BAB I
PENDAHULUAN

1.1. 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.

Bank asal Australia, Commonwealth Bank, pada hari Kamis (3/5/2018) mengaku telah kehilangan catatan keuangan milik hampir 20 juta pelanggannya akibat kesalahan keamanan yang fatal. Perusahaan terbesar di negara itu mengatakan tidak dapat menemukan dua pita data magnetik yang menyimpan nama, alamat, nomor rekening, dan rincian transaksi dari tahun 2000 hingga 2016 (CNBC, 2018).

Dikutip dari laman *Wired*, Jumat (1/2/2019), 2,2 miliar nama pengguna dan kata sandi unik ini dibagikan secara gratis melalui forum dan torrent yang sering digunakan oleh hacker. Informasi, kemunculan data rahasia pengguna ini merupakan lanjutan dari tersebarnya 773 juta alamat *email* dan 22 juta *password user* dalam database berkode *Collection* #1. Database tambaham dari jenis yang sama kini telah muncul di internet, dengan total hingga 845GB data curian. Sebagian besar data yang dicuri berasal dari aksi serangan peretasan besar-besaran terhadap perusahaan, seperti Yahoo, Dropbox, dan LinkedIn. Aksi peretasan ini merupakan masalah besar bagi mereka yang memiliki kebiasaan menggunakan password yang sama untuk semua

akun mereka, dan tidak mengetahui apakah informasi mereka bocor atau tidak, dan sudah dicuri oleh *hacker* (Liputan6, 2019).

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 objektif kontrol dan kontrol keamanan dan mengidentifikasi kontrol sesuai klausul yang ada pada ISO/IEC 27001:2013. Pelaksanaan penelitian ini akan dilakukan dengan laporan berjudul "**ANALISIS RISIKO KEAMANAN INFORMASI DENGAN METODE *OCTAVE ALLEGRO* PADA PT. TIRTA INVESTAMA".**

1.2. Perumusan Masalah

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

i) Bagaimana tingkat keamanan informasi berdasarkan profil risiko pada PT. Tirta Investama dengan metode analisis *OCTAVE Allegro*?

ii) Rekomendasi upaya untuk meminimalkan risiko keamanan informasi dengan kontrol ISO 27001 Tahun 2013.

1.3. Tujuan Penelitian

Berdasarkan perumusan masalah maka tujuan penelitian, yaitu:

i) Untuk mendapatkan profil risiko keamanan informasi PT. Tirta Investama menggunakan metode *OCTAVE Allegro*.
ii) Mengidentifikasi solusi *people*, *process*, dan *technology* terkait manajemen keamanan informasi.

1.4. Manfaat Penelitian

Adapun manfaat dari penelitian, yaitu:

i) Membantu perusahaan dalam mengidentifikasi profil risiko keamanan informasinya.
ii) Memberikan referensi berupa rekomendasi dan perancangan kontrol keamanan informasi pada perusahaan menggunakan metode risk assessment *OCTAVE Allegro* dan *framework* ISO 27001:2013.

1.5. Ruang Lingkup dan Objek Penelitian

Adapun ruang lingkup dan objek penelitian ini, yaitu:

i) Objek penelitian ini adalah aset informasi yang dikelola oleh divisi DAN'IS PT Tirta Investama.
ii) Analisis Risiko menggunakan metode *OCTAVE Allegro*.
iii) Rekomendasi disusun dengan mengacu pada klausul-klausul ISO 27001:2013.

1.6. 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 KESIMPULAN DAN SARAN

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