# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang

Perusahaan *e-health* di Belanda memiliki sejumlah tantangan dimana mereka harus mampu menjaga keamanan informasi dan privasi data pengguna. Seperti yang diteliti oleh (Gelder et al., 2017), dimana *telenephrology* dilakukan untuk melakukan konsultasi penyakit ginjal dengan menggunakan internet. Sistem yang dibangun untuk melakukan *telenephrology* mengikuti NEN 7510 untuk memastikan *third-party* mematuhi *standard* keamanan informasi. S elain itu, ada juga penelitian yang bergerak dalam penyediaan layanan kesehatan secara *online* (*e-health*) untuk manula di Belanda (Beishuizen et al., 2017), pengobatan *severe mental illness* (SMI) dengan melalui *video conference* (Blankers, Emmerik, Richters, & Dekker, 2016), manajemen data kesehatan di instansi kesehatan (Hoeijmakers, Beck, Wouters, Prins, & Steup, 2018) dan penelitian tentang membuat sistem pengawasan data kesehatan (Schaap, Zwart, Roosmalen, Bloemenkamp, & Akker, 2017). Semua penelitian yang dilakukan mematuhi NEN 7510 dan standard lainnya yang ada di Belanda.

Melihat beberapa contoh kasus yang telah disebutkan di penelitian tentang *e-health*, lokasi penelitian juga merupakan sebuah *enterprise* yang memiliki bisnis *e-health* untuk *mental healthcare* dan memiliki aktivitas bisnis di Rotterdam, Belanda. Beberapa isu yang dapat diteliti adalah keamanan informasi serta privasi

data pengguna. Keamanan informasi bagi setiap *enterprise* yang menjalankan *e-health* di Belanda, berkewajiban patuh terhadap NEN 7510-2:2017. Selain itu, bila suatu *enterprise* ingin memiliki reputasi internasional, maka mereka harus mengikuti serangkaian akreditasi yang disediakan oleh ISO 27001:2013.

*Enterprise* tersebut sudah memiliki sertifikasi ISO 27001:2013 dan sedang mengikuti proses sertifikasi NEN 7510-2:2017. Dari fakta tersebut, sistem manajemen keamanan informasi (SMKI) harus dipelihara sedemikian rupa dan tidak hanya dijadikan sebagai syarat untuk meloloskan suatu proyek dan akhirnya keamanan informasi pun terbengkalai. SMKI yang baik adalah yang memiliki siklus *maintenance* yang periodik dan *compliance* terhadap *standard* yang sudah berlaku. Untuk melihat bahwa keamanan informasi di perusahaan *e-health* tersebut sudah mengikuti kontrol - kontrol di ISO 27001:2013 dan NEN 7510-2:2017. COBIT 4.1 dapat digunakan untuk melakukan audit karena *framework* ini sudah mencakup standard ISO 27001:2013.

Melakukan audit teknologi informasi itu sendiri merupakan bagian dari SMKI yang memang harus dilakukan oleh sebuah *enterprise*. Di dalam penelitian ini akan dilakukan langkah – langkah dalam menerapkan proses audit dengan menggunakan COBIT 4.1. . Kontrol dari NEN 7510-2:2017 akan dicari irisannya dengan objektif kontrol yang ada di COBIT 4.1. Bila tidak ada kontrol NEN 7510-2:2017 yang relevan, maka kontrol tersebut akan diukur dengan model kematangan COBIT 4.1 untuk meninjau maturitasnya. NEN 7510-2:2017 Toolkit saat ini tidak memiliki model kematangan seperti yang ada di COBIT 4.1.

Kemudian, diakhiri dengan memberikan laporan dan rekomendasi yang diberikan untuk menjadi tumpuan dalam peningkatan terhadap target maturitas dan kepatuhan di dalam perencanaan yang disusun oleh *enterprise* tersebut. Selain itu, mencari bukti – bukti dari tiap kontrol dan menjadikannya sebagai objektif yang harus dipenuhi dalam penelitian ini.

## 1.2. **Identifikasi Masalah**

Langkah identifikasi terhadap masalah yang diangkat dalam penelitian ini antara lain:

1. Bagaimana melakukan *internal audit* terhadap keamanan sistem informasi sebuah perusahaan penyedia layanan kesehatan untuk melihat kesesuaiannya dengan ISO 27001 dan NEN 7510-2
2. Bagaimana mengukur sebuah keamanan sistem informasi dengan mengukur maturitasnya untuk melihat potensi lain yang dapat ditambah dari proses yang sudah diterapkan dan berjalan
3. Bagaimana mencari perangkat *internal audit* yang sesuai untuk diterapkan dalam mengevaluasi keamanan sistem informasi untuk mengacu dan sesuai dengan ISO 27001 dan NEN 7510-2
4. Rekomendasi apa saja yang dapat diberikan kepada perusahaan berdasarkan hasil internal audit menggunakan COBIT 4.1 berdasarkan ISO 27001 dan NEN 7510-2 untuk peningkatan proses keamanan sistem informasi

## 1.3. **Tujuan Penelitian**

Penelitian ini bertujuan untuk membantu *enterprise* dalam meninjau kondisi keamanan sistem informasi dari dua standard yang berbeda. E*nterprise* yang memiliki bisnis di dalam *mental healthcare* ini menggunakan sarana teknologi informasi untuk membantu pasiennya lebih cepat tertangani dan dapat melakukan psikoterapi dimanapun. Berikut ini adalah tujuan dari penelitian yang akan dilakukan:

1. Melakukan audit untuk melihat kepatuhan keamanan informasi terhadap proses dan infrastruktur yang telah ada dan berjalan sesuai dengan ISO 27001.
2. Melakukan audit untuk melihat kepatuhan keamanan informasi dari sistem informasi kesehatan yang mengacu kepada NEN 7510-2:2017.
3. Kerangka kerja yang digunakan untuk audit keamanan TI adalah COBIT 4.1
4. Mengkombinasikan NEN 7510-2:2017 dengan COBIT 4.1 untuk melihat apakah COBIT 4.1 dapat digunakan untuk mengaudit TI di sebuah *enterprise* yang menjalankan sistem informasi kesehatan di Belanda dan menjadikannya sebuah model baru dalam melakukan audit TI terhadap sistem informasi kesehatan.

## 1.4. **Manfaat Penelitian**

Penelitian yang dilakukan diharapkan memberikan beberapa manfaat bagi *enterprise* yang menjadi tempat penelitian ataupun bagi khalayak publik yang

akan membaca hasil penelitian ini. Berikut adalah beberapa manfaat yang dapat digunakan dari hasil penelitian ini:

1. Mengetahui tata cara melakukan *internal audit* dengan menggunakan COBIT 4.1 untuk ISO 27001:2013 dan NEN 7510-2:2017
2. Mengetahui dan memahami cara melakukan *internal audit* terhadap suatu sistem informasi di perusahaan Belanda yang memberikan layanan kesehatan
3. Mengetahui apakah NEN 7510-2:2017 dapat diaudit menggunakan COBIT 4.1
4. Memberikan hasil berupa laporan *internal audit* dan rekomendasi kepada pihak manajemen di perusahaan untuk memberikan gambaran strategik yang dapat diambil oleh perusahaan.

## 1.5. **Batasan Masalah**

Berikut ini adalah beberapa batasan masalah yang dibahas di dalam penelitian ini:

1. Penelitian hanya dibatasi hingga masalah keamanan sistem informasi yang lebih spesifik pada implementasi dan pengelolaan *information security management system (ISMS).*
2. Standard yang menjadi acuan adalah ISO 27001:2013 dan NEN 7510-2:2017.

3. Sistem informasi yang diteliti merupakan sistem informasi kesehatan yang melayani *mental healthcare*
4. Audit dilakukan dengan menggunakan COBIT 4.1. Proses COBIT 4.1 yang akan digunakan dalam penelitian hanya satu proses setelah melewati pemetaan visi misi ke *IT goals*
5. Dari proses COBIT 4.1 yang dipilih, hanya beberapa objektif kontrol yang dipilih. Dua diantaranya harus memiliki irisan dengan NEN 7510-2:2017 sedangkan dua lainnya tidak perlu memiliki irisan.
6. Penelitian dilakukan dengan kaidah *self-assessment* yang berperan sebagai *internal auditor* agar tidak menimbulkan disrupsi terhadap para karyawan di *enterprise* tersebut

## 1.6. Sistematika Penulisan

Sistematika penulisan akan diuraikan menjadi lima bab, yaitu:

**Bab I Pendahuluan**: bab ini berisi latar belakang penelitian, identifikasi masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

**Bab II Kajian Pustaka:** bab ini berisi uraian berbagai teori yang menjadi penunjang penelitian dari topik yang diusung. Kajian pustaka juga berisi tentang komparasi terhadap beberapa penelitian yang telah dilakukan sebelumnya dan dijadikan acuan untuk menentukan fokus penelitian. Teori

yang dibahas meliputi sistem informasi, keamanan sistem informasi, layanan kesehatan berbasis *web*, ISO 27001, NEN 7510-2:2017, COBIT 4.1, COBIT 5 dan membuat kajian terhadap penelitian sebelumnya yang relevan dengan topik penelitian ini.

**Bab III Metodologi Penelitian:** bab ini berisi persiapan penelitian berupa penjelasan tentang tempat penelitian, objek dan lingkup yang diteliti, penentuan perangkat *internal audit* yang terdiri dari pemilihan proses COBIT 4.1 dan melihat irisan serta memilih objektif kontrol yang sesuai dengan NEN 7510-2:2017 yang digunakan untuk penelitian ini dan menjelaskan alur penelitian yang dilakukan.

**Bab IV Hasil Penelitian dan Pembahasan**: bab ini berisi pemabahasan yang lebih detail dari hasil *internal audit* dengan menggunakan COBIT 4.1 serta memberikan gambaran berbagai potensi kekurangan dalam sistem manajemen keamanan informasi (SMKI) yang sudah ada di *enterprise*. Kemudian, memberikan laporan hasil *internal audit* dan rekomendasi untuk peningkatan proses menjadi lebih baik sesuai perangkat yang digunakan.

**Bab V Kesimpulan**: bab ini berisi kesimpulan dari hasil penelitian serta saran dan rekomendasi yang dapat diberikan untuk peningkatan penelitian berikutnya yang memiliki topik ISO 27001:2013 dan NEN 7510-2:2017.

Khususnya bagi peneliti selanjutnya yang ingin melakukan penelitian dalam melakukan *internal audit* di perusahaan Belanda.

**Daftar Pustaka:** bagian ini berisi daftar dari seluruh kepustakaan yang digunakan dalam penelitian. Penulisan daftar pustaka mengikuti kaidah yang berlaku dalam tata naskah di lingkungan Universitas Komputer Indonesia.

**Lampiran:** Pelengkap informasi mengenai instrumen penelitian, seperti dokumen pendukung dan hasil penelitian yang dihasilkan perangkat penelitian jika diperlukan.