TUGAS AKHIR – KS 141501

IDENTIFIKASI, PENILAIAN, DAN MITIGASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001 : 2005 DAN ISO 27002 : 2013 MENGGUNAKAN METODE FMEA (STUDI KASUS : ISNET)

KRISNA HARINDA DEWANTARA
NRP 5211 100 148

Dosen Pembimbing
Bekti Cahyo H, S.Si., M.Kom
Hanim Maria Astuti, S.Kom, M.Sc

Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2016

FINAL PROJECT – KS 141501

IDENTIFICATION, ASSESSMENT AND RISK MITIGATION BASED ON ISO 27001 : 2005 & ISO 27002 : 2013 WITH FMEA METHOD

Krisna Harinda Dewantara
NRP 5211 100 148

Supervisor
Bekti Cahyo H, S.Si., M.Kom
Hanim Maria Astuti, S.Kom, M.Sc

Information System Department
Faculty of Information Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2016

LEMBAR PENGESAHAN

IDENTIFIKASI, PENILAIAN, DAN MITIGASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001 : 2005 DAN ISO 27002 :2013 MENGGUNAKAN METODE FMEA (STUDI KASUS : ISNET)

TUGAS AKHIR

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

Oleh:

KRISNA HARINDA DEWANTARA
NRP 5211 100 148

Surabaya, Januari 2016

KETUA
JURUSAN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

IDENTIFIKASI, PENILAIAN, DAN MITIGASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001 : 2005 DAN ISO 27002 :2013 MENGGUNAKAN METODE FMEA (STUDI KASUS : ISNET)

TUGAS AKHIR

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

Oleh:

KRISNA HARINDA DEWANTARA
NRP 5211 100 148

Disetujui Tim Penguji: Tanggal Ujian : 13 Januari 2016

Periode Wisuda : Maret 2016

Bekti Cahyo Hidayanto, S.Si, M.Kom **(Pembimbing 1)**

Hanim Maria Astuti, S.Kom, M.Sc **(Pembimbing 2)**

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

Eko Wahyu Tyas, S.Kom, M.BA **(Penguji 2)**

IDENTIFIKASI, PENILAIAN, DAN MITIGASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2005 DAN ISO 27002 : 2013 MENGGUNAKAN METODE FMEA (STUDI KASUS : ISNET)

Nama Mahasiswa : KRISNA HARINDA D
NRP : 5211100148
Jurusan : Sistem Informasi FTIf – ITS
Dosen Pembimbing 1 : Bekti Cahyo H, S.Si., M.Sc
Dosen Pembimbing 2 : Hanim Maria Astuti, S.Kom, M.Sc

ABSTRAK

Sebuah sistem informasi yang sudah berjalan dengan baik belum dapat dijamin keamanan informasinya dikarenakan adanya ancaman dari pihak luar yang dapat terjadi jika suatu organisasi tidak memperhatikan adanya risiko yang melekat pada proses tersebut. Untuk itu, dibutuhkan manajemen risiko yang meliputi pengidentifikasian dan penilaian risiko yang dapat terjadi sehingga sebuah organisasi dapat menentukan tindakan mitigasi yang tepat dalam menghadapi ancaman tersebut. Kebijakan tentang keamanan informasi harus baik dan setidaknya harus mencakup beberapa prosedur seperti prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamanan logical security, prosedur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi. Untuk itu diperlukan evaluasi keamanan sistem manajemen informasi untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur.

Pada penelitian untuk usulan tugas akhir ini digunakan metode FMEA berdasarkan standar ISO 27001:2005 yang didalamnya mencakup identifikasi risiko, penilaian risiko, dan saran untuk

memitigasi risiko tersebut. Setelah proses tersebut, dapat diambil tindakan solusi dalam perancangan control objectives yang tepat sesuai dengan standar ISO 27001:2005 dan 27002:2013.

Tujuan dari penelitian ini adalah untuk memberikan gambaran terkait risiko – risiko yang berpotensi pada proses bisnis JSI-Net serta bagaimana saran tindakan untuk menangani risiko tersebut. Dengan begitu akan didapatkan hasil sebuah dokumen manajemen risiko beserta dokumen pengimplementasian manajemen risiko JSI-Net untuk kemudian dapat diimplementasikan di kehidupan nyata.

Kata kunci: analisis risiko, mitigasi, FMEA, ISO 27001:2005, ISO 27002:2013

IDENTIFICATION, ASSESSMENT AND RISK MITIGATION BASED ON ISO 27001 : 2005 & ISO 27002 WITH FMEA (STUDI KASUS : ISNet)

Student Name	**: KRISNA HARINDA D**
Student Number	**: 5211100148**
Department	**: Sistem Informasi FTIf – ITS**
Supervisor 1	**: Bekti Cahyo H, S.Si., M.Sc**
Supervisor 2	**:Hanim Maria Astuti, S.Kom, M.Sc**

ABSTRACT

An information system that is already well under its information security can not be guaranteed due to the threat of outsiders can occur if an organization does not pay attention to the risk inherent in the process. For that, it takes the risk management which includes the identification and assessment of risks that can occur so that an organization can determine appropriate mitigation actions in the face of such threats. Policy on information security must be good and should at least include several procedures such as asset management procedures, human resource management procedures, physical and environmental security procedures, security procedures logical security, operational security procedures and procedures for handling information technology in information security incident. It is necessary for the evaluation of information security management system to ensure information security is applied in accordance with the procedure.

In the research for this thesis used the proposed FMEA method based on the standard ISO 27001: 2005 also includes risk identification, risk assessment, and advice to mitigate such

risks. After the process, the solution can be taken in the design of appropriate control objectives according to the standard ISO 27001: 2005 and 27002: 2013.

The aim of this study is to provide an overview of risk associated - the potential risks to the business process JSI-Net as well as how the recommended action to address such risks. That way we will get the results of a risk management document and documents the implementation of risk management JSI-Net to then be implemented in real life.

Keywords: Risk Analysis, Mitigation, FMEA, ISO 27001:2005, ISO 2002:2013

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan pada Allah SWT yang telah memberikan rahmat dan ridhonya kepada penulis sehingga dapat menyelesaikan buku tugas akhir dengan judul

"IDENTIFIKASI, PENILAIAN, DAN MITIGASI RISIKO KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001 : 2005 DAN ISO 27002 : 2013 MENGGUNAKAN METODE FMEA (STUDI KASUS : ISNET)"

sebagai salah syarat untuk memperoleh gelar Sarjana Komputer di Jurusan Sistem Informasi – Institut Teknologi Sepuluh Nopember Surabaya.

Pada kesempatan ini, penulis ingin menyampaikan terima kasih kepada semua pihak yang telah memberikan doa, dukungan, bimbingan, arahan, bantuan, dan semangat dalam menyelesaikan tugas akhir ini, yaitu kepada:

1. Bapak Dr. Ir. Aris Tjahyanto, M.Kom, selaku Ketua Jurusan Sistem Informasi ITS
2. Bapak Bekti Cahyo Hidayanto, S.Si, M.Sc, selaku dosen pembimbing yang telah meluangkan waktu dan pikiran untuk mendukung dan membimbing dalam penyelesaian tugas akhir penulis.
3. Ibu Hanim Maria Astuti selaku dosen wali dan pembimbing yang telah memberikan pengarahan selama penulis menempuh masa perkuliahan dan penelitian tugas akhir.
4. Pak Hermono, selaku admin laboratoriun PPSI yang membantu penulis dalam hal administrasi penyelesaian tugas akhir dan mendukung penyelesaian tugas akhir ini.
5. Orang tua dan keluarga penulis yang telah mendoakan dan senantiasa mendukung serta selalu memberikan semangat dalam penyelesaian tugas akhir ini.
6. Kepada mas Nanok Adi Saputra, Pak Hermono, Mbak Maya, dan Mas Ricky selaku narasumber yang memberi

informasi kepada penulis untuk menyelesaikan tugas akhir ini.

7. Terima kasih kepada Retno Kuspinasih yang selalu mendukung dan memberikan semangat serta menemani penulis untuk menyelesaikan tugas akhir ini.
8. Sahabat-sahabat begadang penulis yaitu Hanggara, Biondi, Syafriandi, Mas Aan, Aro, dan lain-lain yang selalu mengganggu, mengingatkan dan nyemangati serta menemani sampai tugas akhir selesai.
9. Teman-teman seperjuangan BASILISK yang tidak dapat disebutkan namanya semua, terima kasih telah memberi semangat dan mendukung untuk segera menyelesaikan tugas akhir.
10. Pihak-pihak lain yang telah mendukung dan membantu dalam kelancaran penyelesaian tugas akhir.

Penyusunan laporan ini masih jauh dari sempurna, untuk itu penulis menerima adanya kritik dan saran yang membangun untuk perbaikan di masa mendatang. Semoga buku tugas akhir ini dapat memberikan manfaat bagi para pembaca dan menjadi sebuah kontribusi bagi ilmu pengetahuan.

Surabaya, Januari 2016

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang masalah, rumusan masalah, batasan masalah dan tujuan penelitian yang mendasari penelitian tugas akhir ini. Serta gambaran terhadap manfaat dari penelitian dan penjelasan sistematika penulisan laporan tugas akhir.

1.1 Latar Belakang Masalah

Dewasa ini, Teknologi informasi (TI) mengambil peranan penting bagi perusahaan. Fungsi TI tidak hanya sebagai fasilitas pendukung utama, tetapi juga dapat menjadi *critical success factor* dalam suatu industri. Penggunaan TI ditujukan untuk meningkatkan pelayanan kepada setiap karyawannya dan meningkatkan *performance* perusahaan. Bagian TI perusahaan telah memainkan peranan yang penting dalam menjalankan roda bisnis sehingga menjadi suatu prinsip dasar bahwa dalam pengelolaan teknologi informasi harus diimbangi dengan perhatian serius terhadap keamanan asetnya. Aset TI berupa data perusahaan maupun berupa perangkat keras TI membutuhkan pengamanan dari ancaman yang mungkin terjadi seperti pencurian, bencana alam, maupun gangguan lain. Keamanan informasi merupakan upaya untuk menjaga informasi dan sistem informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan dan menjamin kelangsungan bisnis, meminimalisasi risiko bisnis, dan meningkatkan peluang bisnis [1].

Informasi merupakan aset yang penting bagi setiap organisasi. Keamanan informasi merupakan upaya untuk menjaga informasi dan sistem informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan dan menjamin kelangsungan bisnis, meminimalisasi resiko bisnis, dan meningkatkan peluang bisnis. [2]

Namun demikian, tidak sedikit organisasi yang masih belum menyadari akan pentingnya keamanan informasi. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan atau gangguan lain terhadap informasi masih sering dialami oleh organisasi. ISNet merupakan pusat pengelolaan data dan informasi di Jurusan Sistem Informasi (JSI). ISNet ini mempunyai proses bisnis utama yaitu sebagai *server database* serta *gateway* akses wifi seluruh JSI. Sebagai server di Jurusan Sistem Informasi, di dalam ISNet terdapat server dari website JSI, CCTV, *database SITV*, database finger print, aplikasi keluhan, databse nilai dan absensi, serta data sharing mahasiswa dan dosen Sistem Informasi. Berdasarkan peranan penting yang ada tersebut, mengharuskan ISNet menjadi unit yang membutuhkan perlindungan keamanan. Akan tetapi, ada beberapa permasalahan yang dihadapi ISNet, yaitu seperti website JSI yang mudah dibobol, belum adanya aturan tertulis terkait siapa saja yang diperbolehkan memasuki ruang server, dan juga instalasi listrik yang kurang tertata dengan baik, serta akses WIFI yang kurang terkontrol. Sedangkan sejauh ini, belumada dokumentasi tertulis mengenai kebijakan penggunaan JSI-Net yang bertujuan untuk menjaga asset dari JSI-Net itu sendiri termasuk keamanan informasi. Hal ini dapat menjadi bukti bahwa ISNet masih belum memperhatikan akan pentingnya keamanan informasi.

Berdasarkan permasalahan di atas, dibutuhkan sebuah solusi yakni penilaian risiko. Penilaian risiko ini sebagai upaya untuk mengantisipasi seluruh potensi serta peluang risiko yang mungkin timbul. Oleh Karena itu, dibutuhkan identifikasi, penilaian, dan mitigasi risiko keamanan informasi di IS - Net. FMEA menjadi salah satu perangkat yang dimanfaatkan untuk menilai resiko keamanan informasi ISNet dengan standar ISO 27001 : 2005 dan ISO 27002:2013.

Dari hasil penilaian risiko tersebut dapat memberikan gambaran mengenai risiko terhadap asset yang dimiliki, kebutuhan dan

kesiapan asset yang dapat menghasilkan rancangan rekomendasi untuk perbaikan dan peningkatan kualitas pada ISNet.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah yang akan dibahas pada usulan tugas akhir ini adalah

1. Resiko apa saja yang terdapat pada jaringan IS – NET?
2. Bagaimana analisis resiko terhadap jaringan IS – NET menggunakan *framework* ISO 27001:2005 dan ISO 27002:2013?
3. Apa saja tindakan mitigasi terhadap risiko yang terjadi pada jaringan IS – NET ?

1.3 Batasan Masalah

Berikut adalah beberapa batasan masalah yang harus diperhatikan dalam pengerjaan tugas akhir ini:

1. Studi Kasus penelitian tugas akhir ini adalah IS – NET
2. *Framework* yang digunakan adalah ISO 27001 : 2005 dan ISO 27002 : 2013?
3. Metode yang digunakan adalah FMEA
4. Penelitian ini menganalisis aset informasi yang berhubungan dengan jaringan.
5. Penelitian menganalisis risiko dari segi asset informasi berdasarkan ISO 27001 : 2005

1.4 Tujuan Penelitian

Tujuan dari pengerjaan tugas akhir ini adalah untuk mengidentifikasi dan menganalisis risiko serta mitigasi keamanan informasi pada jaringan ISNET

1.5 Manfaat Penelitian

Manfaat yang diberikan dengan adanya tugas akhir ini adalah sebagai rekomendasi untuk perbaikan dan peningkatan kualitas pada ISNet sesuai dengan *framework* ISO 27001:2005.

1.6 Relevansi

Penelitian ini memiliki relevansi atau keterkaitan dengan mata kuliah pengelolaan risiko teknologi informasi yang tercakup pada laboratorium perencanaan dan pengembangan sistem informasi.

BAB II
TINJAUAN PUSTAKA

Bab tinjauan pustaka ini menjelaskan tentang referensi-referensi berkaitan dengan tugas akhir dan dasar teori yang akan digunakan.

2.1 Penelitian Terdahulu

Dalam penelitian ini, digunakan beberapa penelitian terdahulu sebagai pedoman dan referensi dalam melaksanakan prosesproses dalam pengerjaan penelitian yaitu pada Tabel 2.1. Informasi yang disampaikan dalam tabel berikut berisi informasi penelitian sebelumnya, hasil penelitian, dan hubungan penelitian terhadap tugas akhir.

Judul : ***A systemic methodology for risk management in healthcare sector***	
Nama peneliti	Anna Corinna Cagliano Sabrina Grimaldi, Carlo Rafele
Tahun penelitian	2010
Hasil penelitian	Penelitian ini berisi identifikasi resiko dan penerapan risk management dengan menggunakan metodologi FMEA untuk proses mitigasi risikonya yang diterapkan pada Instalasi rumah sakit besar Italia
Hubungan dengan penelitian	Sebagai bahan referensi utama dalam menentukan prioritasi risiko dengan menggunakan metodologi yaitu FMEA dalam penilaian risikonya.

2.2 Dasar Teori

Pada bagian ini, akan dijelaskan mengenai teori-teori yang digunakan untuk mendukung pengerjaan tugas akhir. Teori tersebut yaitu mengenai: aset, keamanan informasi, risiko, metode FMEA, ISO 27001 dan ISO 27002.

2.3 Aset

Aset adalah sumber daya ekonomi yang dikuasai dan/atau dimiliki oleh pemerintah sebagai akibat dari peristiwa masa lalu dan dari mana manfaat ekonomi dan social di masa 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[3].

2.4 Aset Informasi

Aset informasi merupakan bagian inti dari aset teknologi informasi. Aset informasi berisikan data dan informasi yang relevan dengan proses bisnis pada suatu organisasi. Aset Informasi pada penelitian ini meliputi komponen-komponen pendukung yang meliputi :

1. Orang (*people*)
   Dalam tugas akhir ini komponen yang akan diidentifikasi adalah pengguna aplikasi yang ada di proses bisnis organisasi tersebut

2. 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 dalam menjalankan proses operasional.

3. Perangkat Keras (*Hardware*)
   Mencakup piranti fisik, seperti computer, printer, dan monitor. Perangkat ini berperan sebagai media penyimpanan dalam system informasi. Setiap perusahaan yang memiliki teknologi informasi yang maju pasti memiliki perangksat keras dalam jumlah banyak.

4. Perangkat Lunak (*Software*)
   Merupakan sekumpulan instruksi yang dapat mempengaruhi kinerja perangkat keras dan memproses data. Tujuan perangkat ini adalah untuk mengolah, menghitung dan memanipulasi data agar menghasilkan informasi yang berguna

5. Jaringan (*Network*)
   Merupakan system penghubung yang memungkinkan suatu sumber yang digunakan bersamaan dalam waktu dan tempat yang berbeda

   Kemudian komponen tersebut saling menyatu dan berinteraksi sehingga dapat berfungsi sebagai pendukung dan penyedia kebutuhan informasi dalam rangka pengambilan keputusan yang lebih baik.

2.5 Risiko SI/TI

Menurut Kamus Besar Bahasa Indonesia, risiko adalah akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan. Dalam referensi lain, "*Risk is the Possibility of Suffering Harm of Loss*" atau dalam Bahasa Indonesia dapat diartikan kemungkinan untuk menderita kerugian atau kehilangan. [5].

Referensi lain juga menyebutkan bahwa risiko adalah kemungkinan (*likelihood*) sumber ancaman (*threat-source*) yang mengeksploitasi kerentanan (*vulnerability*) potensial, serta mengasilkan dampak (*impact*) berupa kejadian yang merugikan organisasi [6].

Risiko Teknologi Informasi merupakan bagian dari risiko operasrional jika dilihat dari sudut pandang industri finansia dan Ilmu Manajemen Risiko. Kesimpulan yang dapat ditarik dari sub bab sebelumnya bahwa kegagalan sistem Teknologi Informasi merupakan bagian dari risiko operasional. Pada dasarnya secara keseluruhan Teknologi Informasi merupakan risiko bagi bisnis, khususnya bagi bisnis yang terkait langsung dengan layanan Teknologi Informasi. Ketika pada sebuah layanan Teknologi Informasi terjadi gangguan ataupun permasalahan, maka secara keseluruhan hal itu akan mengganggu bisnis dan organisasi secara langsung maupun tidak langsung.

Menurut "*Risk IT Framework ISACA*" (2009), risiko teknologi informasi dapat dikategorikan sebagai berikut:

- Risiko nilai/keuntungan penggunaan Teknologi Informasi (*IT benefit/value enablement risk*).
- Risiko pelaksanaan program dan proyek (*IT programme and project delivery risk*).
- Risiko penghantaran operasional dan layanan Teknologi Informasi (*IT operations and service delivery risk*).

Oleh karena itu, kemampuan memahami dan mengidentifikasi risiko merupakan hal yang dibutuhkan bagi organisasi. Dengan kemampuan tersebut, maka organisasi dapat meminimalisir dampak yang dapat terjadi.

2.6 Manajemen Risiko SI/TI

Manajemen risiko merupakan serangkaian proses dalam mengidentifikasi risiko, melakukan penilaian risiko, dan menyusun serangkaian tindakan untuk menurunkan risiko tersebut sampai level yang dapat diterima oleh organisasi [7].

Pada pengimplementasiannya TI di organisasi, tentu akan banyak ditemukan ancaman yang dapat menimbulkan risiko dan mengganggu jalannya proses bisnis. Pada penelitian yang sudah dilakukan sebelumnya dalam melakukan manajemen risiko TI, dilakukan pengidentifikasian ancaman berdasarkan asset TI yang ada. Berikut adalah contoh dari ancaman TI yang bisa terjadi [8], [9], [10]:

Tabel 2. 1 Tabel Kategori Aset TI

No.	Kategori Aset TI	Ancaman
1.	Hardware	- Pelanggaran pemeliharaan system informasi - Hilangnya pasokan listrik - Debu, korosi, kerusakan fisik - Dicuri
2.	Software	- *User interface* sulit dipahami dan digunakan - Serangan virus
3.	Network	- Adanya gangguan pada *gateway* - Kesalahan konfigurasi - Ada kesalahan pada data center - Kerusakan fisik pada kabel dan komponen lain
4.	Data dan Informasi	- Kebocoran data - Data hilang / rusak

No.	Kategori Aset TI	Ancaman
		- Penyalahgunaan atau modifikasi data - Data *overload*
5.	*People*	- Kekurangan tenaga kerja - Kesalahan operasional (*human error)* - Pemalsuan hak - Penyalahgunaan wewenang

Dengan adanya daftar ancaman tersebut, diperlukan tindakan preventif untuk bagaimana menindaklanjuti risiko-risiko tersebut sehingga dibutuhkan tindakan manajemen risiko. Berdasarkan fase PLAN pada ISO 27001, didalamnya mencakup proses manajemen risiko diantaranya sebagai berikut:

1. Menetapkan pendekatan asesmen risiko pada organisasi
   - Mengidentifikasi suatu metodologi asesmen risiko yang sesuai dengan SMKI, dan keamanan informasi bisnis yang teridentifikasi, dan persyaratan dan perundang – undangan
   - Mengembangkan kriteria untuk menerima risiko dan mengidentifikasi tingkat risiko yang dapat diterima
2. Mengidentifikasi risiko
   - Mengidentifikasi aset dalam ruang lingkup SMKI dan pemilik aset
   - Mengidentifikasi ancaman – ancaman terhadap aset
   - Mengidentifikasi kelemahan yang mungkin dieksploitasi oleh ancaman
   - Mengidentifikasi dampak hilangnya kerahasiaan, integritas, dan ketersediaan dari aset
3. Menganalisis dan mengevaluasi risiko
   - Mengases dampak bisnis bagi organisasi yang mungkin berasal dari kegagalan keamanan, yang

mempertimbangkan konsekuensi hilangnya kerahasiaan, integritas, atau ketersediaan aset
- Mengases kemungkinan terjadinya kegagalan keamanan yang berkenaan dengan ancaman dan kelemahan, dan dampak yang terkait dengan aset serta pengendalian yang diterapkan saat ini
- Memperkirakan tingkat risiko
- Menetapkan apakah risiko dapat diterima atau memerlukan perlakuan dengan menggunakan kriteria untuk risiko yang dapat diterima sebagaimana ditetapkan pada nomor 1.

Pada alur proses pelaksanaan Manajemen Resiko, ketika memasuki tahapan penanganan terdapat 4 pilihan penanganan terhadap risiko potensial tersebut, yaitu [11]:

1. *Take* : Jika risiko yang ada dirasakan cukup besar dan tidak dapat dihindari, sehingga perusahaan dapat mengalami dampak yang mengganggu dan bersifat merusak secara alamiah, maka diambil tindakan "*Take*" atau menerima risiko tersebut. Seperti bencana alam, gempa bumi, banjir, badai, dan sebagainya. Karena perusahaan tentunya tidak dapat melawan alam.

2. *Treat* : Jika risiko yang ada dirasakan dapat ditanggapi dengan tindakan untuk menurunkan tingkat risikonya, maka diambil tindakan "*Treat*" untuk mnegontrol risiko tersebut. Tindakan nyatanya adalah dengan menerapkan kontrol atau mitigasi terhadap risiko yang ada sehingga risiko tersebut dapat diturunkan levelnya.

3. *Terminate* : Jika risiko yang ada dirasakan terlalu besar (misalnya dalam rangka membuat suatu produk IT baru), maka dapat diambil tindakan "*Terminate*" terhadap risiko tersebut, artinya kita harus menghindar dan tidak mau mengambil risiko dengan membuat produk IT baru tersebut, sehingga tindakan nyatanya adalah membatalkan rencana pembuatan produk IT tersebut.

4. *Transfer* : Jika risiko yang *ada* dianggap akan lebih baik jika dialihkan ke pihak lain yang sesuai dengan bidang ahlinya, misalnya ke pihak asuransi, maka dapat diambil tindakan "*Transfe*r" terhadap risiko tersebut.

2.7 Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) adalah cara untuk melindungi dan mengelola informasi berdasarkan pendekatan risiko bisnis yang sistematis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara dan meningkatkan keamanan informasi [12].

Sistem manajemen keamanan informasi (SMKI) rata-rata digunakan para manajer untuk mengukur, memonitor dan mengendalikan keamanan informasi mereka. SMKI ini memberikan perlindungan informasi dan penghitungan asset yang ada pada perusahaan. SMKI mengadopsi konsep siklus PDCA (*Plan-Do-Check-Act*) sehingga perusahaan dapat menyeseuaikan tingkat kebutuhan pengamanan informasi yang efektif dan efisien sesusai dengan level/jenis perusahaan.

SMKI bertujuan untuk meninimalisir tingkat risiko yang ditimbulkan akibat pertukaran, pemrosesan, penyimpanan, lalu-lintas dan disposal data dan informasi [13].

Dalam penerapan siklus PDCA (*Plan-Do-Check-Act*) dalam manajemen keamanan informasi akan memberikan cara bagaimana suatu metode manajemen keamanan informasi akan ditingkatkan sehingga dapat menyesuaikan dengan setiap perubahan baik internal maupaun eksternal perusahaan. Struktur dokumentasi manajemen keamanan informasi pada umumnya terdiri dari 3 (tiga) tingkat, yaitu :

a. Tingkat 1

Dokumen tingkat 1 merupakan dokumen dengan hirarki tertinggi dalam struktur dokumentasi SMKI. Dokumen ini bersifat strategis yang memuat komitmen yang dituangkan dalam bentuk kebijakan, standar, sasaran dan rencana terkait pengembangan (*development*), penerapan (*implementation*) dan peningkatan (*improvement*) manajemen keamanan informasi. Dokumen Tingkat 1 minimum terdiri dari:

- Kebijakan Keamanan Informasi
- Peran dan tanggung jawab organisasi keamanan informasi
- Klasifikasi informasi
- Kebijakan Pengamanan Akses Fisik dan Lojik Kebijakan Manajemen Risiko TIK
- Manajemen Kelangsungan Usaha (*Business Continuity Management*)
- Ketentuan Penggunaan Sumber Daya TIK

b. Tingkat 2

Dokumen tingkat 2 ini umumnya meliputi prosedur dan panduan yang dikembangkan secara internal oleh instansi/lembaga penyelenggara pelayanan publik dan memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan. Dokumen ini bersifat operasional. Prosedur-prosedur dalam dokumen tingkat 2 meliputi antara lain:

- Prosedur pengendalian dokumen
- Prosedur pengendalian rekaman
- Prosedur audit internal SMKI
- Prosedur tindakan perbaikan dan pencegahan
- Prosedur penanganan informasi (penyimpanan, pelabelan, pengiriman/ pertukaran, pemusnahan)
- Prosedur penanganan insiden/ gangguan keamanan informasi

- Prosedur pemantauan penggunaan fasilitas teknologi informasi

c. Tingkat 3

Dokumen tingkat 3 meliputi petunjuk teknis, instruksi kerja dan formulir yang digunakan untuk mendukung pelaksanaan prosedur tertentu sampai ke tingkatan teknis. Instruksi kerja tidak selalu diperlukan untuk setiap prosedur. Sepanjang prosedur sudah menguraikan langkah-langkah aktivitas yang jelas dan mudah dipahami penanggung jawab kegiatan, petunjuk teknis/ instruksi kerja tidak diperlukan lagi [14].

Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

- ISO/IEC 27000:2009 – *ISMS Overview and Vocabulary*
- ISO/IEC 27001:2005 – *ISMS Requirements*
- ISO/IEC 27002:2005– *Code of Practice for ISMS*
- ISO/IEC 27003:2010 – *ISMS Implementation Guidance*
- ISO/IEC 27004:2009 – *ISMS Measurements*
- ISO/IEC 27005:2008 – *Information Security Risk Management*
- ISO/IEC 27006: 2007 – *ISMS Certification Body Requirements*
- ISO/IEC 27007 – *Guidelines for ISMS Auditing*

Namun dari semua seri ISO 27000 tersebut yang akan dijelaskan lebih lanjut adalah ISO/IEC 27001:2005 dan ISO/IEC 27002 [14].

2.8 ISO 27001:2005

ISO IEC merupakan standar internasional keamanan informasi yang dipakai di semua organisasi misalnya usaha komersial, pemerintah, organisasi nirlaba. Standar ini menetapkan persyaratan untuk penetapan, penerapan, pengoperasian,

pemantauan, pengkajian, peningkatan, dan pemeliharan Sistem Manajemen Keamanan Informasi (SMKI) yang terdokumentasi dalam konteks risiko bisnis organisasi secara keseluruhan [15].

Standar ISO/IEC 27001 diresmikan secara resmi pada Oktober 2005 [12]. ISO 27001 meliputi seluruh aspek proses bisnis bukan hanya yang berkaitan dengan teknologi informasi termasuk juga yang berkaitan dengan pihak ketiga atau *outsourcing*. Secara definisi, ISO 27001 dirancang supaya mampu diimplemetasikan pada perusahaan dalam [16].

Pada standar ISO/IEC 27001 mengatur beberapa penerapan ISMS (*Information Security Management System)* dalam organisasi yaitu [17]:

1. Seluruh kegiatan harus sesuai dengan tujuan dan proses pengamanan informasi yang didefinisikan dengan jelas dan didokumentasikan dalam suatu kebijakan dan prosedur.
2. Standar ini memberikan control pengamanan yang dapat digunakan oleh organisasi untuk diimplementasikan berdasarkan kebutuhan spesifik bisnis dan organisasi.
3. Semua pengukuran pengamanan yang digunkana dalam ISMS harus diimplementasikan sebagai hasil dari analisis resiko untuk mengeliminasi atau mengurangi level resiko hinga level yang dapat diterima.
4. Suatu proses harus dapat memastikan *continuous improvement* atau perbaikan yang berkelanjutan dari semua elemen informasi dan sistem manajemen pengamanan sebagai basisi dalam pelaksanaan ISMS.

Standar ini mengadopsi model "*Plan-Do-Check-Act*" (PDCA), yang diterapkan untuk penerapan ISMS. Adopsi dari model PDCA dapat mencerminkan prinsip-prinsip dalam Panduan OECD (2002) yang mengatur keamanan sistem informasi dan jaringan. Standar ini memberikan model yang kokoh untuk menerapkan prinsip-prinsip yang ada dalam panduan tersebut yang mengatur asesmen risiko, desain keamanan dan penerapan, manajemen keamanan dan reasesmen [18].

Tabel 2. 2 Tabel PDCA

Plan (establish the ISMS)	Membangun kebijakan, objektif, proses, dan prosedur ISMS yang berhubungan dengan pengelolaan risiko dan peningkatan keamanan informasi untuk memberikan hasil – hasil yang sesuai dengan kebijakan dan objektif yang menyeluruh dari suatu organisasi
Do (implement and operate the ISMS	Menerapkan dan mengoperasikan kebijakan, kontrol, proses, dan prosedur ISMS
Check (monitor and review the ISMS)	Menilai dan jika dapat dilakukan, mengukur performa proses terhadap kebijakan, objektif, dan pengalaman praktis ISMS dan melaporkan hasilnya ke manajemen sebagai tinjauan
Act (maintain and improve the ISMS)	Mengambil tindakan perbaikan dan pencegahan, berdasarkan hasil audit ISMS internal dan tinjauan manajemen atau informasi lain yang relevan, untuk mencapai peningkatan yang berkesinambungan dari ISMS

Standar ini berlandaskan sistem manajemen berbasis risiko dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko.

2.9 ISO 27002 : 2013

Standar ini merupakan penamaan ulang dari ISO/IEC 17799:2005. Standar ini dapat digunakan sebagai titik awal dalam penyusunan dan pengembangan ISMS. Standar ini memberikan panduan dalam perencanaan dan implementasi suatu program untuk melindungi aset – aset informasi [19].

Standar ini mengatur beberapa penerapan ISMS sebagai berikut [19]:

- Semua kegiatan harus sesuai dengan tujuan dan proses pengamanan informasi yang didefinisikan dengan jelas dan didokumentasikan dalam suatu kebijakan dan prosedur
- Standar ini memberikan kontrol pengamanan, yang dapat digunakan oleh organisasi untuk diimplementasikan berdasarkan kebutuhan spesifik bisnis organisasi
- Semua pengukuran pengamanan yang digunakan dalam ISMS harus diimplementasikan sebagai hasil dari analisis risiko untuk mengeliminasi atau untuk mengurangi level risiko hingga level yang dapat diterima
- Suatu proses harus dapat memastikan adanya verifikasi secara berkelanjutan terhadap semua elemen sistem pengamanan melalui audit dan review
- Suatu proses harus dapat memastikan *continuous improvement* dari semua element informasi dan sistem manajemen pengamanan.

Tujuan ISO/IEC 27002 adalah untuk memberikan rekomendasi manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab dalam: inisiasi, implementasi, atau pengelolaan keamanan informasi pada organisasinya. ISO/IEC 27002 terdiri atas 127 kendali dalam 11 kategori keamanan informasi [19]:

- ***Security Policy***
- ***Organization of Information Security***
- ***Asset Management***
- ***Human Resource Security***
- ***Physical and Environmental Security***
- ***Communications and Operations Management***
- ***Access Control***
- ***Information System Acquisition Development and Maintenance***
- ***Information Security Incident management***
- ***Business Continuity Management***

- ***Compliance***

Dalam penerapannya, berikut beberapa contoh untuk beberapa kebijakan dan pengendalian keamanan informasi yang berkaitan dengan 3 dari 11 kendali berdasarkan ISO/IEC 27002

Physical and Environmental Security

1. Akses fisik ke lokasi dan infrastruktur pendukung harus diawasi dan dibatasi untuk mencegah, mendeteksi, dan meminimalkan efek dari akses yang tidak sah, kerusakan, vandalisme, tindak kriminal, pencurian dll
2. Daftar orang yang berwenang untuk mengakses daerah aman harus ditinjau dan disetujui secara berkala (minimal sekali setahun) oleh departemen keamanan fisik dan periksa kembali oleh manajer departemen masing-masing.
3. Fotografi atau merekam video dilarang di dalam area terlarang tanpa izin terlebih dahulu dari otoritas yang ditunjuk.
4. Kamera video pengintai yang digunakan harus berada di semua pintu masuk dan keluar ke lokasi dan titik-titik strategis lainnya seperti area terbatas. Rekaman tersebut dicatat dan disimpan untuk setidaknya satu bulan dan dipantau secara berkala tiap jamnya oleh personel yang terlatih.
5. Tanggal dan waktu masuk kedatangan pengunjung beserta dengan tujuan kunjungan harus dicatat dan dikendalikan oleh keamanan situs atau bagian penerimaan.

Human Resource Security

1. Semua karyawan harus diseleksi sebelum kerja, termasuk verifikasi identitas menggunakan paspor atau ID foto dan setidaknya memiliki dua referensi dari professional bahwa kredibilitasnya memuaskan. Pemeriksaan tambahan diperlukan bagi karyawan mengambil posisi lebih tinggi
2. Semua karyawan harus secara resmi menerima kerahasiaan atau *non-disclosure* perjanjian yang mengikat mengenai

informasi pribadi dan eksklusif yang diberikan kepada atau dihasilkan oleh mereka selama bekerja

3. Departemen sumber daya manusia harus menginformasikan kepada bagian administrasi, keuangan dan operasi ketika seorang karyawan didaftarkan, ditransfer, ditangguhkan atau dihentikan.
4. setelah menerima pemberitahuan dari HR status karyawan terkait perubahan pada karyawan, administrasi harus memperbarui hak akses fisik dan TI administrasi keamanan harus memperbarui hak akses mereka sesuai dengan ketentuan.
5. Manajer HRD harus memastikan bahwa semua kartu akses, kunci, peralatan IT, media penyimpanan dan aset perusahaan yang berharga lainnya dikembalikan oleh karyawan pada atau sebelum hari terakhir kerja mereka.

Access Control

1. Pengguna dari perusahaan sistem TI, jaringan, aplikasi dan informasi harus diidentifikasi secara individu dan dikonfirmasi.
2. Akses pengguna ke perusahaan sistem TI, jaringan, aplikasi dan informasi harus dikontrol sesuai dengan kebutuhan akses yang ditentukan oleh pemilik aset informasi yang relevan, biasanya menurut peran pengguna dalam perusahaan tersebut.
3. ID generik atau tes tidak boleh dibuat atau diaktifkan pada sistem produksi kecuali secara khusus diizinkan oleh pemilik aset informasi yang relevan
4. *Password* harus panjang dan rumit, terdiri dari kombinasi huruf, angka dan karakter khusus sehingga sulit untuk ditebak.
5. *Password* tidak harus ditulis atau disimpan dalam format yang dapat dibaca.
6. Pengguna harus log off atau mengunci sesi mereka sebelum meninggalkan tanpa pengawasan.

7. *Screen saver* yang dilindungi dengan *password* dengan batas waktu tidak aktif tidak lebih dari 10 menit harus diaktifkan pada semua PC
8. Akses removable media harus dinonaktifkan pada semua desktop kecuali ada alasan bisnis tertentu dan disetujui oleh pihak berwenang.

2.10 *Failure Model Effect Analysis (FMEA)*

FMEA adalah teknologi yang dirancang untuk mengidentifikasi mode kegagalan potensial pada suatu proses sebelum terjadi, dengan mempertimbangkan risiko yang berkaitan dengan mode kegagalan tersebut serta efeknya [20]. Menurut Chrysler (1995), FMEA dapat dilakukan dengan cara:

1. Mengenali dan mengevaluasi kegagalan potensi suatu produk dan efeknya
2. Mengidentifikasi tindakan yang bisa menghilangkan atau mengurangi kesempatan dari kegagalan potensi terjadi
3. Pencatatan proses sehingga dokumen perlu di *update* secara teratur agar dapat digunakan untuk mencegah dan mengantisipasi terjadinya kegagalan

Dalam memberikan penilaian, digolongkan menjadi tiga bagian yaitu *severity* (tingkat keparahan), *occurance* (kemungkinan terjadi kesalahan), dan *detection* (deteksi tiap kesalahan) yang nantinya ketiga penilaian tersebut digunakan untuk menghitung RPN (tingkat prioritas risiko) [21].

Severity

Severity atau keseriusan efek kegagalan merupakan pengukuran dalam memperkirakan subjektif numeric dari seberapa parah efek kegagalan yang akan dirasakan oleh pengguna akhir. Berikut ini adalah ukuran parameter dari *severity* [22]

Tabel 2. 3 Tabel Penilaian Severity

Peringkat	Efek	Efek dari severity
10	Berbahaya; tanpa peringatan	Menyebabkan proses bisnis terhenti untuk waktu lama > 1 minggu
9	Berbahaya; dengan peringatan	Menyebabkan proses bisnis terhenti untuk waktu cukup lama > 1 hari
8	Sangat Tinggi *(very high)*	Menyebabkan proses bisnis terhenti sebentar < 1 hari
7	Tinggi *(high)*	Menghambat berjalannya proses bisnis
6	Sedang *(moderate)*	Menyebabkan tidak berfungsinya layanan seperti semestinya
5	Rendah *(low)*	Menimbulkan komplain
4	Sangat Rendah *(very low)*	Menyebabkan gangguan yang cukup berpengaruh
3	Sedikit *(minor)*	Menyebabkan sedikit gangguan
2	Sangat sedikit *(very minor)*	Tidak diperhatikan, berpengaruh minor terhadap kinerja

Peringkat	Efek	Efek dari severity
1	Tidak ada *(none)*	Tidak diperhatikan maupun mempengaruhi kinerja

Occurance

Occurance atau frekuensi kegagalan merupakan pengukuran dalam memperkirakan subjektif numerik dari probabilitas penyebab kemungkinan terjadinya kegagalan akan menghasilkan mode kegagalan yang menyebabkan akibat tertentu. Berikut ini adalah ukuran parameter dari *occurance* [22].

Tabel 2. 4 Tabel Penilaian Occurance

Peringkat	Efek	Kemungkinan terjadi
10	*Sangat tinggi* – kegagalan hampir tak terelakan	> 1 kali / hari
9		1 kali / hari
8	*Tinggi* – Kegagalan Sering terjadi	1 kali / 3-4 hari
7	*Sedang* – Cukup sering terjadi	1 kali / minggu
6		1 kali / 2 minggu
5		1 kali / bulan

Peringkat	Efek	Kemungkinan terjadi
4	*Rendah* – cukup jarang terjadi	1 kali / 3 bulan
3		1 kali / 6 bulan
2	*Sangat Rendah* – Jarang terjadi	1 kali / tahun
1	*Hampir tidak mungkin* :Hampir tidak mungkin terjadi	1 kali / beberapa tahun

Detection

Detection atau sejauh mana peluang potensi kegagalan tersebut dapat teridentifikasi merupakan pengukuran dalam memperkirakan subjektif numerik dari kontrol untuk mencegah atau mendeteksi penyebab kegagalan sebelum kegagalan mencapai pengguna akhir atau pelanggan. Berikut ini adalah ukuran parameter dari *detection* [22]

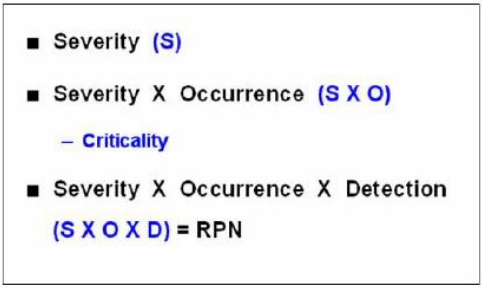
Tabel 2. 5 Tabel Penilaian Detection

Peringkat	Efek	Deteksi
10	*Hampir tidak mungkin*	Potensi penyebab tidak terdeteksi atau tidak dapat dikontrol

Peringkat	Efek	Deteksi
9	*Sangat sulit*	Sangat sulit untuk mendeteksi risiko , sangat sulit dikendalikan
8	*Sulit*	Sulit dideteksi, sulit dikendalikan
7	*Cukup sulit*	Cukup sulit dideteksi, cukup sulit dikendalikan
6	*Normal*	Dapat dideteksi dengan usaha ekstra, dapat dikendalikan dengan usaha extra
5	*Sedang*	Dapat dideteksi, dapat dikendalikan
4	*Cukup mudah*	Cukup mudah dideteksi, cukup mudah dikendalikan

Peringkat	Efek	Deteksi
3	*Mudah*	Mudah dideteksi, mudah dikendalikan
2	*Sangat mudah*	Sangat mudah dideteksi, sangat mudah dikendalikan
1	*Hampir pasti*	Terlihat jelas, sangat mudah pengendaliannya

Selanjutnya ketiga komponen pengukuran kegagalan tersebut dibobotkan, sehingga didapatkan Risk Priority Number (RPN). RPN adalah hasil ukuran yang digunakan ketika menilai risiko untuk membantu mengidentifikasi *critical failure modes* atau mode kegagalan kritis terkait dengan suatu sistem mencakupi desain atau proses. Nilai RPN berkisar dari 1(terbaik mutlak) hingga 1000 (absolut terburuk). Dibawah ini adalah penggambaran untuk proses factor – factor yang membentuk RPN dan bagaimana hal tersebut dihitung untuk setiap *failure modes*.



Gambar 2. 1 Rumus Penilaian RPN

Setelah itu, hasil dari penilaian RPN tersebut diurutkan sesuai level. Dibawah ini merupakan tabel level RPN menurut FMEA.

CLASS OF RPN CATAGORISM	
RPN Calculation	Level
< 20	Very Low
< 80	Low
< 120	Medium
< 200	High
>200	Very High

Gambar 2. 2 Klasifikasi level risiko berdasarkan RPN

2.11 Risk Management Berdasarkan PMBoK

Pada literatur lain, terdapat cara bagaimana penulis mengkategorikan risiko berdasarkan dampaknya atau dengan kata lain menilai risiko. Pada PMBoK, berikut adalah skema untuk proses manajemen risikonya:

Tabel 2. 6 Skema Proses Manajemen Risiko

No.	Process	Output
1.	Risk Management Planning	• Risk Management Plan
2	Risk Identification	• Risks • Triggers • Inputs to other processes
3.	Qualitative Risk Analysis	• Overall risk rangking • List of prioritized risk • List of risk • Trends in qualitative risk analysis results
4.	Quantitative Risk Analysis	• Prioritized list of quantified risks • Probabilistic analysis of the project • Trends in quantitave risk analysis results
5.	Risk Response Planning	• Risk response plan • Residual risk • Secondary risk • Contractual agreements • Input to a revised project plan
6.	Risk Monitoring and Control	• Workaround plan • Corrective action • Project change request • Update to the risk response plan • Risk database • Update to risk identification checklist

Manajemen risiko di dalam proyek adalah tentang menyeimbangkan dampak dari risiko dan tingkat ketidakpastian dari risiko organisasi tersebut. Manajemen risiko membutuhkan penentuan tingkat risiko yang sudah divalidasi dai diberikan kepada perusahaan atau organisasi

Berikut adalah salah satu contoh dalam pengembangan nilai probabilitas dampak dari suatu risiko ke dalam *grid* atau table.

Probability					
VH (0.9)	4.5%	9%	18%	36%	72%
H (0.7)	3.5%	7%	14%	28%	56%
M (0.5)	2.5%	5%	10%	20%	40%
L (0.3)	1.5%	3%	6%	12%	24%
VL (0.1)	0.5%	1%	2%	4%	8%
	VL (0.05)	L (0.1)	M (0.2)	H (0.4)	VH (0.8)
	Impact				

Gambar 2. 3 Contoh pengembangan nilai probabilitas

Masing-masing risiko memiliki tingkat kemungkinan terjadi dan dampak terhadap proyek. Gambar diatas jika diimplementasikan maka akan menghasilkan nilai untuk masing-masing risiko ke dalam persentase seperti berikut:

Probability x Impact x 100 = Risk Percentage

Gambar 2. 4 Rumus Prosentase Risk Percentage

Dengan begitu dapat ditentukan berapa tingkat risiko untuk masing-masing risiko yang sudah diidentifikasi berdasarkan kemungkinan terjadi dan dampaknya.

2.12 Keamanan Informasi

Menurut Sarno dan Iffano, keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara

tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, mengoptimalkan pengembalian investasi *(return on investment)*. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-*sharing*-kan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan [23].

Menurut ISO/IEC 17799:2005 tentang *information security management system* bahwa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis. Keamanan Informasi memiliki 3 aspek, yaitu [11]:

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. A***vailability*** meyakinkan bahwa pengguna mempunyai kesempatan dan akses pada suatu informasi.

Tiga elemen dasar ***confidentiality, integrity,*** dan ***availability*** (CIA) merupakan dasar diantara program program keamanan yang dikembangkan. Ketiga elemen tersebut merupakan mata rantai yang saling berhubungan dalam konsep ***information protection.***

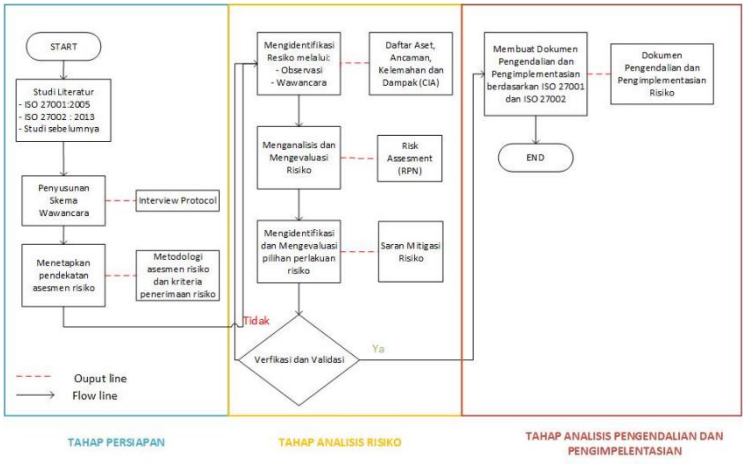
Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan

BAB III
METODOLOGI

Bab ini menjelaskan alur metode penelitian yang akan dilakukan oleh penulis dalam pembuatan tugas akhir. Metode penelitian juga digunakan sebagai panduan dalam pengerjaan tugas akhir agar terarah dan sistematis. Adapun urutan dari pengerjaan tugas akhir dapat dilihat pada gambar dibawah ini:

3.1 Flowchart Metodologi

Tahapan penelitian akan digambarkan dalam bentuk alur proses secara runtut atau *flowchart*. *Flowchart* menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses (instruksi) dengan proses lainnya. Berikut ini *flowchart* pada penelitian tugas akhir ini.



Gambar 3. 1 Flowchart Metodologi

3.2 Aktivitas Metodologi

Berdasarkan alur proses secara runtut atau *flowchart* diatas, maka dapat dijabarkan tiap proses/aktivitasnya pada table berikut.

Tabel 3. 1 Aktivitas Metodologi Penelitian

Tahap	Aktivitas	Tujuan	Metode/Teknik/Tools	Input	Output
1	Studi Literatur	Untuk mendapatkan landasan teori dan perhitungan dari Studi sebelumnya	Membaca	Sumber informasi : jurnal/ penelitian sebelumnya	Acuan yang akan digunakan.
2	Penyusunan Skema wawancara	Untuk mendapatkan Interview Protocol	Membaca	Sumber Informasi : Literatur Mengenai Interview Protocool dan Hal yang diteliti	Interview Protocool
3	Menetapkan Pendekatan	Untuk Menentukan Metodologi	Membaca	Sumber Informasi :	Metodologi Assesmen

Tahap	Aktivitas	Tujuan	Metode/Teknik/Tools	Input	Output
	Assessment Resiko	Assesmen Resiko dan kriteria resiko yang sesuai		ISO 27001 : 2005	Resiko yang Sesuai dengan yang dibutuhkan
4	Mengidentifikasi Resiko	Mengidentifikasi Resiko – Resiko yang mungkin muncul	Observasi Wawancara	*Interview Protocool*	Daftar Aset, Ancaman, Kelemahan dan Dampak
5	Menganalisis dan Mengevaluasi Resiko	Untuk menentukan Tingkat resiko	Penilaian Menggunakan Metode FMEA	Daftar Resiko	Daftar Resiko yang sudah terurutkan prioritasnya
6	Mengidentifikasi dan mengevaluasi pilihan migitasi resiko	Untuk menentukan perlakuan / mitigasi risiko	Menggunakan acuan Standar ISO 27001	Daftar Resiko yang sudah terurutkan prioritasnya	Tindakan secara tertulis (Mitigasi Resiko)
7	Membuat Dokumen Pengendalian	Untuk Mendokumentasikan Pengendalian Risiko	Menggunakan acuan Standar ISO 27002	Daftar Resiko yang sudah terurutkan prioritasnya	Dokumen Pengendalian Berdasarkan ISO 27002

BAB IV
PERANCANGAN

Bagian ini menjelaskan perancangan penelitian tugas akhir sebagai panduan dalam melakukan penelitian tugas akhir.

4.1 Pengumpulan Data

Pada bagian ini akan dijelaskan mengenai persiapan pengumpulan data pada penelitian tugas akhir ini. Terdapat beberapa metode yang digunakan untuk pengumpulan data, diantaranya pengamatan langsung wawancara, catatan arsip, dan observasi. Dalam penelitian tugas akhir ini, metode pengumpulan data yang digunakan adalah wawancara dan observasi.

4.1.1 Wawancara

Pengumpulan data dengan teknik *in-depth interview* atau wawancara, yang akan dilaksanakan terhadap teknisi IS-Net yang memiliki wewenang dan tanggung jawab pada asset informasi yang ada di IS-Net. Beberapa poin penting yang akan diajukan kepada interviewer yaitu :

- Mengetahui Kondisi Kekinian IS Net
- Penggalian Informasi risiko apa saja yang pernah atau sering terjadi dalam IS – Net

Poin-poin tersebut kemudian disusun menjadi sebuah pertanyaan yang disusun dalam interview protocol. Interview protocol dilampirkan pada **Lampiran A.** Dalam proses wawancara akan digunakan *recorder* untuk merekam semua jawaban dari interviewer.

4.1.2 Observasi

Observasi merupakan pengamatan dan juga pencatatan sistematik atas unsur-unsur yang mucul. Observasi dilakukan untuk memahami aktivitas-aktivitas yang berlangsung, menjelaskan siapa saja orang-orang yang terlibat di dalam suatu aktivitas.

4.2 Metode Pengolahan Data

Pengolahan hasil wawancara akan dilakukan dengan menulis ulang rekaman wawancara yang tersimpan pada *recorder* dengan rekaman wawancara dengan menggunakan *tools Microsoft word.* Sedangkan pengolahan data akan diolah berdasarkan proses yang ada pada manajemen resiko pada acuan standar ISO 27001. Dengan pengolahan data hasil wawancara dan observasi tersebut, didapatkan risiko-risiko yang kritis pada IS-Net.

4.3 Pendekatan Analisis

Dalam penelitian studi kasus, data digunakan mencari hubungan antara objek dan jawaban dari pertanyaan pertanyaan penelitian yang diajukan. Untuk itu data yang sudah diolah akan dilakukan analisis. Analisis yang dilakukan adalah dengan melakukan proses penilaian resiko berdasarkan metode FMEA

BAB V
IMPLEMENTASI

Bab ini menjelaskan tentang implementasi setiap tahap & proses – proses didalam metodologi tugas akhir ini, yang dapat berupa hasil, waktu pelaksanaan dan lampiran terkait yang memuat pencatatan tertentu dengan implementasi proses itu sendiri.

12.1 Identity Staff Knowledge

Untuk menggali informasi dari bagian staf, maka peneliti menggunakan *interview protocol* dengan staff langsung dari ISNet. Dan hasil dari interview protocol dapat dilihat pada Lampiran A. Poin penting dari hasil identifikasi pengetahuan staf di ISNet mencakup hal-hal berikut :

a. Aset-Aset penting menurut Staff ISNet adalah
    1. Server
    2. Jaringan
    3. SDM
    4. Hardware (Router, Switch, dll)
b. ISNet memiliki proses bisnis lebih ke arah jaringan, yang mana saat ada kendala baru diatasi, seperti halnya internet mati, kerusakan hardware, dan lain-lain.
c. Selama staff ISNet yang sekarang bekerja, belum ada training khusus untuk proses bisnis yg terkait.
d. Proses backup dulu dilakukan 6 bulan sekali untuk e-learning JSI, dan saat ini e-learning JSI digantikan oleh Share ITS. Jadi sudah tidak pernah melakukan backup.
e. Server tidak memiliki proteksi khusus, dan antisipasi virus dan malware dengan menggunakan linux sebagai system operasinya.
f. Setiap user memiliki ID untuk menggunakan fasilitas internet dan mengakses ke file share JSI yang tersedia.

g. ISNet memiliki SIM Keluhan untuk menjembatani komunikasi antara user dengan stakeholder terkait kendala apa saja yang dihadapi oleh user. Namun jarang sekali digunakan.
h. Untuk pengamanan ruang server hanya mengatur siapa saja yang bisa masuk kedalam ruang server dan mengunci ruangan tersebut jika tidak ada orang didalam.
i. Belum ada prosedur kebijakan untuk mengatasi masalah yang terjadi. Jika ada permasalahan, ISNet menangani langsung dengan tindakan yang sesuai.

12.2 Daftar Kriteria Risk Acceptance

Berikut merupakan kriteria penerimaan risiko yang dapat diajadikan acuan dalam menganalisis resiko pada jaringan ISNet.

Tabel 5. 1 Daftar Kriteria Risk Acceptance

Kriteria	Keterangan
Tidak Mengganggu	Dampak yang terjadi tidak mempengaruhi jalannya proses bisnis
Membahayakan	Dampak yang terjadi mempunyai kemungkinan untuk mempengaruhi jalannya proses bisnis
Mengganggu	Dampak yang terjadi mempengaruhi jalannya proses bisnis
Terhenti	Dampak yang terjadi membuat proses bisnis tidak dapat berjalan.

12.4 Daftar Aset

Untuk menentukan aset yang berharga dan penting, perlu dibuat daftar aset yang ada terlebih dahulu untuk mengetahui aset apa saja yang dimiliki serta kebutuhan keamanan ancaman dan kekuatan serta kelemahan di organisasi tersebut. Berikut daftar aset terkait jaringan ISNet :

Tabel 5. 2 Daftar Asset

Daftar Aset			
Kategori	**Aset**	**Fungsi Aset**	**Konektifitas Proses Bisnis**
Hardware	**Server**	➢ Menyediakan fitur keamanan computer. ➢ Melindungi semua computer yg terhubung menggunakan firewall ➢ Menyediakan IP Address untuk mesin computer yang terhubung	Akademik
	Access Point	Access Point digunakan sebagai jalur akses nirkabel	Akademik
	Switch	Switch digunakan sebagai pengatur dan pembagi sinyal data dari suatu komputer ke komputer lainnya.	Akademik
	UPS	UPS digunakan untuk situasi tertentu, dimana sumber tegangan utama nya hilang, UPS dapat	Akademik

Daftar Aset			
Kategori	**Aset**	**Fungsi Aset**	**Konektifitas Proses Bisnis**
		menggantikan peran tersebut (cadangan)	
	PABX	PABX digunakan untuk mengatur komunikasi telpon masuk dan telpon keluar agar efisien dan efektif.	Non Akademik
	Fiber Optik	Fiber Optik digunakan untuk mentransmisikan sinyal dari suatu tempat ke tempat lain	Akademik
	Panel Fiber Optik	Panel Fiber optic digunakan untuk mengelola kabel fiber optic agar siap di konversikan	Akademik
	Media Converter (FO to Ethernet)	Media Converter digunakan untuk mengkonversikan Fiber Optik ke kabel UTP	Akademik
	Kabel UTP	Kabel UTP digunakan sebagai kabel untuk jaringan Local Area Network (LAN) pada system network/jaringan computer	Akademik
	Free NAS (Dosen)	Free NAS digunakan sebagai Media Penyimpanan	Non-Akademik

Daftar Aset			
Kategori	**Aset**	**Fungsi Aset**	**Konektifitas Proses Bisnis**
		Khusus untuk Dosen JSI.	
	CCTV	CCTV digunakan sebagai media pengawas dengan	Non-Akademik
	IPTV	IPTV digunakan sebagai media pengawas dengan menggunakan kamera IP	Non-Akademik
	ISTV	ISTV digunakan sebagai media sarana informasi visual	Non-Akademik
Software	**SIM-Keluhan**	Sistem Informasi yang digunakan untuk menyampaikan keluhan terkait sarana dan prasarana di Sistem Informasi	Non-Akademik
	SIM-Kepegawaian	Sistem Informasi yang digunakan untuk mencatat aktifitas seputar kepegawaian	Non-Akademik
	E-Learning	Sistem Informasi yang digunakan untuk menyimpan serta pemberian informasi seputar kegiatan akademik	Non-Akademik
	Fingerprint	Sistem Informasi yang digunakan untuk merekap absensi.	Non-Akademik

Daftar Aset			
Kategori	**Aset**	**Fungsi Aset**	**Konektifitas Proses Bisnis**
Informasi	**File Sharing**	Data yang disimpan oleh mahasiswa dan dosen di server	Non-Akademik
	Kepegawaian	Data kepegawaian yang dibackup di server	Non-Akademik
	E-Learning	Data E-learning JSI	Non-Akademik
	Fingerprint	Data rekapan Fingerprint	Non-Akademik
Network	**Bandwith**	Nilai hitung atau perhitungan konsumsi transfer data telekomunikasi yang dihitung dalam satuan bit per detik atau yang biasa disingkat bps.	Akademik
SDM	**Staff IS Net**	Staff yang bertanggung jawab dan mengawasi keseluruhan kegiatan seputar aset informasi yang ada di IS Net dan dilingkungannya.	Akademik
	Staff Laboran	Staff yang bertanggung jawab dan mengawasi keseluruhan	Akademik

12.5 Daftar Aset Kritis

Penentuan aset yang penting dilakukan melalui pengumpulan informasi tentang aset, kebutuhan keamanan, ancaman dan kekuatan serta kelemahan organisasi dari narasumber yang berperan langsung setiap harinya.

Aset Kritis	Alasan / Sebab	Dampak Proses Bisnis
Server	Server sangat dibutuhkan sebagai penyedia sumberdaya dan mengendalikan akses didalam suatu jaringan	Jika aset ini tidak berjalan sebagai mana mestinya, maka akan ada lebih dari 500 pengguna server mulai dari seluruh mahasiswa, dosen, dan karyawan yang memiliki akses ke server.
Access point	Access point dibutuhkan stakeholder untuk terhubung dengan internet maupun intranet	Jika aset ini tidak berjalan sebagai mana mestinya, layanan informasi berupa pintu akses intranet dan internet di jaringan ISNet menjadi terhambat.
Switch	Switch digunakan untuk distribusi penyebaran dari satu kabel UTP ke banyak kabel UTP	Jika aset ini tidak berjalan sebagai mana mestinya, layanan informasi berupa pintu akses intranet dan internet di jaringan ISNet menjadi terhambat.
UPS	UPS digunakan untuk sumberdaya cadangan saat terjadinya *power failure*	Jika aset ini tidak berfungsi sebagai mana mestinya, akan berakibat aset yg lain seperti server tidak

Aset Kritis	Alasan / Sebab	Dampak Proses Bisnis
		dapat diakses saat terjadi power failure.
Fiber Optik	Fiber Optik merupakan sumber utama transmisi sinyal internet dari pusat	Jika aset ini tidak tersedia, layanan informasi berupa pintu akses internet untuk jaringan ISNet menjadi terhenti.
Converter FO to UTP	Jika tidak ada Converter ini, FO tidak bisa dengan mudah di distribusikan	Jika aset ini tidak berfungsi, layanan informasi berupa pintu akses internet untuk jaringan ISNet menjadi terhenti.
Kabel UTP	Kabel UTP berfungsi untuk pendistribusian dari ISNet ke access point dan switch yang ada di seluruh gedung	Jika kabel UTP tidak berfungsi sebagai mana mestinya, layanan informasi berupa pintu akses intranet dan internet di jaringan ISNet menjadi terhambat.
SDM	SDM bertanggung jawab akan aset yang ada di wilayah tanggung jawabnya.	Jika aset ini mengalami gangguan, layanan informasi berupa pintu akses internet untuk jaringan ISNet menjadi terhenti.
Bandwith	Bandwidth merupakan satuan kapasitas koneksi internet dalam suatu jaringan	Jika bandwidth tidak tersedia, layanan informasi berupa pintu akses internet di jaringan ISNet menjadi terhenti.

12.6 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. 3 Daftar Kebutuhan Keamanan Aset Kritis

Aset Kritis	Kebutuhan Keamanan	Penjelasan
Server	Kerahasiaan *(Confidentiality)*	Tersedianya akses untuk pihak yang berwenang.
	Integritas *(Integrity)*	Server tidak boleh diakses oleh pihak yang tidak berwenang yang dapat mengubah konten.
	Ketersediaan *(Availability)*	Server harus bisa di akses 24 jam
Access point	Kerahasiaan *(Confidentiality)*	Adanya Firewall dan proxy untuk melakukan filtering access (hanya yang memiliki email dan password)
	Integritas *(Integrity)*	Access point dipastikan berada di tempat yang aman dan memiliki password agar terhindar dari pengguna yang tidak dikenal
	Ketersediaan *(Availability)*	Access point harus bisa di akses 24 jam
Switch	Kerahasiaan *(Confidentiality)*	Tersedianya akses untuk pihak yang berwenang.

Aset Kritis	Kebutuhan Keamanan	Penjelasan
	Integritas *(Integrity)*	Switch dipastikan hanya diakses oleh pihak yang berwenang
	Ketersediaan *(Availability)*	Switch harus bisa di akses 24 jam
UPS	Kerahasiaan *(Confidentiality)*	Berada di tempat yang aman.
	Integritas *(Integrity)*	UPS dipastikan berada di tempat yg aman
	Ketersediaan *(Availability)*	Terpasangnya sensor otomatis untuk memonitor peralatan agar selalu dapat digunakan jika dibutuhkan
Fiber Optik	Kerahasiaan *(Confidentiality)*	Akses fisik hanya dimiliki oleh pihak yang berwenang
	Integritas *(Integrity)*	Fiber optik dipastikan dalam pengawasan pihak yang berwenang
	Ketersediaan *(Availability)*	Terpasangnya sensor untuk memonitor peralatan jaringan agar selalu dapat digunakan
Panel Fiber Optik	Kerahasiaan *(Confidentiality)*	Akses fisik hanya dimiliki oleh pihak yang berwenang
	Integritas *(Integrity)*	Fiber optik dipastikan dalam pengawasan pihak yang berwenang
	Ketersediaan *(Availability)*	Terpasangnya sensor untuk memonitor peralatan jaringan agar selalu dapat digunakan
Converter PO to UTP	Kerahasiaan *(Confidentiality)*	Akses fisik hanya dimiliki oleh pihak yang berwenang
	Integritas *(Integrity)*	Fiber optik dipastikan dalam pengawasan pihak yang berwenang
	Ketersediaan *(Availability)*	Terpasangnya sensor untuk memonitor peralatan jaringan agar selalu dapat digunakan
Kabel UTP	Kerahasiaan *(Confidentiality)*	Akses fisik hanya dimiliki oleh pihak yang berwenang

Aset Kritis	Kebutuhan Keamanan	Penjelasan
	Integritas *(Integrity)*	Fiber optik dipastikan dalam pengawasan pihak yang berwenang
	Ketersediaan *(Availability)*	Terpasangnya sensor untuk memonitor peralatan jaringan agar selalu dapat digunakan
SDM	Kerahasiaan *(Confidentiality)*	Organisasi harus memastikan bahwa SDM yang memiliki hak akses dapat dipertanggungjawabkan
	Integritas *(Integrity)*	Staff harus mengikuti training agar bisa mengoperasikan hal-hal terkait atas tanggung jawabnya.
	Ketersediaan *(Availability)*	Kurangnya jumlah SDM yang berperan langsung pada kegiatan sehari-hari.

12.7 Identifikasi ancaman ke aset kritis

Proses identifikasi ancaman aset kritis dengan menggabungkan informasi dari narasumber dengan profil ancaman terhadap aset kritis. Selain itu beberapa daftar ancaman juga mengacu kepada ISO 27005.

Tabel 5. 4 Identifikasi Ancaman ke Aset Kritis

Aset	Ancaman	Status
Server	Kesalahan konfigurasi dan perawatan server	Belum Pernah Terjadi
	Server lemot	Belum Pernah Terjadi
	Terjadi kebocoran air ac di ruangan server	Belum Pernah Terjadi
	AC diruangan server mati/rusak	Belum Pernah Terjadi
	Memori server penuh	Sudah Terjadi
	Overloaded user	Sudah Terjadi

Aset	Ancaman	Status
	Server terserang virus/malware	Belum Pernah Terjadi
	Hilangnya pasokan listrik	Sudah terjadi
	Kerentanan terhadap voltase yang bervariasi	Sudah terjadi
	Debu & Korosi pada Hardware	Sudah terjadi
Access point	Hilang / Rusak nya Perangkat	Belum Pernah Terjadi
	Brute attack	Belum Pernah Terjadi
	Phising	Belum Pernah Terjadi
	Koneksi terputus	Sudah terjadi
	Hilangnya pasokan listrik	Sudah terjadi
	Debu & Korosi pada Hardware	Sudah terjadi
Switch	Hilang / rusaknya perangkat	Belum Pernah Terjadi
	Kesalahan konfigurasi	Sudah terjadi
	Hilangnya pasokan listrik	Sudah terjadi
	Debu & Korosi pada Hardware	Sudah terjadi
UPS	Hilang / rusaknya perangkat	Belum Pernah Terjadi
	Baterai UPS tidak dapat tahan lama.	Sudah terjadi
	Debu & Korosi pada Hardware	Belum Pernah Terjadi
Fiber Optik	Kabel fiber Optik rusak	Belum Pernah Terjadi
Panel Fiber Optik	Hilang / rusaknya perangkat	Belum Pernah Terjadi
	Konsleting panel	Belum Pernah Terjadi
	Debu & Korosi pada Hardware	Belum Pernah Terjadi
Converter FO to UTP	Hilang / rusaknya perangkat	Belum Pernah Terjadi

Aset	Ancaman	Status
	Debu & Korosi pada Hardware	Belum Pernah Terjadi
Kabel UTP	Kabel digigit tikus	Sudah terjadi
	Debu & Korosi pada Hardware	Sudah terjadi
SDM	Kekurangan tenaga kerja	Belum Pernah Terjadi
	Penggunaan peralatan yang tidak sah	Belum Pernah Terjadi
	Penyangkalan atas tindakan	Belum Pernah Terjadi
Bandwidth	Kapasitas tidak memadai	Sudah terjadi

12.8 Identifikasi kerentanan

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 aset kritis yang nantinya akan digunakan sebagai refrensi untuk membuat risk register. Proses identifikasi kerentanan asset kritis dari narasumber ISNet. Selain itu beberapa daftar kerentanan mengacu kepada ISO .

Tabel 5. 5 Identifikasi Kerentanan

Aset	Kerentanan
Server	Beban kerja server yang tinggi
	Kerentanan terhadap supply listrik yang tidak stabil
	Hubungan arus pendek pada panel listrik
	Kerentanan pertambahan memori yang cepat dalam pemrosesan data.
	Kerentanan terhadap voltase yang bervariasi.
Access point	Maintenance hardware tidak teratur
	Koneksi jaringan public yang tidak dilindungi.
	Kualitas jaringan yang kurang baik

Aset	Kerentanan
	Kerentanan terhadap keberadaan lalu lintas sensitive.
	Arsitektur jaringan yang tidak aman
Switch	Maintenance hardware tidak teratur
	Tidak tersedianya back-up pasokan listrik
UPS	Maintenance hardware tidak teratur
	Power Outage lebih dari kapasitas UPS
Fiber Optik	Terjadi trouble pada kabel fiber optik
Panel Fiber Optik	Maintenance hardware tidak teratur
	Hubungan arus pendek pada panel FO
	Kerentanan terhadap kelembapan, debu, kotoran
Converter FO to UTP	Maintenance hardware tidak teratur
	Kerentanan terhadap kelembapan, debu, kotoran
Kabel UTP	Peletakan Kabel Sembarangan
	Tidak ada pelindung kabel
	Jalur komunikasi yang tidak dilindungi
SDM	Ketidakhadiran SDM
	Pelatihan keamanan yang tidak cukup
	Kurangnya kesadaran akan keamanan
	Kurangnya mekanisme pemantauan
	Kurangnya kebijakan untuk penanganan insiden terkait jaringan
Bandwidth	Banyaknya akses pada waktu yang bersamaan

BAB VI
HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai hasil dan pembahasan yang didapatkan dari penilitian ini agar dapat menjawab rumusan masalah penelitian.

6.1 Pembahasan identifikasi risiko

Pembahasan hasil identifikasi risiko dibuat berdasarkan daftar ancaman yang sudah diidentifikasi sebelumnya pada aset-aset yang ada.

Di tabel ini, risiko yang dibentuk berdasarkan ancaman dan penyebab yang sudah ditentukan sebelumnya berdasarkan hasil wawancara dengan narasumber. Kemudian disertai dengan dampak yang mengakibatkan

Tabel 13.1 Risk Register

Kategori	Nama Aset	Ancaman	ID Risiko	Penyebab	Risiko	Dampak
People	SDM	Lupa membackup data	P01	Tidak menggunakan konfigurasi RAID	Tidak memiliki data backup	Terhambatnya proses bisnis
				Ketidaksengajaan dan kelalaian dari admin dan laboran		
				Tidak adanya peringatan khusus dalam penjadwalan backup data		
				Proses back up data masih secara manual		
		Penduplikasian data	P02	Kurangnya kesadaran	Penyebaran data dan informasi rahasia	Kerugian internal organisasi
				Terdapat kepentingan pribadi yang menyimpang		
				Adanya *unauthorized access*		
		Penyalahgunaan aset	P03	Kurangnya kesadaran terhadap pentingnya aset	Kerusakan aset	Kerugian secara finansial dan non – finansial
				Kurangnya pemahaman dan kesadaran terhadap SOP dalam penggunaan aset ISNet		
		Kesalahan konfigurasi		Kurangnya pengetahuan dalam mengoperasikan aset		
Hardware	Server	Pencurian	H01	Lokasi server yang mudah dijangkau	Kehilangan server	Kerugian secara finansial dan non – finansial
				Tidak ada pengamanan khusus berlapis pada server		
		Penyalahgunaan akses server	H02	Terdapat celah keamanan pada akses server di ISNet	Penyebaran data dan informasi rahasia	Kerahasiaan data dan informasi ISNet bocor
		D-DOS, SQL-Injection, Sniffing		Adanya praktik ilegal dari seseorang yang tidak bertanggung jawab	Server down	Terhambatnya proses bisnis
			H03	Terdapat kerentanan terhadap sistem keamanan server		
		Overload Request		Banyak pengguna yang mengakses server dalam satu waktu		
				Terlalu banyak yang mengunggah file pada share		
				Kapasitas memori data yang tidak memadai		

Kategori	Nama Aset	Ancaman	ID Risiko	Penyebab	Risiko	Dampak
		Bencana alam	H04	Kerentanan alam dan lokasi	Kerusakan server	Kerugian secara finansial dan non – finansial
		Overheat		Aliran udara di server yang kurang baik		Terhambatnya proses bisnis
				Suhu ruangan yang terlalu panas		
				Kualitas server yang kurang baik		
				Umur server yang sudah tua dan usang		
				Terlalu banyak debu		
		Listrik padam		Jadwal pemadam mati listrik		Kerugian secara finansial dan non – finansial
				Hewan yang mengigit kabel listrik		
				Beban listrik yang terlalu besar		
				Hubungan arus pendek		
Hardware	Switch	Pencurian	H05	Lokasi switch yang mudah dijangkau	Kehilangan switch	Kerugian secara finansial dan non – finansial
				Tidak ada pengamanan khusus pada switch		
		Bencana alam	H06	Kerentanan alam dan lokasi	Kerusakan switch	
		Overheat		Suhu ruangan yang terlalu panas		Terhambatnya proses bisnis
				Kualitas switch yang kurang baik		
				Umur switch yang sudah tua dan usang		
		Listrik padam		Jadwal pemadam mati listrik		
				Hewan yang mengigit kabel listrik		
				Beban listrik yang terlalu besar		
				Hubungan arus pendek		
Hardware	Access Point	Pencurian	H07	Sistem keamanan JSI kurang baik	Kehilangan router	Kerugian secara finansial dan non – finansial
		Bencana alam	H08	Kerentanan alam dan lokasi	Kerusakan access point	
		Overheat		Suhu ruangan yang terlalu panas		Terhambatnya proses bisnis
				Kualitas router yang kurang baik		

Kategori	Nama Aset	Ancaman	ID Risiko	Penyebab	Risiko	Dampak
				Umur router yang sudah tua dan usang		
		Listrik padam		Jadwal pemadam mati listrik		
				Hewan yang mengigit kabel listrik		
				Beban listrik yang terlalu besar		
				Hubungan arus pendek		
Hardware	UPS	Pencurian	H09	Sistem Keamanan di ISNet kurang baik	Kehilangan UPS	Kerugian secara finansial dan non – finansial
		Bencana alam	H10	Kerentanan alam dan lokasi	Kerusakan UPS	
		UPS tidak berfungsi semestinya		Baterai UPS sudah tua dan usang		Terhambatnya proses bisnis
Hardware	Fiber Optik	Bencana Alam	H11	Kerentanan alam dan lokasi	Kerusakan Fiber Optik	Kerugian secara finansial dan non – finansial
		Kabel Terputus		Kabel digigit tikus		
Hardware	Converter FO To UTP	Pencurian	H12	Tidak ada pengamanan khusus terhadap converter	Kehilangan Converter FO	Kerugian secara finansial dan non – finansial
				Lokasi converter yang mudah dijangkau oleh		
		Bencana alam	H13	Kerentanan alam dan lokasi	Kerusakan Converter FO	
		Listrik padam		Jadwal pemadaman mati listrik		Terhambatnya proses bisnis
				Hubungan arus pendek		
				Hewan yang menggigit kabel listrik		
Hardware		Pencurian	H14	Tidak ada pengamanan khusus terhadap kabel		

Kategori	Nama Aset	Ancaman	ID Risiko	Penyebab	Risiko	Dampak
	Kabel UTP			Lokasi kabel yang mudah dijangkau oleh pengguna jaringan ISNet	Kehilangan kabel UTP	Terhambatnya proses bisnis
		Bencana alam	H15	Kerentanan alam dan lokasi	Kerusakan fisik	Kerugian secara finansial
		Listrik padam		Jadwal pemadam mati listrik		
				Hewan yang mengigit kabel listrik		
				Beban listrik yang terlalu besar		
				Hubungan arus pendek		
		Kabel terputus	H16	RJ45 Rusak	Kabel tidak dapat mentransfer data	Terhambatnya proses bisnis
				Kabel digigit hewan		Kerugian secara finansial
		Kabel tergulung		Kelalaian pengguna		
Network	Bandwidth	Overload Request	N01	Banyak pengguna yang mengakses jaringan dalam satu waktu	Bandwidth habis	Terhambatnya proses bisnis
		DoS Attack		Adanya praktik illegal dari seseorang yang tidak bertanggung jawab		
				Terdapat kerentanan terhadap sistem keamanan jaringan		

6.3 Risk Assesment (RPN)

Dalam tahapan ini, dilakukan menggabungan data dari daftar risiko, ancaman serta kerentanan untuk dilakukan penilaian berdasarkan metode yang digunakan di penelitian ini yaitu FMEA.

Dalam memberikan penilaian, digolongkan menjadi tiga bagian yaitu *severity* (tingkat keparahan), *occurance* (kemungkinan terjadi kesalahan), dan *detection* (deteksi tiap kesalahan) yang nantinya ketiga penilaian tersebut digunakan untuk menghitung RPN (tingkat prioritas risiko). Dibawah ini adalah hasil penilaian yang telah dilakukan penulis dengan menggunakan metode FMEA.

Tabel 13.2 Tabel Penilaian RPN

Kategori	Nama Aset	ID Risiko	Penyebab	Risiko	SEV	JUSTIFIKASI	OCU	JUSTIFIKASI	DET	JUSTIFIKASI	RPN	Dampak
People	SDM	P01	Tidak menggunakan konfigurasi RAID	Tidak memiliki data backup	5	Data berisikan informasi terkait aset	4	Aktivitas backup masih manual	4	Aktifitas backup masih manual	100	Terhambatnya proses bisnis
			Ketidaksengajaan dan kelalaian dari admin dan laboran									
			Tidak adanya peringatan khusus dalam penjadwalan backup data									
			Proses back up data masih secara manual									
		P02	Kurangnya kesadaran	Penyebaran data dan informasi rahasia	3	Data berisikan informasi terkait aset	4	Data yang tersebar cukup jarang terjadi	4	Tingkat control terhadap data yang cukup tinggi	48	Kerugian internal organisasi
			Terdapat kepentingan pribadi yang menyimpang									
			Adanya *unauthorized access*									
		P03	Kurangnya kesadaran terhadap pentingnya aset	Kerusakan aset	8	Kerusakan terhadap aset dapat mengganggu berjalannya	2	Jarang terjadinya adanya kerusakan aset yang	2	Kontrol terhadap pencegahan perusakan aset sudah	32	Kerugian secara finansial dan non – finansial
			Kurangnya pemahaman dan kesadaran terhadap SOP dalam penggunaan aset ISNet									

			Kurangnya pengetahuan dalam mengoperasikan aset			proses bisnis ISNet		disebabkan oleh SDM				
Hardware	Server	H01	Lokasi server yang mudah dijangkau	Kehilangan server	9	Berdampak sangat besar karena menggangu proses bisnis pada ISNet	1	Sangat jarang terjadi	6	Sudah dilakukan tindakan kemanan yang cukup	54	Kerugian secara finansial dan non – finansial
			Tidak ada pengamanan khusus berlapis pada server									
		H02	Terdapat celah keamanan pada akses server di ISNet	Penyebaran data dan informasi rahasia	7	Resiko cukup berdampak	2	Jarang terjadi penyebaran data dan informasi	3	Mudah untuk dilakukan tindakan pencegahan	42	Kerahasiaan data dan informasi ISNet bocor
		H03	Adanya praktik ilegal dari seseorang yang tidak bertanggung jawab	Server down	8	Berdampak sangat besar karena menggangu proses bisnis pada LPSI	7	Cukup sering terjadinya server down	7	Tindakan pencegagan yang sudah masih kurang	392	Terhambatnya proses bisnis
			Terdapat kerentanan terhadap sistem keamanan server									
			Banyak pengguna yang mengakses server dalam satu waktu									
			Terlalu banyak yang mengunggah file pada share									
			Kapasitas memori data yang tidak memadai									
		H04	Kerentanan alam dan lokasi	Kerusakan server	9	Berdampak sangat besar karena menggangu proses bisnis pada LPSI	1	Sangat jarang terjadi	2	Kontol terhadap pencegahan perusakan aset sudah tinggi	18	Kerugian secara finansial dan non – finansial
			Aliran udara di server yang kurang baik									Terhambatnya proses bisnis
			Suhu ruangan yang terlalu panas									
			Kualitas server yang kurang baik									
			Umur server yang sudah tua dan usang									

			Terlalu banyak debu									
			Jadwal pemadam mati listrik									Kerugian secara finansial dan non – finansial
			Hewan yang mengigit kabel listrik									
			Beban listrik yang terlalu besar									
			Hubungan arus pendek									
Hardware	Switch	H05	Lokasi switch yang mudah dijangkau	Kehilangan switch	6	Resiko cukup berdampak	1	Sangat jarang terjadi	2	Kontol terhadap pencegahan perusakan aset sudah tinggi	12	Kerugian secara finansial dan non – finansial
			Tidak ada pengamanan khusus pada switch									
		H06	Kerentanan alam dan lokasi	Kerusakan switch	5	Resiko cukup berdampak	2	Cukup jarang terjadinya kerusakan switch	3	Tingkat kontrol terhadap aset yang cukup tinggi	30	
			Suhu ruangan yang terlalu panas									Terhambatnya proses bisnis
			Kualitas switch yang kurang baik									
			Umur switch yang sudah tua dan usang									
			Jadwal pemadam mati listrik									
			Hewan yang mengigit kabel listrik									
			Beban listrik yang terlalu besar									
			Hubungan arus pendek									

Hardware	Access Point	H07	Sistem keamanan JSI kurang baik	Kehilangan access point	7	Ketika terjadi kehilangan memiliki dampak yang cukup pada proses bisnis	1	Cukup jarang terjadinya kehilangan router	3	Tingkat kontrol terhadap aset yang cukup tinggi	21	Kerugian secara finansial dan non – finansial
		H08	Kerentanan alam dan lokasi	Kerusakan access point	6	Ketika terjadi kerusakan memiliki dampak yang cukup pada proses bisnis	2	Cukup jarang terjadinya kerusakan router	5	Tingkat kontrol terhadap aset yang sudah cukup	60	Terhambatnya proses bisnis
			Suhu ruangan yang terlalu panas									
			Kualitas router yang kurang baik									
			Umur router yang sudah tua dan usang									
			Jadwal pemadam mati listrik									
			Hewan yang mengigit kabel listrik									
			Beban listrik yang terlalu besar									
			Hubungan arus pendek									
Hardware	UPS	H09	Sistem Keamanan di ISNet kurang baik	Kehilangan UPS	7	Ketika terjadi kehilangan memiliki dampak yang cukup pada proses bisnis	1	Cukup jarang terjadinya kehilangan UPS	3	Tingkat kontrol terhadap aset yang cukup tinggi	21	Kerugian secara finansial dan non – finansial
		H10	Kerentanan alam dan lokasi	Kerusakan UPS	5	Ketika terjadi kerusakan memiliki dampak yang cukup pada proses bisnis	2	Cukup jarang terjadinya kerusakan UPS	5	Tingkat kontrol terhadap aset yang sudah cukup	50	Terhambatnya proses bisnis
			Baterai UPS sudah tua dan usang									

Hardware	Fiber Optik	H11	Kerentanan alam dan lokasi	Kerusakan Fiber Optik	9	Berdampak sangat besar karena menggangu proses bisnis pada LPSI	1	Sangat jarang terjadi	6	Tingkat kontrol terhadap aset yang agak cukup	54	Kerugian secara finansial dan non – finansial
			Kabel digigit tikus									
Hardware	Converter FO To UTP	H12	Tidak ada pengamanan khusus terhadap converter	Kehilangan Converter FO	9	Berdampak sangat besar karena menggangu proses bisnis pada LPSI	1	Sangat jarang terjadi	6	Tingkat kontrol terhadap aset yang agak cukup	54	Kerugian secara finansial dan non – finansial
			Lokasi converter yang mudah dijangkau oleh									
		H13	Kerentanan alam dan lokasi	Kerusakan Converter FO	9	Berdampak sangat besar karena menggangu proses bisnis pada LPSI	1	Sangat jarang terjadi	6	Tingkat kontrol terhadap aset yang agak cukup	54	Terhambatnya proses bisnis
			Jadwal pemadaman mati listrik									
			Hubungan arus pendek									
			Hewan yang menggigit kabel listrik									
Hardware	Kabel UTP	H14	Tidak ada pengamanan khusus terhadap kabel	Kehilangan kabel UTP	6	Ketika terjadi kehilangan memiliki dampak yang cukup pada proses bisnis	2	Cukup jarang terjadinya kehilangan kabel LAN	6	Tingkat kontrol terhadap aset yang agak cukup	72	Terhambatnya proses bisnis
			Lokasi kabel yang mudah dijangkau oleh pengguna jaringan ISNet									
		H15	Kerentanan alam dan lokasi	Kerusakan fisik	5	Ketika terjadi kerusakan memiliki dampak yang cukup pada proses bisnis	6	Cukup jarang terjadinya kerusakan kabel LAN	6	Tingkat kontrol terhadap aset yang agak cukup	180	Kerugian secara finansial
			Jadwal pemadam mati listrik									
			Hewan yang mengigit kabel listrik									
			Beban listrik yang terlalu besar									
			Hubungan arus pendek									

		H16	RJ45 Rusak	Kabel tidak dapat mentransfer data	6	Memiliki dampak yang cukup signifikan	6	Cukup jarang terjadinya malfungsi pada kabel LAN	5	Tingkat kontrol terhadap aset yang cukup	180	Terhambatnya proses bisnis
			Kabel digigit hewan									Kerugian secara finansial
			Kelalaian pengguna									
Network	Bandwidth	N01	Banyak pengguna yang mengakses jaringan dalam satu waktu	Bandwidth habis	6	Memiliki dampak yang cukup signifikan	6	Cukup jarang terjadinya kehabisan bandwidth	5	Tingkat kontrol terhadap aset yang cukup	180	Terhambatnya proses bisnis
			Adanya praktik illegal dari seseorang yang tidak bertanggung jawab									
			Terdapat kerentanan terhadap sistem keamanan jaringan									

6.4 Mitigasi Risiko

Kemudian setelah dilakukan penilaian menggunakan RPN, langkah selanjutnya adalah pembentukan langkah mitigasi yang disarankan oleh ISO 27001 dan 27002. Dari saran tersebut barulah ditentukan opsi mitigasi yang digunakan yaitu 4T (*Treat, Transfer, Take, Terminate*). Dibawah ini adalah hasil dari mitigasi risiko berdasarkan nilai RPN pada sub bab sebelumnya :

Halaman ini sengaja dikosongkan

Tabel 13.3 Tabel Mitigasi Resiko

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
H03	Server Down	Hardware	Adanya praktik ilegal dari seseorang yang tidak bertanggung jawab	●Terhambatnya proes bisnis ISNet ●Penurunan integritas ISNet ●Penurunan tingkat kepercayaan pengguna ISNet ●Kerugian finansial & non-finansial	392	VERY HIGH	Treat	Melakukan konfigurasi pembatasan akses pada server	Pengguna hanya diperbolehkan untuk mengakses ke layanan yang telah diizinkan(11.4.1)
			Terdapat kerentanan terhadap sistem keamanan server				Treat	Melakukan konfigurasi pembatasan akses pada server	Integritas dari informasi tersedia untuk umum harus dilindungi untuk mencegah modifikasi yang tidak diizinkan(10.9.3)
			Banyak pengguna yang mengakses server dalam satu waktu				Treat	Melakukan konfigurasi pembatasan akses pada server	*Network* harus dikelola dan dikontrol untuk emlindunginya dari ancaman dan untuk menjaga keamanan sistem dan aplikasi yang menggunakan *network* tersebut termasuk informasi didalamnya(10.6.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
H15	Kerusakan kabel UTP	Hardware	Kerentanan alam dan lokasi	●Terhambatnya proes bisnis ISNet	180	High	Take	Membuat *Disaster Recovery Plan*	Mendesain dan mengaplikasikan perlindungan fisik terhadap kerusakan yang disebabkan kebakaran, bajir, gempa bumi, ledakan, kerusuhan, dan bentuk lainnya yang berasal dari alam maupun manusia(9.1.4)
			Jadwal pemadam mati listrik	●Terputusnya koneksi pada jaringan			Treat	Mempunyai genset cadangan untuk menyuplai listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)
			Hewan yang mengigit kabel listrik				Treat	Meletakkan kabel pada tempat yang tidak dapat dijangkau hewan	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
			Beban listrik yang terlalu besar				Treat	Mengurangi penggunaan perangkat yang memiliki daya listrik yang besar yang tidak terlalu bermanfaat	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)
			Hubungan arus pendek				Treat	Mengurangi penumpukan steker/colokan listrik Melakukan peemeriksaan rutin terhadap kabel listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)
H16	Kabel UTP tidak dapat mentransfer data	Hardware	Kabel sering dicabut pasang	Terhambatnya proses bisnis ISNet	180	HIGH	Treat	Memberikan pengamanan, semacam rantai atau kunci.	Barang, informasi atau perangkat lunak tidak boleh diambil/dicabut dari tempatnya tanpa ada izin sebelumnya (9.2.7)
			Kabel digigit hewan	Terputusnnya koneksi internet yang ada di ISNet			Treat	Meletakan kabel pada lokasi yang aman dan terlindungi dari gangguan	Kabel tenaga dan telekomunikasi yang membawa data atau informasi pendukung harus terlindungi dari intersepsi atau kerusakan (9.2.3)
				Kerugian dari sisi finansial dan non-finansial					

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
			Kelalaian pengguna	Terhambatnya proses bisnis ISNet			Treat	Memberikan sanksi kepada pengguna yang tidak bisa menjaga aset yang ia pakai	Pengguna harus memastikan bahwa aset tanpa pengawasan harus memiliki kebutuhan perlindungan atau sistem keamanan yang tepat(11.3.2)
P01	Tidak memiliki data backup	People	Tidak menggunakan konfigurasi RAID		100	MEDIUM	Treat	Memperbaharui prosedur dalam memback-up data yaitu dengan melakukan menggunakan konfigurasi RAID	Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada (10.5.1)
			Ketidaksengajaan dan kelalaian dari admin dan laboran	Akan menjadi kerugian finansial apablia data utama hilang, apabila tidak membackup data tersebut sebelumnya			Treat	Memberikan pelatihan dan evaluasi kepada setiap laboran dan admin	Pihak manajemen harus mempunyai karyawan, kontraktor, dan pihak ketiga yang mematuhi kebijakan dan prosedur keamanan yang telah diterapkan pihak organisasi (8.2.1)
			Tidak adanya peringatan khusus dalam penjadwalan backup data				Treat	Membuat prosedur dan penjadwalan yang jelas untuk melakukan back-up data	Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada (10.5.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
			Proses back up data masih secara manual				Treat	Memperharui prosedur dalam memback-up data dengan melakukan otomasi konfigurasi backup data	Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada (10.5.1)
H01	Kehilangan Server	Hardware	Lokasi server yang mudah dijangkau	Terhambatnya proses bisnis ISNet	54	LOW	Treat	Mendesain lokasi server yang tidak mudah dijangkau dengan memindahkan lokasi server ke tempat yang lebih aman dari jangkauan orang lain.	Merancang dan menerapkan keamanan fisik untuk kantor, ruangan, dan lokasi falisitas dari ancaman luar(9.1.3)
			Tidak ada pengamanan khusus berlapis pada server				Treat	Menerapkan sistem pengamanan fisik khusus untuk server ISNet menggunakan cage dan gembok pada ruangan.	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal(9.2.1)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
H04	Kerusakan Server	Hardware	Kerentanan alam dan lokasi	●Terhambatnya proes bisnis	18	Very Low	Take	Membuat *Disaster Recovery Plan*	Mendesain dan mengaplikasikan perlindungan fisik terhadap kerusakan yang disebabkan kebakaran, bajir, gempa bumi, ledakan, kerusuhan, dan bentuk lainnya yang berasal dari alam maupun manusia(9.1.4)
			Aliran udara di server yang kurang baik	●Penurunan integritas LPSI			Treat	Mengubah aliran udara pada Server menjadi lebih baik	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal(9.2.1)
			Suhu ruangan yang terlalu panas	●Penurunan tingkat kepercayaan pengguna LPSI			Treat	Melakukan *maintenance* secara berkala pada *AC*	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal(9.2.1)
			Kualitas server yang kurang baik	●Kerugian finansial & non-finansial			Treat	Melakukan *maintenance* secara berkala pada Server	Peralatan harus dipelihara dengan benar untuk memeastikan availability dan integrity-nya(9.2.4)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
			Umur server yang sudah tua dan usang				Treat	Melakukan pembelian untuk melakukan penggantian terhadap komponen Server	Peralatan harus dipelihara dengan benar untuk memeastikan availability dan integrity-nya(9.2.4)
			Terlalu banyak debu				Treat	Melakukan pembersihan pada PC secara berkala	Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal(9.2.1)
			Jadwal pemadam mati listrik				Treat	Mempunyai genset cadangan untuk menyuplai listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)
			Hewan yang mengigit kabel listrik				Treat	Meletakkan kabel pada tempat yang tidak dapat dijangkau hewan	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)

ID Risiko	Risiko	Kategori	Penyebab	Dampak	RPN	Level	Opsi Mitigasi	Bentuk Mitigasi	Kontrol(ISO 27001/27002)
			Beban listrik yang terlalu besar				Treat	Mengurangi penggunaan perangkat yang memiliki daya listrik yang besar yang tidak terlalu bermanfaat	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)
			Hubungan arus pendek				Treat	Mengurangi penumpukan steker/colokan listrik Melakukan peemeriksaan rutin terhadap kabel listrik	Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung(9.2.2)

6.5 Validasi

Proses validasi dilakukan langsung ke organisasi yaitu ISNet. Validasi dilakukan hari Rabu, 6 Januari 2015, bertemu dengan orang yang bertanggung jawab di ISNet yaitu Bapak Nanok Adi Saputra. Validasi dilakukan untuk memenuhi hal sebagai berikut.

1. Kesesuaian strategi pengendalian risiko dengan kondisi perusahaan
2. Kesesuaian penilaian ancaman sesuai dengan kondisi perusahaan
3. Kesesuaian penelian kerentanan sesuai dengan kondisi perusahaan
4. Kesesuaian identifikasi karakter risiko dapat diterima perusahaan
5. Kesesuaian risiko sesuai dengan kondisi perusahaan
6. Penerimaan hasil prioritas risiko sesuai dengan kondisi perusahaan
7. Penerimaan hasil mitigasi berdasarkan standar ISO 27002

Sebagaimana validasi digunakan untuk memastikan bahwa yang diteliti sudah sesuai dengan yang diharapkan.

6.5 Detail dan Informasi *Control Objectives*

Dibawah ini adalah informasi terkait *control objectives* yang mengacu pada ISO 27001 dan ISO 27002:

Tabel 13.4 Tabel Control Objectives H03

ID Risk	: H03
Kategori	: Hardware
Risiko	: Server Down
Penyebab	: Adanya praktik ilegal dari seseorang yang tidak bertanggung jawab
Control Objective **11.4.1 [Pembatasan Akses]** Pengguna hanya diperbolehkan untuk mengakses ke layanan yang telah diizinkan	
Implementasi : • Menentukan jaringan dan layanan jaringan yang boleh diakses • Prosedur autorisasi untuk menentukan pihak mana saja yang dapat mengakses jaringan • Manajemen kontrol dan prosedur untuk memproteksi akses ke jaringan	

Tabel 13.5 Tabel Control Objectives H03

ID Risk	: H03
Kategori	: Hardware
Risiko	: Server Down
Penyebab	: Terdapat kerentanan terhadap sistem keamanan server
Control Objective **10.9.3 [Perlindungan Informasi]**	

Integritas dari informasi tersedia untuk umum harus dilindungi untuk mencegah modifikasi yang tidak diizinkan
Implementasi : • Informasi yang diperoleh sesuai dengan undang - undang perlindungan data • Informasi sensitif dilindungi selama proses pengumpulan, pengolahan dan penyimpanan • Akses ke sistem yang tidak diijinkan tidak boleh diakses

Tabel 13.6 Tabel Control Objectives H03

ID Risk	: H03
Kategori	: Hardware
Risiko	: Server Down
Penyebab	: Banyak pengguna yang mengakses server dalam satu waktu
Control Objective **10.6.1 [Pengelolaan jaringan]** Network harus dikelola dan dikontrol untuk emlindunginya dari ancaman dan untuk menjaga keamanan sistem dan aplikasi yang menggunakan network tersebut termasuk informasi didalamnya	
Implementasi : • Tanggung jawab terhadap jaringan harus dipisahkan dengan operasional komputer • Tanggung jawab dan prosedur untuk manajemen remote *equipment* • Kontrol khusus untuk membangun kemanan yang konfidential dan integritas data	

ID Risk	: H03
Kategori	: Hardware
Risiko	: Server Down

Penyebab	: Terlalu banyak yang mengunggah file pada share
Control Objective **10.6.1 [Pengelolaan jaringan]** Network harus dikelola dan dikontrol untuk emlindunginya dari ancaman dan untuk menjaga keamanan sistem dan aplikasi yang menggunakan network tersebut termasuk informasi didalamnya	
Implementasi : • Tanggung jawab terhadap jaringan harus dipisahkan dengan operasional komputer • Tanggung jawab dan prosedur untuk manajemen remote equipment • Kontrol khusus untuk membangun kemanan yang konfidential dan integritas data	

Tabel 13.7 Tabel Control Objectives H03

ID Risk	: H03
Kategori	: Hardware
Risiko	: Server Down
Penyebab	: Kapasitas memori data yang tidak memadai
Control Objective **9.2.4 [Pengelolaan jaringan]** Peralatan harus dipelihara dengan benar untuk memeastikan availability dan integrity-nya	
Implementasi : • Harus dilakukan tindakan maintenance berdasarkan dari rekomendasi interval dan spesifikasi pemasok aset • Hanya staff yang diizinkan yang dapat melakukan perbaikan dan servis • Tindakan kontrol yang dilakukan ketika aset dijadwalkan untuk dilakukan maintenance	

Tabel 13.8 Tabel Control Objectives H15

ID Risk	: H15
Kategori	: Hardware
Risiko	: Kerusakan kabel UTP
Penyebab	: Hewan yang mengigit kabel listrik
Control Objective **9.2.2 [Perlindungan Aset terhadap listrik]** Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung	
Implementasi : • Penggunaan UPS • Emergency power off switches diletakkan di dekat emergency door • Penggunaan Genset	

Tabel 13.9 Tabel Control Objectives H15

ID Risk	: H15
Kategori	: Hardware
Risiko	: Kerusakan kabel UTP
Penyebab	: Beban listrik yang terlalu besar
Control Objective **9.2.2 [Perlindungan Aset terhadap listrik]** Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung	
Implementasi : • Penggunaan UPS • Emergency power off switches diletakkan di dekat emergency door • Penggunaan Genset	

Tabel 13.10 Tabel Control Objectives H15

ID Risk	: H15
Kategori	: Hardware
Risiko	: Kerusakan kabel UTP
Penyebab	: Hubungan arus pendek
Control Objective **9.2.2 [Perlindungan Aset terhadap listrik]** Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung	
Implementasi : • Penggunaan UPS • Emergency power off switches diletakkan di dekat emergency door • Penggunaan Genset	

Tabel 13.11 Tabel Control Objectives H16

ID Risiko	: H16
Kategori	: Hardware
Risiko	: Kabel UTP tidak dapat mentransfer data
Penyebab	: Kabel sering dicabut pasang
Control Objective : **9.2.7 [Pemindahan Properti]** Barang, informasi atau perangkat lunak tidak boleh diambil/dicabut dari tempatnya tanpa ada izin sebelumnya	
Implementasi : 1) Aset, informasi atau perangkat lunak tidak boleh dipindahkan tanpa ada izin sebelumnya 2) Karyawan, kontraktor dan pengguna pihak ketiga yang memiliki otoritas untuk mengizinkan pemindahan aset 3) Batas waktu untuk pemindahan harus ditetapkan dan dilakukan penyesuaian ulang	

Tabel 13.12 Tabel Control Objectives H16

ID Risiko	: H16
Kategori	: Hardware
Risiko	: Kabel UTP idak dapat mentransfer data
Penyebab	: Kabel digigit hewan
Control Objective : **9.2.3 [Keamanan Kabel]** Kabel tenaga dan telekomunikasi yang membawa data atau informasi pendukung harus terlindungi dari intersepsi atau kerusakan	
Implementasi : 1) Kabel ditempatkan di bawah tanah dan berada pada tempat yang sulit dijangkau 2) Kabel harus dilindungi 3) Melakukan pengecekan dan kontrol secara berkala dengan menyeluruh pada kabel	

Tabel 13.13 Tabel Control Objectives H16

ID Risiko	: H16
Kategori	: Hardware
Risiko	: Kabel UTP tidak dapat mentransfer data
Penyebab	: Kelalaian pengguna
Control Objective : **11.3.2 [Pengguna Aset Tanpa Pengawasan]** Pengguna harus memastikan bahwa aset tanpa pengawasan harus memiliki kebutuhan perlindungan atau sistem keamanan yang tepat	
Implementasi : 1) Melakukan penguncian pada PC yang telah dipakai	

2) Mengamankan PC dari pemakaian tanpa izin dengan menggunakan password akses ketika akan dipakai 3) Melakukan log-off PC dan server ketika selesai pemakaian

Tabel 13.14 Tabel Control Objectives P01

ID Risiko	: P01
Kategori	: People
Risiko	: Tidak memiliki data backup
Penyebab	: Tidak menggunakan konfigurasi RAID
Control Objective : **11.4.1 [Backup Informasi]** Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada	
Implementasi : 1) Tingkat kepentingan dari informasi yang akan dibackup harus didefinisikan 2) Back-up media harus diuji secara teratur untuk memastikan bahwa mereka dapat diandalkan untuk penggunaan darurat bila diperlukan 3) Kerahasiaan merupakan hal penting, backup harus dilindungi dengan enkripsi	

Tabel 13.15 Tabel Control Objectives P01

ID Risiko	: P01
Kategori	: People
Risiko	: Tidak memiliki data backup
Penyebab	: Ketidaksengajaan dan kelalaian dari admin dan laboran
Control Objective : **8.2.1 [Manajemen Tanggung Jawab]**	

Pihak manajemen harus mempunyai karyawan, kontraktor, dan pihak ketiga yang mematuhi kebijakan dan prosedur keamanan yang telah diterapkan pihak organisasi
Implementasi : 1) Penjelasan tentang peran keamanan informasi dan tanggung jawab sebelum akses yang diberikan kepada informasi atau sistem informasi yang bersifat sensitif 2) Disediakan pedoman untuk menyatakan ekspetasi keamanan dan peran mereka dalam organisasi 3) Memotivasi untuk menjalankan kebijakan keamanan organisasi

Tabel 13.16 Tabel Control Objectives P01

ID Risiko	: P01
Kategori	: People
Risiko	: Tidak memiliki data backup
Penyebab	: Tidak adanya peringatan khusus dalam penjadwalan backup data
Control Objective : **10.5.1 [Backup Informasi]** Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada	
Implementasi : 1) Mendefinisikan tingkat kebutuhan informasi yang harus dicakup 2) Mencatat secara akurat dan lengkap dari proses backup 3) Mendefinisikan media backup harus diuji digunakkan untk	

Tabel 13.17 Tabel Control Objectives P01

ID Risiko	: P01
Kategori	: People
Risiko	: Tidak memiliki data backup
Penyebab	: Proses back up data masih secara manual
Control Objective : **10.5.1 [Backup Informasi]** Back-up informasi dan perangkat lunak harus ada dan sesuai dengan kebijakan back-up yang ada	
Implementasi : 1) Mendefinisikan tingkat kebutuhan informasi yang harus dicakup 2) Mencatat secara akurat dan lengkap dari proses backup 3) Mendefinisikan media backup harus diuji digunakkan untk	

Tabel 13.18 Tabel Control Objectives H01

ID Risiko	H01
Kategori	Hardware
Risiko	Kehilangan Server
Penyebab	Lokasi server yang mudah dijangkau
Control Objective : **9.1.3 [Pengamanan Kantor, Ruangan, dan Fasilitas]** Merancang dan menerapkan keamanan fisik untuk kantor, ruangan, dan lokasi falisitas dari ancaman luar	
Implementasi : 1) Menetapkan standar dan regulasi lokasi server yang aman dari jangkauan orang lain 2) Menggunakan kunci atau password pada lokasi tempat penyimpanan server untuk mencegah akses masuk dari publik	

3) Menjaga server dari orang - orang yang tidak berkepentingan dan ilegal

Tabel 13.19 Tabel Control Objectives H01

ID Risiko	H01
Kategori	Hardware
Risiko	Kehilangan Server
Penyebab	Tidak ada pengamanan khusus berlapis pada server
Control Objective : **9.2.1 [Penempatan dan Proteksi Aset]** Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal	
Implementasi : 1) Server diletakkan di tempat yang aman dan terawasi oleh CCTV dan laboran maupun admin 2) Server diberikan perlindungan keamanan khusus berlapis seperti pemberian password, sensor, dan cage 3) Pengawasan dan pemeriksaan rutin kondisi server harus dilakukan secara berkala untuk meminimalkan risiko pencurian Server	

Tabel 13.20 Tabel Control Objectives H04

ID Risk	: H04
Kategori	: Hardware
Risiko	: Kerusakan Server
Penyebab	: Aliran udara di server yang kurang baik

Control Objective **9.2.1 [Perlindungan Aset]** Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal
Implementasi : • Kontrol untuk meminimalkan potensi dari risiko fisik • Aset yang membutuhkan perlindungan khusus harus diisolasi • Terdapat peraturan terhadap makanan, minuman, merokok

Tabel 13.21 Tabel Control Objectives H04

ID Risk	: H04
Kategori	: Hardware
Risiko	: Kerusakan Server
Penyebab	: Suhu ruangan yang terlalu panas
Control Objective **9.2.1 [Perlindungan Aset]** Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal	
Implementasi : • Kontrol untuk meminimalkan potensi dari risiko fisik • Aset yang membutuhkan perlindungan khusus harus diisolasi • Terdapat peraturan terhadap makanan, minuman, merokok	

Tabel 13.22 Tabel Control Objectives H04

ID Risk	: H04
Kategori	: Hardware
Risiko	: Kerusakan Server

Penyebab	: Kualitas server yang kurang baik
Control Objective **9.2.4 [Pemeliharaan Aset]** Peralatan harus dipelihara dengan benar untuk memeastikan availability dan integrity-nya	
Implementasi : • Harus dilakukan tindakan maintenance berdasarkan dari rekomendasi interval dan spesifikasi pemasok aset • Hanya staff yang diizinkan yang dapat melakukan perbaikan dan servis • Tindakan kontrol yang dilakukan ketika aset dijadwalkan untuk dilakukan maintenance	
ID Risk	: H06
Kategori	: Hardware
Risiko	: Kerusakan Server
Penyebab	: Umur server yang sudah tua dan usang
Control Objective **9.2.4 [Pemeliharaan Aset]** Peralatan harus dipelihara dengan benar untuk memeastikan availability dan integrity-nya	
Implementasi : • Harus dilakukan tindakan maintenance berdasarkan dari rekomendasi interval dan spesifikasi pemasok aset • Hanya staff yang diizinkan yang dapat melakukan perbaikan dan servis • Tindakan kontrol yang dilakukan ketika aset dijadwalkan untuk dilakukan maintenance	

Tabel 13.23 Tabel Control Objectives H04

ID Risk	: H04
Kategori	: Hardware
Risiko	: Kerusakan Server
Penyebab	: Terlalu banyak debu

Control Objective **9.2.1 [Perlindungan Aset]** Segala peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman lingkungan, bahaya, akses yang tidak legal
Implementasi : • Kontrol untuk meminimalkan potensi dari risiko fisik • Aset yang membutuhkan perlindungan khusus harus diisolasi • Terdapat peraturan terhadap makanan, minuman, merokok

Tabel 13.24 Tabel Control Objectives H04

ID Risk	: H04
Kategori	: Hardware
Risiko	: Kerusakan Server
Penyebab	: Jadwal pemadam mati listrik
Control Objective **9.2.2 [Perlindungan Aset terhadap listrik]** Setiap aset harus dilindungi dari gangguan listrik dan gangguan lainnya yang disebabkan oleh kegagalan pada utilitas pendukung	
Implementasi : • Penggunaan UPS • Emergency power off switches diletakkan di dekat emergency door • Penggunaan Genset	

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini merangkum hasil akhir dari pembuatan tugas akhir menjadi sebuah kesimpulan dan dilengkapi dengan saran-saran untuk perbaikan ataupun penelitian lanjutan. Kesimpulan merupakan rangkuman dari hasil analisis dan mitigasi risiko. Sedangkan saran merupakan usulan atau rekomendasi peneliti terhadap hasil tugas akhir untuk perbaikan ataupun penelitian lanjutan

7.1 Kesimpulan

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

1. Dari proses identifikasi risiko yang terdapat pada aset informasi jaringan di ISNet diperoleh 20 Risiko. Hasil penilaian dikategorikan dalam lima level penilaian risiko yaitu *very high, high, medium, low,* dan *very low*.

a. **Satu Risiko** masuk kedalam level ***very high*** yaitu:
   - Risiko **Server Down** dengan nilai **RPN 392**

b. **Tiga Risiko** masuk kedalam level ***high*** yaitu:
   - Risiko **Kerusakan Kabel UTP** dengan nilai **RPN 180**
   - Risiko **Kabel UTP tidak dapat mentrasfer data** dengan nilai **RPN 180**
   - Risiko **Bandwidth habis** dengan nilai **RPN 180**

c. **Satu Risiko** masuk kedalam level *medium* yaitu:
   - Risiko **Tidak memiliki data backup** dengan nilai **RPN 100**

d. **Tiga Belas Risiko** masuk kedalam level ***low*** dengan range nilai **RPN 21-72**
   - Risiko **Kehilangan Kabel UTP** dengan nilai **RPN 72**
   - Risiko **Kerusakan Access Point** dengan nilai **RPN 60**
   - Risiko **Kehilangan Server** dengan nilai **RPN 54**
   - Risiko **Kerusakan Fiber Optik** dengan nilai **RPN 54**
   - Risiko **Kehilangan Converter FO** dengan nilai **RPN 54**
   - Risiko **Kerusakan Converter FO** dengan nilai **RPN 54**
   - Risiko **Kerusakan UPS** dengan nilai **RPN 50**
   - Risiko **Penyebaran Data dan Informasi Rahasia** dengan nilai **RPN 48**
   - Risiko **Penyebaran Data dan Informasi Rahasia** dengan nilai **RPN 42**
   - Risiko **Kerusakan Aset** dengan nilai **RPN 32**
   - Risiko **Kerusakan Switch** dengan nilai **RPN 30**
   - Risiko **Kehilangan Access Point** dengan nilai **RPN 21**
   - Risiko **Kehilangan UPS** dengan nilai **RPN 21**
e. Dan **Dua Risiko** masuk kedalam level ***very low*** yaitu:
   - Risiko **Kerusakan Server** dengan nilai **RPN 18**
   - Risiko **Kehilangan Switch** dengan nilai **RPN 12**

Untuk risiko yang paling tinggi dengan nilai RPN 392 terdapat pada risiko **server down**. Untuk risiko paling rendah dengan RPN 12 terdapat pada risiko **kehilangan switch**

2. Dari 4 opsi mitigasi yaitu *Take , Treat, Transfer & Terminate.* Ditentukan opsi mitigasi yang terkait dengan ancaman yang terdapat pada risiko yang muncul dalam

penelitian ini. Opsi mitigasi yang digunakan yaitu *Take & Treat.*

7.2 Saran

Berdasarkan pelaksanaan penelitian tugas akhir ini , saran yang dapat diberikan agar bisa dijadikan rekomendasi untuk penelitian selanjutnya adalah ISO 27001 dan ISO 27002 memiliki banyak klausul yang bisa dijadikan acuan untuk standar dalam organisasi serta basic yang luas untuk sebuah metode. Tetapi karena keterbatasan ruang lingkup dan batasan masalah serta informasi yang didapat. Penulis hanya perlu menggunakan sebagian dari seluruh klausul yg ada didalam ISO tersebut. Maka untuk penelitian selanjutnya perlu dipertimbangkan organisasi mana yang akan diambil dan metode tambahan yang mengiringi penelitian menggunakan ISO tersebut

7.1 Kesimpulan

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

1. Dari proses identifikasi risiko yang terdapat pada aset informasi jaringan di ISNet diperoleh 20 Risiko. Hasil penilaian dikategorikan dalam lima level penilaian risiko yaitu *very high, high, medium, low,* dan *very low.*

a. **Satu Risiko** masuk kedalam level ***very high*** yaitu:
   - Risiko **Server Down** dengan nilai **RPN 392**

b. **Tiga Risiko** masuk kedalam level ***high*** yaitu:
   - Risiko **Kerusakan Kabel UTP** dengan nilai **RPN 180**
   - Risiko **Kabel UTP tidak dapat mentrasfer data** dengan nilai **RPN 180**
   - Risiko **Bandwidth habis** dengan nilai **RPN 180**

c. **Satu Risiko** masuk kedalam level *medium* yaitu:
   - Risiko **Tidak memiliki data backup** dengan nilai **RPN 100**

d. **Tiga Belas Risiko** masuk kedalam level ***low*** dengan range nilai **RPN 21-72**
   - Risiko **Kehilangan Kabel UTP** dengan nilai **RPN 72**
   - Risiko **Kerusakan Access Point** dengan nilai **RPN 60**
   - Risiko **Kehilangan Server** dengan nilai **RPN 54**
   - Risiko **Kerusakan Fiber Optik** dengan nilai **RPN 54**
   - Risiko **Kehilangan Converter FO** dengan nilai **RPN 54**

- Risiko **Kerusakan Converter FO** dengan nilai **RPN 54**
- Risiko **Kerusakan UPS** dengan nilai **RPN 50**
- Risiko **Penyebaran Data dan Informasi Rahasia** dengan nilai **RPN 48**
- Risiko **Penyebaran Data dan Informasi Rahasia** dengan nilai **RPN 42**
- Risiko **Kerusakan Aset** dengan nilai **RPN 32**
- Risiko **Kerusakan Switch** dengan nilai **RPN 30**
- Risiko **Kehilangan Access Point** dengan nilai **RPN 21**
- Risiko **Kehilangan UPS** dengan nilai **RPN 21**

e. Dan **Dua Risiko** masuk kedalam level ***very low*** yaitu:
- Risiko **Kerusakan Server** dengan nilai **RPN 18**
- Risiko **Kehilangan Switch** dengan nilai **RPN 12**

Untuk risiko yang paling tinggi dengan nilai RPN 392 terdapat pada risiko **server down**. Untuk risiko paling rendah dengan RPN 12 terdapat pada risiko **kehilangan switch**

2. Dari 4 opsi mitigasi yaitu *Take , Treat, Transfer & Terminate*. Ditentukan opsi mitigasi yang terkait dengan ancaman yang terdapat pada risiko yang muncul dalam penelitian ini. Opsi mitigasi yang digunakan yaitu *Take & Treat.*

DAFTAR PUSTAKA

[1] N. A. Widodo and S. M. Adian Fatchur Rochim, "MAKALAH SEMINAR KERJA PRAKTEK :PERANCANGAN AUDIT INTERNAL SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) BERDASARKAN STANDAR ISO/IEC 27001:2005 DI PT. BPR KARYAJATNIKA SADAYA".

[2] N. A. Widodo and A. F. Rochim, "PERANCANGAN AUDIT INTERNAL SISTEM MANAJEMEN KEAMANAN," 2012.

[3] K. N. W and S. Muslihah, Analisis Implementasi Prosedur Standar Pencatatan Aset pada Direktorat Aset UGM, Yogyakarta: Universitas Gadjah Mada, 2015.

[4] V. M. Atmaja, Analisis Pengendalian Kualitas Bagian Finishing dengan Diagram Pareto dan Fsihbone pada CV. Teknika Jaya Batur Ceper Klaten, Surakarta: Universitas Sebelas Maret, 2005.

[5] A. Gui, S. Gondodiyoto and I. Timotius, "Pengukuran Resiko Teknologi Informasi (TI) dengan Metode Octave-S," *Bina Nusantara,* p. 34, 2013.

[6] M. Spremic, "Emerging issues in IT Governance: Implementing the Corporate IT Risk Management Model," in *WSEAS Transaction on Systems*, 2008.

[7] G. Stoneburner, "Risk Management Guide fo Information Technology Systems," 2002.

[8] B. C. H. H. M. A. Innike Desy, "Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effects Analysis di Divisi TI PT. Bank XYZ Surabaya," *Seminar Nasional Sistem Informasi Indonesia,* p. 5, 2014.

[9] A. G. Y. Pratomo, "Perencanaan Proyek Berbasis Risiko Pembangunan Sistem Informasi Manajemen Aset di PDAM Kotamadya Malang Berbasis ISO/FDIS 31000:2009," *Makalah Seminar Nasional Manajemen Teknologi XIV MMT-ITS,* p. 7, 2011.

[10] A. P. S. A. H. Dea Anjani, "Identifikasi, Penilaian dan Mitigasi Risiko Keamanan Informasi pada Sistem Electronic Medical Record (Studi Kasus: Aplikasi Healthy plus Model Rekam Medis di RSU Haji Surabaya)," *Digilib ITS,* p. 4, 2015.

[11] I. Desy, B. C. Hidayanto and H. M. Astuti, "Penilaian Risiko Keamanan Informasi menggunakan Metode Failure Mode and Effects Analysis di Divisi TI PT. Bank XYZ Surabaya," *Seminar Nasional Sistem Informasi Indonesia,* 2014.

[12] ISO, ISO/IEC 27001, Switzerland: ISO, 2005.

[13] Jip, "what is and ISMS?," 14 November 2007. [Online]. Available: http://www.isms.jipdec.jp/en/isms/. [Accessed 2 November 2013].

[14] Tim Direktorat Keamanan Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik," pp. 13-14, 2011.

[15] L. Ulinnuha, B. C. H and B. Setiawan, "Evaluasi Pengelolaan Keamanan Jaringan di Perguruan Tinggi dengan menggunakan Standar Indeks Keamanan Informasi (KAMI) Studi kasus ITS Surabaya," *Jurnal Teknik Pomits,* vol. 1, no. 1, pp. 1-5, 2013.

[16] Diskominfo Bogor, "Penerapan Teknologi Informasi untuk mendukung e-Government Pemerintah kota Bogor," 2013.

[17] Diskominfo , Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik, 2011.

[18] Badan Standardisasi Nasional, Standar Nasional Indonesia, Jakarta : Badan Standardisasi Nasional, 2009.

[19] M. A. Ramadhana, "Pembuatan Perangkat Audit Internal TI berbasis Risiko menggunakan ISO/IEC 27002:2007 pada Proses Pengelolaan Data Studi Kasus Digital Library ITS," 2011.

[20] D. Nurkertamanda and F. T. Wulandari, "Analisa Moda dan Efek Kegagalan (FMEA) pada Produk Kursi Lipat Chitose Yamato HAA," 2009.

[21] F. Kustiyaningsih, Penentuan Prioritas Penanganan Kecelakaan Kerja di PT Ge Lighting Indonesia dengan Metode FMEA, Surakarta: UNS, 2011, pp. 1-73.

[22] Dyadem Press, Guidelines for Failure Mode and Effects Analysis for Automotive, Aerospace, and General Manufacturing Industries, Richmond Hill: CRC Press, 2003.

[23] M. Syafrizal,S.Kom, "Information Security Management System menggunakan Standar ISO/IEC 27001:2005".

LAMPIRAN A
HASIL WAWANCARA

Keterangan Pelaksanaan

Tanggal	10 September 2015
Waktu	15.30 – 17.00 WIB
Tempat	Ruang ISNet Sistem Informasi
Narasumber	Bp. Nanok Adi Saputra
Topik	Evaluasi Keamanan Informasi pada IS-NET di Jurusan Sistem Informasi ITS.

Pembahasan Wawancara

No	Uraian
1	**Pertanyaan :** ISNET itu apa? Bagaimana kondisinya saat ini?
	Jawaban : ISNET merupakan HUB yang terhubung dengan ITSNET, D3, Teknik Industri dan UPT Bahasa yang sangat bergantung pada BTSI yang berada pada lantai 6 Perpustakaan pusat ITS. Selain itu ISNET juga tidak memiliki router sama sekali. ISNET merupakan server dari website Jurusan Sistem Informasi dan aplikasi-aplikasi yang ada di jurusan Sistem Informasi seperi aplikasi perpustakaan, aplikasi keluhan dan aplikasi lainnya. Data yang paling banya ditampung di ISNET adalah data Share-sharean. Selain itu ISNET juga menyimpan server data fingerprint, server SI TV dan server CCTV yang dimiliki Jurusan Sistem Informasi.

	Namun banyaknya data yang tersimpan di dalam ISNET tidak diimbangi dengan keamanan atas data-data tersebut. Keamanan aplikasi yang masih sangat lemah, ditandai dengan kasus pembobolan website Jurusan Sistem Informasi yang terjadi sudah terjadi berulangkali. Keamanan fisik ISNET belum sepenuhnya dipenuhi karena belum adanya aturan-aturan tertulis mengenai siapa saja pihak yang memiliki akses terhadap ruangan ISNET. Selama ini aturan-aturan mengenai hak akses, siapa yang memiliki wewenang untuk memegang kunci ruangan ISNET diatur melalui mulut ke mulut saja, belum ada dokumentasi terhadap peraturan tersebut.
2	**Pertanyaan :** Permasalahan apa yang sering terjadi pada ISNET?
	Jawaban : Berikut ini merupakan permasalahan yang sering terjadi pad ISNET, antara lain sebagai berikut : a. Mati listrik Mati listrik yang terjdi pada Jurusan Sistem Informasi ini disebabkan oleh instalasi listrik jurusan yang tidak tertata dengan baik. Tidak ada perencanaan di awal mengenai pembagian beban listrik, padahal setiap lantai terdapat mcb yang menghubungkan ke masing-masing ruang, dan setiap mcb tersebut memiliki batasan beban yang harus direncanakan sehingga tidak terjadi kelebihan beban seperti yang dialami Jurusan Sistem Informasi saat ini. Jurusan Sistem Informasi tidak memperhitungkan beban ketika memasang AC tambahan, hanya mengambil jaringan listrik dari kabel terdekat, bahkan jaringan listrik untuk server juga dibebani AC dan komputer client. Sehingga Jurusan Sistem Informasi mempunyai rencana untuk menambahkan UPS SI 3000VA.

	Apabila terjadi mati listrik di Jurusan Sistem informasi maka, hanya dapat bertahan selama 1 jam, karena ups yang lama digunakan untuk 10 unit komputer. Sedangkan untuk server hanya dapat bertahan selama 15 menit karena ups digunakan bersama 12 komputer dan AC. Tidak akan menjadi masalah apabila ada pengurus yang stanby untuk mematikan server, yang menjadi masalah adalah karena jumlah pengurus yang terbatas maka ketika mati tidak ada yang mematikan sehingga server mati secara terpaksa. b. Layanan Wifi Layanan wifi yang disediakan kurang aman dikarenakan akses wifi mudah dibobol. Enkripsi pada proxy merupakan enkripsi plain sehingga tingkat keamanannya kurang. c. Virus Masalah virus tidak terlalu menjadi masalah yang berat karena server menggunakan Linux yang cenderung tidak banyak virus. Masalah virus lebih banyak terjadi pada komputer client yang ada di ruangan tata usaha. Virus juga paling mudah menyerang aplikasi SI TV, karena SI TV menggunakan windows.
2	**Pertanyaan :** Bagaimana keamanan jaringan di Sistem Informasi? Apakah sudah ada *hacker* yang berhasil membobol jaringannya?
	Jawaban : Jaringan di Jurusan Sistem Informasi ini masih sangat mudah untuk di bobol. Untuk contoh yang masih sering terjadi adalah akun dari dosen sampai saat ini masih sering digunakan oleh mahasiswa hanya untuk menambah kecepatan internet.
3	**Pertanyaan :**

	Apakah peranan ketua Jurusan Sistem Informasi Ini terkait dengan IS-NET?
	Jawaban : Peranan dari ketua jurusan disini sangat penting, karena ketua jurusan adalah orang yang menentukan arah jurusan ini akan dibawa seperti apa, termasuk terkait dengan SI/TI. Kebijakan SI/TI itu mengikuti arahan dari keetua jurusan. Seberapa perannya untuk keamanan? Sangat besar!
4	**Pertanyaan :** Siapa sajakah *stakeholder* dari IS-NET?
	Jawaban : Di dalam struktur organisasi Jurusan Sistem Informasi, terdapat beberapa koordinator, yaitu koordinator TA, koordinator SDM, koordinator akademik, dan koordinator SI/TI (letaknya dibawah kajur). Untuk koordinator SI/TI saat ini adalah Pak Radityo (sebelumnya adalah Pak Rio). Dibawah Pak Radit ada Pak Nanok yang khusus bertugas menangani IS-NET. Secara tertulis memang hanya ada Pak Radit dan Pak Nanok, tetapi secara tidak struktural, terdapat Pak Bekti, sebagai konsultan SI/TI. Tetapi Pak Nanok juga menangani peralatan sarana pra-sarana (dibawah nya Pak Sony) dan menangani pengadaan (dibawah Pak Bambang Setiawan). Beberapa coordinator bisa mempunyai anak buah yang sama.
5	**Pertanyaan :** Bagaimanakan untuk anggaran TIK di Jurusan Sistem Informasi?
	Jawaban : Untuk anggaran TIK sebenarnya dilihat sesuai dengan kebutuhan. Pada tahun 2012, jaringan di jurusan Sistem Informasi sudah mencapai *Gigabyte*, kemudian di list di tiap-tiap lab membutuhkan apa, baru keluarlah anggaran keuangan. Jadi anggaran ini

	tidak setiap tahun, tetapi disesuaikan dengan kebutuhan. Pada tahun 2012 kemarin anggaran keuangan mencapai 250 juta. Tetapi untuk tahun ini kira-kira membutuhkan sekitar 65 juta. Jadi kalau di rata-rata, Jurusan Sistem Informasi membutuhkan 150 juta – 200 juta/tahun.
6	**Pertanyaan :** Kemudian jika akun dosen sudah berhail di bobol, solusi apa yang dilakukan?
	Jawaban : Masih solusi sederhana, yaitu dosen diminta untuk mengganti passwordnya dan disarankan untuk menggunakan subnet khusus dosen dan karyawan yang ada di lantai 2. Meskipun untuk menggunakannya memang lebih ribet dan membutuhkan waktu yang lama, tetapi subnet khusus dosen dan karyawan tersebut lebih aman.
7	**Pertanyaan :** Apakah sudah ada aturan tertulis yang menjelaskan aturan-aturan yang ada di IS-NET?
	Jawaban : Selama ini masih belum ada aturan tertulis yang menjelaskan siapa saja yang berhak untuk memasuki ruangan server, masih hanya berdasarkan omongan saja. Hak akses nya pun masih berdasarkan siapa yang mempunyai kunci ruangan server saja.
8	**Pertanyaan :** apakah server/computer-komputer yang ada di lab/TU sudah terdapat anti virus yang handal?
	Jawaban : Saat ini, untuk server dan setiap computer yang digunakan sudah terdapat anti virus. Tetapi untuk computer yang masih menggunakan winXP sampai saat ini masih sering terkena virus.
9	**Pertanyaan :**

	Apakah anti virus yang ada sudah ter-*update* dengan baik?
	Jawaban : *Update* sudah dilakukan secara otomatis.
10	**Pertanyaan :** Apakah sistem keamana informasi yang diterapkan di IS-NET sudah bisa dibilang aman?
	Jawaban : Belum, masih belum aman, karena jurusan Sistem Informasi masih belum mempunyai *back-up* server. Sehingga apabila terjadi kerusakan ataupun hal-hal yang tidak diinginkan, jurusan tidak mempunyai *recovery* data.
11	**Pertanyaan :** Bagaimana kesiapan Jurusan Sistem Informasi untuk melakukan audit?
	Jawaban : Jurusan Sistem Informasi masih belum siap untuk melakukan audit, karena tata kelola nya masih belum berjalan dengan baik, hanya beberapa sisi saja yang sudah berjalan. Jadi kalau dilaukan audit saat ini, maka nilainya akan sangat jelek.
12	**Pertanyaan :** Apakah dilakukan monitoring jika terjadi perubahan-perubahan?
	Jawaban : Seharusnya dengan menggunakan proxy, sudah berfungsi sebagai monitor kegiatan yang ada di dalamnya, apa yang di akses dan siapa yang meng-akses sudah terekam didalamnya. Tetapi dari informasi yang saya dengar, karena banyaknya data dan kurangnya staf di ITS, akhirnya hal tersebut jadi tidak termonitor. Proxy mahasiswa sebenarnya sudah ada *record* nya. Untuk perubahan jaringan dan hardware masih belum ada.
13	**Pertanyaan :**

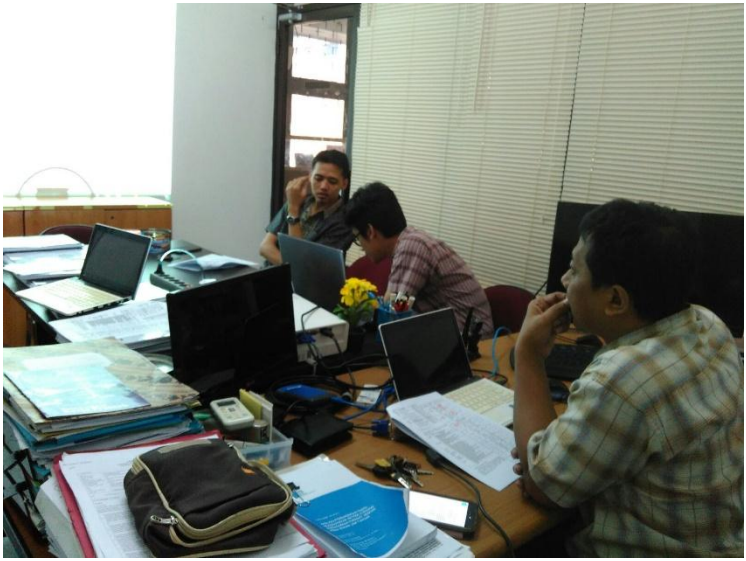
	Apakah ancaman dan kelemahan yang terkait dengan asset informasi, terutama untuk setiap asset utama sudah teridentifikasi?
	Jawaban : Kalau untuk saya pribadi, sudah ada. Jadi ketika akses point mati, ada server yang mati, saya bisa langsung mengetahui. Itu ada aplikasinya. Jadi ada alat untuk melakukan monitoring untuk mendeteksi kesalahan jaringan. Tapi kalau untuk mendeteksi kekurangan, itu mash belum ada. Kalau untuk jaringan, bisa *connect* ataupun tidak, bisa menggunakan *ping*. Kalau saya *ping* dan berhasil, berarti tidak ada masalah.
14	**Pertanyaan :** Apakah dilakukan *back-up* secara rutin? Bagaimana dengan prosedurnya?
	Jawaban : *Back-up* nya masih belum rutin, kalau untuk prosedur, kalau dulu, sebelum e-learning dipindah ke **share.its.ac.id**, kita melakukan *bak-up* setiap 6 bulan sekali, di akhir semester. Baru setelah itu kita membuat mata kuliah baru.
15	**Pertanyaan :** Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?
	Jawaban : Ketika akan melakukan migrasi ke teknologi terbaru, harus dilakukan pembelajaran ulang untuk user-user yang menggunakan. Jadi hal ini tidak dilakukan, karena selama teknologi tersebut masih bisa digunakan dan masih mampu untuk menjalankan proses bisnisnya, jadi tidak diganti.

16	**Pertanyaan :** Kemudian jika akun dosen sudah berhail di bobol, solusi apa yang dilakukan?
	Jawaban : Masih solusi sederhana, yaitu dosen diminta untuk mengganti passwordnya dan disarankan untuk menggunakan subnet khusus dosen dan karyawan yang ada di lantai 2. Meskipun untuk menggunakannya memang lebih ribet dan membutuhkan waktu yang lama, tetapi subnet khusus dosen dan karyawan tersebut lebih aman.
17	**Pertanyaan :** Apakah sudah ada aturan tertulis yang menjelaskan aturan-aturan yang ada di IS-NET?
	Jawaban : Selama ini masih belum ada aturan tertulis yang menjelaskan siapa saja yang berhak untuk memasuki ruangan server, masih hanya berdasarkan omongan saja. Hak akses nya pun masih berdasarkan siapa yang mempunyai kunci ruangan server saja.
18	**Pertanyaan :** apakah server/computer-komputer yang ada di lab/TU sudah terdapat anti virus yang handal?
	Jawaban : Saat ini, untuk server dan setiap computer yang digunakan sudah terdapat anti virus. Tetapi untuk computer yang masih menggunakan winXP sampai saat ini masih sering terkena virus.
19	**Pertanyaan :** Apakah anti virus yang ada sudah ter-*update* dengan baik?
	Jawaban : *Update* sudah dilakukan secara otomatis.
20	**Pertanyaan :** Apakah sistem keamana informasi yang diterapkan di IS-NET sudah bisa dibilang aman?
	Jawaban :

	Belum, masih belum aman, karena jurusan Sistem Informasi masih belum mempunyai *back-up* server. Sehingga apabila terjadi kerusakan ataupun hal-hal yang tidak diinginkan, jurusan tidak mempunyai *recovery* data.
21	**Pertanyaan :** Bagaimana kesiapan Jurusan Sistem Informasi untuk melakukan audit?
	Jawaban : Jurusan Sistem Informasi masih belum siap untuk melakukan audit, karena tata kelola nya masih belum berjalan dengan baik, hanya beberapa sisi saja yang sudah berjalan. Jadi kalau dilaukan audit saat ini, maka nilainya akan sangat jelek.
22	**Pertanyaan :** Apakah dilakukan monitoring jika terjadi perubahan-perubahan?
	Jawaban : Seharusnya dengan menggunakan proxy, sudah berfungsi sebagai monitor kegiatan yang ada di dalamnya, apa yang di akses dan siapa yang meng-akses sudah terekam didalamnya. Tetapi dari informasi yang saya dengar, karena banyaknya data dan kurangnya staf di ITS, akhirnya hal tersebut jadi tidak termonitor. Proxy mahasiswa sebenarnya sudah ada *record* nya. Untuk perubahan jaringan dan hardware masih belum ada.
23	**Pertanyaan :** Apakah ancaman dan kelemahan yang terkait dengan asset informasi, terutama untuk setiap asset utama sudah teridentifikasi?
	Jawaban : Kalau untuk saya pribadi, sudah ada. Jadi ketika akses point mati, ada server yang mati, saya bisa langsung mengetahui. Itu ada aplikasinya. Jadi ada alat untuk melakukan monitoring untuk mendeteksi kesalahan

	jaringan. Tapi kalau untuk mendeteksi kekurangan, itu mash belum ada. Kalau untuk jaringan, bisa *connect* ataupun tidak, bisa menggunakan *ping*. Kalau saya *ping* dan berhasil, berarti tidak ada masalah.
24	**Pertanyaan :** Apakah dilakukan *back-up* secara rutin? Bagaimana dengan prosedurnya?
	Jawaban : *Back-up* nya masih belum rutin, kalau untuk prosedur, kalau dulu, sebelum e-learning dipindah ke **share.its.ac.id**, kita melakukan *bak-up* setiap 6 bulan sekali, di akhir semester. Baru setelah itu kita membuat mata kuliah baru.
25	**Pertanyaan :** Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?
	Jawaban : Ketika akan melakukan migrasi ke teknologi terbaru, harus dilakukan pembelajaran ulang untuk user-user yang menggunakan. Jadi hal ini tidak dilakukan, karena selama teknologi tersebut masih bisa digunakan dan masih mampu untuk menjalankan proses bisnisnya, jadi tidak diganti.

LAMPIRAN B
DOKUMENTASI PROSES VALIDASI



BIODATA PENULIS

Penulis memiliki nama lengkap Krisna Harinda Dewantara. Penulis merupakan anak kedua dari dua bersaudara. Penulis telah menempuh pendidikan formal yaitu di TK Yaabunayya, SD Muhammadiyah 4 Pucang Surabaya, SMP Negeri 19 Surabaya, SMA Negeri 2 Surabaya. Setelah lulus dari SMA pada tahun 2011, penulis diterima di Jurusan Sistem Informasi ITS Surabaya pada tahun 2011 dan terdaftar dengan NRP 5211100148.

Selama menjadi mahasiswa penulis aktif dalam kepengurusan Himpunan Mahasiswa Sistem Informasi FTIF ITS Surabaya periode 2012/2013-2013/2014. Penulis juga mengikuti kegiatan pelatihan LKMM Pra TD. Penulis juga pernah menjadi ketua panitia Studi Ekskursi pada tahun 2014. Penulis memiliki hobi berenang dan bersepeda.

Untuk kepentingan penelitian, penulis dapat dihubungi melalui email krisnaharinda@gmail.com