BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi pada perkembangannya terus dimanfaatkan oleh segala pihak. Salah satu ranah penggunaan ini berupa implementasi pada perusahaan yang dalam penerapannya akan mendapatkan manfaat yang lebih baik. Namun, tentunya dalam penerapan tersebut terdapat berbagai aspek yang perlu diperhatikan perusahaan, salah satunya yaitu aspek keamanan informasi.

Sebuah instansi atau perusahaan untuk melakukan proses bisnisnya tidak lepas dari berbagai ancaman dan serangan keamanan informasi dari pihak luar. Kelalaian pegawai sebuah instansi atau perusahaan dalam menanggapi informasi itu sendiri dapat merugikan kebanyakan sektor, salah satunya sektor keuangan instansi atau perusahaan itu sendiri.

Pentingnya pemahaman terhadap keamanan informasi bagi karyawan atau pegawai untuk sebuah instansi atau perusahaan sangat mempengaruhi tingkat keamanan informasi perusahaan. Menurut Doni dkk, aset adalah informasi yang rahasia untuk sebuah instansi atau perusahaan akan terancam jika perusahaan atau instansi itu sendiri mengabaikan kesadaran keamanan informasi bagi karyawan. Instansi atau perusahaan harus memiliki cara untuk meningkatkan kesadaran keamanan informasi bagi karyawan atau pegawai [1]

Dengan adanya teknologi informasi membuat munculnya perusahaan yang berdiri dalam bidang teknologi informasi yang membuat munculnya tempat kerja baru untuk masyarakat, karena peran teknologi informasi di banyaknya perusahaan pada saat ini sangat penting, maka informasi yang berkaitan di dalamnya juga menjadi sangat penting, terutama pada proses manajemen pengelolaan data dan informasi yang ada, agar data-data penting tersebut tidak disalah gunakan oleh pihak-pihak yang tidak bertanggung jawab. Dalam ISO 27002:2022 terdapat tiga aspek penting yaitu kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan *(Availability)*, tiga aspek ini disebut dengan CIA Triad yang merupakan model yang digunakan untuk membantu individu dan organisasi dalam membuat aplikasi, sistem, prosedur, atau kebijakan keamanan informasi. Ketiga komponen ini dianggap sebagai yang paling penting untuk membuat sistem keamanan informasi yang kuat dan efisien.[2]

Perkembangan teknologi ini juga yang menuntut bagi sektor pendidikan untuk mengembangkan proses belajar dan mengajar dengan memanfaatkan teknologi informasi. Dengan berkembangnya sistem kemanan informasi juga dapat mencegah terjadinya ancaman kerentanan dan risiko yang terjadi pada lembaga pendidikan.[3]

1.2 Rumusan masalah

Berdasarkan pemaparan latar belakang penelitian ini, ada beberapa rumusan masalah yang dapat difokuskan menjadi beberapa hal untuk dibahas pada penelitian kali ini. Permasalahan yang ada meliputi :

1. Bagaimana penilaian resiko yang terjadi pada lembaga pendidikan menengah atas menggunakan standard ISO 27005:2022?
2. Bagaimana mitigasi yang tepat pada risiko yang terdapapat pada lembaga pedidikan menengah atas?

1.3 Batasan masalah

Berikut merupakan baatasan masalah yang akan diangkat oleh penulis:

1. Studi kasus pada penelitian ini adalah lembaga pendidikan menengah atas yang menggunakan bidang teknologi
2. Penelitian ini menggunakan Standar yang di terapkan dalam penelitian ini ISO/27005:2022.
3. Penelitian ini akan menganalisis risiko berdasarkan aset-aset keamanan dan informasi yang dimiliki pada lembaga pendidikan menengah atas berpendoman pada ISO 27005:2022

1.4 Tujuan penelitian

Berdasarkan dengan apa yang telah dirumuskan dalam rumusan masalah pada penelitian ini, dapat dideduksi bahwa tujuan dari dilakukannya penelitian ini adalah :

1. Melakukan proses penilian resiko terhadap resiko yang kemungkinan akan terjadi pada aset lembaga pendidikan menengah atas menggunakan basis framework 27005:2022.
2. Memberikan rekomendasi yang dapat diberikan kepada lembaga pendidikan menengah atas terhadap hasil tingkat privasi keamanan informasi.