BAB I PENDAHULUAN

I.1 Latar Belakang

Paul Hopkin dalam bukunya *"Fundamental of Risk Management"* berpendapat bahwa risiko adalah suatu peristiwa dengan kemampuan untuk mempengaruhi (menghambat, meningkatkan atau menimbulkan keraguan tentang) efektivitas dan efisiensi proses inti suatu organisasi. Segala sesuatu yang berharga akan selalu ada risiko yang menyertai layaknya dua sisi koin. Maka dari itu pula, risiko tidak dapat dieliminir sepenuhnya, akan tetapi harus dikelola agar dampak yang timbul dari risiko tersebut dapat terkalkulasi dan juga ditolerir oleh organisasi (Hopkins, 2017).

Pada era digitalisasi saat ini, sebuah organisasi yang berbentuk suatu badan usaha lazimnya memiliki unit Teknologi Informasi (TI) yang menunjang operasional perusahaan tersebut. Selayaknya suatu yang berharga dan membawa manfaat besar bagi perusahaan, risiko dari unit TI pun juga menjadi bagian dari risiko bisnis itu sendiri yang memerlukan suatu mekanisme pengelolaan secara holistik.

Konsep kerahasiaan, keutuhan, dan ketersediaan (Confidentiality, integrity & availability) adalah hal pokok yang paling diperhatikan dalam menjaga faktor keamanan sistem suatu informasi karena dengan tidak terjaganya salah satu faktor tadi akan menjadi gerbang terbukanya masalah dalam keutuhan informasi yang tidak terjamin keamanannya (Yudha, 2016). Manajemen risiko adalah suatu proses identifikasi, analisis, penilaian, pengendalian, dan upaya menghindari, meminimalisir, atau bahkan menghapus risiko yang tidak dapat diterima (Ramadhan, Febriansah, & Dewi, 2020). Manajemen Risiko Keamanan dan pengendalian keamanan informasi pada aset kritis organisasi merupakan aspek penting dalam memberikan perlindungan, menjaga kelangsungan proses bisnis, dan meningkatkan tingkat keamanan informasi (Wibowo & Ramli, 2022).

PT Nusantara Turbin Dan Propulsi adalah perusahaan Indonesia yang bergerak di bidang teknik, perawatan, perbaikan dan perbaikan turbin gas dan peralatan berputar. Manajemen Keamanan Informasi IT yang merupakan ranah dari Departemen *Management Information System* (selanjutnya akan disingkat

menjadi Departemen MIS) bertujuan untuk melindungi sumberdaya informasi yang dimiliki PT Nusantara Turbin dan Propulsi supaya tercipta integritas dan keamanan pada semua sumber daya informasi. Menurut PERMEN BUMN NOMOR PER-2/MBU/03/2023 (2023) pasal 208 menegaskan bahwa:

1) BUMN wajib menjaga keamanan siber sesuai dengan prinsip utama keamanan informasi, yang meliputi keharahsiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) serta mengikuti ketentuan peraturan perundang-undangan yang berkaitan dengan keamanan siber.

2) BUMN wajib mengidentifikasi ancaman dan kerentanan pada aset teknologi informasi yang dimiliki dan menyusun rencana atau prosedur penanggulangan dan pemulihan insiden siber dengan mengacu pada praktik terbaik.

Berlandaskan dari PERMEN BUMN tersebut, identifikasi ancaman dan kerentanan pada aset TI menjadi aspek penting yang harus dilakukan oleh PT Nusantara Turbin dan Propulsi.

ISO/IEC 27005:2018 memberikan panduan untuk manajemen risiko keamanan informasi dalam sebuah organisasi, terutama mendukung persyaratan Sistem Manajemen Keamanan Informasi (SMKI) menurut ISO/IEC 27001. Namun, standar ini tidak menyediakan metodologi khusus dan spesifik untuk semua bentuk perusahaan dalam melaksanakan manajemen risiko keamanan informasi. Pendekatan dalam manajemen risiko tergantung pada ruang lingkup SMKI, konteks manajemen risiko, atau sektor industri bergantung pada kebutuhan serta kondisi dari organisasi (Ariyani & Sudarma, 2016). Akan tetapi, ISO/IEC 27005 secara merinci memberikan panduan langkah demi langkah tentang cara melakukan analisis dan evaluasi risiko untuk meningkatkan pengelolaan keamanan informasi (Patiño, 2018).

Fokus utama manajemen risiko keamanan informasi dibahas lebih lanjut pada ISO/IEC 27005:2018 memiliki proses langkah demi langkah yang mencakup pengaturan konteks, penilaian risiko keamanan informasi, penanganan risiko keamanan informasi, penerimaan risiko keamanan informasi, komunikasi risiko

keamanan informasi, dan memantau dan meninjau risiko keamanan informasi (Fikri, Putra, Suryanto, & Ramli, 2019).

Penelitian ini dilakukan untuk membantu penilaian tingkat risiko pada aset yang dikelola oleh Departemen MIS berdasarkan ketidakterpenuhan kontrol keamanan informasi ISO/IEC 27002:2022 dan memberikan rekomendasi berupa *best practice* yang ditujukan untuk menjaga keamanan informasi dengan langkah mitigasi terhadap potensi ancaman yang telah dinilai.

I.2 Perumusan Masalah

Dari latar belakang yang telah dikemukakan di atas, Tugas Akhir ini akan dirumuskan beberapa permasalahan sebagai berikut:

a. Bagaimana kondisi pengelolaan risiko terkait keamanan informasi yang ada di Departemen MIS PT Nusantara Turbin dan Propulsi.
b. Bagaimana rancangan proses pengelolaan risiko pada Departemen MIS PT Nusantara Turbin dan Propulsi ISO/IEC 27005:2018.
c. Apa saja rekomendasi yang dapat diberikan untuk mengelola risiko keamanan informasi pada Departemen MIS PT Nusantara Turbin dan Propulsi.

I.3 Tujuan Penelitian

Adapun berdasarkan rumusam masalah yang telah disebutkan pada subbab sebelumnya, maka penelitian ini memiliki tujuan untuk:

a. Melakukan *assessment* pada pengelolaan risiko kemanan informasi pada Departemen MIS PT Nusantara Turbin dan Propulsi sesuai dengan standar ISO/IEC 27005:2018.
b. Merancang pengelolaan risiko keamanan informasi pada Departemen MIS PT Nusantara Turbin dan Propulsi sesuai dengan standar ISO/IEC 27005:2018.

c. Memberikan rekomendasi perbaikan proses pengelolaan risiko keamanan informasi pada Departemen MIS PT Nusantara Turbin dan Propulsi sesuai dengan standar ISO/IEC 27005:2018.

I.4 Batasan Penelitian

Berikut ini merupakan batasan dan ruang lingkup yang penulis tetapkan pada penelitian ini:

1. Penelitian ini berfokus pada identifikasi dan penilaian risiko keamanan informasi dengan menggunakan ISO/IEC 27005:2018 dengan mempertimbangkan tingkat keseuaian pemenuhan terhadap kontrol keamanan informasi yang telah ditetapkan oleh standar ISO/IEC 27002:2022.
2. Penelitian ini dibatasi hanya pada rekomendasi untuk risiko yang telah diidentifikasi, tidak sampai tahap implementasi pada Departemen MIS PT Nusantara Turbin dan Propulsi.

I.5 Manfaat Penelitian

Diharapkan penelitian ini akan memberikan manfaat sebagai berikut:

1. Bagi penulis
   - Penelitian ini bermanfaat untuk mengasah kompetensi dan pemahaman terkait penulis dengan Manajemen Risiko TI
   - Menambah pengalaman penulis dalam melakukan analisa dan perancangan manajemen risiko keamanan informasi.
   - Menghasilkan solusi yang bermanfaat bagi perusahaan
2. Bagi PT Nusantara Turbin dan Propulsi
   - Memberikan evaluasi terhadap risiko keamanan informasi yang ada di PT Nusantara Turbin dan Propulsi.
   - Membantu PT Nusantara Turbin dan Propulsi dalam menentukan *Risk Treatment* terhadap risiko keamanan informasi yang berpengaruh pada keamanan aset TI