TUGAS AKHIR – KS 141501

ANALISIS RISIKO DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DINAS PERHUBUNGAN KOMUNIKASI DAN INFORMATIKA KABUPATEN TULUNGAGUNG

Balqis Lembah Mahersmi
5212 100 066

Dosen Pembimbing
Feby Artwodini Muqtadiroh, S.Kom, M.T
Bekti Cahyo Hidayanto, S.Si, M.Kom

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

FINAL PROJECT – KS 141501

RISK ANALYSIS USING OCTAVE METHOD AND CONTROL ISO 27001 IN THE DEPARTEMENT OF TRANSPORTATION COMMUNICATION AND INFORMATION DISTRICT TULUNGAGUNG

Balqis Lembah Mahersmi
5212 100 066

Academic Promotors
Feby Artowini Muqtadiroh, S.Kom, M.T
Bekti Cahyo Hidayanto, S.Si, M.Kom

INFORMATION SYSTEMS DEPARTMENT
Information Technology Faculty
Sepuluh Nopember Institut of Technology
Surabaya 2016

LEMBAR PENGESAHAN

ANALISIS RISKO DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DINAS PERHUBUNGAN KOMUNIKASI DAN INFORMATIKA KABUPATEN TULUNGAGUNG

TUGAS AKHIR
Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

Balqis Lembah Mahersmi
5212 100 066

Surabaya, Juli 2016

KETUA
JURUSAN SISTEM INFORMASI

Ir. Aris Tjahyanto, M.Kom
NIP. 19650310 199102 1 001

LEMBAR PERSETUJUAN

ANALISIS RISIKO DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DINAS PERHUBUNGAN KOMUNIKASI DAN INFORMATIKA KABUPATEN TULUNGAGUNG

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

Balqis Lembah Mahersmi

5212 100 066

Disetujui Tim Penguji: Tanggal Ujian : Juli 2016
Periode Wisuda : September 2016

Feby Artwodini Muqtadiroh, S.Kom, M.T **(Pembimbing 1)**

Bekti Cahyo Hidayanto, S.Si, M.Kom **(Pembimbing 2)**

Tony Dwi Susanto, S.T, M.T, Ph.D **(Penguji 1)**

Anisah Herdiyanti S.Kom, M.Sc **(Penguji 2)**

ANALISIS RISIKO DENGAN MENGGUNAKAN METODE OCTAVE DAN KONTROL ISO 27001 PADA DINAS PERHUBUNGAN KOMUNIKASI DAN INFORMATIKA KABUPATEN TULUNGAGUNG

Nama Mahasiswa : Balqis Lembah Mahersmi
NRP : 5212100066
Jurusan : Sistem Informasi FTIf – ITS
Dosen Pembimbing 1 : Feby Artwodini Muqtadiroh, S.Kom, M.T
Dosen Pembimbing 2 : Bekti Cahyo Hidayanto, S.Si, M.Kom

ABSTRAK

Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung adalah unit pelayanan masyarakat bidang tranportasi dan teknologi informasi. Untuk mencapai tujuan dan melaksanakan tugas fungsi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung, diperlukan adanya suatu manajemen risiko untuk mengarahkan dan mengendalian organisasi dalam mengelola risiko yang mungkin terjadi. Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung telah mengimplementasikan Teknologi Informasi sebagai pendukung keberlangsungan bisnisnya. Implementasi Teknologi Informasi(TI) di Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung selain memberikan keuntungan juga menimbulkan berbagai ancaman timbulnya risiko.

Tujuan dari penelitian ini adalah untuk mengidentifikasi, menilai dan memitigasi risiko yang berkaitan dengan teknologi informasi yang dikelola oleh Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung berdasarkan metode OCTAVE. Dalam penerapan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung tentu mempunyai banyak permasalahan dan hambatan yang menyebabkan proses binis organisasi tersebut terganggu. Misalnya kehilangan data, penyalahgunaan hak akses. Hal ini akan menyebabkan data-data penting hilang dan bisa diakses oleh pihak yang tidak berwenang. Adanya kemungkinan munculnya permasalahan-permasalahan terkait penerapan teknologi informasi itulah yang mendasari pentingnya analisis risiko terkait penerapan teknologi informasi di Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung. Dengan melakukan analisis risiko Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung dapat mengetahui risiko-risiko apa saja yang mungkin akan dihadapi di kemudian hari.Metode analisis risiko yang digunakan dalam tugas akhir ini adalah metode OCTAVE yang merupakan metodologi yang berfungsi untuk meningkatkan proses pengambilan keputusan terhadap perlindungan dan pengelolaan sumberdaya di suatu informasi berdasarkan penilaian risiko.

Hasil dari tugas akhir ini adalah melakukan identifikasi risko yang dapat terjadi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung terkait implementasi teknologi informasi dan memberikan masukan atau rekomendasi kepada pihak Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung bagaimana langkah mitigasi risiko yang tepat sesuai dengan hasil identifikasi risiko yang akan muncul terkait implementasi teknologi informasi. Pada akhir penelitian ada 13 risiko yang muncul dengan 31

kejadian risiko. nilai RPN tertinggi sebesar 378 dan terendah sebesar 45. Mitigasi risiko menggunakan 12 kontrol pada ISO 27001.

Kata Kunci: *Analisis risiko, Octave, Teknologi Informasi*

Halaman ini sengaja dikosongkan

RISK ANALYSIS USING OCTAVE METHOD AND CONTROL ISO 27001 IN THE DEPARTMENT OF TRANSPORTATION COMMUNICATION AND INFORMATION DISTRICT TULUNGAGUNG

Student Name	**: Balqis Lembah Mahersmi**
NRP	**: 5212100066**
Department	**: Sistem Informasi FTIf – ITS**
Supervisor 1	**: Feby Artwodini Muqtadiroh, S.Kom, M.T**
Supervisor 2	**: Bekti Cahyo Hidayanto, S.Si, M.Kom**

ABSTRACT

Department of transportation Communication and Information district Tulungagung is a community service unit areas of transport and information technology. To succeed and perform tasks on the Department of Communication and Information Tulungagung, needed a risk management organization control to direct and manage the risks that may occur. Department of Communication and Information Tulungagung has implemented information technology to support business continuity. Implementation of Information Technology (IT) in the Department of Communication and Information Tulungagung besides providing the advantages also pose various threats onset of risk.

Purpose of this study is to identify, assess and mitigate risks of information technology managed by the Department of Communication and Information Tulungagung based OCTAVE method. When applying information technology in the Department of Communication and Information Tulungagung certainly has many problems and obstacles that led to the

organization business is disrupted. Such as loss of data, abuse of access rights. This will cause critical data is lost and can be accessed by unauthorized parties. The emergence of problems related to applaying information technologies that underlie risk analysis related to the implementation of information technology in the Department of Communication and Information Tulungagung. By performing a risk analysis Department of Communication and Information Tulungagung can know any risks that may be encountered in later. Risk analysis used in this thesis is the OCTAVE method a method that serves to improve the decisions on the protection and resource management in an information on risk assessment.

The results of this thesis is to identify risking which can occur at the Department of Communication and Information Tulungagung related information technology implementation and provide input or recommendations to the Department of Communication and Information Tulungagung how measures proper risk mitigation to the results of risk identification will appear related to the implementation of information technology. At ending the study there is a risk that appeared 13 to 31 the risk event. The highest RPN value of 378 and a low of 45. Risk mitigation using 12 controls in ISO 27001.

Keywords: *Risk analysis, Octave, Information Technology*

DAFTAR ISI

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

DAFTAR TABEL

DAFTAR LAMPIRAN

Berikut ini adalah lampiran dokumen dari penelitian ini. Dokumen-dokumen ini dapat disajikan sebagai bukti pengerjaan penelitian ini.

Kode Lampiran	Lampiran
A	Interview protocol
B	Hasil wawancara
C	Mitigasi risiko
D	Validasi

BAB I
PENDAHULUAN

Pada bagian ini terdapat penjelasan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan relevansi tugas akhir dengan mata kuliah.

1.1 Latar Belakang

Teknologi informasi merupakan bagian yang tidak terpisahkan dari suatu perusahaan karena dapat membantu meningkatkan efektifitas dan efisiensi proses bisnis perusahaan. Tetapi untuk mencapai hal tersebut, diperlukan adanya pengelolaan TI yang baik dan benar agar keberadaan TI mampu menunjang kesuksesan organisasi dalam pencapaian tujuannya. Begitu pula dengan pelayanan publik bidang transportasi dan teknologi informasi bertumpu pada informasi.

Dinas Perhubungan Komunikasi dan Informatika yang selanjutnya disingkat dishubkominfo merupakan sebuah instansi kedinasan yang bertanggungjawab langsung terhadap negara. Seperti halnya instansi kedinasan pada umumnya, dinas perhubungan komunkasi dan informatika terletak di setiap kabupaten / kota. Salah satunya adalah yang terletak di kabupaten Tulungagung.

Tugas utama dari dinas perhubungan komunkasi dan informatika kabupaten Tulungagung adalah memberikan pelayanan jasa transportasi dan pelayanan informasi publik yang efektif, efisien, aman, nyaman dan tepat waktu. Selain itu terdapat bidang baru di dinas perhubungan komunkasi dan informatika Kabupaten Tulungagung yakni komunikasi dan informatika yang bertugas dalam melaksanakan pengendalian

dan pengawasan kegiatan usaha jasa Komunikasi dan jasa Informatika selain itu juga melakukan penyiapan pengembangan Teknologi Elektronik Informatika di kabupaten Tulungagung [1].

Analisis risiko digunakan organisasi untuk melakukan identifikasi risiko yang timbul akibat penggunaan teknologi informasi. Dengan melakukan analisis risko, dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung dapat membuat langkah-langkah penanganan terhadap masing-masing risiko apa saja yang mungkin akan dihadapi di kemudian hari. Selain itu, pihak rumah sakit akan lebih siap dalam menghadapi dampak yang muncul apabila risiko tersebut terjadi.

OCTAVE merupakan sebuah kerangka kerja yang memungkinkan organisasi untuk memahami, menilai dan menangani risiko keamanan informasi mereka dari perspektif organisasi. Metode OCTAVE cocok digunakan untuk menganalisi risiko keamanan informasi karena menilai terjadinya risko dari berbagai perspektif organisasi [2].

Oleh karena itu, tujuan dari penelitian ini adalah untuk melakukan identifikasi risiko yang terdapat pada dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung terkait dengan aset teknologi informasi yang digunakan dalam layanan teknologi informasi dan memberikan rekomendasi mitigasi risiko yang tepat sesuai dengan hasil identifikasi risiko serta sesuai harapan organisasi. Harapan dari penulis adalah mampu menghasilkan sebuah dokumen mitigasi risiko pada layanan teknologi informasi yang dikendalikan oleh dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan, maka rumusan masalah yang menjadi fokus untuk diselesaikan dalam penelitian ini antara lain:

1. Apa hasil identifikasi risiko pada layanan teknologi informasi yang dikendalikan dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung?
2. Apa hasil dari penilaian risiko dengan menggunakan metode FMEA?
3. Apa langkah mitigasi risiko yang sesuai untuk masingmasing risiko berdasarkan ISO 27001?

1.3 Batasan Masalah

Batasan masalah pada penelitian tugas akhir ini adalah sebagai berikut:

1. Mengidentifikasi risiko yang berkaitan dengan layanan teknologi informasi yang dikendalikan dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung berdasarkan metode OCTAVE.
2. Penilaian Risiko dilakukan dengan menggunakan metode FMEA *(Failure Mode Analysis)* .
3. Mitigasi risiko dilakukan dengan mengacu kepada ISO 27001 dan hasil diskusi dengan pihak dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung.

1.4 Tujuan Penelitian

Tujuan pembuatan tugas akhir ini adalah:

1. Mengindentifikasi, menilai, dan memitigasi risiko berdasarkan metode OCTAVE.
2. Melakukan penilaian risiko dengan metodologi FMEA untuk mengetahui risiko mana yang paling tinggi dan harus segera dilakukan penanganan dengan langkah mitigasi risiko.
3. Memberikan masukan atau rekomendasi kepada pihak dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung bagaimana langkah mitigasi risiko yang tepat sesuai dengan hasil penilaian risiko yang dapat digunakan sebagai pedoman dalam menangani permasalahan yang terjadi pada layanan teknologi informasi pada dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung.

1.5 Manfaat Penelitian

Melaluti penelitian tugas akhir ini, maka diharapkan dapat memberi manfaat sebagai berikut:

1. Menghasilkan daftar risko pada layanan teknologi dinas perhubungan komunkasi dan informatika kabupaten Tulungagaung.
2. Mampu menghasilkan dokumen mitigasi risiko untuk layanan teknologi informasi yang dapat digunakan sebagai pedoman dalam menangani permasalah yang terjadi pada layanan teknologi informasi dinas perhubungan komunikasi dan informatika kabupaten tulungagung.
3. Memberikan rekomendasi mitigasi risko berdasarkan standar ISO 27001, sehingga dinas perhubungan komunikasi dan informatika

kabupaten tulungagung dapat menanggulangi risiko ketika risiko tersebut terjadi.

1.6 Relevansi

Tugas akhir ini disusun dalam rangka memenuhi syarat kelulusan sebagai sarjana. Topik yang diangkat pada tugas akhir ini mengenai analisis risko keamanan informasi. Dimana topik ini terdapat pada matakuliah manajemen risko dan matakuliah keamanan aset informasi. Selain itu, topik ini juga membahas menganai OCTAVE dan ISO 27001 yang terdapat pada matakuliah manajemen risiko.

Halaman ini sengaja dikosongkan

BAB II
TINJAUAN PUSTAKA

Pada bagian ini dijelaskan mengenai teori yang dijadikan sebagai tinjauan pustaka dasar dalam mendukung penelitian tugas akhir ini.

2.1 Studi Sebelumnya

Sebelum melakukan penelitian tugas akhir, telah dilakukan beberapa penelitian terdahulu terkait analisis risiko pada organisasi. Berikut merupakan hasil penelitian sebelumnya:

Tabel 2.1 Studi sebelumnya

Judul: ***Information System Project-Selection Criteria Variations within Strategic Classes***	
Nama peneliti	Muhammad Bachtyar Rosyadi, Bekti Cahyo Hidayanto, S.Si., M.Kom. Hanim Maria Astuti, S.Kom., M.Sc
Tahun penelitian	2013
Hasil penelitian	Identifikasi risiko keamanan informasi dengan menggunakan metode OCTAVE pada implementasi TI di organisasi.

Hubungan dengan penelitian	Sebagai referensi utama dalam pedoman dalam mengidentifikasi risiko dengan menggunakan metode yang sama yaitu OCTAVE.
Judul: **Identifikasi, Penilaian, Dan Mitigasi Risiko Keamanan Informasi Pada Sistem Electronic Medical Record (Emr) (Studi Kasus: Aplikasi Healthy Plus Modul Rekam Medis Di Rsu Haji Surabaya)**	
Nama peneliti	Dea Anjani, Dr. Apol Pribadi Subriadi.S.T,M.T, Anisah Herdiyanti, S.Kom., M.Sc.
Tahun penelitian	2015
Hasil penelitian	Identifikasi risiko keamanan informasi dengan menggunakan metode OCTAVE dan penilaian risiko dengan menggunakan FMEA
Hubungan dengan penelitian	Sebagai referensi utama dalam pedoman dalam mengidentifikasi risiko dengan menggunakan metode yang sama yaitu OCTAVE dan penilian risko dengan menggunakan FMEA.

2.2 Profil Organisasi

Berikut ini merupakan penjelasan mengenai profil Dinas Komunikasi dan Informatika Kabupaten Tulungagung.

2.2.1 Visi, Misi dan Tujuan Organnisasi

1. Visi

Dalam konteks ini Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung memiliki kompetensi sebagai perumus kebijakan dan pelaksana kebijakan di Bidang Perhubungan Komunikasi dan Informatika. Berdasarkan pada tugas pokok dan fungsi dan RPJM Kabupaten Tulungagung Tahun 2014-2018, maka Visi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung sebagai berikut : "*Terwujudnya Pelayanan Perhubungan, dan Sistem Pelayanan Informasi Publik yang Handal dan Berdaya Saing*".

2. Misi

Misi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung dirumuskan sebagai upaya untuk mencapai Visi. Rumusan Misi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung adalah sebagai berikut :

- Meningkatkan kapasitas pelayanan transportasi darat, dan pelayanan informasi publik.
- Meningkatkan kualitas dan kuantitas sarana dan prasarana Transportasi dan Informatika.
- Meningkatkan jaringan palayanan jasa transportasi, Komunikasi dan Informatika.
- Meningkatkan daya jangkau infrastruktur jaringan teknologi informasi untuk memperluas aksebilitas masyarakat terhadap informasi dalam rangka mengurangi kesenjangan informasi.
- Meningkatkan kualitas pelayanan transportasi darat, dan peningkatan pemerataan penyebarluasan informasi publik kepada masyarakat Kabupaten Tulungagung.

- Meningkatkan kualitas SDM dibidang Transportasi, Komunikasi dan Informatika.

3. Tujuan Organisasi
   - Tujuan Organisasi

   Dalam kaitanya dengan Rencana Strategis, tujuan adalah hasil atau outcome yang ingin dicapai dalam kurun waktu yang direncanakan dalam 1 tahun dan harus mempunyai keterkaitan dengan visi dan misi yang telah ditetapkan. Untuk mewujudkan visi dan misi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung sebagaimana dikemukakan diatas, Dinas Perhubungan Komunikasi dan Informatika telah menetapkan beberapa tujuan yang ingin dicapai antara lain :

   - Terselenggaranya pelayanan angkutan yang selamat, lancar dan tertib operasional transportasi, penyebarluasan informasi.
   - Terpeliharanya sarana dan prasarana transportasi dan informatika.
   - Tersedianya kualitas sumberdaya manusia yangprofesional dan mampu menguasi perkembangan teknologi informatika.
   - Terwujudnya iklim usaha jasa Transportasi dan Komunikasi yang lebih kondusip dengan pemberdayaan masyarakat melalui pola kemitraan.
   - Meningkatkan disiplin dan ketertiban usaha pengelola jasa transportasi.
   - Meningkatkan produktifitas, keamanan dan kelancaran tugas.
   - Peningkatan kualitas pelayanan administrasi perkantoran.
   - Peningkatan kualitas pelayanan informasi dan komunikasi melalui media cetak, tradisional, tatap

muka, media massa serta media luar ruang dan teknologi modern.

- Sasaran Organisasi

Sasaran adalah penjabaran lebih lanjut dan lebih spesifik dari tujuan, oleh karena itu sasaran harus mempunyai keterkaitan dengan tujuan. Sasaran yang ingin dicapai oleh Dinas Perhubungan Komunikasi dan Informatika adalah sebagai berikut:

- Terjaga dan tersedianya fasilitas transportasi darat yang memadai.
- Terbinanya manajemen angkutan umum yang aman dan tertib.
- Tersedianya sarana dan prasarana perhubungan.
- Terwujudnya peningkatan kualitas pelayanan administrasi perkantoran.
- Terwujudnya peningkatanan kualitas pelayanan informasi dan komunikasi melalui media cetak, tradisional, tatap muka dan media massa.
- Terwujudnya peningkatan kualitas pelayanan informasi dan komunikasi melalui media luar ruang.
- Terwujudnya peningkatan kualitas pelayanan penyebaran informasi dan komunikasi melalui teknologi modern.

2.2.2 Tugas Pokok dan Fungsi Organisasi

1. Tugas Pokok dan Fungsi Organisasi

Dinas Perhubungan Komunikasi dan Informatika mempunyai tugas "melaksanakan urusan Pemerintah Daerah di bidang Perhubungan, Komunikasi dan Informatika berdasarkan Asas Otonomi dan Tugas Pembantuan". Dinas Perhubungan

Komunikasi dan Informatika dalam melaksanakan tugas sebagaimana dimaksud diatas menyelenggarakan fungsi:

- Perumusan kebijakan teknis di bidang Perhubungan, Komunikasi dan Informatika.
- Penyelenggaraan urusan Pemerintahan dan Pelayanan umum bidang Perhubungan, Komunikasi dan Informatika.
- Pembinaan dan pelaksanaan tugas di bidang Perhubungan Komunikasi dan Informatika.
- Pembinaan terhadap Unit Pelaksana Teknis Dinas Bidang Perhubungan Komunikasi dan Informatika.
- Pelaksanaan tugas lain yang diberikan oleh Bupati

2. Tugas Pokok dan Fungsi Bidang Komunikasi Informatika

Bidang Komunikasi dan Informatika mempunyai tugas sebagai berikut:

- Melaksanakan perumusan kebijakan teknis telekomunikasi dan informatika di bidang perhubungan.
- Melaksanakan pengendalian dan pengawasan kegiatan usaha jasa Telekomunikasi dan jasa Informatika.
- Melaksanakan pembinaan usaha jasa telekomunikasi dan informatika.
- Menyusunan laporan pertanggungjawaban atas pelaksanaan tugas sesuai dengan bidangnya.
- Melaksanakan tugas-tugas lain yang diberikan oleh Kepala Dinas.

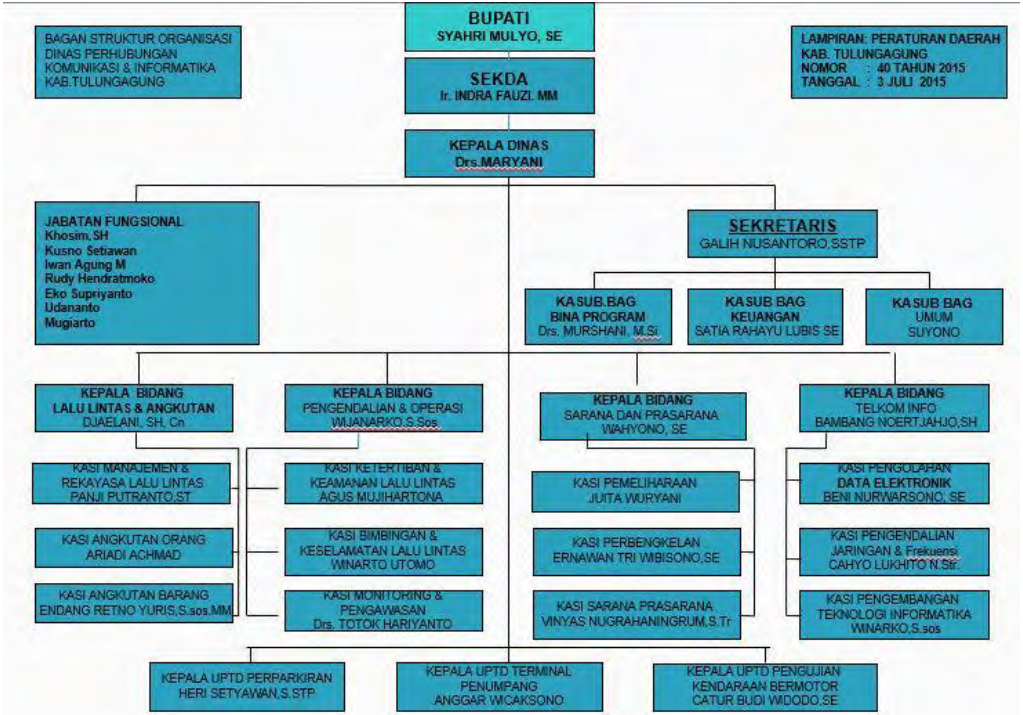
Untuk melaksanakan tugas sebagaimana dimaksud Bidang Komunikasi dan Informatika mempunyai fungsi:

- Penyiapan perencanaan, pengaturan, pengawasan dan pengendalian usaha jasa informatika.

- Perencanaan, pengaturan, pengawasan dan pengendalian usaha jasa informatika.
- Penyiapan bahan dan memproses pemberian ijin usaha jasa Komunikasi dann Infornatika.
- Penyiapan pengembangan Teknologi Elektronik Informatika.
- Penyiapan bahan evaluasi dan pelaporan di bidang Komunikasi dan informatika.

2.2.3 Struktur Organisasi

Berikut ini merupakan struktur organisasi Dinas Perhubungan, Komunikasi dan Informatika KabupatenTulungagung.



Gambar 2.1 Struktur Organisasi Dinas Perhubungan Komunikasi dan Informatika

Dari gambar struktur organisasi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung secara keseluruhan, susunan organisasi Dinas Perhubungan Komunikasi dan Informatika terdiri dari :

a. Kepala Dinas
b. Sekretariat membawahi:
    1. Sub Bagian Umum
    2. Sub Bagian Keuangan
    3. Sub Bagian Bina Program
c. Bidang Lalu Lintas dan Angkutan membawahi :
    1. Seksi Manajemen dan Rekayasa Lalu Lintas
    2. Seksi Angkutan Orang
    3. Seksi Angkutan Barang
d. Bidang Pengendalian dan Operasi membawahi :
    1. Seksi Ketertiban dan Keamanan Lalu Lintas
    2. Seksi Bimbingan dan Keselamatan Lalu Lintas
    3. Seksi Monitoring dan Pengawasan
e. Bidang Sarana dan Prasarana membawahi :
    1. Seksi Pemeliharaan
    2. Seksi Perbengkelan
    3. Seksi Pengembangan Sarana dan Prasarana
f. Bidang Komunikasi dan Informatika membawahi :
    1. Seksi Pengendalian Jaringan dan Frekuensi
    2. Seksi Pengolahan Data Elektronik
    3. Seksi Pengembangan Teknologi dan Informatika
g. Unit Pelaksana Teknis Dinas
h. Kelompok Jabatan Fungsional

Berikut ini merupakan struktur organisasi bidang komunikasi dan informatika pada dinas perhubungan, komunikasi dan informatika

Gambar 2.2 Struktur Organisasi Bidang Komunikasi dan Informatika

Pada bidang Komunikasi dan Informatika terdapat seksi-seksi dibawah bidang Komunikasi dan Informatika Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung yaitu:

1. Seksi pengelolaan data elektronik.
2. Seksi pengendalian jaringan dan frekuensi.
3. Seksi pengembangan teknologi informatika.

2.2.4 Layanan Publik Organisasi

Berikut ini merupakan layanan publik yang dikeluarkan oleh Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung:

- Peningkatan dan Intensifikasi retribusi daerah.
- Perencanaan pembangunan prasarana dan fasilitas Perhubungan.
- Rehabilitasi/ pemeliharaan prasarana dan fasilitas Perhubungan.
- Pengendalian disiplin pengoperasian angkutan umum di jalan raya.

- Penciptaan keamanan dan kenyamanan di lingkungan terminal.
    - Pengawasan peralatan keamanan dalam keadaan darurat dan perlengkapan pertolongan pertama.
    - Pemilihan dan pemberian penghargaan sopir / juru mudi/ awak angkutan umum teladan.
    - Koordinasi dalam peningkatan pelayanan angkutan.
    - Operasi gabungan, penertiban hari besar keagamaan, pasar murah dan patroli keliling.
    - Pengujian dan sertifikasi Pas Kecil kapal Nelayan.
    - Peningkatan sarana dan prasarana transportasi pedesaan di daerah tertinggal.
    - Pembangunan dan penataan tempat parkir.
    - Pengadaan fasilitas keselamatan angkutan jalan.
    - Pengadaan alat Pengujian Kendaraan Bermotor.
    - Pengujian dan penertiban kendaraan tidak bermotor (KTB).
    - Pembinaan dan pengembangan jaringan informasi melalui penyelenggaraan layanan jasa internet.
    - Pengkajian dan pengembangan system informasi melalui aplikasi telematika (pengelolaan dan pengoperasian website).
    - Pengkajian dan pengembangan system informasi melalui pemutakhiran data sarana informasi.
    - Perencanaan pengembangan kebijakan Komunikasi dan informasi melalui penertiban usaha-usaha pos dan komunikasi.
    - Pelatihan SDM dalam bidang komunikasi dan informatika pada Dinas Perhubungan Komunikasi dan Informtika.

- Penyebarluasan informasi pembangunan daerah melalui pembuatan Leaflet.
- Penyebarluasan informasi yang bersifat penyuluhan bagi masyarakat melalui Spanduk.

Berikut ini merupakan beberapa sistem informasi yang dikelola oleh dinas perhubungan komunikasi dan informatika kabupaten Tulungagung:

Tabel 2.2 Layanan Publik Teknologi Informasi

No.	Sistem Informasi	Informasi / Data	Accessible
1.	Website pemerintah kabupaten Tulungagung.	Berikut ini merupakan informasi/ data yang terdapat pada website kabupaten Tulungagung: - Informasi seputar daerah Tulungagung seperti: peta, wisata, produk unggulan, seni dan budaya serta berita. - Data Pejabat Pengelola Informasi dan	Dinas perhubungan Komunikasi dan Informatika

No.	Sistem Informasi	Informasi / Data	Accessible
		Dokumentasi (PPID). - Berita resmi statistic. - Dokumen Sistem Akuntabilitas Instansi Pemerintah (SAKIP) - Peraturan daerah (PERDA) - Data pengelolaan anggaran daerah	
2.	LPSE (Layanan Pengadaan Secara Elektronik).	Berikut ini merupakan informasi/ data yang terdapat pada layanan pengadaan secara elektronik (LPSE): - Tata cara melakukan E-tandering. - Informasi yang memuat	Panitia lelang, pejabat pembuat komitmen, dinas perhubungan komunikasi dan informatika (bidang komunikasi dan informatika).

No.	Sistem Informasi	Informasi / Data	Accessible
		daftar,jenis, spesifikasi teknis dan harga barang tertentu dari berbagai penyedia barang/jasa pemerintah - Tata cara pembelian barang/jasa melalui katalog elektronik. - Pemenang dalam proses pelelangan.	
3.	Badan pelayanan perijinan dan penanaman modal Kabupaten tulungagung	Memberikan informasi kepada masyarakat tentang mekanisme pelayanan perizinan dan jenis pelayanan perizinan yang diselenggarakan di Badan Pelayanan Perijinan dan	Badan pelayanan perijinan terpadu

No.	Sistem Informasi	Informasi / Data	Accessible
		Penanaman Modal Kabupaten Tulungagung, selain itu juga sebagai media untuk mempromosikan segala bentuk potensi dan peluang investasi yang ada di Kabupaten Tulungagung.	

2.3 Keamanan Informasi

Keamanan informasi adalah suatu upaya dalam mengamankan aset informasi dari berbagai sumber ancaman untuk memastikan keberlangsungan bisnis, meminimalisisr dampak yan terjadi akibat adanya ancaman tersebut. Dengan kata lain, keaman informasi dapat menjamin keberlangsungan bisnis, mengurangi risiko-risiko yang terjadi pada saat mengalami ancaman. Sebuah organisasi yang memiliki informasi baik informasi yang di-sharing ke public maupun dikonsumsi secara internal maka semakin besar risikoyang terjadi misalnya kerusakan, kehilangan atau terekspos nya informasi yang tidak diingikan ke public.

Organisasi keamanan informasi memiliki tiga aspek yang harus dipahami untuk bisa menerapkannya, aspek tersebut biasa disebut dengan CIA Triad [3].

Gambar 2.3 CIA Triad

1. Confidentiality

Keamanan informasi menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu. Pengertian lain dari confidentiality merupakan tindakan pencegahan dari orang atau pihak yang tidak berhak untuk mengakses informasi

2. Integrity

Keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Pengertian lain dari integrity adalah memastikan bahwa informasi tersebut masih utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak.

3. Availability

Keamanan informasi menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Pengguna dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini

memiliki otorisasi untuk mengakses informasi. Availability meyakinkan bahwa pengguna mempunyai kesempatan dan akses pada suatu informasi.

Ancaman terhadap keamanan informasi dibagi menjadi 2 ancaman yaitu ancaman aktif dan ancaman pasif [4]. Ancaman aktif mencakup:

1. Pencurian data
   Jika informasi penting yang terdapat dalam database dapat diakses oleh orang yang tidak berwenang makahasilnya dapat kehilangan informasi atau uang.
2. Penggunaan sistem secara ilegal
   Orang yang tidak berhak mengakses informasi pada suatu sistem yang bukan menjadi hak-nya, dapat mengakses sistem tersebut.
3. Penghancuran data secara ilegal
   Orang yang dapat merusak atau menghancurkan data atau informasi dan membuat berhentinya suatu sistem operasi komputer.
4. Modifikasi secara illegal
   Perubahan-perubahan pada data atau informasi dan perangkat lunak secara tidak disadari. Jenis modifikasi yang membuat pemilik sistem menjadi bingung karena adanya perubahan pada data dan perangkat lunak disebabkan oleh progam aplikasi yang merusak (malicious software).

a. Ancaman pasif mencakup:

1. Kegagalan sistem
   Kegagalan sistem atau kegagalan software dan hardware dapat menyebabkan data tidak konsisten, transaksi tidak berjalan dengan lancar sehingga data menjadi tidak lengkap atau bahkan data menjadi rusak. Selain itu, tegangan listrik yang tidak stabil dapat

membuat peralatan-peralatan menjadi rusak dan terbakar.

2. Kesalahan manusia
   Kesalahan pengoperasian sistem yang dilakukan oleh manusia dapat mengancam integritas sistem dan data.
3. Bencana alam

Bencana alam seperti gempa bumi, banjir, kebakaran, hujan badai merupakan faktor yang tidak terduga yang dapat mengancam sistem informasi sehingga mengakibatkan sumber daya pendukung sistem informasi menjadi luluhlantah dalam waktu yang singkat.

Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Contoh dari keamanan informasi antara lain [5]:

1. *Physical secu*rity adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individuatau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal security* adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup physical security.
3. *Operasional security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
4. *Communication security* adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada didalamnya. Serta kemampuan untuk memanfaatkan

media dan teknologi komunikasi untuk mencapai tujuan organisasi.

5. *Network security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Masing-masing komponen tersebut berkontribusi dalam program keamanan informasi secara keseluruhan. Jadi keamanan informasi melindungi informasi baik sistem maupun perangkat yang digunakan untuk menyimpan dan mengirimkannya.

2.4 Manajemen Risiko

Risiko muncul karena adanya ketidakpastian yang disebabkan karena ketidaktersediaan informasi yang cukup tentang apa yang akan terjadi. Ketidakpastian yang menimbulkan akibat yang merugikan disebut risiko (Risk), sedangkan ketidakpastian yang menguntungkan disebut peluang (Opportunity).

Manajemen risiko adalah proses pengelolaan risiko yang mencakup identifikasi, evaluasi, dan pengendalian risiko yang dapat mengancam kelangsungan usaha atau aktivitas perusahaan. Manajemen risiko TI adalah penerapan manajemen risiko dengan konteks teknologi informasi untuk mengelola risiko TI, yaitu: Risiko bisnis yang terkait dengan penggunaan, kepemilikan, operasi, keterlibatan, pengaruh dan penerapan TI dalam suatu perusahaan.

Manajemen risiko TI dapat dianggap sebagai komponen dari sistem manajemen risiko perusahaan yang lebih luas. Pembentukan, pemeliharaan dan pembaruan terus menerus Information Security Management System atau sistem manajemen keamanan informasi memberikan indikasi kuat bahwa suatu perusahaan menggunakan pendekatan sistematis

untuk identifikasi, penilaian dan manajemen risiko keamanan informasi.

Manajemen risiko merupakan suatu proses yang sistematis dan terorganisir mulai dari identifikasi risiko, analisa risiko, pengurangan atau peniadaan risiko secara efektif untuk mencapai sasaran/tujuan. Adapun yang menjadi tujuan manajemen risiko adalah sebagai berikut:

- Membatasi kemungkinan-kemungkinan dari ketidakpastian
- Membuat langkah-langkah yang lebih mengarah pada tindakan proaktif dalam memandang kemungkinan ancaman dan kerugian yang besar.
- Membatasi kerugian dan ketidakpastian pada stake holder
- Menjaga kesinambungan program operasi, sehingga tidak terganggu dengan kejadian-kejadian yang belum terantisipasi sebelumnya.
- Menjalankan program manajemen risiko secara efektif sehingga mempunyai pengaruh yang menguntungkan dan bukan menimbulkan biaya baru.

2.4.1 Aset

Aset adalah sumber daya ekonomi yang dikuasai dan/atau dimiliki oleh pemerintah sebagai akibat dari peristiwa masalalu dan dari mana manfaat ekonomi dan/atau social dimasa depan diharapkan dapat diperoleh, baik oleh pemerintah maupun masyarakat, serta dapat diukur dengan satuan uang, termasuk sumber daya non keuangan yang diperlukan untuk penyediaan jasa bagi masyarakat umum dan sumber-sumber daya yang dipelihara karena alasan sejarah dan budaya [6].

Aset informasi merupakan sekumpulan pengetahuan yang diatur dan dikelola sebagai satu kesatuan oleh organisasi sehingga dapat dipahami, dibagikan, dilindungi dan dapat dimanfaatkan dengan baik. Aset informasi pada penelitian ini

akan mengacu pada definisi komponen Sistem Informasi yang akan dijelaskan berikut ini:

- Orang *(People)*

Dalam tugas akhir ini komponen yang akan diidentifikasi adalah karyawan yang mengoperasikan layanan teknologi informasi yang dikelola oleh dians perhubungan komunikasi dan informatika kabupaten Tulungagung.

- Data

Dalam dunia teknologi informasi, yang disebut data adalah individu dari sebuah database, yang disimpan dalam basis data untuk keperluan penyediaan informasi dalam tujuannya untuk mendukung perusahaan melakukan kegiatan operasional.

- Perangkat Keras *(Hardware)*

Mencakup piranti fisik, seperti: komputer, printer, monitor. Berperan penting sebagai media penyimpanan vital dalam dunia system informasi. Setiap perusahaan yang memiliki teknologi informasi yang maju pasti memiliki hardware yang komplek dan berjumlah banyak.

- Perangkat Lunak *(Software)*

Merupakan sekumpulan instruksi yang dapat mempengaruhi kinerja perangkat keras dan memproses data. Tujuan adanya perangkat ini adalah untuk mengolah, menghitung dan memanipulasi data agar menghasilkan informasi yang berguna.

- Jaringan *(Network)*

Merupakan system penghubung yang memungkinkan suatu sumber (utamanya perangkat keras & lunak) digunakan secara bersama-sama, meskipun di waktu dan tempat yang berbeda.

- Prosedur *(Procedure)*

Prosedur : sekumpulan aturan yang dipakai untuk mewujudkan pemrosesan data dan pembangkitan keluaran yang dikehendaki

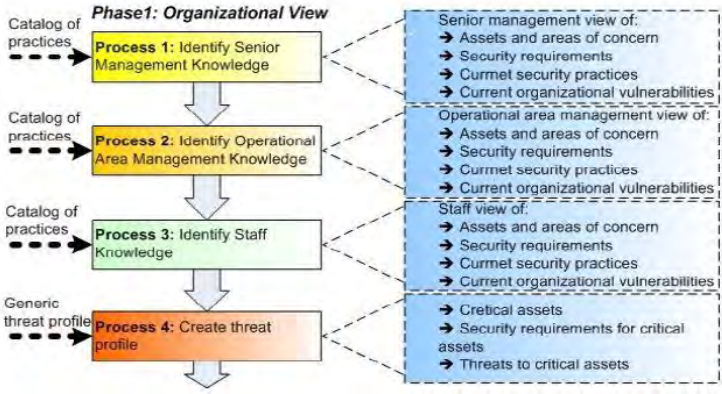
2.4.2 OCTAVE

OCTAVE merupakan sebuah kerangka kerja yang memungkinkan organisasi untuk memahami, menilai dan menangani risiko keamanan informasi mereka dari perspektif organisasi. OCTAVE bukanlah sebuah produk, melainkan merupakan metodologi untuk mengidentifikasi, memprioritaskan dan mengelola risiko keamanan informasi. OCTAVE adalah kerangka keamanan untuk menentukan tingkat risiko dan perencanaan pertahanan terhadap serangan cyber. Kerangka tersebut mendefinisikan metodologi untuk membantu organisasi meminimalkan kemungkinan terjadinya ancaman, menentukan kemungkinan konsekuensi dari serangan dan menangani serangan.

OCTAVE berguna dalam mencegah kerugian, bukan memperbaiki kerusakan. OCTAVE hanya dapat menghitung risiko terjadinya peristiwa tertentu. Mengembangkan rencana darurat , yang harus diterapkan dalam kasus peristiwa yang tidak diperkirakan. Strategi peningkatan keamanan berdasarkan metodologi OCTAVE adalah pedoman yang baik untuk perusahaan dan karyawan, karena metode ini memberitahu apa yang harus dilakukan untuk meminimalkan risiko kerugian yang terjadi.OCTAVE memiliki 3 fase [2], yaitu:

- Fase 1: Build Asset-Based Threat Profiles

Tim analisis menentukan aset kritis dan apa yang saat ini sedang dilakukan untuk melindungi mereka. Persyaratan keamanan untuksetiap aset kritis kemudian diidentifikasi. Akhirnya, kerentanan organisasi dengan praktek-praktek yang ada dan profil ancamanuntuk setiap aset kritis ditetapkan.



Gambar 2.4 Fase Organizational View

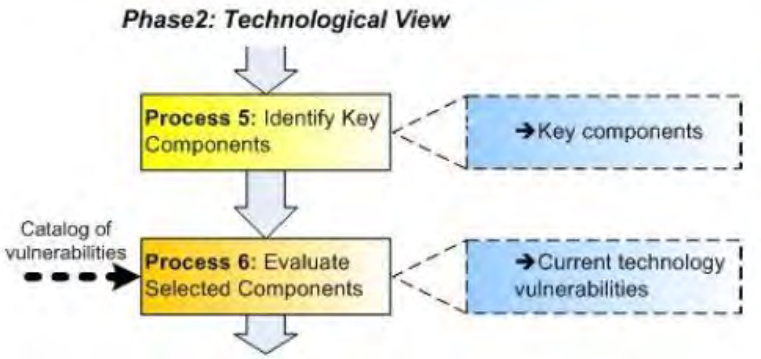
Terdapat 4 proses pada fase ini, yaitu:

- Proses 1: Identify Senior Management Knowledge. Para peserta dalam proses ini adalah manajer senior organisasi.
- Proses 2: Identify Operational Area Management Knowledge. Para peserta dalam proses ini adalah manajer wilayah operasional.
- Proses 3: Identify Staff Knowledge. Para peserta dalam proses ini adalah anggota staf organisasi. Anggota staf TI biasanya berpartisipasi dalam workshop terpisah dari yang dihadiri oleh anggota staf umum.
- Proses 4: Create Threat Profiles. Para peserta dalam proses ini adalah anggota tim analisis.

- Fase 2: Identify Infrastructure Vulnerabilities

Tim analisis mengidentifikasi jalur akses jaringan dan kelas komponen IT yang terkait dengan setiap aset kritis. Tim kemudian menentukan sejauh mana masing-masing kelas dari komponen yang tahan terhadap serangan jaringan dan menetapkan kerentanan teknologi yang

mengekspos aset kritis. Fase 2 juga disebut sebagai "technological view" dari Metode OCTAVE , karena fase ini fokus pada infrastruktur komputasi organisasi.



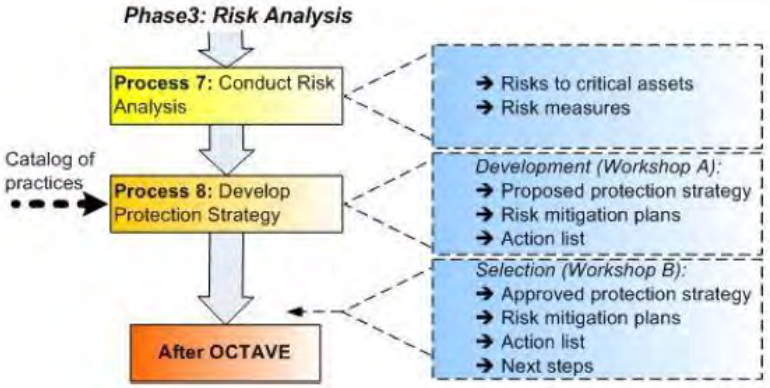
Gambar 2.5 Fase Technological View

- Proses 5: Identify Key Components. Para peserta dalam proses ini adalah tim analisis dan beberapa anggota staf TI. Tujuan dari proses 5 adalah untuk memilih komponen infrastruktur yang akan diperiksa untuk kelemahan teknologi selama proses 6. Proses 5 terdiri dari dua kegiatan, yaitu mengidentifikasi kelas kunci komponen dan mengidentifikasi komponen infrastruktur untuk diperiksa .
- Proses 6: Evaluate Selected Components. Para peserta dalam proses ini adalah tim analisis dan beberapa anggota staf TI. Tujuan dari proses 6 adalah untuk mengidentifikasi kelemahan teknologi dalam komponen infrastruktur yang diidentifikasi selama proses 5. Kelemahan teknologi memberikan indikasi betapa rapuhnya infrastruktur komputasi organisasi. Proses 6 terdiri dari dua kegiatan, yaitu menjalankan alat evaluasi kerentanan pada komponen infrastruktur yang dipilih, meninjau kerentanan teknologi dan meringkas hasilnya.

- Fase 3: Develop Security Strategy and Plans

Tim analisis menetapkan risiko terhadap aset kritis organisasi berbasis analisis informasi yang dikumpulkan dan kemudian memutuskan apa yang harus dilakukan. Tim ini menciptakan strategi perlindungan bagi organisasi dan rencana mitigasi untuk mengatasi risiko yang telah diidentifikasi. Tim juga menentukan 'langkah selanjutnya' yang diperlukan untuk dilaksanakan dan mendapatkan persetujuan manajemen senior pada hasil dari keseluruhan proses.

Fase 3 dirancang untuk memahami informasi yang telah dikumpulkan sejauh ini dalam evaluasi yang telah dilakukan. Fase ini mengembangkan strategi keamanan dan rencana strategi yang dirancang untuk mengatasi risiko dan permasalahan unik organisasi.



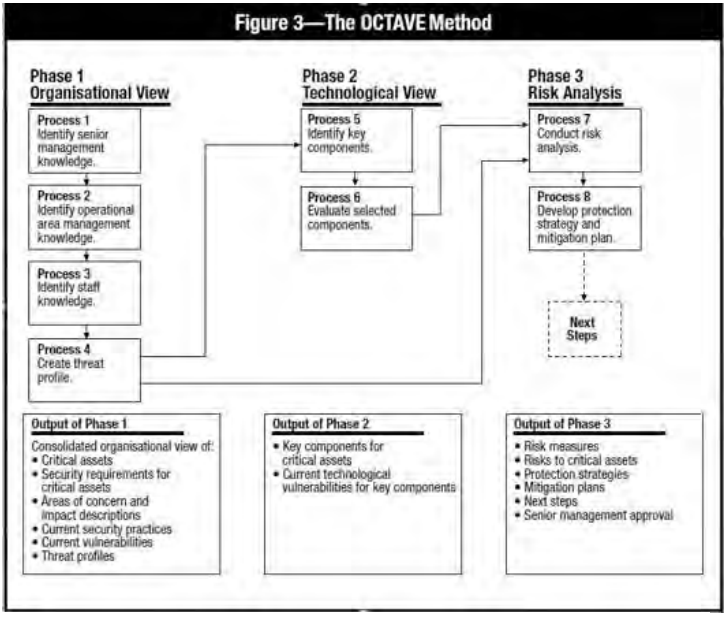
Gambar 2.6 Fase Risk Analysis

- Proses 7: Conduct Risk Analysis. Para peserta dalam proses 7 adalah anggota tim analisis, tujuan dari proses ini adalah untuk mengidentifikasi dan menganalisis risiko terhadap aset kritis organisasi. Proses 7 meliputi tiga kegiatan, yaitu mengidentifikasi dampak

dari ancaman terhadap aset kritis, membuat kriteria evaluasi risiko, dan mengevaluasi dampak dari ancaman terhadap aset kritis.

- Proses 8: Develop Protection Strategy. Proses 8 mencakup dua workshop. Para peserta dalam workshop pertama untuk proses 8 adalah anggota tim analisis dan beberapa anggota organisasi. Tujuan dari proses 8 adalah untuk mengembangkan strategi perlindungan bagi organisasi, rencana mitigasi untuk risiko terhadap aset kritis, dan daftar tindakan tindakan jangka pendek.

Gambar berikut merepresentasikan gambaran metode OCTAVE yang berisi fase, proses, dan output dari setiap fase yang ada:



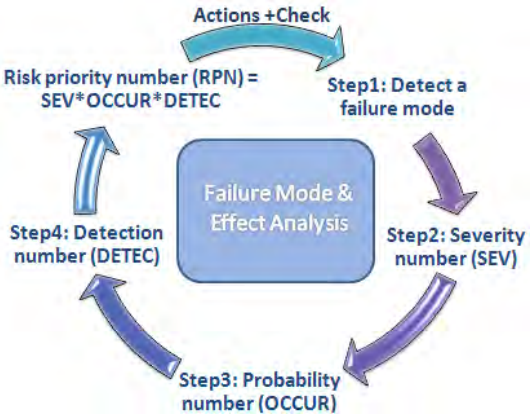
Gambar 2.7 Metode OCTAVE

2.4.3 FMEA

Failure Mode and Effect Analysis (FMEA) merupakan metode yang digunakan menganalisa potensi kesalahan atau kegagalan dalam sistem atau proses, dan potensi yang teridentifikasi akan diklasifikasikan menurut besarnya potensi kegagalan dan efeknya terhadap proses.Tujuan dari FMEA adalah untuk meminimalisir dan menghindari terjadinya kesalahan maupun kegagalan. FMEA mengidentifikasi tiga hal [7]:

1. Penyebab kegagalan dari sistem, desain produk, serta proses selama siklus hidupnya,
2. Efek dari kegagalan,
3. Tingkat kekritisan efek dari suatu kegagalan.

Proses yang dilakukan dalam penerapan FMEA adalah mengukur potensi terjadinya kesalahan maupun kegagalan melalui tiga komponen. Berikut merupakan diagram alur dari tahapan proses FMEA.



Gambar 2.8 Diagram Alur FMEA

Komponen-komponen kegagalan tersebut adalah sebagai berikut.

1. ***Severity Number* atau SEV(tingkat keparahan)/*Impact***

Tingkat keparahan merupakan ukuran dalam memperkirakan subjektif numeric, seberapa parah penggunaakan merasakan efek dari kegagalan tersebut. Berikut merupakan ukuran parameter dari SEV.

Tabel 2.3 Skala Tingkat Keparahan

Dampak	Kriteria	Ranking
Berbahaya: Tanpa Peringatan	Melukai pekerja/pihak ketiga/customer	10
Berbahaya: Tanpa Peringatan	Kegiatan yang tidak diperbolehkan oleh perusahaan	9
Sangat Tinggi	Kesalahan dalam penggunaan alat yang ada	8
Tinggi	Menyebabkan complain dari pihak ketiga/customer	7
Sedang	Menyebabkan kerugian untuk perusahaan	6
Rendah	Menyebabkan penurunan kinerja dari pekerja	5
Sangat Rendah	Menyebabkan sedikit kerugian	4
Minor	Menyebabkankan gangguan kecil yang dapat diatasi tanpa kehilangan sesuatu	3
Sangat Minor	Tanpa disadari dan memberikan dampak kecil pada kinerja	2
Tidak berdampak	Tanpa disadari dan tidak mempengaruhi kinerja	1

2. *Probability Number* atau OCCUR(tingkat kejadian)/*Likelihood*

Tingkat kejadianmerupakan ukuran dalam memperkirakan probabilitas penyebab kemungkinan terjadinya risiko yang akan menghasilkan modus kegagalan atau yang dapat menyebabkan akibat tertentu. Berikut merupakan ukuran parameter dari OCCUR.

Tabel 2.4 Skala Tingkat Kejadian

Probabilitas Risiko	Periode Waktu	Ranking
Sangat tinggi	Lebih dari satu kali tiap harinya	10
Failure is almost inevitable	Satu kali dalam 4 hari	9
Tinggi: secara umum terkait dengan proses yang sebelumnya sering kali gagal	Satu kali dalam seminggu	8
Proses yang sering kali gagal	Satu kali dalam sebulan	7
Moderate: secara umum terkait dengan proses yang sebelumnya sering kali gagal	Satu kali setiap 3 bulan	6
Proses sebelumnya yang memiliki	Satu kali setiap 6 bulan	5
Kegagalan yang pernah terjadi, tapi tidak dalam proporsi yang besar	Satu kali dalam setahun	4
Rendah: Kegagalan yang terisolasi terkait dengan proses serupa	Satu kali dalam 1-3 tahun	3

Sangat rendah: Kegagalan hanya terisolasi terkait dengan proses yang hampir sama	Satu kali dalam 3-6 tahun	2
Remote: Kegagalan tidak mungkin terjadi. Tidak ada kegagalan yang pernah terkait dengan proses yang hampir serupa	Satu kali dalam 6-100 tahun	1

3. *Detection Number* atauDETEC(Deteksi)/*Cause*

Tingkat deteksi meruapakan ukuran dari sejauh mana peluang potensi kegagalan dapat terdeteksi. Pengukuran deteksi adalah perkiraan subjektif numerik tentang kontrol untuk mencegah atau mendeteksi penyebab kegagalan sebelum kegagalan mencapai pelanggan.Berikut merupakan ukuran parameter dari DETEC.

Tabel 2.5 Skala Deteksi

Deteksi	Kriteria	Ranking
Hampir tidak mungkin	Pengontrolan tidak dapat mendeteksi kegagalan	10
Sangat kecil	Sangat jauh kemungkinan pengontrol akan menemukan potensi kegagalan	9
Kecil	Jarang kemungkinan pengontrol akan menemukan potensi kegagalan	8
Sangat rendah	Kemungkinan pengontrol untuk mendeteksi kegagalan sangat rendah	7
Rendah	Kemungkinan pengontrol untuk mendeteksi kegagalan rendah	6

Sedang / Moderat	Kemungkinan pengontrol untuk mendeteksi kegagalan sedang	5
Cukup Tinggi	Kemungkinan pengontrol untuk mendeteksi kegagalan cukup tinggi	4
Tinggi	Kemungkinan pengontrol untuk mendeteksi kegagalan tinggi	3
Sangat tinggi	Kemungkinan pengontrol untuk mendeteksi kegagalan sangat tinggi	2
Hampir pasti	Kegagalan dalam proses tidak dapat terjadi karena telah dicegah melalui system solusi	1

2.5 ISO 27001

Standar ISO 27001 diterbitkan pada bulan Oktober 2005, pada dasarnya ISO ini dikeluarkan untuk menggantikan standar BS7799-2 yang lama. Ini adalah spesifikasi untuk ISMS, Information Security Management System. ISMS adalah seperangkat unsur yang saling terkait yang organisasi gunakan untuk mengelola dan mengendalikan risiko keamanan informasi dan untuk melindungi dan menjaga kerahasiaan, integritas, dan ketersediaan informasi (SYfirazaal). Elemen-elemen ini mencakup semua kebijakan, prosedur, proses, rencana, praktek, peran, tanggung jawab, sumber daya, dan struktur yang digunakan untuk mengelola risiko keamanan dan untuk melindungi informasi.

Tujuan utama dari ISO 27001 adalah untuk membangun, mempertahankan, mengembangkan, dan terus meningkatkan sistem informasi manajemen yang efektif. ISO 27001 menjelaskan bagaimana mengelola keamanan informasi melalui sistem manajemen keamanan informasi. Sistem manajemen tersebut terdiri dari empat fase yang harus terus

dilakukan untuk meminimalkan risiko terhadap kerahasiaan, integritas dan ketersediaan informasi.
Fase-fase tersebut adalah sebagai berikut [8]:

Gambar 2.9 Siklus PDCA

- The Plan Phase

Fase ini berfungsi untuk merencanakan dasar organisasi keamanan informasi, tujuan yang ditetapkan untuk keamanan informasi dan memilih kontrol keamanan yang sesuai.

- The Do Fase

Fase ini termasuk melakukan segala sesuatu yang direncanakan selama fase sebelumnya.

- The Check Phase

Tujuan dari tahap ini adalah untuk memantau fungsi melalui berbagai "channels", dan periksa apakah hasil memenuhi tujuan yang telah ditetapkan.

- The Act Phase

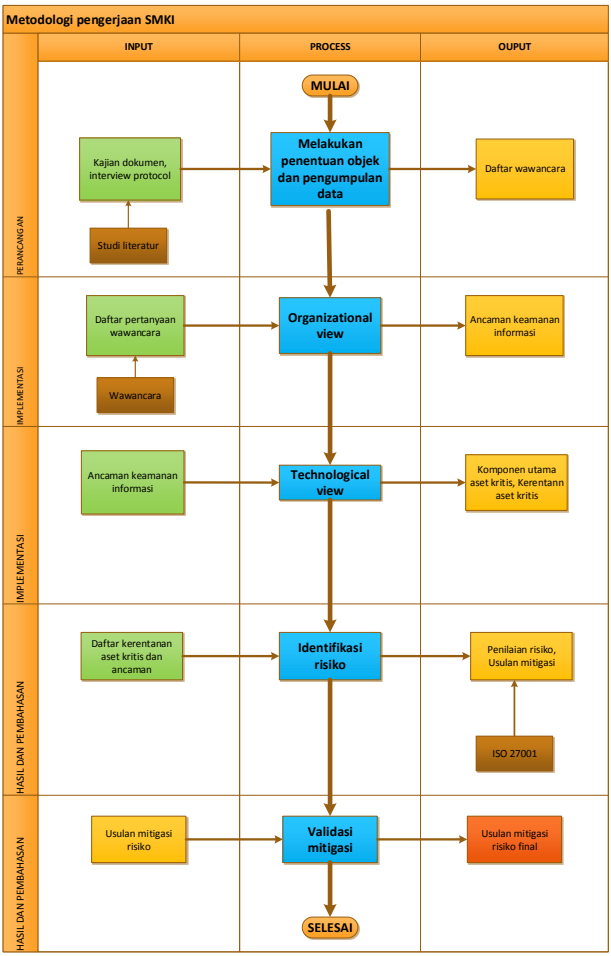
Tujuan dari tahap ini adalah untuk meningkatkan segala sesuatu yang diidentifikasi sebagai non-compliant pada fase sebelumnya.
Siklus dari empat fase ini tidak pernah berakhir, dan semua kegiatan harus dilaksanakan secara siklus untuk menjaga keefektifan efektifitas mitigasi.

Beberapa manfaat dari ISO 27001 adalah:

- Menyimpan informasi rahasia secara aman.
- Memberikan rasa percaya pada pelanggan dan stakeholder dalam bagaimana mengelola risiko.
- Memungkinkan untuk pertukaran informasi secara.
- Memberikan competitive advantage.
- Meningkatkan kepuasan pelanggan yang meningkatkan retensi klien.
- Konsistensi dalam pengiriman layanan atau produk.
- Mengelola dan meminimalkan eksposur risiko.
- Membangun budaya keamanan.
- Melindungi perusahaan, aset, pemegang saham dan direksi.

BAB III
METODOLOGI

Pada bagian ini dijelaskan mengenai metodologi yang digunakan sebagai tahap-tahap yang dilakukan dalam penelitian tugas akhir. Berikut merupakan metode pengerjaan tugas akhir.



Gambar 3.1 Metodologi

3.1 Melakukan penentuan objek dan pengumpulan data

Pada tahap menggunakan fase pertama melakukan penentuan objek dan pengumpulan data yaitu melakukan analisis objek tujuan penelitian. Hasil dari fase pertama adalah interview protocol yang akan digunakan untuk melakukan analisis risiko pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.

Melakukan Studi Literatur

Studi litiratur yang digunakan dalam penyusunan tugas akhir ini terkait dengan peraturan kabupaten yang dikeluarkan oleh bupati, aturan-aturan yang dikeluarkan oleh kementerian republik Indonesia serta tugas pokok fungsi dinas perhubungan komunikasi dan informatika kabupaten Tulungagung.

3.2 Organizational view

Fase ini merupakan tahapan untuk membuat profil ancaman *(threat profile)* dengan cara menentukan aset yang penting bagi organisasi dan kebutuhan pengamanannya. Penentuan aset yang penting dilakukan melalui pengumpulan informasi tentang aset, kebutuhan keamanan, ancaman, dan kekuatan serta kelemahan organisasi dari beberapa tingkatan manajemen mulai dari senior manajer, operasional, sampai dengan staf. Hasil dari fase ini adalah pendefinisian kebutuhan keamanan informasi dan profil ancaman untuk aset – aset penting.

3.3 Technological view

Pada tahapan *Technological View* dilakukan identifikasi proses bisnis dan profil ancaman terhadap asset kritis yang didukung layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung dan identifikasi kelemahan infrastruktur.

3.4 Identifikasi risiko

Pada tahap ini melakukan identifiksi risiko yaitu melakukan penilaian risiko dan melakukan mitigasi risiko berdasarkan ISO 27001 serta diskusi bersama dengan pihak Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung. Pembahasan hasil identifikasi risiko dibuat berdasarkan daftar ancaman yang terjadi pada asset-aset yang telah diidentifikasikan sebelumnya.

3.5 Validasi

Pada tahap ini validasi yang telah selesai dilakukan pengecekan kesesuaian dengan keadaan yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung. Validasi dilakukan dengan cara mewawancarai penanggungjawab pengelolaan teknologi informasi yang ada pada dinas tersebut. Sehingga menghasilkan mitigasi serta usulan kontrol yang sesuai dengan harapan dinas perhubungan komunikasi dan informatika kabupaten Tulungagung.

Halaman ini sengaja dikosongkan

BAB IV
PERANCANGAN

Pada bagian ini menjelaskan metode perancangan tugas akhir. Perancangan pada bagian ini diperlukan sebagai panduan dalam melakukan penelitian tugas akhir.

4.1 Perancangan Studi Kasus

Studi kasus dalam penelitian merupakan sebuah hal penting. Menurut Gummeson pentingnya studi kasus dalam penelitian adalah kesempatan untuk melihat proses secara menyeluruh, mempelajari berbagai aspek, menguji hubungan satu sama lain dan menggunakan kapasitas peneliti untuk memahami. Studi kasus adalah cara unik yang bertujuan untuk mengamati fenomena alam yang ada pada sebuah set data [9]. Terdapat tiga kategori studi kasus, yaitu:

1. Studi kasus eksplorasi (menggali), yaitu melakukan eksplorasi terhadap fenomena apapun dalam data yang berfungsi sebagai tempat tujuan untuk peneliti.
2. Studi kasus deskriptif, yairu digunakan untuk menggambarkan fenomena alamiah yang terjadi pada data.
3. Studi kasus explanatory (memperjelas), yaitu digunakan untuk menjelaskan fenomena dalam data secara jelas mulai dari hal dasar hingga mendalam.

Selain itu, juga ada kategori studi kasus menurut McDonough, kategori tersebut adalah kategori interpretatif dan evaluatif. Studi kasus interpretatif dapat digunakan untuk menafsirkan data dengan mengembangkan kategori konseptual, dan juga dapat mendukung atau menentang asumsi yang dibuat terkait data – data tersebut. Sementara, studi kasus evaluatif digunakan untuk menilai fenomena yang ditemukan dalam data [10].

Dalam pengerjaan tugas akhir ini menggunakan kategori studi kasus eksplorasi atau penggalian. Dari rumusan masalah, mengindikasikan perlunya studi kasus, untuk itu tujuan adanya studi kasus adalah untuk mendapatkan fenomena yang terjadi dan dijadikan sebagai dasar analisis risiko.

4.2 Subjek dan Objek Penelitian

Penilitian ini dilakukan pada Dinas Perhubungan Komunikasi dan Informatika kabupaten Tulungagung yang merupakam salah satu layanan publik terkait perhubungan dan teknologi informasi. Objek yang akan diteliti adalah proses layanan teknologi informasi yang dikelola dinas Dinas Perhubungan Komunikasi dan Informatika kabupaten Tulungagung. Layanan teknologi informasi tersebut nantinya akan dibuatkan dokumen sistem manajemen keamanan informasi dengan menggunakan metode octave untuk penggalian aset kritis dan indentifikasi risiko serta menggunakan ISO 27001 sebagai kontrolnya. Sehingga layanan publik teknologi informasi yang terdapat pada dinas terkait akan menjadi lebih baik. Selama melakukan penelitian ini, penulis mendapat bantuan dari pihak dinas perhubungan komunikasi dan informatika kabupaten Tulungagung terutama bidang komunikasi dan informatika yang merupakan narasumber utama dalam proses penggalian kebutuhan.

4.3 Perancangan Perangkat Penggalian Data

Pada bagaian ini merupakan perancangan perangkat penggalian data kondisi kekinian organisasi, sehingga dapat mengetahui gambaran terkait layanan publik teknologi informasi pada Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung. Gambaran yang ingin diketahui diketahui antara lain:

1. Layanan publik terkait teknologi informasi yang dikelola organisasi.

2. Aset teknologi informasi yang dimiliki organisasi.
3. Pengelolaan keamanan informasi didalam organisasi

Perancangan Interview Protocol

Perancangan perangkat penggalian data yang akan dilakukan meliputi perancangan *interview protocol*. Perangkat tersebut akan digunakan ketika melakukan wawancara.

Perancangan *interview protocol* merupakan perancangan daftar pertanyaan yang digunakan sebagai panduan penelitian agar ketika melakukan wawancara tidak bias dan terarah. *Interview protocol* ini nantinya akan digunakan untuk menggali kondisi kemanan organisasi pada Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung.

Perancangan awal pada *interview protocol* adalah perlu menambahkan informasi terkait pelaksanaan interview dan narasumber yang akan dituju, sebelum merancang daftar pertanyaan. Adapun tujuan dari penambahan informasi pelaksanaan interview dan narasumber ini adalah untuk mendokumentasikan hasil interview dengan baik, karena dapat memberikan informasi kapan dan dimana pelaksanaan interview dan siapa yang dapat memberikan informasi – informasi terkait kondisi kemanan organisasi pada Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung. Konten dari informasi pelaksanaan interview dan narasumber dapat dilihat pada tabel berikut ini:

Tabel 4.1 Konten Informasi Pelaksanaan Wawancara

Informasi Pelaksanaan Interview	
Interviewer	:
Narasumber	:

Hari, Tanggal	:
Pukul	:
Lokasi	:
Informasi Narasumber	
Nama	:
Jabatan	: :
Instansi	:
Lama bekerja	:

Interview protocol digunakan untuk idnetifikasi risiko pada organisasi dan pengelolaan keamanan informasi. Nantinya interview protocol akan mengacu pada metode octave. Didalam metode octave terdapat 3 fase untuk mengatahu aset kritis organisasi dan pengelolaan keamanan informasi. Berikut adalah ketigas fase metode octave:

- **F**ase 1 Orgaizational View

Tujuannya adalah untuk mengetahui aset kritis organisasi, keamanan untuk aset krtis, fokus area, keamanan informasi yang telah diimplementasikan**.** Pada fase ini peneliti melakukan *interview* dengan kepala bidang teknologi informasi pada dinas perhubungan komunikasi dan informatika kabupaten Tulungangunga. Berikut ini merupakan interview protocol fase 1:

Tabel 4.2 Interview Protocol Fase Organization View

No	ORGANIZATION VIEW
	Critical Assets
1	**Pertanyaan:**
	Proses bisnis apa yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
2	**Pertanyaan:**
	Aset apa saja yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
3	**Pertanyaan:**
	Aset apa yang paling penting di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
4	**Pertanyaan:**
	Seberapa besar pengaruh jaringan terhadap keberlangsungan proses bisnis yang ada pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
5	**Pertanyaan:**
	Sistem informasi apa yang terdapat pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
7	**Pertanyaan:**
	Siapa saja yang mempunyai kepentingan menggunakan aplikasi dan layanan TI?
	Jawaban:
	Security Requirement for Critical Assets
1	**Pertanyaan:**
	Apakah aplikasi dan layanan TI di lingkungan dinas perhubungan komunikasi dan informatika sudah

	memberikan *checklist* terkait kebutuhan keamanan aset informasi yang dimiliki? a. Jika sudah, apa saja kebutuhan keamanan yang dilihat dari *checklist* tersebut yang sudah terpenuhi? b. Jika belum, perlukan adanya *checklist* terkait kebutuhan keamanan aset informasi yang dimiliki?
	Jawaban:
2	**Pertanyaan:**
	Adakah aturan dalam melakukan pengamanan terkait akses informasi pada aplikasi dan layanan TI?
	Jawaban:
3	**Pertanyaan:**
	Apakah ada pemeriksaan secara rutin terhadap keamanan aset?
	Jawaban:
4	**Pertanyaan:**
	Apakah ada kegiatan maintenance pada aset?
	Jawaban:
5	**Pertanyaan:**
	Apakah ada mekanisme untuk mencegah pembobolan aset?
	Jawaban:
6	**Pertanyaan:**

	Apakah sensitifitas informasi dilindungi oleh tempat penyimpanan yang aman?
	Jawaban:
	Threat to Critical Assets
1	**Pertanyaan:**
	Apakah aset informasi dinas perhubungan komunikasi dan informatika pernah mengalami ancaman? a. Jika pernah, apa saja ancaman yang pernah dialami? b. Jika belum, ancaman apakah yang memungkinkan terjadi?
	Jawaban:
2	**Pertanyaan:**
	Berikan contoh bagaimana pihak dalam yang bertindak secara tidak sengaja dapat menggunakan akses fisik untuk mengancam sistem ini?
	Jawaban:
3	**Pertanyaan:**
	Bagaimana melakukan pencegahan terhadap ancaman aset TI?
	Jawaban:
4	**Pertanyaan:**
	Seberapa sering terjadinya server down pada server?
	Jawaban:

5	**Pertanyaan:**
	Seberapa sering terjadinya pembobolan data?
	Jawaban:
6	**Pertanyaan:**
	Apakah pada aplikasi dan layanan TI dilakukan *update* anti virus?
	Jawaban:
7	**Pertanyaan:**
	Apakah ada SOP untuk meng*update* sistem tersebut?
	Jawaban:
	Current Security Practice
1	**Pertanyaan:**
	Apakah ada informasi mengenai aplikasi dan layanan TI di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
2	**Pertanyaan:**
	Apakah aplikasi dan layanan TI menerapkan *framework* atau standar keamanan khusus aset informasi? a. Jika iya, standart atau *framework* apa yang digunakan? b. Jika tidak, perlukan adanya standart atau *framework* khusus pengamanan aset informasi?
	Jawaban:

3	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung sudah melakukan penilaian risiko untuk keamanan informasi?
	Jawaban:
4	**Pertanyaan:**
	Apakah bidang komunikasi dan informatika menerima dan bertindak atas laporan rutin dari informasi yang berhubungan dengan keamanan?
	Jawaban:
5	**Pertanyaan:**
	Apakah kendala dalam melakukan implementasi standart atau *framework* pengamanan aset informasi pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
6	**Pertanyaan:**
	Apakah di dinas perhubungan komuniasi dan informatika sudah memiliki kebijakan dan prosedur dalam melindungi informasi ketika bekerja sama dengan perusahaan lain?
	Jawaban:
	Current Organizational
1	**Pertanyaan:**

	Apa masalah yang sering terjadi di dinas perhubungan komunikasi dan informatika terkait *asset informasi?*
	Jawaban:
2	**Pertanyaan:**
	Pernahkah terjadi pencurian informasi pada dinas perhubungan komunikasi dan informatika a. Jika pernah, informasi apa yang telah dicuri? Apa penyebab *asset informasi* tersebut bermasalah? b. Jika belum, informasi apa saja yang memungkinkan terjadinya pencurian?
	Jawaban:
3	**Pertanyaan:**
	Apakah kapasitas server yang dimiliki dinas perhubungan komunikasi dan informatika sudah mencukupi?
	Jawaban:
4	**Pertanyaan:**
	Berapa kali dalam setahun dinas perhubungan komunikasi dan informatika melakukan evaluasi terhadap keamanan teknologi informasi?
	Jawaban:
5	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika sudah melakukan verifikasi untuk setiap divisi dalam mengurus hak akses dan otorisasi?
	Jawaban:

6	**Pertanyaan:**
	Bagaimana kode etik yang diterapkan pada dinas perhubungan komunikasi dan informaika terkait pengamanan aset informasi?
	Jawaban:

- **F**ase 2 Technological View

Tujuananya adalah untuk mengetahui komponen utama dari aaset kritis, teknologi untuk mengamankan komponen utama aset kritis. Pada fase ini peneliti melakukan *interview* dengan staf bidang IT. Berikut adalah pertanyaan digunakan untuk melakukan fase 2:

Tabel 4.3 Interview Protocol Fase Technological View

	TECHNOLOGICAL VIEW
	Key Component
1	**Pertanyaan:**
	Perangkat IT apa saja yang dimiliki oleh dinas perhubungan komunikasi dan informatika kabupaten Tulunggung?
	Jawaban:
	Current Technology Vulnerability
1	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika terdapat prosedur untuk menjaga kerentanan teknologi seperti meninjau sumber informasi, mengelola keamanan tempat penyimpanan dan mengidentifikasi komponen infrastruktur?

	Jawaban:
2	**Pertanyaan:**
	Bagaimana bentuk penanggulangan terkait adanya gangguan TI?
	Jawaban:
3	**Pertanyaan:**
	Apakah dinas komunikasi dan informatika menjadwalkan dan melakukan evaluasi kerentanan TI secara berkala?
	Jawaban:
4	**Pertanyaan:**
	Apakah dinas komunikasi dan informatika memiliki dokumen mengenai jenis-jenis kerentanan dan metode serangannya?
	Jawaban:
5	**Pertanyaan:**
	Siapa yang bertanggung jawab memanajemen kerentanan TI dinas komunikasi dan informatika?
	Jawaban:
6	**Pertanyaan:**
	Apakah dinas perhubungan komunikasi dan informatika menyediakan kesempatan bagi staff TI

	untuk mengikuti pelatihan untuk mengelola kerentanan teknologi dan menggunakan alat-alat evaluasi kerentanan?
	Jawaban:

- **F**ase 3 Risk Analysis

Tujuannya adalah melakukan identifikasi risiko, perencanaan mitigasi. Pada fase ini peneliti melakukan *interview* dengan kepala bidang teknologi informatika dan staf bidang IT. Berikut adalah pertanyaan digunakan untuk melakukan fase 3:

Tabel 4.4 Interview Protocol Fase Risk Analysis

	RISK ANALYSIS
	Protection Strategy
1	**Pertanyaan:**
	Adakah strategi dalam melakukan pengamanan data dan informasi di dinas perhubungan komunikasi dan informatika? a. Jika sudah ada, strategi pengamanan data dan informasi apa yang diterapkan? b. Jika belum ada, perlukah adanya pengamanan data dan informasi?
	Jawaban:
	Risk Mitigation Plans
1	**Pertanyaan:**
	Apakah aplikasi dan layanan TI dinas perhubungan komunikasi dan informatika memiliki *Disaster Recovery Plan (DRP)* pada aset informasinya?

	a. Jika sudah ada, aset informasi apakah yang sudah ter-*cover* oleh DRP tersebut? b. Jika belum ada, perlukah adanya *Disaster Recovery Plan (DRP)* pada aset informasi?
	Jawaban:

4.4 Penggalian Data

Penggalian data yang dilakukan dalam pengerjaan tugas akhir ini adalah dengan menggunakan teknik wawancara.Wawancara dilakukan dengan menggunakan perangkat *interview protocol.*

4.4.1 Wawancara

Wawancara dilakukan untuk mengumpulkan informasi langsung dari narasumber. Teknik wawancara terdiri dari 3 jenis yaitu: wawancara terstuktur (*structured interview*), wawancara semi tersruktur (*semistructured interview*), dan wawancara tidak terstruktur (*unstructured interview*).

- Wawancara terstruktur adalah wawancara yang sesuai dengan pedoman penelitian, apabila muncul kejadian di luar pedoman tersebut, maka hal tersebut tidak dihiraukan.
- Wawancara semi terstruktur adalah wawancara yang dilakukan dengan mengembangkan instrument penelitian. Selain itu, pelaksanaan dari wawancara ini bersifat bebas dan terbuka.
- Wawancara tidak terstruktur adalah wawancara yang dilakukan tanpa adanya instrument dan bersifat lebih mendalam, terbuka, dan bebas (D).

Pada tugas akhir ini, penulis menggunakan teknik wawancara semi terstruktur. Hal ini dikarenakan penulis menggunakan instrument atau perangkat namun ketika wawancara sedang

berlangsung, penulis tidak harus berfokus pada perangkat tersebut.

Wawancara yang akan dilakukan ditunjukan kepada narasumber yang memahami proses pelayanan publik terkait teknologi informasi yaitu kepala bidang teknologi informasi yaitu Bapak Bambang dan staf bidang teknologi informasi yaitu Bapak Andhi. Berikut ini adalah beberapa poin penting yang akan diajukan kepada Bapak Bambang dan Bapak Andhi:

1. Layanan publik terkait teknologi informasi yang dikelola organisasi.
2. Aset teknologi informasi yang dimiliki organisasi.
3. Pengelolaan keamanan informasi didalam organisasi.

4.4.2 Observasi

Metode ini dilakukan dengan cara melakukan pengamatan secara langsung pada Dinas Perhubungan Komunikasi dan Informatika kabupaten Tulungagung. Metode ini bertujuan untuk mendapatkan informasi mengenai kondisi nyata yang terjadi dalam pelayanan publik terkait teknologi informasi. Selain itu, dengan adanya metode ini penulis dapat mempelajari perilaku manusia dan proses kerja yang tidak bisa didapatkan melalui komunikasi, sehingga peneliti dapat melakukan pencatatan terhadap hasil pengamatan tersebut.

4.4.3 Metode Pengelohan Data

Sebelum melekaukan wawancara, penulis mengirimkan interview protocol kepada narasumber untuk mempersiapkan bahan untuk menjawabnya. Kemudian penulis, melakukan wawancara secara langsung dan diakhir wawancara penulis diberikan *softcopy* interview protocol yang sudah dijawab oleh narasumber.

4.5 Penentuan Pendekatan Analisis

Pada penelitian studi kasus diperlukan suatu pendekatan analisis untuk mengetahui hubungan antaradata yang sudah diolah.

1. **Pendekatan Analisis Standar**

   Analisis dengan menggunakan standar dilakukan menentukan kontrol dalam pembuatan mitgasi risiko.

2. **Pendekatan Analisis Metode Octave**

   Analisis metode OCTAVE diguanakan untuk identifikasi aset kritis yang dimiliki oleh organisasi. Selain itu, metode octave digunakan untuk mencari tahu kondisi pengelolaan risiko didalam organisasi.

BAB V
IMPLEMENTASI

Dalam bab ini berisi penjelasan mengenai proses implementasi yang dilakukan dalam penelitian.

5.1 Organizational View

Fase ini merupakan tahapan untuk membuat profil ancaman *(threat profile)* dengan cara menentukan aset yang penting bagi organisasi dan kebutuhan pengamanannya. Penentuan aset yang penting dilakukan melalui pengumpulan informasi tentang aset, kebutuhan keamanan, ancaman, dan kekuatan serta kelemahan organisasi dari beberapa tingkatan manajemen mulai dari senior manajer, operasional, sampai dengan staf. Hasil dari fase ini adalah pendefinisian kebutuhan keamanan informasi dan profil ancaman untuk aset – aset penting.

5.1.1 Identify Senior Management Knowledge

Untuk menggali informasi dari bagian senior management maka peneliti menggunakan *interview protocol* kepada pihak operational karena peneliti tidak mendapatkan akses untuk melakukan interview dengan pihak senior management di Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.

5.1.2 Identify Operational Area Management Knowledge

Untuk menggali informasi dari bagian operasional, maka peneliti menggunakan *interview protocol* dengan kepala bidang komunikasi informatika. Hasil dari kesimpulan *interview protocol* terdapat pada lampiran B.

5.1.3 Identify IT Staff Knowledge

Untuk menggali informasi dari bagian staf IT, maka peneliti menggunakan *interview protocol* dengan staf IT. Hasil dari kesimpulan *interview protocol* dapat dilihat pada Lampiran B.

5.1.4 Membuat Profil Ancaman

Ancaman adalah suatu entitas atau peristiwa yang berpotensi membahayakan system. Ancaman harus diidentifikasi dan dianalisis untuk menentukan kemungkinan terjadinya ancaman tipikal dan potensinya untuk merusak asset. Analisis risiko harus berkonsentrasi pada ancaman-ancaman yang paling mungkin terjadi dan yang bisa mempengaruhi asset penting.

Dari tahap implementasi yang dilakukan, maka akan dihasilkan pendefinisian kebutuhan keamanan informasi dan profil ancaman untuk aset – aset penting dan daftar kelemahan infrastruktur.

5.1.4.1 Daftar aset kritis

Penentuan aset yang penting dilakukan melalui pengumpulan informasi tentang aset, kebutuhan keamanan, ancaman, dan kekuatan serta kelemahan organisasi dari beberapa tingkatan manajemen yaitu operasional dan staf TI.

Tabel 5.1 Aset kritis organisasi

No.	Aset	Kategori Aset
1.	Data vendor LPSE	Data
2.	Data pengadaan barang setiap dinas	

No.	Aset	Kategori Aset
	Data informasi seputar kegiatan di Kabapuaten Tulungagung	
3.	Server	Hardware
4.	Komputer	
5.	CCTV	
6.	Genset	
7.	Printer	
8.	Perangkat Jaringan	Network
11.	Sistem Pemantauan kondisi lalu lintas	Software
12.	Website Pemerintah	
13.	Sistem Pengadaan Barang dan Jasa	
14.	Karyawan bidang kominfo	People
15.	Admin Sistem Informasi dan Website	

5.1.4.2 Kebutuhan keamanan aset kritis

Keamanan informasi merupakan perlindungan informasi dari semua ancaman yang mungkin terjadi dalam upaya untuk memastikan keberlangsungan proses bisnis, meminimalisir

risiko bisnis, memaksimalkan pengembalian investasi dan memanfaatkan peluang bisnis yang ada. CIA merupakan prinsip-prinsip dasar yang digunakan sebagai dasar keamanan informasi dan didalam tugas akhir ini CIA akan digunakan sebagai kategori dalam mengidentifikasi kebutuhan keamanan asset kritis.

Tabel 5.2 Kebutuhan keamanan aset kritis

Aset Kritis	Kebutuhan Keamanan	Keterangan
• Data vendor LPSE • Data pengadaan barang setiap dinas	Kerahasiaan (*Confidentiality*)	Data hanya bisa diakses dan dilihat oleh staff IT yang bertanggungjawab atas kegiatan LPSE.
	Integritas (*Integrity*)	Data-data harus lengkap dan akurat.
	Ketersediaan (*Availability*)	Data harus bisa diakses 24 jam.
Server	Kerahasiaan *(Confidentiality)*	Tersedianya akses untuk pihak yang berwenang.
	Integritas *(Integrity)*	Server tidak boleh diakses oleh mesin atau pihak yang tidak berwenang yang dapat mengubah konten.

Aset Kritis	Kebutuhan Keamanan	Keterangan
	Ketersediaan *(Availability)*	Akses harus tersedia selama 24 jam
• Komputer • CCTV • Printer	Kerahasiaan (*Confidentiality*)	Tersedianya akses untuk pihak berwenang.
	Integritas (*Integrity*)	Melakukan *monitoring* untuk memastikan daya kerja.
	Ketersediaan (*Availability*)	Akses harus tersedia selama 24 jam.
Genset	Kerahasiaan (*Confidentiality*)	Tersedianya akses untuk pihak berwenang.
	Integritas (*Integrity*)	Melakukan *monitoring* untuk memastikan daya kerja.
	Ketersediaan (*Availability*)	Dapat digunakan ketika dibutuhkan.
• Sistem Pemantauan kondisi lalu lintas • Website Pemerintah	Kerahasiaan (*Confidentiality*)	Aplikasi hanya dapat diakses oleh karyawan bidang kominfo dan karyawan yang mempunyai wewenang

Aset Kritis	Kebutuhan Keamanan	Keterangan
• Sistem Pengadaan Barang dan Jasa	Integritas (*Integrity*)	Informasi harus lengkap dan akurat
	Ketersediaan (*Availability*)	• Dapat diakses 24 jam oleh publik. • Data yang tersedia harus sering ter*update*.
• Perangkat Jaringan • Sistem Jaringan • Jaringan Komunikasi	Kerahasiaan (*Confidentiality*)	Adanya firewall untuk melakukan filtering access dan memastikan tidak terjadi pelanggaran yang dapat menimbulkan masalah fatal.
	Integritas (*Integrity*)	Memonitoring jaringan untuk memastikan keaslian data.
	Ketersediaan (*Availability*)	Terpasangnya sensor untuk memonitor peralatan jaringan agar selalu dapat digunakan.
• Karyawan bidang kominfo	Kerahasiaan (*Confidentiality*)	Senior management harus memastikan bahwa karyawan tidak membocorkan

Aset Kritis	Kebutuhan Keamanan	Keterangan
• Admin Sistem Informasi dan Website		informasi penting kepada pihak yang tidak berwenang.
	Integritas (*Integrity*)	• Staf harus memastikan semua informasi sudah lengkap dan akurat. • Staf harus mengikuti training terkait teknologi informasi.
	Ketersediaan (*Availability*)	Kurangnya staf IT pada bidang komunikasi informatika.

5.1.4.3 Identifikasi ancaman ke aset kritis

Proses identifikasi ancaman asset kritis menggabungkan semua informasi yang diperoleh dalam proses identifikasi senior, operational, staff knowledge dan membuat sebuah profil ancaman terhadap aset kritis.

Tabel 5.3 Ancaman aset kritis

Aset kritis	Ancaman
• Data vendor LPSE • Data pengadaan barang setiap dinas	Redudansi data
	Data tidak lengkap

Aset kritis	Ancaman
• Data informasi seputar kegiatan di Kabapuaten Tulungagung	Data hilang
	Data tidak terbackup
	Data korup
	Pembobolan data
	Database penuh
Server	Kesalahan konfigurasi dan perawatan server
	Server lemot
	Server diakses oleh pihak yang tidak berwenang
	AC diruangan server mati/rusak
	Memori server penuh
	Overloaded user
	Server terserang virus/malware
• Komputer • CCTV • Printer	Perusakan peralatan atau media
	Debu, korosi, pendingin, air
	Hilangnya pasokan listrik
	Pencurian

Aset kritis	Ancaman
	Maintenance yang kurang teratur
	Terserang virus
Genset	Perusakan peralatan atau media
	Pencurian
	Maintenance yang kurang teratur
	Debu, korosi, air
• Sistem Pemantauan kondisi lalu lintas • Website Pemerintah • Sistem Pengadaan Barang dan Jasa	Aplikasi terserang virus
	Aplikasi eror
	Aplikasi terserang hacker
Perangkat Jaringan	Penyadapan informasi penting melalui jaringan
	Kabel LAN digigit tikus
	Remote Spying
	Kejenuhan system informasi
	Konektifitas internet menurun
	Jaringan LAN lemot
	Koneksi terputus
	Celah masuknya hacker

Aset kritis	Ancaman
	Kesalahan pengalamatan IP
• Karyawan bidang kominfo • Admin Sistem Informasi dan Website	Kekurangan tenaga kerja
	Penggunaan peralatan yang tidak sah
	Kesalahan penginputan dan penghapusan data
	Penyalahgunaan wewenang pada hak akses yang dimiliki
	Pemalsuan hak
	Penyangkalan atas tindakan
	SDM tidak memperhatikan prosedur yang ada
	Tidak ada batasan hak akses
	Share login
	Password PC diketahui orang lain
	Penyangkalan atas tindakan
	Pengolahan data ilegal
	Kesalahan penggunaan
	Kesalahan konfigurasi PC

5.1.5 Technological View

Pada tahapan *Technological View* dilakukan identifikasi proses bisnis dan profil ancaman terhadap asset kritis yang didukung layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung dan identifikasi kelemahan infrastruktur.

5.1.5.1 Identify Key Components

Proses ini berfokus untuk menggali informasi yang lebih detail terkait layanan teknologi informasi. Pada proses ini mengidentifikasi proses bisnis dan aset informasi yang didukung oleh layanan teknologi informasi.

5.1.5.1.1 Systems of Interest and Key Classes of Components

System of interest merupakan sistem yang menjadi inti dari analisis risiko. Sistem yang menjadi inti dari analisis risiko dalam tugas akhir ini adalah layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.

Tabel 5.4 System of interest dan key classess of component

Layanan Teknologi Informasi	
Systems of interest	Layanan teknologi informasi berfokus pada layanan teknologi informasi yang dikelola oleh Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung yaitu website pemerintah, pemantauan kondisi lalu lintas, pengadaan barang LPSE.

Key Classes of Components	Data vendor LPSE Data pengadaan barang setiap dinas Data informasi seputar kegiatan di Kabapuaten Tulungagung Komputer Server CCTV Perangkat jaringan

5.1.5.1.2 Classes of Components

Kelas utama komponen dipilih berdasarkan bagaimana aset tersebut diakses dan digunakan. Kelas dari komponen merupakan bagian dari *system of interest*.

Tabel 5.5 Class of component

Class of Component	Rationale for Selection
• Data vendor LPSE • Data pengadaan barang setiap dinas • Data informasi seputar kegiatan di Kabapuaten Tulungagung	Data-data tersebut sangat diperlukan untuk melakukan proses bisnis dalam layanan teknologi informasi yang dikeluarkan oleh Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.
Komputer	Karyawan menggunakan komputer untuk melakukan

Class of Component	Rationale for Selection
	kegiatan terkait layanan teknologi informasi.
Server	Komputer yang menyediakan sumberdaya dan mengendalikan akses didalam suatu jaringan. Semua informasi terkait layanan teknologi infrmasi dikelola didalam server.
CCTV	Karyawab menggunakan CCTV untuk melakukan pemantauan lalu lintas jalan.
Perangkat jaringan	Perangakat jaringan yang dapat mengakses layanan teknologi informasi.

5.1.5.2 Mengevaluasi komponen yang dipilih

Setelah mendapatkan profil ancaman asset kritis maka proses yang akan dilakukan adalah menganalisa kelemahan atau kerentanan dari aset-aset tersebut secara teknologi dan organisasi. *Key component* terdiri dari *system of interest* dan *classes of component* berdasarkan aset kritis.

Identifikasi kerentanan aset

Kerentanan adalah kondisi tidak adanya prosedur keamanan, kontrol teknik, kontrol fisik, atau kontrol lain yang dapat dieksploitasi oleh ancaman. Kerentanan berkontribusi mengambil risiko karena memungkinkan ancaman untuk membahayakan system. Kerentanan akan diidentifikasi

berdasarkan *key classes of component* dan aset kritis. Proses identifikasi kerentanan asset kritis menggabungkan semua informasi yang diperoleh dalam proses identifikasi operational, staff, dan IT staf knowledge.

Untuk *class of component* komputer, server, CCTV termasuk dalam *hardware*, perangkat jaringan termasuk dalam *network* serta data vendor LPSE, data pengadaan barang setiap dinas, data informasi seputar kegiatan di Kabapuaten Tulungagung termasuk dalam data.

Tabel 5.6 Kerentanan aset

Aset	Kerentanan
• Data vendor LPSE • Data pengadaan barang setiap dinas • Data informasi seputar kegiatan di Kabapuaten Tulungagung	Terlalu banyak data yang diinputkan
	Kurangnya salinan back-up
	Data terlalu sering diupdate
	Data tidak terupdate
Komputer	Kurangnya pemeliharaan/prosedur untuk pemeliharaan rumit
	Kurangnya skema pergantian secara berkala
	Kerentanan terhadap kelembapan, debu, kotoran
	Kerentanan terhadap nilai informasi yang tersimpan pada PC

Aset	Kerentanan
	Kerentanan terhadap voltase yang bervariasi
Server	Beban kerja server yang tinggi
	Supply listrik yang tidak stabil
	Hubungan arus pendek pada panel listrik
	Pertambahan memori yang cepat dalam pemrosesan data
	Voltase yang bervariasi
CCTV	Kurangnya pemeliharaan/prosedur untuk pemeliharaan rumit
	Kurangnya skema pergantian perangkat keras secara berkala
	Kerentanan terhadap kelembapan, debu, kotoran, air
Perangkat jaringan	Jalur komunikasi yang tidak dilindungi
	Sambungan kabel yang buruk
	Arsitektur jaringan yang tidak aman
	Manajemen jaringan yang tidak cukup (ketahanan routing)
	Kualitas jaringan yang kurang baik
	Peletakan kabel yang sembarangan

Aset	Kerentanan
	Tidak ada pelindung kabel

Berdasarkan aset kritis masih terdapat layanan teknologi informasi dan *people* yang belum diidentifikasi kerentanannya, hal ini perlu dilakukan karena kerentanan berpotensi terjadi untuk setiap aset kritis. Tidak semua aset kritis masuk kedalam *key classes of component* dari *system of interest* dengan pertimbangan *key classes of component* yang mencakup infrastruktur yang berkaitan dengan layanan teknologi informasi yang dikelola Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.

Tabel 5.7 Kerentanan Aset

Aset	Kerentanan
Layanan teknologi informasi	Tidak ada atau tidak cukup pengujian perangkat lunak
	Menerapkan program aplikasi untuk data yang salah dalam hal waktu
	Kurangnya dokumentasi user manual untuk aplikasi
	Kurangnya mekanisme identifikasi dan otentifikasi pengguna aplikasi
	Kekurangan yang telah diketahui pada perangkat lunak

Aset	Kerentanan
People	Ketidakhadiran karyawan
	Pelatihan terkait teknologi informasi tidak cukup
	Pelatihan keamanan yang tidak cukup
	Kurangnya kesadaran akan keamanan
	Kurangnya mekanisme pemantauan
	Bekerja tanpa pengawasan senior management
	Kurangnya kebijakan untuk penggunaan yang benar atas media telekomunikasi

Halaman ini sengaja dikosongkan

BAB VI
HASIL DAN PEMBAHASAN

Dalam bab ini berisi penjelasan mengenai hasil dan pembahasan yang dilakukan dalam penelitian.

6.1 Identifikasi Risiko

Pada tahapan *Risk Abalys* dilakukan identifikasi risko, penilian risiko serta mitigasi risiko terhadap asset kritis yang didukung layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.

6.1.1 Identifikasi Potential Cause

Potensial causes merupakan penyebab dari timbulnya risiko yang terjadi dan didapatkan dari identifikasi kerentanan dan ancaman dari aset informasi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung yang penting yang telah dipaparkan sebelumnya.

Tabel 6.1 Potential cause

Aset	Kerentanan	Ancaman	Potential Cause
Hardware • Komputer • Server • CCTV	• Kurangnya skema pergantian perangkat keras secara berkala • Kurangnya pemeliharaan/prosedur untuk pemeliharaan yang rumit	Perusakan peralatan atau media	*Maintenance* yang tidak teratur
	Kerentanan terhadap kelembapan, debu, kotoran.	Debu, korosi, pendingin, air	Kerusakan fisik pada server
	Kerentanan terhadap nilai informasi yang tersimpan pada PC	Pencurian	Kurangnya pengamanan organisasi
	Kerentanan terhadap voltase yang bervariasi	Hilangnya pasokan listrik	Korsleting listrik

Aset	Kerentanan	Ancaman	Potential Cause
	Hubungan arus pendek pada panel listrik		
	Supply listrik yang tidak stabil	Hilangnya pasokan listrik	Pemadaman listrik
	Beban kerja server yang tinggi	AC diruangan server mati/rusak	Server overheat
	Pertambahan memori yang cepat dalam pemrosesan data	Server lemot	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)
Data: • Data vendor LPSE	• Data terlalu sering diupdate • Data tidak terupdate	• Redudansi data • Data tidak lengkap	Kesalahan dalam penginputan dan penghapusan data

Aset	Kerentanan	Ancaman	Potential Cause
• Data pengadaan barang setiap dinas • Data informasi seputar kegiatan di Kabapuaten Tulungagung	Kurangnya salinan back-up	• Data hilang • Data tidak terbackup	Organisasi tidak melakukan prosedur *backup*
	Jaringan internet kurang optimal	Data korup	Speed koneksi internet yang lemah dan tidak stabil
	Kesalahan penempatan hak akses	Pembobolan data	Tidak ada penggunaan hak akses
	Terlalu banyak data yang diinputkan	Database penuh	Server down
Layanan teknologi informasi:	Kurangnya dokumentasi user manual untuk aplikasi	Kesalahan pengguna	Kurangnya dokumentasi (user manual) untuk karyawan baru

Aset	Kerentanan	Ancaman	Potential Cause
• Website pemerintah • Pemantauan kondisi lalu lintas • Pengadaan barang LPSE.	Kurangnya mekanisme identifikasi dan otentifikasi pengguna aplikasi	Aplikasi terserang hacker	Password tidak pernah diganti
	Karyawan kurang memperhatikan pentingnya antivirus	Aplikasi terserang virus	PC terserang virus
	• Kekurangan yang telah diketahui pada perangkat lunak • Tidak ada atau tidak cukup pengujian perangkat lunak	Penyalahgunaan wewenang pada hak akses yang dimiliki	Staf mengetahui kelemahan pada aplikasi
	Karyawan kurang teliti dan competen	Aplikasi eror	Kesalahan coding pada fungsional software

Aset	Kerentanan	Ancaman	Potential Cause
Perangkat jaringan (*network*)	• Jalur komunikasi yang tidak dilindungi • Arsitektur jaringan yang tidak aman	• Penyadapan informasi penting melalui jaringan • Celah masuknya hacker • Remote Spying	Lemahnya keamanan di sistem internal TI
	• Manajemen jaringan yang tidak cukup (ketahanan routing) • Sambungan kabel yang buruk	Jaringan LAN lemot	Kurangnya mekanisme pemantauan terhadap jaringan
	Kualitas jaringan yang kurang baik	Konektifitas internet menurun	Gangguan jaringan pada provider
	Bencana alam dan kerjadian yang tidak terduga	Koneksi terputus	Kerusakan pada infrastruktur jaringan

Aset	Kerentanan	Ancaman	Potential Cause
	SDM yang tidak kompeten	Kesalahan pengalamatan IP	Kesalahan dalam melakukan konfigurasi access point
	• Peletakan kabel yang sembarangan • Tidak ada pelindung kabel	Kabel LAN digigit tikus	Kabel digigit oleh hewan
	Karyawan yang tidak kompeten	Kesalahan pengalamatan IP	Kesalahan dalam melakukan konfigurasi access point
Karyawan (*People*)	Ketidakhadiran karyawan	Kekurangan tenaga kerja	Adanya share login
	Pelatihan terkait teknologi informasi tidak cukup	Kesalahan penggunaan	Kurangnya training prosedur penggunaan TI yang diberikan

Aset	Kerentanan	Ancaman	Potential Cause
	Kurangnya kesadaran akan keamanan	Kesalahan penggunaan	Kurangnya sosialisasi tentang regulasi dan sanksinya
	Kurangnya mekanisme pemantauan	Pengolahan data illegal	Pengolahan data illegal oleh karyawan
	Bekerja tanpa pengawasan senior management	• Karyawan tidak memperhatikan prosedur yang ada • Pencurian PC	Kurangnya mekanisme pemantauan
	Kurangnya kebijakan untuk penggunaan yang benar atas media telekomunikasi	• Penggunaan peralatan yang tidak sah • Penyangkalan atas tindakan	Tidak ada peraturan terkait keamanan informasi
	Karyawang kurang teliti	Kesalahan penginputan dan penghapusan data	Kesalahan penginputan dan penghapusan data

Aset	Kerentanan	Ancaman	Potential Cause
	Pelatihan keamanan yang tidak cukup	• Penyalahgunaan wewenang pada hak akses yang dimiliki • Password PC diketahui orang lain • Pemalsuan hak	Staf tidak logout ketika meninggalkan komputer
	Karyawan bidang kominfo bisa mengakses	Tidak ada batasan hak akses	Tidak ada pengaturan untuk manajemen hak akses user atau user privilege

6.1.2 Identifikasi Risiko

Sebelum tahapan penilaian risiko, terlebih dahulu akan diidentifikasi risiko-risiko yang dapat mengancam asset informasi Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung. Risiko yang dimaksudkan adalah berupa kejadian yang memiliki probabilitas untuk terjadi bahkan sering terjadi baik disebabkan oleh faktor yang berasal dari kondisi eksternal maupun kondisi internal perusahaan yaitu bencana alam, gangguan fasilitas umum, social, dan operasional.

Tabel 6.2 Identifikasi risiko

Aset	Potential Cause	Risiko
Hardware • Komputer • Server • CCTV	• *Maintenance* yang tidak teratur • Server overheat • Kerusakan fisik pada server	Hardware failure
	Kurangnya pengamanan organisasi	Pencurian media atau informasi penting
	Korsleting listrik	Kebakaran
	Pemadaman listrik	Power failure
	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)	Memory penuh

Aset	Potential Cause	Risiko
Data: • Data vendor LPSE • Data pengadaan barang setiap dinas • Data informasi seputar kegiatan di Kabapuaten Tulungagung	Kesalahan dalam penginputan dan penghapusan data	Human atau technician error
	• Organisasi tidak melakukan prosedur *backup* • Server down	Backup data failure
	Speed koneksi internet yang lemah dan tidak stabil	Network failure
	Password disimpan pada desktop komputer	Penyalahgunaan hak akses
Layanan teknologi informasi: • Website pemerintah • Pemantauan kondisi lalu lintas • Pengadaan barang LPSE.	• Kurangnya dokumentasi (user manual) untuk karyawan baru • PC terserang virus	Human atau technician error
	Kesalahan coding pada fungsional software	Software failure
	Password tidak pernah diganti	Penyalahgunaan hak akses
	Staf mengetahui kelemahan pada aplikasi	Modifikasi dan pencurian database

Aset	Potential Cause	Risiko
Perangkat jaringan (*network*)	Lemahnya keamanan di sistem internal TI	Serangan hacker
	• Kurangnya mekanisme pemantauan terhadap jaringan • Gangguan jaringan pada provider • Kerusakan pada infrastruktur jaringan • Kesalahan dalam melakukan konfigurasi access point • Kabel digigit oleh hewan • Kesalahan dalam melakukan konfigurasi access point	Network failure
Karyawan (*People*)	• Adanya share login • Tidak ada pengaturan untuk manajemen hak	Penyalahgunaan hak akses

Aset	Potential Cause	Risiko
	akses user atau user privilege	
	• Kurangnya training prosedur penggunaan TI yang diberikan • Kesalahan penginputan dan penghapusan data • Staf tidak logout ketika meninggalkan komputer	Human atau technician error
	Kurangnya sosialisasi tentang regulasi dan sanksinya	Pelanggaran terhadap aturan atau regulasi yang berlaku
	Pengolahan data illegal oleh karyawan	Modifikasi dan pencurian database
	• Kurangnya mekanisme pemantauan • Tidak ada peraturan terkait keamanan informasi	Pencurian media atau informasi penting

6.1.3 Peniliaian Risiko

Pada tahap ini dilakukan penentuan tingkat severity, occutance, dan detection. Tahapan ini dilakukan dengan mendeskripsikan informasi secara lebih dalam terhadap risiko yang telah diidentifikasi. Hasil dari tahap ini adalah nilai severity, occurance dan detection pada setiap proses risiko yang nantinya akan digunakan untuk menghitung RPN (Risk Priority Number) parameter dari level severity, occurance, dan detection. Dari proses penilaian risiko menggunakan metode FMEA (Failure Mode & Effect Analysis) didapatkan risiko yang mempunyai skor assessment tertinggi hingga terendah. Nilai RPN dikelompokkan menjadi Very High, High, Medium, Low dan Very Low. Berikut ini merupakan tabel skala pelevelan risiko dengan menggunakan RPN:

Tabel 6.3 Skala RPN

RPN	Level Resiko
200>	Very High
151-200	High
101-150	Medium
51-100	Low
0-50	Very Low

Tabel 6.4 Penilaian risiko

Risiko	Potential Cause	SEV	OCC	DEC	RPN	LEVEL
Hardware failure	*Maintenance* yang tidak teratur	9	3	3	45	*Low*
	Server overheat	9	1	6	54	*Low*
	Kerusakan fisik pada hardware	9	3	3	81	*Low*
Software failure	Kesalahan coding pada fungsional software	5	4	3	60	*Low*
Network failure	Speed koneksi internet yang lemah dan tidak stabil	9	7	6	378	*Very high*
	Kurangnya mekanisme pemantauan terhadap jaringan	7	1	6	42	*Very low*

Risiko	Potential Cause	SEV	OCC	DEC	RPN	LEVEL
	Gangguan jaringan pada provider	9	7	6	378	*Very high*
	Kerusakan pada infrastruktur jaringan	7	3	6	125	*Medium*
	Kesalahan dalam melakukan konfigurasi access point	7	4	6	168	*High*
	Kabel digigit oleh hewan	7	3	6	125	*Medium*
Power failure	Pemadaman listrik	9	7	6	378	*Very high*
Backup data failure	Organisasi tidak melakukan prosedur *backup*	6	4	4	96	*Low*

Risiko	Potential Cause	SEV	OCC	DEC	RPN	LEVEL
	Server down	9	7	6	378	*Very high*
Human atau technician error	Kurangnya dokumentasi (user manual) untuk karyawan baru	5	4	4	80	*Low*
	PC terserang virus	5	4	3	60	*Low*
	Kesalahan dalam penginputan dan penghapusan data	6	4	4	96	*Low*
	Kurangnya training prosedur penggunaan TI yang diberikan	5	3	4	60	*Low*
	Staf tidak logout ketika	6	5	4	120	*Medium*

Risiko	Potential Cause	SEV	OCC	DEC	RPN	LEVEL
	meninggalkan komputer					
Serangan hacker	Lemahnya keamanan di sistem internal TI	6	4	5	120	*Medium*
Penyalahgunaan hak akses	Tidak ada penggunaan hak akses	6	4	5	120	*Medium*
	Adanya share login	6	4	5	120	*Medium*
	Tidak ada pengaturan untuk manajemen hak akses user atau user privilege	6	3	5	72	*Low*
	Password tidak pernah diganti	6	4	5	120	*Medium*

Risiko	Potential Cause	SEV	OCC	DEC	RPN	LEVEL
Pencurian media atau informasi penting	Kurangnya pengamanan organisasi	6	4	4	96	*Very low*
	Kurangnya mekanisme pemantauan	5	3	3	45	*Very low*
	Tidak ada peraturan terkait keamanan informasi	6	4	4	96	*Low*
Kebakaran	Korsleting listrik	9	1	6	54	*Low*
Memory penuh	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori full)	9	7	6	378	*High*

Risiko	Potential Cause	SEV	OCC	DEC	RPN	LEVEL
Modifikasi dan pencurian database	Staf mengetahui kelemahan pada aplikasi	9	1	5	45	*Very low*
	Pengolahan data illegal oleh karyawan	9	1	5	45	*Very low*
Pelanggaran terhadap aturan atau regulasi yang berlaku	Kurangnya sosialisasi tentang regulasi dan sanksinya	5	4	4	80	*Low*

6.1.4 Mitigasi Risiko

Setelah melaukan identifikasi aset kritis, identifikasi risko dan penilaian risiko selanjutnya adalah melakukan mitigasi terhadap risiko tersebut. Mitigasi dilakukan dengan menggunakan standar dan diskusi langsung dengan pihak dinas perhubungan komunikasi dan informatika kabupaten tulungagung. Standar yang digunakan untuk membuat mitigasi adalah ISO 27001.

Dari hasil identifikasi dan penilaian risiko maka berikut beberapa kontrol objektif dari standar ISO/IEC 27001 yang direkomendasikan untuk penanganan risiko-risiko yang telah diidentifikasi tersebut adalah :

a. *Performance evaluation*
b. *Information security incident management*
c. *System and aplication acess control*
d. *Supllier service delivery management*
e. *Equipment*
f. *Backup*
g. *Human resource security*
h. *Control of operational software*
i. *Assess control*
j. *Information transfer*
k. *Organization of information security*
l. *Leadership*

Berikut ini merupakan penjelasan singkat mengenai mitigasi risiko pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung:

Tabel 6.5 Mitigasi Risiko

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
Hardware: • Komputer • CCTV • Server	Hardware failure	*Maintenance* yang tidak teratur	• Kerusakan asset teknologi • Kinerja hardware menurun	**Performance evaluation :** Untuk menjaga kualitas hardware diperlukan evluasi performa.	**Monitoring, measurement, analysis adn evaluation:** Merupakan prosedur monitoring terhadar aset teknologi informasi yang dimiliki oleh organisasi.	• Organisasi menetapkan kebijakan mengenai monitorng aset teknologi informasi. • Monitoring dilakukan secara berkala untuk memastikan aset teknologi

Penjelasan dari alasan dipilihnya 12 rekomendasi kontrol yang diberikan diatas sesuai dengan risiko-risiko tersebut adalah sebagai berikut :

1. **Identifikasi risiko modifikasi dan pencurian database**

   Dengan penyebab data diakses oleh pihak yang tidak berwenang yang berdampak pada data diketahui dan dimanfaatkan oleh pihak yang tidak berwenang maka dilakukan tindakan pembatasan akses yaitu akses terhadap informasi dan aplikasi oleh user harus dibatasi sesuai dengan kebijakan keamanan yang telah ditentukan. Selain itu dilakukan pemberhentian pegawai yaitu dengan penghapusan hak akses pegawai terhadap informasi dan fasilitas pemrosesan informasi sejak mereka dinyatakan berhenti.

2. **Identifikasi risiko backup data failure**

Data tidak terback-up biasanya terjadi karena kapasitas media penyimpanan yang tidak mencukupi yang berdampal informasi yang ditampilkan tidak updaye maka perlu dilakukan tindakan backup secara berkala dan manajemen kapasitas yaitu kebutuhan kapasitas harus dimonitor dan ditinjau secara berkala.

3. **Identifikasi risiko human/technician error**

Dengan penyebab kesalahan dalam pengoperasian system hardware maupun software yang berdampak kerusakan pada system hardware maupun software dalam kegiatan operasional terganggu maka perlau dilakukan tindakan pendidikan dan pelatihan keamanan informasi pada karyawan sehingga dapat memahami keamanan informasi yang ditetapkan perusahaan demi mengurangi terjadinya kesalahan kerja (human eror).

4. **Identifikasi risiko memory full**

Dengan penyebab kapasitas media penyimpanan tidak mencukupi dan banyak sekali data yang harus diinputkan setiap harinya yang berdampak tidak mampu meyimpan data-data baru maka perlu dilakukan tindakan back-up secara berkala dan manajemen kapasitas yaitu kebutuhan kapasitas harus dimonitor secara berkala.

5. **Identifikasi risiko Serangan hacker**

Dengan penyebab lemahnya keamanan di system internal TI yang berdampak data diketahui dan dimanfaatkan oleh pihak yang tidak berwenang yang menyebabkan terhambatnya proses bisnis dan merusak citra pelayanan publik maka perlu dilakukan tindakan control akses jaringan yaitu dengan prosedur monitoring dalam

penggunaan system pengolahan informasi harus dilakukan secara berkala.

6. **Identifikasi risiko Hardware failure**

Hardware failure disebabkan oleh beberapa hal yaitu diantaranya adanya virus yang menyerang computer, server terserang malware, maintenance yang tidak teratur, dan kesalahan melakukan konfigurasi yang berdampak kehilangan data, database korup, bahkan kerusakan pada aset dan teknologi tersebut maka diperlukan adanya pemeliharaan dan control secara berkala terhadap hardware untuk memastikan ketersediaan dan integritas hardware.

7. **Identifikasi risiko software failure**

Dengan penyebab kesalahan coding pada fungsional software dan pc terserang virus yang dapat menyebabkan application crashed, kehilangan data, database korup maka diperlukan pembatasan akses ke source code program dan harus dikontrol dengan ketat untuk mencegah masuknya fungsionalitas yang tidak sah dan untuk menghindari perubahan yang tidak disengaja selain itu diperlukan adanya deteksi, pencegahan, dan pemulihan untuk melindungi software dari virus, trojan, dan malware sesuai dengan prosedur.

8. **Identifikasi risiko power failure**.

Dengan penyebab korsleting listrik berdampak kerusakan pada aset teknologi seperti server dan pc yang tiba-tiba mati dan dapat menyebabkan kehilangan data yang berdampak tidak dapat mengoperasionalkan server dan pc sehingga kegiatan operasional terhenti maka dari itu dibutuhkan perlindungan fisik terhadap kerusakan dan perlu dilakukan

back-up agar data tetap tersimpan walaupun terjadi power failure.

9. **Identifikasi risiko network failure**

Dengan penyebab kerusakan pada komponen infrastruktur jaringan internal yang berdampak beberapa kegiatan operasioal organisasi yang terhubung dengan jaringan LAN dan internet terhenti, maka perlu dilakukan tindakan control jaringan dengan cara dimonitoring dan dipelihara keamanan sistemnya yang ditinjau secara berkala.

10. **Identifikasi risiko kebakaran**

Dengan penyebab terjadinya korsleting listrik dan terbakarnya generator berdampak tidak dapat mengoperasionalkan server dan pc sehingga kegiatan operasional terhenti dan memunculkan waktu dan biaya tambahan untuk perbaikannya maka perlu dilakukan tindakan perlindungan keamanan pengkabelan dari kerusakan dan juga dilakukan monitoring yang ditinjau secara berkala. Selain itu untuk melindungi data yang ada pada server juga perlu dilakukan back-up.

11. **Identifikasi risiko Pencurian media atau dokumen penting**

Dengan penyebab pencurian hardware yang berdampak benefit loss dan kekurangan hardware untuk menjalankan proses bisnis maka perlu dilakukan tindakan pengamanan pada setiap ruangan yaitu misalnya harus dilindungi dengan control akses masuk yang memadai untuk memastikan hanya orang yang berhak saja diizinkan masuk sehingga cara tersebut dapat mencegah terjadinya pencurian.

12. **Identifikasi risiko penyalahgunaan hak akses**

Dengan penyebab semua karyawan memiliki hak akses yang sama dan adanya share login yang sering dilakukan antar karyawan maka perlu dilakukan pembatasan akses terhadap informasi dan aplikasi oleh pengguna dan personel pendukung sesuai dengan kebijakan pengendalian akses yang ditetapkan serta diperlukan adanya perjanjian dengan user bahwa password pribadi yang bersifat rahasia harus dijaga dan tidak boleh diberitahukan kepada orang lain untuk menghindari terjadinya risiko penyalahgunaan hak akses.

13. **Pelanggaran terhadap aturan atau regulasi yang berlaku**

Dengan penyebab kurangnya sosialisasi tentang regulasi dan sanksinya yang berdampak terjadinya penurunan etika kerja karyawan terhadap keamanan system dan mengakibatkan pekerjaan yang tidak efektif maka diperlukan adanya pelatihan kesadaran yang tepat dalam kebijakan keamanan organisasi bagi semua karyawan di organisasi.

6.2 Validasi

Pada kelima adalah melakukan validasi mitigasi yang digunakan serta kontrol dan subkontrol dalam pembuatan mitigasi risiko. Validasi dilakukan dengan tujuan untuk melihat apakah mitigasi dan kontrol ISO 270001 sesuai dengan kondisi yang ada diorganiasi dan kondisi yang diharapkan organisasi.
Validasi dilakukan dengan cara mewawancarai penanggungjawab pengelolaan teknologi informasi yang ada pada dinas tersebut. Sehingga menghasilkan mitgasi dan kontrol yang sesuai dengan harapan dinas perhubungan komunikasi dan informatika kabupaten Tulungagung.

LAMPIRAN A
INTERVIEW PROTOCOL

Berikut ini merupakan interview protocol yang digunakan dalam melakukan identifikasi risiko pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung.

Informasi Pelaksanaan Interview	
Interviewer	:
Narasumber	:
Hari, Tanggal	:
Pukul	:
Lokasi	:
Informasi Narasumber	
Nama	:
Jabatan	:
Instansi	:
Lama bekerja	:

Tabel A.1 Interview Protocol

No	**ORGANIZATION VIEW**
	Critical Assets
1	**Pertanyaan:**
	Proses bisnis apa yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?

	Jawaban:
2	**Pertanyaan:**
	Aset apa saja yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
3	**Pertanyaan:**
	Aset apa yang paling penting di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
4	**Pertanyaan:**
	Seberapa besar pengaruh jaringan terhadap keberlangsungan proses bisnis yang ada pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
5	**Pertanyaan:**
	Sistem informasi apa yang terdapat pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
7	**Pertanyaan:**
	Siapa saja yang mempunyai kepentingan menggunakan aplikasi dan layanan TI?
	Jawaban:
	Security Requirement for Critical Assets
1	**Pertanyaan:**
	Apakah aplikasi dan layanan TI di lingkungan dinas perhubungan komunikasi dan informatika sudah memberikan *checklist* terkait kebutuhan keamanan aset informasi yang dimiliki? c. Jika sudah, apa saja kebutuhan keamanan yang dilihat dari *checklist* tersebut yang sudah terpenuhi?

	d. Jika belum, perlukan adanya *checklist* terkait kebutuhan keamanan aset informasi yang dimiliki?
	Jawaban:
2	**Pertanyaan:**
	Adakah aturan dalam melakukan pengamanan terkait akses informasi pada aplikasi dan layanan TI?
	Jawaban:
3	**Pertanyaan:**
	Apakah ada pemeriksaan secara rutin terhadap keamanan aset?
	Jawaban:
4	**Pertanyaan:**
	Apakah ada kegiatan maintenance pada aset?
	Jawaban:
5	**Pertanyaan:**
	Apakah ada mekanisme untuk mencegah pembobolan aset?
	Jawaban:
6	**Pertanyaan:**
	Apakah sensitifitas informasi dilindungi oleh tempat penyimpanan yang aman?
	Jawaban:

A-4

	Threat to Critical Assets
1	**Pertanyaan:**
	Apakah aset informasi dinas perhubungan komunikasi dan informatika pernah mengalami ancaman? c. Jika pernah, apa saja ancaman yang pernah dialami? d. Jika belum, ancaman apakah yang memungkinkan terjadi?
	Jawaban:
2	**Pertanyaan:**
	Berikan contoh bagaimana pihak dalam yang bertindak secara tidak sengaja dapat menggunakan akses fisik untuk mengancam sistem ini?
	Jawaban:
3	**Pertanyaan:**
	Bagaimana melakukan pencegahan terhadap ancaman aset TI?
	Jawaban:
4	**Pertanyaan:**
	Seberapa sering terjadinya server down pada server?
	Jawaban:
5	**Pertanyaan:**
	Seberapa sering terjadinya pembobolan data?

	Jawaban:
6	**Pertanyaan:**
	Apakah pada aplikasi dan layanan TI dilakukan *update* anti virus?
	Jawaban:
7	**Pertanyaan:**
	Apakah ada SOP untuk meng*update* sistem tersebut?
	Jawaban:
	Current Security Practice
1	**Pertanyaan:**
	Apakah ada informasi mengenai aplikasi dan layanan TI di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
2	**Pertanyaan:**
	Apakah aplikasi dan layanan TI menerapkan *framework* atau standar keamanan khusus aset informasi? c. Jika iya, standart atau *framework* apa yang digunakan? d. Jika tidak, perlukan adanya standart atau *framework* khusus pengamanan aset informasi?
	Jawaban:
3	**Pertanyaan:**

	Apakah di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung sudah melakukan penilaian risiko untuk keamanan informasi?
	Jawaban:
4	**Pertanyaan:**
	Apakah bidang komunikasi dan informatika menerima dan bertindak atas laporan rutin dari informasi yang berhubungan dengan keamanan?
	Jawaban:
5	**Pertanyaan:**
	Apakah kendala dalam melakukan implementasi standart atau *framework* pengamanan aset informasi pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
6	**Pertanyaan:**
	Apakah di dinas perhubungan komuniasi dan informatika sudah memiliki kebijakan dan prosedur dalam melindungi informasi ketika bekerja sama dengan perusahaan lain?
	Jawaban:
	Current Organizational
1	**Pertanyaan:**
	Apa masalah yang sering terjadi di dinas perhubungan komunikasi dan informatika terkait *asset informasi?*
	Jawaban:

2	**Pertanyaan:**
	Pernahkah terjadi pencurian informasi pada dinas perhubungan komunikasi dan informatika c. Jika pernah, informasi apa yang telah dicuri? Apa penyebab *asset informasi* tersebut bermasalah? d. Jika belum, informasi apa saja yang memungkinkan terjadinya pencurian?
	Jawaban:
3	**Pertanyaan:**
	Apakah kapasitas server yang dimiliki dinas perhubungan komunikasi dan informatika sudah mencukupi?
	Jawaban:
4	**Pertanyaan:**
	Berapa kali dalam setahun dinas perhubungan komunikasi dan informatika melakukan evaluasi terhadap keamanan teknologi informasi?
	Jawaban:
5	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika sudah melakukan verifikasi untuk setiap divisi dalam mengurus hak akses dan otorisasi?
	Jawaban:
6	**Pertanyaan:**

	Bagaimana kode etik yang diterapkan pada dinas perhubungan komunikasi dan informaika terkait pengamanan aset informasi?
	Jawaban:
	TECHNOLOGICAL VIEW
	Key Component
1	**Pertanyaan:**
	Perangkat IT apa saja yang dimiliki oleh dinas perhubungan komunikasi dan informatika kabupaten Tulunggung?
	Jawaban:
	Current Technology Vulnerability
1	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika terdapat prosedur untuk menjaga kerentanan teknologi seperti meninjau sumber informasi, mengelola keamanan tempat penyimpanan dan mengidentifikasi komponen infrastruktur?
	Jawaban:
2	**Pertanyaan:**
	Bagaimana bentuk penanggulangan terkait adanya gangguan TI?
	Jawaban:
3	**Pertanyaan:**
	Apakah dinas komunikasi dan informatika menjadwalkan dan melakukan evaluasi kerentanan TI secara berkala?
	Jawaban:

4	**Pertanyaan:**
	Apakah dinas komunikasi dan informatika memiliki dokumen mengenai jenis-jenis kerentanan dan metode serangannya?
	Jawaban:
5	**Pertanyaan:**
	Siapa yang bertanggung jawab memanajemen kerentanan TI dinas komunikasi dan informatika?
	Jawaban:
6	**Pertanyaan:**
	Apakah dinas perhubungan komunikasi dan informatika menyediakan kesempatan bagi staff TI untuk mengikuti pelatihan untuk mengelola kerentanan teknologi dan menggunakan alat-alat evaluasi kerentanan?
	Jawaban:
	RISK ANALYSIS
	Protection Strategy
1	**Pertanyaan:**
	Adakah strategi dalam melakukan pengamanan data dan informasi di dinas perhubungan komunikasi dan informatika? c. Jika sudah ada, strategi pengamanan data dan informasi apa yang diterapkan? d. Jika belum ada, perlukah adanya pengamanan data dan informasi?
	Jawaban:

	Risk Mitigation Plans
1	**Pertanyaan:**
	Apakah aplikasi dan layanan TI dinas perhubungan komunikasi dan informatika memiliki *Disaster Recovery Plan (DRP)* pada aset informasinya? c. Jika sudah ada, aset informasi apakah yang sudah ter-*cover* oleh DRP tersebut? d. Jika belum ada, perlukah adanya *Disaster Recovery Plan (DRP)* pada aset informasi?
	Jawaban:

LAMPIRAN B
HASIL WAWANCARA

Berikut merupakan hasil wawancara dengan menggunakan interview protocol pada lampiran A.

Informasi Pelaksanaan Interview	
Interviewer	:Balqis Lembah M
Narasumber	: Bambang Noertjahjo
Hari, Tanggal	:Kamis, 7 April 2016
Pukul	: 09.00 - selesai
Lokasi	:Ruangan bidang komunikasi dan informatika
Informasi Narasumber I	
Nama	: Bambang Noertjahjo
Jabatan	: Kepala bidang komunikasi dan informatika
Instansi	:Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung
Lama bekerja	:2 tahun
Informasi Narasumber II	
Nama	: Andhi Priono
Jabatan	: Staff bidang komunikasi dan informatika

Instansi :Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung Lama bekerja :3 tahun

Tabel B.1 Hasil wawancara

No	ORGANIZATION VIEW
	Critical Assets
1	**Pertanyaan:**
	Proses bisnis apa yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
	Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung melakukan proses bisnis sesuai dengan peraturan daerah kabupaten Tulungagung dan sesuai dengan aturan kementerian komunikasi dan informatika RI.
2	**Pertanyaan:**
	Aset apa saja yang ada di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
	Komputer, Server, CCTV, Printer, Genset, Jaringan,Data
3	**Pertanyaan:**
	Aset apa yang paling penting di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
	Semua aset yang ada di dinas perhubungan komunikasi dan informatika penting, tetapi yang paling penting adalah jaringan. Jaringan digunakan untuk memantau lalu lintas yang ada di kabupaten Tulungagung dan digunakan untuk proses pengadaan barang secara elektronik. Selain jaringan, data juga termasuk aset penting karena data tersebut berisikan vendor-vendor untuk pengadaan barang, data barang yang perlu dibeli pada setiap dinas.
4	**Pertanyaan:**
	Seberapa besar pengaruh jaringan terhadap keberlangsungan proses bisnis yang ada pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?

	Jawaban:
	Sangat besar pengaruhnya karena jaringan diperlukan untuk memantau lalu lintas, pengelolaan pengadaan barang secara elektronik dan pengelolaan website pemerintah
5	**Pertanyaan:**
	Sistem informasi apa yang terdapat pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
	1. Website pemerintah: berisi informasi seputar kabupaten Tulungagung, komentar masyarakat terkait kepemimpinan bupati, keluh kesah masyarakat Tulungagung. 2. LPSE: pengadaan barang diseluruh dinas dikabupaten Tulungaung, berisi data pihak penyedia barang, dinas yang akan melakukan pengadaan barang, harga barang, dll. 3. Pemantauan lalin: memantau kondisi lalu lintas dengan melihat CCTV yang terpasang didaerah rawan macet.
7	**Pertanyaan:**
	Siapa saja yang mempunyai kepentingan menggunakan aplikasi dan layanan TI?
	Jawaban:
	Bidang lalu lintas dan angkutan, bidang pengendalian dan operasi, bidang komunikasi dan informatika
	Security Requirement for Critical Assets
1	**Pertanyaan:**
	Apakah aplikasi dan layanan TI di lingkungan dinas perhubungan komunikasi dan informatika sudah memberikan *checklist* terkait kebutuhan keamanan aset informasi yang dimiliki? e. Jika sudah, apa saja kebutuhan keamanan yang dilihat dari *checklist* tersebut yang sudah terpenuhi? f. Jika belum, perlukan adanya *checklist* terkait kebutuhan keamanan aset informasi yang dimiliki?
	Jawaban:

	Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung belum memiliki checklist terkait keamanan informasi.
2	**Pertanyaan:**
	Adakah aturan dalam melakukan pengamanan terkait akses informasi pada aplikasi dan layanan TI?
	Jawaban:
	Ada
3	**Pertanyaan:**
	Apakah ada pemeriksaan secara rutin terhadap keamanan aset?
	Jawaban:
	Tidak ada
4	**Pertanyaan:**
	Apakah ada kegiatan maintenance pada aset?
	Jawaban:
	Tidak ada
5	**Pertanyaan:**
	Apakah ada mekanisme untuk mencegah pembobolan aset?
	Jawaban:
	Ada, dengan memasang CCTV disetiap ruangan.
6	**Pertanyaan:**
	Apakah sensitifitas informasi dilindungi oleh tempat penyimpanan yang aman?
	Jawaban:
	Belum
	Threat to Critical Assets
1	**Pertanyaan:**

	Apakah aset informasi dinas perhubungan komunikasi dan informatika pernah mengalami ancaman? e. Jika pernah, apa saja ancaman yang pernah dialami? f. Jika belum, ancaman apakah yang memungkinkan terjadi?
	Jawaban:
	Pasokan listrik, gangguan jaringan, gangguan server, malware, gempa bumi
2	**Pertanyaan:**
	Berikan contoh bagaimana pihak dalam yang bertindak secara tidak sengaja dapat menggunakan akses fisik untuk mengancam sistem ini?
	Jawaban:
	bisa jadi dengan melakukan sabotase dan mengakses komputer admin
3	**Pertanyaan:**
	Bagaimana melakukan pencegahan terhadap ancaman aset TI?
	Jawaban:
	Pada dinas perhubungan kabupaten Tulungagung belum ada pencegahan terhadap aset TI dikarenakan karyawan pada bidang komunikasi dan informasi sedikit sehingga hafal siapa saja yang ada didalam ruangan. Selain itu dilengkapi dengan pemasangan CCTV
4	**Pertanyaan:**
	Seberapa sering terjadinya server down pada server?
	Jawaban:
	Sekali dalam sebulan
5	**Pertanyaan:**

	Seberapa sering terjadinya pembobolan data?
	Jawaban:
	Belum pernah
6	**Pertanyaan:**
	Apakah pada aplikasi dan layanan TI dilakukan *update* anti virus?
	Jawaban:
	Sudah dilakukan update anti virus
7	**Pertanyaan:**
	Apakah ada SOP untuk meng*update* sistem tersebut?
	Jawaban:
	Tidak ada
	Current Security Practice
1	**Pertanyaan:**
	Apakah ada informasi mengenai aplikasi dan layanan TI di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
	Ada di perda kabupaten Tulungaganung dan pedoman yang dikeluarkan kementrian komunikasi dan informatika
2	**Pertanyaan:**
	Apakah aplikasi dan layanan TI menerapkan *framework* atau standar keamanan khusus aset informasi? e. Jika iya, standart atau *framework* apa yang digunakan? f. Jika tidak, perlukan adanya standart atau *framework* khusus pengamanan aset informasi?
	Jawaban:

	Dinas perhubungan komunikasi dan informatika kabupaten Tulungagung perlu mempunyai standar/framework khusus terkait aset informasi.
3	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika kabupaten Tulungagung sudah melakukan penilaian risiko untuk keamanan informasi?
	Jawaban:
	Belum
4	**Pertanyaan:**
	Apakah bidang komunikasi dan informatika menerima dan bertindak atas laporan rutin dari informasi yang berhubungan dengan keamanan?
	Jawaban:
	Ya, dinas bertindak atas laporan yang berhubungan dengan keamanan informasi
5	**Pertanyaan:**
	Apakah kendala dalam melakukan implementasi standart atau *framework* pengamanan aset informasi pada dinas perhubungan komunikasi dan informatika kabupaten Tulungagung?
	Jawaban:
	Kendala yang ada adalah dinas terkait tidak memiliki standar/framework terkait pengamanan aset informasi
6	**Pertanyaan:**
	Apakah di dinas perhubungan komuniasi dan informatika sudah memiliki kebijakan dan prosedur dalam melindungi informasi ketika bekerja sama dengan perusahaan lain?
	Jawaban:

	Dinas terkait belum memiliki kebijakan dan prosedur secara jelas untuk melindungi informasi ketika bekerja sama dengan perusahaan lain.
	Current Organizational
1	**Pertanyaan:**
	Apa masalah yang sering terjadi di dinas perhubungan komunikasi dan informatika terkait *asset informasi?*
	Jawaban:
	Server dan perangkat jaringan
2	**Pertanyaan:**
	Pernahkah terjadi pencurian informasi pada dinas perhubungan komunikasi dan informatika e. Jika pernah, informasi apa yang telah dicuri? Apa penyebab *asset informasi* tersebut bermasalah? f. Jika belum, informasi apa saja yang memungkinkan terjadinya pencurian?
	Jawaban:
	belum pernah, data aset yang dimiliki seluruh dinas dikabupaten Tulungagung
3	**Pertanyaan:**
	Apakah kapasitas server yang dimiliki dinas perhubungan komunikasi dan informatika sudah mencukupi?
	Jawaban:
	sementara ini cukup, akan tetapi dikarenakan kebutuhan pemantauan kelancaran lalulintas, penambagan data terkait pengadaaan aset diseluruh dinas dan penambahan informasi di website pemerintah server overload sehingga menyebabkan server down untuk kedepannya ada kemungkinan diperlukan penambahan server serta pembaharuan server untuk backup.
4	**Pertanyaan:**

	Berapa kali dalam setahun dinas perhubungan komunikasi dan informatika melakukan evaluasi terhadap keamanan teknologi informasi?
	Jawaban:
	Tidak ada patokan khusus terkait kapan evaluasi keamanan teknologi informasi dilakukan.
5	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika sudah melakukan verifikasi untuk setiap divisi dalam mengurus hak akses dan otorisasi?
	Jawaban:
	Sudah dilakukan
6	**Pertanyaan:**
	Bagaimana kode etik yang diterapkan pada dinas perhubungan komunikasi dan informaika terkait pengamanan aset informasi?
	Jawaban:
	Untuk kode etik secara umum dari pihak dinas sudah ada, seperti aturan yang berisi tentang hukuman jika terdapat karyawan yang membagikan data *confidential* ke pihak yang tidak berwenang. Namun untuk penerapan kode etik secara spesifik yang hanya berfokus pada pengamanan aset informasi belum ada.
	TECHNOLOGICAL VIEW
	Key Component
1	**Pertanyaan:**
	Perangkat IT apa saja yang dimiliki oleh dinas perhubungan komunikasi dan informatika kabupaten Tulunggung?
	Jawaban:
	• Software: sistem pemantauan lalu lintas, sistem pengadaan barang dan jasa • Hardware: server, CCTV, komputer

	• Network: sistem jaringan • Data: data vendor LPSE
	Current Technology Vulnerability
1	**Pertanyaan:**
	Apakah di dinas perhubungan komunikasi dan informatika terdapat prosedur untuk menjaga kerentanan teknologi seperti meninjau sumber informasi, mengelola keamanan tempat penyimpanan dan mengidentifikasi komponen infrastruktur?
	Jawaban:
	Untuk saat ini dinas perhubungan komunikasi dan informatika belum memiliki prosedur manajemen kerentanan teknologi. Dalam operasioalnya melakukan evaluasi kerentanan teknologi meskipun tidak membuat penjadwalannya secara rutin.
2	**Pertanyaan:**
	Bagaimana bentuk penanggulangan terkait adanya gangguan TI?
	Jawaban:
	Melakukan perbaikan sendiri atau menghubungi pihak ketiga jika diperlukan
3	**Pertanyaan:**
	Apakah dinas komunikasi dan informatika menjadwalkan dan melakukan evaluasi kerentanan TI secara berkala?
	Jawaban:
	Tidak
4	**Pertanyaan:**
	Apakah dinas komunikasi dan informatika memiliki dokumen mengenai jenis-jenis kerentanan dan metode serangannya?
	Jawaban:

	Tidak
5	**Pertanyaan:**
	Siapa yang bertanggung jawab memanajemen kerentanan TI dinas komunikasi dan informatika?
	Jawaban:
	kepala seksi pengembangan TI dibawah bidang komunikasi dan informatika
6	**Pertanyaan:**
	Apakah dinas perhubungan komunikasi dan informatika menyediakan kesempatan bagi staff TI untuk mengikuti pelatihan untuk mengelola kerentanan teknologi dan menggunakan alat-alat evaluasi kerentanan?
	Jawaban:
	Iya
	RISK ANALYSIS
	Protection Strategy
1	**Pertanyaan:**
	Adakah strategi dalam melakukan pengamanan data dan informasi di dinas perhubungan komunikasi dan informatika? e. Jika sudah ada, strategi pengamanan data dan informasi apa yang diterapkan? f. Jika belum ada, perlukah adanya pengamanan data dan informasi?
	Jawaban:
	Belum ada. Perlu adanya pengamanan data dan informasi
	Risk Mitigation Plans
1	**Pertanyaan:**

	Apakah aplikasi dan layanan TI dinas perhubungan komunikasi dan informatika memiliki *Disaster Recovery Plan (DRP)* pada aset informasinya? e. Jika sudah ada, aset informasi apakah yang sudah ter-*cover* oleh DRP tersebut? f. Jika belum ada, perlukah adanya *Disaster Recovery Plan (DRP)* pada aset informasi?
	Jawaban:
	Belum ada. Perlu adanya DRP pada aset informasi

LAMPIRAN C
MITIGASI RISKO

Tabel C.1 Mitigasi risiko

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
Hardware: • Komputer • CCTV • Server	Hardware failure	*Maintenance* yang tidak teratur	• Kerusakan asset teknologi • Kinerja hardware menurun	**Performance evaluation:** Untuk menjaga kualitas hardware diperlukan evluasi performa.	**Monitoring, measurement, analysis adn evaluation:** Merupakan prosedur monitoring terhadar aset	• Organisasi menetapkan kebijakan mengenai monitorng aset teknologi informasi. • Monitoring dilakukan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
					teknologi informasi yang dimiliki oleh organisasi.	secara berkala untuk memastikan aset teknologi informasi berjalan sesuai dengan apa yang diharapkan organisasi.
		Server overheat	• Kerusakan aset teknologi	**Information security incident management:**	**Responbilities and procedures:**	• Organisasi harus menerapkan prosedur manajemen

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
			• Kehilangan data • Database corrupt	Untuk menjaga performa teknologi informasi ketika mengalami gangguan diperlukan prosedur incident management.	Merupakan prosedur untuk melakukan manajemen insiden keamanan informasi pada organisasi.	insiden keamanan informasi. • Prosedur harus mencakup semua aset teknologi informasi. • Orang yang bertanggung jawab atas prosedur ini harus mengerti dan pahan terkait pengelolaan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						insiden keamanan informasi.
		Kerusakan fisik pada hardware	Kerusakan aset teknologi informasi	**Performance evaluation:** Untuk menjaga kualitas hardware diperlukan evluasi performa.	**Monitoring, measurement, analysis adn evaluation:** Merupakan prosedur monitoring terhadar aset teknologi informasi yang	• Organisasi menetapkan kebijakan mengenai monitorng aset teknologi informasi. • Monitoring dilakukan secara berkala untuk memastikan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
					dimiliki oleh organisasi.	aset teknologi informasi berjalan sesuai dengan apa yang diharapkan organisasi. • Aset teknologi harus mempunyai "masa" yaitu kapan aset teknologi informasi

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						tersebut diganti yang baru.
Layanan teknologi informasi: • Website pemerintah • Pemantauan kondisi lalu lintas • Pengadaan barang LPSE.	Software failure	Kesalahan coding pada fungsional software	Aplikasi crash	**System and aplication acess control:** Untuk menjaga software berjalan sesuai dengan harapan organisasi.	**Access control to program source code:** Merupakan prosedur untuk menbatasi source code yang digunakan.	• Organisasi harus menetapkan kebijakan terkait dengan kontrol akses pada sistem dan aplikasi. • Aplikasi harus sesuai dengan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						permintaan organisasi. • Pemilihan vendor dalam pembuatan aplikasi harus jelas. • Organisasi mempunyai kontrak keja dengan vendor, sebagai bukti MOU.
	Network failure	Speed koneksi	Kegagalan konektifitas	**Supllier service**	**Monitoring and review**	• Organisasi harus

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
Jaringan (*network*)		internet yang lemah dan tidak stabil	internet untuk melakukan aktivitas bisnis	**delivery management:** Untuk menjaga kualitas layanan organisasi	**of supllier services:** Merupakan kegiatas review service yang diberiakan oleh supplier kepada organisasi.	menerapkan prosedur pelayanan suplier untuk menjaga kualiatas layanan publik. • Monitoring suplier dilakukan secara berkala untuk mengukur kualitas

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						servis supllier. • Ketika kualiatas servis menurun, organisasi berhak memperingatkan untuk meningkatkan kualitas tersebut.
		Kurangnya mekanisme pemantaua	IP spoofing	**Performance evaluation:** Untuk menjaga	**Monitoring, measurement, analysis**	• Organisasi menetapkan kebijakan mengenai

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
		n terhadap jaringan		kualitas hardware diperlukan evluasi performa.	**adn evaluation:** Merupakan prosedur monitoring terhadar aset teknologi informasi yang dimiliki oleh organisasi.	monitorng aset teknologi informasi. • Monitoring dilakukan secara berkala untuk memastikan aset teknologi informasi berjalan sesuai dengan apa yang

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
						diharapkan organisasi. • Aset teknologi jaringan merupakan aset terpenting dalam organisasi, untuk diperlukan pemantauan terhadap mekanisme jaringan.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
		Gangguan jaringan pada provider	Jaringan menjadi lambat	**Supllier service delivery management:** Untuk menjaga kualitas layanan organisasi	**Monitoring and review of supllier services:** Merupakan kegiatas review service yang diberiakan oleh supplier kepada organisasi.	• Organisasi harus menerapkan prosedur pelayanan suplier untuk menjaga kualiatas layanan publik. • Monitoring suplier dilakukan secara berkala untuk mengukur

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
						kualitas servis supllier. • Ketika kualiats servis menurun, organisasi berhak memperingatkan untuk meningkatkan kualitas tersebut. • Orgaisasi melaporakan gangguan yang

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						disebabkan oleh servis suplier.
		Kerusakan pada infrastruktur jaringan	Jaringan menjadi lambat	**Equipment:** Untk meningkatkan kualitas layanan diperlukan peralatan pendukung yang terjamin.	**Supporting utilies:** Merupakan prosedur pemelikihan peralatan pendukung layanan organisasi.	• Organisasi harus menerapkan prosedur terkait dengan perlatan pendukung layanan yang dikeluarkan organisasi. • Peralatan tersebut

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						harus sesuai dengan kebutuhan organisasi dan terjamin kualitasnya.
		Kesalahan dalam melakukan konfigurasi access point	Jaringan internet lambat	**Equipment:** Untk meningkatkan kualitas layanan diperlukan peralatan pendukung yang terjamin.	**Equipment siting and protection:** Merupakan prosedur peletakan dan keamanan peralatan	• Organisasi harus menerapkan prosedur terkait dengan perlatan pendukung layanan yang dikeluarkan organisasi.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
					yang digunakan.	• Peralatan tersebut harus sesuai dengan kebutuhan organisasi dan terjamin kualitasnya.
		Kabel digigit oleh hewan	Kerusakan aset teknologi Jaringan internet lambat	**Equipment:** Untk meningkatkan kualitas layanan diperlukan peralatan	**Equipment siting and protection:** Merupakan prosedur peletakan dan keamanan peralatan	• Organisasi harus menerapkan prosedur terkait dengan perlatan pendukung layanan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
				pendukung yang terjamin.	yang digunakan.	yang dikeluarkan organisasi. • Peralatan tersebut harus sesuai dengan kebutuhan organisasi dan terjamin kualitasnya. • Peralatan harus dilindungi secara fisik, misalnya kabel harus dilindungi

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						dengan menggunakan pipa atau yang lainnya.
Jaringan (*network*)	Power failure	Pemadaman listrik	• Komputer mati • Jaringan terganggu • Menurunkan kinerja karyawan	**Supllier service delivery management:** Untuk menjaga kualitas layanan organisasi	**Monitoring and review of supllier services:** Merupakan kegiatas review service yang diberiakan oleh supplier	• Organisasi harus menerapkan prosedur pelayanan suplier untuk menjaga kualiatas layanan publik.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
					kepada organisasi.	• Monitoring suplier dilakukan secara berkala untuk mengukur kualitas servis supllier. • Ketika kualiatas servis menurun, organisasi berhak memperingatkan untuk

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						meningkatkan kualitas tersebut.
Data: • Data vendor LPSE • Data pengadaan barang setiap dinas • Data informasi seputar kegiatan di Kabapuate	Backup data failure	Organisasi tidak melakukan prosedur *backup*	• Kehilangan data • Data termanipulasi	**Backup:** Untuk menjaga data agar tetap terjaga.	**Information backup:** Merupakan prosedur terkait dengan backup data.	• Organisasi menerapkan terkait prosedur backup data. • Backup data harus dilakukan secara teratur. • Tanggungjawab operasional backup

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
n Tulungagung						harus dipisah. • Diperlukan kontrol untuk menjaga integritas data yang dibackup.
		Server down	• Menurunkan kinerja pegawai • Layanan teknologi nformasi putus	**Performance evaluation:** Untuk menjaga kualitas hardware diperlukan	**Monitoring, measurement, analysis adn evaluation:** Merupakan prosedur monitoring	• Organisasi menetapkan kebijakan mengenai monitorng aset teknologi informasi.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
				evluasi performa.	terhadar aset teknologi informasi yang dimiliki oleh organisasi.	• Monitoring dilakukan secara berkala untuk memastikan aset teknologi informasi berjalan sesuai dengan apa yang diharapkan organisasi. • Aset teknologi jaringan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						merupakan aset terpenting dalam organisasi, untuk diperlukan pemantauan terhadap mekanisme jaringan.
Karyawan (*people*)	Human atau technician error	Kurangnya dokumentasi (user manual) untuk	Informasi penting bisa diakses oleh pihak yang tidak berwenang	**Human resource security:** Merupakan pemilihan karyawan	**Prior to employment:** Merupakan persyaratan yang	• Organisasi harus mempunyai persyaratan khusus yang ditujukan oleh calon

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
		karyawan baru	Kehilangan data penting	yang cocok terhadap tanggungjawab yang diberikan	diberikan oleh organisasi terhadap karyawan baru	karyawan yang bekerja akan bekerja pada organisasi • Mendefinisikan tanggungjawab karyawan yang bertanggung jawab atas pengelolaan data.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
		PC terserang virus	Menurunkan kinerja karyawan dalam pelayanan publik TI	**Control of operational software:** Untuk melakukan kontrol terhadap software yang digunakan organisasi.	**Installation of software on operating system:** Merupakan prosedur instalasi software pada sistem operasi.	• Organisasi harus menetapkan prosedur terkait pemilihan software. • Software yang digunakan harus legal dan mempunyai lisensi. • Pada setiap desktop terdapat

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
						software scanning untuk mencegas software yang tidak diijinkan diinstal pada komputer terinstal. • Semua komputer harus ada antivirus untuk mencegas virus

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						menyerang komputer. • Update antivirus harus dilakukan secara berkala.
		Kesalahan dalam penginputan dan penghapusan data	• Data termanupulasi • Kehilangan data	**Human resource security:** Merupakan pemilihan karyawan yang cocok	**During employment :** Merupakan peraturan yang dikeluarkan	• Organisasi harus menyampaikan aturan keamanan informasi pada seluruh karyawan.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
				terhadap tanggungjawab yang diberikan	organisai terkait dengan keamanan informasi	• Melakukan log aktivitas dalam proses pengelolaan data. • Mendefinisikan tanggungjawab karyawan yang bertanggung jawab atas pengelolaan data.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
		Kurangnya training prosedur penggunaan TI yang diberikan	• Kinerja pegawai tidak optimal • Kerusakan aset teknologi	**Human resource security:** Merupakan pemilihan karyawan yang cocok terhadap tanggungjawab yang diberikan	**During employment :** Merupakan peraturan yang dikeluarkan organisai terkait dengan keamanan informasi	• Organisasi harus menyampaikan aturan keamanan informasi pada seluruh karyawan. • Organisasi harus mempunyai persyaratan khusus yang ditujukan oleh calon karyawan yang bekerja akan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						bekerja pada organisasi
		Karyawan tidak logout ketika meninggalkan komputer	Informasi penting diakses oleh pihak yang tidak berwenang	**System and aplication acess control:** Untuk menjaga software dan aplikasi berjalan sesuai dengan harapan organisasi.	**Access control to program source code:** Merupakan prosedur untuk menbatasi source code yang digunakan.	• Organisasi harus menetapkan kebijakan terkait dengan kontrol akses pada sistem dan aplikasi. • Organisasi menetapkan aktivitas log untuk

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						menjaga agar pihak luar tidak bisa mengakses informasi penting.
Jaringan (*network*)	Serangan hacker	Lemahnya keamanan di sistem internal TI	IP spoofing	**Performance evaluation:** Untuk menjaga kualitas hardware diperlukan evluasi performa.	**Monitoring, measurement, analysis adn evaluation:** Merupakan prosedur monitoring terhadar aset teknologi	• Organisasi menetapkan kebijakan mengenai monitorng aset teknologi informasi. • Monitoring dilakukan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
					informasi yang dimiliki oleh organisasi.	secara berkala untuk memastikan aset teknologi informasi berjalan sesuai dengan apa yang diharapkan organisasi. • Aset teknologi jaringan merupakan aset

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						terpenting dalam organisasi, untuk diperlukan pemantauan terhadap mekanisme jaringan.
Karyawan (*people*)	Penyalahgunaan hak akses	Tidak ada penggunaan hak akses	Informasi penting diakses oleh pihak yang tidak berwenang	**Assess control** Merupakan pembatasan hak akses	**User acssess managemen**t: Merupakan pembatasan hak akses untuk meminimalis	• Organisasi harus melakukan pembatasan hak akses pada setiap karyawan supaya informasi

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
					ir gangguan keamanan melalui pihak internal dan eksternal	penting tetap terjaga. • Memberikan prosedur verifikasi pengguna ketika pengguna akan mengakses data penting. • Pengguna diminta untuk menandatangani untuk

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						menjaga password pribadi agar tidak dibertahukan ke publik. • Melakukan sanksi ketika tahu password disebarluakan.
		Adanya share login	Semua orang tahu informasi penting	**Information transfer**: Merupakan pembatasan transfer	**Information transfer policies and procedure:**	• Organisasi harus melakukan pembatasan transfer

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
				informasi yang dilakukan oleh organisasi	Merupakan kebijakan pertukaran informasi dengan pihak internal dan eksternal organisasi	informasi didalam internal organisasi maupun di eksternal organisasi. • Pengguna diminta untuk menandatangani untuk menjaga password pribadi agar tidak dibertahukan ke publik.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						• Melakukan sanksi ketika tahu password disebarluakan.
		Tidak ada pengaturan untuk manajemen hak akses user atau user privilege	Semua karyawan bisa mengakses informasi yang bersifat penting	**System and aplication acess control:** Untuk menjaga software dan aplikasi berjalan sesuai dengan	**Use of priviliege uitilities program:** Merupakan prosedur dalam menggunakan program/keg	• Organisasi harus menetapkan kebijakan terkait dengan kontrol akses pada sistem dan aplikasi.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
				harapan organisasi.	iatan penting.	• Organisasi menetapkan aktivitas log untuk menjaga agar pihak luar tidak bisa mengakses informasi penting. • Penggunaan password ketika mengakses sistem dan aplikasi penting.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
		Password tidak pernah diganti	Hak akses disalahgunakan oleh orang lain	**System and aplication acess control:** Untuk menjaga software dan aplikasi berjalan sesuai dengan harapan organisasi.	**Password managemen t system:** Merupakan prosedur terkait dengan pembuatan password.	• Organisasi harus menetapkan kebijakan terkait dengan kontrol akses pada sistem dan aplikasi. • Password yang dibuat harus unik. • Password tidak boleh disimpan dalam

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						sistem komputer tanpa dilindungi.
	Pencurian media atau informasi penting	Kurangnya pengamanan organisasi	Informasi yang bersifat penting bisa diakses oleh pihak yang tidak mempunyai wewenang	**System and aplication acess control:** Untuk menjaga software dan aplikasi berjalan sesuai dengan harapan organisasi.	**Information access restriction:** Merupakan prosedur akses terhadap informasi penting.	• Organisasi harus menetapkan kebijakan terkait dengan kontrol akses pada sistem dan aplikasi. • Organisasi menetapkan aktivitas log

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
						untuk menjaga agar pihak luar tidak bisa mengakses informasi penting. • Menyediakan menu untuk mengontrol akses ke fungsi sistem aplikasi.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
		Kurangnya mekanisme pemantauan	Layanan publik teknologi informasi tidak optimal	**Equipment:** Untk meningkatkan kualitas layanan diperlukan peralatan pendukung yang terjamin.	**Equipment maintenance:** Merupakan prosedur perawatan peraltan yang digunakan oleh organisasi.	• Organisasi harus menerapkan prosedur terkait dengan perlatan pendukung layanan yang dikeluarkan organisasi. • Peralatan yang sudah tidak berjalan dengan baik harus

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						diupdate atau diganti dengan yang beru.
		Tidak ada peraturan terkait keamanan informasi	Informasi yang bersifat penting bisa diakses oleh pihak yang tidak mempunyai wewenang	**System and aplication acess control:** Untuk menjaga software dan aplikasi berjalan sesuai dengan harapan organisasi.	**Secure logon procedure:** Merupakan prosedur keamanan ketika logon.	• Organisasi harus menetapkan kebijakan terkait dengan kontrol akses pada sistem dan aplikasi. • Organisasi menetapkan aktivitas log

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
						untuk menjaga agar pihak luar tidak bisa mengakses informasi penting. • Karyawan diminta untuk menandatangi perjanjian tidak boleh menyebarluaskan passwor

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						yang dimiliki. • Pemberikan sanki ketika karyawan menyebarluaskan passwor yang dimiliki.
Jaringan (*network*)	Kebakaran	Korsleting listrik	• Dapat mengancam keselamatan karyawan	**Organization of information security:** Organisasi menerapkan	**Internal organization:** Penerapakan keamanan organisasi terlebih	• Organisasi harus menerapkan prosedur keamanan informasi untuk

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
			• Terjadi kerusakan aset teknologi • Menyebabkan jaringan lemot	keamanan informasi	dahulu dilakukan oleh internal organisasi	menjamin keamanan informasinya. • Organisasi melakukan perlindungan terhadap aset teknologi yang dimiliki. • Bahan berbahaya dan mudah terbakar harus disimpan

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						pada jarak yang aman. • Organisasi harus mempunyai peralatan pemadam kebakaran yang diletakkan pada titik rawan.
Data: • Data vendor LPSE	Memory penuh	Kapasitas memori server yang sudah tidak	Server tidak bisa menyimpan database baru	**Performance evaluation:** Untuk menjaga kualitas	**Monitoring, measurement, analysis adn evaluation:**	• Organisasi menetapkan kebijakan mengenai monitorng

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
• Data pengadaan barang setiap dinas • Data informasi seputar kegiatan di Kabapuaten Tulungagung		memenuhi kebutuhan (memori full)		hardware diperlukan evluasi performa.	Merupakan prosedur monitoring terhadar aset teknologi informasi yang dimiliki oleh organisasi.	aset teknologi informasi. • Monitoring dilakukan secara berkala untuk memastikan aset teknologi informasi berjalan sesuai dengan apa yang diharapkan organisasi.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						• Aset yang tidak bekerja dengan baik harus segera diupdate ata diganti.
	Modifikasi dan pencurian database	Staf mengetahui kelemahan pada aplikasi	Membocorkan informasi kepada orang lain	**Leadership:** Untuk menjaga layanan publik teknologi informasi agar tetap optimal.	**Leadership and commitment:** Meupakan prosdur terkait dengan komitmen dan	• Organisasi harus menetapkan prosedur terkait dengan komitmen pegwai dan pimpinan organisasi.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
					pimpinan perusahaan.	• Organisasi harus menjaga tanggungjawab yang telah diberikan oleh negara. • Organisasi menjamin layanan teknologi informasi sesuai dengan harapan masyarakat.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
		Pengolahan data illegal oleh karyawan	• Data termanipulasi • Kehilangan data	**Leadership:** Untuk menjaga layanan publik teknologi informasi agar tetap optimal.	**Organizational roles, responbilities, authorities:** Merupakan prosedur terkait aturan yang dikelurkan organisasi.	• Organisasi harus menetapkan prosedur terkait dengan komitmen pegwai dan pimpinan organisasi. • Organisasi harus menjaga tanggungjawab yang telah diberikan oleh negara.

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	**Sub-Kontrol**	**Keterangan**
						• Adanya sakni ketika komitmen tidak dijalankan dengan optimal.
Karyawan (*people*)	Pelanggaran terhadap aturan atau regulasi yang berlaku	Kurangnya sosialisasi tentang regulasi dan sanksinya	Kinerja pegawai tidak optimal	**Organization of information security:** Organisasi menerapkan keamanan informasi	**Internal organization:** Penerapakan keamanan organisasi terlebih dahulu dilakukan	• Organisasi harus melakukan pengamanan informasi. • Sumberdaya manusia yang ada dalam organisasi

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
					oleh internal organisasi	tahu mengenai pentingnya keamanan informasi. • Sumberdaya manusias yanga dalam organisasi mempunyai keahlian dalam bidang teknologi informasi. • Pemberian sanki ketika terjadi

Aset	Risiko	Penyebab Risiko	Dampak Risiko	Tindakan Mitigasi Berdasarkan ISO 27001		
				Kontrol	Sub-Kontrol	Keterangan
						kesalahan yang berasal dari keceroboha n karyawan.

LAMPIRAN D
VALIDASI

Berikut ini merupakan buktit validasi yang digunakan untuk menilai kesesuaian mitigasi dan control ISO 27001.

Gambar D.1 Validasi

Gambar D.2 Proses validasi

BAB VII
PENUTUP

7.1 Kesimpulan

Berdasarkan hasil penelitian, berikut ini merupakan beberapa kesimpulan yang dapat diambil :

1. Dari proses identifikai risiko terhadap layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung diperoleh 13 risko dan 31 kejadian risiko dengan demikian terdapat risiko yang memiliki kejadian risiko lebih dari satu dikarenakan perbedaan penyebab.
2. Hasil penilaian dikategorikan dalam empat level penilaian risiko yaitu *very high, high, medium, low,* dan *very low*.
    a) Level *very high mempunyai* 4 risiko dengan nilai RPN sebesar 378.
    b) Level *high* mempunyai 2 risiko dengan nilai RPN antara 151-200.
    c) Level *medium* mempunyai 7 risiko dengan nilai RPN antara 101-150.
    d) Level *low* mempunyai 13 risiko dengan nilai RPN antara 51-100.
    e) Level *very low* mempunyai 5 risiko dengan nilai RPN antara 0-50.
3. Dari hasil identifikasi risiko terdapat 12 kontrol dalam ISO 27001 yang dapat dijadikan acuan penentuan rekomendasi mitigasi risiko.

7.2 Saran

Berdasarkan pelaksanaan penelitian tugas akhir ini, saran yang dapat diberikan agar bisa dijadikan rekomendasi untuk penelitian selanjutnya adalah:

- Metode OCTAVE seharusnya menerapkan metode identify senior management knowledge, tetapi karena keterbatasan akses peneliti melakukan pendekatan dengan menanyakan bagaimana senior management dipandang dukungannya terhadap keamanan informasi oleh pihak operasional dan staf. Maka untuk penelitian selanjutnya perlu dipertimbangkan untuk melakukan penggalian informasi terhadap senior management di organisasi.

DAFTAR PUSTAKA

[1] P. K. Tulungagung, PERDA & Pembentukan Struktur Organisasi TUPOKSI, Tulungagung, 2013.

[2] P. M. J, The OCTAVE methodology as a risk analysis tool for business resources. roceedings of the International Multiconference on Computer Science and Information Technology.

[3] "What is security analys?," [Online]. Available: http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm. [Accessed 16 January 2016].

[4] Paryati, "Keamanan Informasi," UPN Veteran, Yogjakarta, 2008.

[5] Widodo, "Perencanaan dan implementasi SMKI," Universitas Diponegoro, Semarang, 2008.

[6] T. Archives, What is an Information Asset?, The National Archives.

[7] Gygi, DeCarlo and William, "FMEA," 2005.

[8] "PDCA Security," [Online]. Available: http://www.pdca-security.com/.

[9] Y. K. R, "Case Study Research Design and Methods Second Edition," *International Educational and Professional Publisher,* vol. 5.

[10] Z. Z, Case Study As A Research Method," J. Kemanus, Bil9, 2007.

[11] K. K. d. I. RI, Panduan Penerapan Tatakelola KIPPP, Jakarta, 2011.

BIODATA PENULIS

Penulis yang lahir di Tulunagaung pada tanggal 11 Juni 1994 ini merupakan anak kedua dari tiga bersaudara. Penulis telah menempuh pendidikan formal di SDN Pojok 3 Tulungagung, SMPN 1 Campurdarat Tulungagung, SMAN 1 Pakel Tulungagung, dan akhirnya masuk menjadi mahasiswi Sistem Informasi angkatan 2012 melalui Jalur tulis. 5212 100 066 adalah NRP dari penulis sebagai mahasiswa JSI-ITS. Penulis merupakan anggota aktif himpunan mahasiswa sistem informasi ITS. Pada tahun terakhir penulis mengambil bidang studi Manajemen Sistem Informasi dengan topik tugas akhir tata kelola keamanan informasi. Penulis dapat dihubungi melalui e-mail: balqislembah@gmail.com.