# BAB I PENDAHULUAN

## I.1 Latar Belakang

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik, mengingat peran TIK yang semakin penting dalam upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Faktor keamanan informasi merupakan aspek yang sangat penting untung diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama mengalami masalah. Keamanan informasi yang meliputi: kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) (KOMINFO, 2011).

Tata Kelola Teknologi Informasi (TI) telah ditetapkan dalam peraturan Menteri Komunikasi dan Informatika No. 41 tahun 2007 tentang Panduan Umum Tata Kelola TIK Nasional yang bertujuan untuk mewujudkan tata kelola pemerintahan yang baik dan bertanggung jawab *(good governance)*. Melalui penerapan prinsip – prinsip akuntabilitas, transparansi dan supremasi hukum serta merta melibatkan partisipasi masyarakat dalam setiap proses kebijakan publik. Dengan dipublikasikannya regulasi tersebut, institusi pemerintahan pada tingkat kota maupun provinsi harus membuat tata kelola TI sebagai panduan pengelolaan TI.

Semakin berkembangnya peran TI dalam dunia bisnis, manajemen TI dituntut untuk menghasilkan Sistem Informasi (SI) yang layak dan mendukung kegiatan bisnis pada perusahaan. Perubahan dilakukan dengan cara penerapan Perancangan Strategis Sistem Informasi untuk menghasilkan SI yang mendukung kegiatan bisnis pada organisasi/perusahaan. Salah satu aspek penting dalam perkembangan TI yaitu keamanan informasi. Seperti yang sudah dijelaskan di atas, Sistem Manajemen Keamanan Informasi (SMKI) sangat diperlukan karena mengingatnya ancaman terhadap aspek keamanan informasi yang semakin meningkat.

Tim Direktorat Keamanan Informasi (KOMINFO, 2011, p. 7) menyebutkan bahwa ”mayoritas instansi belum memiliki atau sedang menyusun kerangka kerja

keamanan informasi yang memenuhi standar", dapat dikatakan bahwa beberapa perusahaan di Indonesia masih sangat minim perhatiannya terhadap tata kelola manajemen keamanan informasi.

Sistem Manajemen Keamanan Informasi (SMKI) sendiri merupakan proses untuk menentukan bagimana mengelola, memonitor, dan memperbaiki informasi agar aman. Penerapan SMKI yang baik akan memberikan dampak yang baik terhadap proses bisnis organisasi agar terhindar dari kemungkinan risiko yang mungkin/akan terjadi. ISO/IEC 27001:2013 merupakan standar internasional yang dapat dijadikan pedoman untuk menerapkan SMKI.

Pada awal tahun 2015, terjadi kasus pencurian data penting pada Kantor Manajemen Pegawai Amerika Serikat, dengan jumlah data yang tercuri / hilang sebanyak 21,5 juta data, data penting (sidik jadi, biodata, dll.) pegawai hingga mantan pegawai federal Amerika (Tribun, 2015). Dengan adanya teknologi informasi yang sudah semakin canggih, pemerintahan Amerika Serikat pun dapat di tembus dengan banyaknya data yang tercuri.

PT. Tirta Investama sudah menerapkan sistem TI sebagai pendukung proses kegiatan bisnisnya. Salah satu elemen penting dalam tata kelola yang baik adalah tata kelola TI, di dalamnya termasuk tata kelola keamanan informasi. Menurut (Sarno, 2009, p. 27) "Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya memastikan atau menjamin kelangsungan bisnis *(business continuity)*, meminimalisasi risiko bisnis *(reduce business risk)* dan memaksimalkan pengembalian investasi serta menunjang peluang bisnis".

PT. Tirta Investama sebagai salah satu perusahaan swasta di Indonesia juga diminta memberikan pelayanan terbaik untuk pihak yang membutuhkan informasi, seperti karyawan ataupun pihak lainnya. Oleh karena itu, PT. Tirta Investama membentuk suatu divisi khusus yang melayani sistem manajemen informasi dan layanan interkoneksi. Dalam hal ini, informasi menjadi aset penting karena selain bersifat rahasia, informasi juga memiliki risiko dari akses tidak sah, modifikasi data, pencurian data, *human error*, kerusakan perangkat keras dan

perangkat lunak, maupun risiko dari bencana alam (Deni Darmawan, 2013, p. 243). Salah satu standar yang dapat digunakan yaitu ISO/IEC 27001:2013. Sangat diperlukannya pengukuran tingkat keamanan informasi untuk menganalisa organisasi yang telah mengamankan informasi sampai sejauh mana, lalu dapat melakukan evaluasi dan perancangan serta pembaharuan SMKI pada organisasi/perusahaan.

Oleh karena itu dilakukan proses perancangan SMKI yang meliputi: penentuan ruang lingkup, tahap analisis risiko, dan tahap penentuan kontrol keamanan yang sesuai dengan standar ISO/IEC 27001:2013. Kemudian mendapatkan obyektif kontrol dan kontrol keamanan dan mengidentifikasi kontrol sesuai klausul yang ada pada ISO/IEC 27001:2013

Dalam jurnal internasional *Information Security Management System Standards : A Comparative Study of Big Five* (Heru Susanto, 2011) menjelaskan bahwa ISO/IEC 27001 telah menjadi *framework* yang paling populer dan banyak digunakan dengan presentase 27% dibanding *framework* lainnya, yaitu COBIT (26%), ITIL (8%), BS7799 (18%), dan PCIDSS (21%). ISO/IEC 27001 dapat digunakan pada semua tipe organisasi, karena standar yang fleksibel, dan dapat disesuaikan dengan kebutuhan dan tujuan dari organisasi. Penggunaan ISO/IEC 27001 juga disebabkan karena fleksibilitas yang tinggi dan dikembangkan karena pemanfaatan standar sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai serta ukuran struktur organisasi. Dan pelaksanaan penelitian ini akan dilakukan dengan laporan berjudul ” **ANALISIS RISIKO SISTEM MANAJEMEN ASET BERBASIS ISO 27001 : 2013 MENGGUNAKAN METODE *FAILURE MODE AND EFFECTS ANALYSIS* PADA PT. TIRTA INVESTAMA**”

## I.2 Perumusan Masalah

Berdasarkan latar belakang penelitian maka dapat dirumuskan masalah yang akan diteliti lebih lanjut dalam penelitian, yaitu:

1) Bagaimana tingkat keamanan informasi pada PT. Tirta Investama berdasarkan standar ISO/IEC 27001 terkait dengan Kebijakan Keamanan Informasi,

Manajemen Aset, Keamanan Fisik dan Lingkungan, Keamanan Operasional dan Keamanan Komunikasi?

2) Bagaimana tingkat kesenjangan terkait Kebijakan Keamanan Informasi, Manajemen Aset, Keamanan Fisik dan Lingkungan, Keamanan Operasional dan Keamanan Komunikasi?
3) Bagaimana perancangan kontrol keamanan informasi?

## I.3 Tujuan Penelitian

Berdasarkan perumusan masalah maka tujuan penelitian, yaitu:

1) Menganalisis risiko tingkat keamanan informasi pada PT. Tirta Investama berdasarkan standar ISO/IEC 27001 terkait dengan Kebijakan Keamanan Informasi, Manajemen Aset, Keamanan Fisik dan Lingkungan, Keamanan Operasional dan Keamanan Komunikasi.
2) Menilai tingkat kesenjangan terkait Kebijakan Keamanan Informasi, Manajemen Aset, Keamanan Fisik dan Lingkungan, Keamanan Operasional dan Keamanan Komunikasi.
3) Memberikan rekomendasi dan perancangan kontrol keamanan informasi.

## I.4 Manfaat Penelitian

Adapun manfaat dari penelitian, yaitu:

1) Membantu perusahaan untuk meminimalisir risiko yang mungkin terjadi
2) Sebagai bahan pertimbangan dalam mengembangkan keamanan sistem informasi.
3) Memberikan referensi berupa rekomendasi dan perancangan kontrol informasi pada perusahaan.
4) Sebagai sumber acuan informasi dan bahan rekomendasi untuk penelitian selanjutnya yang berkaitan dengan keamanan informasi menggunakan *framework* ISO 27001:2013

## I.5 Ruang Lingkup dan Objek Penelitian

Adapun ruang lingkup dan objek penelitian ini, yaitu:

1) Analisis risiko sistem manajemen aset pada PT. Tirta Investama menggunakan standar ISO/IEC 27001.
2) Penelitian ini hanya difokuskan pada klausul A.5 Kebijakan Keamanan Informasi, A.8 Manajemen Aset, A.11 Keamanan Fisik dan Lingkungan, A.12 Keamanan Operasional dan A.13 Keamanan Komunikasi.
3) Penelitian ini hanya difokuskan pada divisi *project & assets.*
4) Penilaian risiko menggunakan metode *Failure Mode and Effects Analysis.*

## I.6 Sistematika Penulisan Tugas Akhir

**BAB I PENDAHULUAN**

Bab ini berisi tentang gambaran umum objek penelitian, latar belakang, perumusan masalah, tujuan, manfaat, ruang lingkup dan objek penelitian, dan sistematika penelitian.

**BAB II TINJAUAN PUSTAKA DAN LINGKUP PENELITIAN**

Bab ini berisi tentang tinjauan pustaka yaitu penelitian-penelitian terdahulu yang pernah membahas mengenai permasalah yang sama atau serupa dan teori-teori yang berhubungan dengan penelitian yang diperlukan dalam analisis data.

**BAB III METODOLOGI PENELITIAN**

Bab ini berisi tentang metode penelitian yang digunakan, teknik pengumpulan data, populasi dan sampel, dan teknik analisis.

**BAB IV ANALISIS DAN PEMBAHASAN**

Bab ini menjelaskan tentang pembahasan yang berisi data-data yang telah dikumpulkan, diolah dan kemudian mendapatkan solusi dari permasalahan yang sedang dihadapi.

**BAB V HASIL REKOMENDASI**

Bab ini berisi hasil rekomendasi yang akan diberikan ke perusahaan.

**BAB VI KESIMPULAN DAN SARAN**

Bab ini akan berisi kesimpulan dari hasil pembahasan, memberikan masukan atau saran yang dapat diimplementasikan oleh organisasi.