# PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA PT ANGKASA PURA 1 (PERSERO) SURABAYA

**TUGAS AKHIR**

**Program Studi**
**S1 SISTEM INFORMASI**

**Oleh:**
**YUSUF BAHRUDIN NIZAR**
**15410100185**

**FAKULTAS TEKNOLOGI DAN INFORMATIKA**
**UNIVERSITAS DINAMIKA**
**2021**

# PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2013 PADA PT ANGKASAPURA 1 (PERSERO) SURABAYA

**TUGAS AKHIR**

**Diajukan sebagai salah satu syarat untuk menyelesaikan**
**Program Sarjana Komputer**



**Oleh:**

**Nama : Yusuf Bahrudin Nizar**
**NIM : 15410100185**
**Program Studi : S1 Sistem Informasi**

**FAKULTAS TEKNOLOGI DAN INFORMATIKA**
**UNIVERSITAS DINAMIKA**
**2021**

**TUGAS AKHIR**

# PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA PT ANGKASA PURA 1 (PERSERO) SURABAYA

Dipersiapkan dan disusun oleh

**Yusuf Bahrudin Nizar**

**NIM: 15410100185**

Telah diperiksa, dibahas dan disetujui oleh Dewan Pembahas

Pada:

05 Agustus , 2021

**Susunan Dewan Pembahas**

**Pembimbing**

I. Pantjawati Sudarmaningtyas, S.Kom., M.Eng.
NIDN 0712066801

Digitally signed by Universitas Dinamika
Date: 2021.08.07 16:52:02 +07'00'

II. Slamet, M.T., CCNA
NIDN 0701127503

Digitally signed by Slamet A, DN: cn=Slamet A, o=Universitas Dinamika, ou=Information System Department, email=slamet@dinamika.ac.id, c=ID
Date: 2021.08.07 10:12:59 +07'00'

**Pembahas**

Dr. Haryanto Tanuwijaya, S.Kom., M.MT.
NIDN 0710036602

Digitally signed by Universitas Dinamika
Date: 2021.08.13 10:24:54 +07'00'

Tugas Akhir ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana

Digitally signed by Universitas Dinamika
Date: 2021.08.17 10:36:13 +07'00'

**Tri Sagirani, S.Kom., M.MT.**
NIDN: 0731017601

Dekan Fakultas Teknologi dan Informatika
UNIVERSITAS DINAMIKA

**PERNYATAAN**
**PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH**

Sebagai mahasiswa Universitas Dinamika, saya:

| | |
|---|---|
| Nama | : Yusuf Bahrudin Nizar |
| NIM | : 15410100185 |
| Program Studi | : S1Sistem Informasi |
| Fakultas | : Teknologi dan Informatika |
| Jenis Karya | : Tugas Akhir |
| Judul Karya | : **PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA PT ANGKASA PURA 1 (PERSERO) SURABAYA** |

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Universitas Dinamika Hak Bebas Royalti Non-Eklusif (*Non-Exclusive Royalti Free Right*) atas seluruh isi/ sebagian karya ilmiah saya tersebut di atas untuk disimpan, dialihmediakan 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 diatas 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 di kemudian 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, 05 Agustus 2021

Yang menyatakan


Yusuf Bahrudin Nizar
Nim: 15410100185

***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

PT Angkasa Pura 1 (Persero) Surabaya merupakan badan usaha milik negara dalam bidang usaha kebandarudaraan yang meliputi layanan pengendalian bagasi, layanan garbarata dan layanan fasilitas pengguna bandara. Kondisi saat ini PT Angkasa Pura 1 (Persero) Surabaya memiliki kendala dalam segi manajemen, teknikal dan operasional dalam penanganan keamanan informasi terkait dengan *asset* informasi sehingga menimbulkan permasalahan terkait dengan *Confidentiality* (kerahasiaan), *Integrity* (keutuhan), *Availability* (ketersediaan). Penelitian ini menyelesaikan masalah tersebut menggunakan metode OCTAVE untuk menghitung seberapa tinggi dampak untuk instansi jika risiko itu terjadi dan membuat ranking prioritas untuk masing-masing risiko. Kemudian dilakukan pengendalian kontrol objektif dan kontrol keamanan menggunakan ISO/IEC 27001:2013. Hasil dari penelitian ini adalah dokumen pengelolaan manajemen risiko dan penyusunan kontrol keamanan untuk kategori kebutuhan manajemen, kebutuhan teknikal, dan kebutuhan operasional. Pada kategori kebutuhan manajemen dihasilkan 1 dokumen kebijakan, 1 SOP, 2 instruksi kerja, dan 1 formulir. Kategori kebutuhan teknikal terdiri dari 3 dokumen kebijakan, 5 SOP, 6 Instruksi kerja dan 10 formulir. Kategori kebutuhan operasional terdiri dari 1 dokumen kebijakan, 1 SOP, 2 instruksi kerja, dan 3 formulir.



**Kata kunci:** ***Keamanan informasi, Aset informasi, SOP, ISO27001:2013, OCTAVE***

# KATA PENGANTAR

Puji dan syukur kami panjatkan kehadirat Tuhan Yang Maha Esa, karena hanya atas berkat dan rahmat-Nya, sehingga Laporan Tugas Akhir yang berjudul "Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 pada PT Angkasa Pura 1 (Persero) Surabaya" dapat diselesaikan dengan baik. Adapun tujuan penulisan laporan ini adalah untuk memenuhi persyaratan dalam menempuh kelulusan Strata Satu Sistem Informasi Universitas Dinamika.

Tanpa bimbingan, bantuan, motivasi, dan doa dari berbagai pihak laporan tugas akhir sistem informasi ini tidak akan terselesaikan dengan baik. Untuk itu pada kesempatan ini penulis menyampaikan rasa penghargaan dan terima kasih kepada yang terhormat:

1) Ayah, Ibu dan nenek yang selalu mendoakan, mendukung penuh penyelesaian tugas akhir ini, dengan memberikan semangat dan motivasi yang tiada henti.
2) Ibu pantjawati Sudarmaningtyas, S.Kom., M.Eng. selaku pembimbing pertama yang telah memberikan banyak masukan saran dalam proses pembuatan laporan tugas akhir ini.
3) Bapak Slamet, M.T., CCNA selaku pembimbing kedua yang telah memberikan banyak masukan, saran dalam pembuatan laporan tugas akhir ini.
4) Bapak Dr. Haryanto Tanuwijaya S.Kom., M.MT. selaku pembahas yang telah memberikan semangat dan masukan dalam penyusunan laporan Tugas Akhir ini.
5) Bapak Yoppy Mirza Maulana, S.Kom., M.MT. selaku dosen yang selalu memberikan semangat dan masukan dalam penyusunan laporan tugas akhir ini.
6) Terimakasih kepada bapak Sukirman, Mas Fikra, Mbak Adel pihak PT Angkasa Pura 1 (Persero) Surabaya yang telah memberikan kesempatan untuk melakukan penelitian.

7) Terimakasih untuk seluruh pihak dan teman-teman lain yang belum dapat penulis sebutkan satu persatu yang secara langsung maupun tidak langsung terlibat dalam proses pengerjaan tugas akhir ini.

Penulis menyadari bahwa laporan tugas akhir ini masih banyak kekurangan di dalamnya, maka kritik dan saran sangat diharapkan penulis untuk perbaikan laporan tugas akhir ini. Semoga Tuhan Yang Maha Esa memberikan imbalan yang setimpal atas segala bantuan yang diberikan.

Surabaya, 05 Agustus 2021

(Yusuf Bahrudin Nizar)

# DAFTAR ISI

Halaman

# DAFTAR TABEL

Halaman

# DAFTAR GAMBAR

Halaman

## DAFTAR LAMPIRAN

Halaman

# BAB I
# PENDAHULUAN

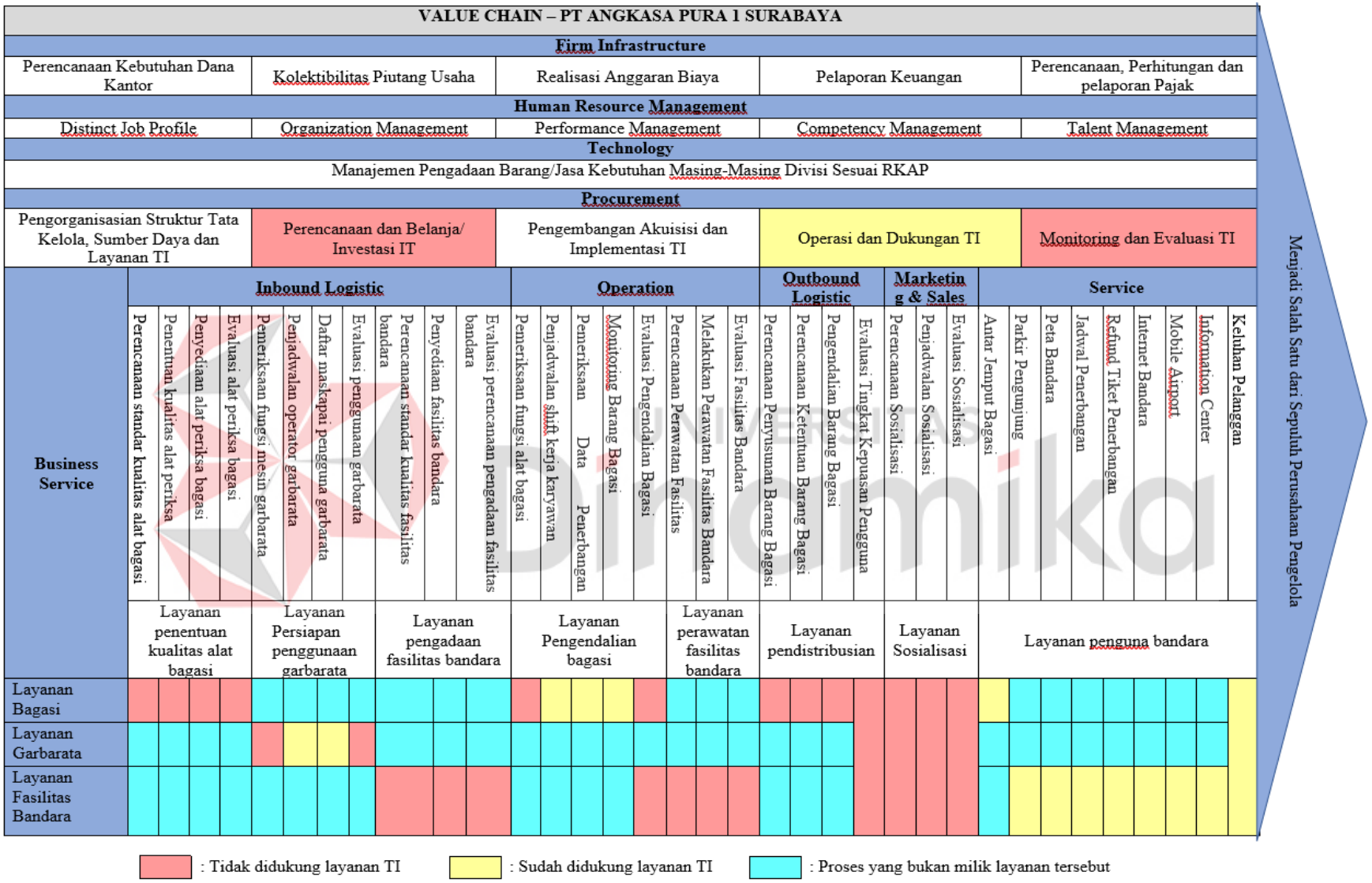
## 1.1 Latar Belakang

PT Angkasa Pura I (Persero) Surabaya merupakan badan usaha milik negara dalam bidang usaha kebandarudaraan yang meliputi layanan pengendalian bagasi, layanan garbarata dan layanan fasilitas pengguna bandara. Salah satu misi PT Angkasa Pura 1 (Persero) Surabaya yaitu mengusahakan jasa kebandarudaraan melalui pelayanan prima yang memenuhi standar keamanan, keselamatan, dan kenyamanan (Laporan Tahunan, 2017). Untuk mengetahui proses yang ada pada layanan bisnis utama PT Angkasa Pura 1 (Persero) Surabaya dapat diperoleh dengan menggunakan konsep analisis *value chain*.

Pada gambar 1.1 terlihat Analisa *value chain* Michael Porter yang menggambarkan kegiatan bisnis perusahaan yang terbagi menjadi 2 kategori yaitu: aktifitas utama dan aktifitas pendukung.

Kualitas pelayanan yang prima diterapkan mulai dari proses: 1. *inbound logistic*: terdiri dari perencanaan penentuan kualitas alat periksa bagasi, persiapan penggunaan mesin garbarata, perencanaan pengadaan fasilitas pengguna bandara; 2. *operations*: terdiri dari pengendalian bagasi, pengoperasian garbarata, dan perawatan fasilitas bandara; 3. *outbound logistic*: terdiri dari pendistribusian barang ke pesawat, pendistribusian penumpang, dan ketersediaan fasilitas pengunjung bandara; 4. *marketing and sales*: terdiri dari *awareness baggage handling*, *awareness* garbarata, dan *awareness* terhadap fasilitas bandara; dan 5. *services*: terdiri dari antar jemput bagasi, bongkar muat kargo dan bagasi, memberi kenyamanan dalam penggunaan garbarata dan memberi fasilitas yang dibutuhkan pengunjung bandara.

Alur informasi pada proses pengendalian bagasi diawali dengan informasi terkait dengan perencanaan penentuan kualitas alat cek bagasi yang dilakukan oleh *Quality Management Department Head* yang akan dilaporkan melalui email ke bagian *Procurement Section Head*.




Gambar 1. 1 Value Chain

Proses kedua yaitu proses pengendalian bagasi yang di dalamnya terdapat alur informasi berupa jadwal pegawai bagian pengendalian bagasi, jadwal penerbangan, dan juga informasi berupa SOP pengendalian bagasi yang diberikan oleh *Airport Operation and Services Department Head* kepada *Airport Operation Landside and Terminal Section Head*. Alur informasi pada proses garbarata dimulai dengan informasi terkait jadwal penerbangan maskapai yang menggunakan fasilitas garbarata yang ada pada aplikasi *Flight Information Display System* (FIDS) yang dikelola oleh bagian *Airport Technology, Network Operation and Support Section Head*, jadwal operator garbarata, dan hasil evaluasi terkait penggunaan garbarata yang dikelola oleh *Airport Operation and Services Department Head*. Alur proses informasi pada proses perencanaan fasilitas pengguna bandara terdiri dari informasi rencana pengadaan, perawatan dan hasil evaluasi tingkat kepuasan pengguna. Informasi yang harus dilindungi pada layanan utama PT Angkasa Pura 1 (Persero) Surabaya antara lain jadwal penerbangan, data maskapai, data penumpang, jadwal karyawan, informasi hasil evaluasi layanan, dan daftar fasilitas bandara.

Kondisi saat ini banyak ditemukan ancaman (*Threat*) dan kelemahan (*Vulnerable*) dari segi manajerial maupun teknis antara lain: Ancaman (*Threat*) yang terjadi dari luar organisasi meliputi *virus, worm,* dan *malware* yang menyebabkan kerusakan, kehilangan, dan lambatnya akses data penerbangan pada aplikasi *Flight Information Display System* (FIDS) yang dibutuhkan untuk menjalankan salah satu layanan utama yaitu *baggage handling*. belum adanya kebijakan *recovery server* Ketika mengalami sebuah kegagalan sistem (*down*) yang menyebabkan informasi penerbangan tidak tersedia untuk pengunjung sehingga proses bisnis perusahaan terganggu. Berdasarkan *Service Level Agreement* (SLA) down time pada permasalahan tersebut paling lama terjadi selama 24 jam.

Belum adanya kebijakan manajemen aset terkait keamanan informasi sehingga tidak ada yang bertanggung jawab dalam mengelola aset informasi. Selain itu belum adanya kebijakan autentikasi dan otorisasi terkait keamanan informasi untuk pengguna yang memiliki hak akses terhadap informasi terkait penentuan kualitas, perencanaan, pengendalian dan evaluasi proses bisnis utama, sehingga ketika terjadi kehilangan atau kesalahan informasi proses bisnis dapat terganggu dan pihak manajer tidak dapat menelusuri terkait kesalahan yang terjadi.

Dampak yang terjadi dengan adanya masalah yang disebabkan oleh kelemahan dari sisi kerahasiaan (*Confidentiality)* adalah kebocoran informasi terkait perencanaan, pengendalian dan evaluasi proses bisnis utama menyebabkan kerugian finansial, mengganggu citra perusahaan, dan juga konsekuensi hukum jika informasi tersebut jatuh ke tangan orang yang tidak bertanggung jawab karena informasi tersebut berdampak pada pemegang saham obligasi. Berdasarkan *Business Impact Analysis*, menurut (Sarno, 2009) hal tersebut memberikan nilai risiko *high.* Sehingga dibutuhkan penanganan permasalahan secara manajerial dan teknikal yang terkait tentang manajemen aset, dan akses kontrol (ISO/IEC, 2010).

Adanya masalah yang disebabkan oleh ancaman dan kelemahan dari sisi keutuhan (*Integrity*) berdampak menyebabkan jadwal penerbangan terganggu yang diakibatkan oleh kerusakan dan kehilangan data penerbangan pada aplikasi *Flight Information Display System*. Selain itu ketika ada kerusakan atau kehilangan informasi terkait perencanaan, pengendalian dan evaluasi yang menyebabkan proses bisnis dan reputasi perusahaan terganggu. dari sisi ketersediaan (*Availability*) informasi menyebabkan terganggunya proses bisnis utama terkait penentuan kualitas, perencanaan, perawatan dan evaluasi proses bisnis utama. Menurut (Sarno, 2009) dampak tersebut memberikan nilai risiko *medium*. Hal ini membutuhkan penanganan secara operasional dan teknikal.

Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi dari sisi *Confidentiality, Integrity, Availability* (CIA) adalah dengan penyusunan dokumen Sistem Manajemen Keamanan Informasi dan pembuatan SOP (*Standard Operational Procedure*) dengan tujuan sebagai acuan kerja dan standarisasi untuk mengatur banyaknya orang yang menggunakan dan membuat proses bisnis yang ada pada PT Angkasa Pura 1 (Persero) Surabaya lebih terstruktur, juga meningkatkan kualitas keamanan informasi yang ada. Pembuatan Dokumen SOP (*Standard Operational Procedure*) dipilih melalui pengendalian kontrol objektif dan kontrol keamanan menggunakan ISO/IEC 27001:2013 yang sesuai dengan kebutuhan keamanan informasi dengan mempertimbangkan hasil pengelolaan risiko keamanan informasi yang dilakukan.

## 1.2 Perumusan Masalah

Berdasarkan latar belakang diatas maka dapat dirumuskan permasalahan yang diselesaikan pada penelitian ini yaitu bagaimana menyusun perencanaan sistem manajemen keamanan informasi berdasarkan ISO/IEC 27001:2013 pada PT Angkasa Pura 1 Surabaya yang meliputi:

1. Penyusunan dokumen pengelolaan risiko terkait keamanan informasi.
2. Penyusunan kontrol objektif dan kontrol keamanan terkait dengan risiko keamanan informasi.
3. Penyusunan SOP (*Standard Operational Procedure*) yang dipilih melalui pengendalian kontrol objektif dan kontrol keamanan menggunakan ISO/IEC 27001:2013 sesuai kebutuhan keamanan informasi.

## 1.3 Batasan Masalah

Adapun batasan masalah dalam pembuatan penelitian Perencanaan Sistem Manajemen Keamanan Informasi ini pada PT Angkasa Pura ini sebagai berikut:

1. Perencanaan sistem manajemen keamanan informasi dilakukan pada proses bisnis utama perusahaan yaitu: Pengendalian bagasi, Garbarata, dan Fasilitas pengguna bandara untuk divisi *Information Communication Technology Department Head*.
2. Perencanaan sistem manajemen keamanan informasi menggunakan standar dari ISO/IEC 27001:2013
3. Penelitian ini sebatas pembuatan dokumen SOP tanpa proses pengujian SOP, dan implementasi bagi proses bisnis organisasi.

## 1.4 Tujuan

Tujuan dari penelitian ini yaitu menghasilkan dokumen perencanaan SMKI sebagai berikut:

1. Dokumen kontrol objektif dan kontrol keamanan.
2. Dokumen pengelolaan risiko terkait keamanan informasi, meliputi: Penilaian risiko, Identifikasi risiko, Analisa dan evaluasi risiko, Identifikasi dan evaluasi penanganan risiko pada PT Angkasa Pura 1 (Persero) Surabaya.

3. Dokumen SOP (*Standard Operational Procedure*), meliputi: dokumen kebijakan, instruksi kerja, dan rekam kerja yang sesuai dengan pemilihan kontrol objektif dan kontrol keamanan dari hasil pengelolaan risiko terkait keamanan informasi.

## 1.5 Manfaat

Berdasarkan tujuan penelitian, maka diharapkan dengan adanya penyusunan perencanaan SMKI pada PT Angkasa Pura 1 Surabaya:

1. Dapat membantu *Information Communication Technology Department Head* (ICT) dalam mengelola keamanan informasi dan pembuatan dokumen *Standar Operational Prosedur* (SOP) yang mengacu pada standar internasional ISO/IEC 27001:2013 tentang S*ecurity techniques Information security management systems Requirements.*
2. Membantu PT Angkasa Pura 1 Surabaya dalam peningkatan keamanan informasi.

# BAB II
# LANDASAN TEORI

## 2.1 Pentingnya Informasi TI

Informasi adalah suatu data yang telah diolah dan menjadi bernilai bagi para penerimanya. Biasanya informasi merupakan suatu sumber daya yang dapat dikelola dan bermanfaat dalam mengambilan keputusan bagi suatu perusahaan untuk saat ini maupun masa mendatang. Oleh karena itu informasi tersebut dikatakan penting. (Sulistiyani, 2011).

## 2.2 Nilai Informasi

Informasi dikatakan penting jika informasi tersebut sangat bermanfaat bagi perusahaan/organsasi untuk mendukung pengambilan keputusan. Penentuan tingkat kepentingan informasi pada suatu perusahaan adalah dengan menentukan beberapa value dari informasi tersebut. Suatu informasi dikatakan bernilai apabila ia dapat mengakibatkan perubahan dalam tindakan yang dapat diambil dalam pengambilan keputusan. Suatu informasi dikatakan bernilai apabila manfaatnya lebih efektif dibandingkan dengan biaya mendapatkannya. (Sarno, 2009).

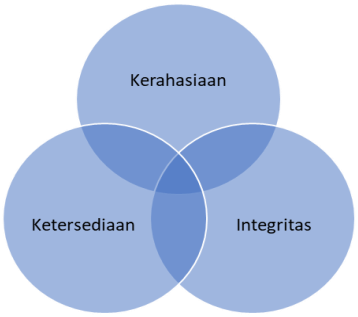
## 2.3 Keamanan Informasi

Mengingat pentingnya informasi bagi suatu organisasi, 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 pengambilan investasi dan peluang bisnis (Sarno, 2009).

Agar dapat mencapai tujuan tersebut, keamanan informasi memiliki 3 (tiga) aspek yang harus dipenuhi, aspek tersebut dapat dilihat pada gambar 2.1, aspek yang harus dipenuhi yaitu:

1. *Confidentiality* (Kerahasiaan): informasi bersifat rahasia dan harus dilindungi agar tidak dapat di akses oleh orang yang tidak memiliki hak akses.

2. *Integrity* (Kelengkapan): keamanan informasi harusnya menjamin kelengkapan informasi dan menjaganya dari kehilangan, kerusakan dan ancaman lain yang menyebabkan data itu berubah.
3. *Availability* (Ketersediaan): informasi harus terjamin ketersediaannya untuk mendukung semua proses bisnis organisasi. Sehingga kapanpun informasi dibutuhkan oleh pengguna selalu tersedia.




Gambar 2. 1 Aspek Keamanan Informasi (Sarno, 2009)

### 2.3.1 Pentingnya Keamanan Informasi

Menurut (Sulistiyani, 2011) informasi adalah suatu data yang telah diolah dan menjadi berarti bagi para penerimanya. Biasanya informasi merupakan suatu sumber daya yang dapat dikelola dan bermanfaat dalam mengambilan keputusan bagi suatu perusahaan untuk saat ini maupun masa mendatang. Oleh karena itu informasi tersebut dikatakan penting.

Untuk meningkatkan keunggulan, keuntungan, nilai komersial, dan citra organisasi yang memiliki aset informasi berharga sangat diperlukan penjagaan keamanan informasi dari keseluruhan piranti, jaringan, dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan informasi (Sarno, 2009).

### 2.3.2 Risiko Teknologi Informasi

Pengertian risiko menurut (Siahaan, 2007) adalah sebagai suatu keadaan yang belum pasti terjadi, dan yang merupakan satu keadaan yang dihadapi oleh manusia dalam setiap kegiatannya dan risiko adalah suatu ketidakpastian dimasa yang datang tentang kerugian.

Menurut (Hughes, 2006) dalam penggunaan teknologi informasi berisiko terhadap kehilangan informasi dan pemulihannya yang tercakup dalam 6 kategori, yang dijelaskan pada lampiran 6:

## 2.4 Identifikasi Risiko Keamanan Informasi

### 2.4.1 Identifikasi Aset

Langkah pertama untuk penilain Risiko adalah identifikasi dan inventarisasi aset yang terkait dengan fasilitas informasi. Identifikasi adalah melakukan pengelompokan aset ke dalam beberapa kategori. Kategori aset berdasarkan ISO/IEC 27002:2013 yang antara lain berupa informasi, aset perangkat lunak, aset fiksik, layanan, orang maupun aset yang tak terukur.

### 2.4.2 Aset Informasi

Aset informasi adalah sepotong informasi yang terdefinisi, disimpan dengan cara apapun, tidak mudah untuk diganti, keahlian, waktu, sumber daya dan kombinasinya serta diakui sebagai sesuatu yang berharga bagi organisasi. Aset informasi pada penelitian ini mengacu pada definisi komponen sistem aset informasi adalah sepotong informasi yang terdefinisi, disimpan dengan cara apapun, tidak mudah untuk diganti, keahlian, waktu, sumber daya dan kombinasinya serta diakui sebagai suatu yang berharga bagi organisasi. Komponen pendukung meliputi: sumber daya manusia *(people),* perangkat keras *(hardware),* perangkat lunak *(software),* data dan jaringan *(network).*

### 2.4.3 Risiko

Pengertian risiko adalah sebagai suatu keadaan yang belum pasti terjadi, dan yang merupakan satu keadaan yang dihadapi oleh manusia dalam setiap kegiatannya dan risiko adalah suatu ketidakpastian dimasa yang datang tentang kerugian (Siahaan, 2007).

Langkah pertama untuk penilaian risiko adalah identifikasi dan inventarisasi aset yang terkait dengan fasilitas informasi. Identifikasi adalah melakukan pengelompokan aset ke dalam beberapa kategori. Kategori aset

berdasarkan ISO/IEC 27002:2013 yang antara lain berupa informasi, aset perangkat lunak, aset fisik, layanan, orang maupun aset yang tak terukur.

### 2.4.4 Identifikasi Ancaman

Ancaman adalah suatu potensi yang disebabkan oleh insiden yang tidak diinginkan yang mungkin terjadi dan membahayakan jalannya proses bisnis organisasi (ISO/IEC, 2010). Tujuan dari identifikasi ancaman adalah agar diketahui ancaman apa yang mungkin dapat terjadi pada organisasi. Sumber ancaman dapat berasal dari alam, lingkungan, manusia.

### 2.4.5 Identifikasi Kelemahan

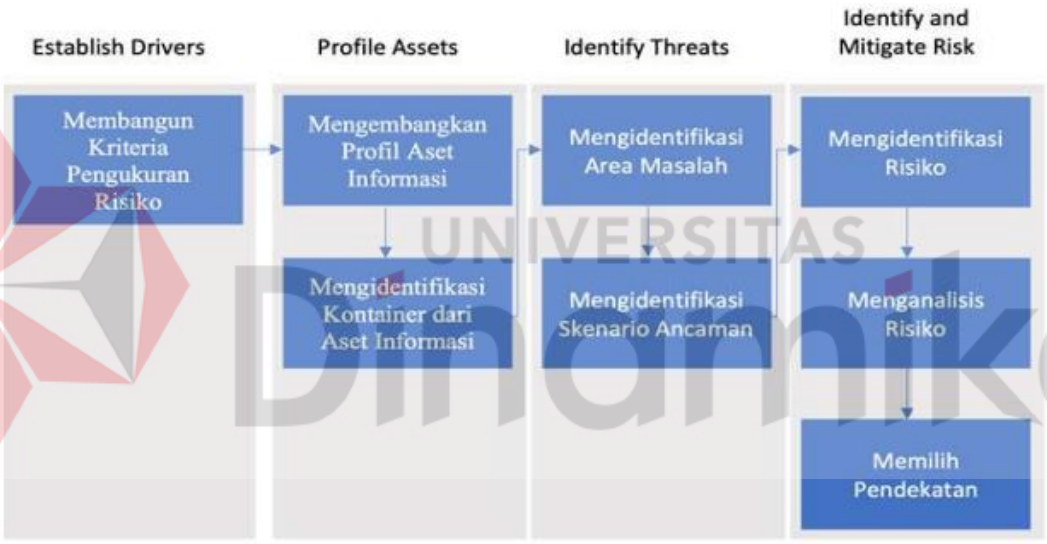
Kelemahan didalam prosedur keamanan informasi, perencanaan dan kontrol internal terhadap penjagaan informasi dapat menimbulkan ancaman. Tujuan utama dari identifikasi kelemahan adalah organisasi dapat memahami kelemahan yang dimiliki dalam manajemen keamanan informasinya.

## 2.5 *Risk Breakdown Structure*

Pengelompokan risiko dalam suatu komposisi hirarki risiko organisasi yang logis, sistematis, dan terstruktur secara alami sesuai dengan struktur organisasi atau proyek. Sasaran penerapan *Risk Breakdown Structure* (RBS) adalah kejelasan pemangku risiko atau peningkatan pemahaman risiko organisasi atau proyek dalam konteks kerangka kerja yang logis serta sistematis. Proses pengembangan RBS digunakan untuk melakukan tinjauan terhadap area-area yang menjadi perhatian dan potensi keterkaitan diantara area-area tersebut. Pelaksanaan pengembangan RBS ini dapat dilakukan dengan pendekatan *top-down* atau *bottom-up*, sama seperti pengembangan *works breakdown structure*. Hal yang perlu diperhatikan adalah tentang pemahaman yang cukup mengenai peringkat dari sumber-sumber risiko yang terdapat dalam organisasi (Susilo & Kaho, 2011).

## 2.6 Metode OCTAVE

Metode *The Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE) ini dikembangkan oleh *Software Engineering Institute*, Carnegie Mellon University pada tahun 1999. Merupakan sebuah perangkat alat, teknik dan metode untuk melakukan penilaian terhadap sistem keamanan informasi berbasis risiko pada organisasi. OCTAVE adalah sebuah pendekatan terhadap evaluasi risiko dari tiga aspek keamanan informasi yaitu *confidentiality*, *integrity*, dan, *availability* yang komprehensif, sistematik, terarah, dan dilakukan sendiri. Pendekatannya disusun dalam satu set kriteria yang mendefinisikan elemen esensial dari evaluasi risiko keamanan informasi. Fase pada metode octave dijelaskan pada lampiran 6.




Gambar 2. 2 Metode OCTAVE Allegro

## 2.7 Standar Sistem Manajemen Keamanan Informasi (SMKI)

Standar yang digunakan adalah *International Organization for Standardization* (ISO), ISO sendiri 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, 2010).

## 2.8 Model Proses

ISO/IEC 27001:2013 menetapkan model tahapan yang dibutuhkan dalam mengimplementasikan pemenuhan manajemen keamanan informasi dengan tujuan organisasi dan kebutuhan bisnis (ISO/IEC, 2010). Gambar dan penjelasan model proses dijelaskan pada lampiran 6.

### 2.8.1 Struktur Organisasi ISO/IEC 27001

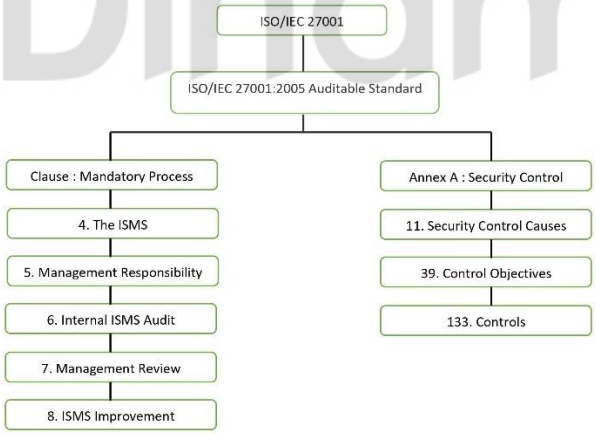
Struktur organisasi dari ISO/IEC 27001 dibagi dalam dua bagian besar seperti pada penjelasan berikut:

A. Klausul: *Mandatory Process*

Klausul (pasal) adalah persyaratan yang harus dipenuhi jika organisasi menerapkan SMKI dengan menggunakan standar ISO/IEC 27001.

B. Annex A: *Security Control*

Annex A adalah dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan yang perlu diimplementasikan di dalam SMKI, yang terdiri dari 18 Klausul, 35 Kontrol Objektif, dan 114 Kontrol Keamanan.




Gambar 2. 3 Aspek Keamanan Informasi

## 2.9 Penjelasan detail kontrol objektif

### 2.9.1 Pemetaan Kontrol Objektif

Berikut pemetaan kontrol objektif (ISO 27001:2013) berdasarkan *Secure Online Business* (Jolly, 2003) yang dapat dilihat pada lampiran 6.

## 2.10 Standard Operational Procedure (SOP)

*Standard 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 menghasilkan kebijakan, instruksi kerja dan rekam kerja. Untuk penjelasan secara detail dapat dilihat pada lampiran 6.

## 2.11 Panduan Perencanaan Sistem Manajemen Keamanan Informasi

Panduan penyusunan langkah-langkah sistem manajemen keamanan informasi (SMKI) yang difokuskan pada Tahap *Plan* (Perencanaan) dijelaskan sebagai berikut.

A. **Menentukan Ruang Lingkup SMKI** adalah menentukan ruang lingkup implementasi SMKI yang diterapkan dalam organisasi pada ruang lingkup mana saja, seluruh bagian organisasi atau hanya sebagian. Penentuan ruang lingkup SMKI ini dilakukan berdasarkan:
   1) Kebutuhan organisasi (Proses, Layanan, dan Lokasi)
   2) Aset yang dimiliki oleh organisasi
   3) Teknologi yang digunakan

B. **Menentukan kebijakan SMKI** adalah komitmen manajemen untuk mendukung, membangun, mengimplementasikan, mengoperasikan, *me monitoring*, melakukan kajian ulang, memelihara dan mengembangkan SMKI.

C. **Penilaian Risiko (*Risk Assessment*)** adalah untuk mengetahui bagaimana cara melakukan penilaian risiko sesuai dengan kebutuhan organisasi. Pelaksanaan penilaian risiko ini tergantung dari ruang lingkup SMKI yang telah ditentukan. Penilaian risiko terdapat dua macam hal yang harus dipaparkan pada lampiran 6.

D. **Identifikasi risiko**

Bertujuan untuk memahami seberapa besar dan risiko apa yang diterima oleh organisasi jika mendapat ancaman atau gangguan terkait informasi penting sehingga menyebabkan gagalnya penjagaan keamanan informasi (ISO/IEC, 2010). langkah-langkah untuk mengidentifikasi risiko dijelaskan pada lampiran 6.

**E. Analisis dan Evaluasi Risiko**

Proses ini bertujuan untuk menganalisa dan evaluasi dari hasil identifikasi risiko yang telah dilakukan sebelumnya, untuk memahami bagaimana dampak risiko terhadap bisnis organisasi, bagaimana level risiko yang mungkin timbul dan menentukan apakah risiko yang terjadi langsung diterima atau masih perlu dilakukan pengelolaan agar risiko dengan dampak yang bisa ditoleransi. Tahapan untuk menganalisa dan evaluasi risiko dijelaskan pada lampiran 6.

**F. Identifikasi dan Evaluasi Pilihan Penanganan Risiko**

Langkah ini menjelaskan bahwa organisasi harus melakukan identifikasi dan evaluasi pilihan penanganan risiko. Maksud dari langkah ini jika risiko yang timbul tidak langsung diterima tetapi perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan yang telah ditentukan pilihan penanganan risiko:

1. Menerima risiko dengan menerapkan kontrol keamanan yang sesuai
2. Menerima risiko dengan menggunakan kriteria risiko yang telah ditetapkan
3. Menerima risiko dengan mentransfer risiko kepada pihak ketiga (asuransi, vendor, supplier, atau pihak tertentu).

**G. Memilih Objektif Kontrol dan Kontrol Keamanan untuk Pengelolaan Risiko *(Risk Mitigation)***

Pemilihan objektif kontrol dan kontrol keamanan pada panduan ISO 27001:2013 (Annex A) yang dapat dilihat lebih detail pada dokumen ISO 27002:2013. Tujuannya yaitu untuk menentukan sasaran keamanan informasi yang dikendalikan secara tepat. ISO 27001:2013 mendefinisikan 14 Klausul, 35 Kontrol Objektif dan 114 Kontrol Keamanan yang dapat diterapkan untuk

membangun sistem manajemen keamanan informasi (ISO/IEC, 2010). Klausul-klausul tersebut dijelaskan pada lampiran 6.

**H. Pengelompokan kebutuhan klausul kontrol keamanan**

Pengelompokan klausul tersebut dibagi menjadi tiga kelompok kebutuhan kontrol keamanan, yaitu: manajemen/organisasi, teknikal, dan operasional. Pengelompokan kebutuhan kontrol keamanan ini sangat penting untuk memudahkan organisasi memilih atau menentukan kontrol keamanan apa yang dibutuhkan secara manajemen, teknikal dan operasional yang dijelaskan pada lampiran 6.

## 2.12 Kebijakan SMKI

Kebijakan disusun dengan memperhatikan Objektif Kontrol dan Kontrol yang telah dipilih dalam tahap sebelumnya. Seluruh kebijakan yang telah disetujui oleh pemimpin kemudian disosialisasikan kepada seluruh pegawai yang terkait sesuai dengan ruang lingkup yang telah ditetapkan diatas. Kegiatan ini untuk memastikan bahwa kebijakan terkait SMKI telah dipahami sehingga penerapannya dapat dilakukan secara tepat.

## 2.13 Instruksi Kerja

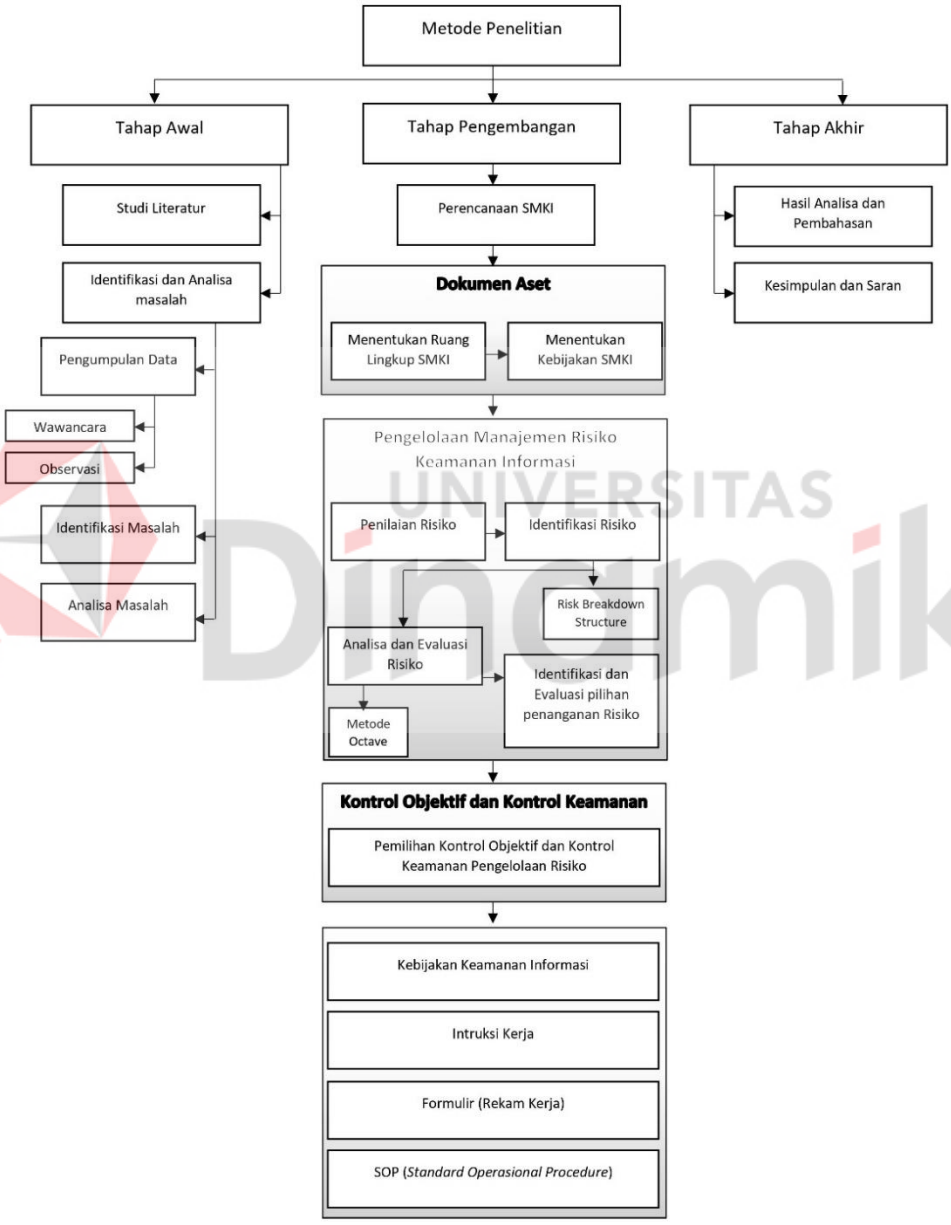
Suatu perintah yang disediakan untuk membantu seseorang dalam melakukan pekerjaan dengan benar atau satu set instruksi untuk melakukan tugas. Instruksi kerja menceritakan deskripsi teknis dari suatu aktifitas atau menggambarkan suatu urutan kerja mulai dari awal sampai pekerjaan itu selesai (ISO/IEC, 2010).

## 2.14 Formulir

Formulir merupakan selembaran kertas bukti bahwa sistem tata kerja yang terdapat pada prosedur dan instruksi kerja telah dilaksanakan. Formulir digunakan untuk memantau pelaksanaan prosedur dan instruksi kerja. Formulir dapat berupa lembar kerja, grafik, laporan, dan bentuk-bentuk lain yang dapat diterima oleh organisasi sebagai bukti yang sah. (Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, 2012)

# BAB III
# METODE PENELITIAN

Pada penelitian ini metode yang digunakan terbagi menjadi tiga tahap yang dijelaskan pada Gambar 3.1 berikut.




Gambar 3. 1 Metode Penelitian

## 3.1 Tahap Awal

### 3.1.1 Studi Literatur

Studi literatur dilakukan untuk mendukung pengerjaan tugas akhir pada tahap pengembangan hingga tahap akhir dilakukan dengan cara mempelajari dan mencari referensi, yang menjadi dasar keterkaitan topik penelitian. Pencarian referensi yang dilakukan yaitu melalui buku di perpustakaan dan jurnal terkait dengan topik penelitian. Berikut ini adalah beberapa jenis studi literatur yang digunakan antara lain:

A. ISO 27001: 2013 (ISO/IEC, 2010).
B. ISO 27002: 2013 (ISO/IEC, 2010).
C. Manajemen Sistem Keamanan Informasi
D. Standard Operasional Prosedur

### 3.1.2 Identifikasi dan Analisa Masalah

Mengidentifikasi permasalahan merupakan langkah awal dalam analisa permasalahan. Identifikasi yang dilakukan sesuai dengan hasil wawancara dan observasi terkait kondisi saat ini pada instansi. Langkah ini diawali dari permasalahan yang ditemukan, maka diperlukan penggalian data dan referensi mengenai topik yang diambil sesuai dengan penelitian ini. Penggalian referensi mengenai daftar risiko keamanan informasi yang digunakan untuk mengetahui risiko yang terkait dengan keamanan informasi, periode dan terulangnya risiko yang terjadi pada PT. Angkasa Pura 1 Surabaya.

## 3.2 Pengumpulan data

### 3.2.1 Wawancara

Wawancara yang dilakukan pada penelitian ini dengan narasumber dari bagian *Information Communication and Technology Department Head, Airport Technology Network Operation & Support Section Head,* dan *Quality Management* pada PT Angkasa Pura 1 mengenai kebutuhan yang dilakukan dalam pelaksanaan tugas akhir. Wawancara bertujuan untuk mengetahui informasi, dan kelemahan apa yang di dapat serta nantinya dapat memberikan solusi bagi permasalahan yang ada. Berikut adalah data-data yang didapat dari hasil wawancara yaitu:

A. Visi, misi, tujuan dan budaya perusahaan
B. Struktur organisasi instansi
C. Proses bisnis utama PT Angkasa Pura 1 (Persero) Surabaya.
D. Tugas pokok dan fungsi setiap Sumber Daya Manusia (SDM)
E. Layanan dan asset informasi yang terdapat pada *Information Communication and Technology Department Head.*
F. Risiko yang terjadi pada instansi terkait dengan keamanan informasi. SOP terkait operasional pada bagian *Information Communication and Technology Department Head.*
G. Pencapaian Sasaran Mutu PT Angkasa Pura 1 (Persero) Surabaya
H. Annual report perusahaan

### 3.2.2 Observasi

Observasi dilakukan pada proses bisnis utama pada PT Angkasa Pura 1 (Persero) Surabaya yang bertujuan untuk mendapatkan data tentang masalah yang diselesaikan sehingga diperoleh pemahaman secara langsung dari pengamatan yang dilakukan. Observasi yang dilakukan menghasilkan permasalahan yang terdapat pada PT Angkasa Pura 1 (Persero) Surabaya saat ini. Berikut adalah data-data yang didapat dari hasil observasi.

A. Penentuan rumusan masalah
B. Pengembangan kajian teori
C. Dokumen SOP
D. Dokumen *tupoksi*
E. Data aset informasi
F. Data risiko yg terjadi pada instansi terkait keamanan informasi
G. Daftar pertanyaan dan hasil wawancara

## 3.3 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 dijelaskan sebagai berikut:

## 3.4 Dokumen Perencanaan Sistem Manajemen Keamanan Informasi (SMKI)

### 3.4.1 Menentukan ruang lingkup SMKI

Penentuan ruang lingkup ini sangat dibutuhkan dengan tujuan dokumen yang dihasilkan sesuai dengan kebutuhan permasalahan keamanan informasi pada divisi ICT. Dalam menentukan ruang lingkup sistem manajemen keamanan informasi yang harus dilakukan dijelaskan pada lampiran 7.

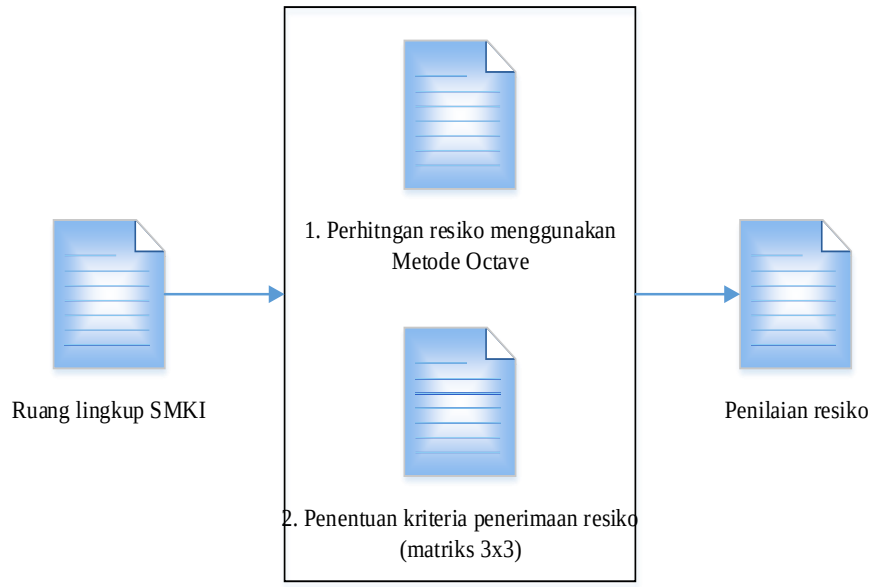
### 3.4.2 Identifikasi Risiko

Identifikasi risiko ini bertujuan untuk mengetahui seberapa besar risiko yang diterima oleh organisasi. Proses identifikasi risiko ini memiliki empat langkah, yang dijelaskan pada lampiran 7.

### 3.4.3 Pengelolaan Penilaian Risiko

Pada tahap Pengelolaan Penilaian risiko ini bertujuan untuk mengetahui seberapa besar dampak dari risiko yang diterima oleh divisi ICT jika terjadi ancaman dari sisi internal ataupun eksternal. jika informasi mendapat ancaman atau gangguan pada pengamanan informasi yaitu:

a) Menentukan kriteria penerimaan risiko menggunakan matriks 3x3
b) Penilaian risiko ini menggunakan metode OCTAVE dengan hitungan matematis dalam analisa penilaian risikonya.
c) Masukan dari proses penilaian risiko ini diambil dari dokumen ruang lingkup.



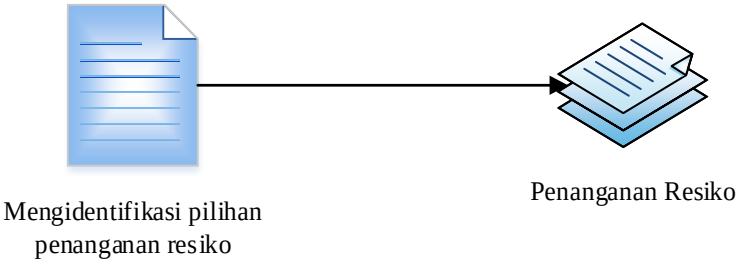

Gambar 3. 2 Penilaian Risiko

### 3.5 Analisa dan Evaluasi Risiko

Analisa dan Evaluasi risiko ini bertujuan untuk mengetahui seberapa besar risiko yang diterima oleh organisasi. Proses identifikasi risiko ini memiliki 3 langkah yang dijelaskan pada lampiran 7.

### 3.6 Identifikasi dan Evaluasi Penanganan Risiko

Pada tahap ini yaitu dilakukan pemilihan penanganan risiko langkah yang harus dilakukan yaitu mengidentifikasi atau menentukan pilihan pengelolaan risikonya. Pilihan pengelolaan risiko, menerima risiko dengan menerapkan kontrol keamanan yang sesuai, menerima risiko dengan menggunakan kriteria risiko yang telah diterapkan, dan menerima risiko dengan men-*transfer* risiko kepada pihak ketiga (asuransi, vendor, atau pihak tertentu). Alur identifikasi dan evaluasi penanganan risiko digambarkan pada Gambar 3.3.




Gambar 3. 3 Alur Informasi dan Evaluasi Penanganan

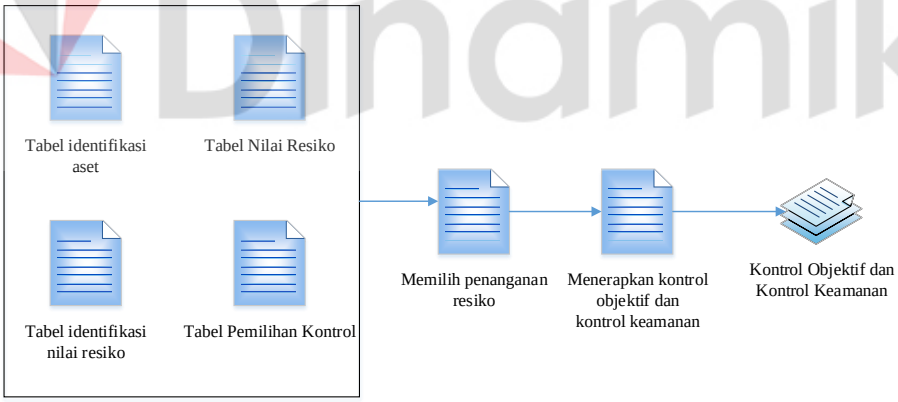
### *3.7 Risk Breakdown Structure*

Proses pengembangan *Risk Breakdown Structure* (RBS) merupakan suatu kegiatan yang sangat berguna untuk melakukan tinjauan terhadap area-area yang menjadi perhatian dan potensi keterkaitan diantara area-area tersebut. Pelaksanaan pengembangan RBS ini dapat dilakukan dengan pendekatan *top-down* atau *bottom-up*, sama seperti pengembangan *works breakdown structure*. Perhatikan tentang perlunya pemahaman yang cukup mengenai peringkat dari sumber-sumber risiko yang terdapat dalam organisasi. Tahapan RBS dijelaskan pada lampiran 7.

### 3.8 Memilih Kontrol Objektif dan Kontrol Keamanan

Pada tahapan ini dilakukan pemilihan kontrol objektif dan kontrol keamanan yang sesuai dengan hasil pengelolaan risiko keamanan informasi. Adapun cara untuk memilih kontrol objektif dan kontrol keamanan, yaitu:

Alur Pemilihan kontrol objektif dan kontrol keamanan digambarkan pada Gambar 3.4.



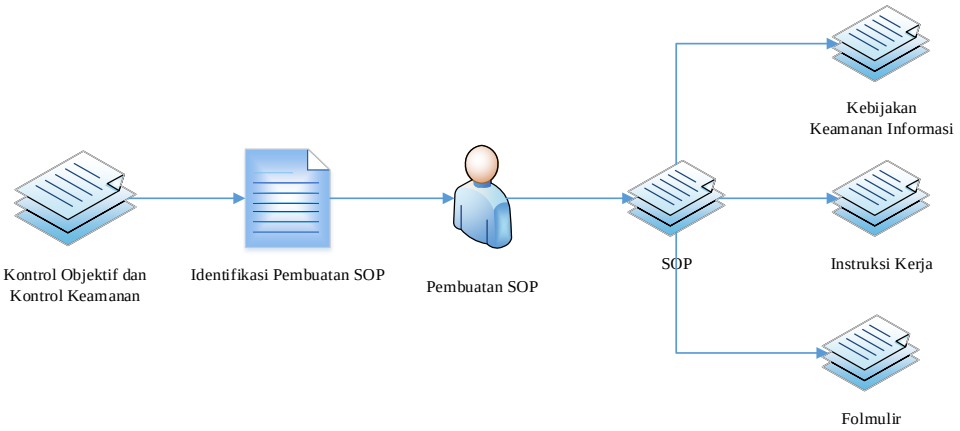

Gambar 3. 4 Tahapan Pemilihan Kontrol Objektif dan Kontrol Keamanan

### 3.9 *Standard Operational Procedure* (SOP)

#### 3.9.1 Pembuatan SOP

Pada tahap ini dilakukan pembuatan *Standard Operational Procedure* (SOP) yang dibuat melalui pemilihan kontrol objektif dan kontrol keamanan dengan identifikasi kebutuhan SOP, lalu dilakukan pembuatan SOP dengan hasil dokumen

SOP meliputi dokumen kebijakan, instruksi kerja dan formulir. Alur Pembuatan *Standar Operational Procedure* (SOP) digambarkan pada gambar 3.5.




Gambar 3. 5 Alur Pembuatan SOP

### 3.10 Instruksi Kerja

Instruksi kerja memuat hasil rinci dari prosedur yang telah dibuat sehingga instruksi kerja merupakan dokumen kompleks yang lebih detail dari prosedur. Alur instruksi kerja dijelaskan pada Gambar 3.5.

### 3.11 Formulir (Rekam Kerja)

Formulir merupakan bukti atau hasil bahwa prosedur telah dilaksanakan berupa tabel yang harus diisi yang sah. Alur rekam kerja dijelaskan pada Gambar 3.5.

### 3.12 Tahap Akhir

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

#### 3.12.1 Hasil Analisa dan Pembahasan

Pada tahap ini dijelaskan mengenai hasil pengerjaan tugas akhir yang diperoleh dari penelitian yang telah dilakukan sesuai dengan metode pelaksanaan yang sudah direncanakan.

### 3.12.2 Kesimpulan dan Saran

Pada tahap ini didapatkan kesimpulan dan saran dari pembahasan yang telah dilakukan dan juga menghasilkan saran yang dapat digunakan dalam pengembangan topik tugas akhir ini.

# BAB IV
# HASIL DAN PEMBAHASAN

Bab IV membahas hasil pembuatan Perencanaan Sistem Manajemen Keamanan Informasi berdasarkan standar ISO 27001:2013 pada PT Angkasa Pura 1 (Persero) Surabaya. Hasil yang di dapatkan dari metode dari tahapan awal, tahap pengembangan, dan tahap akhir adalah sebagai berikut.

## 4.1 Tahap Awal

### 4.1.1 Studi Literatur

Dalam menyusun penelitian perlu dilakukan teknik penyusunan secara sistematis dengan tujuan memudahkan langkah-langkah yang diambil pada tahap penyusunan. Sesuai dengan tahapan yang sudah ada pada metodologi penelitian, tahap awal yaitu melakukan studi literatur, dengan mencari referensi berupa buku di perpustakaan dan jurnal terkait dengan topik penelitian. Adapun studi literatur yang digunakan dalam proses penyusunan laporan ini sebagai berikut:

1. Konsep keamanan informasi yang digunakan untuk menyusun dokumen aset, mengelola keamanan informasi dan menentukan kontrol objektif serta kontrol keamanan.
2. Konsep pengelolaan risiko keamanan informasi digunakan dalam penyusunan pengelolaan risiko keamanan informasi.
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 Analisa Masalah

**A. Pengumpulan Data**

**A. Wawancara**

Tujuan dari wawancara ini adalah untuk mengetahui dan mendapatkan kebutuhan informasi serta data yang berkaitan dengan topik penelitian, wawancara

dilakukan bersama dengan Bapak Didik Hermanto selaku kepala bagian ICT Department head. Adapun uraian dari hasil wawancara adalah sebagai berikut:

**a) Visi, misi PT Angkasa Pura 1 Surabaya**

Berdasarkan hasil wawancara terkait visi, misi organisasi yang dilakukan bersama Bapak Didik Hermanto selaku kepala bagian ICT Department Head dapat dilihat pada lampiran 2.

**b) Struktur organisasi dan tugas pokok setiap bagian pada ICT**

Struktur organisasi beserta tugas pokok dan fungsi setiap bagian pada divisi ICT dijelaskan pada lampiran 3.

**c) Proses bisnis dan kebijakan pelayanan**

Kebijakan pelayanan ini terkait proses layanan pada operasional yang dijalankan oleh ICT dan berkaitan dengan proses bisnis yang dimiliki oleh ICT. Proses bisnis dan kebijakan pelayanan ini di jelaskan pada lampiran 2.

**d) Daftar kejadian terkait keamanan informasi yang ada pada ICT**

Daftar kejadian ini merupakan hasil rekapitulasi kejadian yang pernah terjadi di ICT, serta tindakan yang pernah dilakukan. Daftar kejadian dapat dilihat pada lampiran 5.

**2. Observasi**

Observasi pada penelitian ini dilakukan pada proses bisnis yang ada pada ICT dengan tujuan mendapatkan data terkait masalah yang diselesaikan pada topik penelitian, sehingga diperoleh pemahaman secara langsung dari pengamatan. Hasil dari observasi yang dilakukan pada bagian ICT yaitu berupa narasi proses bisnis, lengkap dengan gambar *flowchart* yang terdapat pada lampiran 2. Proses bisnis pada divisi ICT meliputi, layanan pengendalian bagasi, layanan garbarata, dan layanan fasilitas pengguna bandara.

## B. Identifikasi Masalah

Identifikasi masalah yang terjadi pada *Information Communication and Department Head* (ICT) yaitu dalam identifikasi masalah berdasarkan metode OCTAVE. Mengidentifikasi aset penting yang dimiliki organisasi, kebutuhan keamanan organisasi, praktek keamanan terkini yang telah atau sedang dilakukan tentang *Threat* (Ancaman), *Vulnerable* (Kerahasiaan) dan *Availability*

(Ketersediaan) yang berdampak pada *Business Impact Analysis (BIA)* pada ICT. Serta aset kritis dan kelemahan infrastruktur TI yang ada saat ini. Hasil identifikasi masalah kemudian dilanjutkan pada proses identifikasi pemilik risiko. Hasil luaran dari proses ini adalah sebuah daftar kejadian yang pernah terjadi yang dapat dilihat pada lampiran 5. Daftar kejadian yang pernah terjadi terkait dengan proses layanan bagasi, layanan garbarata, dan layanan fasilitas bandara. Daftar kejadian tersebut menjadi masukan untuk proses analisis masalah. Identifikasi masalah pada ICT yaitu terkait dengan penanganan keamanan informasi.

**C. Analisa Masalah**

Analisa masalah yang di dapatkan dari identifikasi masalah yaitu adanya kejadian yang ditemukan dan belum adanya kebijakan manajemen aset terkait keamanan informasi. Misalnya, pernah terjadi kehilangan atau kesalahan informasi proses bisnis yang disebabkan oleh kurangnya manajemen asset terkait keamanan informasi. Solusi terhadap permasalahan yang ditentukan terkait dengan keamanan informasi yang mempengaruhi *Confidentiality* (kerahasiaan), *Integrity* (keutuhan), dan *Availability* (ketersediaan) yang berdampak pada *Business Impact Analysis (BIA)* terkait dengan proses layanan bagasi, layanan garbarata, dan layanan fasilitas bandara. Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi dari sisi CIA adalah dengan menyusun dokumen pengelolaan kejadian terkait dengan keamanan informasi dan pembuatan dokumen SOP (*Standar Operational Procedure*) dengan tujuan sebagai acuan kerja dan standarisasi pada *Information Communication and Technology Department Head* (ICT) agar lebih terstruktur dan meningkatkan kualitas keamanan informasi yang ada.

## 4.2 Tahap Pengembangan

Tahap pengembangan merupakan tahapan inti yang dilakukan pada penelitian tugas akhir ini. Pada sub 4.2 ini telah menjelaskan proses dari tahap pengembangan yaitu dokumen asset yang berisi penentuan ruang lingkup SMKI dan menentukan kebijakan SMKI, dokumen pengelolaan risiko keamanan informasi yang berisi penilaian risiko, identifikasi risiko, analisa dan evaluasi risiko, identifikasi dan evaluasi penanganan risiko, dokumen kontrol objektif dan kontrol keamanan

meliputi pemilihan kontrol objektif dan kontrol keamanan dan selanjutnya yaitu pembuatan *Standar Operational Prosedur (SOP).*

### 4.2.1 Dokumen Perencanaan Sistem Manajemen Keamanan Informasi

#### A. Menentukan Ruang Lingkup SMKI

Menentukan ruang lingkup SMKI dari hasil wawancara dan kesepakatan yang dilakukan dengan Bapak Didik Hermanto selaku kepala ICT Department Head. Keamanan Teknologi Informasi PT Angkasa Pura 1 Surabaya berada pada divisi *Information Communication and Department Head* (ICT). ICT memiliki fungsi menyiapkan kebijakan teknis, perencanaan, dan pelaksanaan pengelola penanganan, pemulihan, monitoring, evaluasi, dan keamanan informasi merupakan salah satu kriteria utama melakukan penilaian pada divisi ICT. Dalam menentukan ruang lingkup SMKI yaitu organisasi harus berkomitmen melindungi informasi, untuk memenuhi kebutuhan organisasi dalam mengimplementasikan SMKI sesuai standar ISO 27001:2013. SMKI organisasi diimplementasikan untuk ruang lingkup bisnis organisasi yaitu pada bagian:

a) Divisi *Information Communication Technology* (ICT).
b) Layanan pengendalian bagasi, layanan garbarata, layanan fasilitas bandara, layanan monitoring rutin keamanan server hosting.
c) Aset-aset TI internal organisasi dan jaringan komputer yang digunakan untuk aktivitas bisnis meliputi aset *hardware*, aset *software* atau aplikasi, asset infrastruktur, aset data atau informasi, dan SDM.

#### B. Menentukan Kebijakan SMKI

Kebijakan yang dibuat untuk melindungi aset organisasi demi kesuksesan bisnis organisasi agar berjalan sesuai dengan apa yang diinginkan dengan baik. Adapun kebijakan yang telah dilaksanakan dapat dilihat pada lampiran 2.

### 4.2.2 Pengelolaan Risiko Keamanan Informasi

#### A. Identifikasi Aset

Identifikasi aset pada *information Communication and Department Head* (ICT) bertujuan untuk menentukan aset-aset yang ada yang digunakan untuk mendukung proses bisnis ICT. Beberapa hasil observasi yang dilakukan dapat

digolongkan menjadi beberapa jenis aset yaitu aset hardware, software atau aplikasi, aset infrastruktur/jaringan, aset data atau informasi, dan aset sumber daya manusia (SDM) yang terdapat pada lampiran 8. Dari hasil identifikasi aset dianalisa kembali dalam menghasilkan aset informasi kritis yang digunakan dalam proses penelitian selanjutnya.

**B. Identifikasi *Flow of Information***

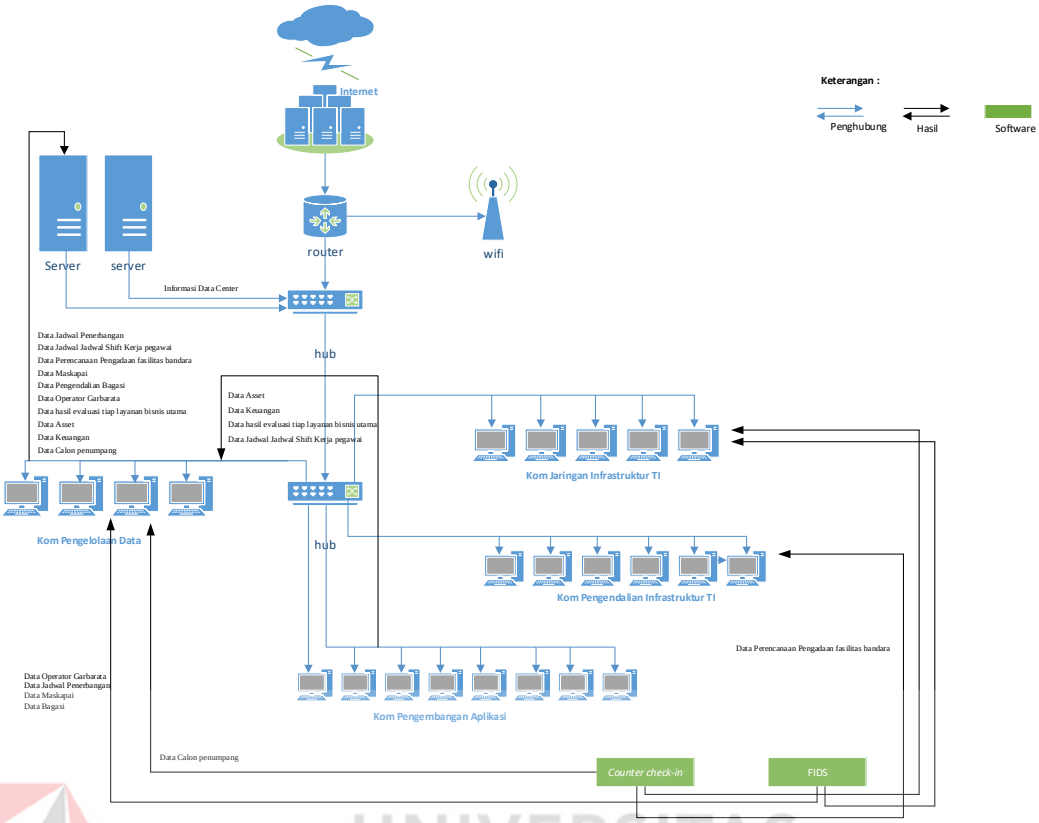
*Flow of information* (arus informasi) yang ada pada aset ICT hardware, software, jaringan, data, dan SDM untuk dapat menentukan letak aset yang ada pada ICT dapat dilihat pada gambar 4.2 1.

**C. Identifikasi Aset Kritis**

Identifikasi penentuan aset kritis ditentukan berdasarkan gangguan atau ancaman pada aset instansi yang mengalami hambatan dalam operasional. Daftar aset kritis dapat dijelaskan pada lampiran 8.

**D. Identifikasi Ancaman dan Kelemahan**

Identifikasi ancaman dan kelemahan pada aset kritis dikategorikan ke dalam hardware, software, jaringan atau infrastruktur, data atau informasi dan SDM pada proses layanan *Flight Information Display System* (FIDS) layanan *Counter check-in*, layanan monitoring rutin keamanan server hosting. Daftar ancaman dan kelemahan berikut ini didapatkan dari hasil wawancara dan observasi kepada narasumber. Tabel identifikasi ancaman dan kelemahan dapat dilihat pada lampiran 8.




Gambar 4. 1 Identifikasi Flow of information

## E. Identifikasi Kerentanan

Identifikasi kerentanan adalah kemungkinan ancaman yang muncul pada aset-aset yang mendukung jalannya proses bisnis yang ada. Tabel identifikasi kerentanan dapat dilihat pada lampiran 8.

## 4.3 Penilaian Risiko

### 4.3.1 Metode Penilaian Risiko

Penentuan Penilaian risiko ini dilihat dari identifikasi permasalahan yang ada pada *Information Communication Technology and Department Head* (ICT) dan hasil analisa dari proses layanan bagasi, layanan garbarata, layanan fasilitas bandara, layanan monitoring rutin keamanan server hosting. Metode yang digunakan dalam penelitian risiko pada ICT yaitu menggunakan metode *OCTAVE* (*The Operationally Critical Threat, Asset, and Vulnerability Evaluation*) dengan menggunakan pendekatan terhadap evaluasi risiko dari tiga aspek keamanan informasi yaitu *confidentiality*, *integrity*, dan *availability* yang komprehensif,

sistematik, terarah dan dilakukan sendiri dan diselesaikan dengan hitungan kuantitatif dengan cara melakukan wawancara, identifikasi, analisa, dan observasi.

### 4.4 Menghitung Nilai Aset Kritis

Menghitung nilai aset kritis informasi yang dimiliki organisasi dengan nilai aset berdasarkan aspek keamanan informasi yaitu kerahasiaan *(Confidentiality),* keutuhan *(Integrity),* dan ketersediaan *(Availability).* Perhitungan nilai aset dapat dilihat pada lampiran 8.

#### 4.4.1 Identifikasi nilai ancaman *(threat)* dan kelemahan *(vulnerability)*

Tujuan dari mengidentifikasi ancaman dan kelemahan adalah agar mengetahui ancaman yang mungkin terjadi dan membahayakan sistem dalam organisasi dan memahami kelemahan yang dimiliki dalam mengelola suatu aset informasi.

#### 4.4.2 Menentukan kemungkinan *(Probability)*

Tujuan menentukan kemungkinan ancaman yang timbul sesuai dengan identifikasi ancaman dan kelemahan. Penentuan kemungkinan (*Probability*) berdasarkan historis kejadian ancaman sebelumnya, atau ditentukan berdasarkan pengamatan kondisi yang dinilai. Penilaian identifikasi ancaman, kelemahan dan *probability* dapat dilihat pada lampiran 8.

#### 4.4.3 Identifikasi dampak jika terjadi kegagalan

Identifikasi dampak bisnis BIA (*Business Impact Analysis*) merupakan penentuan seberapa besar dampak atau pengaruhnya suatu risiko yang diakibatkan oleh ancaman atau kelemahan terhadap organisasi atau jalannya proses bisnis organisasi jika terjadi kegagalan penjagaan aspek keamanan informasi (CIA). Tabel identifikasi dampak jika terjadi kegagalan pada masing-masing aset dapat dilihat pada lampiran 8.

### 4.5 Analisa dan Evaluasi Risiko

Analisa risiko dan evaluasi risiko untuk menentukan level risiko dari masing-

masing aset dilakukan dengan beberapa langkah adalah sebagai berikut.

### 4.5.1 Melakukan Analisa Dampak Bisnis

Analisa Dampak Bisnis dilakukan dengan menentukan BIA pada aset yang sudah diidentifikasi pada langkah sebelumnya mengacu pada skala BIA yang dapat dilihat pada lampiran 8. nilai BIA pada masing-masing aset proses layanan bagasi, layanan garbarata, dan layanan fasilitas bandara.

### 4.5.2 Identifikasi Level Risiko

Identifikasi level risiko yaitu mengidentifikasi tingkat risiko yang timbul jika dihubungkan dengan dampak dan probabilitas ancaman yang mungkin terjadi dengan dampak yang mungkin ditimbulkan. Pada masing-masing aset dan apakah risiko tersebut di terima atau tidak pada organisasi. Tabel identifikasi risiko terdapat pada lampiran 8.

### 4.5.3 Menentukan Risiko diterima atau perlu penanganan risiko

Menentukan risiko diterima atau tidak (perlunya penanganan risiko) yaitu dengan menghitung terlebih dahulu nilai risiko dari masing-masing aset yang telah di identifikasi sebelumnya. Hasil dari perhitungan yang telah dilakukan, maka ditentukan nilai risiko dari masing-masing aset yang ditunjukkan pada lampiran 8.

### 4.5.4 Identifikasi dan Evaluasi Penanganan Risiko

Identifikasi dan evaluasi risiko bertujuan untuk menentukan pemilihan penanganan risiko jika risiko yang timbul tidak dapat diterima langsung tetapi diterima tetapi perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan risiko yang telah ditetapkan sebelumnya. Pemilihan penanganan risiko pada ICT ditentukan sebagai berikut:

a) Menerima risiko dengan menetapkan kontrol keamanan yang sesuai.
b) Menerima risiko dengan menggunakan kriteria penerimaan risiko

Setelah menentukan pilihan penanganan risiko langkah selanjutnya adalah melakukan pilihan penanganan risiko pada setiap aset yang bernilai *High*, *medium* dan *low* yaitu server, pc, wifi, router dan switch, kabel, FIDS, Counter *check-in*,

data center, data shift kerja pegawai, pegawai (SDM), data pengadaan fasilitas, data keuangan, data operator garbarata, data evaluasi tiap layanan bisnis utama, dan data calon penumpang. data jadwal penerbangan, data maskapai, dan data pengendalian bagasi, data aset, satuan pengamanan dan data pegawai. Pilihan penanganan risiko pada masing-masing aset yaitu Status risiko *risk reduction* yaitu dengan menetapkan pengendalian dengan kontrol objektif dan kontrol keamanan yang sesuai dengan ISO 27002:2013.

## 4.6 Kontrol Objektif dan kontrol keamanan

### 4.6.1 Memilih Kontrol Objektif dan Kontrol Keamanan

Setelah melakukan evaluasi dan penetapan penanganan risiko, langkah selanjutnya yaitu memilih kontrol keamanan yang sesuai dengan aset yang memiliki risiko tertinggi, dimana 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 penentuan kontrol keamanan ini dijadikan dasar untuk membuat prosedur kontrol dalam pengelolaan risiko. Berikut adalah kontrol objektif dan kontrol berdasarkan ISO/IEC 27001:2013 yang digunakan untuk masing-masing aset. Pemetaan kontrol objektif dan kontrol keamanan ISO 27001:2013 terdapat 6 Klausul, 11 Kontrol Objektif, dan 17 Kontrol Keamanan yang terdapat pada lampiran 8.

## 4.7 *Standar Operational Procedure* (SOP)

### 4.7.1 *Standar Operational Procedure* (SOP) yang dihasilkan

Berdasarkan hasil Pemetaan rekomendasi penyesuaian pengendalian risiko, didefinisikan beberapa prosedur yang dapat diusulkan dalam penelitian. Kebijakan 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 diatas didapatkan 4 kebijakan dan 6 prosedur dimana kebijakan dan prosedur dibuat berdasarkan hasil rekomendasi pengendalian risiko dan risiko yang terjadi. Penjelasan dari pembentukan dapat dilihat pada lampiran 8. Pada lampiran 8 terdapat tabel pemetaan risiko dengan klausul dan kategori kebutuhan, tabel

pemetaan risiko dengan dokumen kebijakan, tabel pemetaan kebijakan dengan prosedur, instruksi kerja, dan formulir

Tabel 4. 1 Contoh Pembahasan Hasil Pemetaan dengan Prosedur, Instruksi Kerja, dan Formulir Rekam Kerja

| Kebijakan | Prosedur | Instruksi Kerja | Formulir |
|---|---|---|---|
| KB -04<br>Human resources security | PO - 06<br>Pelatihan dan pengembangan SDM | IK - 08<br>Pelatihan dan pengembangan SDM<br>- Proses pendaftaran Pelatihan dan pengembangan<br>- Proses persiapan pelatihan dan pengembangan<br>- Proses pelatihan dan pengembangan<br>- Evaluasi pelatihan dan pengembangan | FM - 12: Data pegawai FM - 13: Evaluasi kegiatan pelatihan dan pengembangan |

### 4.7.2 Penjelasan pembentukan prosedur dan kebijakan

Pada tahap ini dijelaskan bagaimana prosedur dan kebijakan dapat dibentuk berdasarkan penilaian risiko keamanan informasi yang memiliki tingkat nilai *High*, *medium*, dan *low* dengan hasil rekomendasi pengendalian risiko dari hasil rekomendasi pengendalian risiko. Dilihat dari hasil pemetaan pada tabel Pemetaan Risiko dengan Kontrol ISO 27001:2013 dengan prosedur dan kebijakan yang dihasilkan diatas didapatkan 4 kebijakan dan 6 prosedur dimana kebijakan dan prosedur dibuat berdasarkan hasil rekomendasi pengendalian risiko dan risiko yang terjadi. penjelasan pembentukan prosedur dan kebijakan yang dihasilkan terdapat pada lampiran 8.

### 4.7.3 Perancangan struktur dan isi SOP

Pada tahap ini dijelaskan mengenai bagaimana peneliti merancang SOP. Perancangan SOP ini mengacu pada peraturan pemerintah yang membahas mengenai penyusunan *Standar Operational Procedure*. Penyusunan SOP pada penelitian ini disesuaikan dengan kebutuhan sehingga isi dari SOP secara keseluruhan memiliki perbedaan dengan isi SOP yang digunakan sebagai acuan. Adapun struktur atau isi yang dimasukkan ke dalam kerangka SOP keamanan informasi pada divisi ICT dapat dilihat pada tabel pada lampiran 8.

## A. Hasil perencanaan SOP

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

## B. Hasil Perencanaan Kebijakan

Hasil dari penyusunan kebijakan ini bertujuan untuk mendukung pelaksanaan SOP yang dimana membutuhkan dokumen-dokumen pendukung yaitu rekam kerja yang digunakan sebagai dokumentasi pada setiap langkah-langkah yang dilakukan. Pada tabel berikut merupakan tabel perencanaan kebijakan Pengendalian Hak Akses. detail dapat dilihat pada tabel 4.2. untuk hasil tabel perencanaan kebijakan yang lain dapat dilihat pada lampiran 10.

Tabel 4. 2 Contoh Tabel Hasil perencanaan Kebijakan Pengendalian Hak Akses

| | | | |
|---|---|---|---|
| | INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT | | |
| KB – 01 | | NO. RILIS : | 00 |
| | | NO. REVISI : | 00 |
| KEBIJAKAN PENGNDALIAN HAK AKSES | | TANGGAL TERBIT : | |
| | | HALAMAN : | |

**1. TUJUAN**

Kebijakan berikut ini dibuat untuk menjamin persyaratan pengendalian hak akses terhadap informasi dan fasilitas informasi yang dimiliki agar dapat di definisikan dengan cepat

1.1 ISO/IEC 27002:2013 – 12.4.1 Pencatatan Kejadian

**C. KEBIJAKAN**

2.1 Pengelolaan hak akses sistem informasi

2.2 Hak akses pada setiap sistem informasi yang terkait dengan informasi instansi harus dibedakan sesuai peran dan fungsi dari masing – masing pengguna

**D. DOKUMEN TERKAIT**

PO – 01 Prosedur Pengelolaan Hak Akses

## C. Hasil perencanaan Prosedur

Hasil perencanaan prosedur ini bertujuan untuk mendukung pelaksanaan SOP yang dimana 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 4.3. untuk hasil perencanaan prosedur yang lain dapat dilihat pada lampiran 11.

Tabel 4. 3 Contoh Tabel Hasil Perencanaan Prosedur Hak Akses

| | | |
|---|---|---|
| AngkasaPura \| AIRPORTS | Nomor SOP | PO – 01 |
| | Tgl. Pembuatan | |
| | Tgl. Revisi | |
| | Tgl. Efektif | |
| | Disahkan Oleh | General Manager |
| | Nama SOP | PERENCANAAN HAK AKSES |
| DESKRIPSI SOP | KLASIFIKASI DAN DAFTAR PELAKSANAAN | |
| Prosedur pengelolaan hak akses merupakan prosedur untuk penggunaan hak akses terhadap sistem informasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun dari luar instansi. | DAFTAR PELAKSANAAN<br>1. Pengguna sistem (staff pegawai)<br>2. Teknisi<br>3. Kepala ICT<br>4. Kepala persandian dan keamanan informasi | |
| KETERKAITAN | | |

## D. Hasil Perencanaan Instruksi Kerja

Hasil dari penyusunan instruksi kerja ini bertujuan untuk mendukung pelaksanaan SOP yang dimana membutuhkan dokumen instruksi kerja yang berguna untuk mendokumentasikan aktivitas. Pada tabel 4.4 berikut merupakan hasil perencanaan instruksi kerja. Untuk hasil dari perencanaan instruksi kerja yang lain dapat dilihat pada tabel 12.

Tabel 4. 4 Contoh Tabel Hasil Perencanaan Instruksi Kerja

| | | | |
|---|---|---|---|
| | INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT<br>*Information Communication* and *Technology Department Head* | | |
| | IK – 01 | NO. RILIS | : 00 |
| | | NO. REVISI | : 00 |
| | INTRUKSI KERJA PEMBERIAN HAK AKSES | TANGGAL TERBIT | : |
| | | HALAMAN | : |
| 1. PELAKSANA | | | |
| *Information Communication* and *Technology Department Head* | | | |
| 2. RINCIAN INSTRUKSI KERJA | | | |
| Pegawai mengajukan permintaan pemberian hak akses baru melalui email | | | |
| 3. RINCIAN INSTRUKSI KERJA | | | |
| No. | Tanggal Revisi | Uraian Revisi | |



## E. Hasil Perencanaan Rekam Kerja

Hasil dari penyusunan prosedur ini bertujuan untuk mendukung pelaksanaan SOP yang dimana membutuhkan dokumen rekam kerja yang berguna untuk mendokumentasikan aktivitas yang mendukung SOP. Pada tabel 4.5 merupakan hasil perencanaan rekam kerja. Untuk hasil perencanaan instruksi kerja yang lain dapat dilihat pada lampiran 16.

Tabel 4. 5 Contoh Tabel Hasil Pengelolaan Rekam Kerja Pengelolaan Hak Akses

| | | | |
|---|---|---|---|
| AngkasaPura \| AIRPORTS | INFORMATION COMMUNICATION TECHNOLOGY DEPARTMENT<br>Information Communication and Technology Department Head | | |
| | FM – 01 | NO. RILIS | : 00 |
| | | NO. REVISI | : 00 |
| | FORMULIR PENGELOLAAN HAK AKSES | TANGGAL TERBIT | : 00 |
| | | HALAMAN | : 01 |

FORMULIR

Tanggal : *(Diisi tanggal pengajuan pengendalian hak akses)*

Waktu : *(Diisi pada pukul jam berapa formulir diajukan)*

Status : *(Diisi status saat ini hak akses)*

| JENIS PENGELOLAAN HAK AKSES | SALURAN |
|---|---|
| ☐ **Penghapusan Hak Akses** | ☐ **E-mail** |
| ☐ **Pemberian Hak akses** | ☐ **Telepon** |
| ☐ **Perubahan Hak akses** | ☐ **Offline** |
| *(centang yang perlu)* | *(centang yang perlu)* |

IDENTITAS PEGAWAI

Nama Pegawai *(nama lengkap pegawai)*
NIP *(Nip Pegawai)*
Jabatan *(keterangan jabatan pegawai)*
Email *(email pegawai)*
No.Hp *(Diisi No.Hp Pegawai)*

| PERMINTAAN HAK AKSES | JENIS APLIKASI |
|---|---|
| Akses Saat ini : *(centang yang perlu)* | ☐ **FIDS** |
| ☐ **Teknisi** | ☐ **Counter *check-in*** |
| ☐ **ICT** | *(centang yang perlu)* |
| ☐ **Airport Technology, network, operation support section head** | |
| ☐ **General Manager** | |

CATATAN :

| | |
|---|---|
| Disetujui Oleh: | Diketahui Oleh: |
| *(ttd)* | *(ttd)* |

## 4.8 Tahap Akhir

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

### 4.8.1 Hasil Analisis dan Pembahasan

Pada tahap analisis membahas terkait dengan proses dan output dari penelitian ini, penjelasannya dapat dilihat pada tabel 4.6.

Tabel 4. 6 Contoh Hasil Analisis dan Pembahasan

| Proses | Output |
|---|---|
| 1. Pemetaan klausul klausul dengan kontrol objektif dan kontrol keamanan<br>2. Pemetaan risiko dengan kontrol keamanan<br>3. Pemetaan klausul dengan kebutuhan keamanan informasi<br>4. Pemetaan risiko dengan dokumen kebijakan<br>5. Pemetaan kebijakan, instruksi kerja, dan rekam kerja | 1. Dokumen Kebijakan:<br>a. Kebijakan pengendalian hak akses<br>b. Kebijakan keamanan informasi<br>c. Kebijakan pengelolaan hardware<br>d. Kebijakan *human resource security*<br>2. Dokumen Intruksi Kerja:<br>a. Instruksi kerja pengelolaan hak akses<br>b. Instruksi kerja perubahan password<br>c. Instruksi kerja reset password<br>d. Instruksi kerja backup data dan file<br>e. Instruksi kerja restore data<br>f. Instruksi kerja perawatan hardware<br>g. Instruksi kerja perawatan kabel dan jaringan<br>h. Instruksi kerja pelatihan dan pengembangan SDM<br>i. Instruksi kerja keamanan informasi<br>j. Instruksi peran dan tanggung jawab keamanan informasi<br>3. Dokumen Prosedur:<br>a. Prosedur pengelolaan hak akses<br>b. Prosedur pengelolaan *password*<br>c. Prosedur *backup* dan *restore*<br>d. Prosedur pengelolaan *hardware*<br>e. Prosedur pengelolaan kabel dan jaringan telekomunikasi<br>f. Prosedur pelatihan dan pengembangan SDM<br>g. Prosedur keamanan informasi<br>4. Dokumen Formulir:<br>a. Formulir pengelolaan hak akses<br>b. Formulir kontrak perjanjian hak akses<br>c. Formulir *log-on* pengelolaan hak akses<br>d. Formulir perbaikan sistem informasi<br>e. Formulir permintaan reset *password*<br>f. Formulir klasifikasi data<br>g. Formulir *log back-up* data<br>h. Formulir *restor*e data<br>i. Formulir pemeliharaan perangkat TI<br>j. Formulir berita acara kerusakan<br>k. Formulir laporan evaluasi pengelolaan perangkat TI<br>l. Formulir data pegawai<br>m. Formulir evaluasi kegiatan pengembangan kompetensi<br>n. Formulir *monitoring* keamanan informasi |

# BAB V
# PENUTUP

## 5.1 Kesimpulan

Berdasarkan hasil pengerjaan tugas akhir yang diperoleh dari penelitian sesuai dengan metode pelaksanaan yang sudah direncanakan kesimpulan yang didapatkan adalah sebagai berikut.

1. Dokumen kontrol objektif dan kontrol keamanan Dokumen pengelolaan risiko terkait keamanan informasi, meliputi: penilaian risiko, identifikasi risiko, analisa dan evaluasi risiko, identifikasi dan evaluasi risiko penanganan risiko pada PT Angkasa Pura 1(Persero) Surabaya.
2. Dokumen SOP (*Standar Operational Procedure*) meliputi: dokumen kebijakan, instruksi kerja, dan rekam kerja yang sesuai dengan pemilihan kontrol objektif dan kontrol keamanan dari hasil pengelolaan risiko terkait keamanan informasi.

## 5.2 Saran

1. Pengembangan tugas akhir dapat dilakukan dengan menambahkan dampak biaya kerugian yang dialami oleh instansi terkait.
2. Penelitian ini sebatas pembuatan dokumen SOP tanpa proses pengujian SOP, dan implementasi pada proses bisnis organisasi
3. Dokumen SOP ini masih dapat terus dikembangkan dilihat dari perkembangan teknologi yang begitu pesat sehingga instansi dapat terus bersaing dan dapat terus menjalankan proses bisnisnya dengan baik.

# DAFTAR PUSTAKA


Hughes, G. (2006). Five Steps to IT Risk Management Best Practices. Risk Management. *Risk Management*, Vol. 53, hlm, 7,34.

ISO/IEC. (2010). *ISO/IEC 27003 Information Security Management System Implementation Guidance* . Swiztzerland: ISO/IEC.

Jolly, A. (2003). *The Secure Online Business.* USA-London: Kogan Page and Contributors.

Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia. (2012). *Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia.2012.Nomor 35*. tentang Pedoman Penyusunan Standar Operational Prosedur Administrasi Pemerintahan.

Sarno, R. (2009). *Sistem Manajemen Keamanan Informasi.* Surabaya: ITSPRess Surabaya.

Siahaan, H. (2007). *Manajemen Resiko.* Jakarta: PT. Elex Media Computindo.

Sulistiyani, S. (2011). *Keamanan Sistem Informasi.* Yogyakarta: CV.ANDI.

Susilo, L. J., & Kaho, V. R. (2011). *Manajemen Risiko Berbasis ISO 31000 Untuk Industri Non-Perbankan.* Jakarta: PPM Manajemen.

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