BAB 1
PENDAHULUAN

1.1. Latar Belakang

Perkembangan pada sektor teknologi informasi saat ini berkembang dengan sangat pesat dan menjadi prioritas utama dikarenakan keefektifan dan keefisienannya [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 disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Dalam ISO 27002 terdapat tiga aspek penting yaitu kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*), tiga aspek ini disebut dengan *CIA Triad. CIA Triad* bisa didefinisikan sebagai sebuah rancangan model yang digunakan untuk menjadi panduan untuk membantu seseorang baik secara individu maupun organisasi tertentu dalam membentuk atau membuat sebuah aplikasi, sistem, prosedur, atau suatu kebijakan yang berhubungan dengan keamanan informasi. Ketiga aspek tersebut dapat disebut sebagai aspek yang paling penting untuk menciptakan sebuah keamanan informasi yang kuat dan efektif [2].

Dalam rangka menjaga kualitas pelayanan ini tidak akan selalu berjalan dengan mulus, pasti akan ada gangguan-gangguan yang akan menghasilkan risiko. Risiko adalah potensi bahaya yang dapat timbul dari beberapa penerapan proses yang dilakukan pada saat ini atau mungkin dari beberapa peristiwa yang akan terjadi di masa depan [4]. Menurut Raharjo keamanan informasi seringkali kurang mendapatkan perhatian dari para pengelola teknologi informasi. Apabila risiko dapat mengganggu performansi dari sistem, seringkali keamanan akan dikurangi atau ditiadakan [3]. dengan hal itu analisis risiko sangat perlu untuk dilakukan agar ancaman yang akan terjadi dapat diatasi dan mengurangi dampak terhadap informasi dan data yang ada pada perusahaan.

Nilai risiko yang ada bisa dikurangi dengan melakukan suatu manajemen keamanan risiko yang tepat. Manajemen risiko adalah pendekatan atau sebuah metodologi dalam mengelola ketidakpastian yang berkaitan dengan potensi terjadinya suatu risiko yang dapat merugikan. Dengan adanya manajemen terhadap risiko maka akan ada aktivitas dan kontrol organisasi untuk menangani risiko [6]. salah satu sistem yang secara khusus mengedepankan faktor manajemen risiko saat ini adalah SMKI. Sistem manajemen keamanan informasi (SMKI) atau yang disebut juga *Information Management Security System* (ISMS) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis yang berfungsi untuk merencanakan (*Plan*), mengimplementasikan (*Do*), memonitor dan meninjau ulang (*Check*), dan memelihara (*Act*) terhadap keamanan informasi pada perusahaan maupun suatu organisasi [5]. Keamanan informasi menjadi bagian yang sangat penting untuk menjamin keutuhan data dan kualitas informasi yang dihasilkan. Beberapa prosedur yang telah dirumuskan untuk melindungi data dan informasi, baik dari faktor kesengajaan maupun masalah teknis dan etika yang diperkirakan dapat merusak, menghilangkan atau menghambat distribusi data dan informasi tersebut [7]. Salah satu standar yang secara khusus mengedepankan faktor keamanan informasi saat ini adalah ISO 27002. ISO 27002 merupakan standar yang berfungsi untuk memberikan panduan standar keamanan informasi dan praktik manajemen keamanan informasi yang mencakup kontrol yang merupakan bagian penting dari manajemen semua organisasi dengan banyaknya kontrol yang dapat diterapkan sesuai dengan kebutuhan organisasi [8]. Adapun kelebihan lain dari standar ISO 27002 ini yaitu fleksibel, dapat dikembangkan sesuai kebutuhan organisasi, serta merupakan metode khusus yang terstruktur dan dapat memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan.

PT. XYZ merupakan perusahaan yang bergerak dibidang teknologi informasi dimana perusahaan ini memberikan layanan dan memfasilitasi setiap bisnis, industri dan individu di dunia dengan solusi digital. Adapun beberapa produk yang diluncurkan oleh perusahaan ini yang berfungsi untuk

memudahkan pekerjaan pada saat WFH (*Work From Home*) dan sudah digunakan oleh perusahaan besar yang bergerak dibidang jasa, dan Internal PT. XYZ. PT. XYZ harus menjaga kerahasiaan, keutuhan dan ketersediaan informasi yang ada agar tidak terjadi risiko yang tidak diharapkan. Adapun hasil wawancara yang didapatkan dimana penerapan teknologi informasi pada PT. XYZ belum memiliki kebijakan terkait dengan keamanan informasi dan sistem manajemen risiko IT, beberapa risiko IT juga terjadi seperti banyaknya masalah pada sistem *website* maupun produk-produknya seperti sulitnya mengakses website serta banyaknya kesalahan pada proses *testing* dan *coding*, dan semakin banyaknya orang-orang yang tidak bertanggung jawab mencoba mengambil data dan informasi yang ada yang berupa aset informasi *client* dimana PT. XYZ juga membantu perusahaan untuk membuat *website* internal *client*. Dengan hal itu untuk mengukur tingkat risiko yang terjadi di PT. XYZ ini akan dilakukan menggunakan metode FMEA sebagai alat pengukuran terhadap risiko yang dimiliki. FMEA *(Failure Modes and Effect Analysis)* merupakan suatu teknik analisa bahaya atau risiko secara kualitatif yang dapat digunakan untuk mengidentifikasi bagaimana suatu peralatan, fasilitas, atau sistem dapat gagal serta apa saja akibat yang dapat ditimbulkan [1]. Metode ini akan membantu mengantisipasi berbagai kemungkinan timbulnya risiko menggunakan tiga parameter yaitu *Severity, Occurrence,* dan *Detection*, sehingga risiko tersebut akan bisa dicegah ataupun mengurangi risikonya dan menggunakan *maturity level* sebagai alat untuk mengetahui kematangan kemampuan proses yang dapat membantu pendefinisian dan pemahaman pada perusahaan. Berdasarkan penjelasan diatas oleh karena itu dibutuhkan penelitian ini untuk dapat bisa memberikan rekomendasi berupa mitigasi risiko yang sesuai standar ISO 27002:2022 untuk membantu PT. XYZ meningkatkan sistem manajemen keamanan informasinya.

1.2. Perumusan 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 kematangan dan kemampuan proses pada PT. XYZ menggunakan Indeks KAMI untuk *maturity level*?
2. Bagaimana analisis dan penilaian risiko yang terjadi pada PT. XYZ menggunakan metode FMEA (*Failure Modes and Effect Analysis*)?
3. Apa saja rekomendasi mitigasi risiko yang tepat untuk risiko tertentu sesuai dengan standar ISO 27002:2022 di PT. XYZ?

1.3. Batasan Masalah

Berikut adalah beberapa dari batasan masalah yang telah ditetapkan dan menjadi perhatian pada pelaksanaan penelitian ini:

1. Studi kasus pada penelitian ini adalah PT. XYZ yang bergerak pada bidang teknologi.
2. Standar yang akan diterapkan sebagai mitigasi risiko adalah ISO/IEC 27002:2022.
3. Metode penilaian risiko yang digunakan adalah FMEA (*Failure Modes and Effect Analysis*).
4. Metode pengukuran kematangan dan kemampuan proses perusahaan yang digunakan adalah Indeks KAMI untuk *Maturity Level.*

1.4. Tujuan

Tujuan dari penelitian ini adalah untuk:

1. Untuk melakukan pengukuran level kematangan PT. XYZ dengan menggunakan Indeks KAMI untuk *maturity level*.
2. Untuk melakukan analisis risiko IT di PT. XYZ dan melakukan penilaian risiko dengan metode FMEA (*Failure Modes and Effect Analysis*).
3. Untuk memberikan rekomendasi mitigasi risiko yang tepat untuk risiko tertentu di PT. XYZ menggunakan standar ISO/IEC 27002:2022.