PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2013 PADA KOMINFO PROVINSI JAWA TIMUR

TUGAS AKHIR

Program Studi

S1 Sistem Informasi

Oleh:

WILDA AYU PRATIWI

14410100156

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

2019

PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2013 PADA KOMINFO PROVINSI JAWA TIMUR

TUGAS AKHIR

Diajukan sebagai syarat untuk mengerjakan

Program Sarjana

Disusun Oleh :

Nama : Wilda Ayu Pratiwi

NIM : 14410100156

Program : S1 (Strata Satu)

Jurusan : Sistem Informasi

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

2019

بِسْمِ اللهِ الرَّحْمنِ الرَّحِيْمِ

Senyum, Syukur, Terima kasih

Seluruh kerja keras, doa, dan usaha tidak akan menghianati hasil

الْحَمْدُ للَّهِ رَبِّ الْعَالَمِيْن

Kupersembahkan tugas akhir ini kepada

Ayah (Alm), Ibu, Nenek Tercinta dan keluarga tersayang..

Sahabatku dan teman-teman yang selalu memberi semangat,

Beserta semua pihak yang telah membantu dalam penyelesaian tugas akhir.

TUGAS AKHIR

PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2013 PADA KOMINFO PROVINSI JAWA TIMUR

Dipersiapkan dan disusun oleh

Wilda Ayu Pratiwi

NIM : 14410100156

Telah diperiksa, diuji dan disetujui oleh Dewan Penguji
Pada: Februari 2019

Susunan Dewan Penguji

Pembimbing

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

II. **Yoppy Mirza Maulana, S.Kom., M.MT.**
NIDN. 0725037505

Pembahas

I. **Dr. Anjik Sukmaaji, S.Kom., M.Eng.**
NIDN. 0731057301

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana

Dr. Jusak
Dekan Fakultas Teknologi dan Informasi

FAKULTAS TEKNOLOGI DAN INFORMATIKA
INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

SURAT PERNYATAAN

PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa Institut Bisnis dan Informatika Stikom Surabaya, saya:

Nama	: Wilda Ayu Pratiwi
NIM	: 14410100156
Program Studi	: S1 Sistem Informasi
Fakultas	: Fakultas Teknologi dan Informatika
Jenis Karya	: Tugas Akhir
Judul Karya	: **PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2013 PADA KOMINFO PROVINSI JAWA TIMUR**

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Institut Bisnis dan Informatika Stikom Surabaya Hak Bebas Royalti Non-Eksklusif (*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 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, Februari 2019

Yang menyatakan

Wilda Ayu Pratiwi

NIM 14410100156

ABSTRAK

Kominfo merupakan instansi pemerintahan jawa timur sebagai pemenuh kebutuhan TIK Berdasarkan Peraturan Daerah Nomor 80 Tahun 2016. Kondisi saat ini Kominfo Jatim memiliki kendala dalam segi manajemen, teknikal dan operasional dalam penanganan keamanan informasi terkait dengan asset informasi sehingga masih menimbulkan permasalahan terkait dengan *Confidentiality* (kerahasiaan), *Integrity* (keutuhan) dan *Availability* (ketersediaan).

Dalam memenuhi kebutuhan keamanan informasi tersebut maka metode penelitian yang digunakan yaitu perhitungan manajemen risiko dengan menggunakan metode OCTAVE digunakan untuk menghitung seberapa tinggi dampak untuk instansi jika risiko itu terjadi dan membuat ranking prioritas untuk masing-masing risiko. Kemudian dilakukan pengendalian risiko yang telah diidentifikasi dengan menggunakan kerangka kerja kontrol keamanan ISO/IEC 27002:2013.

Hasil dari penelitian ini adalah dokumen pengelolaan manajemen risiko dan penyusuanan kontrol keamanan untuk mendukung pembuatan dokumen SOP dari kategori kebutuhan manajemen terdiri dari 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: Kominfo, ISO27001, SMKI.

KATA PENGANTAR

Puji dan syukur kami panjatkan kehadirat Tuhan Yang Maha Esa, karena hanya atas berkat dan rahmat-Nya, sehingga Laporan Tugas Akhir sistem informasi yang berjudul "Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 Pada Kominfo Provinsi Jawa Timur " dapat diselesaikan dengan baik dan tepat waktu. Adapun tujuan penulisan laporan ini adalah untuk memenuhi persyaratan dalam menempuh kelulusan Strata Satu Sistem Informasi Institut Bisnis dan Informatika Stikom Surabaya.

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(Alm), Ibu dan Nenek yang selalu mendoakan, mendukung penuh penyelesaian tugas akhir ini, dengan memberikan semangat dan motivasi yang tiada henti.
2. Bapak Erwin Sutomo S.Kom., M.Eng selaku pembimbing pertama yang telah memberikan banyak masukan dan saran dalam proses pembuatan laporan tugas akhir ini.
3. Bapak Yoppy Mirza Maulana, S.Kom., M.MT selaku pembimbing kedua yang telah memberikan banyak masukan, saran serta membangun cara berpikir logic dan kritis, dalam proses penyususnan laporan tugas akhir ini.

4. Terima kasih kepada Bapak Dendy, Ibu Tutik Worawari, Bapak Aulia dan pihak instansi Kominfo Jatim yang telah memberikan kesempatan untuk melakukan penelitian.
5. Terima kasih untuk kedua sahabat saya yang selalu memberikan motivasi, dukungan dan doanya (Nuris Sabith dan Fitri Dwi)
6. Terima kasih untuk San yang selalu setia mendampingi, mengarahkan, serta memberikan semangat penuh penulis dalam menyelesaikan Tugas Akhir.
7. Terima kasih kepada rekan tim Tugas Akhir (Rozak, Ester Debora, Nur Qoriah, Diva) yang telah memberikan dukungan, imotivasi, dan doa dalam penyelesaian tugas akhir ini.
8. Terima kasih kepada seluruh pihak dan teman-teman lain yang belum dapat penulis sebutkan satu persatu yang secara langsung maupun tidak langsung terlibat dalam proses pengerjaan laporan tugas akhir ini.

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

Surabaya, Februari 2019

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dinas Komunikasi dan Informatika Provinsi Jawa Timur adalah Dinas yang mempunyai tugas melaksanakan kewenangan daerah di bidang pengelolaan TIK. Berdasarkan Peraturan Daerah Nomor 80 Tahun 2016 tentang kedudukan, susunan organisasi, uraian tugas dan fungsi serta tata kelola kerja Kominfo merupakan unsur pelaksana urusan pemerintahan di bidang Komunikasi dan Informatika, bidang Statistik dan bidang Persandian. Tujuan dari Kominfo adalah meningkatkan pengetahuan, kecerdasan, pemberdayaan dan kesejahteraan masyarakat melalui penyelenggaraan komunikasi dan informatika dalam rangka meningkatkan keterbukaan informasi publik.

Pada Seksi Keamanan dan Persandian Kominfo memiliki proses bisnis diantaranya layanan kirim dan terima berita dinas, aplikasi pihak ke tiga yaitu aplikasi pengajuan permohonan meliputi internal kominfo maupun eksternal, monitoring rutin keamanan *server* hosting, pembaharuan aplikasi *website*, pembuatan aplikasi swakelola salah satunya yaitu aplikasi SIM kepegawaian, pengajuan email dan sub domain, pembuatan dokumen laporan aptika serta terkait tata kelola teknologi informasi. Aset informasi yang diperlukan dalam pendukung proses bisnis pada Seksi Keamanan dan Persandian Kominfo yaitu meliputi aset informasi, aset perangkat lunak, aset perangkat keras, dan layanan teknologi informasi dan komunikasi. Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting.

Pentingnya informasi yang dimiliki Kominfo membuat keamanan informasi itu penting untuk dilakukan. Nilai sebuah informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang-orang tertentu. Kondisi saat ini masih terjadi kurangnya penanganan keamanan informasi sehingga masih menimbulkan *Threat* (Ancaman) dan *Vulnerable* (Kelemahan) yang mengakibatkan target tidak terpenuhi dan mempengaruhi *Confidentiality* (kerahasiaan), *Integrity* (keutuhan) dan *Availability* (ketersediaan) yang akan berdampak pada *Business Impact Analysis (*BIA*)*, (Sarno dan Iffano, 2009).

Pada kondisi saat ini ditemukan adanya *Threat* (Ancaman) dan *Vulnerable* (Kelemahan) dari segi manajemen, teknikal dan operasional yaitu: *Threat* (Ancaman) yang terjadi serangan dari luar meliputi: (*Hacker* dan *Computer criminal*) diantaranya penyusupan ke sistem dan akses ilegal yaitu adanya laporan terkait dengan ditemukan web yang terkena hack dan penyusupan atau akses ilegal web Kominfo. Serangan virus *ransomeware* yaitu adanya laporan terkait sengan serangan virus yang menimbulkan adanya data yang hilang, serangan *black mail/spam email, dan spam account* yaitu adanya laporan dari hasil teknisi dilakukan refreshing dan memungkinkan untuk *restart* semua, laporan hasil bulanan yang menunjukkan hasil yang tidak memuaskan, laporan terjadinya perubahan *password* yang tidak tepat (tidak sesuai aturan) . Solusi yang diberikan dengan adanya ancaman untuk saat ini yaitu dengan cara melakukan *upgrade* dan *backup* secara berkala. *Vulnerable* (Kelemahan) yang terjadi yaitu kesalahan sumber daya manusia, meliputi: adanya kegagalan dalam fungsi pencatatan dan pendataan pada *software* (Aplikasi Presensi Pegawai) adanya laporan yang mengakibatkan tidak dapat membedakan penambahan data baru dan mengedit data

yang sudah ada. Adanya kesalahan dalam *hardware* (server web *fingerprint* tidak berfungsi dengan baik) karena penggunaan kapasitas yang berlebihan, dan kesalahan dalam pengelolaan data dari hasil monitoring diketahui bahwa penggunaan CPU untuk server ini sangat tinggi. Solusi yang diberikan dengan adanya kelemahan untuk saat ini yaitu dengan cara melakukan memberikan notifikasi kepada pihak pengembang aplikasi agar segera memperbaiki aplikasi tersebut, penambahan server untuk web *fingerprint* dan melakukan monitoring secara rutin, dan melakukan pengecekan ulang terkait data atau file yang tersimpan.

Dampak yang terjadi yaitu dari sisi *Confidentiality* (kerahasiaan) adalah kesalahan dalam pengelolaan hak akses dan penggunaan *password* yang masih belum dikelola dengan baik sehingga dapat menghambat kelancaran proses bisnis dan terjadinya gangguan dalam *mail server*. *Integrity* (keutuhan) adalah kurangnya penaganan *hardware* yang baik dan kurangnya pengamanan di lingkungan ruang server, pemrosesan informasi terganggu oleh *virus ransomeware* yang menyebabkan data hilang yang menghambat kinerja organisasi. *Availability* (ketersediaan) yaitu adanya berita dan dokumen terkait perubahan yang tidak *update* dan informasi yang diberikan tidak akurat yang dapat mengganggu reputasi instansi. Informasi yang bernilai penting dan harus di lindungi tersebut merupakan aset bagi organisasi diantaranya informasi mengenai *data center*, informasi berita yang akan dipublikasikan dan laporan terkait perencanaan, pengganggaran, pengendalian, pengembangan dan evaluasi program merupakan beberapa aset informasi yang harus dilakukan pengamanan untuk memenuhi karakteristik nilai informasi. Solusi yang diterapkan saat ini belum bisa membawa perubahan yang signifikan untuk penanganan aset informasi penting yang ada pada Kominfo.

Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi dari sisi *CIA* adalah dengan penyusunan dokumen pengelolaan risiko terkait dengan keamanan informasi dan pembuatan dokumen SOP (*Standar Operational Procedure*) dengan tujuan sebagai acuan kerja dan standarisasi untuk mengatur banyaknya orang yang menggunakan dan membuat proses bisnis yang ada pada Kominfo lebih terstruktur, juga meningkatkan kualitas keamanana informasi yang ada. Pembuatan dokumen SOP (*Standar Operational Procedure*) dipilih melalui pengendalian kontrol objektif dan kontol keamanan menggunakan ISO/IEC 27001:2013 yang sesuai dengan kebutuhan keamanana informasi dengan mempertimbangkan hasil pengelolaan risiko keamanan informasi yang dilakukan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan diatas, maka dapat dirumuskan permasalahan yang akan diselesaikan pada penelitian ini yaitu bagaimana perencanaan sistem manajemen keamanan informasi berdasarkan standar ISO 27001:2013 pada Kominfo Provinsi Jawa Timur, yang dapat diuraikan sebagai berikut:

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

1.3 Batasan Masalah

Berdasarkan perumusan masalah yang telah dipaparkan sebelumnya, dalam penelitian ini batasan masalah yang harus diperhatikan adalah sebagai berikut :

1. Perencanaan sistem manajemen keamanan sistem informasi dilakukan pada kinerja proses untuk sub bagian Bidang Teknologi Informasi khususnya bagian Seksi Keamanan Informasi dan Persandian.
2. Data yang digunakan yaitu data risiko pada tahun 2017.

1.4 Tujuan

Tujuan dalam penelitian ini yaitu menghasilkan dokumen perencanaan SMKI sebagai berikut.

3. Dokumen pengelolaan risiko terkait keamanan informasi, meliputi: Penilaian risiko, Identifikasi risiko, Analisa dan evaluasi risiko, Identifikasi dan evaluasi penanganan risiko pada Kominfo.
4. Dokumen kontrol objektif dan kontrol keamanan
5. 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.

1.5 Manfaat

Adapun manfaat dari penelitian yang akan diperoleh adalah sebagai berikut :

1. Dapat menambah pengetahuan tentang proses perencanaan sistem manajemen keaman informasi dan apa saja aktivitas yang harus dilaukan pada setiap

prosesnya.

2. Membantu Seksi Keamanan Informasi dan Persandian dalam mengelola risiko keamanan informasi dan pembuatan SOP yang mengacu ke dalam standar internasional ISO 27001:2013 tentang *Security techniques Information security management systems Requirements.*
3. Membantu Kominfo dalam melakukan *improvement* keamanan informasi.

BAB II

LANDASAN TEORI

2.1 Kerangka Teori

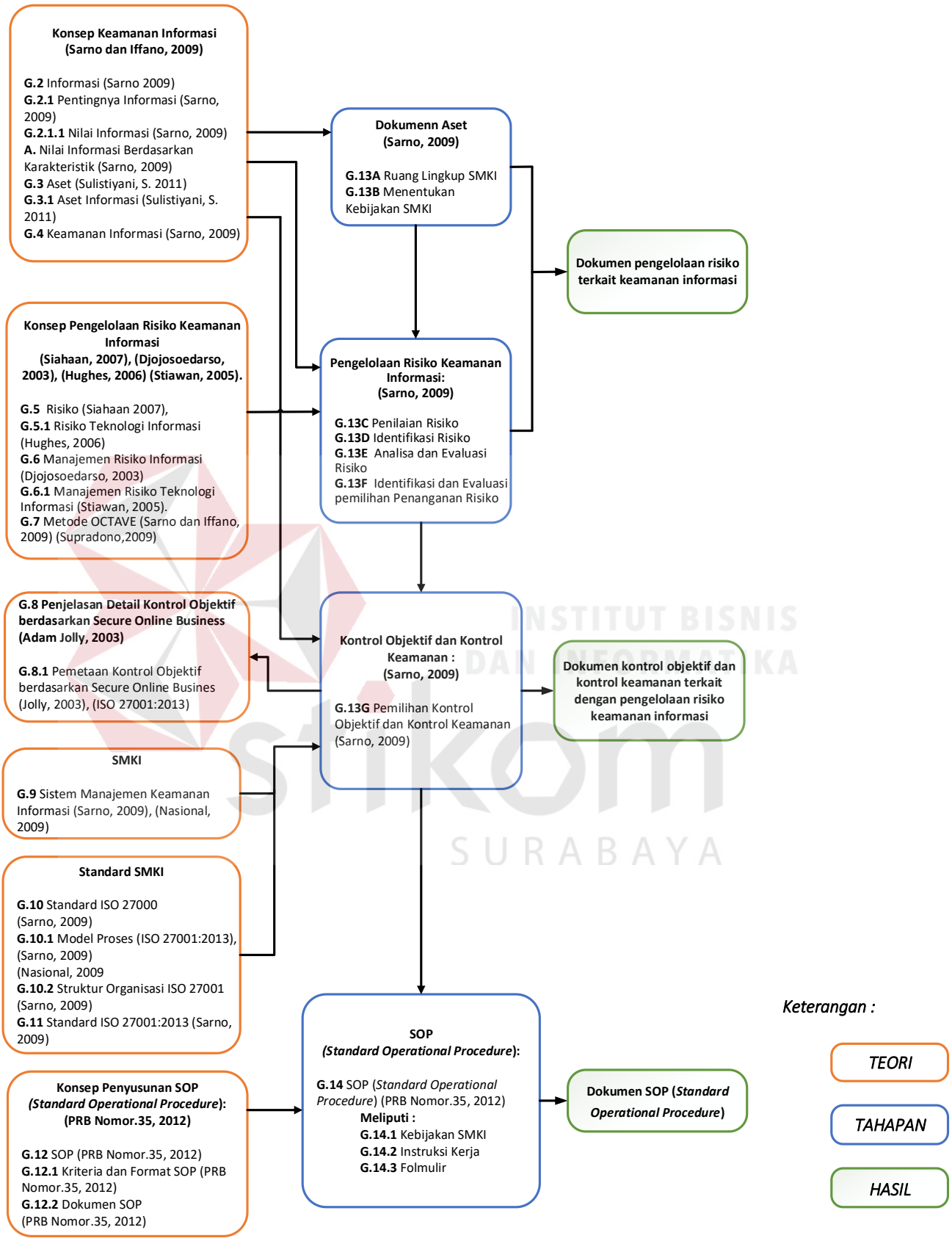
Kerangka teori adalah kemampuan seorang peneliti dalam mengaplikasikan pola berpikirnya dalam menyusun secara sistematis teori-teori yang mendukung permasalahan penelitian. Teori adalah himpunan konstruk (konsep), definisi, dan pandangan sistemantis tentang gejala dengan menjabarkan relasi antara variabel untuk menjelaskan dan meramalkan gejala tersebut (Rakhmat, 2004). Teori berguna manjadi titik tolak atau landasan berpikir dalam memecahkan atau menyoroti masalah. Teori-teori yang akan digunakan untuk membantu dalam melakukakan penelitian ini dapat dilihat pada gambar 2.1

2.2 Informasi

Informasi adalah salah satu aset bagi sebuah instansi atau organisasi, yang sebagaimana aset lainnya memiliki nilai tertentu bagi instansi atau organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan instansi atau organisasi, meminimalisir kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinya investasi dan memperluas peluang usaha.

2.2.1 Pentingnya Informasi

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 instansi untuk saat ini maupun masa mendatang. Oleh karena itu informasi tersebut dikatakan penting. (Sulistiyani, S. 2011).



Gambar 2.1 - Kerangka Teori

2.2.2.1 Nilai Informasi (*Value of Information*)

Penentuan tingkat kepentingan informasi pada suatu instansi adalah dengan menetukan 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. Sebagian besar informasi dinikmati oleh lebih dari satu pihak sehingga sulit untuk menghubungkan suatu informasi dengan biaya untuk memperolehnya dan sebagian besar informasi tidak dapat ditaksirkan keuntungannya dengan satuan uang tetapi dapat ditaksir nilai efektivitasnya. (TataSutabri, 2003) berpendapat bahwa nilai informasi tidak mudah untuk dinyatakan dengan ukuran yang bersifat kuantitatif. Namun, nilai informasi dapat dijelaskan menurut skala relatif. Misalnya, jika suatu informasi dapat menghasilkan hal yang mengurangi ketidakpastian bagi pengambilan keputusan, maka nilai informasinya tinggi. Sebaliknya, jika suatu informasi kurang memberikan relevansi bagi pengambilan keputusan, informasi tersebut dikatakan kurang bernilai atau informasinya rendah (Abdul Kadir, 2003).

A. Nilai informasi

Nilai informasi dapat ditentukan berdasarkan karakteristik atau sifat informasi yang dimiliki (Sarno dan Iffano, 2009) yaitu sebagai berikut :

1. Mudah diperoleh, sifat ini menunjukkan mudahnya dan cepatnya informasi dapat diperoleh keluaran informasinya.
2. Sifatnya luas dan lengkap, sifat ini menunjukan lengkapnya isi informasi yang dibutuhkan.
3. Ketelitian, sifat ini berhubungan dengan tingkat kebebasan dari kesalahan

keluaran informasinya

4. Kecocokan, sifat ini menunjukkan nilai informasi semakin baik nila ada hubungannya dengan permintaan para pemakai.
5. Ketepatan waktu, sifat ini berhubungan dengan waktu yang dilakukan yang baik pendek daripada siklus perolehan informasi: msukan, pengelolaan, dan pelaporan keluaran kepada pemakai.
6. Kejelasan, sifat ini menunjukkan tingkay keluaran informasi bebas dari istilah-istilah yang tidak jelas.
7. Keluwesan, sifat ini berhubungan dengan lebih dari satu keputusan, tetapi juga dengan lebih dari seorang pengambil keputusan.
8. Dapat dibuktikan, sifat ini menunjukkan beberaoa pemakai informasi untuk menguji keluaran informasi hingga sampai pada kesimpulan yang sama.
9. Tidak ada prasangka, sifai ini berhubungan dengan tidak adanya keinginan untuk mengubah informasi guna mendapatkan kesimpulan yang telah dipertimbangkan sebelumnya.
10. Dapat diukur, informasi seharusnya bisa diukur dan sifat ini menunjukkan bahwa hakikat informasi adalah yang dihasilkan dari sistem informasi formal.

2.3 Aset

Aset merupakan sumber daya yang dimiliki oleh instansi atau semua hak yang dapat digunakan dalam instansi. Aset juga termasuk didalamnya pembebanan yang ditunda yang dinilai dan diakui sesuai dengan prinsip ekonomi yang berlaku (Sulistyani,2011). Sementara menurut FASB (*Financial Accounting Standars Boards)* menjelaskan aset adalah kemungkinan keuntungan ekonomi yang diperoleh atau dikuasai di masa yang akan datang oleh instansi sebagai akibat

transaksi atau kejadian yang sudah berlalu.

2.3.1 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 akan 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 sesuatu yang berharga bagi organisasi. Komponen sistem informasi dibangun berdasarkan komponen-komponen pendukung yang meliputi: sumber daya manusia *(people)*, perangkat keras *(hardware)*, perangkat lunak *(software)*, data dan jaringan *(network)*.

2.4 Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (business continuity), meminimalisi risiko bisnis (reduce business risk) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno dan Iffano, 2009).

Aspek Keamanan Informasi meliputi tiga hal, yitu: *Confidentiality*, *Integrity, dan Availability* (CIA). Aspek tersebuut dapat dilihat pada Gambar G.2 yang lebih lanjut akan di jelaskan sebagai berikut.

1. Kerahasiaan *(Confidentiality)* : Informasi bersifat rahasia dan harus dilindungi terhadap keterbuakaan dari pengguna yang tidak berkepentingan.
2. Ketersediaan *(Integrity)* : Layanan, fungsi sistem, informasi harus terjamin dan

tersedia bagi pengguna saat diperlukan.

3. Integritas *(Availibility)* : Informasi harus komplit dan tidak dirubah. Dalam teknologi informasi, kata informasi terkait dengan berita. Hilangnya integritas informasi berarti berita tersebut tidak akurat.

Gambar 2.2 - Aspek Keamanan Informasi (Sarno, 2009).

2.5 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).

2.5.1 Risiko Teknologi Informasi

Menurut Hughes (2006, p. 36), dalam penggunaan teknologi informasi berisiko terhadap kehilangan informasi dan pemulihannya yang tercakup dalam 6 kategori, yaitu:

1. Keamanan, yaitu Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berwenang.
2. Ketersediaan, yaitu Risiko yang datanya tidak dapat diakses setelah kegagalan sistem, karena kesalahan manusia (human error), Instansi konfigurasi, dan kurangnya pengurangan arsitektur.

3. Daya pulih, yaitu Risiko dimana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah terjadinya kegagalan dalam perangkat lunak atau keras, ancaman eksternal, atau bencana alam.
4. Performa, yaitu Risiko dimana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaan yang tinggi dan topografi informasi teknologi yang beragam.
5. Daya skala, yaitu Risiko yang perkembangan bisnis, pengaturan bottleneck, dan bentuk arsitekturnya membuatnya tidak mungkin menangani banyak aplikasi baru dan biaya bisnis secara efektif.
6. Ketaatan, yaitu Risiko yang manajemen atau penggunaan informasinya melanggar keperluan dari pihak pengatur yang dipersalahkan dalam hal ini mencakup aturan pemerintah, panduan pengaturan instansi dan kebijakan internal.

2.6 Manajemen Risiko Keamanan Informasi

Manajemen risiko adalah sebuah bidang ilmu yang membahas bagaimana sebuah instansi atau organisasi dapat menerapkan ukuran dalam melakukan pemetaan permasalahan dengan pendekatan manajemen secara komprehensif dan sistematis (Siahaan, 2007). Manajemen risiko adalah sebuah proses yang meliputi identifikasi, penilaian dan menentukan risiko, pengambilan tindakan untuk melakukan mitigasi atau antisipasi serta pemantauan dan melakukan *review* progres dari setiap tahapan yang ada. (Djojosoedarso, 2003).

2.6.1 Manajemen Risiko Teknologi Informasi

Manajemen risiko teknologi informasi adalah pengelolaan risiko teknologi informasi /sistem informasi pada sebuah organisasi atau instansi tertentu yang

memiliki tujuan untuk meminimalisasi risiko yang mungkin muncul dengan solusi yang berhubungan dengan aspek teknologi informasi/sistem informasi (Stiawan, 2005).

2.7 Metode OCTAVE

Metode OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) yang dikembangkan Software Engineering Institute, Carnegie Mellon University, 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. Terdapat beberapa fase pada Metode OCTAVE, yaitu sebagai berikut:

Fase 1: Melihat dari sisi organisasi

a. Proses

1) Mengidentifikasi berdasarkan pengetahuan pihak manajemen senior
2) Mengidentifikasi berdasarkan pengetahuan pihak manajemen wilayah operasional
3) Mengidentifikasi berdasarkan pengetahuan staff
4) Membuat Profil ancaman

b. Output

1) Melakukan *list* aset penting pada organisasi
2) Kebutuhan keamanan bagi aset penting

3) *List* upaya untuk melindungi aset informasi penting

4) *List* ancaman terhadap aset kritis

5) *List* kelemahan kebijakan pada organisasi

Fase 2: Melihat sisi teknologi

a. Proses

1) Melakukan identifikasi komponen kunci

2) *Evaluate* Infrastruktur komponen

b. Output

1) *List* Komponen utama dan infrastruktur

2) Mendapatkan Identifikasi kerentanan teknologi pada organisasi

Fase 3: Menganalisa risiko teknologi informasi

a. Proses

1) Melakukan analisa risiko

2) Mengembangkan strategi keamanan

b. Output

1) Daftar Risiko terhadap aset kritis

2) Hasil Pengukuran tingkat Risiko

3) Strategi keamanan berdasarkan implementasi Octave

4) Rencana-rencana dari pengurangan atau mitigasi risiko

2.8 Penjelasan Detail Kontrol Objektif

2.8.1 Pemetaan Kontrol Objektif

Berikut adalah pemetaan kontrol objektif (ISO 27001:2013) berdasarkan Secure Online Business (Jolly, 2003) yang dapat dilihat pada Tabel 2.1

Tabel 2.1 - Pemetaan Kontrol Objektif berdasarkan Secure Online Business (Jolly, 2003)

No.	ISO 27001: 2013	Contents
1.	Klausul 5 : Kebijakan Keamanan Informasi Klausul 8 : Manajemen Asset Klausul 11 : Keamanan Fisik Dan Lingkungan Klausul 18 : Kesesuaian	Kebijakan Keamanan
2.	Klausul 6 : Organisasi Keamanan Informasi Kontrol Objektif : 6.2 Kontrol Keamanan : 6.2.2	Bekerja Jarak Jauh
3.	Klausul 7 : Keamanan Sumber Daya Manusia	Pengendalian Musuh Internal
		Kerahasiaan SDM dan Budaya Keamanan
4.	Klausul 9 : Kontrol Akses Kontrol Objektif : 9.2 Kontol Keamanan : 9.2.4	Otentikasi dan Enkripsi
	Klausul 10 : Kriptografi	
5.	Klausul 9 : Kontrol Akses	Jaringan
	Klausul 13 : Keamanan Komunikasi	
	Klausul 14 : Sistem Akuisisi, Pengembangan Dan Pemeliharaan	
6.	Klausul 12 : Keamanan Operasi Kontrol Objektif : 12.2 Kontrol Keamanan : 12.2.1	Data Recovery
7.	Klausul 13 : Keamanan Komunikasi Kontol Ojbektif : 13.2 Kontrol Keamanan : 13.2.3	*Email*
8.	Klausul 14 : Sistem Akuisisi, Pengembangan Dan Pemeliharaan	Perilindungan Perangkat Lunak
9.	Klausul 15 : Manajemen Penyampaian Layanan Pemasok	Manajemen Layanan Keamanan

Tabel 2.1 (Lanjutan)

No.	ISO 27001: 2013	Contents
10.	Klausul 16 : Informasi Manajemen Insiden Keamanan	Risiko Informasi
11.	Klausul 17 : Aspek Keamanan Informasi Manajemen Kontinuitas Bisnis	Manajemen Kelangsungan Bisnis

Di dalam tabel Pemetaan Kontrol Objektif berdasarkan Secure Online Business (Jolly, 2003) tersebut adapun penanganan teknis yang tertulis pada table 2.2.

Tabel 2.2 - Penanganan Teknis (Jolly, 2003)

No.	Contents	Penanganan Teknis
1.	Kebijakan Keamanan	- Data dan Informasi - Aset organisasi - Hukum - Cybercrime : Perlindungan data, Whistle-blowing kebijakan
2.	Bekerja Jarak Jauh	- Teknik koneksi dial-up point-to point - Business internet-driven - VPN (Virtual Private Network) - Teleworkers
3.	Pengendalian Musuh Internal	- Pegawai/SDM - Password - Virus - Kejahatan internet - *E-mail* - Jaringan
	Kerahasiaan SDM dan Budaya Keamanan	- Teknik rekrutmen outsourcing (kontrak kerja dan kebijakan), pelatihan
4.	Otentikasi dan Enkripsi	- Otentikasi : password - Privasi data : Secure Socket Layer (SSL) - Integrasi : sertfikat digital (identitas fisik dan identitas digital), Kriptografi - Otorisasi : URL, akses kontrol

Tabel 2.2 (Lanjutan)

No.	Contents	Penanganan Teknis
5.	Jaringan	- Teknik keamanan software : firewall dan fungsi enkripsi VPN (Virtual Private Network), VLAN - Teknik penolakan layanan - Pencegahan intrusi / deteksi jaringan
6.	Data Recovery	- Back-up - Merekam file - Simpan dalam hardisk
7.	*Email*	- Enkripsi data - Enkripsi teknik anti-virus - Tanda tangan digital / teknik kriptografi
8.	Perilindungan Perangkat Lunak	- Deteksi gangguan : Intrusion Detection Systems (IDS) - Firewall : IP, filter paket berdasarakan jenis data atau TCP/IP nomor port, aplikasi proxy - Virus :software anti-virus - Otentikasi dan enkripsi - Manajemen Hak digital dan Lisensi elektronik: teknik DMR
9.	Manajemen Layanan Keamanan	- Service-level agreements (SLAs) - Network operations centre (NOC)
10.	Risiko Informasi	- Menghitung probabilis dampak informasi - Menghitung Return On Investment (ROI)
11.	Manajemen Kelangsungan Bisnis	- Teknik Stategi Business Continuity Management (BCM) - Strategi kelangsungan bisnis : Tahap 0 : Perencanaan Pra-Proyek Tahap 1 : Penilain Tahap 2 : Desain Tahap 3 : Pelaksanaan Tahap 4 : Pengujian, pemeliharaan dan perbaikan

Adapun penjelasan dari penanganan teknis pada tabel 2.2 sebagai berikut:

1. Kebijakan Whistle-blowing yaitu sistem pelaporan pelanggaran yang memungkinkan setiap orang untuk melaporkan adanya dugaan tindakan kecurangan, pelanggaran hukum, etika, dan kode etik Instansi yang dilakukan oleh Pegawai.
2. Teknik koneksi dial-up-point-to-point yaitu metode yang menghubungkan pekerjaan jarak jauh melalui internet ke sistem instansi.
3. VPN (Virtual Private Network) Teleworkers yaitu teknik menghubungkan jaringan jarak jauh instansi dan mengakses sistem bisnis dan informasi yang penting
4. VPN (Virtual Private Network) yaitu jaringan pribadi virtual keamanan antara dua titik, antara kantor pusat jaringan instansi dan kantor cabang terpencil. Melewati enkripsi data melalui Internet publik, kemudian mendekripsi itu pada titik tujuan dan melindungi data dari hacker pada jalurnya melalui Internet, dan membuat data tidak terbaca selama proses pengiriman.
5. Secure Socket Layer (SSL) yaitu kemampuan untuk memastikan privasi informasi yang ditransfer antara server web dan web browser pengguna. Hal ini dilakukan dengan mengenkripsi informasi sebelum mengirimnya dan kemudian mendekripsikan kepada penerima, sehingga hampir tidak mungkin untuk diterjemahkan jika terjadi kecurangan.
6. Sertfikat Digital (identitas fisik dan identitas digital) yaitu sebagai bentuk otentikasi dalam pertumbuhan trasaksi internet. Sertifikat digital membantu mengidentifikasi pengguna dengan mengharuskan untuk mengkases

kredensial digital yang seharusnya hnya digunakan oleh pemilik yang sah.

7. Akses bersyarat yaitu sebuah direktori dari file berdasarkan daftar kontrol akses yang bertujuan untuk mengakses data pengguna atau sumber daya yang dilindungi
8. Teknik penolakan layanan yaitu serangan berbasis hacker pada web server yang mencegah pelanggan / pengunjung dari mendapatkan akses ke situs web organisasi. Biasanya diluncurkan oleh virus worm (misalnya Code Red, Code Blue) yang dapat mereplikasi dari komputer ke komputer. Ada juga 'distributed denial of service' serangan, yang secara bersamaan menyerang beberapa server sekaligus.
9. Pencegahan intrusi / deteksi jaringan yaitu aplikasi yang memberikan alarm untuk operator pencegahan intrusi. Hal ini juga memiliki kemampuan untuk menjatuhkan serangan dari jaringan untuk menghentikannya dari mencapai target.
10. Backdoor atau U-turn yaitu metode serangan jaringan yang bertujuan untuk kantor cabang kecil yang memiliki akses Internet baik lokal maupun melalui VPN instansi masuk secara ilegal diperoleh melalui link lokal dan, sekali di balik situs remote VPN.
11. Enkripsi *email* yaitu metode praktis untuk memastikan bahwa informasi yang berkaitan dengan out-of-date/yang sudah kedaluarsa di catatan dan dibuang dengan benar .
12. Tanda tangan digital yaitu cara penandatangannan dan penyegelan elektroik yang terintegrasi dan menggunakan kriptografi kunci public. Sebuah email yang telah ditandatangani secara digital memastikan bahwa pesan tidak

dapat ditolak atau dianggap tidak sah (ditolak oleh pengirim).

13. Intrusion Detection Systems (IDS) yaitu memberikan arahan untuk mendeteksi sistem dalam menyediakan kesempatan yang ideal untuk mengelola dan mengevaluasi layanan keamanan jaringan tanpa menimbulkan risiko biaya yang besar.
14. Filter paket yaitu jenis yang paling dasar dari firewall dan sering gratis dan tersedia pada router populer. Sebuah filter paket hanya memeriksa alamat IP daftar kontrol akses (ACL), dan akan menolak akses ke alamat yang tidak sesuai dengan daftar. Filter paket juga dapat memiliki aturan berdasarkan jenis data atau TCP / IP (transmisi protokol kontrol / protokol Internet) nomor port.
15. Infrastruktur kunci dan publik (PKI) yaitu sebuah cara untuk menarik atau meningkatnya minat dari sejumlah instansi besar dan menengah dan organisasi, sebagai penyedia layanan untuk memperoleh keuntungan strategis dan financial.
16. Managemen Hak digital dan Lisensi elektronik: teknik DMR yaitu sebuah lisensi atau hak cipta elektronik untuk aplikasi yang diberikan langsung atau dalam pengembangan yang masih mempertahankan hak akses penuh kapan atas bagaimana dan kapan merekan dapat membuka aplikasi tersebut melalui lisensi elektronik.
17. Service-level agreements (SLAs) yaitu komponen kunci tujuan dan sasran dari pemasok dan klien bersama yang bertujuan untuk memberikan playanan keamanan yang memenuhi bisnis dan persyaratan teknis yang telah disepakati.

18. Network operations centre (NOC) yaitu merupakan indikasi bahwa penyedia layanan pemiliki pusat operasi keamanan jaringan (memantau, mengelola, dan mengatur).
19. Menghitung Return On Investment (ROI) yaitu cara analisa biaya/risiko atau manfaat yang komprehensif untuk setiap pengeluaran keamanan.
20. Teknik Stategi Business Continuity Management (BCM) yaitu suatu proses mengidentifikasi potensi dampak yang mengancam organisasi dan menyediakan kerangka kerja untuk membangun ketahanan dan kemampuan untuk respon yang efektif melindungi kepentingan stakeholder, reputasi organisasi, brand, dan kegiatan penciptaan nilai.
21. Strategi kelangsungan bisnis yaitu strategi untuk mencapai BCM yang dibagi dengan 5 tahap.

Pemetaan ISO 27001:2013 dengan contents buku Secure Online Business (Jolly, 2003) bertujuan untuk mempermudah memberikan penaganan dari hasil pengelolaan risiko keamanan informasi secara teknis.

2.9 Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (Plan), mengimplementasikan (Do), memonitor adan meninjau ulang (Check) dan memelihara (Act) terhadap keamanan informasi instansi [ISO/IEC 27001:2013]. Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (Confidentially), Keutuhan (Integrity), dan Ketersediaan (Avaibillity) dari informasi. (Sarno, 2009).

SMKI berdasarkan ISO/IEC 27001:2013 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara

serta mendokumentasikan sistem manajemen keamanan informasi (SMKI). ISO/IEC 27001 mendefinisikan keperluan-keperluan untuk sistem manajemen keamanan informasi yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang terpenting agar terhindar dari resiko kerugian/bencana dan kegagalan pada pengamanan informasi. ISO 27001 digunakan sebagai ikon sertifikasi ISO 27000. ISO 27000 merupakan dokumen standar sistem manajemen keamanan informasi yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi dalam usaha untuk mengimplementasikan konsep-konsep keamanan informasi dalam organisasi. (Sarno, 2009) (Nasional, 2009).

2.10 Standar ISO/IEC27000 Security techniques Information security management systems Requirements.

Dalam standar keamanan informasi ISO/IEC 27000 memiliki beberapa series yang telah dikembangkan untuk manajemen keamanan informasi atau ISMS. Series dari ISO/IEC 27000 terdiri dari :

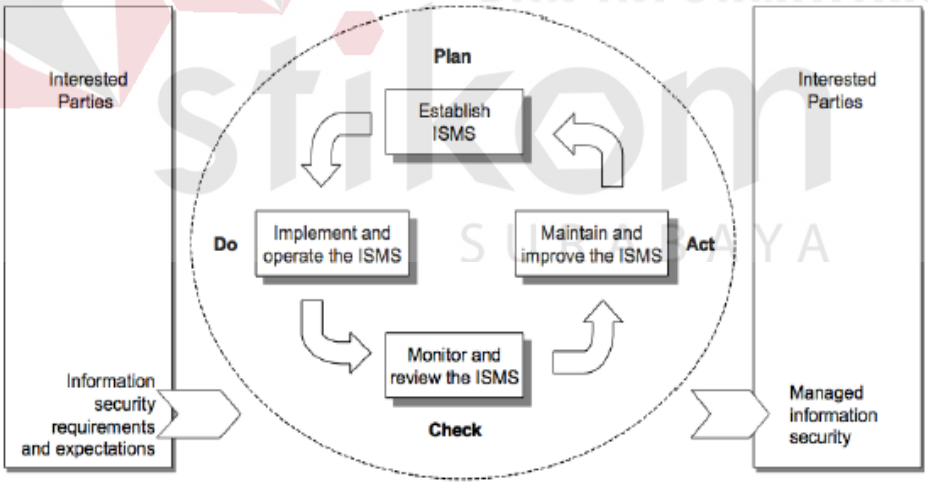
a. ISO/IEC 27000 - Information security management systems Overview and vocabulary.
b. ISO/IEC 27001 - Information security management systems Requirements.
c. ISO/IEC 27002 - Code of practice for information security management .
d. ISO/IEC 27003 - Information security management system implementation guidance.
e. ISO/IEC 27004 - Information security management Measurement
f. ISO/IEC 27005 - Information security risk management
g. ISO/IEC 27006 - information security management system certification

h. ISO/IEC 27007 - auditing enterprise information security management system.

Standar internaisonal ini telah dipersiapkan untuk menyediakan sebuah model pembangunan, penerapan, pengerjaan, pengawasan, peninjauan, pemeiliharaan, peningkatan sebuah SMKI. Standar ini mengadopsi model Plan-Do-Check-Act (PDCA) yang diterapkan untuk menyusun sebuah proses SMKI. (Humphreys, 2007).

2.10.1 Model Proses

ISO/IEC 27001:2013 menetapkan model tahapan yang dibutuhkan dalam mengimplementasikan pemenuhan manajemen keamaman informasi dengan tujuan orgnisasi dan kebutuhan bisnis. (ISO/IEC, ISO/IEC 27001 Security techniques Information security management systems Requirements,2013)



Gambar 2.3 - Model PDCA (Sarno, 2009)

Gambar 2.3 diatas adalah gambar dari model PDCA yang terdapat pada ISO 27001 yang akan dijelaskan pada uraian sebagai berikut :

1. **Plan (penetapan SMKI).**

Menetapkan kebijakan, sasaran, dan prosedur SMKI yang sesuai untuk pengolahan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan. (Nasional, 2009).

2. **Do (Penerapan dan pengoperasian SMKI).**

Menerapkan dan mengoperasikan kebijakan, pengendalian, proses, dan prosedur SMKI yang telah direncanakan pada tahap Plan. (Nasional, 2009)

3. **Check (Pemantauan dan pengkajian SMKI).**

Mengakses dan apabila berlaku mengukur kinerja proses terhadap kebijakan, sasaran, SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian. (Nasional, 2009)

4. **Act (Peningkatan dan pemeliharaan SMKI).**

Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya untuk mencapai perbaikan berkesinambungan dalam SMKI (Nasional, 2009).

2.10.2 Struktur Organisasi ISO/IEC 27001

Struktur organisasi ISO/IEC 27001 dibagi dalam dua bagian sebagaimana yang telah dipaparkan sebagai berikut.

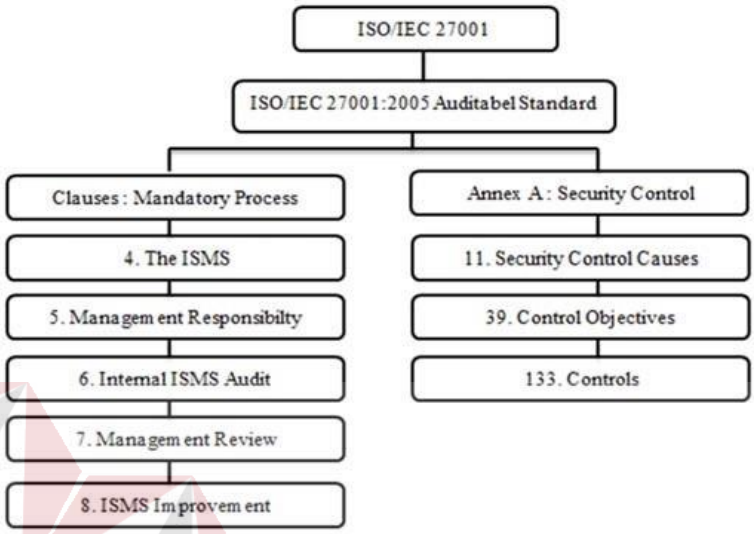
a) Klausul : Mandatory Process

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 2.4 - Struktur Organisasi ISO/IEC 27001 (Sarno, 2009)

2.11 Standar ISO:IEC 27001:2013 Code Of Practice for ISMS

ISO 27001 berisi panduan yang menjelaskan contoh penerapan keamana informasi dengan menggunakan bentuk-bentuk konrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 14 area pengamanan sebagaimana ditetapkan dalam ISO 27001:2013.

ISO 27001:2013 memiliki 14 Klausul, 35 Objektif Kontrol dan 114 Kontrol antara lain :

1. Klausul 5 Information Security Policies
2. Klausul 6 Organization Of Information Security
3. Klausul 7 Human Resource Security
4. Klausul 8 Asset Management

5.	Klausul 9	Access Control
6.	Klausul 10	Cryptography
7.	Klausul 11	Physical And Environmental Security
8.	Klausul 12	Operations Security
9.	Klausul 13	Communication Security
10.	Klausul 14	System Acquisition, Development And Maintenanc
11.	Klausul 15	Supplier Relationships
12.	Klausul 16	Information Security Incident Management
13.	Klausul 17	Information Security Aspects Of Business Continuity Management
14.	Klausul 18	Compliance

2.12 *Standar Operating Procedure* (SOP)

Standar Operating Procedure (SOP) adalah serangkaian instruksi tertulis yang dibakukan (terdokumentasi) mengenai berbagai proses penyelenggaraan administrasi instansi, bagaimana dan kapan harus dilakukan, dimanan dan oleh siapa dilakukan.

Standar Operasional Prosedur merupakan suatu pedoman atau acuan untuk melaksanakan tugas pekerjaan sesuai dengan fungsi dan alat penilaian kinerja instansi pemerintah berdasarkan indikator-indikator teknis, administratif dan prosedural sesuai tata kerja, prosedur kerja dan sistem kerjapada unit kerja yang bersangkutan.

2.12.1 Kriteria dan Format *Standar Operating Procedure* (SOP)

Dalam membuat SOP, diperlukan adanya kriteria dan format yang berfungsi sebagai standarisasi dokumen. Tidak adanya aturan mengenai batasan panjang pendeknya SOP memberikan kemudahan bagi organisasi dalam membuat SOP karena dapat disesuaikan dengan kebutuhan organisasi. Namun, SOP yang ringkas akan memudahkan para pengguna SOP. Penentuan kriteria dan format dalam SOP juga dapat disesuaikan dengan kebutuhan organisasi. Yang perlu diperhatikan dalam penyusunan SOP adalah terdapat langkah-langkah yang jelas, terstruktur dan terperinci. Hilangnya salah satu langkah penting akan menyebabkan penyimpangan dalam menjalankan prosedur. Terdapat tujuh kriteria SOP yang dapat digunakan sebagai acuan, yaitu (Budihardjo, 2016):

1. Spesifik
2. Lengkap
3. Mudah dipahami
4. Mudah diaplikasikan
5. Mudah dikontrol dan diubah
6. Mudah diaudit

2.12.2 Dokumen Standar Operating Procedure (SOP)

Dalam penyusunan dokumen SOP, menurut perturan pemerintah (Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan) didasarkan pada format SOP yang telah disusun. Namun ketidakbakuan format SOP menyebabkan organisasi dapat menyusun dokumen SOP sesuai dengan kebutuhannya masing-masing.

Format SOP dipengaruhi oleh tujuan pembuatan SOP. Sehingga apabila tujuan pembuatan SOP maka format SOP juga dapat berbeda.

Sesuai dengan anatomi dokumen SOP yang pada hakekatnya berisi prosedur-prosedur yang distandarkan dan membentuk satu kesatuan proses, maka informasi yang dimuat dalam dokumen SOP terdiri dari 2 macam unsur, yaitu Unsur Dokumentasi dan Unsur Prosedur. Adapun informasi yang terdapat dalam Unsur Dokumentasi dan Unsur Prosedur adalah:

1. Unsur Dokumentasi

Unsur dokumentasi merupakan unsur dari dokumen SOP yang berisi hal-hal terkait dalam proses pendokumentasian SOP sebagai sebuah dokumen. Adapun unsur dokumen SOP antara lain:

a. Halaman Judul (*Cover*)

Merupakan halaman pertama sebuah dokumen SOP. Halaman judul berisi informasi mengenai:

1) Judul SOP
2) Instansi / Satuan Kerja
3) Tahun pembuatan
4) Informasi lain yang diperlukan

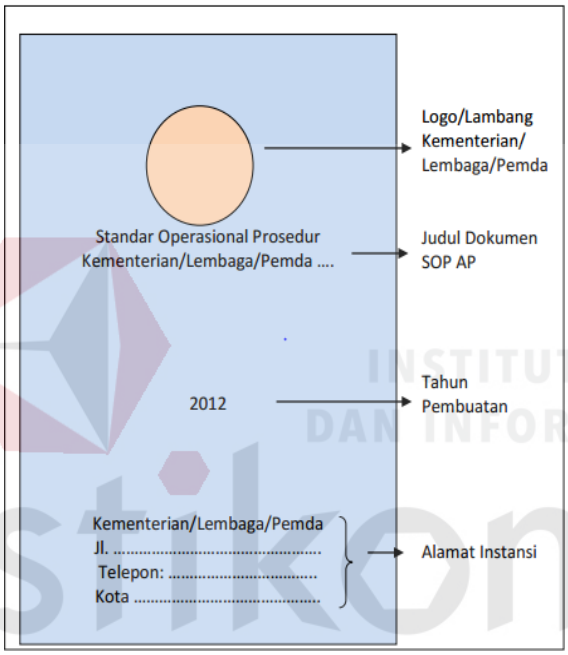
Halaman judul dapat disesuaikan sesuai dengan kebutuhan organisasi. Berikut adalah contoh halaman judul sebuah dokumen SOP yang dapat dilihat pada Gambar 2.5

b. Keputusan Pimpinan Kementrian/ Lembaga/Pemda Setelah halaman judul, maka disajikan keputusan Pimpinan Kementrian/Lembaga/Pemda terkait ketetapan dokumen SOP ini. Hal ini bertujuan sebagai dasar hukum yang berlaku dan sifatnya

adalah mengikat. Selain itu keputusan pimpinan dalam dokumen SOP merupakan pedoman bagi semua pegawai untuk melaksanakan SOP.

c. Daftar isi dokumen SOP

Daftar isi dibutuhkan untuk membantu pencarian informasi secara lebih cepat dan tepat. Selain itu di dalam daftar isi terdapat pula informasi mengenai perubahan / revisi yang dibuat untuk bagian tertentu dari SOP.



Gambar 2.5 - Bagan Penyusunan SOP

(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

d. Penjelasan singkat penggunaan

Sebagai sebuah dokumen yang menjadi manual, maka dokumen SOP hendaknya memuat penjelasan bagaimana membaca dan menggunakan dokumen tersebut. Di dalam bagian ini terdapat informasi mengenai Ruang Lingkup yang berisi penjelasan tujuan pembuatan prosedur, Ringkasan yang berisi ringkasan singkat mengenai prosedur, dan Definisi/Pengertian-pengertian umum yang berisi beberapa

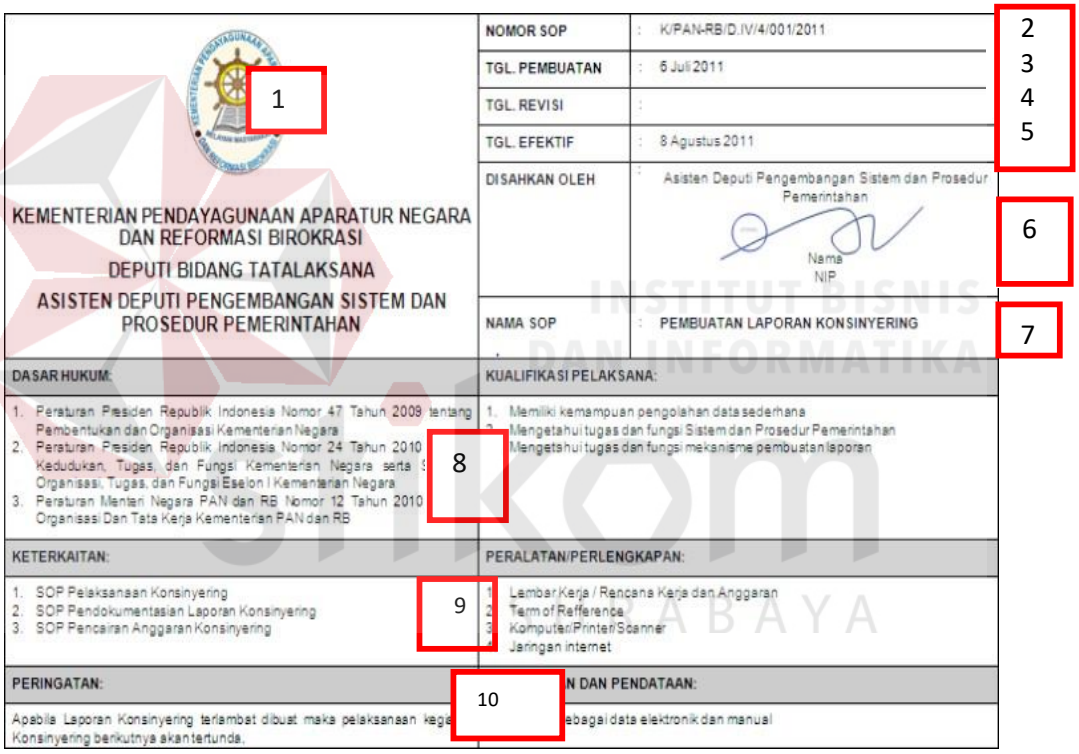
definisi yang terkait dengan prosedur yang distandarkan.

2. Unsur Prosedur

Unsur prosedur merupakan unsur dari dokumen SOP yang berisi hal-hal inti dari dokumen SOP. Unsur prosedur dibagi dalam dua bagian, yaitu Bagian Identitas dan Bagian *Flowchart*. Adapun penjelasan unsur prosedur adalah:

a. Bagian Identitas

Berikut adalah contoh bagian identitas SOP yang dapat dilihat pada Gambar 2.6



Gambar 2.6 - Contoh Bagian SOP

(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

Pada gambar diatas akan dijelaksan penjelasan setiap nomornya pada di dalam bagian identitas berisi hal-hal yang tertulis pada table 2.3.

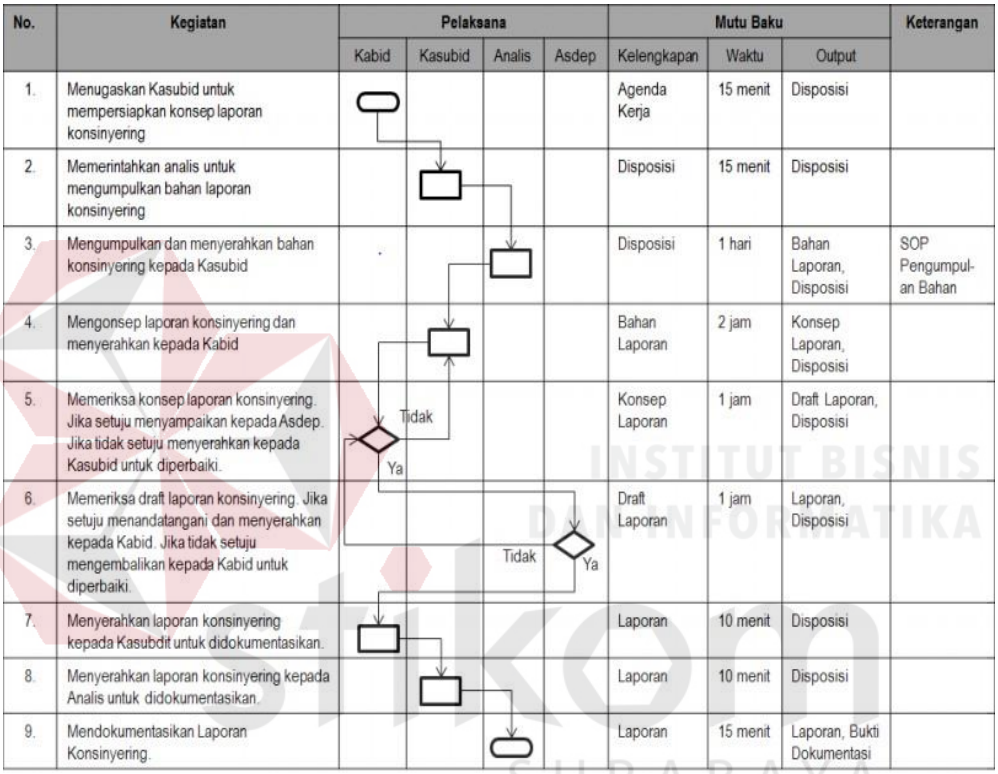
Tabel 2.3 - Penjelasan Identitas SOP
(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

No.	Bagian Identitas	Penjelasan
1.	Logo dan Nama Instansi/ Unit Kerja	Nomenklatur unit organisasi pembuat
2.	Nomor SOP	Nomor prosedur yang di-SOP-kan sesuai dengan tata naskah dinas yang berlaku di Kementerian/Lembaga/Pemda
3.	Tanggal Pembuatan	Tanggal pertama kali SOP dibuat berupa tanggal selesainya SOP dibuat bukan tanggal dimulainya pembuatannya
4.	Tanggal Revisi	Tanggal SOP direvisi atau tanggal rencana ditinjau ulangnya SOP yang bersangkutan
5.	Tanggal Efektif	Tanggal mulai diberlakukan SOP atau sama dengan tanggal ditandantanganinya dokumen SOP
6.	Pengesahan oleh pejabat yang berkompeten pada tingkat satuan kerja	Item pengesahan berisi nomenlektur jabatan, tanda tangan, nama pejabat yang disertai dengan NIP serta stempel/cap instansi
7.	Judul SOP	Judul prosedur yang di-SOP-kan dengan kegiatan yang sesuai dengan tugas dan fungsi yang dimiliki
8.	Dasar Hukum	Berupa peraturan perundang- undangan yang mendasari prosedur yang diSOP-kan berserta aturan pelaksanaannya
9.	Keterkaitan	Penjelasan mengenai keterkaitan prosedu yang distandarkan dengan prosedur lain distandarkan
10.	Peringatan	Penjelasan mengenai kemungkinan-kemungkinan yang terjadi ketika prosedur dilaksanakan atau tidak dilaksanakan

b. Bagian *Flowchart*

Di dalam bagian *flowchart* ini berisi uraian mengenai langkah-langkah (prosedur) kegiatan beserta mutu baku dan keterangan yang diperlukan. Bagian ini

berisi langkah- langkah secara sistematis. Adapun isi bagian ini adalah Nomor kegiatan; Uraian kegiatan yang berisi langkah-langkah : Pelaksana yang merupakan pelaku kegiatan : Mutu baku yang berisi kelengkapan, waktu, output, dan keterangan. Berikut adalah contoh bagian *flowchart* SOP yang dapat dilihat pada gambar 2.7.

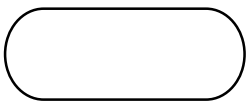


No.	Kegiatan	Pelaksana				Mutu Baku			Keterangan
		Kabid	Kasubid	Analis	Asdep	Kelengkapan	Waktu	Output	
1.	Menugaskan Kasubid untuk mempersiapkan konsep laporan konsinyering					Agenda Kerja	15 menit	Disposisi	
2.	Memerintahkan analis untuk mengumpulkan bahan laporan konsinyering					Disposisi	15 menit	Disposisi	
3.	Mengumpulkan dan menyerahkan bahan konsinyering kepada Kasubid					Disposisi	1 hari	Bahan Laporan, Disposisi	SOP Pengumpul-an Bahan
4.	Mengonsep laporan konsinyering dan menyerahkan kepada Kabid					Bahan Laporan	2 jam	Konsep Laporan, Disposisi	
5.	Memeriksa konsep laporan konsinyering. Jika setuju menyampaikan kepada Asdep. Jika tidak setuju menyerahkan kepada Kasubid untuk diperbaiki.					Konsep Laporan	1 jam	Draft Laporan, Disposisi	
6.	Memeriksa draft laporan konsinyering. Jika setuju menandatangani dan menyerahkan kepada Kabid. Jika tidak setuju mengembalikan kepada Kabid untuk diperbaiki.					Draft Laporan	1 jam	Laporan, Disposisi	
7.	Menyerahkan laporan konsinyering kepada Kasubdit untuk didokumentasikan.					Laporan	10 menit	Disposisi	
8.	Menyerahkan laporan konsinyering kepada Analis untuk didokumentasikan.					Laporan	10 menit	Disposisi	
9.	Mendokumentasikan Laporan Konsinyering.					Laporan	15 menit	Laporan, Bukti Dokumentasi	

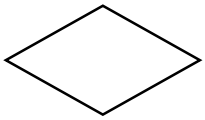
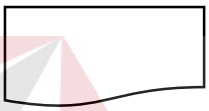
Gambar 2.7 - Contoh Bagian Flowchart SOP
(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

Simbol-simbol pada bagian *flowchart* SOP dapat dilihat pada Tabel 2.4

Tabel 2.4 - Penjelasan Simbol Flowchart SOP
(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

No	Simbol	Nama	Fungsi
1		Terminal	Memulai dan mengakhiri sebuah proses

Tabel 2.4 (Lanjutan)

No	Simbol	Nama	Fungsi
2		Proses	Aktivitas yang dilakukan sebuah fungsi/unit kerja/jabatan , bisa berupa kegiatan atau perhitungan. Proses ini menghasilkan barang, jasa, konsep, dokumen ,saran, dan sebagainya.
3		Keputusan	Menggambarkan proses pengambilan keputusan yang diambiloleh unit / kerja/ jabatan. Hasilnya bisa berupa "Ya" atau "Tidak".
4		Dokumen	Data yang berbentuk informasi, bisa bisa dalam bentuk dokumen tertulis atau file komputer. Bisa merupakan hasil sebuah proses, atau merupakan masukan proses.
5		Penghubung	Penghubung digunakan jika diagram alir tidak dapat ditampung dalam satu bagian atau satu halaman, menunjukkan menyambungan ke bagian lain atau halaman lain.
6		Anak Panah	Menunjukkan arah aliran dari suatu kegiatan ke kegiatan lain, atau menunjukkan arah pilihan yang dapat diambil.

2.13 Panduan Perencanaan Sistem Manajemen Keamanan Informasi

Panduan penyusunan langkah-langkah sistem manajemen keamanan informasi (SMKI) yang difokuskan pada tahap Plan (perencanaan) akan dijelaskan sebagai berikut.

A. Menentukan Ruang Lingkup SMKI adalah menentukan ruang lingkup implementasi SMKI yang akan diterpakan 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, memonitoring, melakukan kajian ulang, memelihara dan mengembangkan SMKI.

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

1) Metode Risk Assessment : Metode yang digunakan untuk melakukan penilaian risiko terhadap informasi dapat dilakukan dengan beberapa metode antara lain : metode statistic atau metode matematis.

2) Kriteria penerimaan risiko : Kriteria penerimaan risiko ditujukan sebagai acuan tindakan yang akan dilakukan dalam menangani risiko yang ada dalam organisasi. (Sarno, 2009). Metode ini menentukan kriteria penerimaan risiko dapat menggunakan tabel matrik 3x3 yang merupakan hubungan variabel berikut :

1) Probabilitas ancaman

2) Biaya pemulihan akibat atau karena dampak dari penerimaan risiko

3) Biaya transfer risiko kepada pihak ketiga

D. Identifikasi Risiko bertujuan untuk memahami seberapa besar dan identifikasi resiko apa yang akan diterima oleh organisasi jika informasi organisasi mendapat ancaman atau gangguan keamananan yang menyebabkan gagalnya penjagaan aspek keamanan informasi. (ISO/IEC, ISO/IEC 27001 Information security management system - Requirements, 2013). Langkah-langkah untuk mengidentifikasi resiko yaitu :

1) Mengidentifikasi aset

   Mengidentifikasi aset dan klasifikasi aset sesuai dengan ruang lingkup dalam SMKI dapat dilakukan dengan menggunakan tabel aset yang telah dikategorikan menurut jenis atau kebutuhan organisasi. (Sarno, 2009).

2) Menghitung nilai aset

   Cara menghitung nilai aset yang dimiliki organisasi berdasarkan aset keamanan informasi yaitu *Confidentiality, Integrity,* dan *Availability* dapat menggunakan contoh tabel penilaian aset berdasarkan kriteria *Confidentiality* yang ditunjukkan pada tabel 2.5. (Sarno, 2009)

Tabel 2.5 - Contoh Penilaian Aset berdasarkan Kriteria Confidentiality

(Sumber: Sarno, 2009)

Kriteria *Confidentiality*	**Nilai *Confidentiality* (NC)**
Public	0
Internal use only	1
Private	2
Confidential	3
Secret	4

Kriteria nilai *Integrity* ditunjukkan pada Tabel 2.6

Tabel 2.6 - Contoh Penilaian Aset berdasarkan Kriteria Integrity

(Sumber: Sarno, 2009)

Kriteria *Integrity*	**Nilai *Integrity* (NI)**
No Impact	0
Minor incident	1
General disturbance	2
Mayor disturbance	3
Uncceptable damage	4

Kriteria nilai *Availability* ditunjukkan pada Tabel 2.7

Tabel 2.7 - Contoh Penilaian Aset berdasarkan Kriteria Availability

(Sumber: Sarno, 2009)

Kriteria *Availability*	**Nilai *Availability* (NV)**
No Availability	0
Office hoursAvailability	1
Strong Availability	2
High Availability	3
Very High Availability	4

Perhitungan nilai aset dapat dihitung dengan enggunakan persamaan matematis berikut :

Nilai Aset (NA)= NC + NI + NV ..... (G.1)

dimana:

NC = Nilai *Confidentialy*

NI = Nilai *Integrity*

NV = Nilai *Availability*

3) Mengidentifikasi ancaman (*threat*) dan kelemahan (*vulnerability*) yang dimiliki oleh aset

Mengidentifikasi ancaman dan kelemahan terhadap aset dapat menggunakan tabel *Probability of Occurance* dengan menentukan rentang nilai probability dari level LOW, MEDIUM, dan HIGH. (Sarno, 2009).

Tabel 2.8 - Contoh Kemungkinan Gangguan Keamanan

(Sumber: Sarno, 2009)

No.	Kejadian	Jenis	Probabilitas	Rerata Probabilitas
1.	Gangguan Sumber daya	Kelemahan	Low	0,1
2.	Gangguan Perangkat kerras	Kelemahan	Medium	0,4
3.	Bencana Alam	Ancaman	Low	0,2
4.	Akses Ilegal	Ancaman	Medium	0,6
5.	Virus Attack	Ancaman	High	0,7

Nilai rerata probabilitas didapatkan dari hasil klasifikasi probabilitas dengan rentang nilai yang dapat didefinisikan sebagai berikut :

1) LOW : nilai rerata probabilitas 0,1-0,3
2) MEDIUM : nilai rerata probabilitas 0,4-0,6
3) HIGH : nilai rerata probabilitas 0,7-1,0

Rumus yang digunakan untuk menghitung nilai ancaman (*threat*) dan kelemahan (*vulnerability*) dari suatu aset yaitu :

Nilai Ancaman (NT) = ∑ PO / ∑ Ancaman ..... (G.2)

dimana :

∑ PO : Jumlah *Probability of Occurance*

∑ Ancaman : Jumlah ancaman terhadap informasi

Tabel 2.9 - Contoh menghitung nilai ancaman

(Sumber: Sarno, 2009)

No.	Ancaman	Jenis	Probabilitas	Rerata Probabilitas
1.	Gangguan Sumber daya	Kelemahan	Low	0,1
2.	Gangguan Perangkat kerras	Kelemahan	Medium	0,4
3.	Bencana Alam	Ancaman	Low	0,2
4.	Akses Ilegal	Ancaman	Medium	0,6
5.	Virus Attack	Ancaman	High	0,7
	∑ Ancaman = 5	**∑ PO**		2,0

Nilai Ancaman (Server) = **∑PO / ∑ Ancaman =** 2,0 / 5 = 0,4

4) Identifikasi dampak (*impact*) jika terjadi kegagalan penjagaan aspek keamanan informasi (CIA) yaitu mengidentifikasi dampak bisnis yang terjadi kegagalan penjagaan terhadap aspek-aspek keamanan informasi. Tujuannya adalah untuk melihat bagaimana dampak terhadap organisasi jika terjadi kegagalan.

E. Analisa dan Evaluasi Risiko

Proses ini bertujuan untuk menganalisa dan mengevaluasi risiko yang sudah di identifikasi pada tahap sebelumnya, untuk memahami bagaimana dampak risiko terhadap bisnis organisasi, bagaimana level risiko yang mungkin timbul dan menetukan apakah risiko yang terjadi lagsung diterima atau masih perlu

dilakukan pengelolaan agar risiko dapat diterima dengan dampak yang bisa ditoleransi. Tahapan melakukan analisa dan evaluasi risiko terdiri dari langkah-langkah berikut:

1) Melakukan analisa dampak bisnis

Analisa dampak bsinis adalah analisa yang menggambarkan seberapa tahan proses bisnis di dalam organisasi berjalan ketika informasi yang dimiliki terganggu dengan menentukan nilai BIA pada masing-masing aset (Sarno, 2009). Skala nilai BIA digunakan untuk menentukan nilai BIA yang ditunjukkan pada tabel 2.10

Tabel 2.2 - Skala Nilai BIA

(Sumber: Sarno, 2009)

Batas Toleransi Gangguan	**Keterangan**	**Nilai BIA**	**Nilai Skala**
< 1 Minggu	*Not Critical*	0	0-20
1 Hari s/d 2 Hari	*Minor Critical*	1	21-40
< 1 Hari	*Mayor Critical*	2	41-60
< 12 Jam	*High Critical*	3	61-80
< 1 Jam	*Very High Critical*	4	81-100

2) Mengidentifikasi level risiko

Level risiko adalah tingkat risiko yang timbul jika dihubungkan dengan dampak dan probabilitas ancaman yang mungkin timbul. Mengidentifikasi level risiko dapat dibuat menggunakan matriks level risiko sesuai dengan menggunakan nilai-nilai probabilitas ancaman yang telah ditentukan. Identifikasi level risiko dapat digambarkan dalam

bentuk matriks level risiko yang ditunjukkan pada tabel 2.11

Tabel 2.11 - Matriks Level Risiko

(Sumber: Sarno, 2009)

Probabilitas Ancaman	Dampak Bisnis				
	Not Critical (20)	**Low Critical (40)**	**Medium Critical (60)**	**High Critical (80)**	**Very High Critical (100)**
Low (0,1)	Low 20x0,1=2	Low 40x0,1=4	Low 60x0,1=6	Low 80x0,1=8	Low 100x0,1=10
Medium (0,5)	Low 20x0,5=10	Medium 40x0,5=20	Medium 60x0,5=30	Medium 80x0,5=40	Medium 100x0,5=50
High (1,0)	Medium 20x1,0=20	Medium 40x1,0=40	High 60x1,0=60	High 80x1,0=80	High 100x1,0=100

3) Menentukan risiko diterima atau perlu pengelolaan risiko adalah penentuan apakah risiko diterima atau masih membutuhkan pengelolaan risiko berdasarkan kriteria penerimaan risiko. Untuk menentukan level risiko diperlukan nilai risiko untuk menentukan letak level dari masing-masing aset yaitu dengan menggunakan perhitungan persamaan matematis berikut:

Nilai Risiko (*Risk Value*) = NA x BIA x NT .....(G.3)

dimana:

NA : Nilai Ast

BIA : Analisa Dampak Bisnis (*Business Impact Analysis*)

NT : Nilai Ancaman (*Nilai Threat*)

F. Identifikasi dan Evaluasi Pilihan Penanganan Risiko

Langkah ini menjelaskan bahwa organisasi harus melakukan identifikasi dan evaluasi pilihan penanganan resiko. Maksud dari langkah ini adalah melakukan kegiatan identifkasi dan menentukan pilihan penanganan resiko jika resiko yang timbul tidak langsung diterima tetapi perlu dikelola lebih

lanjut dengan menggunakan kriteria penerimaan yang telah ditentukan. Pilihan pengelolaan risiko :

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

G. Memilih Objektif Kontrol dan Kontrol 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 akan dikendalikan secara tepat. ISO 27001:2013 mendifinisikan 14 Klausul, 35 Kontrol Objektif dan 114 Kontrol Keamanan yang dapat diterapkan untuk membangun sistem manajemen keamanan informasi (SMKI) ((ISO/IEC, ISO/IEC 27001 Information security management system - Requirements, 2013). Klausul-klausul tersebut antara lain:

1. Klausul 5 : Kebijakan Keamanan Informasi (Information Security Policies)
2. Klausul 6 : Organisasi Keamanan Informasi (Organization of Information Security)
3. Klausul 7 : Keamanan Sumber Daya Manusia (Human Resource Security)
4. Klausul 8 : Manajemen Asset (Asset Management)

5.	Klausul 9	:	Kontrol Akses (Access Control)
6.	Klausul 10	:	Kriptografi (Cryptography)
7.	Klausul 11	:	Keamanan Fisik Dan Lingkungan (Physical and Environmental Security)
8.	Klausul 12	:	Keamanan Operasi (Operations Security)
9.	Klausul 13	:	Keamanan Komunikasi (Communication Security)
10.	Klausul 14	:	Sistem Akuisisi, Pengembangan Dan Pemeliharaan (System Acquisition, Development and Maintenanc)
11.	Klausul 15	:	Manajemen Penyampaian Layanan Pemasok (Supplier Relationships)
12	Klausul 16	:	Informasi Manajemen Insiden Keamanan (Information Security Incident Management)
13.	Klausul 17	:	Aspek Keamanan Informasi Manajemen Kontinuitas Bisnis (Information Security Aspects of Business Continuity Management)
14	Klausul 18	:	Kesesuaian (Compliance)

1. 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 menetukan kontrol keamanan apa yang dibutuhkan secara manajemen, teknikal, dan operasional yang ditunjukkan pada tabel 2.12

Tabel 2.12 - Kebutuhan Kontrol Objektif
(Sumber: Sarno, 2009)

Kategori Kebutuhan	No. Klausul	Klausul	Kontrol Objektif
Manajemen/Organisasi	5	Kebijakan Keamanan	Manajemen Kebijakan Keamanan Informasi
	6	Organisasi Keamanan Informasi	Organisasi Internal Keamanan Informasi
			Perangkat mobile dan teleworking
	8	Manajemen aset	Tanggung jawab aset
			Informasi klasifikasi
			Penanganan media
Teknikal	18	Kesesuaian	Kepatuhan terhadap persyaratan hukum dan kontrak
			Tinjauan keamanan informasi
	7	Keamanan sumber daya manusia	Keamanan SDM sebelum menjadi pegawai
			Keamanan SDM selama menjadi pegawai
			Pemberhentian atau pemindahan pegawai
	9	Kontrol Akses	Persyaratan bisnis pengendalian akses
			Manajemen akses pengguna
			Tanggung jawab pengguna
			Kontrol akses sistem dan aplikasi
	10	Kriptografi	Kontrol kriptografi
	11	Keamanan fisik dan lingkungan	Keamanan area/wilayah
			Keamanan peralatan

Tabel 2.12 (Lanjutan)

Kategori Kebutuhan	No. Klausul	Klausul	Kontrol Objektif
	14	Akuisisi, pengembangan dan pemeliharaan sistem	Persyaratan keamanan sistem informasi
			Keamanan dalam proses pengembangan dan pendukung
			Uji data
Operasional	12	Keamanan operasi	Prosedur dan tanggung jawab operasional
			Proteksi dari malware
			Backup
			Pengembangan dan pemantauan
			Pengendalian perangkat lunak operasional
			Pengelolaan kerentanan teknis
			Pertimbangan audit sistem informasi
	13	Keamanan komunikasi	Manajemen keamanan jaringan
			Transfer informasi
	17	Aspek keamanan informasi manajemen kelangsungan bisnis	keamanan informasi kelangsungan bisnis
	15	Hubungan pemasok	Redudansi
			Keamanan informasi dalam hubungan pemasok
Operasional	16	Manajemen insiden keamanan informasi	Manajemen penyampaian layanan pemasok
			Pengelolaan insiden dan perbaikan keamanan informasi

2.14 SOP (Standar Operational Procedure)

Standart Operational Procedure (SOP) adalah serangkaian instruksi tertulis yang dibakukan (terdokumentasi) mengenai berbagai proses penyelenggaraan administrasi instansi, bagaimana dan kapan harus dilakukan, dimana dan oleh siapa dilakukan. Standar Operasional Prosedur merupakan suatu pedoman atau acuan untuk melaksanakan tugas pekerjaan sesuai dengan fungsi dan alat penilaian kinerja instansi pemerintah berdasarkan indikator. Indikator teknis, administratif dan prosedural sesuai tata kerja, prosedur kerja dan sistem kerja pada unit kerja yang bersangkutan. (Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

2.14.1 Kebijakan SMKI

Kebijakan disusun dengan memperhatikan Objektif kontrol dan Kontrol yang telah dipilih dalam tahap sebelumnya. Seluruh kebijakan yang telah disetujui oleh pimpinan kemudian disosialisasikan kepada seluruh personel/pegawai yang terkait sesuai dengan ruang lingkup yang ditetapkan di atas. Kegiatan ini untuk menjamin bahwa kebijakan terkait SMKI telah dipahami sehingga penerapannya dilakukan secara tepat.

2.14.2 Instruksi Kerja

Instruksi kerja merupakan dokumen yang mengatur secara rinci dan jelas urutan suatu aktifitas yang hanya melibatkan satu fungsi saja sebagai pendukung. Di dalam dokumen instruksi kerja biasanya merinci langkah demi langkah urutan sebuah aktivitas yang bersifat spesifik atau bersifat teknis. (Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

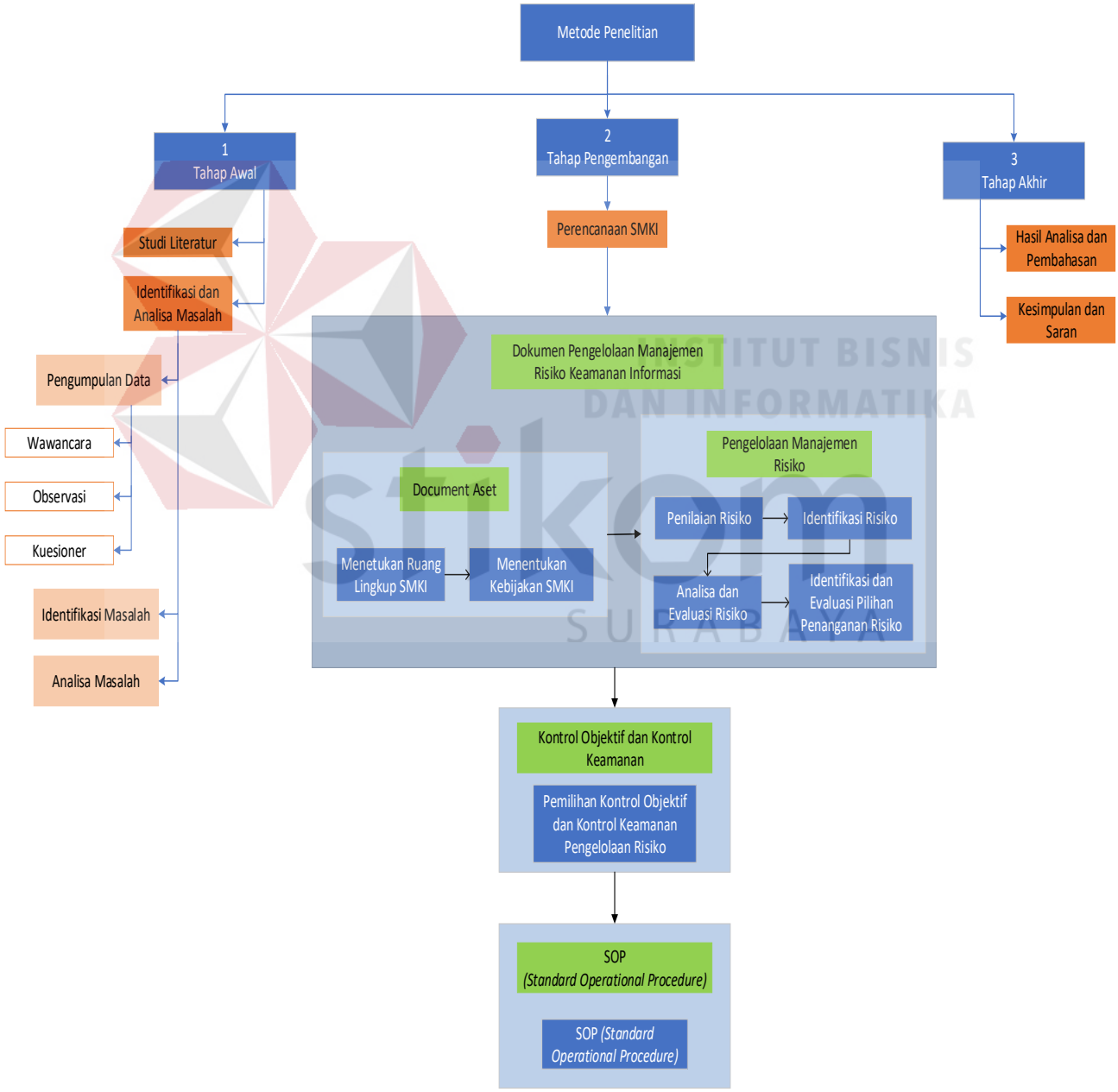
2.14.3 Folmulir

Folmulir merupakan bukti bahwa sistem tata kerja yang tertuang dalam prosedur dan instruksi kerja telah dilaksanakan. Folmulir bertujuan untuk memantau pelaksanaan prosedur dan instruksi kerja. Folmulir dapat berupa lembar kerja, grafik, laporan, dan bentuk-bentuk lain yang dapat diterima oleh organisasi sebagai bukti yang sah. (Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012).

BAB III

METODE PENELITIAN

Pada penelitian ini metode yang akan digunakan terbagi menjadi tiga tahap yaitu tahap awal, tahap pengembangan, dan tahap akhir. Metode penelitian akan dijelaskan lebih detai pada Gambar 3.1.



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 jural terkait dengan topik penelitian, sehinggan nantinya dapat menunjang dalam pengerjaan sistem manajemen keamanan informasi pada Kominfo Jatim.

3.1.2 Identifikasi dan Analisa Masalah

A. Pengumpulan Data

1. Wawancara

Wawancara yang dilakukan pada penelitian ini dengan Bapak Dendy Eka Puspawadi, S.Si selaku kepala seksi keamanan informasi dan persandian, Ibu Tutik Worawari selaku kepala seksi pengelolaan informasi publik pada Kominfo mengenai kebutuhan yang akan 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 struktur organisasi instansi

b. Proses bisnis dalam Seksi Keamanan Informasi dan persandian

c. Tugas pokok dan fungsi setiap Sumber Daya Manusia (SDM)

d. Layanan dan aset informasi yang terdapat pada Seksi Keamanan Informasi dan persandian

e. Risiko yang terjadi pada instansi terkait dengan keamana informasi

2. Observasi

Observasi dilakukan pada proses bisnis dari Seksi Keamanan Informasi dan persandian yang bertujuan untuk mendapatkan data tentang masalah yang akan diselesaikan dan form presensi studi lapangan sehingga diperoleh pemahaman secara langsung dari pengamatan yang dlakukan. Observasi yang dilakukan menghasilkan permasalahan yang terdapat pada Kominfo saat ini. Berikut adalah data-data yang didapat dari hasil observasi yaitu :

a. Penentuan perumusan masalah
b. Pengembangan kajian teori
c. Dokumen Peraturan Gubernur No.80 tahun 2016
d. Data aset informasi
e. Data risiko yang terjadi pada instansi terkait dengan keamana informasi
f. Daftar pertanyaan wawancara dan hasil wawancara
g. Form presensi studi lapangan dan laporan progress penelitian

3. Kuesioner

Kuesioner dilakukan untuk proses pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan tertulis kepada responden untuk dijawabnya, dapat diberikan secara langsung. Jenis angket ada dua, yaitu tertutup dan terbuka. Kuesioner yang digunakan dalam hal ini adalah kuesioner tertutup yakni kuesioner yang sudah disediakan jawabannya, sehingga responden tinggal memilih dan menjawab secara langsung.(Sugiyono, 2008: 142). Kuesioner ini ditujukan kepada bidang aplikasi dan informatika.

B. Identifikasi Masalah

Identifikasi masalah yang terjadi pada Kominfo bertujuan untuk mengetahui permasalahan yang terjadi saat ini dari hasil wawancara dan observasi yang dilakukan. Langkah ini dilakukan mulai dari masukan berupa permasalahan yang ditemukan saat ini, maka diperlukan penggalian data dan referensi mengenai topik yang diambil sesuai dengan penelitian ini.

Identifikasi masalah pada Kominfo yaitu terkait dengan penanganan keamanan informasi tentang Threat (Ancaman) dan Vulnerable (Kelemahan) yang terjadi pada Kominfo yang mempengaruhi Confidentiality (kerahasiaan), Integrity (keutuhan) dan Availability (ketersediaan) yang akan berdampak pada Business Impact Analysis (BIA) pada Kominfo.

C. Analisa Masalah

Analisis Masalah bertujuan untuk memecahkan masalah atau memberikan solusi terhadap pokok permasalahan yang ditemukan, dengan melakukan merinci masalah-masalah yang akan diteliti, mempertegas batasan, serta mempertegas latar belakang dari ancaman dan kelemahan yang ada pada kominfo yang mempengaruhi *Confidentiality* (kerahasiaan), *Integrity* (keutuhan) dan *Availability* (ketersediaan) yang akan berdampak pada *Business Impact Analysis (*BIA*)*. Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi dari sisi CIA adalah dengan penyusunan dokumen pengelolaan risiko terkait dengan keamanan informasi dan pembuatan dokumen SOP (Standar Operational Procedure) dengan tujuan sebagai acuan kerja dan standarisasi Kominfo agar lebih terstruktur dan meningkatkan kualitas keamanana informasi yang ada.

3.2 Tahap Pengembangan

Tahap pengembangan dilakukan sesuai dengan langkah-langkah pada sistem manajemen keamanan informasi yang ada pada standar ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 mengenai tahap perencanaan sistem manajemen keamanan informasi yang akan dijelaskan sebagai berikut:

3.2.1 Dokumen Pengelolaan Majemen Risiko Keamanan Informasi

A. Dokumen Aset

1. Menentukan Ruang Lingkup SMKI

Menentukan ruang lingkup sangat diperlukan untuk pemenuhan dalam tahapan penelitian agar tujuan dokumen yang akan dihasilkan dapat dibuat dengan tepat sesuai dengan kebutuhan permasalahan keamanan informasi instansi. Penentuan Ruang lingkup sistem manajemen keamanan informasi, yang harus dilakukan yaitu :

1. Menidentifikasi masalah eksternal dan internal pada Kominfo yang relevan dengan tujuan dan yang mempengaruhi kemampuan untuk mencapai hasil yang diharapkan dari sistem manjemen keamanan informasi.
2. Identifikasi kondisi eksisting organisasi pada Kominfo, antara lain : karakteristik proses bisnis yang diniliki organisasi, lokasi organisasi, aset-aset yang miliki, teknologi yang digunakan.
3. Menetapkan persyaratan pihak yang berkepentingan. Persyaratan ini mencakup komitmen manajemen (persyaratan hukum, peraturan dan kebijakan)

2. Menentukan Kebijakan SMKI

Menentukan kebijakan SMKI yang akan dibuat dalam penelitian ini meliputi:

1. Dokumen komitmen manajemen Kominfo adalah salah satu inputan dalam pembuatan dokumen ruang lingkup SMKI menjadi inputan juga dalam proses penentujan kebijakan SMKI.
2. Dokumen penyediaan sumber daya yang cukup (sususnan organisasi)

B. Pengelolaan Risiko Keamanan Informasi

1. Penilaian Risiko

Pada tahap ini Penilaian resiko dilakukan untuk mengetahui seberapa besar dan identifikasi resiko apa yang akan diterima oleh Kominfo jika informasi unit mendapat ancaman atau gangguan pada pengamanan informasi, yaitu :

a. Dokumen ruang lingkup menjadi input dari proses penilaian risiko karena dokumen ruang lingkup mementukan sejauh mana identifikasi penilaian risiko yang akan dilakukan
b. Penilaian risiko ini menggunakan metode OCTAVE dengan hitungan matematis dalam analisa penilaian risikonya.
c. Penentuan kriteria penerimaan risiko dengan menggunakan metode matriks 3x3

2. Identifikasi Risiko

Identifikasi risiko ini bertujuan untuk mengetahui seberapa besar risiko yang akan diterima oleh organisasi. Proses identifikasi risiko ini memiliki 4 langkah, yaitu:

a. Langkah 1 : Identifikasi aset dan klasifikasi aset yang ada pada Kominfo dengan menggunakan tabel aset
b. Langkah 2 : Menghitung nilai aset berdasarkan aspek keamanan informasi (*CIA)* dengan memberikan nilai masing-masing, setelah ini dihitung nilai asetnya yaitu dengan menggunakan persamaan matematis berikut :

c. Langkah 3 : Menghitung nilai ancaman dan kelemahan aset
    1) Membuat tabel kemungkinan kejadian atau gangguan keamanan (*Probability of Occurrence)*.
    2) Membuat tabel menghitung nilai ancaman dan menghitung nilai ancaman (NT)
d. Langkah 4 : Identifikasi dampak kegagalan terhadap aspek keamanan informasi (*CIA*) yaitu dengam membuat tabel identifikasi dampak bisnis disertai level dampak yang terjadi.

3. Analisa dan Evaluasi Risiko

Identifikasi risiko ini bertujuan untuk mengetahui seberapa besar risiko yang akan diterima oleh organisasi. Proses identifikasi risiko ini memiliki 3 langkah, yaitu:

a. Langkah 1 : Melakukan Analisa dampak bisnis pada Kominfo yang dilakukan dengan cara pembutan tabel skala nilai *Business Impact Analysis (BIA),* setelah itu dibuat tabel *BIA* sesuai dengan fasilitas informasi yang dimiliki organisasi dengan mengacu pada tabel nilai skala *BIA*.
b. Langkah 2 : Identifikasi level risiko dilakukan dengan membuat tabel matrik level risiko dengan menggunakan nilai probabilitas ancaman dan nilai *BIA*.
c. Langkah 3 : menentukan risiko diterima atau perlunya pengelolaan.

Selanjutanya perlu ditentukan level risikonya dari hasil perhitungan matematis.

4. Identifikasi dan Evaluasi Penanganan Risiko

Pada tahap ini yaitu dilakukan pemilihan penanganan risiko langkah yang harus dilakukan yaitu :

a. Mengidentifikasi atau menentukan pilihan pengelolaan risikonya. Pilihan

pengelolaan risiko : menerina risiko dengan menerapaka kontrol keamanana yang sesuai, menerima risiko dengan menggunakan kriteria risiko yang telah diterapkan, dan menerima risiko dengan men-*transfer* risiko kepada pihak ketiga (Asuransi, vendor, supplier, atau pihak tertentu).

3.2.2 Kontrol Objektif dan Kontrol Keamanan Pengelolaan Risiko

1. Memilih Kontrol Objektif dan Kontrol Keamanan

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

a. Membuat tabel pengisian hasil identifikasi aset yang didapatkan dari penerapan identifikasi risiko.
b. Membutan tabel pengisian identifikasi nilai risiko yang didapatkan dari penilaian risiko informasi.
c. Membutan tabel pengisian nilai risiko yang didapantkan dari hasil penilaian risiko
d. Membuat tabel pemilihan kontrol yang sesuai dengan penilaian risiko informasi. Kemudian berikan penilaian apakah kontrol yang dipilih sudah cukup untuk risiko tersebut
e. Memilih opsi penanganan risiko keamanan informasi yang tepat dengan mempertimbangkan hasil pengelolaan risiko.
f. Menentukan kontrol objektif dan kontrol keamanan yang diperlukan untuk menerapkan opsi-opsi perlakuakn risiko keamanan informasi yang dipilih.

3.2.3 Standart Operational Procedure (SOP)

1. Pembuatan *Standart Operational Procedure* (SOP)

Pada tahap ini dilakukan pembutan Standar Operasional Prosedur (SOP) yang dibuat melalui pemilihan kontrol objektif dan kontrol keamanan dengan identifikasi kebutuhan SOP, lalu dilakukan pembutan SOP dengan hasil dokumen SOP meliputi dokumen kebijakan , instruksi kerja dan folmulir

2. Instruksi Kerja

Instruksi kerja memuat hasil rinci dari prosedur yang telah dibuat sehingga intruksi kerja merupakan dokumen kompleks yang lebih detail dari prosedur.

3. Folmulir

Formulir merupakan bukti atau hasil bahwa prosedur telah dilaksanakan berupa tabel yang harus diisi yang sah.

3.3 Tahap Akhir

Tahap terakhir yang di lakukan adalah menentukan hasil dari proses - proses yang telah dilaksanakan pada tahap pengembangan yang telah dilakukan sebelumnya dan akan menghasilkan keluaran sebagai berikut.

3.3.1 Hasil Analisa dan Pembahasan

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

3.3.2 Kesimpulan dan Saran

Pada tahap ini akan 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

Pada Bab IV ini akan membahas hasil pembuatan Perencanaan Sistem Manajemen Keamanan Informasi berdasarkan Standartd ISO 27001:2013 pada Kominfo Provinsi Jawa Timur. Hasil yang didapatkan dari metode dari tahapan awal, tahap pengembangan, dan tahap akhir adalah sebagai berikut.

4.1 Tahap Awal

4.1.1 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, sehinggan nantinya dapat menunjang dan menjawab tujuan dan permasalahan yang ada terkait dengan topik tersebut. Adapun permasalahan tersebut yang terjadi pada Kominfo dan tujuan yang akan dicapai yaitu penerapan sistem manajemen keamanan informasi pada Kominfo Jatim. Adapun studi literatur yang digunakan dalam proses penyusunan laporan ini sebagai berikut:

a. Konsep keamanan informasi digunakan dalam penyusunan dokumen aset, pengelolaan risiko keamanan informasi, penentuan Kontrol objektif dan kontrol keamanan
b. Konsep pengelolaan risiko keamanan informasi digunakan dalam penyusunan pengelolaan risiko keamanan informasi

c. Penjelasan detail kontrol objektif berdasarka *Secure Online Business* digunakan dalam penentuan pemilihan Kontrol objektif dan kontrol keamanan sesuai dengan penanagannyan secara teknis
d. Sistem manajemen keamanan informasi digunakan dalam proses penyusunan langkah-langkah untuk menentukan Kontrol objektif dan kontrol keamanan
e. Konsep penyusunan SOP digunakan dalam proses penyusunan SOP

4.1.2. Identifikasi dan Analisa Masalah

A. Pengumpulan Data

1. Wawancara

Wawancara yang dilakukan pada penelitian ini dengan Bapak Dendy Eka Puspawadi, S.Si selaku kepala seksi keamanan informasi dan persandian, Ibu Tutik Worawari selaku kepala seksi pengelolaan informasi publik pada Kominfo mengenai kebutuhan yang akan 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. Adapun uraian hasil wawancara adalah sebagi berikut :

a. Tujuan Wawancara

Tujuan wawancara terdapat pada lampiran 2 hasil wawancara yaitu untuk mendapatkan informasi yang tepat dari narasumber yang terpercaya.

b. Visi, misi, tujuan instansi

Berdasarkan informasi yang diperoleh pada tahap wawancara visi, misi, dan tujuan instansi dijelaskan pada lampiran 3 dokumen kepemimpinan, kebijakan dan tupoksi.

c. Tugas, Fungsi dan Struktur organisasi Kominfo Jatim

Fungsional bisnis pada Kominfo Jatim digambarkan dalam sebuah susunan organisasi yang akan dijelaskan pada subbab struktur organisasi dan proses bisnis yang berjalan pada Kominfo Jatim yang akan dijelaskan adalah proses bisnis yang terkait dalam penelitian. Struktur organisasi Kominfo dapat dilihat pada lampiran 3 dokumen kepemimpinan, kebijakan dan tupoksi.

d. Daftar Risiko

Daftar risiko ini adalah catatan atau laporan rekapitulasi kejadian yang pernah terjadi pada Kominfo terdiri dari permasalahan yang terjadi, tindakan yang diberikan, dan sumber laporan kejadian dan saran yang diberikan. Daftar risiko tersebut dapat dilihat pada lampiran 5 daftar risiko.

2. Observasi

Observasi ini dilakukan pada proses bisnis Kominfo yang bertujuan untuk melakukan pengamatan secara langsung di lokasi atau tempat kejadian. Pada tahapan ini keluaran yang akan dihasilkan berupa narasi proses bisnis dan dilengkapi dengan gambar *flowchart* pada lampiran 4 proses bisnis.

a. Proses bisnis Kominfo

1. Layanan kirim berita dinas

Berdasarkan informasi yang diperoleh pada tahap wawancara dijelaskan pada Lampiran proses bisnis (lampiran 4). Layanan kirim berita dinas merupakan proses kirim berita dinas. Aktor pada proses bisnis ini yaitu kepala seksi persandin dan keamanan informasi, petugas sandi/operator, dan petugas administrasi. Alur dimulai dari petugas administrasi menerima berita/radiogram yang akan dikirim, yang akan diperiksa/diteliti dan memberikan klarifikasi berita/radiogram oleh

kepala seksi persandian dan keamanan radiogram, lalu memberikan kode sandi terhadap konsep berita/radiogram sesuai tingkat kerahasiaannya, setelah itu mnegagenda berita/radiogram untuk dikirimkan dan diberi nomor registrasi, lalu melaksanaakan proses pengiriman berita/radiogram yang dilakukan oleh petugas sandi/operator, lalu menerima berita/radiogram yang akan dikirim oleh petugas administrasi.

2. Pembuatan Aplikasi

Pada proses pembuatan aplikasi ini alur flowchat dapat dilihat pada Lampiran proses bisnis (lampiran 4). Pada proses ini terdapat aktor yaitu kepala dinas, kepala bidang aplikasi informatika, kepala seksi pengembangan aplikasi, pihak ketiga, dan pihak yang mengajukan permohonan. Proses pertama yaitu dimulai dari kepala dinas meneyerahkan hasil kajian kebutuhan aplikasi yang akan menerbitkan surat perintah kerja peegrjaan aplikasi kepadapihak pengajuan permohonan aplikasi, setelah itu akan dikoordinasikan kepada pihak ketiga mengenai algoritma dan flowchart program yang akan dikerjakan. Jika koordinasi dan konfirmasi di setujui maka implementasi program akan dibuat , apabila tidak maka koordinasi dan konfirmasi program akan dilakukan ulang. Proses selanjutnya yaitu pelaporan program kerja selama 1 bulan dan pengecekan pengerjaan aplikasi oleh kepala seksi pengembangan aplikasi, selanjutnya program akan dibuat dan di testing dan sesuai atau tidak, jika tidak sesuai maka program akan firevisi dan menyerahakan dokumentasi kepada pihak ketiga dan di cek kembali berbaikan telah sesuai atau tidak. Jika sudah sesuai maka aplikasi siap disajikan dan pengerahan laporan pengerjaan berserta dokumentasi kepada pemohon aplikasi dan pemohon menyerahkan surat pemenuhan kebutuhan apliaksi kepada kepala dinas,

selanjutanya proses maintenace dilaukan oleh pemohon dan proses selesai.

3. Monitoring Rutin Keamanan *Server Hosting*

Pada proses pembuatan aplikasi ini alur flowchat dapat dilihat pada Lampiran proses bisnis (lampiran 4). Pada proses ini terdapat aktor yaitu kepala dinas, kepala bidang aplikasi informatika, kepala seksi keamanan informasi dan staf teknis. Proses pertaman dimulai dari kepaa seksi keamanan informasi melihat penggunaan resource dan hosting server yang paling tinggi, laulu memeriksa direktori berdasarkan URL yang menggunakan resource tinggi dan tidak wajar dan melakukan pencarian unggahan file berdasarkan tanggal tertentu. Apabila terdapat file berbahaya maka proses akan dilakukan konfirmasi dan direspon oleh teknisi terkait dengan akun dan hosting yang perlu dilakukan pengamanan. Jika tidak proses monitoing aplikasi akan selesai.

3. Kuesioner

Kuesioner dilakukan untuk proses pengumpulan data yang dilakukan dengan cara memberi seperangkat pertanyaan tertulis kepada responden untuk dijawabnya, dapat diberikan secara langsung. Jenis kuesionert ada dua, yaitu tertutup dan terbuka. Kuesioner yang digunakan dalam hal ini adalah kuesioner tertutup yakni kuesioner yang sudah disediakan jawabannya, sehingga responden tinggal memilih dan menjawab secara langsung. Kuesioner ini ditujukan kepada bidang aplikasi dan informatika.

B. Identifikasi Masalah

Identifikasi masalah yang terjadi pada Kominfo yaitu dalam identifikasi risiko akan berdasarkan dengan metode OCTAVE. Mengidentifikasi aset penting yang dimiliki organisasi, kebutuhan keamanann organisasi, praktik keamanan

terkini yang telah atau sedang dilakukan tentang *Threat* (Ancaman) dan *Vulnerable* (Kelemahan) yang terjadi pada Kominfo yang mempengaruhi *Confidentiality* (kerahasiaan), *Integrity* (keutuhan) dan *Availability* (ketersediaan) yang akan berdampak pada *Business Impact Analysis (BIA)* pada Kominfo. Aset kritis dan kelemahan inftrastruktur TI yang ada saat ini. Hasil dari identifikasi risiko kemudian akan dilanjutkan pada proses identifikasi pemilik risiko. Hasil luaran dari proses ini adalah sebuah daftar risiko yang dapat dilihat pada lampiran 4. Daftar risiko ini terkait dengan proses layanan kirim berita dinas, layanan pembuatan aplikasi, layanan monitoring rutin keamanan *server hosting*. Daftar risiko tersebut selanjutnya akn menjadi masukan untuk proses analisis masalah. Identifikasi masalah pada Kominfo yaitu terkait dengan penanganan keamanan informasi.

C. Analisa Masalah

Analisis Masalah yang dapat diberikan dari identifikasi masalah pada tabel daftar risiko yang ada pada lampiran 4 yaitu bertujuan untuk memecahkan masalah atau memberikan solusi terhadap pokok permasalahan yang ditemukan terkait dengan keamanan informasi yang mempengaruhi *Confidentiality* (kerahasiaan), *Integrity* (keutuhan) dan *Availability* (ketersediaan) yang akan berdampak pada *Business Impact Analysis* (*BIA*) terkait dengan proses layanan kirim berita dinas, layanan pembuatan aplikasi, layanan monitoring rutin keamanan server hosting. Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi dari sisi CIA adalah dengan penyusunan dokumen pengelolaan risiko terkait dengan keamanan informasi dan pembuatan dokumen SOP (*Standar Operational Procedure*) dengan tujuan sebagai acuan kerja dan standarisasi Kominfo agar lebih terstruktur dan meningkatkan kualitas keamanana

informasi yang ada.

4.2 Tahap Pengembangan

Tahap pengembangan merupakan tahapan inti yang dilakukan pada penelitian tugas akhir ini. Pada sub 4.2 telah menjelaskan proses dari tahap pengembangan yaitu dokumen aset yang berisi penentuan ruang lingkup SMKI dan menentukan kebikajakan SMKI, dokumen pengeolaan risiko keamanan informasi yang berisi penilaian risiko, identifikasi risiko, analisa dan evaluasi risiko, identidikasi dan evaluasi penanganan risiko, dokumen kontrol objektif dan kontrol keamanan meliputi pemilihan kontrol objektif dan kontrol keamanan dan selanjutnya yaitu pembutan *Standart Operational Prosedur (SOP)*.

4.2.1 Dokumen Pengelolaan Manajemen Risiko Kemanan Informasi

A. Dokumen Aset

1. Menentukan Ruang Lingkup SMKI

Penentukan ruang lingkup SMKI dari hasil wawancara dan kesepakatan yang dilakukan dengan Bapak Dendy Eka Puspawadi, S.Si selaku kepala seksi keamanan informasi dan persandian, Ibu Tutik Worawari selaku kepala seksi pengelolaan informasi publik pada Kominfo. Keamanan Teknologi informasi Kominfo berada pada sub direktorat sumber daya manausia teknologi informasi yaitu berada pada bagian Seksi persandian dan keamanan informasi. Seksi persandian dan keamanan informasi memiliki fungsi memyiapkan kebijakan teknis, perencanaan dan pelaksanaan pengelolaan, penanganan, pemulihan, monitoring, evaluasi dan pelaporan persandian dan keamanan informasi merupakan salah satu kriteria utama melakuakan penilaian pada Seksi persandian dan keamanan informasi. Dalam menentukan ruang lingkup SMKI yaitu organisasi harus berkomitmen melindungi

informasi, untuk memenuhi kebutuhan organisasi dalam mengimplementasikan SMKI sesuai standart ISO 27001:2013. SMKI organisasi di implementasika untuk ruang lingkup bisnis organisasi yanitu pada bagain :

a. Bidang aplikasi informatika, Bidang infrastruktur TIK, Bidang pengelolaan data dan statistika dan satuan pengamanan.
b. Proses layanan kirim berita dinas, layanan pembuatan aplikasi, layanan monitoring rutin keamanan server hosting.
c. Aset-aset TI internal organisasi dan jaringan komputer yang digunakan unuk aktifitas bisnis meliputi aset hardware, aset software atau aplikasi, aset infrastrutur, aset data atau informasi, dan SDM.

2. 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.

B. Pengelolaan Risiko Keamanan Informasi

1. Penilaian Risiko

1.1 Metode Penilaian Risiko

Penentuan Penilaian risiko ini dilihat dari identifikasi permasalahan yang ada pada Kominfo dan hasil analisa dari proses layanan kirim berita dinas, layanan pembuatan aplikasi, layanan monitoring rutin keamanan server hosting. Metode yang digunaakan dalam penelitian risiko pada Seksi persandian dan keamanan informasi Kominfo yaitu menggunakan metode *OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation)* dengan menggunakan pendekatana terhadap evaluasi risiko dari tiga aspek keamanan informasi yaitu

confidentiality, integrity, dan availability yang komprehensif, sistematik, terarah, dan dilakukan sendiri dan diselesaian dengan hitungan kuantitatif dengan cara melakukan wawancara, identifikasi, analisa, dan observasi.

2. Identifikasi Risiko

2.1 Identifikasi Aset

Identifikasi aset pada Kominfo bertujuan untuk menentukan aset-aset yang ada yang diguakan utuk mendukung proses bisnis kominfo. Beberapa hasil observasi yang dilakukan dapat digolongkan menjadi beberapa jenis aset yaitu aset hardware, software atau aplikasi, aset infrastrutur/jaringan, aset data atau informasi dan SDM.

Tabel 4.1 - Aset Organisasi

No.	Kategori Aset	Daftar Aset
1.	Hardware	Server
		PC
		Camera CCTV
		Printer
		IP Telpon
		Scanner
		LCD Proyektor
		Mesin Shredder
2.	Software	Sistem informasi Presensi
		Sistem Informasi *e-government*
		Sistem Informasi Pengajuan Permohonan
3.	Jaringan	Wifi
		Router
		Switch
		Kabel
4.	Data	Data *center*

Tabel 4.1 (Lanjutan)

No.	Kategori Aset	Daftar Aset
		Data Presensi pegawai
		Data Kepegawaian
		Data Keuangan
		Data Pelayanan dan Pengajuan Permohonan
		Data Aset
5.	Sumber Daya Manusia/SDM	Pegawai
		Satuan Pengamanan

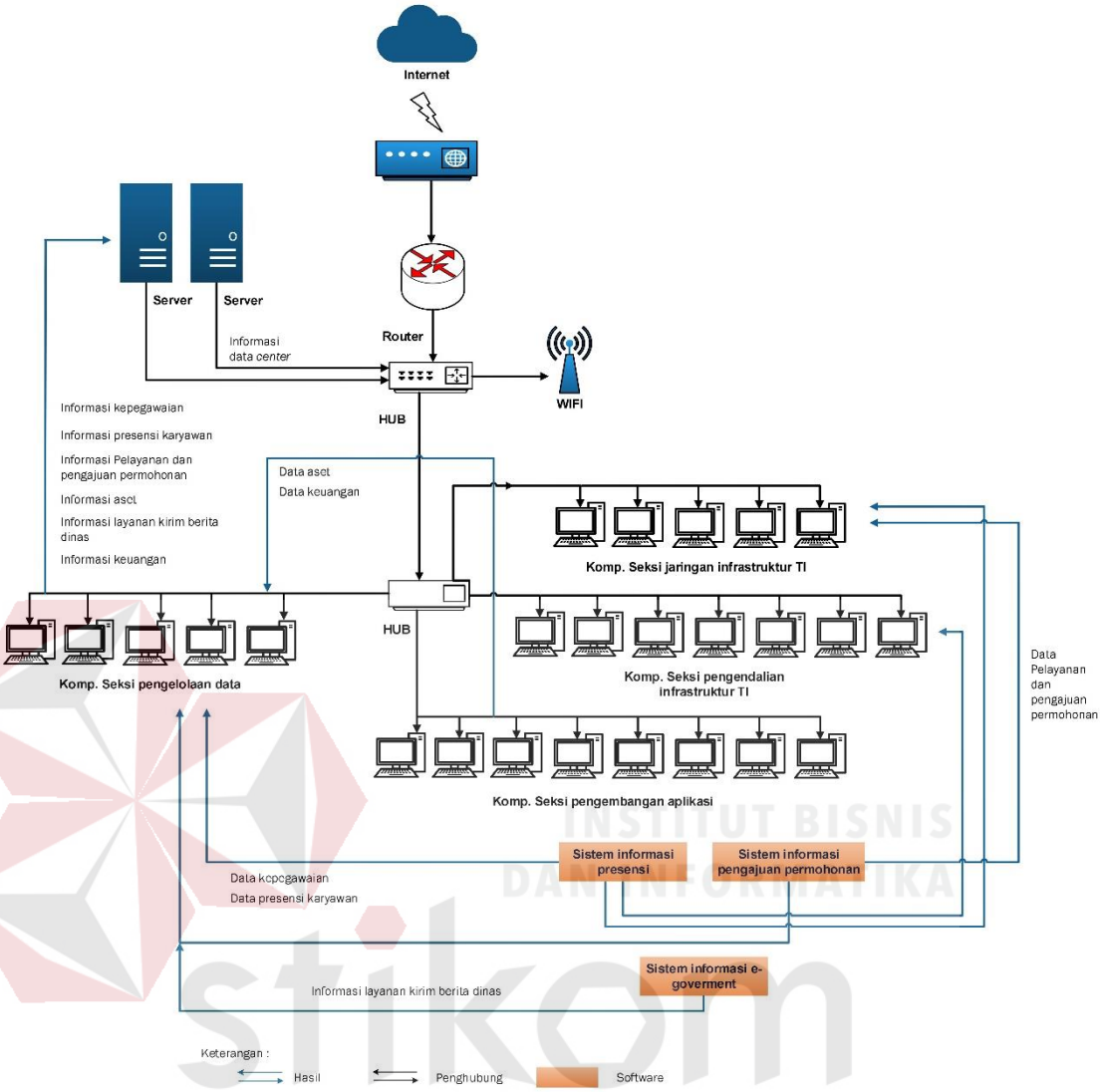
Dari hasil observasi akan dianalisa kembali dalam menghasilkan aset informasi kritis yang akan digunakan dalam proses penelitian selanjutnya.

2.2 Identifikasi *Flow of Information*

Flow of Information (arus informasi) yang ada pada aset kominfo dari hardware, software, jaringan, data, dan SDM untuk dapat menentukan letak aset yang ada pada kominfo dapat dilihat pada gambar 4.1.

1.2.1 Identifikasi Aset Kritis

Identifikasi penentuan aset kritis ditentuan berdasarkan gangguan atau ancaman pada aset instansi yang mengalami hambatan dalam operasional. Daftar aset kritis dapat dijelaskan pada tabel 4.2.



Gambar 4.1 - Identifikasi *Flow of Information*

1.2.2 Identifikasi Aset Kritis

Identifikasi penentuan aset kritis ditentuan berdasarkan gangguan atau ancaman pada aset instansi yang mengalami hambatan dalam operasional. Daftar aset kritis dapat dijelaskan pada tabel 4.2.

Tabel 4.2 – Daftar Aset Kritis

No.	Kategori Aset	Daftar Aset	Alasan/Sebab
1.	Hardware	Server	Server bertujuan untuk memastikan data dan sistem selalu dapat diakses setiap saat
		PC	Komputer juga digunakan untuk proses operasional dan juga sebagai media untuk mengakses data PC
2.	Software	Sistem Informasi Presensi	Sistem Informasi Presensi bertujuan untuk mengetahui daftar kehadiran pegawai
		Sistem Informasi *e-government*	Sistem Informasi *e-government* yaitu bertujuan untuk memberikan informasi mulai dari urusan bisnis atau hal-hal lain yang berkenaan dengan urusan pemerintahan.
		Sistem Informasi Pengajuan Permohonan	Sistem Informasi Pengajuan Permohonan bertujuan untuk proses awal pengajuan permohonan kepada kominfo baik internal maupun eksternal dalam memberikan pelayanan
3.	Jaringan	Wifi	Jaringan digunakan untuk mengakses informasi, seperti mengakses database dan mengakses internet
		Router	
		Switch	
		Kabel	
4.	Data	Data *center*	Seluruh data sangat penting bagi

Tabel 4.2 (Lanjutan)

No.	Kategori Aset	Daftar Aset	Alasan/Sebab
		Data Presensi Pegawai	instansi karena terkait dengan keberlangsungan proses bisnis instansi sehingga keamanan dari setiap data sangat penting
		Data Kepegawaian	
		Data Keuangan	
		Data Pelayanan dan Pengajuan Permohonan	
		Data Aset	
5.	Sumber Daya Manusia/SDM	Pegawai	Suatu aset yang penting dalam sebuah organisasi karena SDM yang memiliki kompetensi dapat mendukung proses bisnis berjalan dengan lancar.
		Satuan Pengamanan	

3.1.1 Identifikasi Ancaman dan Kelemahan

Identifikasi ancaman dan kelemahan pada aset kritis dikategorikan kedalam hardware, software, jaringan atau infrastruktur, data atau informasi dan SDM pada proses layanan kirim berita dinas, layanan pembuatan aplikasi, layanan monitoring rutin keamanan server hosting. Daftar ancaman dan kelemahan berikut ini didapatkan dari hasil wawancara dan observasi kepada narasumber pada tabel 4.3.

Tabel 4.3 - Daftar Ancaman dan Kelemahan Aset

No.	Kategori Aset	Daftar Aset	Ancaman dan Kelemahan
1.	Hardware	Server	- Bencana alam - Kehilangan data - Krusakan server - Pencurian komponen server - Kesalahan konfigurasi

Tabel 4.3 (Lanjutan)

No.	Kategori Aset	Daftar Aset	Ancaman dan Kelemahan
			hardware - Akses ilegal - Server mati - Server down
		PC	- Bencana alam - PC rusak - Kehilangan data - Kerusakan komponen PC - Pencurian komponen hadware - Akes ilegal - Kesalahan konfigurasi hardware
2.	Software	Sistem Informasi Presensi Sistem Informasi *e-government* Sistem Informasi Pengajuan Permohonan	- Bug pada aplikasi/sistem tidak berjalan dengan nornal - Serangan virus - Kesalahan konfigurasi dan input data pada sistem - Pembobolan sistem/akses ilegal - Sistem tidak dapat diakses
3.	Jaringan	Wifi Router Switch Kabel	- Akses ilegal - Monolopy bandwitch - Seranga virus - Service down - Kerusakan hardware - Gangguan router - Hilangnya kompone hardware - Pembobolan jaringan
4.	Data	Data *center* Data Presensi Pegawai	- Kesalahan input data - Manipulasi data

Tabel 4.3 (Lanjutan)

No.	Kategori Aset	Daftar Aset	Ancaman dan Kelemahan
		Data Kepegawaian	- Data hilang - Pencurian data - Data tidak dapat diakses - Data corrupt/rusak - Pencurian data - Akses ilegal
		Data Keuangan	
		Data Pelayanan dan Pengajuan Permohonan	
		Data Aset	
5.	Sumber Daya Manusia/SDM	Pegawai	- Penyalahgunaan data organisasi - Penyalahgunaan hak akses - Data tidak sesuai - Password shared
		Satuan Pengamanan	Tidak melakukan monitoring keamanan

3.1.2 Identifikasi Kerentanan

Identifikasi kerentanan adalah kemungkinan ancaman yang muncul pada aset-aset yang mendukung jalannya proses bisnis yang ada. Pada tabel 4.4 berikut merupakan daftar kerentanan pada teknologi yang dibagi kedalam masing-masing aset kritis.

Tabel 4.4 - Daftar Kerentanan pada Teknologi

Server	
System of Interest	Server pada instansi
Komponen Utama	**Kemungkinan Ancaman**
• Sistem Operasi • Processor • RAM • Harddisk • Listrik	• Tidak mendapatkan aliran listrik karena terjadi pmadaman listrik • Genset tidak dapat berfungsi karena mengalami kerusakan • RAM mengalami kelebihan memori

Tabel 4.4 (Lanjutan)

Server	
System of Interest	Server pada instansi
Komponen Utama	**Kemungkinan Ancaman**
• Keamanan Jaringan • Genset • UPS • Kabel • Pendingin ruangan • Ruang *Server*	• Kinerja Procesor menurun akibat terlalu banyak kapasitas data • Tempat penyimpanan (Harddisk) penuh • Keamanan jaringan dapat ditembus • UPS tidak berfungsi • Ruang Server kurang diberi pengamanan • Komponen dicuri karena kelalaian pihak keamanan
PC	
System of Interest	PC yang ada pada instansi
Komponen Utama	**Kemungkinan Ancaman**
• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • Antivirus • Sistem Operasi • *Software* • Listrik • UPS • Genset • Firewall	• Monitor, Keyboard ataupun mouse mengalami kerusakan • Firewall ditembus oleh bagian yang tidak berwenang • Kabel LAN putus akibat hewan pengerat • Tidak mendapatkan aliran listrik karena terjadi pemadaman pada PLN • UPS tidak berfungsi • Virus yang menyerang tidak dapat tertangani oleh antivirus • Komponen di curi karena kelalaian pihak keamanan
Data	
System of Interest	Seluruh data yang dimiliki instansi
Komponen Utama	**Kemungkinan Ancaman**

Tabel 4.4 (Lanjutan)

Data	
System of Interest	Seluruh data yang dimiliki instansi
Komponen Utama	**Kemungkinan Ancaman**
• Database • Server • Listrik • PC • Firewall • Database Teknisi	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Firewall ditembus oleh bagian yang tidak berwenang • PC berhenti beroperasi karena terserang virus • Database Admnistrator salah dalah melakukan pengolahan data (ubah dan hapus) • Data dicuri karena Database Teknisi kurang melakukan kontrol keamanan
Perangkat Lunak	
System of Interest	Sistem informasi keuangan, system informasi administrasi, sistem pendataan dan penjadwalan, Sistem pemasaran
Komponen Utama	**Kemungkinan Ancaman**
• Firewall • Server • Antivirus	• Firewall ditembus oleh bagian yang tidak berwenang • Virus yang menyerang tidak dapat tertangani oleh antivirus • Server mengalami kerusakan sehingga sistem tidak dapat diakses
Wifi	
System of Interest	wifi yang terpasang semua berada dalam 1 kantor
Komponen Utama	**Kemungkinan Ancaman**
• Listrik • Kabel • Keamanan Jaringan	• Tidak mendapatkan aliran listrik karena terjadi pemadaman • Kabel rusak akibat gigitan hewan • Keamanan jaringan dapat ditembus oleh pihak yang tidak berwenang
Router	
System of Interest	4 Router pada kantor Kominfo

Tabel 4.4 (Lanjutan)

Router	
System of Interest	4 Router pada kantor Kominfo
Komponen Utama	**Kemungkinan Ancaman**
• Listrik • Kabel • Keamanan Jaringan	• Tidak mendapatkan aliran listrik karena terjadi pemadaman • Kabel rusak akibat digigit hewan pengerat • Komponen dicuri karena kelalaian pihak keamanan

3.2 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 tabel 4.5

Tabel 4.5 - Menghitung Nilai Aset

No	Kategori Aset	Daftar Aset	Kriteria			Nilai Aset (NC+NI+NV)
			Nilai Confidentiality (NC)	Nilai Integrity (NI)	Nilai Availability (NV)	
1.	Hardware	Server	4	4	3	11
		PC	3	3	3	9
2.	Software	Sistem Informasi Presensi	3	3	3	9
		Sistem Informasi *e-government*	3	3	3	9
		Sistem Informasi Pengajuan Permohonan	3	3	4	10
3.	Jaringan	Wifi	2	2	3	7

Tabel 4.5 (Lanjutan)

No	Kategori Aset	Daftar Aset	Kriteria			Nilai Aset (NC+NI+NV)
			Nilai Confidentiality (NC)	Nilai Integrity (NI)	Nilai Availability (NV)	
		Router dan Switch	3	3	3	9
		Kabel	2	3	3	8
4.	Data	Data *center*	4	4	3	11
		Data Presensi Pegawai	3	3	3	9
		Data Kepegawaian	4	4	3	11
		Data Keuangan	4	4	4	12
		Data Pelayanan dan Pengajuan Permohonan	3	3	3	9
		Data Aset	3	2	2	7
5.	SDM	Pegawai	4	3	3	10
		Satuan Pengamanan	3	3	3	9

3.3 Identifikasi nilai ancaman (*threat*) dan kelemahan (*vulnerability*)

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

2.3.1 Menetukan Kemungkinan (*Probability*)

Tujuan menentukan kemungkinan ancaman yang timbul sesuai dengan

identifikasi ancaman dan kelemahan. Penentuan kemungkinan (*Probability*) berdasarkan historiskejadian ancaman sebelumnya, atau ditentukan berdasarkan pengamatan kondisi yang dinilai. Penilaian identifikasi ancaman, kelemahan, dan *probability* dapat dilihat pada tabel 4.6

1. Penilaian Identifikasi ancaman dan kelemahan

Tabel 4.6 - Penilaian ancaman, kelemahan, dan probabilitas pada Server

Nama Aset	Server		
Jenis Aset	Hardware		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Bencana alam	Threat	Low	0,3
Kehilangan data	Vulnerable	Medium	0,6
Kerusakan server	Threat	Medium	0,4
Pencurian komponen server	Threat	Medium	0,4
Kesalahan konfigurasi server	Vulnerable	Medium	0,5
Akses ilegal	Threat	Medium	0,5
Server mati/down	Threat	Low	0,3
Serangan virus	Vulnerable	High	0,7
Jumlah Ancamanan = 8	**Jumlah rata-rata probabilitas**		**3,7**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,7 / 8 = 0,46**		

Identifikasi pada aset Server memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,7 dan nilai ancamannya adalah 0,46. Identifikasi ancaman, kelemahan, dan probabilitas pada PC dapat dilihat pada Tabel 4.7

Tabel 4.7 - Penilaian ancaman, kelemahan, dan probabilitas pada PC

Nama Aset	PC		
Jenis Aset	Hardware		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Bencana alam	Threat	Low	0,2
PC rusak	Threat	Medium	0,5
Kehilangan data	Threat	High	0,7
Kerusakan komponen PC	Vulnerable	Medium	0,5
Pencurian komponen hadware	Vulnerable	Low	0,3
Akes ilegal	Threat	High	0,8
Kesalahan konfigurasi hardware	Vulnerable	High	0,7
Jumlah Ancamanan = 7	**Jumlah rata-rata probabilitas**		**3,7**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,7 /7 = 0,5**		

Identifikasi pada aset PC memiliki 7 ancaman, dengan jumlah rata-rata probabilitasnya 3,7 dan nilai ancamannya adalah 0,5. Identifikasi ancaman, kelemahan, dan probabilitas pada Sistem Informasi Presensi (software) dapat dilihat pada Tabel 4.8

Tabel 4.8 - Penilaian ancaman, kelemahan, dan probabilitas pada SIP

Nama Aset	Sistem Informasi Presensi		
Jenis Aset	Software		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Bug pada aplikasi/sistem tidak berjalan dengan normal	Vulnerable	Low	0,3

Tabel 4.8 (Lanjutan)

Nama Aset	Sistem Informasi Presensi		
Jenis Aset	Software		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Serangan virus	Threat	Medium	0,5
Kesalahan konfigurasi dan input data pada sistem	Vulnerable	Medium	0,6
Pembobolan sistem/akses ilegal	Threat	High	0,7
Sistem tidak dapat diakses	Vulnerable	Madium	0,5
Jumlah Ancamanan = 5	**Jumlah rata-rata probabilitas**		**2,6**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 2,6 /5 = 0,52**		

Identifikasi pada aset sistem informasi presensi memiliki 5 ancaman, dengan jumlah rata-rata probabilitasnya 2,6 dan nilai ancamannya adalah 0,52. Identifikasi ancaman, kelemahan, dan probabilitas pada Sistem Informasi *e-goverment* (software) dapat dilihat pada Tabel 4.9

Tabel 4.9 - Penilaian ancaman, kelemahan, dan probabilitas pada SI e-gov

Nama Aset	Sistem Informasi *e-goverment*		
Jenis Aset	Software		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Bug pada aplikasi/sistem tidak berjalan dengan normal	Vulnerable	Low	0,3
Serangan virus	Threat	Medium	0,4

Tabe 4.9 (Lanjutan)

Nama Aset	Sistem Informasi *e-goverment*		
Jenis Aset	Software		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Kesalahan konfigurasi dan input data pada sistem	Vulnerable	Medium	0,4
Pembobolan sistem/akses ilegal	Threat	Medium	0,5
Sistem tidak dapat diakses	Vulnerable	High	0,7
Jumlah Ancamanan = 5	**Jumlah rata-rata probabilitas**		**2,3**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 2,3 /5 = 0,46**		

Identifikasi pada aset sistem informasi presensi memiliki 5 ancaman, dengan jumlah rata-rata probabilitasnya 2,3 dan nilai ancamannya adalah 0,46. Identifikasi ancaman, kelemahan, dan probabilitas pada Sistem Informasi Pengajuan Permohonan (software) dapat dilihat pada Tabel 4.10

Tabel 4.10 - Penilaian ancaman, kelemahan, dan probabilitas pada PP Software

Nama Aset	Sistem Informasi Pengajuan Permohonan		
Jenis Aset	Software		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Bug pada aplikasi/sistem tidak berjalan dengan nornal	Vulnerable	Low	0,3
Serangan virus	Threat	Medium	0,4
Kesalahan konfigurasi dan input data pada sistem	Vulnerable	Medium	0,4
Pembobolan sistem/akses ilegal	Threat	High	0,7
Sistem tidak dapat diakses	Vulnerable	Medium	0,6

Tabel 4.10 (Lanjutan)

Nama Aset	Sistem Informasi Pengajuan Permohonan		
Jenis Aset	Software		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Jumlah Ancamanan = 5	**Jumlah rata-rata probabilitas**		**2,4**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 2,4/5 = 0,48**		

Identifikasi pada aset sistem informasi presensi memiliki 5 ancaman, dengan jumlah rata-rata probabilitasnya 2,4 dan nilai ancamannya adalah 0,48. Identifikasi ancaman, kelemahan, dan probabilitas pada wifi (jaringan)dapat dilihat pada Tabel 4.11

Tabel 4.11 - Penilaian ancaman, kelemahan, dan probabilitas pada Wifi

Nama Aset	Wifi		
Jenis Aset	Jaringan		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Akses ilegal	Threat	High	0,7
Monolopy bandwitch	Vulnerable	High	0,8
Serangan virus	Threat	Medium	0,5
Kerusakan hardware	Vulnerable	Medium	0,4
Gangguan wifi	Vulnerable	Medium	0,4
Hilangnya kompone hardware	Vulnerable	Medium	0,4
Pembobolan jaringan	Threat	High	0,7
Jumlah Ancamanan = 7	**Jumlah rata-rata probabilitas**		**3,9**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,9 /7 = 0,56**		

Identifikasi pada aset sistem informasi presensi memiliki 7 ancaman, dengan jumlah rata-rata probabilitasnya 3,9 dan nilai ancamannya adalah 0,56.

Identifikasi ancaman, kelemahan, dan probabilitas pada Router dan Switch (jaringan) dapat dilihat pada Tabel 4.12

Tabel 4.12 - Penilaian ancaman, kelemahan, dan probabilitas pada Router Switch

Nama Aset	Router dan Switch		
Jenis Aset	Jaringan		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Akses ilegal	Threat	Medium	0,6
Monolopy bandwitch	Vulnerable	High	0,7
Serangan virus	Threat	Medium	0,5
Kerusakan hardware	Vulnerable	Medium	0,4
Gangguan router	Vulnerable	Medium	0,4
Hilangnya kompone hardware	Vulnerable	Medium	0,4
Pembobolan jaringan	Threat	High	0,7
Jumlah Ancamanan = 7	**Jumlah rata-rata probabilitas**		**3,7**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,7 /7 = 0,53**		

Identifikasi pada aset sistem informasi presensi memiliki 7 ancaman, dengan jumlah rata-rata probabilitasnya 3,7 dan nilai ancamannya adalah 0,53. Identifikasi ancaman, kelemahan, dan probabilitas pada kabel (jaringan) dapat dilihat pada Tabel 4.13

Tabel 4.13 - Penilaian ancaman, kelemahan, dan probabilitas pada kabel jaringan

Nama Aset	Kabel		
Jenis Aset	Jaringan		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Kerusakan hardware	Vulnerable	Medium	0,4
Gangguan kabel	Vulnerable	Medium	0,4
Hilangnya komponen	Vulnerable	Low	0,3

Tabel 4.13 (Lanjutan)

hardware			
Jumlah Ancamanan = 3	**Jumlah rata-rata probabilitas**		**1,1**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 1,1 /3 = 0,37**		

Identifikasi pada aset sistem informasi presensi memiliki 3 ancaman, dengan jumlah rata-rata probabilitasnya 1,1 dan nilai ancamannya adalah 0,37. Identifikasi ancaman, kelemahan, dan probabilitas pada Data *center* (data) dapat dilihat pada Tabel 4.14

Tabel 4 14 - Penilaian ancaman, kelemahan, dan probabilitas pada data center

Nama Aset	Data *Center*		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Kesalahan input data	Vulnerable	Medium	0,4
Manipulasi data	Threat	High	0,7
Data hilang	Threat	Medium	0,4
Pencurian data	Threat	High	0,7
Data tidak dapat diakses	Vulnerable	Medium	0,4
Data corrupt/rusak	Vulnerable	Low	0,3
Serangan virus	Threat	Medium	0,4
Akses ilegal	Threat	Medium	0,5
Jumlah Ancamanan = 8	**Jumlah rata-rata probabilitas**		**3,8**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,8 /8 = 0,48**		

Identifikasi pada aset sistem informasi presensi memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,8 dan nilai ancamannya adalah 0,48. Identifikasi ancaman, kelemahan, dan probabilitas pada Data presensi pegawai (data) dapat dilihat pada Tabel 4.15

Tabel 4.15 - Penilaian ancaman, kelemahan, dan probabilitas pada D.Presensi Pegawai

Nama Aset	Data Presensi pegawai		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Kesalahan input data	Vulnerable	Low	0,3
Manipulasi data	Threat	Low	0,3
Data hilang	Threat	Medium	0,4
Pencurian data	Threat	Medium	0,4
Data tidak dapat diakses	Vulnerable	High	0,7
Data corrupt/rusak	Vulnerable	Medium	0,4
Serangan virus	Threat	Medium	0,4
Akses ilegal	Threat	High	0,7
Jumlah Ancamanan = 8	**Jumlah rata-rata probabilitas**		**3,6**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,6 /8 = 0,45**		

Identifikasi pada aset sistem informasi presensi memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,6 dan nilai ancamannya adalah 0,45. Identifikasi ancaman, kelemahan, dan probabilitas pada Data Kepegawaian (data) dapat dilihat pada Tabel 4.16

Tabel 4.16 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Pegawai

Nama Aset	Data Pegawai		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Kesalahan input data	Vulnerable	Medium	0,4
Manipulasi data	Threat	Medium	0,4
Data hilang	Threat	Medium	0,4
Pencurian data	Threat	Medium	0,5
Data tidak dapat diakses	Vulnerable	Low	0,3
Data corrupt/rusak	Vulnerable	Low	0,3
Serangan virus	Threat	Low	0,3
Akses ilegal	Threat	High	0,7
Jumlah Ancamanan = 8	**Jumlah rata-rata probabilitas**		**3,3**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,3 /8 = 0,41**		

Identifikasi pada aset sistem informasi presensi memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,3 dan nilai ancamannya adalah 0,41. Identifikasi ancaman, kelemahan, dan probabilitas pada Data Keuangan (data) dapat dilihat pada Tabel 4.17

Tabel 4.17 - Penilaian ancaman, kelemahan, dan probabilitas pada data keungan

Nama Aset	Data Keuangan		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Kesalahan input data	Vulnerable	Low	0,3
Manipulasi data	Threat	Medium	0,4
Data hilang	Threat	Low	0,4
Pencurian data	Threat	Medium	0,4

Tabel 4.17 (Lanjutan)

Nama Aset	Data Keuangan		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Data tidak dapat diakses	Vulnerable	Low	0,6
Data corrupt/rusak	Vulnerable	Low	0,3
Serangan virus	Threat	Medium	0,6
Akses ilegal	Threat	Medium	0,6
Jumlah Ancamanan = 8	**Jumlah rata-rata probabilitas**		**3,6**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,6 /8 = 0,45**		

Identifikasi pada aset sistem informasi presensi memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,6 dan nilai ancamannya adalah 0,45. Identifikasi ancaman, kelemahan, dan probabilitas pada Data Pelayanan dan Pengajuan Permohonan (data) dapat dilihat pada Tabel 4.18

Tabel 4.18 - Penilaian ancaman, kelemahan, dan probabilitas pada Data PPP

Nama Aset	Data Pelayanan dan Pengajuan Permohonan		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Kesalahan input data	Vulnerable	Medium	0,4
Manipulasi data	Threat	Medium	0,5
Data hilang	Threat	Medium	0,4
Pencurian data	Threat	Medium	0,4
Data tidak dapat diakses	Vulnerable	Low	0,3
Data corrupt/rusak	Vulnerable	Low	0,3
Serangan virus	Threat	Medium	0,5
Akses ilegal	Threat	High	0,7
Jumlah Ancamanan = 8	**Jumlah rata-rata probabilitas**		**3,5**

Tabel 4.18 (Lanjutan)

Nama Aset	Data Pelayanan dan Pengajuan Permohonan		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 3,5 /8 = 0,44**		

Identifikasi pada aset sistem informasi presensi memiliki 8 ancaman, dengan jumlah rata-rata probabilitasnya 3,5 dan nilai ancamannya adalah 0,44. Identifikasi ancaman, kelemahan, dan probabilitas pada Data aset (data) dapat dilihat pada Tabel 4.19

Tabel 4.19 - Penilaian ancaman, kelemahan, dan probabilitas pada Data Aset

Nama Aset	Data Aset		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	**Probability**	**Rata-rata Probability**
Kesalahan input data	Vulnerable	High	0,7
Manipulasi data	Threat	Medium	0,6
Data hilang	Threat	Medium	0.4
Pencurian data	Threat	Medium	0,5
Data tidak dapat diakses	Vulnerable	Medium	0,4
Data corrupt/rusak	Vulnerable	Medium	0,4
Serangan virus	Threat	High	0,7
Akses ilegal	Threat	High	0,7
Jumlah Ancamanan = 8	**Jumlah rata-rata probabilitas**		**4,4**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 4,4 /8 = 0,55**		

Identifikasi pada aset sistem informasi presensi memiliki 8 ancaman,

dengan jumlah rata-rata probabilitasnya 4,4 dan nilai ancamannya adalah 0,55. Identifikasi ancaman, kelemahan, dan probabilitas pada pegawai (SDM) dapat dilihat pada Tabel 4.20

Tabel 4.20 - Penilaian ancaman, kelemahan, dan probabilitas pada (SDM)

Nama Aset	Pegawai		
Jenis Aset	SDM		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Penyalahgunaan data organisasi	Vulnerable	Low	0,3
Penyalahgunaan hak akses	Threat	Low	0,3
Data tidak sesuai	Vulnerable	Medium	0,5
Password shared	Threat	Medium	0,4
Jumlah Ancamanan = 4	**Jumlah rata-rata probabilitas**		**1,5**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman 1, 5/4 = 0,38**		

Identifikasi pada aset sistem informasi presensi memiliki 4 ancaman, dengan jumlah rata-rata probabilitasnya 1,5 dan nilai ancamannya adalah 0,38. Identifikasi ancaman, kelemahan, dan probabilitas pada Satuan pengamanan (SDM) dapat dilihat pada Tabel 4.21

Tabel 4.21 - Penilaian ancaman, kelemahan, dan probabilitas Satuan pengemanan

Nama Aset	Satuan Pengamanan		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Tidak melakukan monitoring keamanan	Vulnerable	Low	0,3
Jumlah Ancamanan = 1	**Jumlah rata-rata probabilitas**		**0,3**

Tabel 4.21 (Lanjutan)

Nama Aset	Satuan Pengamanan		
Jenis Aset	Data		
Risiko	**Jenis Kejadian**	***Probability***	**Rata-rata *Probability***
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah ancaman** **0,3 /1 = 0,3**		

Identifikasi pada aset sistem informasi presensi memiliki 1 ancaman, dengan jumlah rata-rata probabilitasnya 0,3 dan nilai ancamannya adalah 0,3.

Hasil penilaian identifikasi ancaman, kelemahan, dan probabilitas pada masing-masing aset dapat dilihat pada tabel 4.22 – rekap nilai ancaman masing-masing aset.

Tabel 4.22 - Rekap nilai ancaman aset

No.	**Kategori Aset**	**Daftar Aset**	**Nilai Ancaman**
1.	Hardware	Server	0,46
		PC	0,5
2.	Software	Sistem Informasi Presensi	0,52
		Sistem Informasi *e-government*	0,46
		Sistem Informasi Pengajuan Permohonan	0,48
3.	Jaringan	Wifi	0,56
		Router dan Switch	0,53
		Kabel	0,37
4.	Data	Data *center*	0,48
		Data Presensi Pegawai	0,45
		Data Kepegawaian	0,41
		Data Keuangan	0,4
		Data Pelayanan dan Pengajuan Permohonan	0,44

Tabel 4.22 (Lanjutan)

		Data Aset	0,55
5.	SDM	Pegawai	0,38
		Satuan Pengamanan	0,3

3.3.1 Identifikasi Dampak jika terjadi kegagalan

Identifikasi dampak bisnis BIA (*Business Impact Analysis*) merupkan 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).

1. Dampak keamanan informasi Server ditunjukkan pada Tabel 4.23

Tabel 4.23 - Idetifikasi dampak server

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Jika data server tidak memiliki access control, maka akan menimbulkan dampak kerugian finansial yang sangat besar bagi internal akibat pencurian data dan kehilangan data yang terdapat pada server disalahgunakan oleh pihak yang tidak bertanggung jawab.
Integrity/ Keutuhan	Medium	Jika server mengalami kerusakan, maka semua data yang terdapat di dalam Server dapat menjadi corupt bahkan hilang akibatnya informasi yang dihasilkan tidak utuh dan valid.
Availability/ Ketersediaan	Medium	Data dan informasi yang disediakan oleh server harus selalu tersedia kapanpun ketika diakses oleh pengguna karena apabila data tersebut tidak dapat diakses akan menggangu kelancaran proses bisnis bagi organisasi akibatnya aplikasi core business tidak dapat diakses oleh semua organisasi.

2. Dampak keamanan informasi PC ditunjukkan pada Tabel 4.24

Tabel 4.24 - Idetifikasi dampak PC

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Jika dat yang terdapat pada PC diakses tanpa izin dapat menyebabkan kerugian seperti kehilangan data utama, perubahan informasi yang diakses secara ilegal, dan kerahasiaan dari data-data utama dapat diketahui oleh pihak lain yang tidak bertanggungjawab dapat menggunakan dan memberikan kerugian bagi individu yang bersangkutan.
Integrity/ Keutuhan	Medium	Jika PC mengalami kerusakan atau terkena virus, data dan informasi yang ada di dalam PC dapat rusak (*corupt*) akibatnya informasi yang ada di dalam PC mejadi tidak utuh dan akurat.
Availability/ Ketersediaan	Medium	Jika PC tidak dapat mengotorifikasi hak akses dari pemilik PC, maka pengguna (pemilik PC) tidak dapat mengakses data dan informasi yang berada pada PC.

3. Dampak keamanan informasi Sistem Informasi Presensi ditunjukkan pada Tabel 4.25

Tabel 4.25 - Idetifikasi dampak SIP

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	Medium	Apabila aplikasi Sistem Informasi Presensi tidak memiliki hak akses bagi orang yang mempunyai hak akses saja dapat mengakibatkan pencurian data, perubahan data atau informasi/kerusakan data oleh pihak yang tidak bertanggung jawab karena aplikasi Sistem Informasi Presensi merupakan

Tabel 4.25 (Lanjutan)

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	Medium	aplikasi untuk presensi pegawai dan seluruh orang yang berada pada instansi.
Integrity/ Keutuhan	Low	Jika pihak yang tidak bertanggung jawab merubah informasi yang ada pada aplikasi Sistem Informasi Presensi dapat mengakibatkan informasi dan data yang dihasilkan menjadi tidak valid dan akurat yang menimbulkan kerugian bagi pihak operasional dan manajerial
Availability/ Ketersediaan	Medium	Apabila aplikasi Sistem Informasi Presensi tidak dapat diakses dimanapun dan kapanpun dapat mengakibatkan kerugian finansial bagi individu serta organisasi. Ketika aplikasi Sistem Informasi Presensi tidak dapat diakses maka proses presensi pegawai pada instansi dapat berhenti dan menyebabkan gangguan bagi kelancaran proses bisnis pada instansi.

4. Dampak keamanan informasi Sistem Informasi *e-government* ditunjukkan pada Tabel 4.26

Tabel 4.26 - Idetifikasi dampak SI *e-government*

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Apabila aplikasi Sistem Informasi *e-government* tidak memiliki hak akses bagi orang yang mempunyai hak akses saja dapat mengakibatkan pencurian data, perubahan data atau informasi/kerusakan data oleh pihak yang tidak bertanggung jawab karena aplikasi Sistem Informasi *e-government* merupakan aplikasi informasi publik tentang pemerintahan yang berada pada Kominfo.

Tabel 4.26 (Lanjutan)

Kategori	Level	Dampak
Integrity/ Keutuhan	Medium	Jika pihak yang tidak bertanggung jawab merubah informasi yang ada pada aplikasi Sistem Informasi *e-government* dapat mengakibatkan informasi dan data yang dihasilkan menjadi tidak valid dan akurat yang menimbulkan kerugian bagi pihak operasional dan manajerial
Availability/ Ketersediaan	Low	Apabila aplikasi Sistem Informasi *e-government* tidak dapat diakses dimanapun dan kapanpun dapat mengakibatkan kerugian finansial bagi individu serta organisasi. Ketika aplikasi Sistem Informasi *e-government* tidak dapat diakses maka informasi publik yang dibutuhkan oleh masyarakat tidak sesuai dan tidak tersedia pada waktu yang dibuuhkan oleh karena itu dapat merugikan instansi dan menyebabkan gangguan bagi kelancaran proses bisnis pada instansi.

5. Dampak keamanan informasi Sistem Informasi Pengajuan Permohonan ditunjukkan pada Tabel 4.27

Tabel 4.27 - Idetifikasi dampak SIPP

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	Medium	Apabila aplikasi Sistem Informasi Pengajuan Permohonan tidak memiliki hak akses bagi orang yang mempunyai hak akses saja dapat mengakibatkan pencurian data, perubahan data atau informasi/kerusakan data oleh pihak yang tidak bertanggung jawab karena aplikasi Sistem Informasi Pengajuan Permohonan merupakan aplikasi informasi permohonan untuk

Tabel 4.27 (Lanjutan)

Kategori	Level	Dampak
		pengajuan terkait dengan pengajuan software instansi lain dengan kominfo.
Integrity/ Keutuhan	Low	Jika pihak yang tidak bertanggung jawab merubah informasi yang ada pada aplikasi Sistem Informasi Pengajuan Permohonan dapat mengakibatkan informasi dan data yang dihasilkan menjadi tidak valid dan akurat yang menimbulkan kerugian bagi pihak operasional dan manajerial
Availability/ Ketersediaan	Low	Apabila aplikasi Sistem Informasi Pengajuan Permohonan tidak dapat diakses dimanapun dan kapanpun dapat mengakibatkan kerugian finansial bagi individu serta organisasi. Ketika aplikasi Sistem Informasi Pengajuan Permohonan tidak dapat diakses maka informasi tentang pengajuan permohonan software yang dibutuhkan oleh instansi lain tidak tersedia pada waktu yang dibutuhkan oleh karena itu dapat merugikan instansi dan menyebabkan gangguan bagi kelancaran proses bisnis pada instansi.

6. Dampak keamanan informasi Wifi ditunjukkan pada Tabel 4.28

Tabel 4.28 - Idetifikasi dampak Wifi

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	Medium	Apabila wifi/*network* diakses oleh pihak yang tidak berkompeten dapat mengakibatkan kerusakan pada salah *hardware* seperti *switch, router* atau hardware utama pada wifi/*network* sehingga jaringan yang ada pada instansi menjadi terganggu

Tabel 4.28 (Lanjutan)

Kategori	Level	Dampak
Integrity/ Keutuhan	Medium	Apabila salah satu perangkat dari wifi/network menagalami gangguan mengakibatkan jaringan pada instansi tidak dapat berjalan dengan baik sehingga informasi yang dari dapat tidak utuh
Availability/ Ketersediaan	Medium	Apabila wifi/*network* tidak tersedia, maka koneksi jaringan yang ada pada instansi/organisasi tidak dapat berjalan dengan baik akibatnya dapat menggangu aktifikas bisnis dan menggangu konesi antar divisi dalam instansi terganggu.

7. Dampak keamanan informasi Router dan Switch ditunjukkan pada Tabel 4.29

Tabel 4.29 - Idetifikasi dampak router dan Switch

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	Medium	Apabila *router* dan *switch* diakses oleh pihak yang tidak berkompeten dapat mengakibatkan kerusakan pada salah *hardware (router* dan *switch)* utama pada *router* dan *switch* sehingga jaringan yang ada pada instansi menjadi terganggu
Integrity/ Keutuhan	Medium	Apabila salah satu perangkat dari *router* dan *switch* menagalami gangguan mengakibatkan jaringan pada instansi tidak dapat berjalan dengan baik sehingga informasi yang dari dapat tidak utuh
Availability/ Ketersediaan	Medium	Apabila *router* dan *switch* tidak tersedia, maka koneksi jaringan yang ada pada instansi/organisasi tidak dapat berjalan dengan baik akibatnya dapat menggangu aktifikas bisnis dan menggangu konesi antar divisi dalam instansi terganggu.

7. Dampak keamanan informasi Kabel ditunjukkan pada Tabel 4.30

Tabel 4.30 - Idetifikasi dampak kabel jaringan

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Apabila kabel ubah oleh pihak yang tidak berkompeten dapat mengakibatkan kerusakan pada salah kabel utama pada *router* dan *switch* sehingga jaringan yang ada pada instansi menjadi terganggu
Integrity/ Keutuhan	Medium	Apabila salah satu perangkat dari kebel menagalami gangguan mengakibatkan jaringan pada instansi tidak dapat berjalan dengan baik sehingga informasi yang dari dapat tidak utuh
Availability/ Ketersediaan	Medium	Apabila kabel tidak tersedia, maka koneksi jaringan yang ada pada instansi/organisasi tidak dapat berjalan dengan baik akibatnya dapat menggangu aktifikas bisnis dan menggangu konesi antar divisi dalam instansi terganggu.

8. Dampak keamanan informasi Data *Center* ditunjukkan pada Tabel 4.31

Tabel 4.31 - Idetifikasi dampakd data center

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Data *center* yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	High	Jika Data *center* yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga

Tabel 4.31 (Lanjutan)

Kategori	Level	Dampak
		informasi yang dihasilkan tidak valid dan idak akurat.
Availability/ Ketersediaan	High	Data *center* tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak akan memiliki akses pribadi bagi data pribadinya, data instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

9. Dampak keamanan informasi Data Presensi Pegawai ditunjukkan pada Tabel 4.32

Tabel 4.32 - Idetifikasi dampak Data presensi pegawai

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Data Presensi Pegawai yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Medium	Jika Data Presensi Pegawai yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan tidak akurat.

Tabel 4.32 (Lanjutan)

Kategori	Level	Dampak
Availability/ Ketersediaan	Medium	Jika Data Presensi Pegawai tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak akan memiliki akses pribadi bagi data presensi pribadinya, dan data presensi pegawai lainnya dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

10. Dampak keamanan informasi Data Pegawai ditunjukkan pada Tabel 4.33

Tabel 4.33 - Idetifikasi dampak data pegawai

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Data Kepegawaian yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Medium	Jika Data Kepegawaian yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan idak akurat.
Availability/ Ketersediaan	Medium	Jika Data Kepegawaian tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak akan memiliki akses pribadi bagi data pribadinya, data pegawai yang lain dan pihak luar

Tabel 4.33 (Lanjutan)

Kategori	Level	Dampak
Availability/ Ketersediaan	Medium	seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

11. Dampak keamanan informasi Data Keungan ditunjukkan pada Tabel 4.34

Tabel 4. 34 - Idetifikasi dampak data keuangan

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Data Keungan yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	High	Jika Data Keungan yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan idak akurat.
Availability/ Ketersediaan	High	Jika Data Keungan tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak akan memiliki akses pribadi bagi data pribadinya, data keuangan yang lain dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

12. Dampak keamanan informasi Data Pelayanan dan Pengajuan Permohonan ditunjukkan pada Tabel 3.35

Tabel 4.35 - Idetifikasi dampak Data Pelayanan dan Pengajuan Permohonan

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	Medium	Data Pelayanan dan Pengajuan Permohonan yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Low	Jika Data Pelayanan dan Pengajuan Permohonan yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan idak akurat.
Availability/ Ketersediaan	Low	Jika Data Pelayanan dan Pengajuan Permohonan tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak akan memiliki akses pribadi bagi data pribadinya, data pengajuan dan permohonan instansi lain yang berkepentingan dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

13. Dampak keamanan informasi Data Aset ditunjukkan pada Tabel. 4.36

Tabel 4.36 - Idetifikasi dampak data aset

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	Medium	Data Aset yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Low	Jika Data Aset yang diakses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan idak akurat.
Availability/ Ketersediaan	Low	Jika Data Aset tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak akan memiliki akses pribadi bagi data pribadinya, data aset instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

14. Dampak keamanan informasi SDM (Pegawai) ditunjukkan pada Tabel 4.37

Tabel 4.37 - Idetifikasi dampak data pegawai (SDM)

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Pegawai yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Medium	Jika Pegawai yang yang tidak bertanggungjawab mendapatkan akses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan idak akurat.
Availability/ Ketersediaan	Medium	Jika akses Pegawai tidak tersedia bagi siapapun yang tidak berwewenang, maka pihak lain tidak akan memiliki akses pribadi bagi data pribadinya, data aset instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

15. Dampak keamanan informasi SDM (Satuan Pengamanan) ditunjukkan pada Tabel 4.38

Tabel 4.38 - Idetifikasi dampak satuan pengamanan

Kategori	Level	Dampak
Confidentiality/ Kerahasiaan	High	Satuan pengamanan yang tidak memiliki hak akses bagi pihak yang tidak memiliki akses dapat menimbulkan dampak besar bagi individu maupun organisasi seperti penyalahgunaan data dan akses yang tidak diperbolehkan sehingg nantinya informasi yang tersedia dapat diketahui oleh pihak-pihak lain.
Integrity/ Keutuhan	Medium	Jika Satuan pengamanan yang memiliki akses ilegal oleh pihak yang tidak bertanggungjawab dapat mengakibatkan perubahan informasi yang disengaja sehingga informasi yang dihasilkan tidak valid dan idak akurat.
Availability/ Ketersediaan	Medium	Jika Satuan pengamanan tidak tersedia maka pihak lain dapat mengakses keamanan bagi data pribadiny atau data instansi dan pihak luar dapat mengetahui data-data penting yang seharusnya tidak disebarkan dengan luas dapat dengan mudah diketahui dengan pihak yang tidak bertanggungjawab yang dapat menyalahgunakan informasi yaang tersedia.

4. Analisa dan Evaluasi Risiko

Analisa risiko dan evaluasi risiko untuk menentukan level risiko dari masing-masing aset dilakukan dengan beberapa langkah adalah sebagai berikut.

4.1 Melakuakan Analisa Dampak Bisnis

Analisa dampak bisnis dilakukan dengan mementukan BIA pada aset yang sudah diidentifikasi pada langkah sebelumnya mengacu pada skala nilai BIA yang dapat dilihat pada Tabel 4.39. Nilai BIA pada masing-masing aset proses layanan kirim berita dinas, layanan pembuatan aplikasi, layanan monitoring rutin keamanan server hosting yang dapat diliht pada tabel 4.39

Tabel 4.39 - Analisa Dampak Bisnis

No.	Kategori Aset	Daftar Aset	Dampak	Skala Dampak	Nilai BIA	Skala BIA
1.	Hardware	Server	Operasi layanan aplikasi pusat dan unit terhenti	Medium	4	Very high critical
		PC	Pelaporan data pada aplikasi individu tertunda karena gangguan pada PC	Low	3	High critical
2.	Software	Sistem Informasi Presensi	Proses presensi terhenti, monitoring dan pelaporan daftar hadir pegawai terhambat	Medium	3	High critical
		Sistem Informasi *e-government*	Pelaporan pelayanan informasi publik terhambat	Medium	4	Very high critical
		Sistem Informasi Pengajuan Permohonan	Proses pengajuan permohonan antar instansi terganggu	Medium	4	Very high critical
3.	Jaringan	Wifi	Transfer data dan koneksi jaringan tidak dapat	Medium	3	High critical

Tabel 4.39 (Lanjutan)

No.	Kategori Aset	Daftar Aset	Dampak	Skala Dampak	Nilai BIA	Skala BIA
			digunakan untuk mengakses aplikasi pusat dan unit, komunikasi online antar bidang terganggu			
		Router dan Switch	Transfer data dan koneksi jaringan tidak dapat digunakan untuk mengakses aplikasi pusat dan unit	Low	3	High critical
		Kabel	Transfer data dan koneksi jaringan tidak dapat digunakan untuk mengakses aplikasi pusat dan unit	Low	3	High critical
4.	Data	Data *center*	Pelayanan terhadap admin data *center* terganggu sehingga dapat menghambat kinerja pengguna.	High	4	Very high critical
		Data Presensi Pegawai	Pelaporan monitoring presensi pegawai tertunda	Medium	3	High critical
		Data Kepegawaian	Pelaporan monitoring data kepegawaian/pegawai tertunda	Low	2	Medium critical
		Data Keuangan	Pelaporan monitoring keuangan instansi terhambat	High	4	Very high critical
		Data Pelayanan dan Pengajuan Permohonan	Pelaporan control dan monitoring engajuan permohonan antar instansi terganggu/tidak dapat	Medium	4	Very high critical

Table 4.39 (Lanjutan)

No.	Kategori Aset	Daftar Aset	Dampak	Skala Dampak	Nilai BIA	Skala BIA
		Pemohon	diproses			
		Data Aset	Pelaporan monitoring aset instansi tertunda	Low	2	Medium critical
5.	SDM	Pegawai	Pengguna tidak mempunyai kontrol akses sehingga dapat menimbulkan akses ilegal oleh pihak lain	High	2	Medium critical
		Satuan Pengamanan	Kelalaian petugas dapat menimbulkan dampak negatif bagi instansi	High	2	Medium critical

4.2 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 yang telah dihitung pada langkah 2.3.1 pada masing-masing aset.f dan apakah risiko tersebut dapat diterima atau tidak pada organisasi.

Tabel 4.40 - Identfikasi level risiko

No.	Kategori Aset	Daftar Aset	Nilai Ancaman	Skala BIA	Level Risiko
1.	Hardware	Server	0,46 (High)	Very high critical	High 100
		PC	0,5 (High)	High critical	High 100
2.	Software	Sistem Informasi Presensi	0,52 (High)	High critical	High 100
		Sistem Informasi *e-government*	0,46 (High)	Very high critical	High 100

Tabel 4.40 (Lanjutan)

No.	Kategori Aset	Daftar Aset	Nilai Ancaman	Skala BIA	Level Risiko
		Sistem Informasi Pengajuan Permohonan	0,48 (High)	Very high critical	High 100
3.	Jaringan	Wifi	0,56 (High)	High critical	High 100
		Router dan Switch	0,53 (High)	High critical	High 100
		Kabel	0,37 (Medium)	High critical	Medium 40
4.	Data	Data *center*	0,48 (High)	Very high critical	High 100
		Data Presensi Pegawai	0,45(High)	High critical	High 80
		Data Kepegawaian	0,41 (Medium)	Medium critical	Medium 30
		Data Keuangan	0,45 (Medium)	Very high critical	Medium 50
		Data Pelayanan dan Pengajuan Permohonan	0,44 (Medium)	Very high critical	Medium 50
		Data Aset	0,55 (High)	Medium critical	Medium 60
5.	SDM	Pegawai	0,38 (Medium)	Medium critical	Medium 30
		Satuan Pengamanan	0,3 (Medium)	Medium critical	Medium 30

4.3 Menentukan Risko diterima atau Perlu Penanganan Risiko

Menentukan risiko diterima atau tidak (perlunya penanagannan risiko) yaitu dengan menghitung terlebih dahulu nilai risiko dari masing-masing aset yang telah

diidentifikasi sebelumnya. Hasil dari perhitungan yang telah dilakukan, maka ditentukan nilai risiko dari masing-masing aset yang ditunjukkan pada tabel 4.41.

Tabel 4.41 - Penentuan risiko

No.	Kategori Aset	Daftar Aset	Nilai Aset (NA)	Nilai BIA (BIA)	Nilai Ancaman (NT)	Nilai Risiko (NA x BIA x NT)
1.	Hardware	Server	11	4	0,31	13,64
		PC	9	3	0,5	13,50
2.	Software	Sistem Informasi Presensi	9	3	0,52	14,04
		Sistem Informasi *e-government*	9	4	0,46	16,56
		Sistem Informasi Pengajuan Permohonan	10	4	0,48	19,20
3.	Jaringan	Wifi	7	3	0,56	11,76
		Router dan Switch	9	3	0,53	14,31
		Kabel	8	3	0,37	8,88
4.	Data	Data *center*	11	4	0,48	21,12
		Data Presensi Pegawai	9	3	0,45	12,15
		Data Kepegawaian	11	2	0,41	9,02
		Data Keuangan	12	4	0,45	21,6
		Data Pelayanan dan Pengajuan Permohonan	9	4	0,44	15,84
		Data Aset	6	2	0,55	6,60
5.	SDM	Pegawai	10	2	0,38	7,60
		Satuan Pengamanan	9	2	0,3	5,40

Setelah dapat diketahui nilai risiko pada masing-masing aset, langkah selanjutnya yaitu menentukan level risiko pada masing-masingaset. Penentuan leverl risiko dilakukan dengan menyesuaikan hasil dari nilai risiko pada matriks level risiko pada Tabel 4.41 yang telah dibuat sebelumnya. Hasil dari level risiko dari masing-masing aset ditunjukkan pada Tabel 4.42

Tabel 4.42 - level risiko

No.	Kategori Aset	Daftar Aset	Nilai Risiko (NA x BIA x NT)	Level Risiko
1.	Hardware	Server	13,64	Medium
		PC	13,50	Medium
2.	Software	Sistem Informasi Presensi	14,04	Medium
		Sistem Informasi *e-government*	16,56	Medium
		Sistem Informasi Pengajuan Permohonan	19,20	Medium
3.	Jaringan	Wifi	11,76	Medium
		Router dan Switch	14,31	Medium
		Kabel	8,88	Low
4.	Data	Data *center*	21,12	High
		Data Presensi Pegawai	12,15	Medium
		Data Kepegawaian	9,02	Low
		Data Keuangan	17,60	High
		Data Pelayanan dan Pengajuan Permohonan	15,84	Medium
		Data Aset	6,60	Low
5.	SDM	Pegawai	7,60	Low
		Satuan Pengamanan	5,40	Low

Dari hasil level risiko diatas, maka dapat ditentukan ada beberapa aset yang

bernilai High yaitu Data *center* dan Data Keuangan. Adapun beberapa aset yang bernilai Medium yaitu Server, PC, Sistem Informasi Presensi, Sistem Informasi *e-government,* Sistem Informasi Pengajuan Permohonan, Wifi, Router dan Switch, Data Presensi Pegawai, Data Pelayanan dan Pengajuan Permohonan. Adapun bebrapa aset yang bernilai Low yaitu kabel, data kepegawaian, data aset, pegawai dan satuan pengamanan. Pengolahan risiko hanya akan dilakukan dengan aset yang bernilai high, medium dan low sesuai dengan kriteria penerimaan risiko yang telah dibuat pada sub tahapan sebelumnya.

5. Identifikasi dan Evaluasi Penanganan Risiko

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

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

Setelah menentukan pilihan penanganann risiko langkah selanjutnya adalah melakukan pilihan penanganann risiko pada setiap aset yang bernilai High, medium dan low yaitu Data *center* dan Data Keuangan, Server, PC, Sistem Informasi Presensi, Sistem Informasi *e-government,* Sistem Informasi Pengajuan Permohonan, Wifi, Router dan Switch, Data Presensi Pegawai, Data Pelayanan dan Pengajuan Permohonan, kabel, data kepegawaian, data aset, pegawai dan satuan pengamanan. 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 27001:2013.

4.2.2 Kontrol Objektif dan Kontrol Keamanan Pengelolaan Risiko

1. Memilih Kontrol Objektif dan Kontrol Keamanan

Setelah menetapkan pilihan penanganan risiko, langkah selanjutnya yaitu menentukan kontrol keamanan yang sesuai pada aset yang memiliki level risiko lebih tinggi. Penetepan kontrol objektif dan kontrol keamanan disesuaikan dengan ancaman dan kelemahan dari masing-masing aset yang dipilih pada subbab 4.2.1. 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

Tabel 4.43 - Pemetaan Kontrol objektif dan Kontrol keamanan

No.	Klausul	Kontrol Objektif	Kontrol Keamanan
1.	A.5 – Kebijakan Keamanan Informasi	A.5.1 – Arahan manjemen untuk keamanan informasi	A.5.1.1 Kebijakan untuk keamaman informasi
			5.1.2 Tinjauan kebijakan untuk keamanan informasi
2.	A.6 – Organisasi Keamanan Informasi	A.6.1 Organisasi internal	A.6.1.1 Peran dan tanggung jawab keamanan informasi
3.	A.7 - Keamanan SDM	A.7.1 – sebelum bekerja	A.7.1.2. Syarat dan ketentuan kerja
		A.7.2 – selama bekerja	A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi

Tabel 4.43 (Lanjutan)

No.	Klausul	Kontrol Objektif	Kontrol Keamanan
4.	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses
		A.9.2 – Manajemen Hak pengguna	A.9.2.3 Manajemen hak akses khusus
		A.9.3 – Tanggung jawab pengguna	A.9.3.1 Penggunaan informasi otentikasi rahasia
		A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.1 Pembatasan akses informasi
			A.9.4.2 Prosedur *log-on* yang aman
			A.9.4.3 Sistem manajemen *password*
5.	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 - Peralatan	A.11.2.3 Pengendalian keamanan kabel
			A.11.2.4 Kontrol pemeliharaan peralatan
6.	A.12 - Keamanan Operasional	A.12.3 - *Backup*	A.12.3.1 *Backup* informasi
		A.12.4 – *Logging* dan pemantauan	A.12.4.1 Pencatatan kejadian
			A.12.4.2 Perlindungan informasi *log*
			A.12.4.3 *Log* administrasi dan operator

Pada tabel 4.44 berikut adalah pemetaan risiko dan kontrol objektif dan kontrol keamanann ISO 27001:2013, untuk lebih lengkapnya kebutuhan kontrol objektif dan kontrol keamanan dapat dilihat pada lampiran 6 Pemetaan hasil rekomendari pengendalian Risiko dengan kebutuhan pada ISO 27001:2013.

Tabel 4.44 - Pemetaan Risiko dengan kebutuhana kontrol keamanan

Kategori Aset	Aset Potensi kegagalan	Potensi penyebab kegagalan	Kontrol Keamanan
Hardware	Kerusakan Server	Kesalahan konfigurasi server	A.11.2.4 Kontrol pemeliharaan peralatan
	Kerusakan PC	Kesalahan konfigurasi PC	
Data	Data Hilang	Kelalaian Teknisi	A.9.1.1 Kebijakan pengendalian kontrol akses
			A.9.3.1 Penggunaan informasi otentikasi rahasia
			A.12.4.3 *Log* administrasi dan operator
	Manipulasi Data	Rusaknya media penyimpanan	A.12.3.1 *Backup* informasi
			A.11.2.4 Kontrol pemeliharaan peralatan
		Username password diketahui orang lain	A.9.1.1 Kebijakan pengendalian kontrol akses
			A.9.2.3 Manajemen hak akses khusus
			A.9.4.2 Prosedur *log-on* yang aman
			A.9.4.3 Sistem manajemen *password*
Informasi	Kesalahan penyampaian informasi	Adanya kesalahan dalam penyampaian informasi akibat Kelalaian pegawai	A.5.1.1 Kebijakan untuk keamaman informasi
			5.1.2 Tinjauan kebijakan untuk keamanan informasi
		Adanya keslahan tanggung jawab peran dalam penyampain informasi	A.6.1.1 Peran dan tanggung jawab keamanan informasi
Software	Aplikasi diakses oleh pihak yang tidak berwewenang	User dan password diketahui oleh pengguna lain	A.9.1.1 Kebijakan pengendalian kontrol akses
			A.9.4.1 Pembatasan akses informasi

Tabel 4.44 (Lanjutan)

Kategori Aset	Aset Potensi kegagalan	Potensi penyebab kegagalan	Kontrol Keamanan
			A.9.4.2 Prosedur *log-on* yang aman
			A.9.4.3 Sistem manajemen *password*
Jaringan	Kerusakan kabel LAN	Kurangnya kontrol pengamanan kabel	A.11.2.3 Pengendalian keamanan kabel
SDM	Sharing password	Kelalaian pegawai yang memiliki hak akses	A.7.1.2. Syarat dan ketentuan kerja
			A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi
			A.9.1.1 Kebijakan pengendalian kontrol akses
	Data tidak sesuai (tidak valid)	Kesalaahan input data	A.12.4.1 Pencatatan kejadian
			A.12.4.2 Perlindungan informasi *log*

4.2.3 Standart Operational Procedure (SOP) .

1. Standart Operational Procedure (SOP) yang dihasilkan

Berdasarkan hasil Pemetaan rekomendasi penyesuaian pengendalian risiko, didefinisikan beberapa prosedur yang dapat diusulkan dalam penelitian dengan hasil penilaian yang telah dilakukan maka penulis melakukan pembuatan dokumen kebijakan yang telah dilakukan oleh instansi terlebih dahulu. Dengan begitu, diharapkan dokumen prosedur, kebijakan, dan instruksi kerja yang telah dibuat dapat dijalankan dengan baik dalam manajemen keamanan informasi. Berikut ini adalah hasil pemetaan risiko dengan klausul dan kategori kebutuhan keamanan infomasi dapat dilihat pada tabel 4.45.

Tabel 4.45 - Pemetaan Risiko dengan klausul dan kategori kebutuhan

No.	Kategori Aset	Risiko yang terjadi	Klausul	Kontrol Objektif	Kontrol Keamanana	Kategori Kebutuhan
1.	Data	Adanya data yang hilang disebabkan oleh kelalaian pegawai yang memiliki hak akses	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
				A.9.3 – Tanggung jawab pengguna	A.9.3.1 Penggunaan informasi otentikasi rahasia	
			A.12 - Keamanan Operasional	A.12.4 – *Logging* dan pemantauan	A.12.4.3 *Log* administrasi dan operator	Operasional
		Adanya manipulasi data akibat Username dan password diketahui pengguna lain	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
		Adanya manipulasi data disebabkan oleh Username dan password diketahui pengguna lain	A.9 - Kontrol Akses	A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.1 Pembatasan akses informasi	
					A.9.4.2 Prosedur *log-on* yang aman	
			A.9 - Kontrol Akses	A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.3 Sistem manajemen *password*	

Tabel 4.45 (Lanjutan)

No.	Kategori Aset	Risiko yang terjadi	Klausul	Kontrol Objektif	Kontrol Keamanana	Kategori Kebutuhan
		Rusaknya media penyimpanan (file data)	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 – Peralatan	A.11.2.4 Kontrol pemeliharaan peralatan	Teknikal
		Kesalahan input data	A.12 - Keamanan Operasional	A.12.3 – *Backup*	A.12.3.1 *Backup* informasi	Operasional
			A.12 - Keamanan Operasional	A.12.4 – *Logging* dan pemantauan	A.12.4.1 Pencatatan kejadian	
					A.12.4.2 Perlindungan informasi *log*	
2.	Informasi	Adanya kesalahan dalam penyampaian informasi disebabkan oleh kelalaian pegawai	A.5 – Kebijakan Keamanan Informasi	A.5.1 – Arahan manjemen untuk keamanan informasi	A.5.1.1 Kebijakan untuk keamaman informasi	Manajemen
		Adanya keslahan tanggung jawab peran dalam penyampain informasi	A.6 – Organisasi Keamanan Informasi	A.6.1 Organisasi internal	A.6.1.1 Peran dan tanggung jawab	
3.	Hardware	Kesalahan konfigurasi server	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 – Peralatan	A.11.2.4 Kontrol pemeliharaan peralatan	Teknikal
		Kesalahan konfigurasi PC				

Tabel 4.45 (Lanjutan)

No.	Kategori Aset	Risiko yang terjadi	Klausul	Kontrol Objektif	Kontrol Keamanana	Kategori Kebutuhan
4.	Jaringan	Kurangnya kontrol pengamanan kabel	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 – Peralatan	A.11.2.3 Pengendalian keamanan kabel	Teknikal
5.	Software	Aplikasi diakses oleh pihak yang tidak berwewenang	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
		Username dan password diketahui oleh pengguna lain		A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.2 Prosedur *log-on* yang aman	
				A.9.4 – Sistem dan kontrol akses aplikasi	A.9.4.3 Sistem manajemen *password*	
6.	SDM	Kelalaian pegawai yang memiliki hak akses	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
				A.9.3 – Tanggung jawab pengguna	A.9.3.1 Penggunaan informasi otentikasi rahasia	
			A.12 - Keamanan Operasional	A.12.4 – *Logging* dan pemantauan	A.12.4.3 *Log* administrasi dan operator	Operasional
			A.7 - Keamanan SDM	A.7.1 – sebelum bekerja	A.7.1.2. Syarat dan ketentuan kerja	Teknikal

Tabel 4.45 (Lanjutan)

No.	Kategori Aset	Risiko yang terjadi	Klausul	Kontrol Objektif	Kontrol Keamanana	Kategori Kebutuhan
				A.7.2 – selama bekerja	A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi	Teknikal

Berdasarkan tabel 4.45 berikut adalah salah satu contoh pembahasan dari hasil pemetaan risiko dengan klausul dan kategori kebutuhan keamanan infomasi dapat dilihat pada tabel 4.46. Berdasarkan kategori aset data adanya risiko yaitu hilangnya data disebabkan oleh kelalaian pegawai yang memiliki hak akses dari risiko tersebut akan dipetakan untuk mengetahui letak kategori kebutuhan perdasarkan pemetaan pada control keamanan.

Tabel 4. 46 - Contoh pembahasan hasil

No	Kategori Aset	Risiko yang terjadi	Klausul	Kontrol Objektif	Kontrol Keamanana	Kategori Kebutuhan
1.	Data	Adanya data yang hilang disebabkan oleh kelalaian pegawai yang memiliki hak akses	A.9 - Kontrol Akses	A.9.1 – persyaratan bisnis untuk kontrol akses	A.9.1.1 Kebijakan pengendalian kontrol akses	Teknikal
				A.9.3 – Tanggung jawab pengguna	A.9.3.1 Penggunaan informasi otentikasi rahasia	

Pada tabel 4.47 berikut adalah pemetaan risiko dengan dokumen kebijakan yang dihasilkan dengan pemilihan kontrol keamanan yang sesuai.

Tabel 4.47 - Pemetaan Risiko dengan Dokumen Kebijakan

No	Kategori Aset	Risiko yang terjadi	Kategori Kebutuhan	Kontrol Keamanana	Dokumen Kebijakan
1.	Data	Adanya data yang hilang akibat Kelalaian pegawai yang memiliki hak akses	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	**KB - 01** **Pengendalian Hak akses**
				A.9.3.1 Penggunaan informasi otentikasi rahasia	**KB - 04** **Human resources security**
			Operasional	A.12.4.3 *Log* administrasi dan operator	**KB - 02** **Keamanan informasi (point 4.1 dan 4.2)**
		Adanya manipulasi data akibat *Username* dan *password* diketahui pengguna lain	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	**KB - 01** **Pengendalian Hak akses**
		Adanya manipulasi data akibat Username dan password diketahui pengguna lain		A.9.4.1 Pembatasan akses informasi	**KB - 02** **Keamanan informasi (point 4.2 dan 4.3)**
				A.9.4.2 Prosedur *log-on* yang aman	
				A.9.4.3 Sistem manajemen *password*	

Tabel 4.47 (Lanjutan)

No	Kategori Aset	Risiko yang terjadi	Kategori Kebutuhan	Kontrol Keamanana	Dokumen Kebijakan
		Rusaknya media penyimpanan (file data)	Teknikal	A.11.2.4 Kontrol pemeliharaan peralatan	**KB – 03** **Pengelolaan hardware dan kabel jaringan telekomunikasi**
		Kesalahan input data	Operasional	A.12.3.1 *Backup* informasi	**KB - 02** **Keamanan informasi (point 4.1)**
				A.12.4.1 Pencatatan kejadian	**KB - 02** **Keamanan informasi (point 4.1 dan 4.2)**
				A.12.4.2 Perlindungan informasi *log*	
2.	Informasi	Adanya kesalahan dalam penyampaian informasi akibat Kelalaian pegawai	Manajemen	A.5.1.1 Kebijakan untuk keamaman informasi	**KB - 02** **Keamanan dan pengendalian informasi (point 4.5)**
		Adanya keslahan tanggung jawab peran dalam penyampain informasi		A.6.1.1 Peran dan tanggung jawab	**KB - 02** **Keamanan dan pengendalian informasi (point 4.5)**
3.	Hardware	Kesalahan konfigurasi server	Teknikal	A.11.2.4 Kontrol pemeliharaan peralatan	**KB – 03** **Pengelolaan hardware dan kabel jaringan telekomunikasi**
		Kesalahan konfigurasi PC			

Tabel 4.47 (Lanjutan)

No	Kategori Aset	Risiko yang terjadi	Kategori Kebutuhan	Kontrol Keamanana	Dokumen Kebijakan
4.	Jaringan	Kurangnya kontrol pengamanan kabel	Teknikal	A.11.2.3 Pengendalian keamanan kabel	**KB - 03 Pengelolaan hardware dan kabel jaringan telekomunikasi**
5.	Software	Aplikasi diakses oleh pihak yang tidak berwewenang	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	**KB - 01 Pengendalian Hak akses**
		Username dan password diketahui oleh pengguna lain		A.9.4.2 Prosedur *log-on* yang aman	**KB - 02 Keamanan informasi (point 4.2 dan 4.3)**
				A.9.4.3 Sistem manajemen *password*	
6.	SDM	Kelalaian pegawai yang memiliki hak akses	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	**KB - 01 Pengendalian Hak akses**
				A.9.3.1 Penggunaan informasi otentikasi rahasia	**KB - 04 Human resources security**
			Operasional	A.12.4.3 *Log* administrasi dan operator	**KB - 02 Keamanan informasi (point 4.1 dan 4.2)**
			Teknikal	A.7.1.2. Syarat dan ketentuan kerja	**KB - 04 Human resources security**

Tabel 4.47 (Lanjutan)

No	Kategori Aset	Risiko yang terjadi	Kategori Kebutuhan	Kontrol Keamanana	Dokumen Kebijakan
				A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi	

Pada tabel 4.47 berikut adalah pemetaan kebijakan dengan dokumen prosedur, instruksi kerja dan formulir yang akan dihasilkan.

Keterrangan :

- KB : Kebijakan
- PO : Prosedur
- IK : Instruksi Kerja
- FM : Formulir

Berdasarkan tabel 4.47 berikut adalah salah satu contoh pembahasan dari pemetaan risiko dengan dokumen kebijakan yang dihasilkan dengan pemilihan kontrol keamanan dapat dilihat pada tabel 4.48. Berdasarkan kategori aset data adanya risiko yaitu hilangnya data disebabkan oleh kelalaian pegawai yang memiliki hak akses dari risiko tersebut kebutuhan kategori yaitu teknikal dengan kontol keamanan A.9.1.1 dan A.9.3.1 dihasilkan 2 dokumen kebijakan yaitu KB-01 pengendalian hak akses dan KB-04 *Human resources security*.

Tabel 4.49 - Contoh pembahasan hasil

No	Kategori Aset	Risiko yang terjadi	Kategori kebutuhan	Kontrol Keamanana	Dokumen Kebijakan
1.	Data	Adanya data yang hilang disebabkan oleh kelalaian pegawai yang memiliki hak akses	Teknikal	A.9.1.1 Kebijakan pengendalian kontrol akses	**KB - 01 Pengendalian Hak akses**
				A.9.3.1 Penggunaan informasi otentikasi rahasia	**KB - 04 Human resources security**

Pada tabel 4.49 berikut adalah pemetaan hasil kebijakan dengan prosedur, instruksi kerja dan formulir.

Tabel 4.49 - Pemetaan kebijakan dengan prosedur, instruksi kerja dan formulir

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB - 01 Pengendalian Hak akses	**PO - 01 Pengelolaan hak akses**	**IK – 01 Perubahan Hak Akses** - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	**FM - 01 :** pengelolaan hak akses **FM - 02 :** kontrak perjanjian hak akses **FM - 03 :** log – on pengelolaan hak akses
KB - 04 Human resources security	**PO - 06 Pelatihan dan pengembangan SDM**	**IK – 08 Pelatihan dan pengembangan SDM** - Proses pendaftaran pelatihan dan pengembangan - proses persiapan pelatihan dan pengembangan - proses pelatihan dan pengembangan - evaluasi pelatihan dan pengembangan	**FM - 12 :** Data pegawai **FM - 13 :** Evaluasi kegiatan pelatihan dan pengembangan

Tabel 4.49 (Lanjutan)

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB - 02 – point 4.1 dan 4.2 Keamanan informasi	**PO - 03 Backup dan Restore**	**IK - 04 Backup data dan file** - backup database - backup file	**FM - 06 :** Klasifikasi data **FM - 07:** log backup data
		IK - 05 Restore data	**FM - 08 :** restore data
KB - 01 Pengendalian Hak akses	**PO - 01 Pengelolaan hak akses**	**IK – 01 Perubahan Hak Akses** - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	**FM - 01 :** pengelolaan hak akses **FM - 02 :** kontrak perjanjian hak akses **FM - 03 :** log – on pengelolaan hak akses
KB - 02 – point 4.2 dan 4.3 Keamanan informasi	**PO - 02 Pengelolaan *password***	**IK – 02 Perubahan password**	**FM - 04 :** perbaikan sistem informasi
		IK – 03 *Reset password*	**FM - 05 :** *reset password*
KB - 03 Pengelolaan hardware dan kabel jaringan telekomunikasi	**PO - 04 Pengelolaan hardware**	**IK – 06 Perawatan Hardware :** - Pelaporan kerusakan hardware - Pemeliharaan hardware - Perbaikan hardware	**FM - 04 :** Perbaikan Sistem informasi **FM - 09 :** Pemeliharaan perangkat TI **FM - 10 :** Berita acara keruskan **FM - 11 :** Laporan Evaluasi penggunaan perangkat TI
	PO - 05 Pengelolaan kabel jaringan telekomunikasi	**IK – 07 Perawatan kabel jaringan telekomunikasi :** - Pemeliharaan kabel telekomukikasi - Pelaporan kerusakan kabel telekomunikasi - perbaikan kabel telekomunikasi	

Tabel 4.49 (Lanjutan)

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB - 02 – point 4.1 Keamanan informasi	**PO - 02 Pengelolaan *password***	**IK – 02 Perubahan password**	**FM - 04 :** perbaikan sistem informasi
		IK – 03 *Reset password*	**FM - 05 :** *reset password*
KB - 02 – point 4.1 dan 4.2 Keamanan informasi	**PO - 03 Backup dan Restore**	**IK - 04 Backup data dan file** - backup database - backup file	**FM - 06 :** Klasifikasi data **FM - 07 :** log backup data
		IK - 05 *Restore* data	**FM - 08 :** restore data
KB - 02 - point 4.5 keamanan dan pengendalian informasi	**PO - 07 Keamanan informasi**	**IK - 09 Klasifikasi Keamanan informasi**	**FM - 14 :** Monitoring Keamanan informasi
		10 Peran dan tanggung jawab informasi	
KB - 03 Pengelolaan hardware dan kabel jaringan telekomunikasi	**PO - 04 Pengelolaan hardware**	**IK – 06 Perawatan Hardware :** - Pelaporan kerusakan hardware - Pemeliharaan hardware - Perbaikan hardware	**FM - 04 :** Perbaikan Sistem informasi **FM - 09 :** Pemeliharaan perangkat TI **FM - 10 :** Berita acara keruskan **FM - 11 :** Laporan Evaluasi penggunaan perangkat TI
KB - 03 Pengelolaan hardware dan kabel jaringan telekomunikasi	**PO - 05 Pengelolaan kabel jaringan telekomunikasi**	**IK – 07 Perawatan kabel jaringan telekomunikasi :** - Pemeliharaan kabel telekomukikasi - Pelaporan kerusakan kabel telekomunikasi - perbaikan kabel telekomunikasi	**FM - 04 :** Perbaikan Sistem informasi **FM - 09 :** Pemeliharaan perangkat TI **FM - 10 :** Berita acara keruskan **FM - 11 :** Laporan Evaluasi penggunaan perangkat TI

Tabel 4.49 (Lanjutan)

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB - 01 Pengendalian Hak akses	**PO - 01 Pengelolaan hak akses**	**IK – 01 Perubahan Hak Akses** - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	**FM - 01 :** pengelolaan hak akses **FM - 02 :** kontrak perjanjian hak akses **FM - 03 :** log – on pengelolaan hak akses
KB - 02 – point 4.2 dan 4.3 Keamanan informasi	**PO - 02 Pengelolaan *password***	**IK - 02 Perubahan password**	**FM - 04 :** perbaikan sistem informasi **FM - 05 :** *reset password*
		IK - 03 *Reset password*	
KB - 01 Pengendalian Hak akses	**PO - 01 Pengelolaan hak akses**	**IK - 01 Perubahan Hak Akses** - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	**FM - 01 :** pengelolaan hak akses **FM - 02 :** kontrak perjanjian hak akses **FM - 03 :** log – on pengelolaan hak akses
KB - 04 Human resources security	**PO - 06 Pelatihan dan pengembangan SDM**	**IK - 08 Pelatihan dan pengembangan SDM** - Proses pendaftaran Pelatihan dan pengembangan - proses persiapan Pelatihan dan pengembangan - proses Pelatihan dan pengembangan - evaluasi Pelatihan dan pengembangan	**FM - 12 :** Data pegawai **FM - 13 :** Evaluasi kegiatan pelatihan dan pengembangan
KB - 02 – point 4.1 dan 4.2 Keamanan informasi	**PO - 03 Backup dan Restore**	**IK - 04 Backup data dan file** - backup database - backup file	**FM - 06 :** Klasifikasi data **FM - 07:** log backup data
		IK - 05 Restore data	**FM - 08 :** restore data

Tabel 4.49 (Lanjutan)

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

Berdasarkan tabel 4.49 berikut adalah salah satu contoh pembahasan dari pemetaan risiko dengan dokumen kebijakan yang dihasilkan dengan pemilihan kontrol keamanan dapat dilihat pada tabel 4.50. Berdasarkan kategori aset data adanya risiko yaitu hilangnya data disebabkan oleh kelalaian pegawai yang memiliki hak akses dari risiko tersebut kebutuhan kategori yaitu teknikal dengan kontol keamanan A.9.1.1 dan A.9.3.1 dihasilkan 2 dokumen kebijakan yaitu KB-01 pengendalian hak akses dan KB-04 *Human resources security* serta dokumen pendukung yaitu 2 prosedur PO-01 Pengelolaan hak akses dan PO-02 Pelatihan dan pengembangan SDM, 2 instruksi kerja yaitu IK-01 Perubhan hak akses dan IK-08 Pelatihan dan pengembangan SDM dan 5 formulir yang dihasilkan yaitu FM-01 pengelolaan hak akses, FM-02 kontrak perjanjian hak akses, FM-03 log-on pengelolaan hak akses, FM-12 Data pegawai, dan FM-13 Evaluasi kegiatan pelatihan dan pengembangan.

Tabel 4.50 - Contoh pembahasan hasil

Kebijakan	Prosedur	Instruksi Kerja	Formulir
KB - 01 Pengendalian Hak akses	**PO - 01 Pengelolaan hak akses**	**IK – 01 Perubahan Hak Akses** - Pemberian hak akses - Penghapusan hak akses - Perubahan hak akses	**FM - 01 :** pengelolaan hak akses **FM - 02 :** kontrak perjanjian hak akses **FM - 03 :** log – on pengelolaan hak akses
KB - 04 Human resources security	**PO - 06 Pelatihan dan pengembangan SDM**	**IK – 08 Pelatihan dan pengembangan SDM** - Proses pendaftaran pelatihan dan pengembangan - proses persiapan pelatihan dan pengembangan - proses pelatihan dan pengembangan - evaluasi pelatihan dan pengembangan	**FM - 12 :** Data pegawai **FM - 13 :** Evaluasi kegiatan pelatihan dan pengembangan

1.1 **Penjelasan pembentukan prosedur dan kebijakan**

Pada tahap ini akan dijekaskan 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 rekomendari penegndalian 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 berikut penjelasan pembentukan prosedur dan kebijakan yang di hasilkan.

1.1.1 Kebijakan pengendalian hak akses

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

a. Aplikasi diakses oleh pihak tidak berwenang
b. Sharing *password* karena kelalaian pegawai
c. Adanya manipulasi data karena *username password* diketahuai orang lain

Berdaraskan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan pengendalian hak akses yang menggunakan acuan ISO27001:2013 pada klausul A.9.1.1 Kebijakan pengendalian kontrol akses yang berisikan mengenai pedoman peraturan hak akses yang diberikan, selain itu instansi juga belum memiliki dokumen kebijakan tertulis mengenai hak akses. Kebijakan ini akan terkait juga dengan prosedur pengelolaan hak akses.

A. Prosedur pengelolaan hak akses

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan hak akses dengan acuan ISO27002:2013 pada klausal A.9.2.3 Manajemen hak akses khusus yang berisikan mengemai cara melakukan pengelolaan hak akses yang benar, selain itu juga aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada Kominfo.

B. Prosedur Keamana Informasi

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis

pada instansi, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan hak akses dengan acuan ISO27002:2013 pada klausal A.5.1.1 Kebijakan untuk keamaman informasi dan klausul A.6.1.1 Peran dan tanggung jawab yang berisikan mengemai cara melakukan pengamanan informasi yang benar, selain itu juga aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada Kominfo.

1.1.2 Kebijakan keamanan informasi

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

a. Data Hilang karena kelalaian Teknisi
b. Manipulasi data karena username password diketahui pengguna lain.
c. Aplikasi diakses oleh tidak berwenang karena username password diketahui pengguna lain
d. Data tidak sesuai karena kesalahan input

Berdaraskan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan keamanan informasi yang menggunakan acuan ISO27002:2013 pada klausal A.9.4.1 Pembatasan akses informasi, A.9.4.2 Prosedur *log-on* yang aman, A.9.4.3 Sistem manajemen *password,* A.12.4.1 Pencatatan kejadian, A.12.4.2 Perlindungan informasi *log,* A.12.4.3 *Log* administrasi dan operator yang berisikan tentang pedoman pengelolaan sistem, pedoman log-on pada sistem, pedoman password pengguna, pedoman pengelolaan backup informasi, dan juga peraturan adanya log kegiatan pada setiap aplikasi, dan pencatatan pada setiap kegiatan, selain itu instansi juga belum memiliki dokumen kebijakan tertulis mengenai keamanan

informasi. Kebijakan ini akan terkait dengan 2 prosedur yaitu prosedur pengelolaan password dan prosedur backup dan restore

A. Prosedur pengelolaan *pasword*

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan *password* dengan acuan ISO27002:2013 pada Klausul A.9.4.3 Sistem manajemen *password* yang berisikan mengenai tata cara dalam manajemen password, selain itu juga aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada Kominfo.

B. Prosedur *backup* dan *restore*

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan *password* dengan acuan ISO27002:2013 pada A.12.3.1 *Backup* informasi yang berisikan tata cara melakukan backup data, selain itu aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada Kominfo.

1.1.3 Kebijakan pngelolaan hardware dan jaringan

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

a. Kerusakan PC karena kesalahan konfigurasi
b. Kerusakan Server karena kesalahan konfigurasi
c. Data hilang karena rusaknya media penyimpanan

d. Kerusakan kabel LAN karena kurangnya kontrol pengamanan kabel

Berdaraskan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan pengelolaan hardware dan jaringan yang menggunakan acuan ISO27002:2013 pada Kominfo klausul A.11.2.4 Kontrol pemeliharaan peralatan, A.11.2.3 Pengendalian keamanan kabel yang berisikan tentang pedoman pengelolaan hardware dan jaringan, selain itu instansi juga belum memiliki dokumen kebijakan yang tertulis mengenai hardware dan jaringan Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

a. Kerusakan PC karena kesalahan konfigurasi
a. Kerusakan Server karena kesalahan konfigurasi
b. Data hilang karena rusaknya media penyimpanan
c. Kerusakan kabel lan karena kurangnya kontrol pengamanan kabel

Berdaraskan risiko yang dijelaskan peneliti menentukan dengan membuat kebijakan pengelolaan hardware dan jaringan yang menggunakan acuan ISO27002:2013 pada klausul A.11.2.4 Kontrol pemeliharaan peralatan, A.11.2.3 Pengendalian keamanan kabel yang berisikan tentang pedoman pengelolaan hardware dan jaringan, selain itu instansi juga belum memiliki dokumen kebijakan yang tertulis mengenai hardware dan jaringan Kebijakan ini akan terkait dengan 2 prosedur yaitu prosedur perawatan hardware dan prosedur pengamanan kabel.

A. Prosedur perawatan hardware

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur

pengelolaan *password* dengan acuan ISO27002:2013 pada Klausul A.12.3.1 *Backup* Informasi yang berisikan tata cara melakukan backup data, selain itu aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada Kominfo.

1.1.4 Kebijakan *human resource security*

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

a. Aplikasi diakses oleh pihak tidak berwenang karena *password* diketahui pengguna lain.
b. Data hilang karena kelalaian Teknisi
c. Sharing *password* karena kelalaian pegawai yang memiliki hak akses

Berdaraskan risiko yang dijelaskan peneliti menentukan dengan membuat *kebijakan human resource security* yang menggunakan acuan ISO27002:2013 pada klausul A.7.1.2. Syarat dan ketentuan kerja, A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi yang berisikan mengenai pembuatan kontrak perjanjian, dan pelatihan serta edukasi mengenai kesadaran mengenai keamanan informasi selain itu instansi juga belum memiliki dokumen kebijakan tertulis mengenai peraturan keamanan sumber daya manusia. Kebijakan ini akan terkait juga dengan prosedur pelatihan dan pengembangan SDM.

B. Prosedur pelatihan dan pengembangan SDM

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada instansi, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam melakukan pelatihan dan pengembangan SDM dengan acuan ISO27002:2013 pada klausul

A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi yang berisikan mengenai tata cara memberikan kesadaran dan edukasi mengenai keamanan informasi, selain itu juga aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada Kominfo.

1.2 Perancangan Struktur dan Isi SOP

Pada sub-bab ini akan dijelaskan mengenai perancangan SOP yang akan dibuat. Perancangan SOP ini mengacu pada peraturan pemerintah (Menteri Pedahayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia nomor 35 tahun 2012) terkait dengan pedoman penyusunan standar operasional prosedur administrasi pemerintah. Namun, dalam perancangan struksur dan isi SOP tidak keseluruhan struktur konten akan mengacu pada standar tersebut karena akan disesuaikan dengan kebutuhan. Struktur dokumen SOP yang akan disusun ini akan menghasilkan sebuah produk sebagai rekomendasi keamanan aset Informasi pada Kominfo. Adapun struktur atau konten yang akan dimasukkan ke dalam kerangka dokumen *Standar Operating Procedure* (SOP) Keamanan Aset Informasi pada Kominfo dapat dilihat pada tabel 4.51

Tabel 4.51 - Deskripsi prosedur dan kebijakan

Sturktur Bab	Sub-Bab	Konten
Pendahuluan	Tujuan	Deskripsi umum dokumen SOP Keamanan Aset Informasi
	Ruang Lingkup	
	Overview Keamanan Data	Aspek Kemanan Aset Informasi
	Evaluasi Penilaian Risiko Keamanan Aset Informasi pada Kominfo	Tabel Daftar Prioritas Risiko Keamanan Aset Informasi

Tabel 4.51 (Lanjutan)

Sturktur Bab	Sub-Bab	Konten
Kebijakan Pengendalian Hak Akses	Tujuan	Deskripsi umum Pengendalian Hak akses dan Keamanan Data
	Ruang lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan kebijakan
Kebijakan Pengendalian Hak Akses	Rincian Kebijakan	• Pengelolaan hak akses • hak akses pihak ketiga
	Dokumen Terkait	• Prosedur pengelolaan hak akses
Kebijakan Keamanan Informasi	Tujuan	Deskripsi umum kebijakan keamanan Informasi
	Ruang Lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Pengelolaan sistem informasi • Pengelolaan sistem *log-on* • Password pengguna • Pengelolaan backup dan restore informasi
	Dokumen Terkait	• Prosedur Pengelolaan Password • Prosedur Backup dan Restore
Kebijakan Pengelolaan Hardware dan Jaringan	Tujuan	• Deskripsi umum kebijakan pengelolaan hardware dan jaringan
	Ruang Lingkup	
Kebijakan Pengelolaan Hardware dan Jaringan	Referensi	• Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Pengelolaan hardware • Pengelolaan jaringan
	Dokumen Terkait	• Prosedur Perawatan Hardware • Prosedur Pengamanan Kabel

Tabel 4.51 (Lanjutan)

Sturktur Bab	Sub-Bab	Konten
Kebijakan *Human Resource Security*	Tujuan	• Deskripsi umum kebijakan human resource security
	Ruang Lingkup	
	Referensi	• Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Keamanan SDM • Tanggung jawab penggunaan hak akses
	Dokumen Terkait	• Prosedur pelatihan dan pengembangan SDM
Prosedur Pengelolaan Hak Akses	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pemberian akses • Pergantian dan prnghapusan hak akses sistem aplikasi
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Pengelolan Password	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pengelolaan password • Proses permintaan pergantian password
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur *Backup* dan *Restore*	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan prosedur
	Rincian Prosedur	• Proses umum sebelum melakukan backup • Proses backup secara berkala • Proses pengujian

Tabel 4.51 (Lanjutan)

Sturktur Bab	Sub-Bab	Konten
		• backup secara berkala • Proses restore data
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Perawatan Hardwre	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pemeliharaan • Proses pemeliharaan secara keseluruhan
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Kemanan Kabel	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	Prosedur pengaman kabel
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur pelatihan dan pengembangan SDM	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pelatihan pegawai instansi • Proses pelatihan pegawai magang
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Keamanan Informasi	Tujuan	Diskripsi umum SOP tentang Memberikan perlindungan aset informasi
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Klasifikasi keamanan informasi • Peran dan tanggung jawab informasi

Tabel 4.51 (Lanjutan)

Sturktur Bab	Sub-Bab	Konten
	Bagan Alur SOP	Tabel Bagan Alur SOP
Instruksi Kerja	Instruksi Kerja Perubahan Hak Akses	
	Instruksi kerja Perubahan password	
	Instruksi kerja reset password	
	Instruksi kerja Backup data dan file	
	Intruksi kerja Restore data	
	Intruksi kerja Perawatan Hardware	
	Instruksi kerja Perawatan kabel jaringan telekomunikasi	
	Instruksi kerja Pelatihan dan pengembangan SDM	
	Instruksi Kerja Klasifikasi Keamanan informasi	
	Instruksi Kerja Peran dan tanggung jawab informasi	
Formulir	Form pengelolaan hak akses	
	Form kontrak perjanjian hak akses	
	Form log pengelolaan hak akses	
	Form perbaikan sistem informasi	
	Form permintaan *reset* password	
	Form klasifikasi data	
	Form *log backup* data	
	Form *restore* data	
	Form pemeliharaan perangkat TI	
	Form berita acara kerusakan	
	Form laporan evaluasi pengelolaan perangkat TI	
	Form data pegawai	

Tabel 4.51 (Lanjutan)

Sturktur Bab	Sub-Bab	Konten
	Form evaluasi kegiatan pengembangan kompetensi	
	Form Monitoring keamanan informasi	

1.3 Hasil Perancangan SOP

Pada sub bab ini kana menjelaksakn dari setiap prosedur dan kebijakan serta dokumen pendukung yaitu instruksi kerjadan formulir yang dibutuhkan pada setiap proses didalamnya.

1.3.1 Hasil Perancangan Kebijakan

Hasil perancangan kebijakan dalam mendukung pelaksanaan SOP, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 4 kebijakan yang dibutuhkan untuk mendukung pelaksanaan SOP yaitu sebagai berikut.

a. Kebijakan pengendalian hak akses

Sesuai dengan kontrol dalam ISO27002:2013 sub klausul *9.1.1* Kebijakan pengendalian kontrol akses, *12.4.1* Pencatatan kejadian, dalam kebijakan ini terdapat beberapa hal yang terkandung di dalamnya yang mengatur mengenai pengelolaan hak akses. terlampir pada Lampiran 7 hasil perancangan kebijakan (KB – 01. Kebijakan pengendalian hak akses).

b. Kebijakan keamanan informasi

Sesuai dalam kontrol ISO 27002:2013 pada klausul 9.4.1 Pembatasan akses informasi, *5.1.1* Kebijakan untuk keamaman informasi, 6.1.1 Peran dan tanggung jawab, *9.4.2* Prosedur *log-on* yang aman, *9.4.3* Sistem manajemen *password, 12.3.1 Backup* informasi, *12.4.1* Pencatatan kejadian, *12.4.2*

Perlindungan informasi *log,* dalam kebijakan memuat peraturan untuk menjamin keamanan dari informasi penting baik informasi digital dan fisik yang dimiliki instansi, terlampir pada Lampiran 7 hasil perancangan kebijakan (KB – 02. Kebijakan keamanan informasi).

c. Kebijakan pengelolaan *hardware* dan jaringan

Sesuai dalam kontrol ISO 27002:2013 pada klausul *11.2.3* Pengendalian keamanan kabel dan *11.2.4.* Kontrol pemeliharaan peralatan dalam kebijakan memuat peraturan untuk menjamin fasilitas perangkat hardware dan jaringan agar dapat selalu beroperasi selama proses bisnis berlangsung, terlampir pada Lampiran 7 hasil perancangan kebijakan (KB – 03. Kebijakan pengelolaan *hardware* dan jaringan).

d. Kebijakan *human resource security*

Sesuai dalam kontrol ISO 27002:2013 pada klausul *7.1.2.* Syarat dan ketentuan kerja*, 7.2.2.* Kepedulian, pendidikan dan pelatihan keamanan informasi*, 9.3.1.* Penggunaan informasi otentikasi rahasia dalam kebijakan memuat peraturan kepada seluruh civitas instansi dalam memberi perlindungan keamanan pada aset informasi yang dimiliki instansi, terlampir pada Lampiran 7 hasil perancangan kebijakan (KB – 04. Kebijakan *human resource security*).

1.3.2 Hasil Perancanagan Prosedur

Hasil perancangan instruksi kerja dalam mendukung pelaksanaan SOP, dibutuhkan beberapa prosedur dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 7 prosedur yang dibutuhkan untuk mendukung pelaksanaan SOP yaitu sebagai berikut.

a. Prosedur Pengelolaan Hak Akses

Prosedur pengelolaan hak akses merupakan prosedur untuk menjadi pedoman dalam memberikan alokasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun luar lingkungan instansi. terlampir pada Lampiran 8 hasil perancangan prosedur (PO – 01. Prosedur pengelolaan hak akses).

b. Prosedur Pengelolaan *Password*

Prosedur Manajemen *password* merupakan prosedur untuk memastikan pengelolaan penggunaan *password* telah memenuhi kualitas standar *strong* password dan memastikan *password* setiap pengguna telah sesuai dengan syarat kualitas password, terlampir pada Lampiran 8 hasil perancangan prosedur (PO – 02. Prosedur pengelolaan *password*).

c. Prosedur Backup dan Restore

Prosedur ini menjelaskan langkah langkah dalam aktivitas backup yang sesuai dengan kontrol ISO27001:2013, sub klausul 12.3.1 *backup* informasi. Prosedur *Back up* dan *restore* dibagi kedalam empat proses utama yang terdiri dari beberapa aktivitas yang berurutan. Namun, sebelum mendeskripsikan prosedur penangan secara terstruktur, terlebih dahulu didefinisikan informasi pendukung yang dibutuhkan untuk menunjang aktivitas didalam prosedur tersebut. Pendefinisan tesebut berguna untuk menentukan strategi *back up* yang sesuai dengan kebutuhan bisnis. Pendefinisan dalam prosedur *Back up* dibagi kedalam tiga yaitu pendefinisian klasifikasi data, pendefinisian kritikalitas data dan pendefinisian tipe *back up*, terlampir pada Lampiran 8 hasil perancangan prosedur

(PO – 03. Prosedur *backup* dan *restore*).

d. Prosedur Pengelolaan *Hardware*

Prosedur pengelolaan *hardware* ini merupakan pedoman dan acuan untuk melakukan pengelolaan aset *hardware* pada instansi baik dalam melakukan pengadaan barang, maintenance, penggunaan serta keamanan dari *hardware* itu sendiri, terlampir pada Lampiran 8 hasil perancangan prosedur (PO – 04. Prosedur pengelolaan *hardware*).

e. Prosedur Prosedur pengelolaan kabel jaringan telekomunikasi

Prosedur Prosedur pengelolaan kabel jaringan telekomunikasi merupakan prosedur yang berguna untuk memastikan bahwa seluruh kabel telekomunikasi yang membawa data dan mendukung layanan informasi pada instansi diatur atau dikelola secara terstruktur sehingga terlindungi dari kerusakan, terlampir pada Lampiran 8 hasil perancangan prosedur (PO – 05. Prosedur pengelolaan kabel jaringan telekomunikasi).

f. Prosedur Pelatihan dan Pengembangan SDM

Prosedur Pelatihan dan Pengembangan SDM merupakan prosedur yang mengatur segala pelatihan atau edukasi terkait keamanan informasi untuk pegawai yang mampu meningkatkan kualitas baik secara intelektual maupun kepribadian, sehingga mampu menjaga aset informasi yang dimiliki oleh instansi, terlampir pada Lampiran 8 hasil perancangan prosedur (PO – 06. Prosedur pelatihan dan pengembangan SDM).

g. Prosedur Keamanan Informasi

Prosedur keamanan informasi merupakan prosedur yang berguna untuk memastikan bahwa seluruh aset informasi pada instansi diatur dan dikelola secara

terstruktur sehingga terlindungi dari kerusakan, terlampir pada Lampiran 8 hasil perancangan prosedur (PO – 07. Prosedur pengelolaan keamanan informasi).

1.3.3 Hasil Perancangan Instruksi Kerja

Hasil perancangan instruksi kerja dalam mendukung pelaksanaan SOP, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 10 instruksi kerja yang dibutuhkan untuk mendukung pelaksanaan SOP yaitu sebagai berikut.

a. Instruksi kerja Pengelolaan hak akses

Dalam dokumen prosedur pemberian hak akses dibutuhkan sebuah instruksi kerja yaitu instruksi dalam melakukan pemberian hak akses yang bertujuan untuk membantu pegawai baru untuk mengakses sistem informasi yang diizinkan. Terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 01. Instruksi kerja pengelolaan hak akses).

b. Instruksi kerja Perubahan *password*

Dalam dokumen prosedur perubahan *password* dibutuhkan sebuah instruksi kerja yaitu instruksi dalam melakukan perubahan *password* yang bertujuan untuk membantu pegawai dalam melekaukan perubahan *password* baik pegawai baru ataupun pegawai tetap. Terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 02. Instruksi kerja perubahan password).

c. Instruksi kerja *reset password*

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja reset *password* yang bertujuan untuk membantu kerja pegawai baru dalam mempelajari proses reset *password*, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 03. Instruksi kerja *resset*

password).

d. Instruksi kerja backup data dan file

Dalam dokumen Prosedur *Backup* dan *Restore*, dibutuhkan sebuah instruksi kerja yaitu instruksi kerja *back up* yang bertujuan untuk membantu kerja DB Teknisi baru dalam mempelajari proses *back up* data maupun *back up file*, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 04. Instruksi kerja *backup* data dan *file*).

e. Instruksi kerja *restore* data

Dalam dokumen Prosedur *Backup* dan *Restore*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja restore yang bertujuan untuk membantu kerja DB Teknisi baru dalam mempelajari proses *restore*, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 05. Instruksi kerja *restore* data).

f. Instruksi kerja perawatan hardware

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja perawatan hardware yang bertujuan untuk membantu kerja pegawai baru dalam mempelajari proses perawatan *hardware,* terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 06. Instruksi kerja perawatan *hardware)*.

g. Instruksi kerja perawatan kabel jaringan telekomunikasi

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja perawatan kabel yang bertujuan untuk membantu kerja pegawai baru dalam mempelajari proses perawatan kabel, terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 07. Instruksi kerja perawatan kabel jaringan telekomunikasi).

h. Instruksi kerja pelatihan dan pengembangan SDM

Dalam dokumen Prosedur pengelolaan *password*, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja pelatihan dan pengembangan SDM instansi yang bertujuan untuk membantu kerja pegawai baru dalam proses pelatihan dan pengembangan SDM instansi terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 08. Instruksi kerja pelatihan dan pengemabangan SDM).

i. Intruksi Kerja Klasifikasi Keamanan informasi

Dalam dokumen Prosedur keamanan informasi, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja klasifikasi keamanan informasi yang bertujuan untuk membantu dalam mengklasifikasikan informasi yang ada dalam instansi. terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 09. Instruksi kerjaklasifikasi keamanan informasi).

j. Intruksi Kerja peran dan tanggung jawab informasi

Dalam dokumen Prosedur keamanan informasi, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja peran dan tanggung jawab informasi yang bertujuan untuk membantu kerja pegawai dalam memahami peran dan tanggung jawab dalam penyampaian informasi instansi. terlampir pada Lampiran 9 Hasil perancangan instruksi kerja (IK – 10. Instruksi kerja peran dan tanggung jawab informasi).

1.3.4 Hasil Perancangan Formulir

Hasil perancangan formulir dalam mendukung pelaksanaan SOP, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 14 formulir yang dibutuhkan untuk mendukung pelaksanaan SOP yaitu sebagai berikut.

a. Formulir Pengelolaan hak akses

Formulir pengelolaan hak akses adalah formulir yang digunakan dalam prosedur pengelolaan hak akses dimana formulir ini berguna untuk mendokumentasikan pemberian hak akses pada pengguna sistem untuk dilakukan persetujuan pada pihak manajemen. terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 01. Formulir pengelolaan hak akses).

b. Formulir kontrak perjanjian hak akses

Formulir kontrak perjanjian hak akses adalah formulir yang digunakan dalam prosedur pengelolaan hak akses yang berfungsi sebagai sebuah peraturan dan tanggung jawab yang harus disetujui oleh pengguna sistem jika hak akses diberikan ,terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 02. Formulir kontrak perjanjian hak akses).

c. Formulir *log* pengelolaan hak akses

Formulir *log* pengelolaan hak akses adalah formulir yang berfungsi sebagai media pencatatan pemberian, penghapusan ataupun pergantian hak akses yang dilakukan ,terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 03. Formulir *log* pengelolaan hak akses).

d. Formulir perbaikan sistem informasi

Formulir perbaikan sistem informasi adalah formulir yang digunakan untuk melakukan perbaikan pada sistem informasi atau aplikasi yang dimiliki instansi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 04. Formulir perbaikan sistem informasi).

e. Formulir permintaan *reset password*

Formulir permintaan pergantian *password* adalah formulir yang digunakan

untuk prosedur pergantian *password* sebelum meminta pergantian *password* pengguna harus mengisi formulir ini,terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 05. Formulir permintaan *reset password)*.

f. Formulir klasifikasi data

Formulir klasifikasi data digunakan untuk menentukan strategi back up yang akan digunakan. Berdasarkan kontrol dalam ISO27001:2013, penentuan strategi *back up* data ditentukan sesuai dengan kebutuhan bisnis organisasi dilihat dari kebutuhan keamanan dan tingkat kritikalitas data. Klasifikasi data akan didasarkan pada tingkat sensitivitas data dan tingkat kritikalitas data, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 06. Formulir klasifikasi data).

g. Formulir *log backup* data

Formulir *log back up* digunakan oleh DB Teknisi untuk melakukan pemantauan (*monitoring*) secara berkala pada hasil eksekusi *back up* data. Tujuan dari formulir log back up data ini adalah untuk memastikan bahwa hasil eksekusi *back up* data telah akurat dan lengkap dan juga untuk memastikan keberhasilan data yang ter-*back up* dan data yang tidak berhasil *di-back up*, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 07. Formulir *log backup* data).

h. Formulir *restore* data

Formulir restore digunakan untuk permintaan kebutuhan *restore* data oleh pihak tertentu/unit kerja tertentu. Formulir *restore* data dibutuhkan untuk menjaga integritas data dan memastikan bahwa setiap proses *restore* data terdokumentasi dengan baik dan telah di validasi oleh pegawai bagian personalia yang bertanggung jawab, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 8. Formulir *restore* data).

i. Formulir pemeliharaan perangkat TI

Formulir pemeliharaan perangkat TI adalah formulir yang digunakan untuk melakukan pencatatan kegitan (*log*) dalam melakukan perbaikan perangkat TI yang dimiliki instansi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 09. Formulir pemeliharaan perangkat TI).

j. Formulir berita acara kerusakan

Formulir berita acara kerusakan adalah formulir yang digunakan untuk pelaporan kerusakan pada perangkat TI yang dimiliki instansi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 10. Formulir berita acara kerusakan).

k. Formulir laporan evaluasi pengelolaan perangkat TI

Formulir laporan evaluasi adalah formulir yang digunakan dalam pencatatan setiap kegiatan pengelolaan perangkat TI baik itu perbaikan secara parsial maupun keseluruhan yang dilakukan, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 11. Formulir laporan evaluasi pengelolaan perangkat TI).

l. Formulir data pegawai

Formulir data pegawai adalah formulir yang digunakan instansi dalam prosedur pelatihan dan pengembangan SDM untuk mencatat peagwai yang mengikuti program pelatihan yang diadakan instansi terkait dengan keamanan aset informasi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 12. Formulir data pegawai).

m. Formulir evaluasi kegiatan pengembangan kompetensi.

Formulir evaluasi kegiatan pengembangan kompetensi adalah formulir

digunakan untuk melakukan evaluasi pelatihan maupun pengembangan pegawai yang dilakukan instansi, terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 13. Formulir pengelol evaluasi kegiatan pengembangan kompetensi).

n. Formulir Monitoring kemanan informasi

Formulir Monitoring kemanan informasi adalah formulir digunakan untuk melakukan monitorng keamanan informasi guna mengetahui informasi apa yang akan disampaikan. terlampir pada Lampiran 10 Hasil perancangan formulir (FM – 14. Formulir Monitoring kemanan 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. Pada tahap penyusuanan dokumen manajemen pengelolaan risiko menghasilkan identifikasi risiko, penilaian risiko dan risk respon dari masing-masing aset informasi.
2. Pada tahap penyusunan dokumen kontrol keamananan dihasilkan 3 kategori kebutuhan yaitu kategori manajemen terdiri dari 2 control keamamann (A.5.1.1 dan A.6.1.1.1), kategori teknikal 9 kontrol keamanan (A.7.1.2, A.7.2.2, A.9.1.1, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.11.2.3, dan A.11.2.4), kategori operasional terdiri dari 3 kontrol keamanan (A.12.4.1, A.12.4.2, dan A.12.4.3).
3. Hasil dokumen SOP dari kategori kebutuhan manajemen terdiri dari 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 untuk mendukung keamanan informasi dan sebagai dokumen acuan implementasi SMKI.

5.2 Saran.

1. Pengembangan tugas akhir dapat dilakukan dengan menambahkan dampak biaya kerugian yang dialami oleh instansi.

2. Penelitian ini sebatas pembuatan dokumen SOP tanpa proses pengujian SOP, dan implementasi bagi 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

Djojosoedarso, S. 2005. *Prinsip-Prinsip Manajemen Risiko Asuransi*, Edisi revisi. Jakarta: Salemba Empat.

Humphreys, E. 2007. *Implementing The Iso/Iec 27001 Information Security Management System.* Artech House.

Intan Rahayu, D. F. 2017. *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI).* Jakarta: Kementerian Komunikasi dan Informatika.

ISO/IEC. 2013. ISO/IEC 27001 *Security Techniques Information Security Management Systems Requirements*: ISO/IEC.

ISO/IEC. 2013. ISO/IEC 27002 *Security Techniques Information Security Management Systems Requirements*: ISO/IEC.

Jolly, A. 2003. *The Secure OnlineBusiness*.USA-London: Kogan Page and Contributors.

Kadir,A. 2003. *Pengenalan Sistem Informasi*, Andi, Yogyakarta.

Peraturan Menteri Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Republik Indonesia.2012.Nomor 35 Tahun 2012. Tentang *Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan*,

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

Rakhmat, Jalaluddin, 2004. *Metode Penelitian Komunikasi*: Dilengkapi Contoh Analisis Statistik, Bandung: PT Remaja Rosdakarya.

Sarno, R. 2009. *Sistem Manajemen Keamanan Informasi berbasis ISO 27001.* Surabaya: ITSPress.

Siahaan, H. 2007. *Manajemen Risiko*. Jakarta: PT. Elex Media Computido

Sulistiyani, S. 2011. *keamanan Sistem Informasi.* Yogyakarta: CV. ANDI.

Suprandono, Bambang. *Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode OCTAVE.* Teknik Elektro Universitas Muhammadiyah Semarang. 2009.

Sutabri, T. 2003. *Analisa Sistem Informasi*.Penerbit Andi Yogjakarta