DOKUMEN PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI ADMINISTRASI AKADEMIK BERDASARKAN ISO 27001:2013 PADA BAGIAN AAK UNIVERSITAS DINAMIKA

TUGAS AKHIR

Program Studi
S1 Sistem Informasi

Oleh:
Rico Kurniawan
15410100036

FAKULTAS TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS DINAMIKA
2020

DOKUMEN PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI ADMINISTRASI AKADEMIK BERDASARKAN ISO 27001:2013 PADA BAGIAN AAK UNIVERSITAS DINAMIKA

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk menyelesaikan
Program Sarjana Komputer

Oleh :

Nama : Rico Kurniawan
NIM : 15.41010.0036
Program : S1 (Strata Satu)
Jurusan : Sistem Informasi

FAKULTAS TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS DINAMIKA
2020

TUGAS AKHIR

DOKUMEN PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI ADMINISTRASI AKADEMIK BERDASARKAN ISO 27001:2013 PADA BAGIAN AAK UNIVERSITAS DINAMIKA

Dipersiapkan dan disusun oleh

Rico Kurniawan

NIM : 15410100036

Telah diperiksa, diuji dan disetujui oleh Dewan Pembahas

Pada : 28 Februari 2020

Susunan Dewan Penguji

Pembimbing:

I. Erwin Sutomo, S.Kom., M.Eng.
NIDN. 0722057501

II. Vivine Nurcahyawati., M.Kom.
NIDN. 0723018101

Pembahas:

I. Ir. Henry Bambang Setyawan, M.M.
NIDN. 0725055701

28.02.2020

Tugas Akhir ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana

Fakultas Teknologi dan Informatika
UNIVERSITAS Dinamika

28/2 '20

Dr. Jusak

NIDN: 0708017101

Dekan Fakultas Teknologi dan Informatika

UNIVERSITAS DINAMIKA

PERNYATAAN

PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa Universitas Dinamika, saya :

Nama	:	Rico Kurniawan
NIM	:	15410100036
Program Studi	:	S1 Sistem Informasi
Fakultas	:	Fakultas Teknologi dan Informatika
Jenis Karya	:	Tugas Akhir
Judul Karya	:	**DOKUMEN PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI ADMINISTRASI AKADEMIK BERDASARKAN ISO 27001:2013 PADA BAGIAN AAK UNIVERSITAS DINAMIKA**

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Universitas Dinamika Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalti Free Right)* atas seluruh isi/ sebagian karya ilmiah saya tersebut di atas untuk disimpan, dialih media kan dan dikelola dalam bentuk pangkalan data *(database)* untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta
2. Karya tersebut di atas adalah karya asli saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya atau pendapat orang lain yang ada dalam karya ilmiah ini adalah semata hanya rujukan yang dicantumkan dalam Daftar Pustaka saya
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiat pada karya ilmiah ini, maka saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Surabaya, 28 Februari 2020

Yang menyatakan

Rico Kurniawan

Nim : 15410100036

My crime is that of curiosity,

My crime is that of judging people

By what they say and think,

Not what they look like,

My crime is that of outsmarting you,

Something that you will never forgive me for.

If you fail, never give up because F.A.I.L means "FIRST ATTEMPT IN LEARNING" end is not the end, if fact E.N.D means "EFFORT NEVER DIES" if you get no as an answer, remember N.O means "NEXT OPPORTUNITY". So let's be positive

ABSTRAK

Bagian Administrasi Akademik dan Kemahasiswaan (Bagian AAK) merupakan unit pendukung yang dimiliki oleh Universitas Dinamika. Pada kondisi saat ini, Bagian AAK masih memiliki kendala dari sisi manajemen dan operasional dalam penanganan keamanan informasi, yang dapat menimbulkan permasalahan terkait dengan *confidentiality* (kerahasiaan data yang dimiliki masih rentan untuk dapat diakses oleh pihak yang tidak bertanggung jawab), *Integrity* (keutuhan), dan *Availability* (ketersediaan) yang dapat mempengaruhi *business continuity*. Berdasarkan permasalahan di atas, dampak yang dapat ditimbulkan yaitu menurunnya kepercayaan mahasiswa dan pihak terkait dengan pelayanan yang diberikan oleh Bagian AAK.

Untuk mengatasi dampak tersebut, maka dibutuhkan penyusunan dokumen terkait dengan perencanaan SMKI dengan menggunakan metode *Failure and Effect Analysis* (FMEA) yang berfungsi untuk menghitung dan mengidentifikasi efek dari dampak risiko terhadap aset jika terjadi pada instansi, sehingga Bagian AAK mampu menyediakan informasi administrasi akademik yang aman dalam sisi manajemen dan operasional.

Hasil dari penelitian ini yaitu dokumen perencanaan SMKI, dokumen penyusunan kontrol objektif dan kontrol keamanan, dan dokumen SOP yang meliputi kebijakan keamanan informasi pada proses bisnis akademik, instruksi kerja dan rekam kerja. Dihasilkan beberapa pengelolaan diantaranya adalah pengelolaan *Human Resource Security,* pengelolaan keamanan fisik, pengelolaan kontrol akses, pengelolaan penanganan keamanan informasi, pengelolaan penggunaan otentikasi, pengelolaan keamanan pengguna, dan pengelolaan perangkat jaringan. Dengan tujuan, dapat membantu Bagian AAK dalam melakukan pengamanan terhadap aset-aset penting yang dimiliki oleh Bagian AAK, juga untuk menghindari adanya insiden terkait keamanan informasi yang disebabkan oleh faktor disengaja atau tidak disengaja dalam melakukan pengelolaan aset informasi atau hal-hal lain terkait dengan tata kelola informasi yang berada di lingkungan Bagian AAK.

Kata Kunci : Bagian AAK, Keamanan informasi, ISO 27001:2013

KATA PENGANTAR

Puji dan syukur kami panjatkan atas kehadirat Tuhan Yang Maha Esa, karena hanya atas berkat dan rahmat-Nya, sehingga Laporan Tugas Akhir sistem informasi dengan judul "Dokumen Perencanaan Sistem Manajemen Keamanan informasi Administrasi Akademik Berdasarkan ISO 27001:2013 Pada Bagian AAK Universitas Dinamika" dapat diselesaikan dengan baik dan tepat waktu.

Tanpa bimbingan, bantuan dan doa dari berbagai pihak laporan Tugas Akhir ini tidak akan selesai dengan baik. Untuk itu pada kesempatan ini penulis menyampaikan rasa terima kasih kepada yang terhormat :

1. Ayah, Ibu dan semua saudara yang sudah mendukung penuh dalam proses penyelesaian Tugas Akhir ini, dengan memberikan semangat dan do'a yang tiada henti
2. Bapak Erwin Sutomo S.Kom., M.Eng selaku pembimbing pertama yang telah memberikan semangat dan motivasi dalam penyusunan laporan Tugas Akhir ini.
3. Ibu Vivine Nurcahyawati, M.Kom., OCP selaku pembimbing kedua yang telah memberikan semangat dan motivasi dalam penyusunan laporan Tugas Akhir ini.
4. Bapak Ir. Henry Bambang Setyawan, M.M. selaku pembahas 1 (Ketua tim pembahas) yang telah memberikan saran dan masukan agar hasil penelitian menjadi lebih baik lagi.
5. Bapak Yoppy Mirza Maulana, S.Kom., M.MT selaku dosen yang selalu memberikan semangat dan masukan dalam penyusunan laporan Tugas Akhir ini.
6. Terima kasih kepada Ibu Sekar Dewanti A.Md selaku kepala Bagian AAK yang telah memberikan kesempatan untuk melakukan penelitian.
7. Terima kasih kepada rekan tim 3 serangkai (Putra, Ilham dan Rico).
8. Terima kasih kepada Wilda Ayu Pratiwi telah membantu dan memberikan masukan dan kepada seluruh teman-teman yang tidak dapat penulis sebutkan satu persatu secara langsung maupun secara tidak langsung.

9. Terima kasih kepada Nizar Ananta Prawirayuda telah memberikan semangat dan masukan dalam penyusunan laporan Tugas Akhir ini.

Penulis menyadari bahwa laporan Tugas Akhir ini masih jauh dari kata sempurna, maka kritik dan saran sangat dibutuhkan penulis untuk memperbaiki laporan Tugas Akhir ini. Semoga tuhan yang maha esa memberikan imbalan yang sesuai atas segala bantuan yang telah diberikan.

Surabaya, 25 Februari 2020

(Rico Kurniawan)

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Universitas Dinamika (Undika) adalah lembaga pendidikan yang bergerak di bidang teknologi informasi. Salah satu misi dari Undika yaitu membentuk Sumber daya manusia yang profesional, unggul, dan berkompetensi. Untuk mendukung misi tersebut, Undika memiliki unit pendukung dalam bidang administrasi akademik yaitu Bagian Administrasi Akademik dan Kemahasiswaan (Bagian AAK).

Berdasarkan wawancara yang dilakukan dengan kepala Bagian AAK yaitu Ibu Sekar Dewanti A.Md, pada kondisi saat ini ditemukan adanya *Threat* (Ancaman) dan *Vulnerability* (Kelemahan) dari internal dan eksternal, yaitu : *Threat* (Ancaman) yang terjadi atas sisi eksternal yaitu serangan yang dilakukan oleh peretas (*Hacker*), di antaranya serangan *Distributed Denial of Service* (DDOS) yaitu terkait adanya laporan sistem yang secara tiba-tiba tidak tersedia atau *Down*. Kemungkinan terjadi serangan lain meliputi : virus *Ransomeware*, *Remote acces trojan*, *Man in the middle attack*. *Vulnerability* (Kelemahan) yang terjadi dari sisi internal yaitu adanya celah keamanan pada sistem terkait dengan adanya laporan mengenai usaha perubahan nilai dan data absen secara paksa pada sistem Bagian AAK. Kemungkinan adanya kelemahan lain yang ada pada sistem meliputi *Sqlinjection*, *Cross site scripting, CSRF, Local file inclution, Click jacking, Bypass Sql injection*.

Kemudian dampak yang dapat ditinjau dari sisi *Confidentiality* (Kerahasiaan) adalah data dan sandi yang digunakan oleh pegawai diketahui oleh

pihak tidak bertanggung jawab. *Integrity* (Keutuhan) adalah data dan informasi yang disediakan oleh Bagian AAK menjadi tidak akurat. *Availability* (Ketersediaan) yaitu terkait dengan adanya laporan mengenai sistem yang tidak tersedia atau *Down*.

Berdasarkan fakta yang ditemukan pada kondisi saat ini, solusi yang sudah dilakukan Bagian AAK untuk menanggulangi ancaman, kelemahan dan dampak meliputi proses secara manajemen, yaitu : pengelolaan hak akses pengguna pada sistem yang digunakan oleh Bagian AAK. Solusi keamanan informasi yang ada saat ini, belum bisa memberikan perubahan yang signifikan terhadap penanganan keamanan informasi yang ada di Bagian AAK.

Mengingat pentingnya keamanan informasi yang dimiliki Bagian AAK, dukungan yang diberikan terhadap pengendalian sistem manajemen keamanan informasi adalah penyusunan dokumen terkait dengan pengendalian keamanan informasi dan pembuatan dokumen *Standard Operational Procedure* (SOP). Dengan tujuan memberikan panduan atau pedoman kerja agar kegiatan dapat terkontrol dengan baik, dan terwujudnya target yang ingin dicapai secara maksimal. Penyusunan dokumen SOP menyesuaikan dengan kontrol objektif dan kontrol keamanan yang ada di *International Organization for Standardization* (ISO/IEC) 27001:2013. Hasil dari penelitian ini adalah berupa dokumen pengelolaan risiko yang berkaitan dengan keamanan informasi, dan dokumen SOP. Harapan dari penelitian ini adalah meningkatkan pengelolaan dan penanganan terkait dengan keamanan informasi di Bagian AAK Undika.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan di atas, maka dapat dirumuskan permasalahan pada penelitian ini yaitu :

1. Bagaimana menyusun dokumen perencanaan SMKI yang berkaitan dengan keamanan informasi ?
2. Bagaimana menyusun kontrol objektif dan kontrol keamanan yang berkaitan dengan pengelolaan risiko keamanan informasi ?
3. Bagaimana menyusun *Standard Operational Procedure* (SOP) meliputi kebijakan keamanan informasi pada proses bisnis akademik, instruksi kerja, dan rekam kerja. yang diambil dari pengendalian kontrol objektif dan kontrol keamanan menggunakan ISO 27001:2013 agar sesuai dengan kebutuhan keamanan informasi ?

1.3 Batasan Masalah

1. Ruang lingkup perencanaan sistem manajemen keamanan informasi dilakukan pada Bagian AAK Universitas Dinamika.
2. Data yang digunakan untuk melakukan perencanaan adalah data atau informasi terkait risiko keamanan informasi, yang dimiliki Bagian AAK pada tahun 2019.

1.4 Tujuan

Tujuan dari penelitian ini yaitu menghasilkan dokumen perencanaan sistem manajemen keamanan informasi sebagai berikut :

1. Dokumen perencanaan SMKI yang berkaitan dengan keamanan informasi yang meliputi menentukan ruang lingkup, menentukan kebijakan keamanan

informasi pada proses bisnis akademik, identifikasi aset, identifikasi *Potential Cause*, identifikasi risiko, penilaian risiko, analisis dan evaluasi risiko, serta identifikasi dan evaluasi penanganan risiko pada Bagian AAK.

2. Proses pemilihan kontrol objektif dan kontrol keamanan.
3. Dokumen *Standard Operational Procedure* (SOP) yang meliputi dokumen kebijakan keamanan informasi pada proses bisnis akademik, instruksi kerja, dan rekam kerja yang sesuai dengan kontrol objektif dan kontrol keamanan yang berkaitan dengan keamanan informasi.

1.5 Manfaat

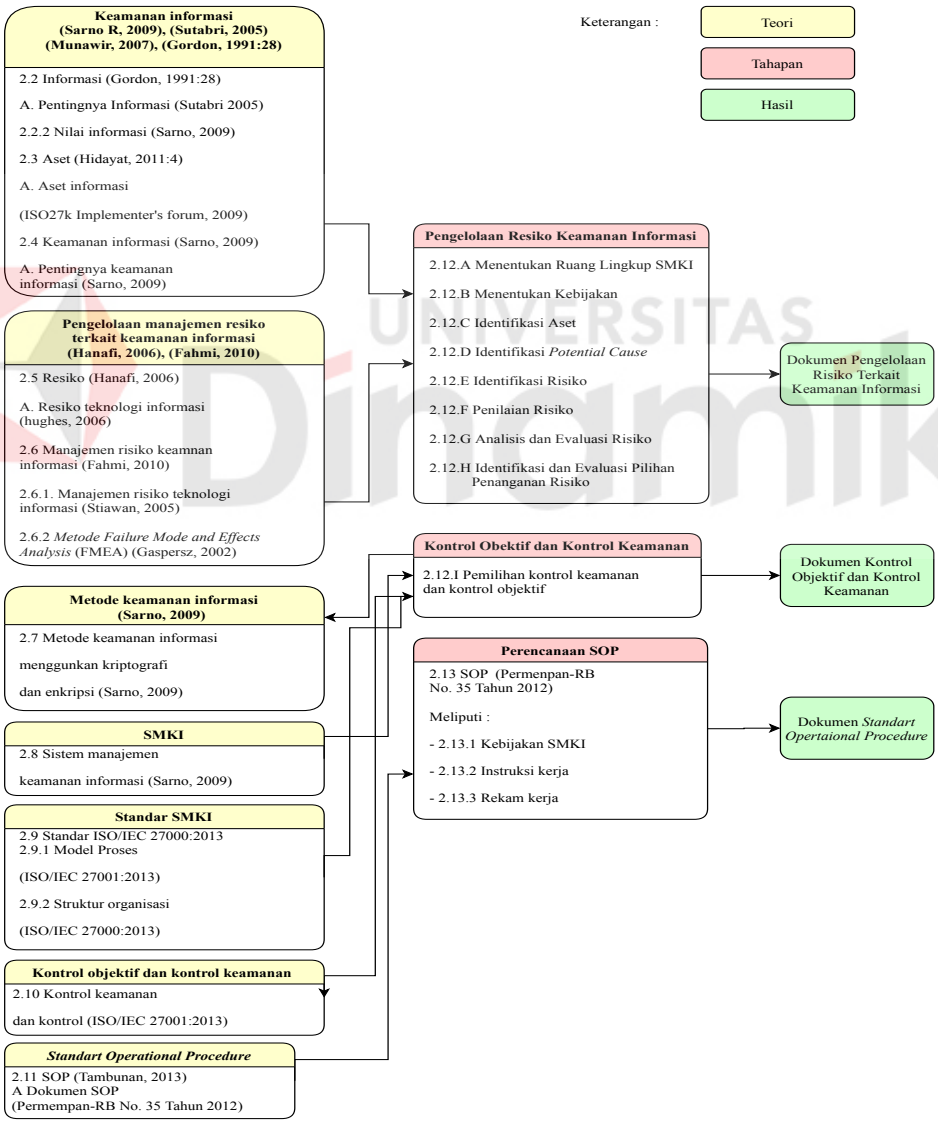
Manfaat yang akan diperoleh dari penelitian ini adalah sebagai berikut :

1. Membantu Bagian AAK dalam melakukan perencanaan sistem manajemen keamanan informasi, melakukan penilaian terhadap aset informasi, serta melakukan pengendalian risiko keamanan informasi.
2. Membantu Bagian AAK dalam melakukan penyusunan dokumen SOP terkait dengan keamanan informasi yang sesuai dengan standar ISO 27001:2013, sehingga dapat mendukung manfaat yang pertama yaitu sebagai kerangka kerja atau pedoman dalam melakukan proses-proses dalam melaksanakan pengendalian risiko keamanan informasi yang disebutkan pada manfaat yang pertama

BAB II

LANDASAN TEORI

Pada bab II ini akan membahas terkait dengan teori yang akan digunakan sebagai landasan dalam menyusun penelitian ini, kemudian di gunakan untuk mendukung tahapan-tahapan yang akan dilakukan. Untuk detail dari teori akan digunakan dapat dilihat pada Gambar 2.1



Gambar 2. 1 Landasan Teori

2.1 Landasan Teori

Kerangka teori adalah kemampuan peneliti dalam mengidentifikasi teori yang dijadikan landasan berpikir untuk melaksanakan suatu penelitian. Teori adalah perangkat atau konsep yang saling berhubungan, yang mencerminkan suatu pandangan sistematik mengenai fenomena dengan menerangkan hubungan antar variabel (Mardalis, 2003).

2.2 Keamanan Informasi

Mengingat pentingnya informasi bagi suatu instansi, maka keamanan informasi sangat dibutuhkan untuk menjaga informasi dari seluruh ancaman yang mungkin terjadi, dalam upaya untuk memastikan atau menjamin kelangsungan bisnis *(business continuity),* meminimalisasi risiko bisnis *(reduce business risk)* dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno & Iffano, 2009).

Agar dapat mencapai tujuan tersebut, keamanan informasi memiliki 3(tiga) aspek yang harus dipenuhi, aspek tersebut dapat dilihat pada gambar 2.2, aspek yang harus dipenuhi yaitu :

1. *Confidentiality* (Kerahasiaan) : Keamanan informasi seharusnya dapat memastikan bahwa informasi sensitif hanya diakses oleh orang yang berwenang, dan dijauhkan dari mereka yang tidak memiliki wewenang.
2. *Integrity* (Integritas) : Keamanan informasi seharusnya dapat memastikan validitas, konsistensi, akurasi informasi dari pihak yang tidak memiliki wewenang.

3. *Availability* (Ketersediaan) : Keamanan informasi seharusnya dapat memastikan informasi dan sumber daya (perangkat keras) tersedia atau tidak dalam format tidak bisa digunakan.

Gambar 2. 2 Aspek Keamanan Informasi
Sumber: Sarno & Iffano, 2009

2.3 Pengelolaan Manajemen Risiko Terkait Keamanan Informasi

Manajemen risiko adalah proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan risiko, dan memonitor serta mengendalikan penganan risiko (Djohanputro, 2008).

Tujuan dari pengelolaan risiko tersendiri adalah mengurangi risiko yang kemungkinan muncul dengan solusi yang berhubungan dengan aspek teknologi informasi /sistem informasi (Setiawan, 2005). Pada solusi yang di sebutkan, solusi yang digunakan adalah pengelolaan dengan menggunakan metode *Metode Failure Mode and Effects Analysis* (FMEA) yang di mana FMEA merupakan teknik analisis risiko yang dilakukan secara *sirkulatif* yang digunakan untuk melakukan identifikasi bagaimana suatu sistem dapat gagal beserta akibat yang dapat ditimbulkan (Gaspersz, 2002).

2.4 Metode Keamanan Informasi

Keamanan informasi tidak hanya dipandang dari sisi manajemen, akan tetapi dari sisi teknik pun harus diperhatikan. Untuk mendukung pengelolaan keamanan

informasi metode keamanan informasi sangat dibutuhkan, metode keamanan yang digunakan salah satunya adalah kriptografi, Menurut Sarno & Iffano, (2009), metode–metode keamanan informasi di bagi menjadi 3 yaitu :

1. *Password* : yaitu mengatur atau membatasi akses ke informasi tersebut melalui mekanisme " *access control* ".
2. *Enkripsi* : yaitu proses pengubahan/konversi/penyajian suatu informasi ke bentuk lain atau tertentu sehingga tidak dapat dimengerti atau tidak dapat dimanfaatkan oleh pihak yang tidak memiliki hak.
3. *Kriptografi* : yaitu metode untuk menyamarkan (merahasiakan) isi dari data sehingga data tidak mudah untuk dibaca oleh orang yang tidak berhak untuk membacanya.

2.5 Standar SMKI

Standar yang digunakan adalah *International Organization For Standardization* (ISO), ISO tersendiri memiliki beberapa versi yang dapat dilihat pada lampiran 6 - Standar SMKI. Dokumen ISO berfungsi untuk mengembangkan dan mengimplementasikan kerangka kerja untuk mengelola keamanan aset informasi dan dapat digunakan mempersiapkan penilaian terhadap SMKI yang diterapkan pada lingkup keamanan informasi (ISO/IEC 27001, 2013).

2.6 Kontrol objektif dan kontrol keamanan

Kontrol objektif dan kontrol keamanan masih terkait dengan penggunaan standar SMKI yaitu standar ISO, pemilihan kontrol objektif dan kontrol keamanan merupakan panduan dalam penerapan keamanan informasi dengan menggunakan bentuk kontrol yang bertujuan untuk mencapai sasaran dari kontrol yang sudah di

tetapkan (ISO/IEC 27001, 2013). Bentuk kontrol yang seluruhnya menyangkut 7 klausul, 4 kontrol objektif, dan 114 kontrol keamanan yang sudah ditetapkan di dalam standar ISO. Beberapa kontrol dapat dilihat pada tabel 2.1 untuk detail dari tabel dapat dilihat pada lampiran 7 – Kontrol Objektif dan kontrol keamanan.

Tabel 2. 1 Kontrol keamanan dan Kontrol Objektif

A.5	***Information security polices***
	Mengelola dan memperbarui kebijakan keamanan informasi organisasi
A.6	***Organization of information security***
	Mengelola informasi organisasi termasuk : identifikasi peran dan tanggung jawab, pemisahan tugas, perangkat IT dan jaringan

(Sumber: (ISO/IEC 27001, 2013))

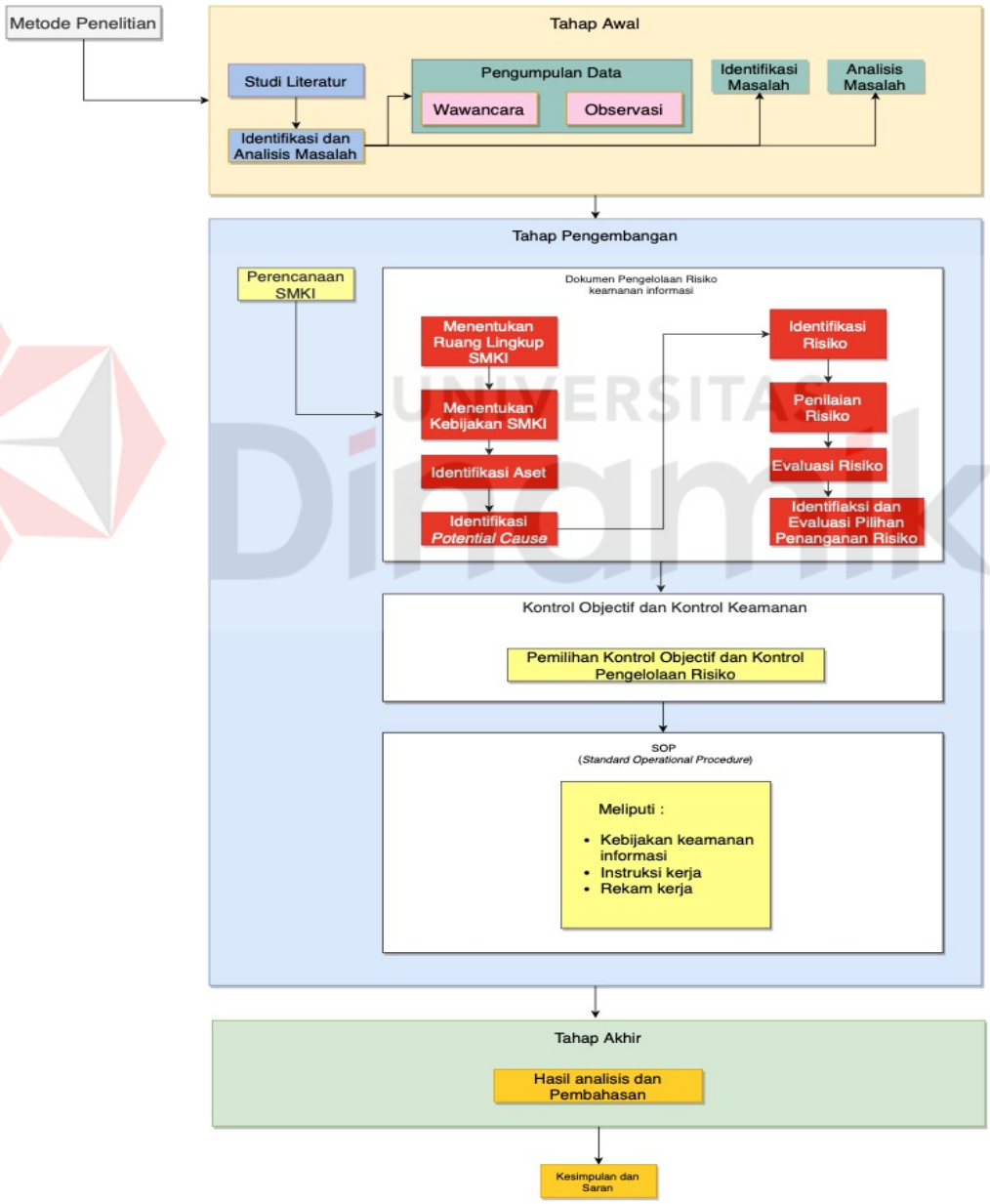
2.7 *Standart Operational Procedure*

Standart Operational Procedure (SOP) adalah pedoman yang berisi prosedur operasional standar yang berada di suatu organisasi yang digunakan untuk memastikan semua keputusan dan tindakan, serta penggunaan fasilitas–fasilitas proses yang dilakukan oleh orang-orang yang berada di organisasi dan merupakan anggota organisasi dapat berjalan dengan efektif, efisien, standar dan sistematis. (Tambunan, 2013). Tujuan dari penggunaan SOP adalah sebagai acuan dalam perencanaan SMKI, yang nantinya akan menghasilkan kebijakan, instruksi kerja dan rekam kerja. Untuk penjelasan secara detail dapat dilihat pada lampiran Lampiran 8 – Standar Operasional Prosedur.

BAB III

METODE PENELITIAN

Pada metode penelitian ini dibagi menjadi 3 (tiga) tahapan, yaitu tahapan awal, tahapan pengembangan, dan tahapan akhir. Untuk detail pada metode penelitian ini dapat dilihat pada gambar 3.1



Gambar 3. 1 Metode Penelitian

3.1 Tahap Awal

Pada tahap awal ini merupakan tahap untuk menggali informasi dari Bagian AAK yang nantinya akan digunakan sebagai bahan pendukung pada tahap pengembangan. Ada beberapa tahapan yang harus dilaksanakan yaitu :

3.1.1 Studi literatur

Dalam menyusun penelitian perlu dilakukan teknik penyusunan secara sistematis dengan tujuan memudahkan langkah–langkah yang akan diambil pada tahap penyusunan. Sesuai dengan tahapan yang sudah ada pada metodologi penelitian, tahap awal yaitu melakukan studi pustaka, dengan mencari referensi berupa buku yang membahas keamanan informasi dan jurnal yang berkaitan dengan keamanan informasi. Data yang di hasilkan dari pelaksanaan studi pustaka digunakan sebagai acuan penyusunan laporan ini, yaitu sebagai berikut :

1. Konsep–konsep keamanan informasi yang digunakan untuk mengelola aset dan keamanan informasi.
2. Konsep-konsep pengelolaan risiko keamanan informasi yang digunakan untuk menyusun pengelolaan risiko.
3. Sistem manajemen keamanan informasi digunakan dalam penyusunan langkah-langkah dalam menentukan kontrol objektif dan kontrol keamanan.

4. Konsep penyusunan SOP berdasarkan peraturan dan langkah-langkah yang ada di peraturan daerah.

3.1.2 Identifikasi dan Analisis Masalah

A. Pengumpulan Data

Selain menggunakan metode dan refrensi yang tepat dalam menyusun penelitian, penggunaan teknik untuk melakukan pengumpulan data yang relevan dan data obyektif juga dibutuhkan.

Teknik dan langkah-langkah yang digunakan dalam mengumpulkan data-data pada penelitian ini adalah sebagai berikut :

1. Wawancara

Wawancara yang dilakukan pada penelitian ini dengan Ibu Sekar Dewanti, A.Md selaku kepala unit kerja administrasi akademik dan kemahasiswaan mengenai kebutuhan data, informasi dan kelemahan yang berkaitan dengan keamanan informasi yang ada di Bagian AAK. berikut adalah data-data yang didapatkan dari hasil wawancara yaitu :

a. Visi, misi, tujuan dan struktur organisasi instansi.
b. Proses bisnis pada Administrasi Akademik dan Kemahasiswaan (Bagian AAK).
c. Tugas pokok dan fungsi setiap Sumber Daya Manusia (SDM).
d. Aset informasi dan Layanan yang ada di Administrasi Akademik dan Kemahasiswaan (Bagian AAK).
e. Informasi risiko yang terjadi di Bagian AAK terkait dengan keamanan informasi.

2. Observasi

Observasi ini dilakukan pada proses bisnis yang ada di Bagian AAK yang bertujuan untuk mendapatkan data, informasi dan masalah terkait keamanan informasi, sehingga diperoleh pemahaman secara langsung dari pengamatan yang dilakukan. Observasi yang dilakukan menghasilkan fakta dan permasalahan terkait dengan keamanan informasi yang ada di Bagian AAK saat ini. Detail dari hasil observasi dapat dilihat pada lampiran 2 proses bisnis. Berikut adalah data-data yang didapatkan dari hasil observasi yaitu :

a. Data aset informasi.
b. Data risiko yang terjadi di Bagian AAK terkait dengan keamanan informasi.
c. Daftar pertanyaan wawancara dan hasil wawancara.
d. Data kebijakan keamanan informasi.
e. Data dan informasi dari Bagian AAK, unit kerja dan bagian lain terkait keamanan informasi.

B. Identifikasi Masalah

Identifikasi masalah yang terjadi di Bagian AAK bertujuan untuk mengetahui maslah yang terjadi saat ini. Identifikasi ini dimulai dari identifikasi permasalahan yang ditemukan saat ini, maka diperlukan pengkajian terkait data dan referensi yang berhubungan dengan topik pada penelitian ini.

Identifikasi masalah di Bagian AAK yaitu terkait dengan penanganan keamanan informasi yang ditinjau melalui *Threat* (Ancaman) dan *Vulnerability* (Kelemahan) yang terjadi di Bagian AAK saat ini, yang mempengaruhi *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan) dan *Availibility* (Ketersediaan) sehingga akan berdampak pada *Business Continuity* di Bagian AAK.

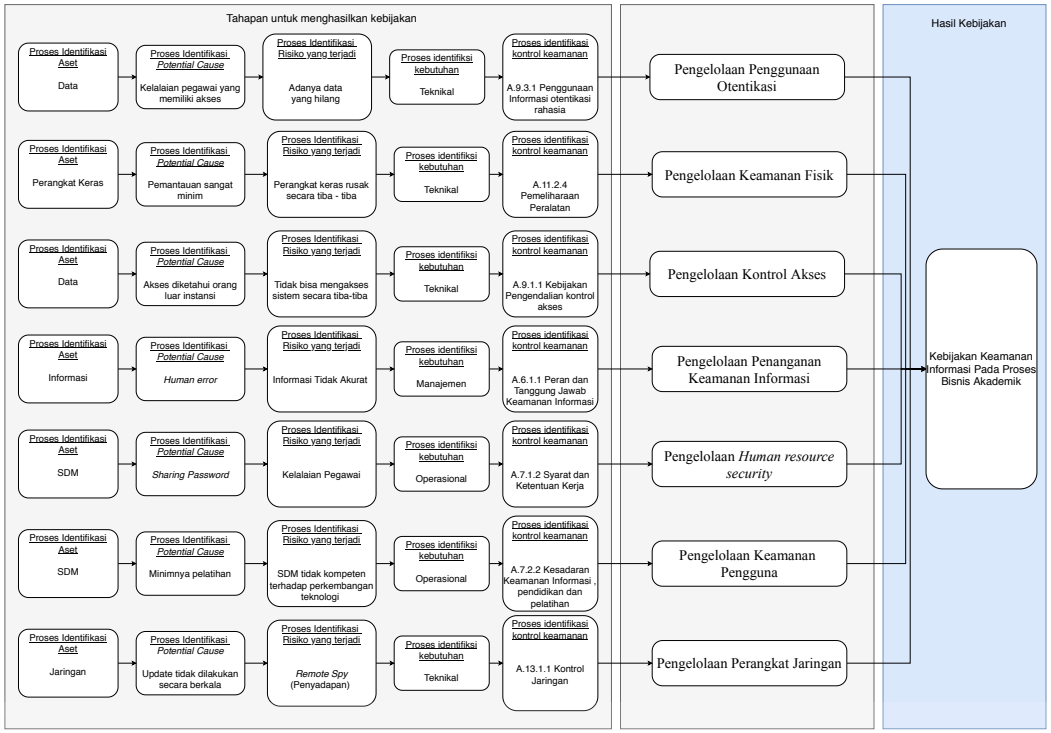
C. Analisis Masalah

Analisis masalah ini bertujuan untuk mempertegas masalah-masalah yang ditemukan dan kemudian akan diteliti, mempertegas batasan-batasan, serta lebih mempertegas latar belakang dari ancaman dan kelemahan yang ada di Bagian AAK.

Dengan tujuan mengetahui pengaruh ancaman dan kelemahan terhadap *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan) dan *Availability* (Ketersediaan) yang dapat berdampak pada *Business Continuity* di Bagian AAK. Dengan demikian dukungan dalam mengendalikan sistem manajemen keamanan informasi yang ditinjau dai sisi CIA yang diberikan pada Bagian AAK yaitu dengan menyusun dokumen perencanaan pengelolaan risiko terkait dengan keamanan informasi dan penyusunan dokumen SOP (*Standar Operational Procedure*) yang berguna sebagai standarisasi dan acuan kerja Bagian AAK agar lebih terstruktur dan dapat meningkatkan keamanan informasi yang ada di Bagian AAK, unit kerja dan bagian lain yang memiliki keterkaitan informasi dengan Bagian AAK.

3.2 Tahap Pengembangan

Tahap pengembangan dilaksanakan dan disesuaikan dengan langkah-langkah pada sistem manajemen keamanan informasi yang ada pada ISO/IEC 27001:2013 yang berkaitan dengan tahap perencanaan sistem manajemen keamanan informasi. Langkah-langkah tersebut dapat dilihat pada gambar 3.2 dan penjelasannya dapat dilihat pada lampiran 18 yang akan dijelaskan sebagai berikut :



Gambar 3. 2 Tahapan untuk menghasilkan kebijakan keamanan informasi pada proses bisnis akademik

Diagram diatas menjelaskan mengenai bagaimana proses untuk menghasilkan kebijakan yang menjadi output pada Tugas Akhir ini, untuk menhasilkan kebijakan ada beberapa proses yang terdiri atas proses identifikasi aset yang berguna untuk mengetahui aset apa yang harus di amankan, kemudian ada proses identifikasi *Potential Cause* yang berguna untuk mengetahui kemungkinan kenapa risiko tersebut terjadi, selanjutnya adalah proses identifikasi risiko yang terjadi sesuai dengan proses sebelumnya. Proses selanjutnya adalah proses identifikasi kebutuhan yang berguna untuk mengetahui penanganan sesuai dengan kebutuhan keamanan informasi dan disesuaikan dengan proses selanjutnya yaitu identifikasi kontrol keamanan. Dari proses tersebut maka dihasilkan sebuah kebijakan untuk menangani risiko terhadap aset yang sudah di identifikasi dan di sesuaikan dengan kebutuhan keamanan informasi.

3.2.1 Perencanaan SMKI

Pada dokumen perencanaan SMKI berisikan proses-proses yang harus dilakukan untuk mengetahui tingkatan risiko, nilai risiko terhadap aset-aset milik Bagian AAK, data aset yang digunakan diambil dari hasil proses pengumpulan data yang nantinya akan dilakukan proses identifikasi dan penilaian. Proses-proses yang akan di lakukan adalah sebagai berikut :

A. Menentukan Ruang Lingkup SMKI

Penentuan ruang lingkup ini sangat dibutuhkan dengan tujuan dokumen yang dihasilkan sesuai dengan kebutuhan permasalahan keamanan informasi di Bagian AAK. dalam menentukan ruang lingkup sistem manajemen keamanan informasi, yang harus dilakukan yaitu :

a. Melakukan identifikasi masalah dari sisi eksternal dan internal di Bagian AAK
b. Identifikasi kondisi saat ini pada Bagian AAK, di antaranya adalah : karakter proses bisnis Bagian AAK, aset yang dimiliki, dan teknologi yang digunakan.
c. Penetapan persyaratan unit kerja dan bagian yang terkait, persyaratan ini mencakup peraturan dan kebijakan.

B. Menentukan Kebijakan SMKI

Penentuan kebijakan sistem manajemen keamanan informasi yang akan dibuat pada penelitian ini terdiri atas :

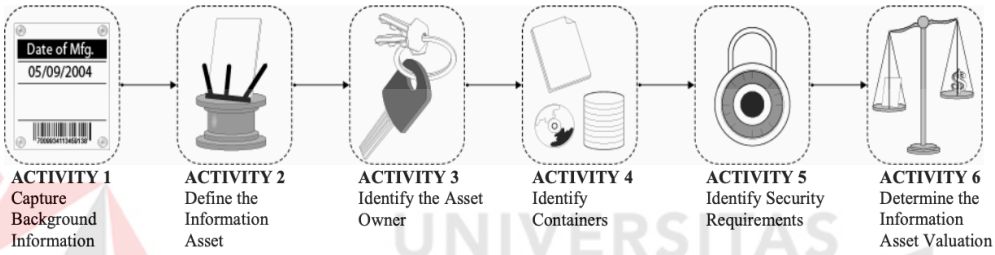
1. Dokumen perencanaan (Renstra) merupakan salah satu masukan dalam pembuatan dokumen ruang lingkup dan menjadi masukan dalam proses penentuan kebijakan terkait SMKI.

C. Identifikasi Aset

Proses identifikasi aset ini bertujuan untuk mengklasifikasi dan memberikan deskripsi umum pada setiap aset milik Bagian AAK yang telah teridentifikasi. Identifikasi aset yang dilakukan menggunakan proses *Information Asset Profiling* (IAP).

Proses dari IAP dapat dilihat pada gambar 3.2.

Hasil dari identifikasi aset ini akan digunakan pada proses identifikasi *Potential Cause* yang di mana membutuhkan aset yang sudah teridentifikasi.



Gambar 3. 3 Information Asset Profiling (IAP)

D. Identifikasi *Potential Cause*

Identifikasi *Potential Cause* ditujukan untuk mengetahui besar risiko yang akan diterima oleh Bagian AAK :

1. Langkah 1 : Melakukan identifikasi terhadap mode kegagalan dan efek tingkat kerusakan yang ditimbulkan
2. Langkah 2 : Identifikasi faktor-faktor potensial yang menyebabkan kerusakan pada keamanan informasi yang ada di Bagian AAK.
3. Langkah 3 : Melakukan identifikasi terkait cara penanganan yang terbaik untuk menangani keamanan informasi.

E. Identifikasi Risiko

Identifikasi risiko ini bertujuan untuk mengukur seberapa besar risiko yang diterima oleh Bagian AAK jika terjadi adanya ancaman dan kelemahan. Berikut merupakan langkah-langkah identifikasi risiko yaitu :

1. Langkah 1 : Mengidentifikasi aset dan mengklasifikasikan aset yang dimiliki Bagian AAK
2. Langkah 2 : Menghitung nilai aset sesuai dengan aspek keamanan informasi (CIA) yaitu dengan memberikan nilai terhadap masing-masing aset.
3. Langkah 3 : Menghitung nilai ancaman dan kelemahan aset dengan membuat tabel gangguan keamanan.
4. Langkah 4 : Identifikasi dampak kegagalan aspek keamanan informasi dengan membuat tabel identifikasi dampak terhadap bisnis beserta level dampak yang terjadi.

F. Penilaian Risiko

Pada tahap penilaian risiko ini bertujuan untuk mengetahui seberapa besar dampak dari risiko yang akan diterima oleh Bagian AAK jika terjadi ancaman dari sisi internal ataupun eksternal. Berikut merupakan langkah-langkah penilaian risiko yaitu :

1. Menentukan kriteria penerimaan risiko menggunakan matriks 3x3
2. Penilaian risiko ini menggunakan metode FMEA dengan hitungan sistematis pada proses penilaian risikonya
3. Masukan dari proses penilaian risiko ini diambil dari dokumen ruang lingkup

G. Analisis dan Evaluasi Risiko

Analisis dan evaluasi risiko ditujukan untuk mengetahui besar risiko yang akan diterima oleh Bagian AAK.

1. Langkah 1 : Melakukan analisis dampak bisnis pada Bagian AAK, dilakukan dengan cara membuat tabel BIA dengan mengacu pada tabel nilai skala BIA
2. Langkah 2 : Mengidentifikasi level risiko dengan membuat tabel matriks level risiko
3. Langkah 3 : Menentukan risiko yang diterima atau perlu adanya pengelolaan dengan menentukan level risiko dari hasil perhitungan matematis.

H. Identifikasi dan Evaluasi Penanganan Risiko

Pada tahap identifikasi dan evaluasi penanganan risiko ini dilakukan pemilihan penanganan risiko yang terdiri atas langkah apa yang harus dilakukan yaitu :

i. Menentukan pilihan terhadap pengelolaan risiko yang terdiri atas : menerima risiko dan menerapkan kontrol yang sesuai, menerima risiko dengan mengirim risiko ke pihak ketiga (*Vendor*, *supplier*, atau pihak ketiga).

Hasil dari proses perencanaan adalah dokumen pengelolaan risiko yang kemudian digunakan untuk mendukung proses penyusunan dokumen kontrol objektif dan kontrol keamanan.

3.2.2 Kontrol Objektif dan Kontrol Keamanan Pengelolaan Risiko

Pada proses ini dilakukan pemilihan kontrol keamanan dan kontrol objektif yang ada di standar ISO 27001:2013 dan disesuaikan dengan hasil identifikasi

Potential Cause, identifikasi risiko, penilaian risiko, evaluasi risiko dan evaluasi penanganan risiko yang nantinya akan digunakan pada proses selanjutnya yaitu perencanaan kebijakan beserta pembuatan SOP, IK, dan RK. Pemilihan kontrol objektif dan kontrol keamanan terdiri atas :

1. Pembuatan tabel pengisian dari identifikasi aset yang dihasilkan dari penerapan identifikasi risiko.
2. Pembuatan tabel kontrol objektif yang disesuaikan dengan hasil penerapan identifikasi risiko.
3. Memilih penanganan risiko keamanan informasi dengan mempertimbangkan hasil dari pengelolaan risiko.
4. Menentukan kontrol objektif dan kontrol yang dibutuhkan untuk menerapkan penanganan risiko keamanan informasi yang dipilih.

Hasil dari proses pemilihan kontrol objektif dan kontrol keamanan adalah dokumen kontrol objektif dan kontrol keamanan yang selanjutnya digunakan untuk mendukung penyusunan dokumen *Standart Operational Procedure* (SOP)

3.2.3 *Standart Operational Procedure* (SOP)

Standar Operasional Prosedur (SOP) ini disusun melalui pemilihan kontrol objektif dan kontrol dengan melakukan identifikasi terhadap kebutuhan yang ada SOP. Setelah dilakukan identifikasi maka dilakukan penyusunan terhadap SOP beserta dokumen kebijakan, instruksi kerja dan rekam kerja.

A. Kebijakan keamanan Informasi

Kebijakan keamanan informasi ini dibuat untuk mengontrol dan mengatur alur dalam mengamankan sebuah informasi secara langsung ataupun secara tidak langsung.

B. Instruksi Kerja

Instruksi kerja ini dibuat untuk menguraikan bagaimana satu langkah dalam suatu prosedur dilakukan dan hanya melibatkan satu fungsi saja sebagai pendukung prosedur kerja.

C. Rekam Kerja

Rekam kerja ini digunakan sebagai bukti jika prosedur sudah dilaksanakan, rekam kerja ini berupa tabel.

3.3 Tahap Akhir

Pada tahapan terakhir yaitu menentukan hasil dari proses yang sudah dilakukan pada tahap pengembangan, sehingga menghasilkan keluaran sebagai berikut.

3.3.1 Hasil Analisis dan Pembahasan

Pada tahap ini menjelaskan mengenai hasil dari pengerjaan Tugas Akhir yang diperoleh dari hasil penelitian yang sudah dilakukan sesuai dengan metode yang digunakan untuk pelaksanaan.

3.3.2 Kesimpulan dan Saran

Pada tahap menjelaskan hasil kesimpulan dan saran yang didapatkan dari pembahasan yang sudah dilakukan dan dapat digunakan untuk mengembangkan topik pada Tugas Akhir ini.

BAB IV

HASIL DAN PEMBAHASAN

Bab IV pada penelitian ini akan membahas mengenai hasil dari Dokumen Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan ISO 27001:2013 Pada Bagian AAK Universitas Dinamika. Maka hasil yang didapat mulai dari proses tahap awal, tahap pengembangan, dan tahap akhir adalah sebagai berikut :

4.1 Tahap Awal

Pada tahap awal dilakukan proses studi literatur, identifikasi dan analisis dengan tujuan mendapatkan data dan sumber untuk melaksanakan penelitian ini, hasil dari tahap awal nantinya akan digunakan pada tahap selanjutnya yaitu tahap pengembangan.

4.1.1 Studi Literatur

Dalam menyusun penelitian perlu dilakukan teknik penyusunan secara sistematis dengan tujuan memudahkan langkah–langkah yang akan diambil pada tahap penyusunan. Sesuai dengan tahapan yang sudah ada pada metodologi penelitian, tahap awal yaitu melakukan studi literatur, dengan mencari referensi berupa buku beserta jurnal yang membahas keamanan informasi dan jurnal yang berkaitan dengan keamanan informasi.

Data yang di hasilkan dari pelaksanaan studi pustaka digunakan sebagai acuan penyusunan laporan ini, yaitu sebagai berikut :

1. Konsep–konsep keamanan informasi yang digunakan untuk menyusun dokumen aset, mengelola keamanan informasi dan menentukan kontrol objektif serta kontrol keamanan.
2. Konsep-konsep pengelolaan risiko keamanan informasi yang digunakan untuk menyusun pengelolaan risiko
3. Sistem manajemen keamanan informasi digunakan dalam penyusunan langkah-langkah dalam menentukan kontrol objektif dan kontrol keamanan.
4. Konsep penyusunan SOP berdasarkan peraturan dan langkah-langkah yang ada di peraturan daerah.

4.1.2 Identifikasi dan Analisis Masalah

A. Pengumpulan Data

Selain menggunakan metode dan referensi yang tepat dalam menyusun penelitian, penggunaan teknik untuk melakukan pengumpulan data yang relevan dan data obyektif juga dibutuhkan.

Teknik dan langkah-langkah yang digunakan dalam mengumpulkan data-data pada penelitian ini adalah sebagai berikut :

1. Wawancara

Tujuan dari wawancara ini adalah untuk mengetahui dan mendapatkan kebutuhan informasi serta data yang berkaitan dengan topik penelitian ini, wawancara ini dilakukan bersama dengan kepala Bagian AAK yaitu Ibu Sekar Dewanti selaku kepala Bagian AAK. Adapun uraian dari hasil wawancara yang dilakukan adalah sebagai berikut :

a. Visi, misi, tujuan instansi

Berdasarkan hasil wawancara terkait visi, misi dan tujuan organisasi yang dilakukan bersama Ibu Sekar Dewanti A.Md selaku kepala Bagian AAK dapat dilihat pada lampiran 2 visi, misi dan tujuan.

b. Struktur organisasi dan tugas pokok setiap bagian pada Bagian AAK

Struktur organisasi beserta tugas pokok setiap bagian pada Bagian AAK dijelaskan pada lampiran 2 struktur organisasi dan tugas pokok

c. Proses bisnis dan kebijakan pelayanan

Kebijakan pelayanan ini terkait proses layanan pada operasional yang dijalankan oleh Bagian AAK dan berkaitan dengan proses bisnis yang dimiliki oleh Bagian AAK, kebijakan pelayanan dan proses bisnis ini dijelaskan pada lampiran 3 dokumen kebijakan layanan dan proses bisnis.

d. Daftar risiko terkait keamanan informasi yang ada pada Bagian AAK

Daftar risiko ini merupakan hasil rekapitulasi kejadian yang pernah terjadi di Bagian AAK, serta tindakan yang pernah dilakukan. Daftar risiko dapat dilihat pada lampiran 4 daftar risiko.

2. Observasi

Observasi pada penelitian ini di lakukan pada proses bisnis yang dimiliki oleh Bagian AAK dengan tujuan mendapatkan data terkait masalah yang akan diselesaikan pada topik penelitian, sehingga diperoleh pemahaman secara langsung dari pengamatan yang dilakukan. Hasil dari observasi yang di lakukan pada Bagian AAK yaitu berupa narasi proses bisnis dan lengkap dengan gambar *flowchart* proses bisnis dan kebijakan pelayanan terdapat pada lampiran 3 proses bisnis, berikut beberapa proses bisnis dari Bagian AAK :

a. Proses bisnis Bagian AAK

1. Registrasi Mahasiswa baru
2. Perencanaan Perkuliahan
3. Perkuliahan
4. Ujian dan penilaian
5. Yudisium
6. Penerbitan surat penting mahasiswa
7. Permintaan *legalisir* ijazah dan transkrip
8. Penyedia penentuan data beasiswa
9. Penerbitan kartu tanda mahasiswa (KTM)

B. Identifikasi Masalah

Identifikasi masalah terjadi pada Bagian AAK saat ini yaitu untuk melakukan identifikasi risiko yang mengacu pada ISO 27005, identifikasi ini berkaitan dengan keamanan informasi, risiko keamanan informasi, aset-aset penting uang dimiliki organisasi termasuk aset kritis, kebutuhan keamanan informasi serta penerapan keamanan informasi yang sudah dilakukan atau sedang dilakukan.

Penerapan keamanan informasi yang sedang dilakukan yaitu tentang *Threat* (Ancaman) dan *Vulnerability* (Kelemahan) yang terjadi pada Bagian AAK, yang mempengaruhi *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan), dan *Availability* (Ketersediaan) yang akan berdampak pada *Business impact Analysis* (BIA) yang ada di Bagian AAK. Hasil lain dari identifikasi masalah dapat dilihat pada lampiran 5 identifikasi masalah. Daftar risiko yang berada pada lampiran berkaitan dengan proses registrasi mahasiswa baru, perencanaan kuliah,

perkuliahan, ujian, penilaian, yudisium. Hasil keluaran daftar risiko tersebut akan menjadi masukan untuk proses analisis masalah yang terkait dengan topik penelitian ini.

C. Analisis Masalah

Analisis masalah yang dapat diberikan berdasarkan identifikasi masalah yang terdapat pada tabel daftar risiko yang ada pada lampiran 5 identifikasi masalah, bertujuan untuk memberikan solusi terhadap permasalahan yang ditemukan terkait keamanan informasi yang mempengaruhi 3 (tiga) faktor keamanan informasi yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan) dan *Availability* (Ketersediaan) yang dapat berdampak pada *Business Impact Analisys* (BIA). Terkait dengan proses registrasi mahasiswa baru, perencanaan kuliah, perkuliahan, ujian, penilaian, yudisium. Oleh karena itu, bentuk dukungan pada pengendalian sistem manajemen keamanan informasi dari sisi faktor-faktor keamanan informasi adalah menyusun dokumen pengelolaan risiko terkait dengan keamanan informasi serta penyusunan dokumen *Standart Operational Procedure* (SOP) dengan tujuan sebagai acuan kerja dan *standarisasi* Bagian AAK agar lebih meningkatkan keamanan informasi yang ada.

4.2 Tahap Pengembangan

Tahap pengembangan merupakan tahap akhir dari tahapan penelitian ini, tahap pengembangan ini akan menjelaskan proses dari tahap-tahap yang ada pada tahap pengembangan yaitu dokumen pengelolaan risiko keamanan informasi yang berisi dokumen aset dengan proses identifikasi aset, menentukan ruang lingkup SMKI, menentukan kebijakan SMKI. Kemudian proses pengelolaan risiko,

identifikasi *Potential Cause,* identifikasi risiko, penilaian risiko, evaluasi penanganan risiko merupakan proses-proses yang menjadi satu pada dokumen pengelolaan risiko keamanan risiko keamanan informasi. Pada dokumen selanjutnya adalah dokumen kontrol objektif dan kontrol keamanan yang berisi tentang pemilihan kontrol objektif dan kontrol keamanan, serta dokumen SOP yang berisi proses pembuatan SOP.

4.2.1 Perencanaan SMKI

pada tahap perencanaan SMKI, terdapat beberapa proses yang nantinya akan digunakn tahap selanjutnya, tahap-tahap tersebut terdiri atas menentukan ruang lingkup, menentukan kebijakan, identifikasi aset, identifikasi risiko, penilaian risiko, analisis dan evaluasi risiko serta identifikasi dan evaluasi. Tahap-tahap nya adalah sebagai berikut :

A. Menentukan Ruang Lingkup SMKI

Berdasarkan wawancara dan kesepakatan yang dilakukan dengan Ibu Sekar Dewanti A.Md selaku kepala di Bagian AAK. Keamanan teknologi informasi universitas dinamika berada pada bagian pengembangan dan penerapan teknologi informasi. Bagian AAK memiliki fungsi mengelola administrasi registrasi mahasiswa baru, pelaksana administrasi akademik, dan pelaksana administrasi kemahasiswaan yang merupakan kriteria utama melakukan penilaian terhadap keamanan informasi pada Bagian AAK. Untuk menentukan ruang lingkup SMKI, organisasi harus memiliki komitmen dalam melindungi informasi, degan tujuan untuk memenuhi kebutuhan organisasi dalam merencanakan SMKI agar sesuai dengan standar uang digunakan sebagai acuan, yaitu ISO 27001:2013. Perencanaan SMKI pada ruang lingkup organisasi yaitu terdiri atas :

a. Bagian Administrasi Akademik, Bagian Kemahasiswaan, Bagian Keuangan, Bagian *Marketing*, Bagian Program Studi, Unit Kerja Perpustakaan, Unit kerja Laboratorium, Unit kerja Administrasi umum, dan Unit kerja Pengembangan dan Penerapan Teknologi Informasi.
b. Proses registrasi mahasiswa baru, perencanaan kuliah, perkuliahan, ujian, penilaian, dan yudisium.
c. Aset TI internal yang digunakan AAK untuk aktivitas bisnis meliputi aset data berupa informasi, jaringan komputer, aset *software* yang berbentuk aplikasi dan *hardware*, serta aset infrastruktur, dan sumber daya manusia.

B. Menentukan Kebijakan SMKI

Penentuan kebijakan ini ditentukan melalui hasil pemetaan yang dapat dilihat pada sub-bab 4.2.3 *Standart Operational Procedure* (SOP). Pada sub-bab tersebut dilakukan perencanaan kebijakan yang di mana mengacu pada sub-bab 4.2.2 Kontrol Objektif dan Kontrol Keamanan yang berisikan hasil pemetaan kontrol objektif dan kontrol keamanan yang di ambil dari standar ISO 27001:2013 yang sudah disesuaikan dengan hasil dari identifikasi *Potential Cause,* identifikasi risiko, dan penilaian risiko.

Setelah perencanaan kebijakan selesai, selanjutnya dilakukan pemetaan untuk menghasilkan prosedur, instruksi kerja, rekam kerja sebagai dokumen pendukung dari kebijakan. Untuk detail kebijakan, prosedur, instruksi kerja dan rekam kerja dapat dilihat pada lampiran 5.

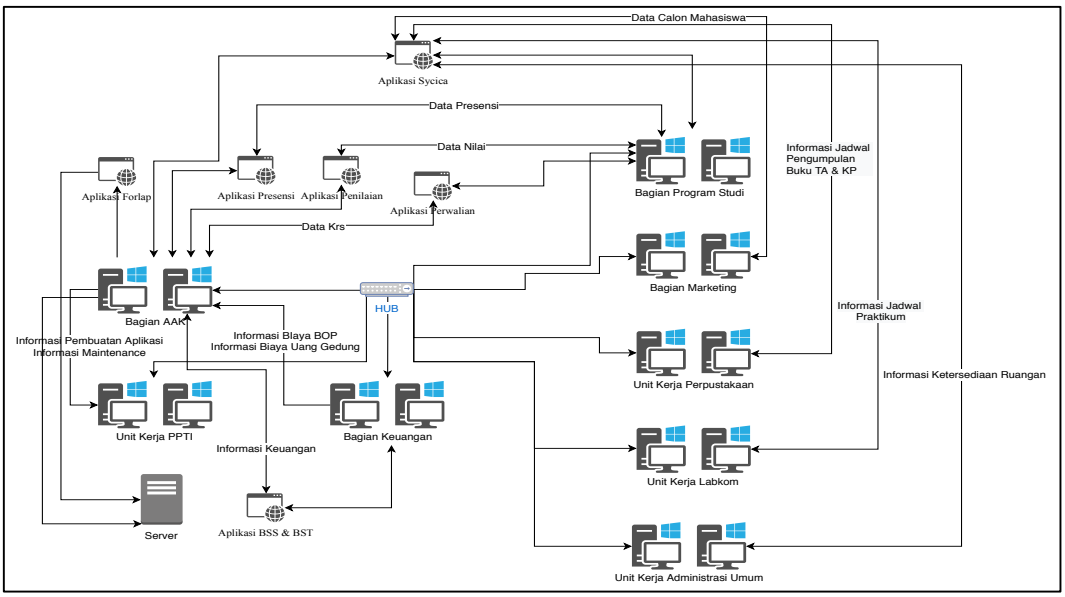
C. Identifikasi Aset

Identifikasi aset yang dilakukan berkaitan dengan aset-aset yang dimiliki oleh Bagian AAK mulai dari aset yang berupa benda seperti infrastruktur maupun yang bersifat informasi seperti data. Berdasarkan proses *Profiling* menggunakan IAP aset dikelompokkan dan disesuaikan melalui latar belakang aset, dan pengguna aset. Untuk detail dari proses identifikasi aset dapat dilihat pada lampiran 9

1. Pengelompokan Aset Berdasarkan Lokasi dan Penanggung jawab

Pada proses ini dilakukan pengelompokan aset yang dimiliki dan digunakan oleh Bagian AAK, dengan tujuan untuk mengetahui siapa penanggung jawab dan lokasi dari aset tersebut, dikarenakan aset yang digunakan oleh Bagian AAK terdapat pada beberapa bagian dan unit kerja di mana memiliki keterkaitan antara satu dengan yang lain, sehingga dilakukan pengelompokan agar lebih pada saat melakukan pengelolaan risiko terhadap aset-aset tersebut. Untuk detail dari pengelompokan dapat dilihat pada lampiran 9.

2. *Flow Of Information*



Gambar 4. 1 *Flow Of Information*

Gambar di atas menjelaskan mengenai alur informasi dari Bagian AAK ke beberapa bagian dan unit kerja, alur informasi tersebut bertujuan untuk mengetahui data dan informasi yang perlu di lindungi dikarenakan Bagian AAK memiliki keterkaitan data dan informasi dengan beberapa bagian lain, sehingga perlu diketahui alur informasi yang mengalir dari Bagian AAK ke bagian lain guna mempermudah dalam melakukan pengelompokan aset yang dimiliki oleh Bagian AAK. Penjelasan lebih detail dapat dilihat pada lampiran 10

3. Perhitungan Nilai Aset

Perhitungan nilai aset memiliki tabel yang digunakan sebagai acuan dalam menghitung nilai-nilai dari *confidentiality* (Kerahasiaan), nilai *Integrity* (Keutuhan), nilai *Availability* (Ketersediaan) dan disesuaikan dengan beberapa kriteria seperti *Public*, *Internal Use Only, Private, Confidential,* dan *Secret.* untuk detail perhitungan dapat dilihat pada lampiran 9.

D. Identifikasi *Potential Cause*

Identifikasi *Potential Cause* ini dimaksudkan untuk mengetahui ancaman dan kelemahan yang dapat mempengaruhi aset-aset yang dimiliki oleh instansi, aset-aset tersebut di kategorikan pada beberapa aset yaitu perangkat keras, data, perangkat lunak, dan jaringan. Tabel ancaman digunakan sebagai acuan untuk pembagian jenis ancaman yang timbul, daftar berikut menunjukkan setiap jenis ancaman di mana A (tidak disengaja), D (disengaja) dan E (lingkungan). D digunakan untuk semua tindakan sengaja ditujukan untuk aset informasi, A digunakan untuk semua tindakan SDM yang tidak sengaja dapat merusak aset informasi, dan E digunakan untuk semua insiden yang tidak didasarkan pada tindakan manusia. Detail dari jenis ancaman dapat dilihat pada lampiran 11

E. Identifikasi Risiko

Sebelum tahapan analisis dan evaluasi risiko, terlebih dahulu akan dilakukan identifikasi risiko yang dapat mengancam aset informasi Bagian AAK Universitas Dinamika. Risiko yang dimaksud adalah kejadian yang memiliki probabilitas untuk terjadi dan bahkan sering terjadi. Baik yang disebabkan oleh faktor internal maupun eksternal instansi yaitu bencana alam, kesalahan manusia, dan operasional. Tabel identifikasi risiko dapat dilihat pada lampiran 12

F. Penilaian Risiko

Pada tahap ini akan menjelaskan secara detail terhadap risiko yang telah diidentifikasi dengan menggunakan metode *Failure and Effect Analysis* (FMEA), penilaian risiko ini ditentukan berdasarkan tingkat *Severity, Occutance*, dan *Detection* yang nantinya akan digunakan untuk menghitung *Risk Priority Number*

(RPN) parameter dari level *Severity, Occutance*, dan *Detection.* Rentang nilai yang digunakan untuk *Risk Priority Number* (RPN), untuk menentukan level yang muncul menggunakan rentang nilai yang dapat dilihat pada lampiran 13

1. Penentuan Kemungkinan (*Probability*)

Pada proses penentuan kemungkinan ini adalah menentukan kemungkinan ancaman yang akan timbul dan di sesuai kan dengan ancaman, dan kelemahan. Setelah dilakukan penilaian risiko, maka selanjutnya adalah menentukan nilai rata-rata probabilitas munculnya ancaman dan kelemahan dengan menggunakan rentang nilai sebagai berikut :

- *Low* : nilai rata-rata probabilitas 0,1 – 0,3
- *Medium* : nilai rata-rata probabilitas 0,4 – 0,6
- *High* : nilai rata-rata probabilitas 0,7 – 1,0

Untuk detail penentuan kemungkinan dapat dilihat pada lampiran 13

2. Identifikasi Konsekuensi Jika Terjadi Kegagalan

Identifikasi konsekuensi atau dampak risiko yang di timbulkan oleh ancaman dan kelemahan terhadap organisasi atau jalannya proses bisnis organisasi jika terjadi kegagalan pada penanganan aspek keamanan informasi (CIA).

Pada proses identifikasi konsekuensi ini dilakukan identifikasi secara satu persatu pada setiap aset agar didapatkan konsekuensi pada setiap aset yang sudah teridentifikasi pada proses identifikasi aset. Untuk detail tabel identifikasi konsekuensi dapat dilihat pada lampiran 14

G. Analisis dan Evaluasi Risiko

1. Analisis Konsekuensi Keamanan Informasi Terhadap Bisnis

Analisis konsekuensi ini dilakukan untuk mengetahui *Business Impact Analysis* pada aset-aset yang sudah di identifikasi pada langkah sebelumnya. Nilai masing-masing layanan yang dimiliki Bagian AAK yang terdiri atas layanan registrasi mahasiswa baru, perencanaan kuliah, perkuliahan, ujian, penilaian, serta yudisium dapat dilihat pada lampiran 15

2. Identifikasi Level Risiko

Identifikasi level risiko yaitu proses identifikasi tingkat risiko yang muncul jika dihubungkan dengan ancaman dan probabilitas ancaman yang mungkin dapat terjadi. Dengan dampak yang mungkin timbul pada masing-masing aset yang sudah dilakukan perhitungan pada langkah 4. Untuk detail tabel dapat dilihat pada lampiran 15

3. Penentuan Risiko Diterima atau Perlu Penanganan

Pada proses ini yaitu menentukan risiko yang dapat diterima atau risiko tersebut memerlukan penanganan atau tidak. Yaitu dengan cara menghitung nilai dari masing-masing yang sudah teridentifikasi, kemudian hasil dari perhitungan yang telah dilakukan, selanjutnya adalah langkah menentukan nilai risiko dari masing-masing aset yang dapat dilihat lampiran 15

H. Identifikasi dan Evaluasi Penanganan Risiko

Evaluasi penanganan risiko ini bertujuan untuk mengetahui langkah penanganan risiko yang timbul, baik risiko yang bisa di terima atau risiko yang di terima akan tetapi perlu pengelolaan lebih lanjut dengan mengacu pada kriteria

risiko yang telah di tetapkan sebelumnya. Pemilihan penanganan risiko pada Bagian AAK ditentukan sebagai berikut :

1. Mengurangi risiko dengan menyesuaikan dan menetapkan kontrol keamanan
2. Mengurangi risiko dengan menggunakan kriteria dan penilaian risiko yang ada

4.2.2 Kontrol Objektif dan Kontrol Keamanan

Setelah melakukan evaluasi dan penetapan penanganan risiko, langkah berikutnya adalah memilih kontrol keamanan yang dengan aset yang memiliki level risiko tertinggi, di mana penetapan kontrol objektif dan kontrol keamanan harus sesuai dengan ancaman dan kelemahan dari masing-masing aset yang telah dipilih di tabel ancaman dan kelemahan.

Tujuan dari pemilihan kontrol objektif dan kontrol keamanan ini dijadikan dasar dalam penyusunan prosedur kontrol dalam pengelolaan risiko. Berikut ini adalah kontrol objektif dan kontrol keamanan yang digunakan untuk masing-masing aset berdasarkan ISO 27001:2013. Detail dari pemetaan kontrol objektif dan kontrol keamanan dapat dilihat pada lampiran 16

4.2.3 *Standart Operational Procedure* (SOP)

A. Penjelasan Perencanaan Kebijakan dan Prosedur

Tahap ini akan menjelaskan mengenai proses penyusunan kebijakan dan prosedur. Kebijakan dan prosedur tersebut di susun berdasarkan penilaian risiko keamanan informasi yang memiliki tingkatan *High, Medium,* dan *Low*. dilihat dari hasil pemetaan risiko dengan kontrol ISO 27001:2013 dengan prosedur dan

kebijakan yang dihasilkan di atas didapatkan 6 kebijakan dan 6 prosedur di mana kebijakan dan prosedur dibuat berdasarkan hasil rekomendasi pengendalian risiko dan risiko yang terjadi. Penjelasan dari pembentukan dapat dilihat pada lampiran 17

B. Perancangan Struktur dan Daftar Isi SOP

Pada tahap ini akan menjelaskan mengenai bagaimana peneliti merancang SOP. Perancangan SOP ini mengacu pada peraturan pemerintah (Lampiran) yang membahas mengenai penyusunan standar operasional prosedur. Penyusunan SOP pada penelitian ini akan disesuaikan dengan kebutuhan sehingga isi dari SOP secara keseluruhan memiliki perbedaan dengan isi dari SOP yang digunakan sebagai acuan. Adapun struktur atau isi yang akan dimasukkan ke dalam kerangka SOP keamanan informasi pada Bagian AAK dapat dilihat pada tabel 4.58 yang berada di lampiran 17

C. Hasil Perencanaan SOP

Pada tahap ini akan menjelaskan mengenai detail dari kebijakan dan prosedur beserta dokumen–dokumen pendukung yang terdiri atas instruksi kerja dan rekam kerja di mana dibutuhkan pada setiap proses yang ada di dalamnya.

1. Hasil Perencanaan Kebijakan

Hasil dari penyusunan kebijakan ini bertujuan untuk mendukung pelaksanaan SOP yang di mana membutuhkan dokumen-dokumen pendukung yaitu rekam kerja yang digunakan sebagai dokumentasi pada setiap langkah-langkah yang dilakukan.

Pada tabel berikut merupakan tabel perencanaan kebijakan *Human Resource Security* detail dapat dilihat pada tabel 4.1. Untuk hasil dari tabel perencanaan kebijakan yang lain dapat dilihat pada lampiran 5

Tabel 4. 1 Tabel Hasil Perencanaan Kebijakan *Human Resource Scurity*

	UNIVERSITAS DINAMIKA SURABAYA	
	Administrasi akademik dan kemahasiswaan	
	No. DOKUMEN	
	TGL PEMBUATAN	
	TGL REVISI	
	NAMA DOKUMEN	KB - *Human resource security*
1. Tujuan Kebijakan ini dibuat untuk memberikan panduan kepada seluruh *staff* instansi dalam memberikan perlindungan keamanan pada aset yang dimiliki oleh instansi		
2. Detail kebijakan • Program *awareness* (peringatan kesadaran) terkait keamanan informasi untuk para pegawai agar menyadari akan tanggung jawab mereka untuk keamanan informasi instansi dan supaya mereka tidak mengabaikannya • Program *awareness* (peringatan kesadaran) terkait keamanan informasi harus ditetapkan sesuai dengan kebijakan dan prosedur instansi • Program *awareness* (peringatan kesadaran) harus direncanakan dengan mempertimbangkan peran pegawai dalam organisasi. Kegiatan ini harus dijadwalkan dari waktu ke waktu secara teratur sehingga kegiatan ini mampu diikuti oleh pegawai yang baru. Program ini juga harus diperbarui secara berkala sehingga tetap sejalan dengan kebijakan dan prosedur organisasi, dan juga dapat diperbarui dari insiden keamanan informasi yang pernah terjadi • Program *awareness* (peringatan kesadaran) harus dilakukan sesuai kebutuhan keamanan informasi organisasi. *Awareness training* dapat menggunakan media pengiriman yang berbeda, pembelajaran jarak jauh berbasis web dan lain-lain		
3. Dokumen terkait • PR – 01 Pelatihan dan pengembangan		

2. Hasil Perencanaan Prosedur

Hasil dari penyusunan prosedur ini bertujuan untuk mendukung pelaksanaan SOP yang di mana membutuhkan dokumen-dokumen pendukung yaitu instruksi kerja yang digunakan sebagai acuan pada setiap langkah-langkah

yang dilakukan. Pada tabel berikut merupakan hasil perencanaan prosedur detail dapat dilihat pada tabel 4.2. Untuk hasil dari perencanaan prosedur dapat dilihat pada lampiran 5

Tabel 4. 2 Tabel Hasil Perencanaan Prosedur Pelatihan dan Pengembangan

UNIVERSITAS DINAMIKA SURABAYA	No. Dokumen	
	Tanggal pembuatan	
	Tanggal revisi	
	Tanggal efektif	
	Disahkan oleh	
Administrasi akademik dan kemahasiswaan	Nama Dokumen	Pelatihan dan pengembangan

Deskripsi	**Daftar pelaksana dan kualifikasi**
Prosedur pelatihan dan pengembangan merupakan prosedur yang mengatur *training* atau edukasi terkait dengan keamanan informasi dengan tujuan meningkatkan kualitas *staff* secara intelektual maupun kepribadian sehingga diharapkan mampu menjaga aset keamanan informasi	**Daftar pelaksana** • *Staff* Bagian AAK • Kepala Bagian AAK • *Staff* administrasi umum **Kualifikasi pelaksana** • Memiliki hak akses data • Memiliki kemampuan pemahaman terhadap proses bisnis • Mampu berkomunikasi dengan baik
Keterkaitan	**Persyaratan**
• KB – 01 Kebijakan *human resource security* • IK – 01 Pelatihan dan pengembangan	• Surat penugasan • RK – 01 evaluasi pelatihan dan pengembangan
Peringatan	**Pencatatan**
Jika SOP tidak di lakukan maka dapat mempengaruhi kinerja *staff* dalam mengelola informasi instansi sehingga dapat menyebabkan risiko hilangnya data Bagian AAK	• Pencatatan rekam kerja evaluasi pelatihan dan pengembangan

3. Hasil Perencanaan Instruksi Kerja

Hasil dari penyusunan instruksi kerja ini bertujuan untuk mendukung pelaksanaan SOP yang di mana membutuhkan dokumen instruksi kerja yang berguna untuk mendokumentasikan aktivitas. Pada tabel berikut merupakan hasil perencanaan instruksi kerja detail dapat dilihat pada tabel 4.3. Berikut merupakan

hasil penyusunan instruksi kerja tersebut. Untuk hasil dari perencanaan instruksi kerja dapat dilihat pada lampiran 5

Tabel 4. 3 Tabel Hasil Instruksi Kerja Pelatihan dan Pengembangan

	UNIVERSITAS DINAMIKA Administrasi akademik dan kemahasiswaan
	No. rilis : No. revisi : Tanggal terbit :
	IK – 01 – PELATIHAN DAN PENGEMBANGAN
1. PELAKSANA a. *Staff* Bagian AAK b. Kepala Bagian AAK c. *Staff* administrasi umum	
2. DETAIL INSTRUKSI KERJA a. Proses pengadaan pelatihan dan pengembangan i. Membuat permintaan pelaksanaan kegiatan pengembangan (a) ii. Membuat permohonan pelaksanaan(a) iii. Apakah permohonan disetujui (b) iv. Disetujui proses berlanjut (b) v. Pemberian informasi mengenai kegiatan pelatihan dan pengembangan (c) b. Proses persiapan pelatihan i. Mempersiapkan tempat dan peralatan(c) c. Proses pelatihan dan pengembangan i. Mengikuti proses pelatihan(a) ii. Mengisi absensi(a) iii. Membuat laporan kegiatan(a) d. Proses evaluasi pelatihan dan pengembangan i. Pembuatan laporan pertanggung jawaban kegiatan(a) ii. Melakukan evaluasi (b) iii. Penilaian tahunan(b) iv. Ditolak kembali melakukan sub – proses 1 – 2(a)	
3. PENCATATAN PERUBAHAN INSTRUKSI KERJA	
No.	**TANGGAL PERUBAHAN** / **DETAIL PERUBAHAN**

4. Hasil Perencanaan Rekam Kerja

Hasil dari penyusunan prosedur ini bertujuan untuk mendukung pelaksanaan SOP yang di mana membutuhkan dokumen rekam kerja yang berguna untuk mendokumentasikan aktivitas yang mendukung SOP. Pada tabel berikut merupakan hasil perencanaan rekam kerja detail dapat dilihat pada tabel 4.3. Untuk

hasil dari perencanaan instruksi kerja dapat dilihat pada lampiran 5. Berikut merupakan hasil penyusunan instruksi kerja tersebut.

Tabel 4. 4 Tabel Hasil Perencanaan Rekam Kerja Evaluasi Pelatihan dan Pengembangan

		UNIVERSITAS DINAMIKA SURABAYA Administrasi akademik dan kemahasiswaan	
		No. rilis	:
		No. revisi	:
		Tanggal terbit	:
		RK – EVALUASI PELATIHAN DAN PENGEMBANGAN	
Nama	**:**	**Jabatan**	**:**
Unit kerja/bagian	**:**	**Tgl pelatihan**	**:**
Tujuan pelatihan :			
Evaluasi	**:**		
	☐ Setelah pelatihan	☐ 2 minggu setelah pelatihan	
	☐ 1 minggu setelah pelatihan	☐ 3 minggu setelah pelatihan	
	☐ Lain – lain.		
Metode yang digunakan	**:**		
	☐ Tes/ujian	☐ Observasi	
Kelengkapan	**:**		
	☐ Ruangan	☐ dan lain – lain . . .	
Di ketahui oleh, **Kepala Bagian AAK**		**Diketahui oleh**	
NIDN.		**NIDN . . . . . .**	

4.3 Tahap Akhir

Pada tahap akhir ini akan menjelaskan mengenai hasil dari penelitian ini yang terdiri atas output atau hasil akhir dari penelitian ini, untu detail akan dijelaskan pada proses berikut :

4.3.1. Hasil Analisis dan Pembahsan

Pada tahap analisis akan membahas terkait dengan proses dan output dari penelitian ini, penjelasanya dapat dilihat pada tabel 4.5

Tabel 4. 5 Hasil Analisis dan Pembahasan

Proses	Output	Deskripsi
1. Pemetaan klausul dengan kontrol objektif dan kontrol keamanan 2. Pemetaan risiko dengan kontrol keamanan 3. Pemetaan klausul dengan kebutuhan keamanan informasi 4. Pemetaan risiko dengan dokumen kebijakan 5. Pemetaan kebijakan, instruksi kerja, dan rekam kerja	1. Kebijakan *Human resource security* 2. Kebijakan keamanan fisik 3. Kebijakan kontrol akses 4. Kebijakan penanganan keamanan informasi 5. Kebijakan penggunaan otentikasi 6. Kebijakan keamanan pengguna 7. Kebijakan penanganan perangkat jaringan 1. Intruksi kerja pelatihan dan pengembangan 2. Instruksi kerja Penanganan fisik hardware 3. instruksi kerja pengelolaan hak akses	1. Pada proses pemetaan klausul dihasilkan dari (Standar ISO 27001:2013) 2. Pada proses pemetaan risiko dengan kontrol keamanan dihasilkan dari (identifikasi aset, identifikasi *Potential Cause*, identifikasi risiko) 3. Pada proses pemetaan klausul dengan kebutuhan keamanan informasi dihasilkan dari (identifikasi aset, identifikasi *Potential Cause*, klausul, kontrol objektif dan kontrol keamanan)

Proses	Output	Deskripsi
	4. Instruksi kerja peran dan tanggung jawab penyampaian informasi 5. Instruksi kerja Pengelolaan otentikasi 6. Instruksi kerja keamanan pengguna 7. Instruksi kerja perawatan perangkat keras jaringan	4. Pada proses pemetaan risiko dengan dokumen kebijakan dihasilkan dari (identifikasi aset, identifikasi risiko, kategori kebutuhan dari hasil pemetaan antara klausul dengan kebutuhan keamanan informasi, kontrol keamanan)
	1. Rekam kerja evaluasi pelatihan dan pengembangan 2. Rekam kerja pemantauan kondisi perangkat 3. Rekam kerja pengelolaan hak akses 4. Rekam kerja log penggunaan hak akses 5. Rekam kerja monitoring keamanan informasi 6. Rekam kerja log otentikasi 7. Rekam kerja log akses pengguna	5. Pada proses pemetaan kebijakan, instruksi kerja, dan rekam kerja dihasilkan dari (pemetaan risiko dengan kebijakan, pemetaan klausul dengan kebutuhan keamanan informasi)

4.3.2 Kesimpulan dan Saran

Pada tahap ini didapat kesimpulan dan saran yaitu hasil dari penelitian ini dapat dikembangkan lagi , yaitu dengan melakukan implementasi dan kemudian dilakukan penyusunan dokumen evaluasi keamanan informasi. Detail dapat dilihat pada bab V.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari penyusunan Tugas Akhir yang didapatkan dari penelitian ini dan sudah disesuaikan dengan metode yang sudah direncanakan, menghasilkan kesimpulan sebagai berikut :

1. Pada penyusunan tahap perencanaan SMKI dihasilkan beberapa proses yang terdiri atas menentukan ruang lingkup SMKI, menentukan kebijakan SMKI, Identifikasi aset, identifikasi *Potential Cause*, identifikasi risiko, penilaian risiko, identifikasi dan evaluasi penanganan risiko. Setelah dilakukan penyusunan tahap pengembangan, selanjutnya adalah menyusun dokumen kontrol objektif dan kontrol keamanan yang digunakan untuk mendukug penyusunan dokumen SOP yang terdiri atas kebijakan, instruksi kerja, dan rekam kerja.
2. Pada tahap penyusunan kontrol objektif dan kontrol keamanan, dihasilkan beberapa kebutuhan keamanan informasi, pemilihan kontrol objektif, dan kontrol keamanan menyesuaikan dengan hasil dari tahap pengembangan yang sudah dilakukan, yaitu dengan melakukan pemetaan terhadap risiko dengan kontrol objektif dan kontrol keamanan. Sehingga mengahasilkan delapan kontrol dari sisi *teknikal*, lima kontrol dari sisi manajemen dan delapan kontrol dari sisi operasional. Kemudian hasil dari kontrol ini akan digunakan untuk pemetaan dari hasil perencanaan SMKI dan digunakan pada tahap penyusunan dokumen SOP.

3. Pada tahap penyusunan dokumen SOP dihasilkan dokumen perencanaan SOP yang meliputi kebijakan keamanan informasi pada proses bisnis akademik, yang di dalam nya berisi instruksi kerja (IK) yang terdiri atas instruksi kerja penanganan fisik hardware, instruksi kerja pengolahan hak akses, instruksi kerja pengolahan kerentanan sistem, instruksi kerja klasifikasi keamanan informasi, instruksi kerja peran dan tanggung jawab, instruksi kerja backup dan restore data. Rekam kerja (RK) pemantauan kondisi perangkat keras, berita acara kerusakan, rekam kerja laporan penggunaan TI, rekam kerja log penggunaan hak akses, rekam kerja pelaporan kerentanan, rekam kerja pemantauan dan monitoring keamanan informasi, rekam kerja reset password, rekam kerja pemeliharaan perangkat keras jaringan, rekam kerja evaluasi kegiatan pelatihan.

5.2 Saran

Berikut ini merupakan beberapa saran yang diberikan pada penelitian Sistem manajemen keamanan informasi pada Bagian AAK :

1. Bagian AAK dapat memperluas ruang lingkup terkait dengan SMKI dengan tujuan perlindungan terhadap keamanan informasi menjadi lebih luas dan lengkap.
2. Bagian AAK dapat melaksanakan proses manajemen risiko keamanan informasi dan melaksanakan implementasi terhadap dokumen perencanaan SMKI yang telah dibuat.
3. Setelah dilakukan implementasi maka dapat dikembangkan dengan melaksanakan penyusunan dokumen evaluasi keamanan informasi

DAFTAR PUSTAKA

A.J McEachern, W. (2001). *Pengantar Ekonomi Makro.* Jakarta: PT. Salemba Empat.

Djohanputro, B. (2008). *Manajemen Risiko Korporat. Pendidikan dan Pembinaan Manajemen.* Jakarta.

Fahmi, I. (2010). *Manajemen Resiko.* Bandung, Jawa Barat: Alfabeta.

Forum, I. I. (2009). *Guideline for Information Asset Valuation.* ISO27k Implementer's Forum.

G.J, S., & Spafford, g. (1996). *Practical UNIX & Internet Security, O'Reilly & Associates,* (Inc,2 nd edition ed.).

Gordon, B. D. (1991). *Kerangka Dasar Sistem Informasi Manajemen Bagian 1.* Jakarta: PT. Pustaka Binamas Pressindo.

Hanafi, M. (2006). *Manajemen Risiko.* Yogyakarta: Unit Penerbit dan Percetakan Sekolah Tinggi Ilmu Manajemen YKPN.

Hughes, G. (2006). *Five Steps to IT Risk Manejement Best Practices.*

Indonesia, P. M. (2012). Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan, .

ISO/IEC 27001. (2013). *Information Technology-Security Techniques-Information Security Management System-Requirements.* ISO/IEC.

M.S, S. (2007). *Risiko Pengunaan Lahandan Analisisnya Laboratorium PPJP Jurusan Tanah.* Malang: FPUB.

Mardalis. (2003). *Metode Penelitian Suatu Pendekatan Proposal.* Jakarta: Bumi Aksara.

Muchtar, H. (2011). *Manajemen Aset (Privat dan Publik)*. Yogyakarta.

Nasional, B. S. (2009). *SNI ISO/IEC 27001 TeknologI Informasi Teknik Keamanan Sistem Manajemen Keamanan Informasi- Persyaratan.* Jakarta: Badan Standaridasi Nasional.

Peraturan Menteri Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Republik Indonesia. (2012). *Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintaha.*

Sarno, R., & Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*. Surabaya: ITSPress.

Sutabri, T. (2005). *Sistem Informasi Manajemen.* Jakarta.

Tambunan, R. M. (2013). *Pedoman Penyusunan Standard Operating Procedures (SOP)*. Jakarta: Masitas Publishing.

DAFTAR RIWAYAT HIDUP

Nama Lengkap	:	Rico Kurniawan
NIM	:	15410100036
Perguruan Tinggi	:	Universitas Dinamika
Jurusan	:	S1 Sistem Informasi
Tempat/Tgl. Lahir	:	Jember, 04 April 1996
Alamat	:	Br. Tunggal Sari Dauh Peken Tabanan bali
Agama	:	Islam
Telp/HP	:	082139619447
Email	:	15410100036@dinamika.ac.id

Riwayat Pendidikan

2003 – 2009	MI. Assalam 1 Wringin Agung Jombang
2009 – 2012	MTs. Al-Amin Tabanan
2012 – 2015	SMK Nasional Tabanan
2015 – Sekarang	Universitas Dinamika

Riwayat Pekerjaan

2017 – 2018	*Front-End Engineer* di Ananta Creative Media
2018 – 2020	*Bug Hunter* in *HackerOne*
2020 – Sekarang	*Penetration Tester* di netSPI llc (*Remote*)

Keorganisasian

2015 – 2016	Anggota Himpunan Mahasiswa Sistem Informasi
	Anggota *Dracos Linux* Region Bali
	Humas di Surabaya BlackHat (SBH)
	Anggota Surabaya HackerLink (SHL)