

BAB I PENDAHULUAN

1.1 Latar Belakang

Informasi merupakan salah satu aset perusahaan yang sangat penting. Dengan perkembangan teknologi informasi yang sangat pesat, kemungkinan terjadinya gangguan keamanan informasi semakin meningkat. Untuk itu perusahaan harus menerapkan kebijakan yang tepat untuk melindungi aset informasi yang dimiliki, maka kebijakan tentang pengamanan informasi harus mencakup sekurang-kurangnya terdapat prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamanan *logical security*, prosedur pengamanan operasional teknologi informasi, terutama untuk sistem informasi yang digunakan dan prosedur penanganan insiden dalam pengamanan informasi.

Untuk itu diperlukan analisis keamanan sistem informasi untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur. Standar yang digunakan yaitu ISO 27001. Beberapa hal penting yang patut dijadikan pertimbangan mengapa standar ISO 27001 dipilih karena dengan standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dan ukuran struktur organisasi

ISO/IEC 27001 adalah standar keamanan informasi yang diterbitkan pada Oktober 2005 oleh International *Organization for Standardization (ISO)* dan *International Electrotechnical Commission (IEC)*. Standar ini menggantikan BS-77992:2002 (*British Standard*). ISO/IEC 27001 merupakan salah satu model manajemen keamanan sistem informasi yang dapat digunakan untuk memberikan arahan

kepada pengguna agar informasi yang dimilikinya aman dari ancaman dan gangguan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan pada bagian 1.1, maka rumusan masalah, yaitu sebagai berikut :

1. Apakah semua prosedur serta proses-proses yang terkait dengan usaha-usaha pengimplementasian keamanan informasi aplikasi *Smart-one* di perusahaan sudah dijalankan dengan benar?
2. Bagaimana kontrol yang dilakukan PT.PLN (Persero) Distribusi Jawa Barat dan Banten dalam menjaga keamanan data dan informasi dari aplikasi *Smart-one* yang ada di perusahaan?
3. Apakah kebijakan dan tindakan yang ditetapkan perusahaan dalam melindungi sistem keamanan informasi aplikasi *Smart-one* sudah dilaksanakan dengan benar ?
4. Bagaimana tanggung jawab pegawai dalam menggunakan aplikasi *Smart-one* perusahaan dan fasilitas perusahaan?

1.3 Tujuan Pembahasan

Tujuan dari penelitian ini adalah sebagai berikut :

1. Pembahasan mengenai bukti – bukti dan prosedur tentang pengelolaan & pengamanan informasi *smart-one* sesuai standar *ISO 27001*.
2. Melaksanakan analisis terhadap kontrol keamanan informasi *smart-one* pada PT. PLN (Persero) Distribusi Jawa Barat dan Banten sesuai standar *ISO 27001* dengan menganalisis hasil wawancara berupa bukti dan temuan-temuan yang ada.
3. Menganalisis kebijakan dan tindakan yang berhubungan dengan keamanan informasi *smart-one* perusahaan.
4. Melakukan analisis terhadap tanggung jawab pegawai yang menggunakan aplikasi *smart-one* dan fasilitas yang diberikan perusahaan.

1.4 Ruang Lingkup Kajian

Dari permasalahan yang sudah dijelaskan, maka yang menjadi batasan dalam penelitian ini adalah :

1. Perencanaan analisis yang dibuat, lebih diarahkan sebagai panduan analisis internal.
2. Penelitian hanya dilakukan pada kantor PT. PLN (Persero) Distribusi Jawa Barat dan Banten khususnya pada kantor APJ Bandung Selatan saja.
3. Penelitian bukan menerapkan *ISO 27001* pada perusahaan, melainkan melakukan analisis keamanan informasi yang dilakukan perusahaan untuk disesuaikan dengan standar *ISO 27001*.
4. Kontrol objek dari standar *ISO 27001* yang terdapat di dalam penelitian ini, diambil berdasarkan kebutuhan perusahaan.

1.5 Sumber Data

Sumber yang di dapat dalam melakukan penelitian ini diantaranya :

1. Wawancara, merupakan metode pengumpulan data yang dilakukan dengan cara mengajukan pertanyaan – pertanyaan dan melakukan tanya jawab secara langsung dengan pembimbing lapangan dari perusahaan.
2. *Observasi*, merupakan metode pengumpulan data yang digunakan dengan cara melakukan pengamatan langsung kegiatan yang ada di perusahaan untuk memperoleh informasi yang akurat.

1.6 Sistematika Penyajian

Sistematika pembahasan laporan Sidang Tugas Akhir dan Tugas Akhir ini dibagi menjadi 4 (empat) bab. Berikut penjelasan tentang masing-masing bab :

1. BAB I PENDAHULUAN

BAB I Pendahuluan membahas mengenai dasar-dasar dan latar belakang, perumusan masalah, tujuan, batasan masalah, sumber data, dan sistematika penulisan.

2. BAB II KAJIAN TEORI

BAB II Kajian Teori membahas mengenai teori-teori yang digunakan untuk melakukan analisis keamanan sistem informasi berdasarkan ISO 27001.

3. BAB III ANALISIS

BAB III Analisis berisi tentang analisis dan hasil analisis keamanan sistem yang dilakukan selama proses pengumpulan data, yang kemudian akan dilakukan analisis dan evaluasi yang disesuaikan dengan standar ISO 27001.

4. Bab IV Simpulan dan Saran

Berisi Kesimpulan dan Saran dari hasil analisis dan evaluasi dari penerapan dan pengendalian yang telah dilakukan disesuaikan terhadap beberapa kontrol yang terdapat di dalam standar ISO 27001.