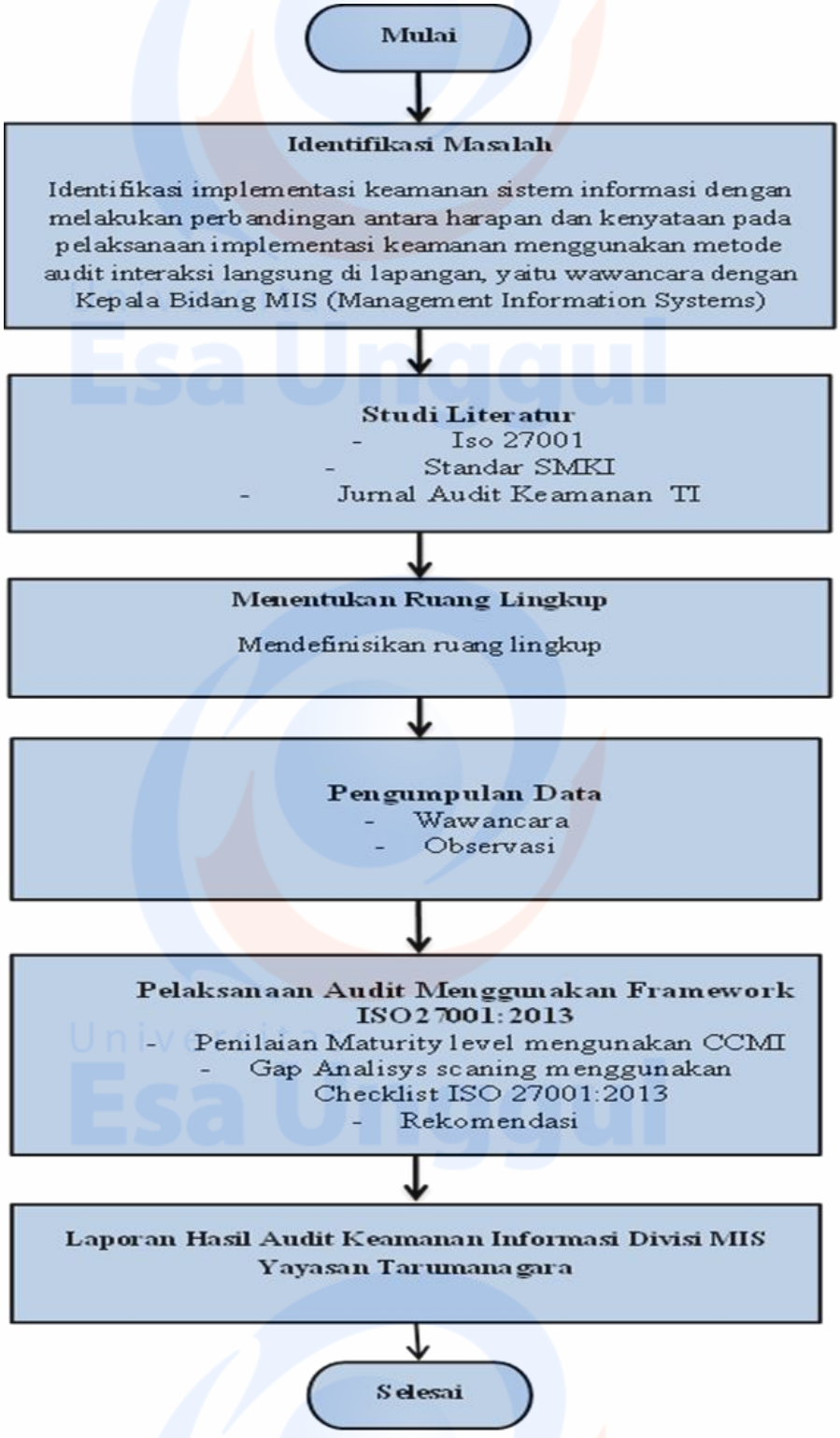



**Gambar 1-1 Kerangka Pemikiran**

5. *Identification* (Identifikasi)

   Adalah prinsip yang menjamin bahwa informasi memiliki karakteristik identifikasi ketika informasi dapat mengenali penggunanya. Identifikasi adalah langkah pertama dalam memperoleh akses ke informasi yang diamankan, dan berfungsi sebagai dasar untuk otentifikasi dan otorisasi.

6. *Authentification* (Otentifikasi)

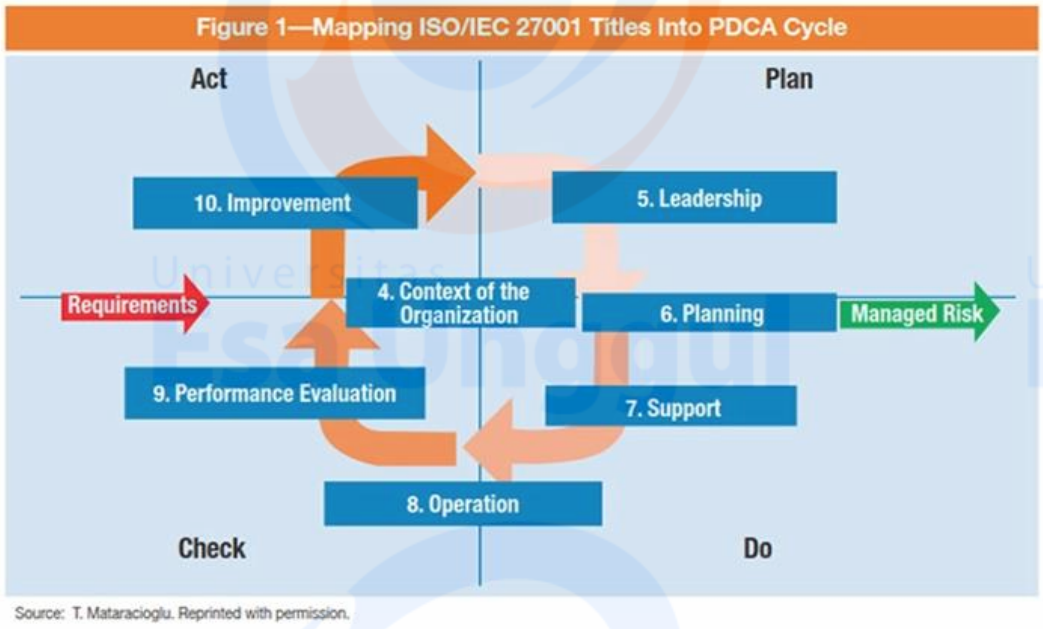
   Adalah suatu prinsip yang menjamin bahwa saat otentifikasi terjadi ketika sistem dapat membuktikan bahwa pengguna memiliki hak klaim.

7. *Authorization* (Otorisasi)

   Adalah prinsip yang menjamin bahwa pengguna telah mendapatkan otorisasi sehingga dapat mengakses, meng-update atau penghapus informasi.

8. *Accountability* (Akuntabilitas)

   Adalah prinsip informasi yang dikatakan eksis ketika sistem dapat menyajikan semua aktifitas terhadap informasi dan siapa yang melakukan aktifitas itu (Whitman & Mattord, 2011)




**Gambar 2-1 Siklus PDCA ISO/IEC 27001:2013**

ISO 27001:2013 terdiri atas 10 klausal manajemen dan 114 kontrol yang harus diterapkan berdasarkan Analisis resiko keamanan informasi. Klausal tersebut antara lain:

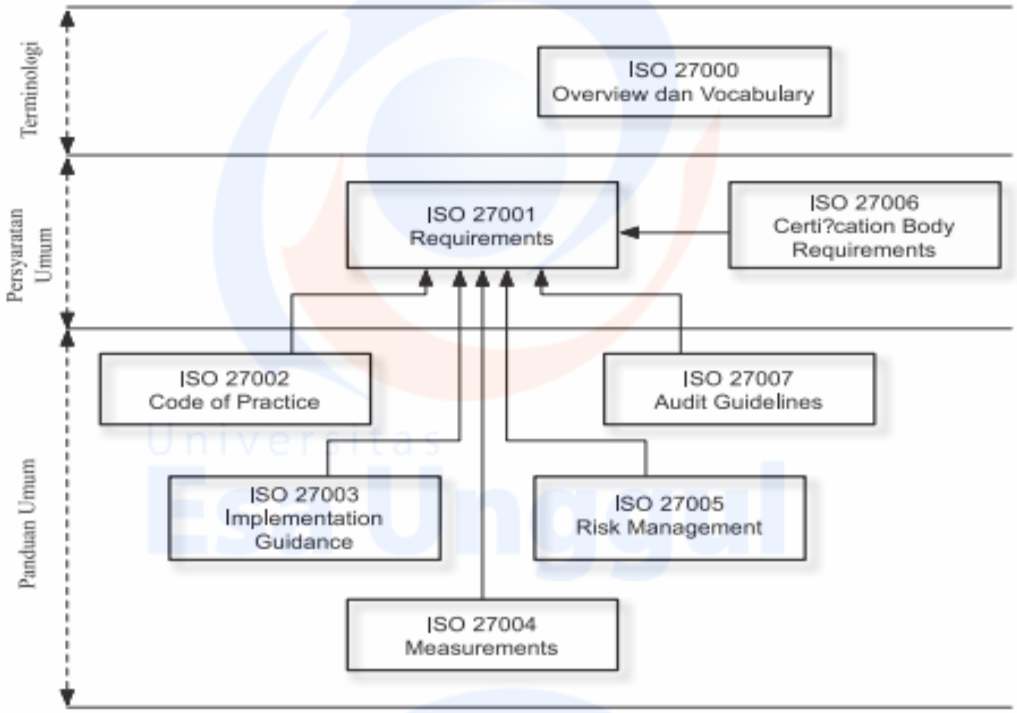
4. ISO/IEC 27003:2010 – *ISMS Implementation Guidance*
5. ISO/IEC 27004:2009 – *ISMS Measurements*
6. ISO/IEC 27005:2008 – *Information Security Risk Management*

Catatan: angka di belakang standar seri ISO 27000 menunjukkan tahun terbit.

## 2.6 *ISO/IEC 27001 ISMS –Overview and Vocabulary*

Standar yang sudah mengalami revisi hingga edisi tahun 2014, memuat prinsip-prinsip dasar *Information Security Management System* (Sistem Manajemen Keamanan Informasi – SMKI), definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga SMKI, baik yang telah diterbitkan maupun sedang dalam tahap pengembangan.

Hubungan antar standar keluarga ISO 27000 dapat digambarkan sebagai berikut :




**Gambar 2-2 Hubungan Antar Standar Keluarga ISO 27000**

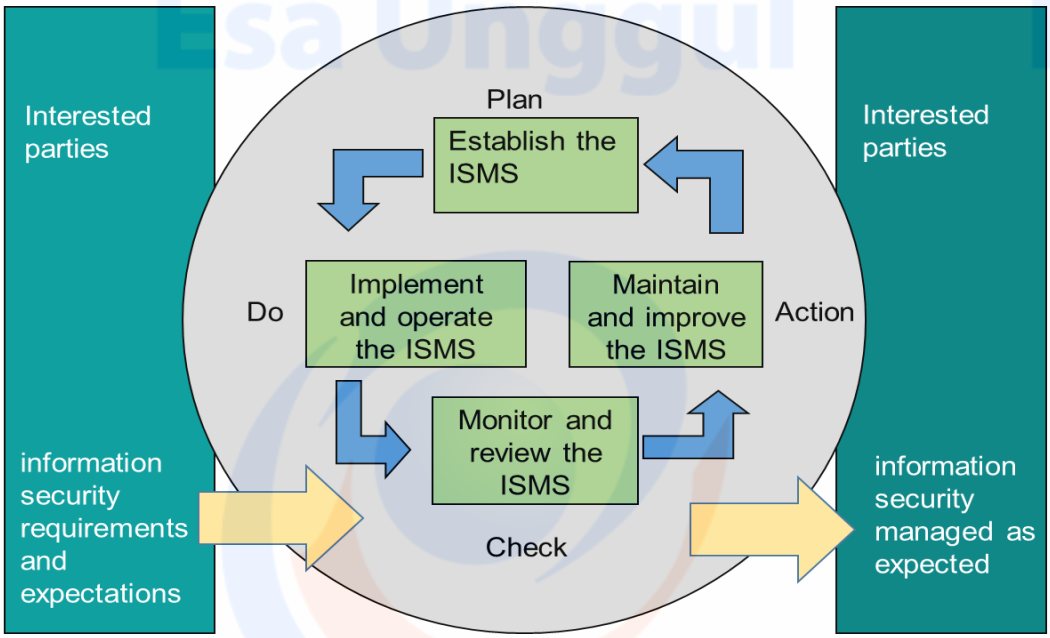
## 2.7 ISO/IEC 27001-Persyaratan Sistem Manajemen Keamanan Informasi

ISO/IEC 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis resiko, dan dirancang untuk

sistem manajemen keamanan informasi (SMKI). Standar ini utamanya dimaksudkan untuk mendukung proses akreditasi Badan Sertifikasi ISO/IEC 27001 oleh Komite Akreditasi dari negara masing-masing

## 2.13 *Proses Of Information Security Management Systems*

Proses *information security management system* menggunakan prinsip *Plan-Do-Check-Act*. Berikut adalah tahapan-tahapan PDCA :




**Gambar 2-3 Poses ISMS**

***Plan (Establish The ISMS)***

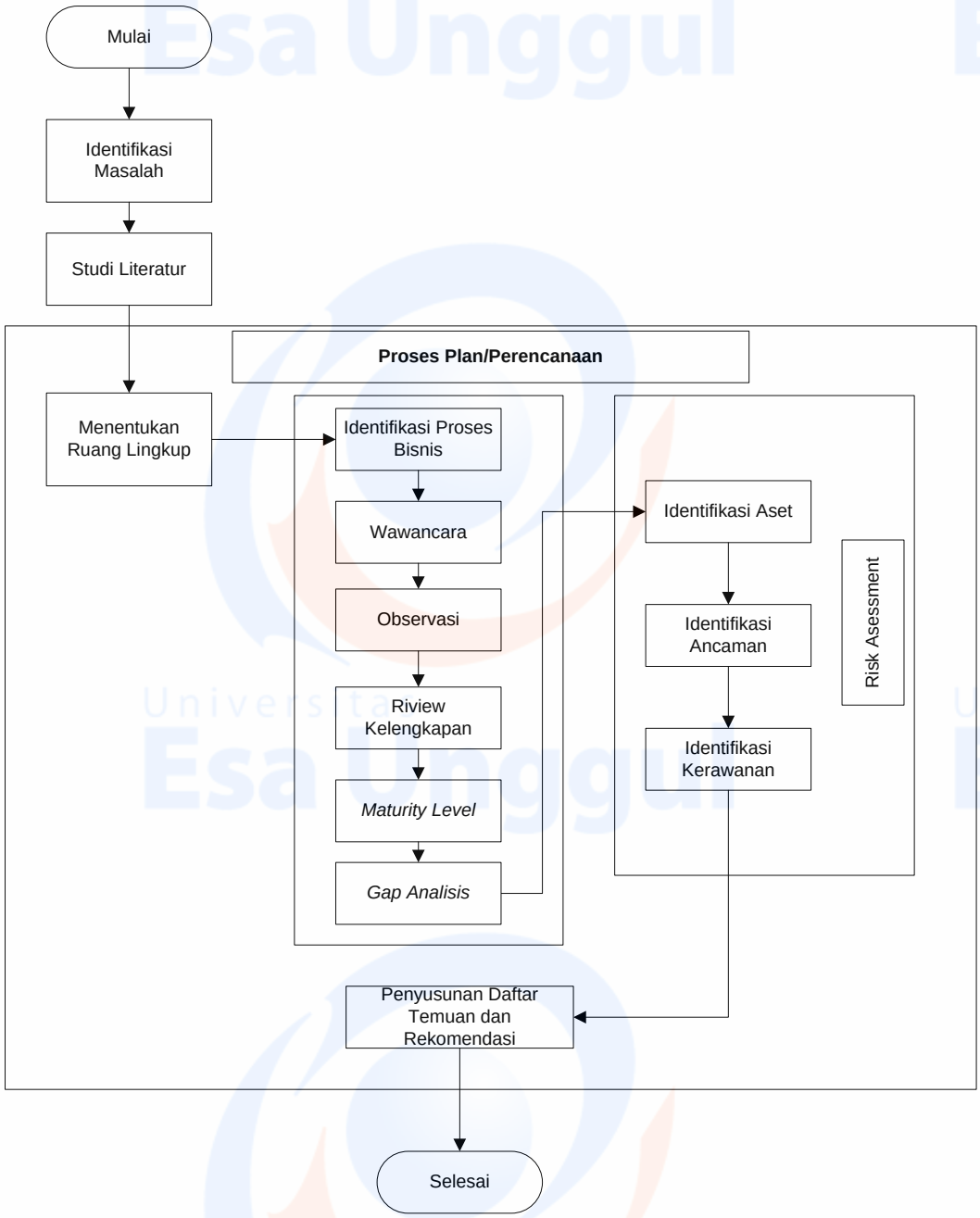
Langkah-langkah dalam mengerjakan *plan* adalah

1. Menentukan ruang lingkup
2. Melakukan *(gap)* Analisis
3. Melakukan *risk assessment*
   a. Mengidentifikasi aset
   b. Mengidentifikasi kerawanan dan ancaman
   c. Menentukan Prioritas Resiko
   d. Mengembangkan Kontrol
   e. Monitoring
4. Menetapkan kontrol
5. Membuat kebijakan dan prosedur Langkah tidak tertulis adalah *statement of applicability (SOA)*

# BAB 3
# METODE PENELITIAN

## 3.1 Rencana Penelitian

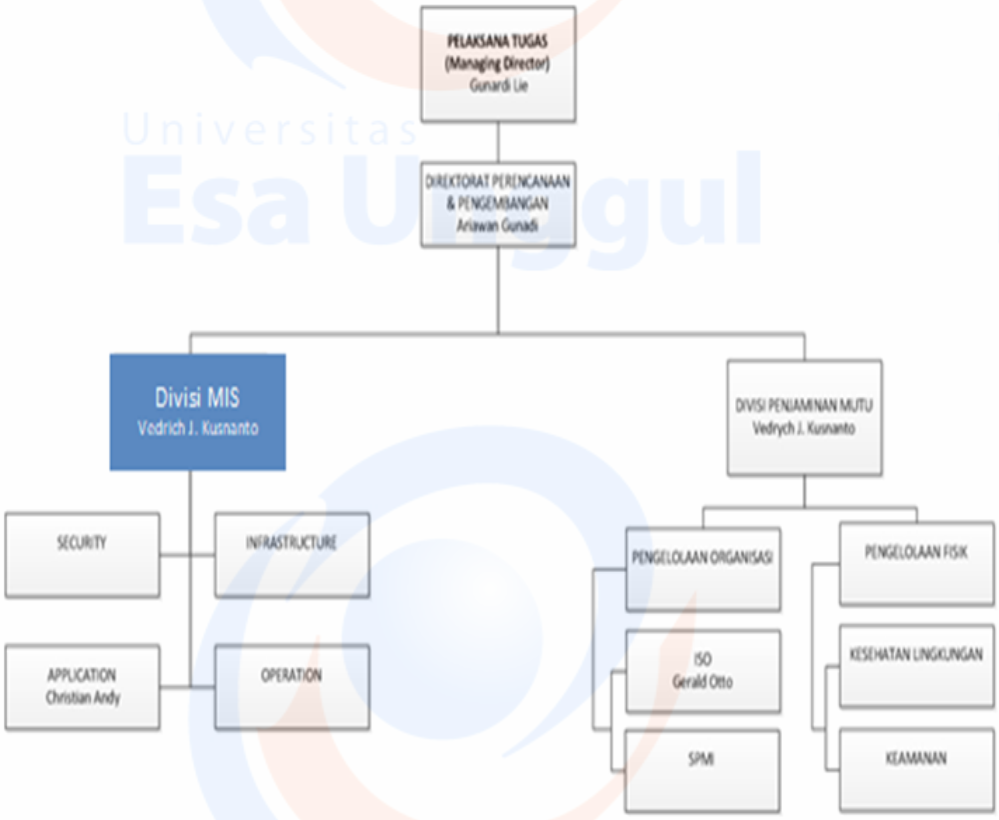
Pada Bab ini akan dilakukan pembahasan mengenai metode audit keamanan informasi menggunakan standar ISO 27001:2013 yang akan dijelaskan pada gambar 3-1.




**Gambar 3-1 Tahap Penelitian**

### 4.1.3 Struktur Organisasi

Struktur Organisasi Divisi *Management Information Systems*



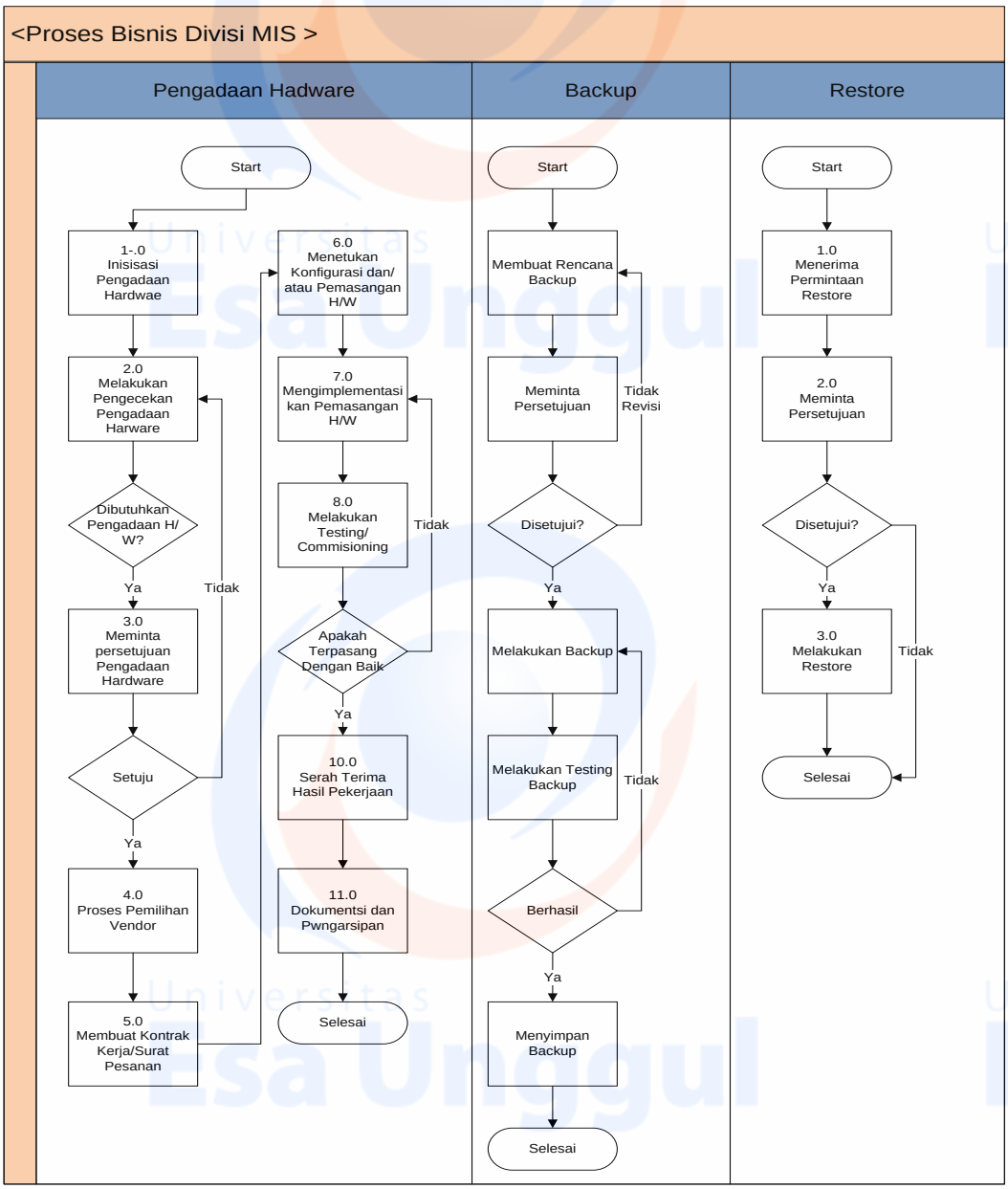

**Gambar 4-1 Struktur Organisasi**

### 4.1.4 Gambaran Umum Divisi MIS Yayasan Tarumanagara

*MIS (Management Information Systems)* merupakan Divisi penyelenggara kegiatan IT atau pengelola semua aktivitas IT di lingkungan Yayasan Tarumanagara dan bertanggung jawab atas keamanan sistem informasi yang ada. Selain sebagai penyelenggara dan pengelolaan keamanan informasi Divisi MIS juga mempunyai beberapa kewenangan tugas seperti Penyusunan *IT Plan*, Pengadaan Lisensi IT, Pengadaan *Hardware*, *Backup Data*, Pengelolaan *Help Desk IT*, pengadaan *Maintenance IT* dan lain-lain.

*Divisi MIS* dipimpin seorang kepala Divisi dan satu orang staf yang mempunyai *job desk* dan tanggung jawab masing-masing.

### 4.1.5 Prosedur Kerja Divisi MIS




**Gambar 4-2 Proses Bisnis Divisi MIS**

Prosedur Kerja (PK) Pengadaan *Hardware*

1. Inisiasi pengadaan H/W dilakukan melalui *project charter*, *IT Plan*, dan/atau permintaan penggantian/penambahan H/W oleh *user*
2. Apabila permintaan berasal dari *user*, maka Staf MIS melakukan pengecekan kebutuhan ke *user* yang bersangkutan. Termasuk memberikan rekomendasi spesifikasi, perkiraan harga, dan pengecekan apakah barang yang dibeli support dengan yang sudah ada (bila diperlukan). Apabila penggantian H/W diperlukan, maka proses

ENGAGEMENT LETTER

AUDIT KEAMANAN INFORMASI PADA DIVISI MIS YAYASAN TARUMANAGARA
MENGGUNAKAN STANDAR ISO/IEC 27001:2013

Yang bertanda tangan dibawah ini :

Nama : Vedrich J. Kusnanto.,S.Kom.,MM
Jabatan : Kepala Divisi Management Information Systems (MIS) Yayasan Tarumanagara

Bertindak selaku kepala Divisi Management Information System (MIS) Yayasan Tarumanagara menugaskan dan memberi wewenang melakukan audit kepada :

Nama : Arno Setiawan
NIM : 201583058
Prodi : Sistem Informasi
Fakultas : Ilmu Komputer - Universitas Esa Unggul Jakarta

Yang melaksanakan audit keamanan sistem informasi, bertindak sebagai auditor.

Tujuan :
Melakukan audit sesuai dengan kesepakatan dan klausul-klausul yang telah ditentukan, tujuan dilakukan audit untuk mengevaluasi dan mengetahui seberapa tingkat keamanan informasi yang dilakukan Divisi MIS sesuai dengan standar ISO 27001:2013 guna peningkatan pengelolaan keamanan informasi di Yayasan Tarumanagara.

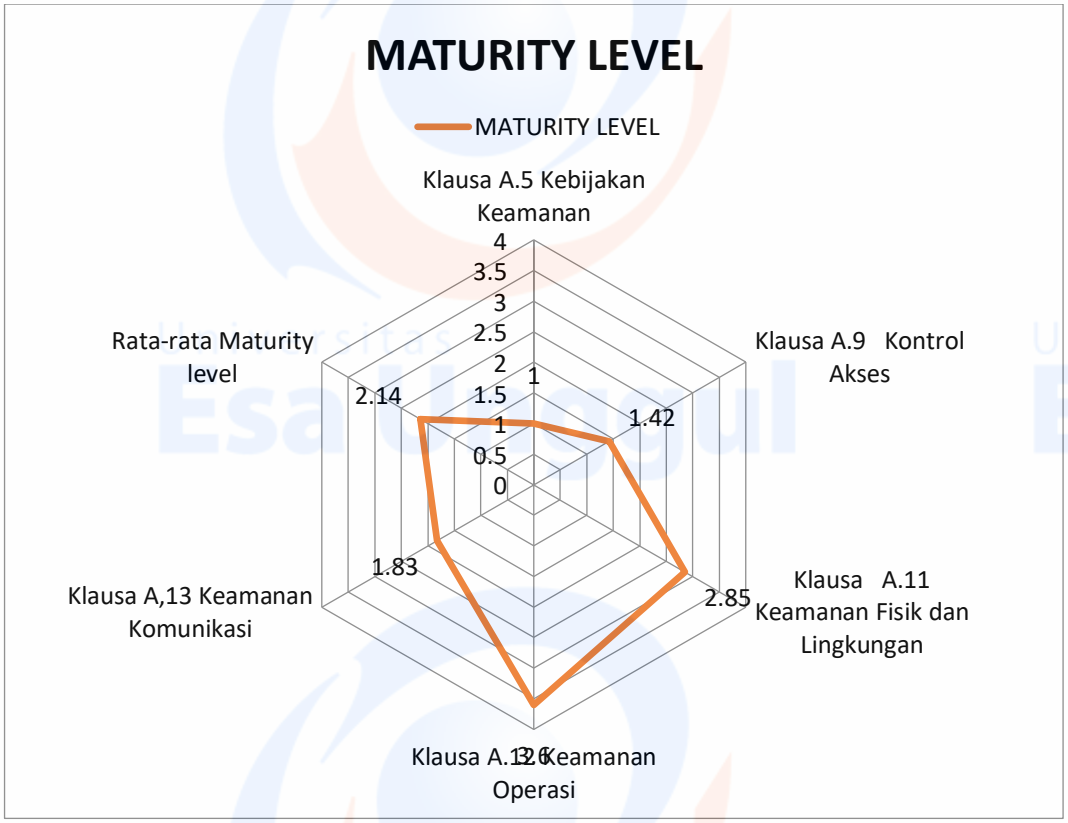
**Gambar 4-3 Engagement Letter**

### 4.3.1 Menentukan Tujauan, Ruang Lingkup

Tujuan Audit Keaman Informasi Divisi MIS Yayasan Tarumanagara. Tujuan dilakukannya audit keamanan informasi pada Divisi MIS Yayasan Tarumanagara adalah untuk mengukur tingkat keamanan informasi yang ada dan *gap* yang terjadi, sehingga dapat menentukan apakah Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan sudah sesuai dengan yang diharapkan. Berdasarkan permasalahan yang ada berkaitan dengan aspek keamanan informasi *Confidentiality, Integrity, dan Availability (CIA).*

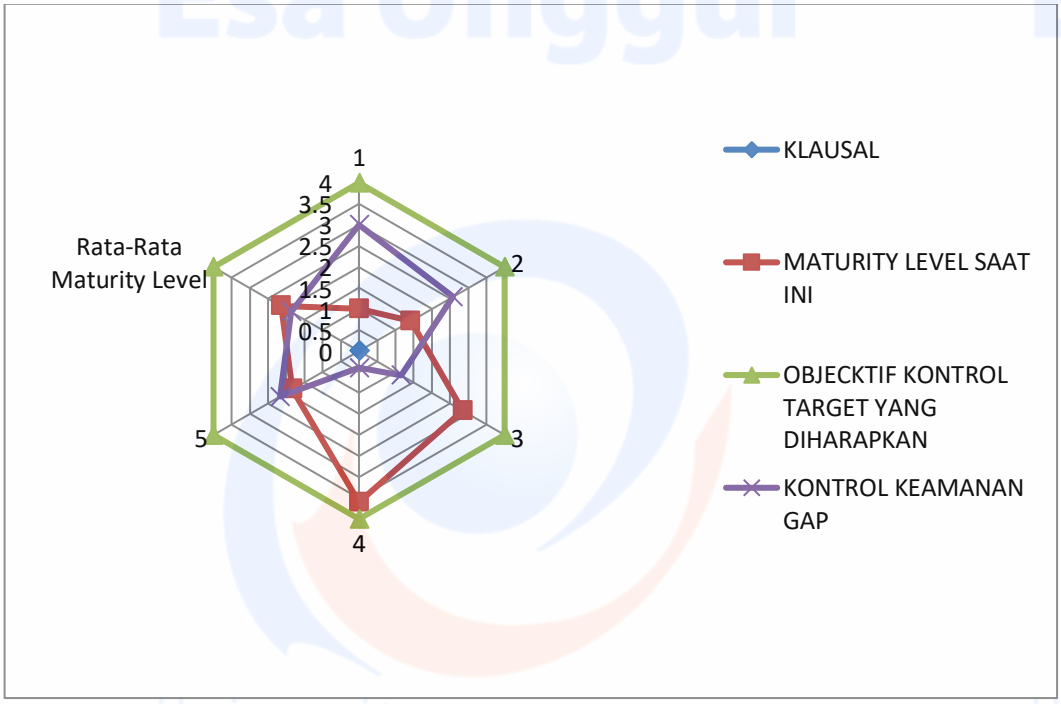
d. Klausal A.12 Keamanan Komunikasi dengan nilai kematangan 3.6 (ditetapkan/*Defined process*) proses telah di dokumentasikan dan dikomunikasikan, prosedur telah disetandarisasi. Proses berada dalam keadaan diamanatkan.
e. Klausal A.13 Keamanan Komunikasi dengan nilai kematangan 1.83 *(repeatable but intuitive)* proses mengikuti pola yang teratur dimana prosedur diikuti pegawai/karyawan lain tetapi tidak ada peraturan formal yang digunakan sebagai acuan.

Jadi nilai rata-rata yang didapat dari seluruh klausal yaitu 2.14 yang artinya tingkat kematangan pengelolaan keamanan informasi pada Divisi MIS *Repeatable but Intuitive* perusahaan telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola tata kelola TI dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen formal.




**Gambar 4-4 Hasil Penilaian *Maturity* Seluruh Klausal**

| No | Klausal | *Maturity level* saat ini | Objektif Kontrol | Kontrol Keamanan |
|---|---|---|---|---|
| | | | Target yang diharapkan | *Gap* |
| 5 | Klausa A,13 Keamanan Komunikasi | 1.83 | 4 | 2.17 |
| **Rata-Rata *Maturity level*** | | **2.14** | **4** | **1.86** |




**Gambar 4-5 Spider Chart Hasil Penilaian Gap**

### 4.5.6 Rekomendasi Hasil Audit

Rekomendasi hasil audit berdasarkan data dan bukti, yang diperoleh dari penghitungan *maturity* dan *(gap)* serta usaha untuk mendapatkan tingkat kematangan yang diharapkan yaitu pada level 4 *(Managed and Measurable)* adalah :

1. Perbaikan pada kebijakan tata kelala TI sebagai payung pelaksanaan pengelolaan keamanan
2. Dibuat kebijakan secara tertulis/terdokumentasi
3. Update berkala untuk sistem yang telah habis masa berlaku (*software* maupun *hardware)*