BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi informasi di kehidupan saat ini memiliki peranan penting khususnya dalam otomatisasi beberapa tugas pada operasional sistem. Proses otomatisasi ini memberikan kemudahan dalam malakukan berbagai pelayanan dan meningkatkan efisiensi serta efektifitas pada suatu perusahaan. Di era digitalisasi ini perusahaan menggunakan sistem digital untuk menunjang layanan kepada para pengguna agar pengguna dapat dengan mudah mengakses informasi ataupun layanan yang ada [1]. Penggunaan teknologi informasi pastinya membutuhkan keamanan sistem untuk membantu mengamankan data penting perusahaan serta digunakan untuk memastikan keamanan yang spesifik agar tercapainya tujuan perusahaan. Peranan dalam keamanan sistem informasi penting karena sebagai pemenuhan kebutuhan perusahaan seperti penyimpanan data dan asset. [2]. Keamanan sistem informasi juga berfungsi untuk menjaga kerahasiaan, integritas, dan ketersediaan data, yang merupakan aspek krusial dalam operasional perusahaan.

Memastikan tingkat keamanan pada perusahaan telah baik digunakan perlu adanya standar penilaian untuk menetapkan persyaratan sistem manajemen keamanan informasi. Standar ini membentuk kerangka kerja yang lebih terstruktur dalam mengamankan informasi pada suatu organisasi. Pengukuran tingkat keamanan perusahaan dilakukan salah satunya dengan ISO 27001:2013. ISO/IEC 27001:2013 merupakan standarisasi keamanan yang diakui secara global dan disajikan dengan metode yang berbeda. Pembangunan sistem manajemen keamanan informasi harus dilakukan dengan menerapkan standar keamanan yang terkontrol dan selaras dengan ISO/IEC 27001:2013 [3]. Pada proses mempertahankan kerahasiaan, ketersediaan, dan integritas informasi dengan menerapkan prosedur

manajemen risiko adalah fungsi utama dari Sistem Manajemen Keamanan Informasi (ISMS). Ini memastikan bahwa risiko-risiko tersebut dikelola dengan efisien dan diminimalkan oleh pihak yang memiliki kewenangan [4]. ISMS mencakup berbagai kebijakan, prosedur, dan kontrol yang dirancang untuk melindungi aset informasi dari ancaman internal maupun eksternal.

PERUMDA Tirta Satria merupakan badan usaha milik daerah yang dikelola oleh pemerintahan Kota Banyumas. Perusahaan ini terletak Jl. Prof. Dr. Suharso No.52, Mangunjaya, Purwokerto Lor, Kecamatan Purwokerto Timur, Kabupaten Banyumas, Jawa Tengah. PERUMDA Tirta Satria berfokus dalam pemasokan, penyaluran, dan pengelolaan dalam pengadaan sumber air bersih bagi masyarakat Kota Banyumas. Proses pelayanan PERUMDA Tirta Satria ini dapat dilayani secara *online* pada aplikasi Info PDAM Tirta Satria yang dapat diunduh melalui *playstore*. Layanan yang disediakan yaitu pengecekan tagihan, layanan pengaduan pelanggan dan non pelanggan, lokasi loket pembayaran, dan informasi lainnya seperti informasi adanya gangguan aliran [6]. Aplikasi ini juga memungkinkan pelanggan untuk melakukan pembayaran tagihan secara langsung, melacak riwayat penggunaan air, dan mendapatkan notifikasi terkait pemutusan sementara atau perbaikan yang sedang berlangsung.

Penggunaan sebuah sistem tidak menutup kemungkinan akan terjadinya ancaman risiko yang mengganggu proses kinerja perusahaan dan keefektifan perusahaan dalam melakukan proses layanan sistem. Seperti adanya serangan siber seperti pencurian data, sabotase, dan *rainsomeware*. Intensitas risiko mengenai serangan keamanan sistem informasi berdampak sesuai dengan besar ancaman yang terjadi[7]. Oleh karena itu, perusahaan harus proaktif dalam menerapkan langkah-langkah pencegahan dan perlindungan, seperti penggunaan firewall, enkripsi data, sistem deteksi intrusi, dan pembaruan perangkat lunak secara berkala.

Berdasarkan proses wawancara sebelumnya kepada pihak PERUMDA Tirta Satria khususnya pada bidang SDM dan IT yang terlampir

pada lampiran 5 diperoleh informasi bahwa pernah terjadi adanya serangan *ransomware* pada sistem keamanan perusahaan ini yang memberikan dampak tidak dapat diaksesnya beberapa server, data rusak, dan adanya perubahan ekstensi file yang mengakibatkan pihak pegawai perusahaan PERUMDA Tirta Satria yang berkepentingan tidak dapat melakukan *upload* foto dan dokumen. Kejadian ini jelas mengganggu jalannya proses kerja dari PERUMDA Tirta Satria. Kegiatan operasioanl perusahaan jelas terganggu tidak dapat mengakses data dan aplikasi yang diperlukan untuk pekerjaan mereka, menyebabkan penurunan produktivitas dan efisiensi, dengan adanya serangan *ransomeware* seperti penguncian data dan kehilangan data. Beberapa aspek keamanan informasi yang mempengaruhi yaitu aspek kerahasiaan. Serangan *ransomeware* ini dapat mengekspos kerahasiaan data kepada pihak yang tidak berwenang, menyebabkan potensi kerugian misalnya, data pelanggan atau rencana strategis perusahaan dapat jatuh ke tangan pihak yang tidak bertanggungjawab. Aspek ketersediaan (*availability)* tidak tersedianya data karena telah diambil alih oleh pihak *hacker.*

Bersumber dari wawancara yang telah dilakukan didapatkan PERUMDA Tirta Satria belum memiliki manajemen keamanan sistem untuk melakukan tindakan mitigasi selain proses *back up* data yang dilakukan setiap hari nya. Proses *back up* data saja tidak cukup untuk melindungi keamanan sistem informasi perusahaan. Berdasarkan hal itu sesuai dengan permasalahan yang ada penting dilakukan penilaian standar keamanan sistem dengan menggunakan metode ISO 27001:2013. Standar ISO 27001:2013 dipilih dalam penelitian ini karena ISO 27001 merupakan standar internasional yang diakui secara luas untuk mengukur dan mengelola keamanan informasi. Standar ini menawarkan kerangka kerja yang komprehensif untuk mengidentifikasi risiko keamanan informasi, sehingga sangat relevan dalam konteks PERUMDA Tirta Satria Banyumas yang menghadapi masalah keamanan sistem yang kurang kuat. Dengan menerapkan ISO 27001:2013, perusahaan dapat mengadopsi langkah-langkah terbaik untuk melindungi data dan sistemnya, memastikan kepatuhan

terhadap regulasi, serta meningkatkan kepercayaan pelanggan dan pemangku kepentingan.Sejalan dengan fokus utama ISO 27001:2013 manajemen keamanan informasi. Berbeda dengan *framework* lainnya seperti COBIT yang memiliki fokus utama tata kelola dan manajemen TI [8]. IS0 27001:2013 dengan fleksibilitas dalam mengembangkan standar ini sangat dipengaruhi oleh persyaratan, tujuan, dan kriteria keamanan organisasi yang berbeda, serta kepatuhan terhadap standar ISO 27001 :2013.

Penelitian dengan judul " Evaluasi Standar Keamanan Sistem Informasi Pada Perumda Tirta Satria Banyumas Berdasarkan ISO 27001:2013" diharapkan memberikan dampak positif bagi perusahaan seperti meningkatkan keamanan sistem informasi, meningkatkan kinerja perusahaan, dan meningkatkan reputasi perusahaan. Hasil dari proses penelitian ini berupa rekomendasi yang dapat menjadi bahan pertimbangan perusahaan dalam peningkatan pada strategi perusahaan yang sejalan dengan tujuan perusahaan. Pemberian rekomendasi ini juga sebegai pemanfaatan dalam pengelolaan teknologi informasi yang lebih baik lagi untuk perusahaan.

1.2 Rumusan Masalah

Berdasarkan uraian yang telah tercantum pada latar belakang dapat dirumuskan permasalahan sebegai berikut :

1. Belum memiliki mekanisme yang secara otomatis melakukan pemantauan perubahan regulasi
2. Tidak ada penanganan efektif dalam serangan ransomeware yang terjadi Pada PERUMDA Tirta Satria.
3. Belum menerapkan pengukuran atau metrik tertentu untuk mengevaluasi efektifitas dalam pengelolaan sumber daya pada konteks sistem manajemen keamanan informasi.

1.3 Pertanyaan Penelitian

Setelah melihat pada latar belakang masalah ditemukan pertanyaan penelitian sebegai berikut :

1. Bagaimana langkah-langkah dalam melakukan pemantauan perubahan regulasi di PERUMDA Tirta Satria Banyumas?
2. Bagaimana melakukan penanganan yang efektif dalam menghadapi serangan ransomeware yang terjadi pada PERUMDA Tirta Satria Banyumas?
3. Bagaimana menghasilkan rekomendasi untuk mengevaluasi efektifitas dalam pengelolaan sumber daya pada konteks sistem manajemen keamanan informasi.

1.4 Batasan Masalah

Batasan masalah atau cakupan diperlukan sebagai penetapan batasan yang jelas dalam penyusunan penelitian ini. Penetapan Batasan dalam penelitian ini sebagai berikut :

1. Objek penelitian dilaksanakan pada PERUMDA Tirta Satria Banyumas.
2. Data diperoleh berdasarkan wawancara dengan unit bagian SDM dan IT pada sub divisi Teknologi Informasi PERUMDA Tirta Satria Banyumas dan dokumen pendukung seperti struktur organisasi dan tata kerja perusahaan.
3. Penelitian ini menganalisis klausul berdasarkan standar ISO 27001:2013.
4. Fokus dalam penelitian ini untuk menganalisis standar ISO pada PERUMDA Tirta Satria Banyumas.

1.5 Tujuan Penelitian

Tujuan dilakukannya penelitian ini antara lain:

1. Mengetahui langkah-langkah dalam melakukan pemantauan perubahan regulasi di PERUMDA Tirta Satria Bnyumas.
2. Menghasilkan rekomendasi untuk memastikan bahwa kebijakan keamanan informasi diterapkan dan dipatuhi dalam setiap tahap operasional.

1.6 Manfaat Penelitian

Adapun manfaat dari penelitian ini terbagi menjadi dua manfaat yaitu, manfaat praktir (bagi perusahaan) dan manfaat teoritis (bagi mahasiswa):

1. Manfaat Praktis:
   a. Membantu perusahaan untuk mengetahui kondisi dari perusahaan saat ini terkait sistem keamanan infirmasi dan memberikan gambaran terkait tindak lanjut kedepannya dalam meingkatkan keamanan pada sistem dan teknologi informasi pada PERUMDA Tirta Satria Banyumas.
   b. Hasil penelitian yang dilakukan selama penelitian dapat menjadi masukan bagi pihak perusahaan di masa yang akan datang khususnya di bagian sistem keamanan informasi.
2. Manfaat Teoritis
   a. Menjadi referensi pada penelitian selanjutnya dalam bidang standar keamanan ISO 27001:2013.
   b. Melakukan identifikasi terhadap sistem keamanan informasi berdasarkan teori dan pengetahuan yang diperoleh selama di perkuliahan.