BAB 1 PENDAHULUAN

1.1 Latar Belakang

Penerapan teknologi informasi terutama internet yang semakin pesat membawa perubahan diberbagai aspek kehidupan manusia dalam mencari dan mendapatkan suatu informasi yang tidak terbatas oleh ruang maupun waktu. Berdasarkan *Internet world stats*, Indonesia menempati urutan ketiga di Asia dengan jumlah pengguna internet yang mencapai 212,35 juta pada bulan Maret 2021 [1]. Tingginya pengguna internet di Indonesia telah mempengaruhi berbagai bidang, salah satunya pada bidang pendidikan yang menggunakan internet sebagai penunjang produktivitas bagi lembaga pendidikan tinggi negeri maupun swasta.

Perguruan tinggi XYZ telah menerapkan teknologi informasi untuk menunjang dan mendukung aktifitas akademik. Salah satu penerapan teknologi informasi pada lembaga pendidikan tingkat XYZ tersebut adalah penggunaan *website*. *Website* merupakan salah satu layanan informasi yang dapat diakses oleh orang diseluruh dunia yang menyajikan informasi berupa teks, gambar, audio, maupun video [2].

Sebagai salah satu layanan informasi publik maka, diperlukan sebuah *website* untuk dikembangkan agar dapat melayani permintaan dari pengguna. Penggunaan *website* yang baik dan benar merupakan aspek yang sangat penting agar dapat diakses dengan tanpa adanya gangguan. Salah satu *website* yang paling sering diakses yaitu *website* akademik. *Website* akademik memudahkan civitas akademik untuk dapat mengakses informasi mengenai layanan akademik. Tetapi, dengan banyaknya jumlah pengunjung *website* akademik maka semakin banyak risiko ancaman bagi *website* [3]. Berdasarkan laporan Badan siber dan sandi negara (BSSN) pada tahun 2020 sektor akademik paling banyak mengalami serangan keamanan sebanyak 34% atau sekitar 3.353 insiden [4].

Website PMB XYZ merupakan website yang sangat penting bagi institut karena *website* PMB XYZ berguna untuk calon mahasiswa yang ingin

mendaftar di perguruan tinggi XYZ. Pada *website* PMB XYZ terdapat data calon mahasiswa sebagai aset informasi penting bagi Perguruan Tinggi XYZ untuk menjalankan alur calon mahasiswa yang ingin mendaftar di perguruan tinggi XYZ. Peran *website* PMB XYZ sangat penting karena menjadi pusat informasi bagi calon mahasiswa seperti pembelian token atau pin pendaftaran, dan input data informasi pribadi calon mahasiswa.

Bagi perguruan tinggi XYZ, data informasi pribadi dalam kegiatan akademik merupakan aset yang sangat penting dan perlu dijaga keamanannya dari pihak eksternal maupun internal [5]. *Websit*e PMB XYZ termasuk layanan sistem informasi yang memuat data aset informasi pribadi calon mahasiswa. Semakin besar aset informasi yang tersimpan maka, semakin besar pula risiko yang akan terjadi. Apabila terdapat suatu risiko maka akan sangat membahayakan perguruan tinggi XYZ dalam keamanan sistem informasi *website* PMB XYZ. Dalam menangani risiko yang ada diperlukan manajemen risiko yang bertujuan sebagai upaya untuk mengantisipasi terjadinya risiko yang akan membahayakan perguruan tinggi XYZ. Akibat apabila risiko terjadi seperti kerugian besar pada organisasi, kehilangan kepercayaan, pencurian data, dan lain sebagainya.

Hasil wawancara pendahuluan bersama informan selaku pengelolah *website* mengatakan bahwa "Pada *Website* PMB belum pernah dilakukannya penilaian risiko dan pernah terjadi server down sehingga beberapa menu tidak dapat berjalan dengan normal". Dan berdasarkan wawancara bersama dengan mahasiswa yang pernah menggunakan *Website* PMB perguruan tinggi XYZ mengatakan bahwa "pernah mengalami sebuah kejadian yaitu salahnya informasi jurusan atau program studi kelulusan yang diberikan dari pihak perguruan tinggi yang mengakibatkan ketidakvalidan data mengenai calon mahasiswa baru".

Berdasarkan latar belakang permasalahan tersebut perlu adanya sebuah evaluasi dan penilaian risiko untuk mengetahui risiko apa yang akan mengancam keamanan sistem informasi. Berdasarkan pembahasan sebelumnya, maka peneliti ingin melakukan identifikasi risiko ancaman dan

melakukan evaluasi risiko untuk dapat mengetahui risiko yang akan mengancam keamanan sistem informasi.

Banyak metode yang dapat digunakan dalam melakukan proses menganalisis manajemen risiko keamanan sistem informasi yaitu ISO 27005, NIST SP 800-30, OCTAVE-S dan OCTAVE Allegro. NIST SP 800-30, metode ini mempunyai 9 langkah dalam melakukan analisis risiko yaitu karakterisasi sistem, mengidentifikasi risiko, mengidentifikasi kerawanan, menganalisis kontrol, analisis kecendrungan, analisis dalam, menentukan risiko, merekomendasikan control dan melakukan dokumentasi [6]. Sedangkan metode ISO 27005 juga membahas mengenai manajemen risiko keamanan informasi yang dimana aset informasi disini dibahas dengan cakupan yang lebih luas yaitu pada, proses, informasi, perangkat lunak, perangkat keras, sistem, jaringan dan orang [7]. *OCTAVE-S* merupakan metode yang dikembangkan untuk dapat memenuhi kebutuhan dari organisasi kecil, *OCTAVE –S* sendiri adalah variasi yang disesuaikan dengan keterbatasan sarana dan kendala. Untuk melakukan analisia tim harus memiliki pengetahuan yang luas mengenai bisnis organisasi, proses keamanan sehingga dapat melakukan kegiatan dengan sendirinya [8]. Pada penelitian *OCTAVE Allegro* yang dimana metode ini difokuskan pada aset informasi yang kritis dimana melakukan analisis risiko dengan memperkenalkan konsep container aset informasi, metode ini dirancang untuk melakukan penilaian risiko tanpa melakukan penilaian yang luas. Metode *OCTAVE Allegro* merupakan salah satu metode yang dirancang untuk mefokuskan dan merampingkan proses penilaian risiko keamanan informasi sehingga sebuah organisasi dapat memperoleh hasil yang cukup [9].

Metode *OCTAVE Allegro* berbeda dari metode-metode lainnya karena mempunyai fokus utama yaitu pada aset informasi yang digunakan pada kontainer aset dimana aset informasi itu disimpan, diolah, diproses dan dikirim. Oleh karena itu, penelitiain ini diangkat dengan judul yaitu "Analisis Manajemen Risiko Keamanan Sistem Informasi pada *Website* PMB XYZ dengan Menggunakan Metode *OCTAVE Allegro"* yang akan memberikan hasil penilaian risiko terhadap *Website* PMB perguruan Tinggi XYZ.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan suatu permasalahan yaitu sebagai berikut:

1. Bagaimana mengidentifikasi risiko ancaman keamanan informasi pada *website* PMB perguruan tinggi XYZ dengan menggunakan *OCTAVE Allegro*?
2. Bagaimana melakukan evaluasi risiko keamanan sistem informasi pada *website* PMB perguruan tinggi XYZ dengan menggunakan *OCTAVE Allegro*?
3. Bagaimana rekomendasi yang diberikan kepada pihak IT berdasarkan evaluasi risiko keamanan sistem informasi pada *websit*e PMB Perguruan tinggi XYZ dengan menggunakan *OCTAVE Allegro*?

1.3 Tujuan dan Manfaat

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui bagaimana mengidentifikasi risiko ancaman keamanan sistem informasi *website* PMB XYZ dengan menggunakan *OCTAVE Allegro*.
2. Mengetahui bagaimana melakukan Penilaian risiko keamanan sistem informasi pada *website* PMB XYZ dengan menggunakan *OCTAVE Allegro*.
3. Memberikan rekomendasi berdasarkan hasil penilaian risiko keamanan sistem informasi yang telah diidentifikasi pada *website* PMB Perguruan tinggi XYZ dengan menggunakan metode *OCTAVE Allegro*.

Selain itu manfaat dari penelitian ini adalah sebagai berikut:

1. Manfaat bagi peneliti:
    - Dapat menambah wawasan dan pengetahuan terkait manajemen risiko keamanan sistem informasi
    - Dapat menambah wawasan mengenai penggunaan metode *OCTAVE Allegro*.
2. Manfaat bagi Pengelolah *Website* PMB perguruan tinggi XYZ:

- Mengetahui tingkat risiko yang akan terjadi pada *website* PMB perguruan tinggi XYZ.
- Perguruan tinggi XYZ dapat menjadikan hasil rekomendasi penelitian sebagai bahan evaluasi keamanan sistem informasi *website* PMB.
- Adanya antisipasi terhadap ancaman risiko sehingga tidak menyebabkan kerugian terhadap pihak-pihak terkait.

1.4 Batasan Masalah

Berdasarkan penjelasan sebelumnya, maka terbentuklah ruang lingkup permasalahan yang penulis dapat uraikan yaitu sebagai berikut:

1. Penelitian dilakukan pada *website* PMB Perguruan Tinggi XYZ.
2. Jangka waktu penelitian ini dari tahun 2019-2022
3. Penelitian menggunakan kerangka kerja *OCTAVE Allegro*.
4. Metode penelitian yang digunakan yaitu Kualitatif Studi kasus
5. Informan yang digunakan sebagai sumber data untuk proses evaluasi adalah Pusat Teknologi Informasi dan Admisi dan Marketing dengan kriteria informan yang telah ditentukan