BAB 1
PENDAHULUAN

1.1 Latar Belakang

Yayasan Tarumanagara sebagai institusi yang bergerak di bidang pendidikan, kesehatan, dan kesejahteraan merupakan *holding* dari Universitas Tarumanagara dan Rumah Sakit Royal Taruma serta beberapa anak perusahaan seperti PT. Taruma Bhakti Usaha dan PT. Taruma Bhakti Medika, telah menerapkan tata kelola teknologi informasi hampir seluruh divisi yang ada sebagai pendukung proses bisnisnya. MIS *(Management Information Systems)* sebagai Divisi penyelenggara IT atau pengelola semua aktivitas IT di lingkungan Yayasan Tarumanagara bertanggung jawab atas keamanan sistem informasi yang dilaksanakan. Dalam perjalanan mengelola teknologi informasi ada beberapa kendala dari segi keamanan teknologi informasi seperti masih adanya celah atau kelemahan dari sisi keamanan jaringan dengan ditemukannya aktifitas mencurigakan di dalam jaringan atau sistem dengan *intrusion name backdoor doublepulsar, necrus bootnet dan malware* yang terdeteksi yaitu W32/Generic.AP.128842 dengan kejadian sebanyak 64 kali, Android/Generic.Z.8F370A dengan kejadian 59 kali dalam 1 bulan. Kurangnya kontrol/limitasi terhadap penggunaaan *bandwith* sehingga *user* secara bebas mengakses aplikasi yang memakan *bandwith* besar seperi *youtube* dengan kuota pemakaian mencapai 377 GB, *Google.Services* mencapai 281 GB per bulan yang mengakibatkan akses yang lambat. Tidak ada perpanjangan lisensi atau *upgrade hardware* maupun *software* yang masa *lifetime*nya sudah habis. Adanya persyaratan *sharing password* untuk aplikasi keuangan yang memungkinkan terjadinya pencurian data oleh pemegang akses. Pelaksanaan kebijakan manajemen yang belum maksimal seperti *policy* tentang pembatasan akses dan penggunaan jaringan serta kelemahan lain yang ada di lingkungan Yayasan Tarumanagara seperti keamanan fisik ruang server yang sesuai dengan standar dan tidak adanya atorisasi akses masuk ke ruang server.

Selama ini Yayasan Tarumanagara belum pernah melakukan audit keamanan sistem informasi di lingkungan organisasi baik oleh audit *internal*

maupun *eksternal* sehingga tidak mengetahui sampai dimana tingkat keamanan informasi yang dimilikinya.

Penerapan tata kelola teknologi informasi *(IT Governace)* yang baik menjadi hal penting bagi organisasi atau perusahaan dalam menjalankan operasional bisnisnya. Untuk memperoleh value (nilai) sebuah bisnis. informasi harus akurat, tepat waktu, dan mudah diakses bagi siapapun yang membutuhkannya dalam konteks aktifitas bisnis yang mereka lakukan (Munawar, 2017). Dengan tata kelola yang baik, maka sistem informasi yang *accountable* serta *sustainable* dapat tercapai, sehingga organisasi tersebut harus menyadari dan menerapkan suatu kebijakan yang tepat untuk melindungi aset informasi yang dimiliki. Salah satu kebijakan yang dapat diambil oleh organisasi untuk mengatasi gangguan keamanan informasi adalah dengan menerapkan manajemen keamanan sistem informasi. Penggunaan standar keamanan dan pelayanan dalam memandu jalannya proses bisnis dapat menjadi salah satu solusi dalam meminimalisir terjadinya gangguan yang tidak diinginkan.

Untuk mengevaluasi hal tersebut maka perlu dilakukan audit keamanan sistem informasi. Salah satu standar yang sering digunakan dalam audit kemanan sistem informasi adalah ISO 27001:2013. ISO 27001 merupakan suatu standar Internasional dalam menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan *Information Security Management Sistems (ISMS)* sebagai acuan mengenai apa saja yang seharusnya diimplementasikan dalam tata kelola kemanan informasi di dalam sebuah perusahaan.

Audit keamanan informasi di Divisi *Management Information Systems* (MIS) Yayasan Tarumanagara di lakukan agar *implementasi* teknologi informasi yang sudah berjalan dapat dijalakan dengan benar dan di *deliver* secara tepat sesuai dengan rencana strategis *(IT strategic)* yang telah dibuat.

Berdasarkan uraian diatas, penulis membuat Tugas Akhir dengan tema Audit Keamanan Informasi dengan judul "Audit Keamanan Informasi Pada Divisi MIS *(Management Information Systems)* Yayasan Tarumanagara Menggunakan Standar ISO/IEC 27001:2013". Dengan dilakukannya penelitian ini tentunya diharapkan dapat memberikan masukan dan rekomendasi terhadap peningkatan pengelolaan keamanan informasi yang dilakukan oleh Divisi MIS *(Management Information Systems)* Yayasan Tarumanagara Jakarta.

1.2 Identifikasi Masalah

1. Bagaimana evaluasi keamanan informasi pada Divisi MIS *(Management Information Systems)* Yayasan Tarumanagara dalam kerangka ISO/IEC 27001?
2. Bagaimana *(gap)* antara kebijakan, prosedur, sistem, dan persyaratan pengelolaan keamanan informasi Yayasan Tarumanagara saat ini apakah sudah sesuai dengan standar ISO/IEC 27001?
3. Bagaimana tingkat kematangan *(maturity level)*, tingkat kesenjangan *(gap analisys)* pada penerapan sistem keamanan informasi informasi Yayasan Tarumanagara berdasarkan CMMI *(Capability Maturity Model Integration)* Cobit.

1.3 Tujuan Tugas Akhir

1. Mengetahui praktik keamanan informasi di yang dilaksanakan oleh Divisi MIS Yayasan Tarumanagara, Jakarta.
2. Menilai sejauh mana kepatuhan mereka terhadap persyaratan keamanan informasi yang dijalankan.
3. Mengukur kesenjangan antara praktek keamanan informasi di perusahaan tersebut dan tingkat yang ingin dicapai sesuai dengan persyaratan ISO/IEC 27001:2013 dan memberikan rekomendasi yang diperlukan untuk meningkatkan kepatuhan terhadap standar, mengurangi kesenjangan dan meningkatkan praktek keamanan informasi.standar ISO/IEC 27001?

1.4 Manfaat Tugas Akhir

1. Memberikan gambaran mengenai kondisi pengelolaan keamanan informasi di Divisi MIS khususnya dan Yayasan Tarumanagara secara keseluruhan sebagai bahan referensi untuk memastikan bahwa kemanan sistem informasi dapat berjalan dengan baik.
2. Memberi masukan berupa kebijakan, prosedur atau Kontrol yang perlu diterapkan untuk meningkatkan pengelolaan keamanan informasi.
3. Menjadi langkah awal persiapan sertifikasi ISO 27001:2013.

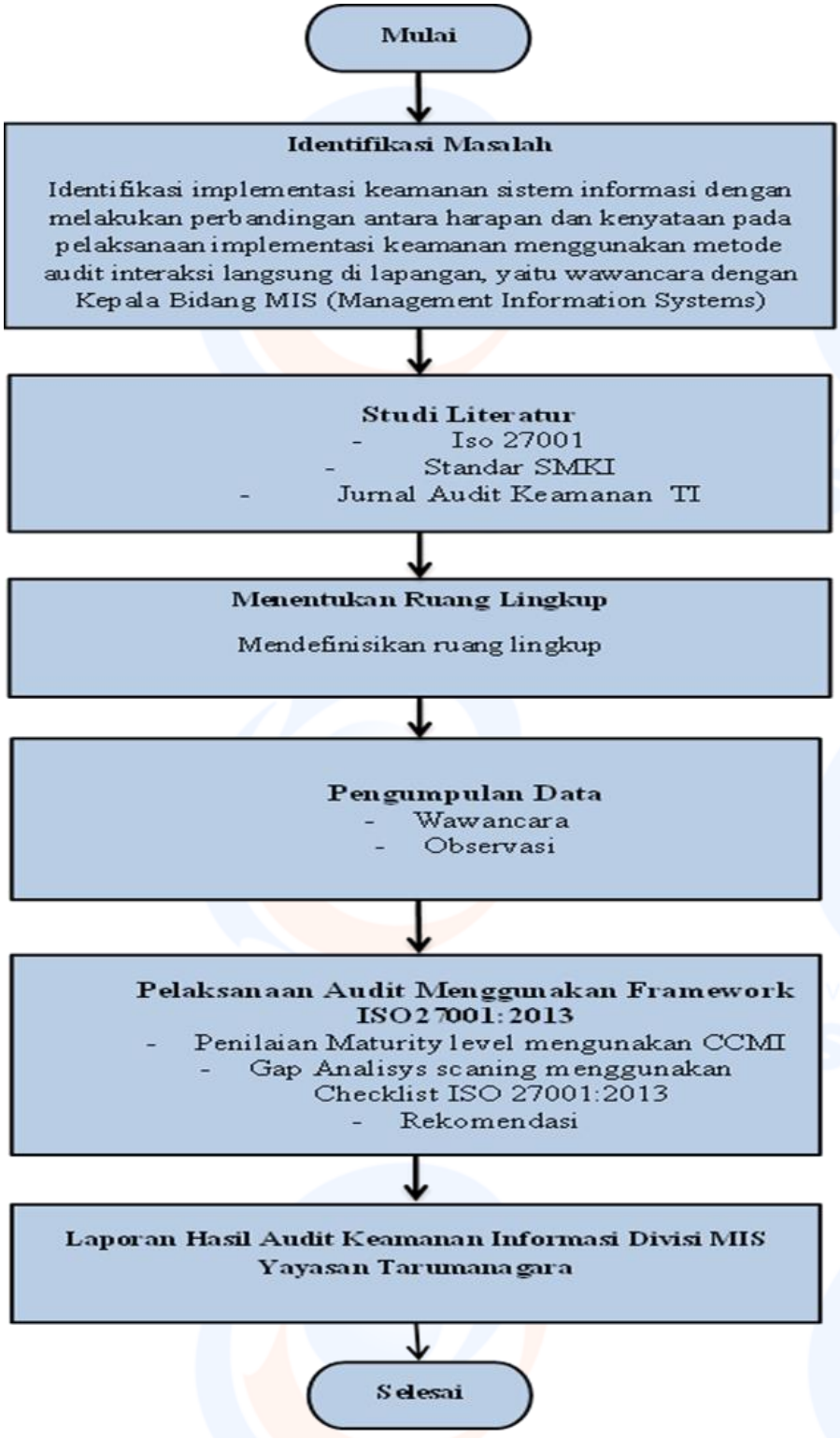
1.5 Lingkup Tugas Akhir

Dalam penulisan tugas akhir peneliti akan menentukan ruang lingkup penelitian agar lebih terfokus, yaitu:

1. Sistem keamanan yang dijalankan pada Divisi *Management Information Systems (MIS)* Yayasan Tarumanagara jakarta mengacu standar ISO 27001:2013
2. Penghitungan *maturity* dan *gap analisys* serta rekomendasi sebagai peningkatan pengelolaan keamanan informasi.
3. Penelitian berfokus pada 5 klausal yaitu Klausal A. 5 Kebijakan Keamanan Informasi, Klausal A. 9 Kontrol akses, Klausal A. 11 keamanan fisik dan lingkungan, Klausal A. 12 keamanan operasional dan A.13 Keamanan Operasi.

1.6 Kerangka Pemikiran

Dalam kerangka berpikir ini peneliti akan mencoba menjelaskan masalah pokok penelitian. Penjelasan yang disusun akan menggabungkan antara teori dengan masalah yang diangkat dalam penelitian ini:



Gambar 1-1 Kerangka Pemikiran

Penjelasan dari gambar 1-1 dalam kerangka berpikir:

1. Identifikasi masalah

   Langkah awal dalam penelitian ini adalah identifikasi masalah. Masalah yang dihadapi yaitu keamanan informasi, dimana keamanan sangat dibutuhkan oleh organisasi sehingga diperlukan suatu audit keamanan menggunakan framework tertentu. Pada penelitian ini, framework yang digunakan dalam Audit Keamanan Informasi adalah ISO/IEC 27001:2013 yaitu mengenai Information Security Management System (ISMS).

2. Studi Literatur

   Setelah memilih masalah dan metode yang digunakan dalam penyelesaian masalah. Studi literatur didapatkan dari berbagai teori yang berhubungan dengan topik penelitian antara lain jurnal, buku, web, dan standar-standar checklist yang dijadikan acuan dalam penelitian ini, serta dokumen-dokumen organisasi seperti kebijakan dan prosedur keamanan informasi.

3. Menentukan Ruang Lingkup

   Ruang lingkup dari penelitian ini adalah Sistem Keaman Informasi Divisi MIS Yayasan Tarumanagara, Jakarta. Penelitian ini bertujuan untuk mengetahui kepatuhan organisasi terhadap prosedur yang terdapat pada checklist ISO 27001:2013. Ruang lingkup audit keamanan sistem informasi ini mengkhususkan pada hal-hal yang akan diperiksa dalam proses audit, khususnya yang terkait dengan batasan penelitian yang telah ditentukan di awal.

4. Pengumpulan Data

   Setelah ruang lingkup audit ditentukan dalam tahap sebelumnya, maka penelitian masuk dalam tahap pengumpulan data. Pengumpulan data dilakukan dengan menggunakan metode wawancara dan *observasi*. Wawancara merupakan metode yang dapat dilakukan untuk mendapatkan data primer. Untuk tahapan audit, data yang didapatkan berasal dari hasil wawancara responden yang dikumpulkan untuk kelengkapan temuan audit. Adapun wawancara dilakukan dengan bagian yang bertanggungjawab dalam pengelolaan kemanan informasi yaitu Divisi Management Information Systems (MIS). Sedangkan *Observasi* dimulai dengan mengidentifikasi dan

membuat pemetaan sehingga didapatkan gambaran umum tentang sasaran penelitian. Pada penelitian ini dilakukan *observasi* mengenai kondisi pengelolaan keamanan informasi. Sehingga nantinya hasil *observasi* digunakan dalam penentuan kontrol objektif yang sesuai.

5. Pelaksanaan Audit

   Penilaian *maturity level*, Analisis (gap) dilakukan berdasarkan checklist hasil wawancara, kuisioner, *observasi* dan pengumpulan dokumen organisasi baik itu kebijakan, prosedur, kontrol, dan dokumen-dokumen terkait keamanan informasi lainnya. Dokumen kemudian diteliti berdasarkan domain dan kontrol objektif yang berasal dari Assessment Checklist Annex A ISO 27001:2013.

6. Temuan dan Rekomendasi

   Pada proses temuan dan rekomendasi yang dilakukan adalah memeriksa data profil, kebijakan, *observasi* standart operating procedure serta melakukan wawancara. Seluruh proses tersebut menghasilkan bukti (data temuan audit) yang terkait dengan sistem yang sedang berlangsung, selain itu analisa sebab dan akibat temuan, serta rekomendasi untuk organisasi agar melakukan penetapan kontrol keamanan yang lebih baik dan sesuai dengan standar ISO 27001.

1.7 Sistematika Penulisan Tugas Akhir

Sistematika penulisan ini terdiri dari dari V bab yang merupakan susanan dari penulisan secara teratur dan terperinci sehingga dapat dengan mudah diketahui hubungan anatara bab yang satu dengan bab lainnya yang dimaksudkan untuk mempermudah pembahasan. Adapun sistematika penulisan tersebut adalah sebagai berikut:

BAB I PENDAHULUAN

Bab I merupakan Bab Pendahuluan yang berisi latar belakang, rumusan masalah, tujuan dan kegunaan penelitian, landasan teori, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi sumber pengetahuan (teori dll) yang menjadi dasar (termasuk "hal" baru) dan mendukung argumentasi TA (sesuai yg diuraikan dalam (kerangka berpikir).

BAB III METODE

Metode disesuaikan dengan konteks kajian TA (konteks rekayasa dan/atau komputasi). Metode dapat juga berupa pendekatan baru dan memberikan justifikasi dari pendekatan yang dipilih. Sesuai konsep/konteks, TA harus mengikuti disiplin metode yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Menjelaskan hasil penelitian, termasuk prosedur yang dijalankan, tolok ukur yang dipakai dan indikator keberhasilannya. Dari hasil evaluasi dapat diperlihatkan kemungkinan ketercapaian pelaksanaan TA (solusi yang ditawarkan dapat menyelesaikan persoalan yang didefinisikan pada pernyataan masalah, atau bagaimana sebuah future dapat direalisasikan/didekati).

BAB V SARAN DAN KESIMPULAN

Kesimpulan harus dapat ditarik dari awal mula identifikasi masalah. tujuan penelitian, pembahasan, dan hasil pembahasan.