BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi informasi (TI) terus berkembang pesat setiap harinya, sehingga organisasi atau perusahaan harus senantiasa beradaptasi dan menerapkan perkembangan TI tersebut. Peranan teknologi informasi sangat signifikan dalam meningkatkan kualitas informasi pada perusahaan yang menjadi alat dan strategi yang kuat untuk mengintegrasikan dan memproses data dengan cepat dan akurat serta sebagai fondasi untuk menciptakan produk dan layanan baru yang menjadi daya saing dalam menghadapi persaingan (Naibaho, 2017). Dengan makin kompleksnya kemajuan teknologi informasi, ada banyak lubang kerentanan yang dapat dimanfaatkan pihak-pihak untuk mengganggu keberjalanan proses di suatu organisasi.

Keamanan informasi merujuk pada tindakan untuk mencegah sumber daya informasi dari dimanfaatkan oleh pihak yang tidak sah untuk memanipulasi, mencuri, atau mengakses informasi tersebut (JR dan Schell, 2008). Keamanan informasi sangatlah penting bagi perusahaan karena informasi merupakan salah satu aset yang sangat penting dalam menjalankan bisnis. Informasi dapat mencakup data-data, rahasia, rancangan produk, serta informasi penting lainnya yang dapat membantu perusahaan untuk bersaing dan memperoleh keuntungan. Jika informasi ini jatuh ke tangan yang salah, maka dapat membahayakan perusahaan secara finansial, operasional, dan reputasi.

Perusahaan yang mengelola informasi penting dan sensitif perlu memperhatikan keamanan informasi sebagai bagian penting dari strategi bisnis mereka. Dengan mengelola keamanan informasi dengan baik, perusahaan dapat meminimalkan kemungkinan terjadinya dampak negatif dan memaksimalkan kemungkinan hasil positif dari data dan informasi yang dimilikinya. Oleh karena itu keamanan informasi penting dilakukan untuk memastikan bahwa informasi perusahaan efektif dan terus menjadi sesuai dengan kebutuhan perusahaan yang terus berkembang. Dalam *master plan* Teknologi Informasi (TI) Badan Usaha Milik Negara (BUMN) 2021, keamanan TI menjadi salah satu fokus utama. Upaya untuk meningkatkan keamanan sistem dan infrastruktur TI menjadi prioritas

penting dalam rangka menjaga kerahasiaan, integritas, dan ketersediaan data serta melindungi dari potensi ancaman siber yang semakin kompleks dan beragam.

PT. Nusantara Turbin dan Propulsi (NTP), adalah salah satu BUMN serta anak perusahaan PT. Dirgantara Indonesia. PT. NTP adalah perusahaan yang terpercaya dan terkemuka di Asia Tenggara dan juga diakui di seluruh dunia untuk layanannya yang berkualitas tinggi dalam bidang pemeliharaan dan *overhaul* turbin gas, mesin *aero*, dan turbin industri. Untuk menjaga informasi-informasi internal PT. NTP dalam mengelola menjaga informasi dibutuhkan sebuah penerapan keamanan informasi karena dengan penerapannya, perusahaan dapat melindungi informasi penting dari ancaman yang berasal dari luar maupun dalam perusahaan yang dihadapi PT. NTP. Menurut PERMEN BUMN NOMOR PER-2/MBU/03/2023 (2023), BUMN memiliki kewajiban untuk menjaga keamanan siber sesuai dengan prinsip utama keamanan informasi, yaitu kerahasiaan, keutuhan, dan ketersediaan, serta mengikuti ketentuan peraturan perundang-undangan yang berkaitan dengan keamanan siber. Selain itu, BUMN juga diharuskan untuk mengidentifikasi ancaman dan kerentanan pada aset teknologi informasi yang dimilikinya. Dalam hal ini, perusahaan diwajibkan menyusun rencana atau prosedur untuk menangani dan memulihkan insiden siber, dengan mengacu pada praktik terbaik yang berlaku. Dengan mengambil langkah-langkah ini, BUMN dapat memastikan bahwa keamanan dan integritas informasi mereka terjaga dengan baik, serta siap menghadapi tantangan persaingan di era teknologi informasi yang terus berkembang pesat.

ISO 27001 merupakan standar internasional yang diakui secara luas dan dirancang untuk membantu organisasi mengidentifikasi dan mengurangi risiko keamanan informasi, serta menetapkan dan memelihara kebijakan dan prosedur keamanan yang ketat. Arsitektur ISO 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi (Chazar, 2015). ISO 27001 adalah sebuah *framework* keamanan informasi yang dapat membantu perusahaan untuk mengembangkan dan menerapkan sistem manajemen keamanan informasi (SMKI) yang efektif. *Framework* ini meningkatkan kepercayaan pelanggan dan meningkatkan kinerja bisnis mereka dengan mengurangi risiko dan memastikan bahwa sistem mereka dilindungi dari

ancaman keamanan yang mungkin timbul. Selain itu, ISO 27001 juga membantu perusahaan memenuhi persyaratan hukum dan peraturan terkait keamanan informasi sehingga PT. Nusantara Turbin dan Propulsi dapat mengembangan bisnis dan jangkauan pemasaran internasional yang lebih luas.

Dalam merencanakan implementasi proses keamanan informasi menggunakan *framework* ISO 27001, perusahaan harus mempertimbangkan tujuan bisnis dan kebutuhan keamanan informasi mereka, serta sumber daya yang tersedia untuk menerapkan standar ini dengan efektif. PT. NTP juga perlu mengidentifikasi risiko keamanan informasi yang ada dan mengembangkan strategi untuk mengurangi risiko tersebut.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana analisis kondisi sistem manajemen keamanan informasi di PT. Nusantara Turbin dan Propulsi saat ini?
b. Bagaimana rancangan sistem manajemen keamanan informasi menggunakan ISO 27001:2022 yang sesuai dengan kebutuhan PT. Nusantara Turbin dan Propulsi?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mengidentifikasi implementasi sistem manajemen keamanan informasi pada PT. Nusantara Turbin dan Propulsi saat ini.
b. Memberikan rekomendasi rancangan sistem manajemen keamanan informasi dengan menggunakan *framework* ISO 27001:2022 untuk PT. Nusantara Turbin dan Propulsi.

I.4 Batasan Penelitian

Batasan masalah yang ada pada penulisan ini adalah sebagai berikut:

1) Penelitian ini hanya berfokus pada perencanaan sistem keamanan informasi menggunakan *framework* ISO 27001:2022.
2) Penelitian ini tidak mencakup aspek pengelolaan risiko keamanan informasi.

3) Penelitian ini hanya dibatasi hingga pada tahapan perancangan, tidak sampai tahap implementasi pada PT. NTP terutama pada Departemen *Management Information Systems*.

I.5 Manfaat Penelitian

Adapun manfaat penelitian ini:

1. Bagi Universitas Telkom, penelitian ini diharapkan bermanfaat menjadi salah satu pedoman implementasi keamanan informasi pada perusahaan.
2. Bagi PT. Nusantara Turbin dan Propulsi, penelitian ini diharapkan dapat dijadikan masukan atau digunakan untuk meningkatkan keamanan informasi pada perusahaan.
3. Bagi peneliti, penelitian ini diharapkan dapat meningkatkan pengetahuan peneliti tentang standar dan prinsip keamanan informasi.