

Nama Mahasiswa	**: Kartika Sari**
NRP	**: 5205 100 063**
Jurusan	**: Sistem Informasi FTIf – ITS**
Dosen Pembimbing	**: Ir. Aris Tjahyanto, M.Kom**

Abstrak

Pengelolaan Sistem Informasi Manajemen Akademik (SIM akademik) adalah salah satu proses di BAAK yang menempatkan informasi sebagai infrastruktur penting. Didasari oleh kepentingan informasi dan terjadinya beberapa kasus yang berkaitan dengan keamananan informasi seperti, pembobolan website SIM akademik menyebabkan perlunya dibuat suatu pengamanan terhadap aset informasi.

Sistem Manajemen Keamanan Informasi (SMKI) merupakan keseluruhan sistem manajemen, berdasarkan pendekatan risiko bisnis untuk memantapkan, menerapkan, menjalankan, memantau, meninjau ulang, memelihara, dan meningkatkan keamanan informasi berdasarkan pendekatan risiko bisnis. SMKI ini dibuat dengan standar ISO 27001:2005 yang merupakan kerangka kerja untuk pengembangan atau peningkatan keamanan informasi dalam organisasi.

Hasil dari Tugas akhir ini adalah dokumentasi SMKI untuk BAAK. Dokumentasi ini digunakan sebagai panduan dalam pengamanan informasi SIM akademik. SMKI juga menawarkan pemilihan kendali keamanan yang sesuai, sebagai usaha perlindungan terhadap ancaman risiko dari proses dan aset pendukung aplikasi SIM akademik.

Kata kunci: Keamanan informasi, Sistem Manajemen Keamanan Informasi, ISO 27001, SIM akademik.

Halaman ini sengaja dikosongkan.

DEVELOPING INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) OF STUDENT ADMINISTRATION & ACADEMIC BEAROU INSTITUT TEKNOLOGI SEPULUH NOPEMBER BASED ON ISO 27001:2005

Name : **Kartika Sari**
Registration Number : **5205 100 063**
Departement : **Sistem Informasi FTIf – ITS**
Supervisor : **Ir. Aris Tjahyanto, M.Kom**

Abstract

Academic Management Information System is one of the important process of Student Administration & Academic Bearou that places information as an important infrastucture. Based on the information importance and some cases occurance that are related to information security such as, Academic Management Information System website fraud. So it needs asset information securing .

Information security management system (ISMS) is a management system to establish, implement, operate, monitor, review, maintain and improve information security based on business risk approachment. ISMS for Student Administration & Academic Bearou is made from ISO 27001:2005 standardization which is a framework to develop and improve information security on organization.

The outcome of this final project is ISMS document for Student Administration & Academic Bearou. This document used as guide line of securing academic MIS application. ISMS also offers appropriate options of security control as protection attempt of process and Academic Management Information System application against the risk threat.

Keyword: Information Security, Information Security Management System, ISO 27001:2005, Academic Management Information System.

Halaman ini sengaja dikosongkan.

KATA PENGANTAR

Terima kasih tak terkira dan ucapan syukur bagi Tuhan Yesus atas segala anugerah, petunjuk, kejatuhan dan cinta yang diberikan, sehingga penulis dapat menyelesaikan laporan tugas akhir dengan judul "PEMBUATAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) DI BAAK INSTITUT TEKNOLOGI SEPULUH NOPEMBER BERDASARKAN ISO 27001:2005", yang merupakan salah satu syarat kelulusan pada Jurusan Studi Sistem Informasi, Fakutas Teknologi Informasi, Institut Teknologi Sepuluh Nopember.

Ucapan terima kasih dan penghargaan penulis sampaikan kepada:

1. Ibu, Bapak dan seluruh keluarga besar atas doa dan dukungan baik secara moril maupun materiil.
2. Bpk. Ir. Aris Tcahyanto, M.Kom selaku dosen pembimbing yang telah dengan sabar memberikan banyak masukan, motivasi dan bimbingan kepada penulis.
3. Ibu Mahendrawathi ER, Ph.D selaku dosen wali penulis, atas segala bimbingannya selama berkuliah di SI.
4. Bapak Bekti Cahyo H. S.si, M.Kom dan Bapak Ahmad Mukhlason S.Kom, M.Sc. selaku dosen penguji atas masukannya.
5. Seluruh Bapak dan Ibu Dosen pengajar SI ITS yang telah memberikan ilmu yang berharga kepada penulis.
6. Bapak Mukayat dan Bapak Agus Gunaryo serta segenap staf BAAK atas bantuannya kepada penulis dalam pengumpulan data.
7. Mbak Rahma dan Anita, trimakasih telah menjadi partner yang sangat baik bagi penulis dalam menyelesaikan tugas akhir ini.
8. Anna, Kembung, Mbak Nisa', Ulfah, Mbak Ratih, Hilda, Mbak Heni, Mbak Enik, Mbak Dita, Zizah, Vahiel, Ito serta anak-anak GR 1 dan GR 3, trimakasih atas

pertemanan dan dukungan yang diberikan kepada penulis.

9. Kaka, Anast, Amna, Jian, Mega, Venty, Afandi, Danu, Nela, Anif dan segenap teman-teman Phoenic' 05, trimakasih untuk persaudaran yang telah diberikan. Penulis bangga menjadi bagian dari kalian.
10. Seluruh Keluarga Besar Sistem Informasi yang tidak dapat disebutkan satu persatu.
11. Dimas, Cheryan, Wahyu, Khalid, Mbak Anis, Mutia, Udin dan Seluruh Keluarga Mahasiswa Klaten di Surabaya (KMKS) untuk rasa persaudaraan dan kekeluargaan yang diberikan kepada penulis.
12. Berbagai pihak yang belum sempat penulis sebutkan atas jasa-jasanya dalam mendukung penyusunan tugas akhir ini.

Penulis sangat menyadari bahwa tugas akhir ini masih jauh dari sempurna. Oleh karena itu penulis mengharapkan komentar, kritik, dan saran dari berbagai pihak.

Akhirnya, penulis berharap semoga keberadaan tugas akhir ini bermanfaat banyak bagi ilmu pengetahuan dan berbagai pihak.

Surabaya, 23 Juli 2009

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH

SMKI	:	Sistem Manajemen Keamanan Informasi
BAAK	:	Biro Administrasi & Akademik Kemahasiswaan
ITS	:	Institut Teknologi Sepuluh Nopember
ISBS	:	*Information Security Breaches Survey*
Framework	:	Area Kerja
SIM-Akademik	:	Sistem Informasi Manajemen Akademik
Stakeholders	:	Seseorang atau kelompok yang berhubungan baik secara langsung maupun tidak langsung dengan organisasi.
PDCA	:	*Plan-Do-Check-Act*
BIA	:	*Business Impact Analysis*
CIA	:	*Confidentially-Integrity-Avaliability*
PUSKOM	:	Pusat Komputer
SOA	:	*Statement of Applicability*
MKI	:	Manual Keamanan Informasi
PKI	:	Prosedur Keamanan Informasi
IK	:	Instruksi Kerja

FM	:	Formulir
RF	:	Referensi
RS	:	Sub bagian Registrasi dan Statistik
SP	:	Sub bagian Sarana dan Prasarana
PE	:	Sub bagian Pendidikan & Evaluasi

BAB I
PENDAHULUAN

Bab ini menjelaskan latar belakang munculnya permasalahan, perumusan masalah, batasan masalah serta tujuan dari tugas akhir, berikut relevansi dan manfaatnya. Dari uraian ini diharapkan pembaca dapat memahami gambaran umum permasalahan dan pemecahan masalah dari tugas akhir ini.

1.1 Latar Belakang

Keamanan informasi menjadi hal yang sangat penting pada perusahaan penyedia jasa Teknologi Informasi (TI) maupun industri lain, seperti: perusahaan *export-import*, tranportasi, lembaga pendidikan, pemberitaan dan perbankan. Demikan juga dengan BAAK ITS yang menggunakan fasilitas TI dan menempatkan keamanan informasi sebagai infrastruktur utamanya. Keamanan informasi yang baik secara tidak langsung dapat mempengaruhi kelangsungan bisnis, pengurangan risiko, mengoptimalkan *return on investment* dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-*sharing* maka semakin besar pula risiko terjadinya kerusakan, kehilangan atau ter-*ekspose*-nya data ke pihak eksternal.

Hasil survey dari *Information Security Breaches Survey* (ISBS) pada tahun 2000 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara atau terlindungi dan menyebabkan kerawanan. Survey tersebut menunjukkan bahwa 60% serangan atau kerusakan data disebabkan oleh kelemahan dalam sistem keamanan. Kegagalan sistem keamanan sendiri lebih banyak disebabkan oleh faktor internal dibandingkan dengan faktor eksternal. Berbagai faktor internal yang berpengaruh diantaranya adalah kesalahan dalam pengoperasian sistem (40%), diskontinuitas *power supply* (32%) dan sisanya ditempati oleh pencurian data, serangan virus, akses tanpa

autorifikasi, dll[1]. Berdasarkan survey tersebut didapatkan sebuah fenomena baru, dimana saat ini kunci keamanan informasi bukan lagi terletak pada kecanggihan aplikasi, namun lebih kepada faktor internal yang merupakan faktor tingkah laku manusia sebagai pelaksana.

Beberapa kendala yang muncul berkaitan dengan pengamanan informasi yang terjadi di BAAK diantaranya adalah pencurian kode program, fenomena *password sharing* (membagi informasi *password* dengan orang lain). Ketiadaan prosedur dalam setiap aktivitas yang berkaitan dengan keamanan informasi juga merupakan salah satu kendala dalam keamanan informasi. Oleh karena itu untuk mencegah terjadinya kerawanan diperlukan suatu standar/pedoman untuk mengamankan aset informasi tersebut. SMKI adalah salah satu contoh pedoman yang digunakan dalam usaha pengamanan terhadap aset informasi. SMKI dapat dibangun berdasarkan beberapa *framework* seperti Cobit, ITIL dan ISO 27001:2005. ISO 27001:2005 adalah suatu standar internasional yang menggunakan pendekatan risiko bisnis untuk mendirikan, melaksanakan, mengawasi, meninjau ulang, merawat dan mengembangkan SMKI organisasi. Tujuan dari perancangan SMKI ini adalah untuk memastikan pemilihan kendali keamanan yang cukup dan sesuai dalam melindungi aset informasi serta memberikan kepercayaan bagi para *stakeholders*.

1.2 Permasalahan

Tugas akhir ini menitikberatkan pada permasalahan sebagai berikut:

1. Bagaimana penggambaran proses bisnis organisasi?
2. Bagaimana melakukan identifikasi risiko terhadap proses bisnis dan aset yang dimiliki organisasi untuk menemukan perbaikan-perbaikan yang perlu dilakukan?
3. Bagaimana membuat SMKI sebagai panduan dalam perlindungan dan pengamanan informasi?

1.3 Batasan Masalah

Dari permasalahan yang telah disebutkan di atas, maka batasan-batasan dalam tugas akhir ini adalah:

1. SMKI yang dibuat hanya berupa usulan dan diperuntukkan bagi BAAK pada umumnya serta SIM akademik pada khususnya.
2. Identifikasi Risiko dilakukan terhadap aset-aset yang berkaitan dengan aplikasi SIM akademik.
3. Pembuatan prosedur dan instruksi kerja hanya untuk beberapa contoh saja dalam lingkup aplikasi SIM akademik.

1.4 Tujuan

Tujuan tugas akhir ini adalah mendapatkan panduan untuk mengamankan informasi berupa SMKI bagi BAAK di Institut Teknologi Sepuluh Nopember (ITS).

1.5 Manfaat

Adapun manfaat langsung yang bisa diperoleh dari penyelesaian tugas akhir ini adalah :

- Mendapatkan pemilihan kendali keamanan yang cukup dan sesuai untuk melindungi aset informasi serta memberikan kepercayaan bagi para *stakeholders*-nya.
- Memperoleh panduan proses untuk mengimplementasikan kontrol terhadap keamanan informasi, agar dapat menjamin bahwa objek-objek keamanan tertentu telah dicapai.
- Memantapkan, menerapkan, menjalankan, memantau, meninjau ulang, memelihara, dan meningkatkan keamanan informasi.
- Memberikan acuan bagi auditor internal maupun eksternal dalam memastikan bahwa organisasi telah mematuhi aturan-aturan, memiliki arah pengembangan manajemen dan standar-standar yang dilaksanakan.

- Merupakan sarana publikasi yang positif untuk meraih kepercayaan *stakeholders* karena penetapan ISO/IEC 27001:2005 akan menunjukkan kepada pelanggan, patner dan pihak pemerintah bahwa kualitas pelayanan dan keamanan yang baik dalam proses bisnis telah dikendalikan dengan benar.

1.6 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir dibagi menjadi 5 bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang menjelaskan latar belakang, tujuan tugas akhir, manfaat tugas akhir, perumusan masalah, batasan masalah, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi kajian pustaka yang mendasari penulis dalam melakukan penelitian, antara lain: Keamanan Informasi, informasi yang perlu dilindungi keamanannya, SMKI, PDCA, Identifikasi Risiko, Sistem Manajemen Mutu (SMM) ISO 9001, standardisasi SMKI dan ISO 27001:2005.

BAB III METODOLOGI

Bab ini menggambarkan uraian dan urutan pekerjaan yang akan dilakukan dalam penyusunan tugas akhir ini.

BAB IV PEMBUATAN DOKUMENTASI

Bab ini menerangkan pembuatan dokumentasi SMKI mulai dari tahap persiapan hingga tahap pelaksanaan SMKI.

BAB V PENUTUP

Bab ini berisi rangkuman hasil akhir dari pembuatan Tugas Akhir berupa simpulan dan dilengkapi dengan saran-saran untuk perbaikan ataupun penelitian selanjutnya.

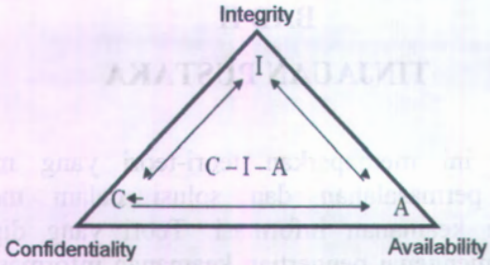
BAB II

TINJAUAN PUSTAKA

Bab ini memaparkan teori-teori yang mendasari munculnya permasalahan dan solusi dalam menangani perlindungan keamanan informasi. Teori yang dipaparkan diantaranya mengenai pengertian keamanan informasi sampai dengan *framework* yang dipakai dalam menunjang pembuatan SMKI.

2.1 Keamanan Informasi

Keamanan informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki dengan fokus utama pada data dan informasi. Sedangkan keamanan teknologi informasi mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan[1]. Usaha-usaha yang dilakukan dalam pengamanan informasi diantaranya dengan merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan penggunaan data dan informasi. Pengamanan informasi bertujuan agar data dan informasi digunakan sesuai dengan fungsinya dan tidak disalahgunakan. Keamanan informasi diperoleh dengan mengimplementasikan seperangkat alat kontrol yang layak, seperti kebijakan, praktek-praktek, prosedur, struktur organisasi dan perangkat lunak. Keamanan informasi sendiri mengandung tiga aspek untuk dikategorikan dalam keadaaan aman. Demikian adalah gambaran dari ketiga aspek tersebut:



Gambar 2. 1 Elemen-elemen keamanan informasi[2]

Elemen-elemen keamanan informasi pada Gambar 2.1 meliputi:

1. Kerahasiaan *(Confidentiality)* adalah aspek yang menjamin kerahasiaan data dan informasi. Aspek ini menjamin kerahasiaan data yang dikirim, diterima dan disimpan serta memastikan hanya dapat diakses oleh pihak yang berwenang.
2. Integritas *(Integrity)* adalah aspek yang menjamin bahwa data tidak diubah tanpa ijin dari pihak yang tidak berwenang. Aspek ini berfungsi dalam menjaga keakuratan dan keutuhan informasi serta metode prosesnya.
3. Ketersediaan *(Availability)* adalah aspek yang menjamin bahwa data tersedia pada saat dibutuhkan dan memastikan informasi serta perangkat terkait hanya berhak digunakan oleh yang berkepentingan.

2.2 Informasi yang perlu dilindungi keamanannya

Keamanan informasi adalah perlindungan informasi terhadap sistem dan perangkat yang digunakan, penyimpanan serta pengiriman informasi. Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan proses dan mengurangi kerusakan akibat terjadinya ancaman. Terdapat beberapa jenis keamanan yang harus dilindungi dalam upaya pengamanan informasi secara

keseluruhan. Demikian dijelaskan jenis keamanan yang berkontribusi dalam keamanan informasi[1] :

- Keamanan fisik *(Physical Security,* berfokus pada strategi untuk mengamankan personil, aset fisik, dan tempat kerja dari berbagai ancaman seperti bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- Keamanan personal *(Personal Security),* merupakan bagian dari keamanan fisik yang berfokus pada perlindungan terhadap sumber daya manusia dalam organisasi.
- Keamanan Operasi *(Operation Security),* berfokus pada strategi pengamanan yaitu kemampuan organisasi atau perusahaan dalam bekerja tanpa gangguan.
- Keamanan Komunikasi *(Communications Security),* bertujuan untuk mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat-alat tersebut dalam mencapai tujuan organisasi.
- Keamanan Jaringan (*Network Security)*, berfokus pada pengamanan peralatan jaringan data organisasi, isi, serta kemampuan untuk menggunakan jaringan.

2.3 Sistem Manajemen Keamanan Informasi (SMKI)

SMKI adalah keseluruhan sistem manajemen, berdasarkan pendekatan risiko bisnis yang bertujuan untuk memantapkan, menerapkan, menjalankan, memantau, meninjau ulang, memelihara, dan meningkatkan keamanan informasi[3]. Perancangan SMKI digunakan untuk memastikan pemilihan kendali keamanan yang sesuai untuk melindungi aset informasi serta memberikan kepercayaan bagi *stakeholders*. SMKI sendiri meliputi struktur organisasi, kebijakan, rencana kegiatan, tanggung jawab dan wewenang, prosedur, proses serta sumber daya yang masing-masing dapat dijelaskan sebagai berikut:

- Struktur organisasi, biasanya berupa keberadaan fungsi-fungsi atau jabatan organisasi.
- Kebijakan keamanan, berupa peraturan yang mengatur pelaporan semua kejadian pelanggaran keamanan, kelemahan sistem informasi serta pengambilan langkah-langkah keamanan yang dianggap perlu dll.
- Prosedur dan proses, yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan, misal: prosedur permohonan ijin akses aplikasi.
- Tanggung jawab, yang dimaksud dengan tanggung jawab di sini adalah tercerminnya konsep dan aspek-aspek keamanan informasi perusahaan di dalam rincian tugas pekerjaan (*job description)* dalam setiap jabatan pada perusahaan.
- Sumber Daya Manusia, adalah pelaksana serta obyek pengembangan keamanan informasi di perusahaan.

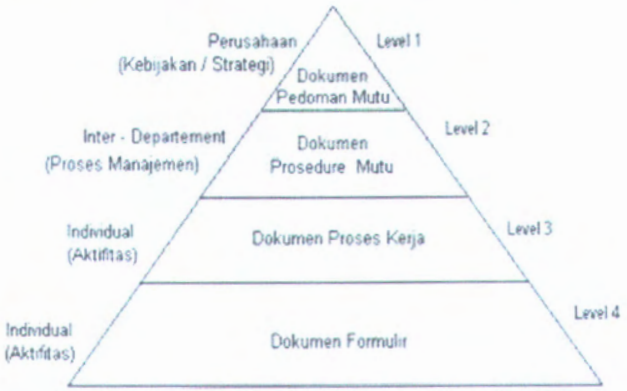
Tahap pendokumentasian SMKI mengadopsi tahap pendokumentasian SMM. Setiap aktivitas dan proses yang dilakukan pada SMKI merupakan representasi dari siklus hidup PDCA. Salah satu proses yang penting dari SMKI adalah proses identifikasi risiko yang bertujuan untuk mengetahui prosedur-prosedur apa saja yang perlu dibuat untuk mengamankan dan melindungi aset informasi organisasi. Demikian merupakan penjelasan lebih lanjut mengenai SMM, PDCA dan identifikasi resiko:

2.3.1 Sistem Manajemen Mutu ISO 9001

Mutu adalah perpaduan sifat-sifat dan karakteristik yang menentukan sampai seberapa jauh keluaran yang dihasilkan suatu perusahaan atau organisasi dapat memenuhi kebutuhan pembelinya[4]. Tujuan mutu sendiri adalah memberikan keyakinan bahwa produk atau jasa yang dihasilkan perusahaan memenuhi persyaratan mutu pembeli. Sistem mutu mencakup jaminan mutu dan pengendalian mutu. Jaminan mutu adalah istilah untuk

menyatakan kesuluruhan kegiatan yang terencana dan resmi dalam rangka memberi kepercayaan bahwa output yang dimaksud akan memenuhi tingkat mutu yang diinginkan[5]. Sistem mutu sendiri adalah program perencanaan kegiatan sumber daya yang didorong oleh manajemen dan berlaku di seluruh organisasi.

ISO 9001 merupakan standar utama bagi perusahaan yang ingin memberikan jaminan mutu kepada pelanggannya. Standar yang dimaksudkan mencakup keseluruhan tahapan proses mulai dari desain, pengembangan produksi, instalasi sampai dengan jasa. Penerapan sistem mutu yang efektif pada suatu organisasi memerlukan sistem yang terstruktur dan terdokumentasi dengan baik. Pembuatan dokumentasi SMM sendiri dipandang sebagai kegiatan yang memberikan nilai tambah dan bukan menjadi tujuan akhir dari pembuatan SMM. Terdapat beberapa tahapan dalam proses pendokumentasian SMM yang sering disebut dengan piramida dokumentasi SMM. Piramida dokumentasi inilah yang kemudian diadosi dalam penyusunan dokumentasi SMKI. Berikut gambarannya:



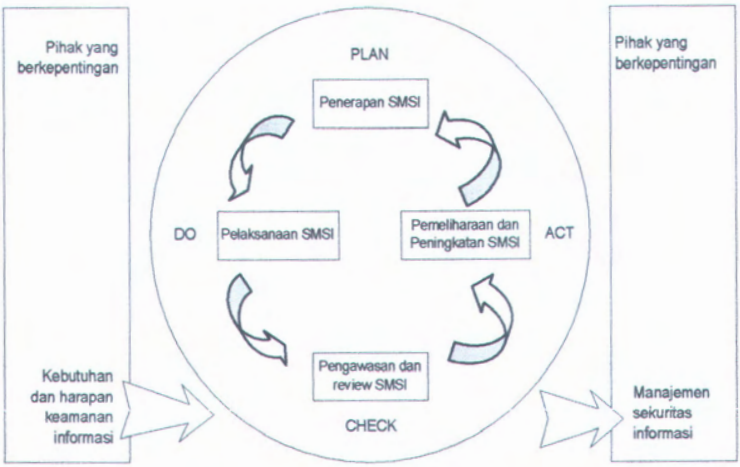
Gambar 2. 2 Piramida Dokumentasi SMM[6]

Dari gambar 2.2 dapat dijelaskan masing-masing tahapan pada proses dokumentasi SMM:

a. Pedoman mutu/manual mutu merupakan kunci utama dalam dokumentasi sistem. Panduan mutu menerangkan dengan jelas kepada setiap orang mengenai komitmen perusahaan terhadap mutu dengan cara memberikan pandangan kedepan, kebijakan, tujuan mutu, sistem-sistem, prosedur dan metodologi.
b. Prosedur mutu, adalah prosedur yang menjelaskan langkah serta mekanisme pelaksanaan semua proses aktifitas dalam sistem penjaminan mutu yang melibatkan berbagai fungsi[7].
c. Instruksi kerja, tidak terdapat format khusus dalam pembuatannya, hanya berupa urutan langkah demi langkah. Instruksi kerja dapat berupa narasi, diagram alir, gambar dll.
d. Formulir, merupakan dokumen berupa catatan mutu sebagai bukti hasil kerja masing - masing proses yang ada, contohnya: daftar induk dokumen, rekaman audit internal, rekaman tinjauan manajemen, *checklist* produksi, laporan harian produksi dll[6].

2.3.2 Model Plan-Do-Check-Act (PDCA)

PDCA adalah suatu proses pemecahan masalah yang digunakan dalam pengendalian mutu[8]. Metode ini dipopulerkan oleh W. Edwards Deming, yang dianggap sebagai bapak pengendalian mutu modern, sehingga sering disebut dengan siklus Deming. Input dalam model ini berupa kebutuhan keamanan informasi dan ekspektasi/harapan, sedangkan output yang dihasilkan berupa pengaturan keamanan informasi. Demikian pada gambar 2.3 ditunjukkan siklus PDCA:



Gambar 2. 3 Model PDCA[9]

Penjelasan dari siklus PDCA adalah sebagai berikut:

1. PLAN *(Established ISMS)*

   Tahap *plan* adalah tahap penyusunan rencana yang akan dilakukan, penentuan masalah yang akan diatasi, kelemahan yang akan diperbaiki serta pencarian solusi untuk mengatasi masalah. Adapun penerapan tahap *plan* dapat mengikuti langkah-langkah berikut:

   b. Memilih masalah atau proses yang dapat dipecahkan terlebih dahulu, kemudian menguraikan faktor-faktor yang dipecahkan dan melakukan perbaikan proses pada masalah tersebut.
   c. Menguraikan proses yang berlaku dalam permasalahan tersebut.
   d. Menguraikan semua hal yang menjadi penyebab timbulnya masalah dan sesuai dengan akar permasalahannya.
   e. Mengembangkan cara pemecahan masalah atau perbaikan efektif yang dapat dilaksanakan.

2. DO *(implement and operate the ISMS)*
   Tahap *Do* adalah tahap dimana solusi dan perubahan dari proses yang telah direncanakan dilaksanakan. Pelaksanaan yang dilakukan adalah penerapan prosedur-prosedur serta instruksi kerja sesuai dengan aktivitas yang terjadi dalam organisasi. Pelaksanaan tahap *do* diantaranya dapat mengikuti langkah sebagai berikut:
   a. Mencoba solusi yang ditemukan pada skala kecil terlebih dahulu.
   b. Mengikuti rencana dan memantau proses serta hasilnya.
   c.Mengadakan penyesuaian cara atau proses bila diperlukan.
3. Check *(monitor and review the ISMS)*
   Tahap pengecekkan adalah tahapan untuk meneliti apa yang telah dilaksanakan dan menemukan kelemahan-kelemahan yang perlu diperbaiki. Berdasarkan kelemahan-kelemahan tersebut kemudian disusun rencana perbaikan. Langkah-langkah yang dapat dilakukan dalam tahap *check* ini adalah sebagai berikut:
   a. Membuat alat atau cara untuk memantau pelaksanaan proses dan hasilnya.
   b. Mengkonfirmasi bahwa cara atau alat tersebut absah digunakan.
   c. Memastikan apakah solusi tersebut mendatangkan dampak yang diinginkan.
   d. Memastikan apakah ada konsekuensi yang tidak diharapkan.
4. ACT *(maintain and improve the ISMS)*
   Tahap berikut ini adalah usaha perbaikan berdasarkan hasil perubahan, meliputi pengambilan langkah korektif dan *preventif* berdasarkan hasil dari audit internal SMKI, tinjauan manajemen atau informasi lain yang relevan.

Langkah-langkah yang dapat dilakukan dalam tahap ini adalah sebagai berikut:

a. Menilai hasil-hasil yang dicapai, termasuk proses pemecahan masalah dan perubahan proses yang direkomendasikan.
b. Meneruskan perbaikan proses bila perlu.

2.3.3 Analisa Risiko

Penerapan TI untuk mendukung operasional sebuah organisasi atau perusahaan memberi dampak yang sangat besar terhadap kinerja organisasi. Semakin besar ketergantungan suatu organisasi terhadap TI semakin besar pula kerugian yang akan dihadapi organisasi tersebut bila terjadi kegagalan sistem informasinya. Bentuk kegagalan fungsi sistem informasi ini dapat beraneka ragam, mulai dari gangguan listrik, serangan *hacker*, virus, pencurian data, *denial of services attack* (DOS), bencana alam hingga serangan teroris.

Perkembangan ini melahirkan beberapa metodologi untuk mengidentifikasi risiko kemungkinan kerusakan aset-aset pendukung proses bisnis organisasi. Oleh karena itu dibutuhkan prediksi besarnya kerugian yang mungkin terjadi sehingga hasil dari identifikasi tersebut dapat digunakan untuk membangun strategi penanganan risiko. Secara umum terdapat dua metode identifikasi risiko *(Risk Analysis)*, yaitu[10]:

1. **Kuantitatif**; Identifikasi berdasarkan angka-angka nyata (nilai finansial) terhadap biaya pembangunan keamanan dan besarnya kerugian yang terjadi. identifikasi kuantitatif membantu dalam menghilangkan keraguan yang meliputi estimasi waktu dan biaya serta keraguan personal.
2. **Kualitatif**; identifikasi kualitatif meliputi kegiatan dan mengenali faktor risiko dilengkapi dengan perkiraan yang menjelaskan masing-masing risiko dan dampaknya.

2.4 Standardisasi SMKI

Terdapat berbagai macam *framework* untuk menunjang pembuatan SMKI. Demikian disebutkan beberapa *framework* dalam pembuatan SMKI:

Tabel 2. 1 Framework SMKI[3]

Area	COBIT	ITIL	ISO 27001
Fungsi	Memetakan proses TI	Memetakan IT service level management	*Framework* Keamanan informasi
Area	4 proses dan 34 domain	9 proses	10 domain
Pengaju	ISACA	OGC	ISO Board
implementasi	Audit keamanan informasi	Mengelola *service level*	Pemenuhan standar keamanan
Konsultan	Perusahaan accounting, perusahaan konsultan IT	Perusahaan konsultan IT	Perusahaan konsultan IT, keamanan perusahaan, konsultan jaringan

Control Objective for Information and related Technology (COBIT), adalah suatu panduan standar praktik manajemen TI. Standar COBIT dikeluarkan oleh *IT Governance Institute* yang merupakan bagian dari ISACA yang merupakan suatu organisasi profesi internasional di bidang tata kelola TI. ISACA didirikan di Amerika Serikat pada tahun 1967. COBIT memiliki 4 cakupan, yaitu[11]:

- Perencanaan dan organisasi (*plan and organise*)
- Pengadaan dan implementasi (*acquire and implement*)
- Pengantaran dan dukungan (*deliver and support*)

- Pengawasan dan evaluasi (*monitor and evaluate*)

Information Technology Infrastructure Library (ITIL) adalah suatu rangkaian konsep dan teknik pengelolaan infrastruktur, pengembangan, serta pengoperasian teknologi informasi. ITIL memberikan deskripsi detail mengenai beberapa praktek TI yang penting melalui daftar cek, tugas, serta prosedur yang menyeluruh yang disesuaikan dengan segala jenis organisasi TI. Pada 30 Juni 2007, OGC *(United Kingdom's Office of Government Commerce)* menerbitkan versi ketiga ITIL (ITIL v3) yang terdiri dari lima bagian dan lebih menekankan pada pengelolaan siklus hidup layanan yang disediakan oleh TI. Kelima bagian tersebut sering disebut dengan siklus hidup ITIL yang meliputi[12]:

1. *Service Strategy*
   Digunakan sebagai panduan untuk melakukan *review* strategis bagi semua proses dan perangkat (peran, tanggung jawab, teknologi pendukung, dll).
2. *Service Design*
   Berisi prinsip-prinsip dan metode-metode desain untuk mengkonversi tujuan-tujuan strategis organisasi TI dan bisnis menjadi portofolio/koleksi layanan TI serta aset-aset layanan, seperti *server, storage* dan sebagainya.
3. *Service Transition*
   Menyediakan panduan kepada organisasi TI untuk dapat mengembangkan kemampuan dalam mengubah hasil desain layanan TI, baik yang baru maupun yang telah dirubah spesifikasinya dalam lingkungan operasional.
4. *Service Operation*
   Merupakan tahapan *lifecycle* yang mencakup semua kegiatan operasional harian dan pengelolaan layanan TI. Di dalamnya terdapat berbagai panduan bagaimana mengelola layanan TI secara efisien dan efektif serta menjamin tingkat kinerja yang telah dijanjikan dengan pelanggan sebelumnya.

5. *Continual Service Improvement*

Mengkombinasikan berbagai prinsip dan metode dari manajemen mutu, salah satunya adalah *Plan-Do-Check-Act* (PDCA) atau yang dikenal sebagi siklus Deming.

Organisasi Internasional untuk Standardisasi (ISO) adalah badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standar nasional setiap negara. ISO menetapkan standar-standar industrial dan komersial dunia[13]. Meski ISO adalah organisasi nonpemerintah, kemampuannya untuk menetapkan standar yang sering menjadi hukum melalui persetujuan atau standar nasional membuatnya lebih berpengaruh daripada kebanyakan organisasi non-pemerintah lainnya. Penerapan ISO di suatu perusahaan berguna untuk:

- Meningkatkan citra perusahaan.
- Meningkatkan kinerja lingkungan perusahaan.
- Meningkatkan efisiensi kegiatan.
- Memperbaiki manajemen organisasi dengan menerapkan perencanaan, pelaksanaan, pengukuran dan tindakan perbaikan (*plan, do, check, act*).
- Meningkatkan penataan terhadap ketentuan peraturan perundang-undangan dalam hal pengelolaan lingkungan.
- Mengurangi ancaman risiko.
- Meningkatkan daya saing.
- Meningkatkan komunikasi internal dan hubungan baik dengan berbagai pihak yang berkepentingan.
- Mendapat kepercayaan dari konsumen/mitra kerja/pemodal.

2.5 ISO/IEC 27001: 2005

ISO/IEC 27001 adalah standar keamanan informasi yang diterbitkan pada bulan oktober 2005 oleh *International Organization for Standardization* dan *International Electrotechnical Commission* yang mencakup semua jenis organisasi seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba. ISO/IEC 27001:2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, mengidentifikasi dan memelihara serta mendokumentasikan SMKI berdasarkan identifikasi risiko bisnis. Standar ini juga menjadi standar dalam penerapan SMKI yang paling banyak dipakai oleh organisasi karena berbasiskan kontrol[13].

ISO/IEC 27001 mendefinisikan keperluan-keperluan untuk membangun SMKI. SMKI yang baik akan membantu memberikan perlindungan pengamanan informasi yang berkaitan dengan proses bisnis terhadap risiko kerugian/bencana dan kegagalan. Implementasi SMKI akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam waktu yang tidak lama. Tujuan kontrol yang digunakan dari ISO 27001 merupakan adoPKI dari ISO 17799. Dalam setiap proses pembuatan SMKI mengandung siklus PDCA. Demikian hubungan antara PDCA, isi ISO 17799 dan ISO 27001:

Tabel 2. 2 Hubungan PDCA, ISO 17799 dan ISO 27001:2005[14]

Asosiasi dengan PDCA	Standard	Klausul	Judul
KESELURUHAN	7799-2	4.1	Persyaratan Umum
	9001	4.1	
	7799-2	4.3	Persyaratan dokumentasi yang mencakup kontrol dokumen dan kontrol rekaman
	9001	4.2.1	
	9001	4.2.3	
	9001	4.2.4	
	7799-2	5.1	Komitmen Manajemen

Tabel 2. 3 Hubungan PDCA, ISO 17799 dan ISO 27001:2005 (lanjutan)

Asosiasi dengan PDCA	Standard	Klausul	Judul
KESELURUHAN	9001	5.1	Komitmen Manajemen
	9001	8.1	Pengukuran, analisis dan peningkatan (umum)
	7799	4.2.4	
	9001	5.5	Tanggung jawab, hak dan komunikasi
PLAN	9001	5.2	Fokus Pelanggan
	7799-2	4.2.1	Penerapan SMKI (termasuk kebijakan dan identifikasi risiko)
	9001	6.3	Infrastruktur
	9001	5.4	Perencanaan
	9001	4.2.2	Manual mutu
	9001	5.3	Kebujakan Muti
	9001	6.4	Lingkungan Kerja
DO	9001	8.3	Kontrol ketidaksesuaian
	9001	6.2	Sumber Daya Manusia
	7799-2	4.2.2	Penerapan dan pengoperasian SMKI
	9001	6.1	Persyaratan sumber daya
	7799-2	5.2	Manajemen Sumber Daya
CHECK	9001	8.4	Analisis data
	9001	5.6	Tinjauan Manajemen
	7799-2	6	
	7799-2	4.2.3	Pengawasan dan peninjauan ulang SMKI
	9001	8.2	Pengawasan dan pengukuran
ACT	7799	8.5	Peningkatan
	7799	4.2.4	
	9001	7	

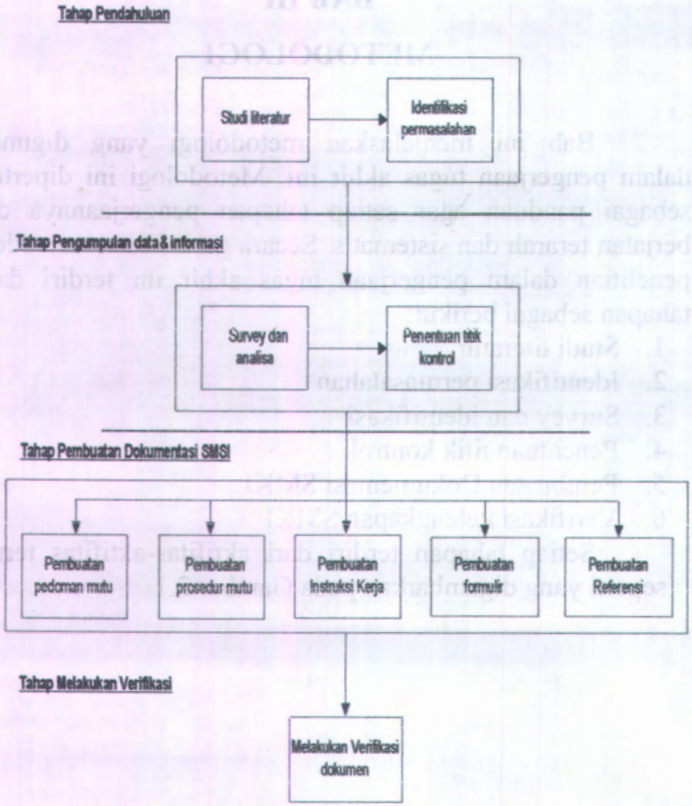
BAB III

METODOLOGI

Bab ini menjelaskan metodologi yang digunakan dalam pengerjaan tugas akhir ini. Metodologi ini diperlukan sebagai panduan agar setiap tahapan pengerjaannya dapat berjalan terarah dan sistematis. Secara garis besar, metodologi penelitian dalam pengerjaan tugas akhir ini terdiri dari 6 tahapan sebagai berikut:

1. Studi literatur
2. Identifikasi permasalahan
3. Survey dan identifikasi
4. Penentuan titik kontrol
5. Pembuatan Dokumentasi SMKI
6. Verifikasi kelengkapan SMKI

Setiap tahapan terdiri dari aktifitas-aktifitas tertentu seperti yang digambarkan pada Gambar 3.1



Gambar 3. 1 Metodologi Penelitian

Berikut adalah penjelasan dari masing-masing tahapan pada Gambar 3.1:

3.1 Studi Literatur

Studi Literatur yang dilakukan dalam pembuatan tugas akhir ini adalah pembelajaran literatur yang terkait dengan permasalahan yang ada, seperti pembelajaran mengenai keamanan informasi, SMM, proses pembuatan SMKI serta standar yang digunakan dalam pembuatan SMKI.

Pembelajaran tersebut dilakukan melalui pencarian berbagai macam literatur yang relevan dan terkait dengan pembuatan SMKI. Literatur terutama didapatkan dari dokumen maupun sumber bacaan *softcopy* dari internet dan buku.

3.2 Identifikasi Permasalahan

Setelah didapatkan berbagai macam informasi yang cukup dan relevan pada tahap studi literatur, selanjutnya dilakukan identifikasi permasalahan untuk membatasi masalah yang dibahas dalam pengerjaan tugas akhir ini. Identifikasi permasalahan berguna untuk melakukan identifikasi terhadap titik-titik yang dijadikan obyek penelitian. Obyek penelitian tugas akhir ini adalah kemananan informasi dari SIM akademik BAAK..

3.3 Survey dan Identifikasi

Tahap ini digunakan untuk memahami keadaaan dan kondisi dari obyek penelitian yaitu, BAAK pada umumnya dan SIM akademik pada khususnya. Metode yang digunakan dalam pengumpulan data adalah sebagai berikut:

3.3.1 *Review* Dokumen

Metode ini berguna dalam memberikan petunjuk mengenai sistem yang ada saat ini. Bentuk dokumen yang biasa digunakan dalam *review* dokumen adalah[15]:

- Form
- Laporan
- Panduan kebijakan

3.3.2 Wawancara

Sebelum dilakukan wawancara biasanya diperlukan persiapan berupa pemilihan narasumber dengan perspektif berbeda dan disesuaikan dengan informasi yang diinginkan. Hal-hal yang perlu disiapkan dalam melakukan wawancara diantaranya[15]:

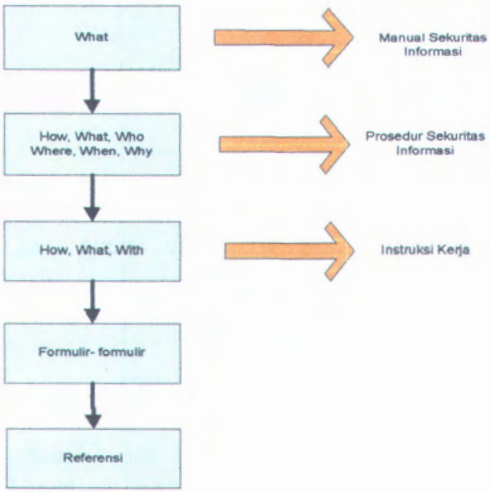
- Menyiapkan rencana umum *interview* seperti daftar pertanyaan dan antisipasi jawaban serta tindak lanjutnya.
- Melakukan konfirmasi pengetahuan narasumber.
- Menetapkan prioritas waktu dalam melakukan wawancara.
- Mempersiapkan sumber informasi diantaranya jadwal, pemberitahuan alasan *interview* dan area yang akan didiskusikan.

3.4 Penentuan Titik Kontrol

Pernentuan titik kontrol merupakan tahapan yang penting dalam pembuatan SMKI. SMKI sendiri dibangun berdasarkan pendekatan risiko bisnis. Dalam penentuan titik kontrol terdapat dua bagian utama yaitu identifikasi proses bisnis SIM akademik dan analisa risiko terhadap aset yang berkaitan dengan aplikasi SIM akademik. Dalam proses analisa risiko terdapat tahapan penilaian dan penentuan level risiko terhadap ancaman risiko yang mungkin muncul. Penilaian risiko bertujuan untuk menemukan kontrol-kontrol dalam mencegah terjadinya risiko serta mengetahui dan menentukan prosedur yang akan dibuat.

3.5 Pembuatan Dokumentasi SMKI

Organisasi menunjuk dan membentuk suatu tim pelaksana yang bertanggung jawab terhadap pembuatan, pengelolaan sampai dengan peningkatan SMKI. Pembuatan dokumentasi SMKI sendiri mengadopsi pembuatan dokumentasi SMM seperti yang ditunjukkan pada Gambar 3.2.



Gambar 3. 2 Struktur Pembuatan Dokumentasi SMKI

Berikut adalah penjelasan dari Gambar 3.2 yang merupakan isi dari dokumentasi SMKI:

3.5.1 Pembuatan Manual Keamanan Informasi (MKI)

Merupakan langkah awal dalam pembuatan dokumentasi SMKI yang berisi komitmen organisasi terhadap penerapan keamanan informasi dan pemenuhan persyaratan standar SMKI yang dipilih. MKI memberikan pandangan kedepan bagi organisasi mengenai kebijakan, tujuan keamananan informasi, sistem-sistem, prosedur dan metodologinya.

3.5.2 Pembuatan Prosedur Keamanan Informasi (PKI)

PKI berisi uraian urutan pekerjaan/langkah-langkah kegiatan yang saling terkait satu sama lain. PKI dilengkapi dengan identifikasi terhadap aktivitas-aktivitas yang bersifat kritis, dimana pendokumentasian prosedur akan menunjang pelaksanaan proses secara konsisten. Proses pembuatan PKI tidak memiliki format khusus, melainkan dibuat sesuai dengan kronologis fungsi-fungsi dalam perusahaan yang meliputi:

- Tujuan
- Ruang lingkup
- Standar atau klausul
- Kriteria keberhasilan
- Rincian prosedur (PDCA)
- Rekaman mutu yang biasanya digunakan dalam laporan penilikan, data pengujian, pengesahan laporan, laporan audit dsb.
- Istilah dan definisi
- Catatan perubahan.

3.5.3 Pembuatan Instruksi Kerja (IK)

Instruksi kerja dibuat secara sederhana, praktis dan mudah untuk dipahami, hal ini dikarenakan instruksi kerja ditujukan bagi pengguna yang berada pada posisi pelaksana. Uraian dari instruksi kerja meliputi hal-hal berikut:

- Tahap pelaksanan pekerjaan,
- Alat yang digunakan,
- Standar atau parameter, metode pengukuran, pengujian dan pemeriksaan yang digunakan,
- Sumber daya pendukung lain.

3.5.4 Pembuatan Formulir-formulir

Merupakan dokumen berupa catatan/rekaman sebagai bukti hasil kerja proses yang ada, contohnya: daftar induk dokumen, rekaman audit internal, rekaman tinjauan manajemen dll.

3.5.5 Pembuatan Referensi

Merupakan dokumen kelengkapan SMKI yang terdiri dari dokumen struktur organisasi, uraian tugas, proses bisnis, kebijakan keamanan informasi, laporan perkiraan risiko, sasaran keamanan informasi, rencana keamanan informasi, daftar dokumentasi SMKI, *statement of applicability*, daftar contoh stempel dan rencana pengelolaan risiko.

3.6 Verifikasi SMKI

Tahap verifikasi SMKI dilakukan untuk mengetahui kelengkapan dokumentasi SMKI yang telah dibuat terhadap persyaratan ISO 27001:2005. Persyaratan kelengkapan dokumen terdapat pada klausul 4.3.1 ISO 27001:2005.

Halaman ini sengaja dikosongkan.

BAB IV
PEMBUATAN SMKI

Bab ini membahas pembuatan SMKI, mulai dari tahap pembentukan tim pelaksana, pembuatan dokumentasi sampai dengan gambaran pelaksanaan SMKI. Hasil dari dokumentasi SMKI pada tugas akhir ini akan dibuat menjadi buku tersendiri di luar buku tugas akhir ini.

4.1 Survey dan Identifikasi

Tahap survey dan identifikasi dilakukan untuk melakukan pemahaman mengenai permasalahan dan proses bisnis dari SIM akademik BAAK. Survey dilakukan menggunakan metode *review* dokumen dan wawancara terhadap beberapa staf dari BAAK dan PUSKOM. Demikian penjelasan dari masing-masing metodenya:

4.1.1 *Review* Dokumen

Dalam pencarian informasi *(gathering information) review* dokumen selalu menempati tahapan utama, karena dapat memberikan gambaran mengenai sistem yang ada saat ini secara obyektif.

Demikian adalah dokumen-dokumen yang di *review*:

- Dokumen Sistem Manajemen Mutu Kantor Pusat Administrasi ITS
- Standar operasi dan prosedur BAAK PCPT 2006.
- *Job Description* bagian Pendidikan & Kerjasama BAAK ITS
- Website BAAK.

Melalui tahapan *review* dokumen yang telah dilakukan diperoleh informasi mengenai visi dan misi, struktur organisasi, serta gambaran proses bisnis secara global dari BAAK.

4.1.2 Wawancara

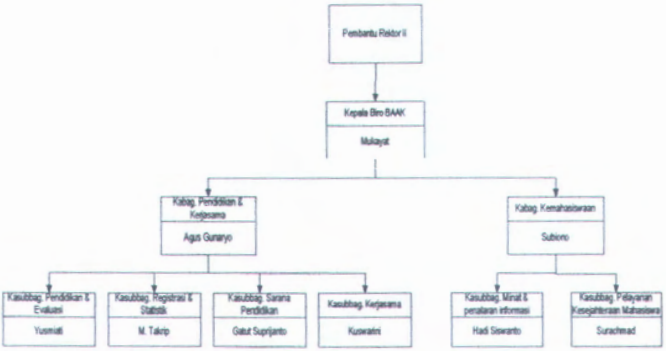
Wawancara dilakukan pada beberapa staf di sub bagian BAAK yang berkaitan langsung dengan SIM akademik dan UPT. PUSKOM. UPT. PUSKOM bertugas mengurusi teknis dari aplikasi SIM akademik. Melalui tahapan wawancara diharapkan dapat diperoleh informasi mengenai gambaran proses bisnis, aset-aset pendukung serta informasi mengenai permasalahan dan ancaman yang berkaitan dengan keamanan informasi SIM akademik. Daftar pertanyaan dibuat berdasarkan pemetaan terhadap tujuan kontrol yang terdapat pada Annex A ISO 27001:2005. Daftar pertanyaan dan jawaban terdapat pada lampiran A.

4.2 Penentuan Titik Kontrol

Dalam melakukan penentuan titik kontrol terdapat 2 bagian utama yaitu identifikasi proses bisnis dan identifikasi aset aplikasi SIM akademik. Demikian penjelasan dari masing-masing bagian tersebut:

4.2.1 Identifikasi Proses Bisnis

BAAK adalah suatu organisasi yang bertugas melayani segala kegiatan administrasi kemahasiswaan di ITS. Sebagaimana layaknya sebuah organisasi, BAAK juga memiliki struktur organisasi dan memiliki pembagian tugas yang jelas pada masing-masing sub bagian. Bagian yang berkaitan langsung dengan proses SIM akademik adalah bagian Pendidikan dan Kerjasama yang memiliki 4 sub bagian. Dari keempat sub bagian ini hanya 3 sub bagian yang memiliki wewenang terhadap SIM akademik yaitu, sub bagian Registrasi dan Statistik, sub bagian Pendidikan dan Evaluasi serta sub bagian Sarana Pendidikan. Demikian digambarkan struktur organisasi dari BAAK



Gambar 4. 1 Struktur organisasi BAAK

Proses bisnis sendiri adalah suatu rangkaian atau kumpulan pekerjaan yang saling terkait untuk menyelesaikan suatu masalah tertentu. Suatu proses bisnis dapat dipecah menjadi beberapa subproses, yang masing-masing memiliki kontribusi untuk mencapai tujuan dari super prosesnya[10].

BAAK belum memiliki dokumentasi gambaran umum mengenai proses bisnis yang dilakukannya terutama untuk proses SIM akademik. Oleh karena itu penulis mencoba memberikan gambaran umum berdasarkan pemotretan dari deskriPKI kerja *(job description)* pada bagian Pendidikan & Kerjasama. Untuk mempermudah penggambaran proses serta pemahamannya maka proses bisnis dibedakan menjadi tiga proses yaitu proses utama, proses penunjang dan proses manajemen. Berikut adalah penjelasan dari masing-masing proses:

- Proses utama adalah proses yang berkaitan langsung dengan pelayanan jasa yang diberikan BAAK kepada para *stakeholders*-nya. Apabila terdapat gangguan terhadap proses utama ini maka dampaknya akan sangat besar terhadap proses pelayanan SIM akademik secara keseluruhan.

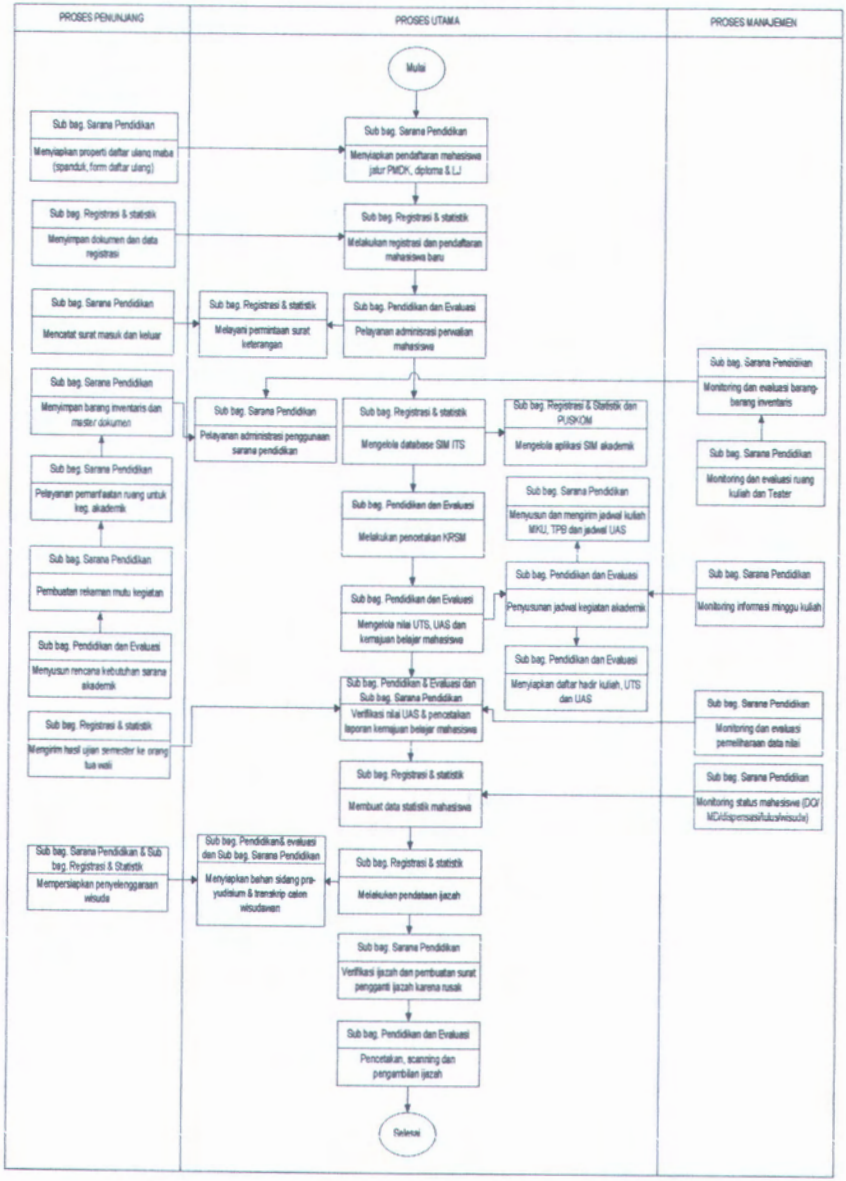
- Proses penunjang merupakan aktivitas yang bertujuan untuk membantu terselenggaranya proses bisnis utama.
- Proses manajemen adalah proses penyusunan rencana, pengorganisasian dan pengendalian sumber daya yang ada. Dalam proses manajemen ini terdapat kegiatan pengawasan atau monitoring dan evaluasi.

Hasil dari penggambaran proses bisnis SIM akademik dapat dilihat pada Gambar 4.2.

4.2.2 Analisa Risiko

Analisa risiko adalah kegiatan yang menitik beratkan pada kemungkinan terjadinya ancaman, kelemahan serta dampak terhadap aset dan proses bisnis. Analisa risiko dilakukan untuk mengetahui ancaman berdasarkan aspek CIA terhadap aset-aset organisasi. Didalam proses analisa risiko terdapat proses identifikasi risiko yang dipergunakan untuk mengetahui dan mengukur seberapa besar dampak risiko terhadap nilai aset yang dapat berupa data, informasi, teknologi, personil/orang dan aset layanan.

Aset yang diidentifikasi dalam tugas akhir ini adalah aset pendukung aplikasi SIM akademik meliputi aset data mahasiswa, *hardware* dan *software* pendukung aplikasi SIM akademik serta kode program SIM akademik. Penggalian informasi dalam proses analisa dan identifikasi risiko ini menggunakan metode wawancara. Wawancara dititikberatkan pada ancaman-ancaman apa saja yang mungkin muncul dari aset-aset pendukung aplikasi SIM akademik. Daftar pertanyaan dan jawaban dapat dilihat pada lampiran A.



Gambar 4. 2 Proses Bisnis SIM akademik

Berikut adalah hasil dari identifikasi risiko yang memunculkan 9 ancaman yang merupakan ancaman aset-aset aplikasi SIM akademik.

Tabel 4. 1 Daftar Risiko

No.	Risiko
1.	Data mahasiswa hilang/rusak
2.	Aset fisik jaringan rusak
3.	Komputer server rusak
4.	Pencurian kode program
5.	Pencurian *password*
6.	Bencana Alam
7.	Server down
8.	Pemadaman Listrik
9.	Pengubahan data mahasiswa secara paksa

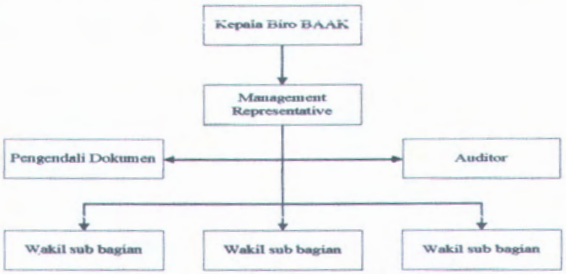
Setelah didapatkan ancaman risiko tersebut kemudian hasil dari identifikasi ini akan dilakukan penilaian dengan kriteria pengukuran tertentu seperti yang terdapat pada lampiran B. Berikut adalah hasil penilaian dari 9 ancaman risiko aplikasi SIM akademik:

Tabel 4. 2 Penilaian Risiko

Kecenderungan Ancaman	Dampak		
	Rendah **(10)**	***Sedang*** **(50)**	***Tinggi*** **(100)**
Sering **(1)**	Rendah	Sedang	Tinggi **5, 7**
Kadang-kadang **(0.5)**	Rendah	Sedang	Sedang **1, 2 dan 8**
Jarang **(0.1)**	Rendah	Rendah	Rendah **3, 4, 6, 9**

4.3 Pembuatan Dokumentasi SMKI

Sebelum melakukan pembuatan SMKI, organisasi menunjuk dan membentuk tim pelaksana pembuatan SMKI. Hal tersebut penting dilakukan karena SMKI merupakan suatu sistem keamanan yang penerapannya adalah tanggung jawab semua pihak mulai dari kepala BAAK sebagai pihak manajemen atas sampai dengan level yang paling bawah dalam struktur organisasi. Demikian digambarkan struktur organisasi tim pelaksana SMKI:



Gambar 4. 3 Struktur organisasi tim pelaksana SMKI

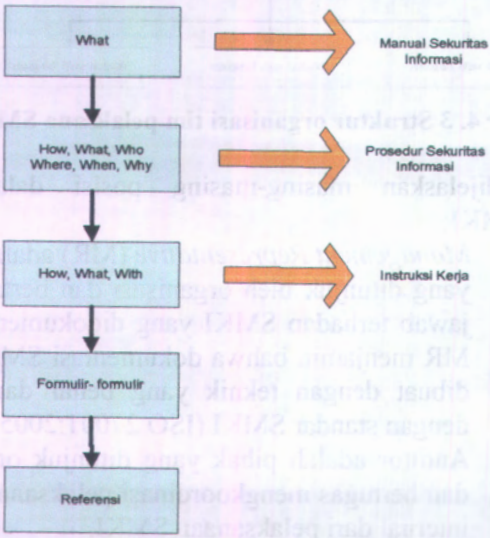
Demikian dijelaskan masing-masing posisi dalam tim pelaksana SMKI:

- *Management Representative* (MR) adalah orang yang ditunjuk oleh organisasi dan bertanggung jawab terhadap SMKI yang didokumentasikan. MR menjamin bahwa dokumentasi SMKI telah dibuat dengan teknik yang benar dan sesuai dengan standar SMKI (ISO 27001:2005).
- Auditor adalah pihak yang ditunjuk organisasi dan bertugas mengkoordinasi pelaksanaan audit internal dari pelaksanaan SMKI.
- Pengendali dokumen adalah seorang yang memiliki tanggung jawab mengendalikan seluruh dokumen keamanan informasi BAAK. Pengendali dokumen juga bertugas dalam penerapan SMKI, mulai dari mendistribusikan,

menyimpan, memelihara, menarik dokumen, menghancurkan dan memastikan bahwa dokumen keamanan informasi yang beredar adalah dokumen terkini.

- Wakil sub bagian merupakan perwakilan dari 3 sub bagian yang mengurusi SIM akademik dan bertindak sebagai pihak pelaksana pembuatan SMKI. Wakil sub bagian bertanggung jawab dalam membuat dan membangun SMKI di lingkungan sub bagiannya masing-masing.

Pembuatan dokumentasi SMKI didasarkan pada klausul 1 sampai dengan 8 yang terdapat pada ISO 27001:2005 dan mengadopsi piramida pembuatan dokumentasi SMM yang dapat dilihat pada Gambar 4.4



Gambar 4. 4 Struktur Pembuatan Dokumentasi SMKI

. Berikut adalah penjelasan dari masing-masing tahap dokumentasi SMKI:

4.3.1 Pembuatan Manual Keamanan Informasi

Pembuatan MKI bertujuan untuk menerangkan setiap personil mengenai komitmen organisasi terhadap keamanan informasi. Manual Keamanan ini memberikan pandangan kedepan mengenai kebijakan, tujuan Keamanan informasi, sistem-sistem, prosedur dan metodologi pembuatan SMKI. Terdapat 8 MKI dalam dokumentasi SMKI yang telah dibuat untuk BAAK, dengan rincian sebagai berikut:

- MKI PENDAHULUAN merujuk pada (MKI-01),
  Manual ini berisi latar belakang dibuatnya SMKI pada organisasi, serta siklus yang digunakan dalam proses pembuatan dan penerapan SMKI, yaitu siklus *Plan – Do – Check – Act* (PDCA).
- MKI RUANG LINGKUP merujuk pada (MKI-02)
  Dalam manual ini dijelaskan mengenai ruang lingkup sertifikasi SMKI, pengecualian penerapan dan acuan *normative* yang digunakan dalam dokumentasi SMKI.
- MKI ISTILAH & DEFINISI merujuk pada (MKI-03)
  Dokumentasi ini menjelaskan kata, definisi dan istilah yang digunakan dalam dokumentasi SMKI dengan tujuan untuk memudahkan pihak yang berkepentingan dan berwenang dalam membaca, menerapkan dan mengembangkan SMKI.
- MKI SISTEM MANAJEMEN KEAMANAN INFORMASI merujuk pada (MKI-04)
  Dokumentasi ini berisi mengenai penetapan & pengelolaan, pengimplementasian & pengoperasian, pengawasan & peninjauan ulang serta pengelolaan dan peningkatan SMKI. Keperluan dokumentasi lain yang diperlukan dalam SMKI juga diatur dalam manual ini.
- MKI TANGGUNG JAWAB MANAJEMEN merujuk pada (MKI-05)
  Dokumentasi ini berisi komitmen manajemen terhadap penetapan, pelaksanaan, pegoperasian, pengawasan,

peninjauan ulang dan peningkatan SMKI, penyediaan sumber daya serta memastikan bahwa seluruh personil yang terlibat dalam pengelolaan SMKI bertanggung jawab serta berkompeten dalam menjalankan tugasnya.

- MKI AUDIT INTERNAL merujuk pada (MKI-06)
  Pelaksanaan audit internal bertujuan untuk melakukan penyesuaian persyaratan standar internasional ISO 27001:2005 dengan peraturan dan kebijakan yang berlaku. Audit internal juga digunakan untuk melakukan penyesuaian kebutuhan keamanan informasi, memastikan keefektifan dan pengelolaan, serta memastikan penyelenggaraan dan proses sesuai dengan harapan dan tujuan SMKI. Pihak manajemen berkomitmen untuk melaksanakan audit internal minimal sekali dalam setahun.
- MKI TINJAUAN MANAJEMEN merujuk pada (MKI-07)
  Pembuatan manual tinjauan manajemen ini bertujuan untuk meninjau penerapan SMKI termasuk pengkajian peluang peningkatan serta kebutuhan pengubahan SMKI di organisasi. Kegiatan peninjauan ini sering disebut dengan Rapat Tinjauan Manajemen (RTM) yang dilaksanakan minimal sekali dalam setahun.
- MKI PENINGKATAN SMKI merujuk pada (MKI-08)
  Dokumentasi ini berisi mengenai peningkatan efektifitas penerapan SMKI dengan cara memperbaiki ketidaksesuaian yang timbul dalam penerapan SMKI. Di dalam dokumentasi ini juga terdapat pencegahan agar ketidaksesuaian dalam pelaksanaan SMKI tidak kembali muncul, sehingga efektifitas dari penerapan SMKI dapat terus meningkat.

4.3.2 Pembuatan Prosedur Keamanan Informasi

PKI merupakan uraian atau urutan pekerjaan yang mendukung MKI yang telah dijelaskan pada 4.3.1.

Dalam SMKI untuk BAAK ini terdapat 2 tipe prosedur yaitu prosedur yang mendukung operasional dari pihak manajemen dan prosedur untuk kegiatan teknis operasional. Tidak semua prosedur operasional teknis yang terkait dengan proses SIM akademik dapat dibuat. Prosedur yang dibuat terbatas pada prosedur yang digunakan untuk pengelolaan risiko yang belevel tinggi sebagaimana dijelaskan penilaian risiko pada LAPORAN PENILAIAN RISIKO RF-MR-05. Demikian prosedur-prosedur yang dibuat dalam SMKI untuk BAAK:

a. Prosedur pendukung operasional manajemen:

- PKI PENGENDALIAN DOKUMEN merujuk pada (PKI–MR–01)
  Prosedur ini dibuat untuk mengendalikan seluruh dokumen keamanan informasi yang dipergunakan dalam penerapan SMKI. Prosedur ini bertujuan agar dokumen-dokumen keamanan informasi adalah dokumen keamanan informasi dengan revisi terkini, mudah didapatkan, mudah diidentifikasi dan tersedia jika diperlukan. Dokumen yang dimaksudkan adalah dokumen internal (MKI, PKI, IK, Referensi dan Formulir) serta dokumen eksternal yang meliputi Peraturan Perundang-undangan, Surat Keputusan Rektor, dan sebagainya.
- PKI PENGENDALIAN REKAMAN KEAMANAN INFORMASI merujuk pada (PKI–MR–02)
  Prosedur ini digunakan untuk memastikan proses pengendalian rekaman agar dilaksanakan sesuai dengan prosedur yang berlaku. Prosedur ini juga digunakan untuk memastikan bahwa rekaman/catatan dapat dibaca, mudah diidentifikasi dan dicari, serta dapat digunakan sebagai bukti kesesuaian terhadap persyaratan dan efektifitas penerapan SMKI. PKI Pengaendalian Rekaman ini meliputi proses

identifikasi rekaman keamanan informasi, penetapan masa simpan rekaman, penetapan lokasi simpan, penetapan metode indeks penyimpanan rekaman serta pengendalian dan pemusnahan rekaman keamanan informasi yang kadaluarsa.

- PKI AUDIT INTERNAL merujuk pada (PKI-MR-10)

  Prosedur ini menjelaskan tata cara dalam melakukan proses audit internal untuk memastikan penerapan SMKI telah dilakukan secara konsisten dan memenuhi persyaratan yang telah ditetapkan serta mengarah pada perbaikan yang berkesinambungan. Prosedur ini meliputi perencanaan dan pelaksanaan audit internal, pembuatan laporan kesimpulan audit internal, verifikasi tindakan perbaikan & pencegahan serta tindak lanjut hasil temuan audit internal serta pelaporan hasil audit internal kepada manajemen puncak (Kepala BAAK ITS).
- PKI TINJAUAN MANAJEMEN merujuk pada (PKI-MR-11)

  Prosedur ini menjelaskan pelaksanaan tinjauan manajemen untuk memastikan kesinambungan, kecukupan & efektifitas penerapan SMKI. Prosedur ini meliputi perencanaan Rapat Tinjauan Manajemen (RTM), penetapan Agenda Tinjauan Manajemen, pelaksanaan RTM, pembuatan dan pengesahan Notulen/Risalah RTM serta tindak lanjut hasil – hasil RTM di BAAK ITS.
- PKI TINDAKAN PERBAIKAN & PENCEGAHAN merujuk pada (PKI-MR-12).

  Prosedur ini menjelaskan tata cara pelaksanaan tindakan perbaikan dan pencegahan untuk menghilangkan akar penyebab ketidaksesuaian serta memastikan suatu ketidaksesuaian tidak terjadi lagi. Tindakan perbaikan dan pencegahan ini merupakan

sarana untuk melaksanakan peningkatan penerapan SMKI secara berkesinambungan. Prosedur ini mencakup identifikasi terjadinya suatu ketidaksesuaian, identifikasi penyebab masalah, penentuan tindakan perbaikan & pencegahan, evaluasi efektifitas dari tindakan perbaikan & pencegahan yang dilakukan serta penyimpanan rekaman hasil perbaikan.

b. Prosedur pendukung operasional teknis:

- PKI PENGAMANAN *PASSWORD* merujuk pada (PKI-MR-05)

  Prosedur pengamanan *password* muncul akibat identifikasi risiko yang mendapati ancaman pencurian *password* menempati level tinggi. Kontrol penanganan terhadap perlindungan *password* ini juga belum dapat melindungi keamanannya secara keseluruhan. Prosedur ini sendiri bertujuan untuk memastikan akses pengguna hanya ditujukan bagi pihak yang terautorifikasi serta mencegah akses pengguna yang tidak terautorifikasi. Hal tersebut dilakukan dalam upaya mencegah pencurian informasi dan fasilitas pendukung informasi.

- PKI PENGAMANAN SERVER merujuk pada (PKI-MR-06)

  Kejadian *server down* dalam identifikasi risiko menempati level tinggi sehingga perlu dibuat prosedur pengamanannya. Prosedur ini digunakan untuk memastikan agar terhadap server hanya dilakukan oleh pihak yang telah terautorifikasi.

- PKI PENYIMPANAN KODE PROGRAM merujuk pada (PKI-MR-07)

  Ancaman pencurian kode program tidak menempati level tinggi dalam proses identifikasi risiko karena ancaman ini sangat jarang terjadi. Prosedur ini digunakan untuk memastikan kode program aplikasi

diakses oleh pengguna yang telah terautorifikasi serta melakukan pencegahan pengaksesan dari pihak yang tidak berwenang. Prosedur ini berlaku dalam melindungi kode program aplikasi SIM akademik.

4.3.3 Pembuatan Instruksi Kerja

Instruksi kerja dibuat sebagai arahan dan petunjuk pelaksana bagi pelaksana teknis. Instruksi kerja dibuat secara sederhana, praktis dan mudah untuk dipahami karena akan diimplementasikan oleh pengguna yang berada dalam posisi pelaksana. Dalam dokumentasi SMKI ini hanya dibuat beberapa instruksi kerja saja berdasarkan tingkat kepentingan dan kerawanannya terjadinya risiko. Untuk instruksi kerja yang belum dibuat dapat dilihat pada daftar dokumentasi SMKI (RF-MR-08) yang akan berguna dalam pengembangan SMKI berikutnya. Demikian instruksi kerja yang telah dibuat:

- IK PEMBUATAN *PASSWORD* merujuk pada (IK-ADM-01)
  Instruksi ini dibuat untuk menerapkan manajemen *password* yang baik sehingga dapat menghasilkan *password* yang berkualitas dan tidak mudah ditebak sehingga fungsi dari *password* sendiri sebagai autentifikasi dapat tercapai. Hal ini mutlak diperlukan karena pasword merupakan sistem yang akan memastikan bahwa benar-benar pemilik saja yang diperkenankan masuk ke dalamnya.
- IK PENYIMPANAN PERANGKAT SERVER merujuk pada (IK-ADM-02)
  Instruksi kerja ini berisi langkah-langkah dan tahapan dalam melakukan penyimpanan perangkat fisik server. Instruksi kerja ini dibuat dengan tujuan memudahkan administrator ruang server dalam meletakkan memelihara dan menyimpan perangkat

fisik server agar aman dan mencegah terjadinya ancaman risiko kerusakan.

- IK PENYIMPANAN KODE PROGRAM merujuk pada (IK-PGM-04)
  Instruksi kerja ini berisi tata cara penyimpanan kode program aplikasi agar terhindar dari terjadinya ancaman risiko yang berkaitan dengan keamanan kode program. Ancaman risiko yang mungkin terjadi misalnya pengaksesan oleh pihak yang tidak berwenang dan pencurian dan pengubahan kode program.

4.3.4 Pembuatan Formulir-formulir

Formulir yang dibuat adalah:

- DAFTAR DOKUMEN EKSTERNAL merujuk pada (FM–MR–01)
  Merupakan daftar yang berisi dokumen-dokumen eksternal yang mendukung pengimplementasian SMKI. Formulir ini memudahkan pengguna untuk melihat dan melakukan penelusuran dokumen eksternal, karena mengandung data historis dokumen.
- LEMBAR BUKTI PENYERAHAN DOKUMEN merujuk pada (FM-MR-02).
  Lembar bukti penyerahan dokumen berisi catatan perubahan/revisi dokumen-dokumen yang membangun SMKI.
- FORMULIR PERMINTAAN PERUBAHAN DOKUMEN merujuk pada (FM–MR–03)
  Merupakan formulir yang digunakan untuk mencatat pengajuan perubahan dokumen SMKI beserta alasannya, yang dijakukan oleh organisasi kepada MR sesuai dengan tahapan pada prosedur pengendalian dokumen.
- FORMULIR PERMINTAAN PEMBUATAN DOKUMEN merujuk pada (FM-MR-04)

Formulir yang digunakan untuk pengajuan pembuatan dokumen pendukung SMKI yang disetujui oleh kepala biro, dan diajukan kepada MR sesuai dengan peraturan yang tertulis pada prosedur pengendalian dokumen.

- MASTERLIST DOKUMEN merujuk pada (FM–MR–05).
  Berisi daftar dokumen-dokumen SMKI yang telah diterbitkan.
- FORMULIR DAFTAR REKAMAN KEAMANAN INFORMASI merujuk pada (FM-MR-07)
  Mencatat segala bukti rekaman yang berkaitan dengan pengelolaan, dan pengimplementasian SMKI.
- FORMULIR PENGUBAHAN KODE PROGRAM merujuk pada (FM-PGM-08)
  Merupakan formulir yang mencatat perubahan, alasan perubahan dan dampak yang ditimbulkan dari perubahan kode program aplikasi SIM akademik. Formulir ini bertujuan untuk mempermudah pengembangan dan peningkatan kode program di kemudian hari.
- FORMULIR PERBAIKAN PERANGKAT FISIK JARINGAN merujuk pada (FM-ADM-09)
  Merupakan formulir yang digunakan dalam pencatatan tindakan yang diambil dalam usaha perbaikan perangkat fisik jaringan, untuk mencegah dan mempercepat penanganan apabila kejadian serupa terulang kembali. Formulir ini merupakan bukti rekaman instruksi kerja perbaikan perangkat fisik jaringan.
- FORMULIR LAPORAN KETIDAKSESUAIAN merujuk pada (FM-MR-14)
  Formulir ini mencatat segala ketidaksesuaian antara praktik nyata dari SMKI dengan dokumen-dokumen

dan peraturan yang tercantum dalam SMKI. Formulir ini nantinya diperlukan dalam proses audit internal.

- AGENDA RAPAT TINJAUAN MANAJEMEN merujuk pada (FM-MR-16).
  Merupakan daftar permasalahan yang perlu dibahas dalam Rapat Tinjauan Manajemen (RTM).
- DAFTAR HADIR RTM merujuk pada (FM-MR-18)
  Daftar hadir ini merupakan rekaman dari pelaksanaan RTM
- FORMULIR KESIMPULAN AUDIT merujuk pada (FM-MR-23)
  Formulir kesimpulan audit merupakan bukti rekaman diadakannya audit internal sesuai dengan klausul 6 pada ISO 27001:2005 yang merupakan syarat dalam penetapan, pengimplementasian SMKI.

4.3.5 Pembuatan Referensi

Referensi berisi dokumen-dokumen pelengkap yang dibutuhkan dalam pembangunan SMKI. Semua referensi ini mengacu pada manual Keamanan informasi dan prosedur Keamanan informasi. Demikian adalah referensi yang dibuat dalam dokumentasi SMKI untuk BAAK:

- STRUKTUR ORGANISASI merujuk pada (RF-MR-01)
  Struktur organisasi BAAK ditinjukkan pada Gambar 4.1
- URAIAN TUGAS merujuk pada (RF-MR-02).
  Dalam uraian ini dijelaskan deskripsi pekerjaan dari bagian Pendidikan dan Kerjasama serta sub bagian yang berada dibawahnya.
- PROSES BINIS merujuk pada (RF-MR-03)
  Proses bisnis telah ditunjukkan pada Gambar 4.2
- KEBIJAKAN KEAMANAN INFORMASI merujuk pada (RF-MR-04)

Kebijakan keamanan informasi yang tercantum dalam dokumen SMKI ini hanya berupa pernyataan saja. Oleh Karena BAAK belum memiliki kebijakan keamanan informasi maka pembuatan SMKI ditinjau secara umum dengan menyesuaikannya terhadap persyaratan klausul ISO 27001:2005. Kebijakan keamanan informasi seharusnya mengandung kerangka kerja untuk menentukan sasaran dan arah Keamanan informasi, persyaratan peraturan perundangan atau kewajiban kontrak keamanan sesuai dengan konteks strategis pengelolaan risiko, pemantapan kriteria terhadap risiko dan telah disahkan oleh pihak manajemen[14].

- LAPORAN PERKIRAAN RISIKO merujuk pada (RF-MR-05)
  Dokumen ini berisi identifikasi risiko sampai dengan pemilihan kontrol obyektif dalam usaha pengelolaan risiko.
- SASARAN KEAMANAN INFORMASI merujuk pada (RF-MR-06)
  Sasaran yang dimaksud adalah sasaran keamanan informasi yang ingin dicapai pada masing-masing sub bagian. Sasaran ini harus dikomunikasikan secara efektif pada personil yang bersangkutan. Personil harus menafsirkan sasaran ini sesuai dengan kontrinbusi masing-masing. Sasaran keamanan informasi harus ditinjau ulang secara periodik dan direvisi sesuai dengan keperluan serta mengandung kriteria SMART [12] :
  - *Spesific*, target yang spesifik dan jelas.
  - *Measurable*, terukur dan terhitung.
  - *Achievable*, dapat tercapai.
  - *Relevant*, sesuai dengan fungsi organisasi.
  - *Time bound*, berjangka waktu.

- RENCANA KEAMANAN INFORMASI merujuk pada (RF-MR-07)
  Rencana keamanan informasi adalah proses atau aktivitas yang perlu dilakukan oleh masing-masing sub bagian sebagai usahanya dalam mencapai sasaran keamanan informasi.
- DAFTAR DOKUMENTASI SMKI merujuk pada (RF-MR-08)
  Berisi daftar dokumentasi yang diperlukan dalam pembangunan SMKI untuk BAAK.
- SURAT PERNYATAAN merujuk pada (RF-MR-09)
  Surat pernyataan berisikan pernyataan organisasi dalam menetapkan SMKI serta kontol obyektif dan tindakan pencegahan yang telah dijalankan.
- DAFTAR CONTOH STEMPEL merujuk pada (RF-MR-10)
  Stempel yang dimaksud adalah stempel untuk menyatakan dokumen terkendali, tidak terkendali, kadaluarsa, dsb.

Setelah SMKI dibuat sesuai dengan struktur dokumentasi SMKI, maka langkah selanjutnya adalah dilakukan pelaksanaan SMKI oleh pihak manajemen. Pihak manajemen melaksanakan SMKI sesuai dengan dokumen TANGGUNG JAWAB MANAJEMEN (MKI-05). Pengimplementasian kontrol yang diperlukan dalam pengamanan informasi aplikasi SIM akademik dilaksanakan melalui pengoperasian PKI dan IK yang telah dibuat.

Dalam setiap pelaksanaan suatu aktivitas dalam SMKI diperlukan pemantauan dan peninjauan ulang terhadap keefektifan dari kontrol yang dijalankan. Hal ini diperlukan agar pelaksanaan SMKI sesuai dengan sasaran organisasi. Oleh karena itu organisasi mengadakan kegiatan audit internal terhadap pelaksanaan SMKI. Proses audit internal diatur dalam dokumen AUDIT INTERNAL (MKI-06) dan PROSEDUR AUDIT INTERNAL (PKI-MR-10). Selain dilakukan audit

internal, organisasi juga mengadakan Rapat Tinjauan Manajemen (RTM) yang dijelaskan pada dokumen TINJAUAN MANAJEMEN (MKI-07) dan PROSEDUR TINJAUAN MANAJEMEN (PKI-MR-11) dalam kurun waktu tertentu (sekali setahun). Tujuan dari pelaksanaan RTM sendiri adalah memastikan kesinambungan, kesesuaian, kecukupan, dan keefektifan SMKI, termasuk pengkajian peluang peningkatan dan kebutuhan untuk meningkatkan SMKI. Melalui RTM, pihak manajemen dapat memperbaiki pelaksanaan SMKI sehingga dapat terus diperbaharui dan disesuaikan dengan proses bisnis dan kondisi yang ada.

4.4 Verifikasi Dokumentasi SMKI

Dokumentasi SMKI yang telah dibuat harus dilakukan verifikasi terhadap persyaratan kelengkapan dokumen yang terdapat pada ISO 27001:2005. Hal ini dikarenakan persyaratan dokumentasi yang harus ada dalam pembangunan SMKI terdapat pada klausul 4.3.1 ISO 27001:2005. Di bawah ini adalah daftar kelengkapan dokumen SMKI-BAAK sesuai dengan persyaratan klausul 4.3.1:

Tabel 4. 3 Verifikasi SMKI

No.	Persyaratan Dokumen	Nama Dokumen	Nomor	Keterangan
1.	Pernyataaan Kebijakan SMKI	KEBIJAKAN KEAMANAN INFORMASI	RF-MR-04	Ada
2.	Ruang Lingkup	RUANG LINGKUP	MKI-02	Ada
3.	Prosedur dan Kontrol pendukung SMKI	PROSEDUR PENGENDALIAN DOKUMEN	PKI–MR–01	Ada
		PROSEDUR PENGENDALIAN REKAMAN KEAMANAN	PKI–MR–02	Ada

Tabel 4. 4 Verifikasi SMKI (lanjutan)

No.	Persyaratan Dokumen	Nama Dokumen	Nomor	Keterangan
3.	Prosedur dan Kontrol pendukung SMKI	PROSEDUR PENGAMANAN *PASSWORD*	PKI-MR-05	Ada
		PROSEDUR PENGAMANAN SERVER	PKI-MR-06	Ada
		PROSEDUR PENYIMPANAN KODE PROGRAM	PKI-MR-07	Ada
		AUDIT INTERNAL	PKI-MR-10	Ada
		PROSEDUR TINJAUAN MANAJEMEN	PKI-MR-11	Ada
		PROSEDUR TINDAKAN PERBAIKAN & PENCEGAHAN	PKI-MR-12	Ada
4.	Deskripsi metodologi penilaian risiko	LAPORAN PERKIRAAN RISIKO	RF-MR-05	Ada
5.	Laporan perkiraan risiko	LAPORAN PERKIRAAN RISIKO	RF-MR-05	Ada
6.	Rencana Pengelolaan Risiko	RENCANA PENGELOLAAN RISIKO	RF-MR-11	Ada
7.	Dokumentasi prosedur yang dibutuhkan oleh organisasi	DAFTAR DOKUMENTASI SMKI	RF-MR-08	Ada

Tabel 4. 5 Verifikasi SMKI (lanjutan)

No.	Persyaratan Dokumen	Nama Dokumen	Nomor	Keterangan
8.	Rekaman yang dibutuhkan oleh standar ISO 27001:2005	DAFTAR DOKUMENTASI SMKI	RF-MR-08	Ada
9.	Statement of Applicability	STATEMENT OF APPLICABILITY	RF-MR-09	Ada

Dalam setiap proses penerapan SMKI merupakan representasi dari siklus PDCA yang merupakan siklus hidup SMKI. Oleh karena itu setiap pendokumentasian SMKI sangat berkaitan dengan proses *Plan-Do-Check-Act* yang ditunjukan pada tabel 4.7:

Tabel 4. 6 Hubungan PDCA-Dokumentasi SMKI

No.	Siklus PDCA	Klausul ISO 27001:2005	Dokumen SMKI
1	Plan	4.2.1	RUANG LINGKUP (MKI-02 Rev.00).
			LAPORAN PENILAIAN RISIKO (RF-MR-05 Rev.00)
			SURAT PERNYATAAN (RF-MR-09 Rev.00)
2	Do	4.2.2	TANGGUNG JAWAB MANAJEMEN (MKI-05)
			LAPORAN PENILAIAN RISIKO (RF-MR-05) - Pemilihan kontrol obyektif
		5.1	KEBIJAKAN KEAMANAN INFORMASI (RF-MR-04 Rev.00)
			SASARAN KEAMANAN INFORMASI (RF-MR-06 Rev.00)
			RENCANA KEAMANAN INFORMASI (RF-MR-07 Rev.00)
			URAIAN TUGAS BAAK (RF-MR-02 Rev.00)
			LAPORAN PENILAIAN RISIKO (RF-MR-05 Rev. 00) - Kriteria Penerimaan risiko
			AUDIT INTERNAL (MKI-06 Rev.00)
			TINJAUAN MANAJEMEN-BAAK (MKI-07 Rev.00)

Tabel 4. 7 Hubungan PDCA-Dokumentasi SMKI (Lanjutan)

No.	Siklus PDCA	Klausul ISO 27001:2005	Dokumen SMKI
2.	Do	5.2	STRUKTUR ORGANISASI (RF-MR-01 Rev.00)
			SISTEM MANAJEMEN KEAMANAN INFORMASI (MKI-04 Rev.00) - Pengendalian Rekaman
3	Check	4.2.3	AUDIT INTERNAL (MKI-06 Rev.00).
			UMUM - TINJAUAN MANAJEMEN (MKI-07 Rev.00).
		6	AUDIT INTERNAL (PKI-MR-05 Rev.00).
		7	PROSEDUR TINJAUAN MANAJEMEN (PKI–MR–11 Rev.00).
4	Act	4.2.4	PENINGKATAN SMKI (MKI-08 Rev.00).
			URAIAN TUGAS (RF-MR-09 Rev.00).
		8	TINJAUAN MANAJEMEN (MKI-MR-07 Rev.00)
			PROSEDUR TINDAKAN PERBAIKAN & PENCEGAHAN (PKI–MR–12 Rev.00)

BAB V
SIMPULAN DAN SARAN

Bab ini berisi mengenai simpulan dari rancangan sistem yang telah dibuat dalam tugas akhir ini, dan dilengkapi dengan saran untuk pengembangan sistem ke depan.

5.1 Simpulan

Simpulan yang dapat diambil dari pengerjaan tugas akhir ini adalah sebagai berikut:

1. Penggambaran proses bisnis SIM-Akademik ITS didasarkan pada deskripsi pekerjaan *(job description)* bagian Pendidikan dan Kerjasama. Proses bisnis digambarkan menjadi proses utama, penunjang dan manajemen sebagaimana terlihat pada gambar 4.2.
2. Identifikasi risiko pada proses bisnis dan aset dilakukan dengan mengidentifikasi risiko yang mungkin muncul pada aset-aset yang berkaitan dengan aplikasi SIM akademik serta kelemahan yang mengancam terjadinya risiko. Identifikasi ini akan diukur dan dinilai dengan kriteria tertentu untuk mengetahui level risiko sebagaimana dijelaskan pada lampiran B.
3. Pembuatan dokumentasi SMKI mengadopsi tata cara pendokumentasian SMM dengan melakukan beberapa penyesuaian terhadap ISO 27001:2005. Struktur atau tahapan pembuatan SMKI terlihat pada Gambar 3.2.
4. Pembuatan dokumentasi SMKI menghasilkan 8 Manual Keamanan Informasi, 8 Prosedur Keamanan Informasi, 3 Instruksi Kerja, 11 Referensi serta 13 formulir dan rekaman.

5.2 Saran

1. Pembuatan SMKI-BAAK ini hanya mencakup proses SIM-Akademik saja, oleh karena itu diharapkan dalam

pengembangan kedepan dapat dilengkapi dengan proses-proses yang lain yang terjadi di BAAK.

2. SMKI-BAAK yang dibuat adalah berdasarkan ISO 27001:2005 yang hanya berbasiskan kontrol. Untuk pengembangan selanjutnya diharapkan dapat dibuat SMKI dengan standar yang lain misalnya ITIL dan COBIT yang memiliki kelebihan masing-masing.

DAFTAR PUSTAKA

[1] Syahrifal, M. November 2007. ISO 17799: Standar Sistem Manajemen Keamanan Informasi. STIMIK AMIKOM YOGYAKARTA.

[2] Puthuseeri Kumar, V. Januari 2006. ISMS Implementation Guide. Information Security Consultant.

[3] Tcahyanto, A. 2005. "Pengantar sistem manajemen Keamanan informasi ISO 27001", bahan ajar mata kuliah pengantar audit dan Keamanan informasi.

[4] Rothery, Brian. 1996. Analisis ISO 9000, PT. Pustaka Binaan Pressindo

[5] Hadiwiardjo, H. B. Wibisono, dkk. Juli 1996. ISO 9000 Sistem Manajemen Mutu. Ghalia Indonesia.

[6] Andiva. Juni 2008. Hirarki Dokumen ISO 9001:2000 http://bonoes.blogspot.com/2008/06/hirarki-dokumen-iso-9001-2000.html diakses pada 15 Juli 2009

[7] Pranashakti, Ipan. Maret 2009. Pengertian prosedur mutu, URL:http://ipan.staff.uii.ac.id/2009/02/perangkat-sistem-penjaminan-mutu-uii-yogyakarta.

[8] Wikipedia. July 2009. Pengertian PDCA, <URL: http://id.wikipedia.org/wiki/PDCA>.

[9] INB. November 2005. Information-technology-security techniques-informastion security management system-requirements. ISO.

[10] Ismiatin, Rahayu, D.D, dkk. Januari 2009. Analisis Risiko Proyek Perusahaan. URL:http://www.scribd.com/doc/11100389/Analisis-Risiko Proyek-an.

[11] Wikipedia. Juni 2009. COBIT, <URL:http://id.wikipedia.org/wiki/COBIT.htm.>

[12] Wikipedia. Mei 2008. Information Technology Infrastructure Library, URL:http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

[13] Wikipedia. Juni 2008. ISMS, <URL: http://id.wikipedia.org/wiki/ISMS>.

[14] Brever, D & Nash, M. 2005. the Similarity between ISO 9001 and BS 7799-2.

[15] Holil, A. 2007. "Pengungkapan kebutuhan", bahan ajar mata kuliah identifikasi desain dan sistem informasi

[16] Jaya Ari, Made. Juni 2008. Pengenalan identifikasi risiko, <URL:http://blimadeari.wordpress.com/2008/06/05/pengenalan-identifikasi-risiko-tsi>

BIODATA PENULIS

Penulis dilahirkan di Klaten, 21 April 1987, merupakan anak keempat dari empat bersaudara. Penulis telah menempuh pendidikan formal di SDN Klepu III Ceper Klaten, SLTPN II Klaten, SMAN I Klaten. Setelah lulus dari Sekolah Menengah tahun 2005 penulis meneruskan pendidikannya di Jurusan Sistem Informasi, Fakultas Teknologi Informasi ITS Surabaya dan terdaftar dengan NRP 5205 100 063.

Di Jurusan Sistem Informasi penulis mengambil bidang minat Perencanaan dan Pengembangan Sistem Informasi (PPSI). Penulis pernah tergabung dalam tim *data entry* PSB-*online* Surabaya pada tahun 2006 dan Tim *trouble shouter* PSB-*online* pada tahun 2007. Bagi yang ingin berdiskusi lebih lanjut silakan hubungi penulis lewat email : ohayo_tika@yahoo.co.id.

LAMPIRAN A

Pertanyaan & Jawaban Wawancara

Organisasi	:	Jurusan Sistem Informasi FTif ITS
Responden	:	Mudji Sukur, A.Md
Jabatan	:	Pelaksana registrasi dan statistik-BAAK
Tanggal	:	13 Mei 2009
Topik	:	SIM Akademik
Surveyor	:	Kartika Sari

No.	Daftar Pertanyaan dan Jawaban
1.	Data apa saja yang mendukung dan digunakan pada SIM akademik? *Data Nilai mahasiswa, data mahasiswa (biodata mahasiswa, status mahasiswa DO, cuti, mengundurkan diri).*
2.	Adakah aset perangkat lunak tambahan yang mendukung kinerja dari SIM akademik? jika ada sebutkan *Ada, aset berupa perangkat lunak misal Dreamweaver, SQL, Microsoft office, aplikasi pendukung perkantoran, dll.*
3.	Pernahkah terjadi pembobolan yang disebabkan oleh perangkat lunak? Bagaimana penanganannya? *Pada tahap awal sengaja diadakan suatu kompetisi untuk menguji keamanan dari aplikasi SIM akademik. Namun sampai saat ini pembobolan aplikasi baik melalui jaringan maupun akses dari aplikasi belum pernah terjadi. Kejadian keamanan yang terkait dengan pembobolan tersebut adalah pernah adanya pencurian source code dari salah satu laptop pengembang yang mengurusi aplikasi SIM akademik. Kejadian ini ditindaklanjuti dengan mengganti konfigurasi firewall yang ada di ruang penyimpanan server di lantai 6 dan untuk pencegahannya adalah dengan membatasi akses langsung terhadap server hanya bisa dilakukan di area lantai 6 saja.*

4.	Apakah terdapat prosedur back up data? *Back up data dilakukan tiap hari.*
5.	Bagaimanakah penanganan terhadap virus dan *malicious code*? *Dengan memasang anti virus terupdate*
6.	Apakah terdapat pembagian hak akses user? *Ya, setiap personil memiliki account tersendiri untuk menghindari penyalahgunaan hak akses.*
7.	Adakah kebijakan mengenai penggantian dan penggunaan *password*? *Selama ini kebijakan yang ada hanya berupa himbauan saja.*
8.	Apakah ada aturan mengenai akses terhadap *source code* program? *Ya, yang berhak memiliki dan mengaksesnya hanyalah programmer dan pengembang aplikasi SIM akademik.*
9.	Apakah aplikasi SIM akademik telah mengadoPKI *session time out*? *Ya, merupakah salah satu pencegahan keamanan informasi yang dilakukan pada aplikasi.*
10.	Apakah terdapat ruangan khusus untuk menyimpan server? *Ya, terdapat ruang server untuk kegiatan pengembangan yang diletakkan di salah satu ruangan di BAAK yang aksesnya hanya diperuntukkan bagi programmer dan orang yang diberi kewenangan khusus. Selain itu terdapat server operasional dari SIM akademik yang diletakkan di lantai 6 perpustakaan dan dikelola oleh PUSKOM.*
11.	Apakah terdapat prosedur yang mengatur mengenai pertukaran data melalui suatu media tertentu? *Selama ini tidak terdapat prosedur tertulis yang mengatur.*

12.	Apakah semua aplikasi baik aplikasi utama maupun pendukung yang digunakan dalam organisasi ini bersifat legal (berlisensi)? *Ya, semua aplikasi yang digunakan berlisensi resmi dari vendor..*
13.	Apakah organisasi mengadakan pelatihan untuk meningkatkan *skill* dari para pegawainya? Jika ya apakah diadakan secara rutin? *Pelatihan yang selama ini ada bersifat insidentiil (jika dibutuhkan)*

Organisasi	:	Jurusan Sistem Informasi FTif ITS
Responden	:	Bp. Ahmad Budi Kurniawan
Jabatan	:	Staf seksi sistem informasi manajemen
Tanggal	:	15 Mei 2009
Topik	:	SIM Akademik
Surveyor	:	Kartika Sari

No.	Daftar Pertanyaan dan Jawaban
1.	Apakah wewenang dan tanggung jawab dari PUSKOM berkenaan dengan FRS-online? *Memelihara server agar dapat terus berjalan/beroperasi (server tidak down) (sebatas penanganan teknis dari server)*
2.	Prosedur atau kebijakan apa saja kah yang dimiliki oleh PUSKOM dan telah terdokumentasi berkenaan dengan FRS-online? *Tidak ada, semua prosedur yang berkenaan dengan SIM akademik dimiliki oleh pihak BAAK*
3.	Apakah terdapat kebijakan mengenai perlindungan sistem akses ke ruangan server? *Kunci ruangan hanya dimiliki oleh orang-orang tertentu yang berwenang, server dari SIM akademik disimpan dalam satu ruangan dengan server-server dari aplikasi ITS lainnya seperti itsnet dan webmail.*
4.	Apakah diperbolehkan membawa laptop masuk ke ruangan server? *Sesuai dengan kondisi dan kebijakan orang-orang di ruangan server.*
5.	Bagaimanakah perlindungan terhadap keamanan aset-aset fisik di ruangan server? (missal: diaturnya kelembapan udara, dipasang AC) *Pada ruangan server dipasang AC untuk menjaga kelembapan dan suhu bagi mesin-mesin server.*

6.	Bagaimanakah pemantauan beban kerja server? *Untuk memperingan kinerja server dan mengurangi kejadian server down maka saat ini terdapat 3 server untuk membagi beban kinerja server.*
7.	Bagaimanakah tanggapan PUSKOM terhadap kejadian pembobolan FRS-online oleh salah seorang mahasiswa ITS? *Kejadian ini disebabkan pada saat terjadinya transisi developer dengan keterkaitannya mengenai lemahnya password laptop. Penanganan yang dilakukan oleh pihak PUSKOM adalah mengembalikan kembali database yang telah diubah ke konfigurasi awal dan mengubah password akses ke data tersebut.*
8.	Kejadian atau aktivitas apa saja kah yang sering menyebabkan server menjadi down? *Biasanya disebabkan oleh banyaknya pengakses sehingga menyebabkan traffic menjadi sibuk. Kemudian juga disebabkan serangan dari virus floading jaringan yang penanggulangannya adalah dengan memutus hardware yang terjangkiti virus dari jaringan agar tidak menyebar kemana-mana.*
9.	Bagaimanakah perlindungan server dari kejadian alam seperti: *Untuk penanggulangan kebakaran maka di ruang server disiapkan tabung pemadam kebakaran dan alat pendeteksi asap.Untuk penanggulangan gempa bumi yang jarang terjadi maka server ditempatkan di 3 ruangan yang berbeda walaupun masih dalam lingkup 1 kampus. Untuk kedepannya ITS berencana menitipkan servernya di UI dan ITB.*
10.	Apakah terdapat pelatihan SDM/karyawan untuk meningkatkan skill keahlian? *Sesuai dengan kebutuhan dan tidak dijadwalkan secara berkala.*

Organisasi	:	Jurusan Sistem Informasi FTif ITS
Responden	:	Bp. Satriyo Wicaksono
Jabatan	:	Staf seksi komunikasi dan *networking*
Tanggal	:	15 Mei 2009
Topik	:	Jaringan SIM Akademik
Surveyor	:	Kartika Sari

No.	Daftar Pertanyaan dan Jawaban
1.	Aset jaringan apa saja yang mendukung proses FRS online? (seperti router, switch dll)? *Aset yang paling utama adalah router dan switch. Digunakan password disetiap hardware jaringan untuk melindungi akses orang-orang yang tidak berkepentingan. Untuk manajemen penyimpananya digunakan pencatatan elektronik mengenai jumlah hardware dan lokasi penempatan hardware.*
2.	Bagaimanakah pengamanan dan pemeliharaan fisik dari aset jaringan tersebut? (missal: adanya perawatan yang terjadwal dalam kurun waktu tertentu) *Perawatan fisik untuk hardware tidak dijadwalkan secara khusus karena belum menjadi prioritas utama, namun perawatan dilakukan bersamaan dengan terjadinya masalah-masalah jaringan. Missal terjadi kerusakan jaringan di suatu sector kemudian pihak PUSKOM akan memperbaiki dan juga memeriksa hardware-hardware jaringan di sekitar sector tersebut.*
3.	Mengenai pembatasan load data dan akses internet? *Selama ini belum ada pembatasan melalui ip pengadkses, namun pihak ITSnet membagi port sesuai dengan jumlah fakultas, yang kemudian pengelolaanya diserahkan ke fakultas masing-masing untuk pembagian per jurusannya.*

4.	Apakah pernah terjadi pembobolan data dan informasi SIM akademik yang dilakukan melalui jaringan? Sampai saat ini belum pernah terjadi kejadian semacam itu.

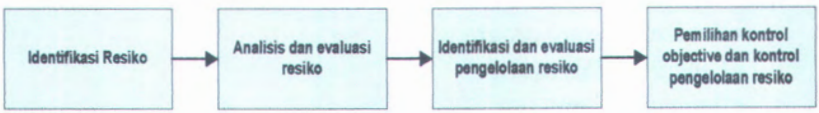
Halaman ini sengaja dikosongkan.

LAMPIRAN B
Laporan Perkiraan Risiko

Perkiraan risiko adalah sebuah proses yang meliputi identifikasi risiko, analisis dan evaluasi risiko, identifikasi dan evaluasi pemilihan pengelolaan risiko serta pemilihan kontrol dan tujuan kontrol. Identifikasi risiko diperlukan untuk mengetahui kerentanan dari aset-aset yang dimiliki serta bagaimana melakukan pencegahan agar aset tersebut bebas dari gangguan. Pencegahan yang dilakukan direpresentasikan dalam bentuk prosedur pelaksanaan. Terdapat kriteria ancaman risiko yang perlu dibuat prosedur pengendaliannya diantaranya adalah:

- Risiko yang memiliki jumlah frekuensi kemunculan yang tinggi.
- Risiko yang bisa menyebabkan kerusakan yang serius.

Adapun tahapan metodologi dalam memperkirakan risiko adalah sebagai berikut:



Gambar B- 1 Metodologi Perkiraan Risiko

B.1 Identifikasi Risiko

Identifikasi risiko bertujuan untuk perkiraan mengetahui risiko apa saja yang mungkin terjadi pada aset-aset yang dimiliki oleh BAAK, khususnya yang berkaitan dengan apalikasi SIM akademik. Demikian dijelaskan tahap identifikasi risikonya:

1.1 Identifikasi Aset

Identifikasi ancaman aset dilakukan dengan cara mencari ancaman apa saja yang mungkin terjadi pada aset-aset yang dimiliki organisasi. Aset yang diidentifikasi ini merupakan aset-aset yang berkaitan dengan aplikasi SIM akademik. Identifikasi aset dilakukan dengan menggunakan metode wawancara sebagaimana terlampir pada LAMPIRAN A. Dari wawancara dapat diketahui bahwa aset yang dimiliki dan

digunakan oleh BAAK ITS berkenaan dengan kegiatan pengelolaan aplikasi SIM akademik adalah:

- Data mahasiswa (biodata mahasiswa, data nilai).
- Hardware dan Software pendukung aplikasi SIM akademik.
- Kode program aplikasi SIM akademik.

1.2 Identifikasi ancaman terhadap aset

Kebutuhan pengaksesan data dan informasi yang telah disebutkan pada 1.1 oleh banyak pihak menimbulkan risiko keamanan terhadap data dan informasi. Semakin banyaknya dilakukan pengaksesan maka semakin besar pula ancaman terhadap keamanan informasi yang akan terjadi. Demikian adalah ancaman yang diperkirakan muncul terhadap aset-aset tersebut:

- Data mahasiswa hilang / rusak
- Aset fisik jaringan rusak
- Komputer *server* rusak
- Pencurian kode program
- Pencurian *Password*
- Bencana Alam

1.3 Identifikasi kelemahan yang mungkin dimanfaatkan oleh ancaman.

Kelemahan pada suatu sistem terkadang menjadi penyebab terjadinya suatu ancaman risiko. Dalam menanggapi masalah tersebut maka organisasi harus memberikan perhatian khusus bagi penanganan kelemahan ini. Demikian adalah kelemahan yang dapat diperkirakan menjadi penyebab terjadinya suatu ancaman risiko yang berdampak pada proses bisnis aplikasi SIM akademik:

- *Server* down
- Pemadaman listrik

1.4 Identifikasi risiko berdasarkan dampak ancaman.

Dampak ancaman yang dimaksudkan adalah dampak terjadinya ancaman risiko terhadap besarnya pengaruh aspek kepercayaan, ketersediaan dan integritas *(confidentially, integrity and availability.* Dalam aplikasi SIM Akademik risiko

yang akan berdampak pada aspek-aspek tersebut adalah ancaman dari Pengubahan data mahasiswa secara paksa

Berdasarkan hasil identifikasi risiko diatas dan setelah dilakukan konfirmasi dengan pihak organisasi, maka dapat disimpulkan bahwa ancaman risiko yang muncul pada aset-aset yang berkaitan dengan aplikasi SIM Akademik adalah sebagai berikut:

Tabel B- 1 Daftar Ancaman Risiko

No.	Risiko
1.	Data mahasiswa hilang/rusak
2.	Aset fisik jaringan rusak
3.	Komputer *server* rusak
4.	Pencurian kode program
5.	Pencurian *password*
6.	Bencana Alam
7.	*Server* down
8.	Pemadaman Listrik
9.	Pengubahan data mahasiswa secara paksa

B.2 Analisis dan Evaluasi Risiko

Setelah melalui tahap identifikasi risiko kemudian dilakukan analisis dan pemberian level pada masing-masing ancaman dengan tahapan sebagai berikut:

2.1 Risiko dan dampak pada proses bisnis

- Data mahasiswa hilang/rusak
  Data mahasiswa terdiri dari nilai, biodata mahasiswa dan status mahasiswa. Data-data ini merupakan data penting yang harus dilindungi. Apabila terjadi kerusakan dari data-data tersebut maka data mahasiswa yang hilang/rusak tidak dapat diakses. Permasalahan tersebut akan menyebabkan pelayanan administrasi mahasiswa yang bersangkutan terganggu atau bahkan tidak dapat dilakukan.
- Aset fisik jaringan rusak

Aset fisik jaringan yang dimaksud contohnya adalah *router* dan *switch*, jika aset ini rusak maka transportasi data tidak dapat dilakukan sehingga membuat pelayanan aplikasi SIM Akademik tidak dapat diakses oleh komputer *client*.

- Komputer *server* rusak
  Komputer yang dimaksud disini adalah komputer *server* yang merupakan pengendali dari aplikasi SIM akademik. Kerusakan dan dampak dari rusaknya komputer *server* ini tergantung pada tingkat kerusakan yang dialami.
- Pencurian kode program
  Kode program merupakan aset yang sangat penting dan sangat perlu dijaga kerahasiaannya. Jika kode program jatuh ke tangan pihak yang tidak berwenang maka akan sangat fatal akibatnya. Pencurian kode ini pernah terjadi akibat dari lemahnya manajemen *password* pada media penyimpanannya.
- Pencurian *password*
  Pencurian *password* berarti membuka lubang keamanan dan memberi kesempatan bagi ancaman-ancaman risiko lainnya untuk terjadi, pencurian *password* lebih banyak disebabkan karena adanya *password sharing*.
- Bencana Alam
  Bencana Alam merupakan faktor lingkungan yang jika terjadi dampaknya dapat menyerang semua aset terutama aset fisik pendukung aplikasi SIM akademik. Hal ini tentu saja sangat mempengaruhi pelayanan dan jalannya proses bisnis dari aplikasi SIM akademik.
- *Server down*
  Server dari aplikasi SIM akademik tidak dapat melaksanakan fungsinya dengan semestinya, sehingga aplikasi SIM akademik tidak dapat diakses

oleh seluruh pengguna. Hal ini menyebabkan gangguan terhadap pelayanan kepada pengguna SIM Akademik.

- Pemadaman Listrik
  SIM akademik tidak dapat berjalan. Karena dengan matinya listrik maka secara otomatis pula komputer *server* akan mati, sehingga segala pelayanan tidak dapat dilakukan
- Pengubahan data mahasiswa secara paksa
  Perubahan data oleh pihak-pihak tidak berwenang dapat mengubah keasliaan data, sehingga melanggar aspek kerahasiiaan, integritas dan kelengkapan.

2.2 Penanganan risiko yang telah diimplementasikan

- Data mahasiswa hilang/rusak
  Dilakukan *back up* data yang dilakukan setiap hari.
- Aset fisik jaringan rusak
  Perawatan *hardware* dilakukan bersamaan dengan terjadinya masalah-masalah jaringan, namun perawatan ini tidak dilakukan secara terjadwal.
- Komputer *server* rusak
  Untuk melindungi kerusakan komputer *server* maka dilakukan pembatasan akses komputer *server* dari pihak luar. Salah satu usaha pengamanannya adalah dengan mengunci ruang *server* dan memberikan kuncinya kepada admin saja. Pemasangan pendingin ruangan dengan suhu tertentu juga dapat mencegah kerusakan komputer yang disebabkan karena kelembaban dan panas.

- Pencurian *password*
  Pemberian himbauan kepada pengguna untuk mengganti *password*nya jika sistem mendeteksi *password* pengguna mudah ditebak.
- Bencana Alam

Dipasang alat pendeteksi asap untuk mencegah kebakaran. Selain itu untuk menghindari bahaya alam maka *server* aplikasi SIM akademik ditanam pada tiga tempat yang berbeda namun masih dalam 1 area ITS.

- *Server down*
  Untuk mengurangi kejadian *server* down maka saat ini disediakan 3 *server* untuk menangani SIM akademik.
- Pemadaman Listrik
  Pihak BAAK menggunakan UPS yang dapat bertahan selama 4 jam untuk menggantikan *supply* listrik PLN jika terjadi pemadaman listrik.

2.3 Penentuan Level Risiko

Terdapat dua sudut pandang dalam menentukan pengukuran level risiko diantaranya adalah pengukuran berdasarkan level probabilitas terjadinya risiko dan pengukuran berdasarkan dampak terjadinya risiko[11]. Masing-masing sudut pandang pengukuran memiliki 3 kriteria dan bobot yang berbeda. Demikian adalah pembobotannya:

- Pengukuran berdasarkan probabilitas terjadinya risiko[16]

- Sering → Sumber ancaman termotivasi dan memiliki kemampuan tinggi, namun kontrol untuk menutupi kelemahannya tidak efektif. Ancaman yang termasuk kategori ini diberikan bobot nilai (1)
- Kadang-kadang → Sumber ancaman termotivasi dan memiliki kemampuan memadai namun kontrol yang ada dapat menghalangi pemanfaatan kelemahan. Ancaman yang masuk kategori kadang-kadang diberikan bobot (0,5)
- Jarang → Sumber ancaman kurang termotivasi, kontrol yang ada sudah cukup untuk mencegah pemanfaatan kelemahan. Bobot untuk ancaman dalam kriteria ini diberikan nilai (0,1)

- Pengukuran berdasarkan dampak terjadinya risiko[16]:

- Rendah *(Low)* → Risiko mengakibatkan kerugian aset atau sumber daya *tangible* dan sedikit mempengaruhi misi, reputasi atau keuntungan organisasi. Diberikan bobot (10)
- Sedang *(Medium)* → Risiko mengakibatkan kerugian yang besar pada aset atau sumber daya *tangible* dan jika terjadi berpengaruh pada misi, reputasi atau keuntungan organisasi. Pembobotan nilainya adalah (50)
- Tinggi *(High)* → Risiko yang terjadi mengakibatkan biaya kerugian yang sangat signifikan pada *aset* atau sumber daya *tangible*. Secara signifikan pula mengancam atau mempengaruhi misi, reputasi atau keuntungan organisasi. Pembobotan nilainya adalah (100).

Demikan adalah perkiraan ancaman risiko beserta pembobotannya:

Tabel B- 2 Level Risiko

Kecenderungan Ancaman	Dampak		
	Rendah **(10)**	***Sedang*** **(50)**	***Tinggi*** **(100)**
Sering **(1)**	Low 10 x 1 = 10	Medium 50 x 1 = 50	High 100 x 1 = 100
Kadang **(0.5)**	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
Jarang **(0.1)**	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

Demikian disajikan tabel perkiraan risiko dari masing-masing Perkiraan ancaman risiko:

Tabel B- 3 Perkiraan Risiko

No.	Risiko	Perkiraan Probabilitas	Perkiraan Dampak	Perhitungan Prioritas
1.	Data mahasiswa hilang/rusak	Kadang-kadang	Tinggi	0.5 x 100 = 50
2.	Aset fisik jaringan rusak	Kadang-kadang	Tinggi	0.5 x 100 = 50
3.	Komputer *server* rusak	Jarang	Tinggi	0.1 x 100 = 10
4.	Pencurian kode program	Jarang	Tinggi	0.1 x 100 = 10
5.	Pencurian *password*	Sering	Tinggi	1 x 100 = 100
6.	Bencana Alam	Jarang	Tinggi	0.1 x 100 = 10
7.	*Server* down	Sering	Tinggi	1 x 100 = 100
8.	Pemadaman Listrik	Kadang-kadang	Tinggi	0.5 x 100 = 50
9.	Pengubahan data mahasiswa secara paksa	Jarang	Tinggi	0.1 x 100 = 10

2.4 Pemilihan risiko berdasarkan kriteria penerimaan risiko

Dalam menentukan pemilihan risiko untuk menentukan prosedur-prosedur yang akan dibuat maka diperlukan pengelompokan ancaman risiko berdasarkan levelnya. Pemberian level terhadap ancaman risiko menggunakan kriteria sebagai berikut:

Tabel B- 4 Level Ancaman Risiko Aplikasi SIM akademik

Kecenderungan Ancaman	Dampak		
	Rendah **(10)**	***Sedang*** **(50)**	***Tinggi*** **(100)**
Sering **(1)**	Rendah	Sedang	Tinggi **5, 7**
Kadang-kadang **(0.5)**	Rendah	Sedang	Sedang **1, 2 dan 8**
Jarang **(0.1)**	Rendah	Rendah	Rendah **3, 4, 6, 9**

Berdasarkan pengukuran risiko dengan indikator perkiraan probabilitas dan dampak, dapat diketahui bahwa risiko-risiko yang perlu dibuat prosedur pengendaliannya adalah risiko yang menempati level nilai tinggi, berdampak besar dan kontrol yang ada belum dapat menanggulangi risiko tersebut. Demikian adalah hasil perkiraan ancaman risiko aplikasi SIM akademik yang akan dibuat prosedur kontrolnya :

1. Pencurian *password*
2. *Server down*
3. Pencurian kode program

Ancaman risiko pencurian kode program perlu dibuat prosedur pengendalian risikonya walaupun menempati level rendah dalam perkiraan risiko. Hal ini dikarenakan

ancaman risiko tersebut menempati level rendah. Level rendah yang dimaksudkan adalah probabilitas terjadinya sangat jarang, namun apabila risiko ini terjadi akan berdampak sangat besar terhadap aplikasi SIM akademik.

B.3 Identifikasi dan Evaluasi Pemilihan Pengelolaan Risiko

- Menetapkan penanganan atau kontrol yang tepat terhadap risiko yang terjadi.
- Pencegahan risiko dengan pembuatan prosedur dan pemilihan tujuan kontrol.
- Menyerahkan penanganan risiko bisnis pada pihak lain seperti asuransi untuk mengurangi dampak risikonya.

B.4 Pemilihan Tujuan Kontrol dan Kontrol Pengelolaan Risiko.

Tujuan kontrol yang digunakan adalah hasil pemilihan tujuan kontrol pada Annex A ISO 27001:2005 yang disesuaikan dengan ancaman risikonya. Disamping itu terdapat pembuatan *cause-effect* diagram yang bertujuan untuk mengetahui akar permasalahan dan penyebab terjadinya risiko. Tujuan kontrol dan *cause-effect* diagram kemudian dijadikan dasar untuk membuat prosedur kontrol guna mencegah dan mengelola ancaman risiko. Adapun tujuan kontrol yang digunakan pada masing-masing ancaman risiko adalah sebagai berikut:

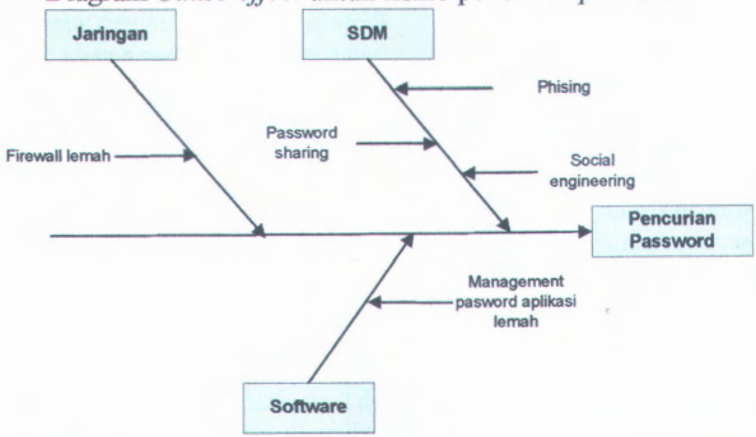
1. Pencurian *password*
   - Tujuan kontrol

A.11.2 Manajemen akses pengguna Tujuan: Untuk memastikan akses terhadap sistem informasi hanya dilakukan oleh pihak yang terautorifikasi dan mencegah akses dari pihak luar.		
A.11.2.3	Manajemen *password* pengguna	Kontrol Pengalokasian *password* harus dikontrol melalui proses manajemen yang formal.

A.11.3 Tanggung jawab pengguna Tujuan: Untuk mencegah akses pengguna yang tak terautorifikasi, kompromi, pencurian informasi dan fasilitas pendukung informasi.		
A.11.3.1	Penggunaan *password*	Kontrol Pengguna seharusnya mengikuti petunjuk pembuatan *password*.

A.11.5 Akses Kontrol sistem operasi Tujuan:Untuk memastikan akses pengguna yang terautentifikasi pada sistem operasi.		
A.11.5.3	Sistem manajemen *password*	Kontrol Sistem yang digunakan untuk mengelola *password* harus interaktif dan dapat menjamin kualitas *password*.

- Diagram *Cause-effect* untuk risiko pencurian *password*



Gambar B- 2 *Cause-effect* diagram untuk risiko pencurian *password*

- Prosedur pengendalian pengamanan *password* sebagaimana terdapat pada **PROSEDUR PENGAMANAN *PASSWORD* (PKI-MR-05 Rev.01).**

2. *Server down*

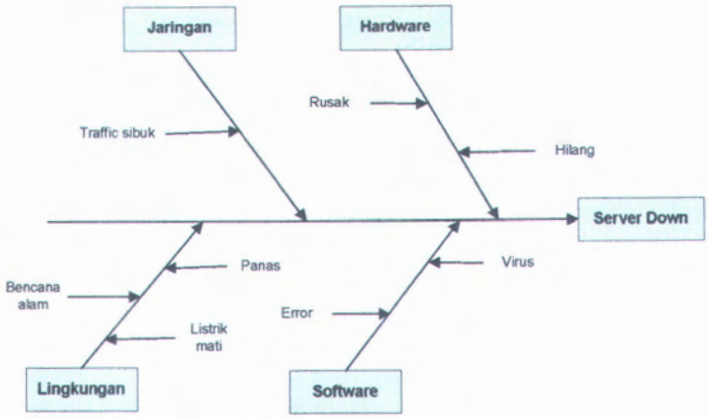
- Tujuan Kontrol

A.9.1 Keamanan area Tujuan:Untuk mencegah akses fisik dari pihak yang tidak terautorifikasi, serta mencegah kerusakan informasi		
A.9.1.1	Keamanan fisik pembatasan area	Kontrol Dalam melindungi kawasan/daerah tempat penyimpanan informasi harus dibuat pembatas area seperti dinding, kartu entry, pagar dll.
A.9.1.4	Perlindungan terhadap kejadian eksternal dan ancaman lingkungan sekitar	Kontrol Perlindungan fisik dari kerusakan yang disebabkan oleh bencana alam harus dibuat dan diimplementasikan
A.9.1.5	Bekerja dalam area yang diamankan	Kontrol: Perlindungan fisik dan peraturan untuk bekerja di ruangan yang diamankan harus dibuat dan diimplementasikan

A.9.2 Keamanan Peralatan Tujuan:Untuk mencegah kehilangan, kerusakan dan pencurian aset serta gangguan terhadap proses bisnis organisasi.		
A.9.2.2	Peralatan Pendukung	Kontrol Peralatan harus dilindungi dari ketidakstabilan power/listrik serta gangguan lain yang disebabkan oleh kegagalan peralatan pendukung.

A.11.4 Akses kontrol Jaringan Tujuan:Untuk mencegah akses pengguna yang tak terautorifikasi pada layanan jaringan.		
A.11.4.6	Kontrol koneksi jaringan	Kontrol Kemampuan pengguna untuk

- Diagram *Cause-effect* untuk risiko *server down.*



Gambar B- 3 *Cause-effect* diagram untuk *server down*

- Prosedur pengendalian pengelolaan *server* untuk menangani dan mencegah *server* menjadi down sebagaimana terdapat pada **PROSEDUR PENGAMANAN SERVER (PKI-MR-06 Rev.01).**

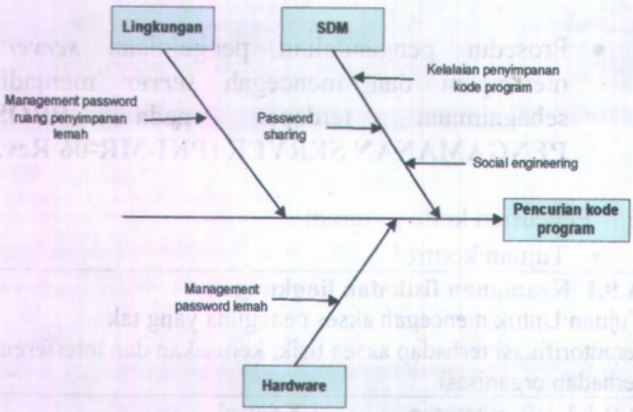
3. Pencurian kode program
   - Tujuan kontrol

A.9.1 Keamanan fisik dan lingkungan Tujuan:Untuk mencegah akses pengguna yang tak terautorifikasi terhadap akses fisik, kerusakan dan interferensi terhadap organisasi.		
A.9.1.1	Pembatasan keamanan fisik	Kontrol Pembatasan keamanan seperti dinding, id card, sidik jari untuk akses masuk harus digunakan untuk melindungi area/tempat penyimpanan informasi dan fasilitasnya..

A.10.8 Pertukaran informasi Tujuan:Untuk mengatur pertukaran informasi dan software dalam suatu organisasi dengan entitas eksternal.		
A.10.8.3	Perpindahan media fisik	Kontrol Akses terhadap kode program harus dibatasi.

A.12.4 Keamanan files sistem Tujuan:Untuk memastikan akses pengguna yang terautentifikasi dan untuk mencegah akses pengguna yang tidak terautentifikasi.		
A.12.4.3	Akses kontrol kode program	Kontrol Akses terhadap kode program harus dibatasi.

- Diagram *Cause-effect* untuk risiko pencurian kode program.



Gambar B- 4 *Cause-Diagram* untuk risiko pencurian kode program

- Prosedur pengendalian penyimpanan kode program dibuat dengan tujuan untuk menangani dan mencegah ancaman risiko pencurian kode program sebagaimana terdapat pada **PROSEDUR PENYIMPANAN KODE PROGRAM (PKI-MR-07 Rev.00).**