BAB 1 PENDAHULUAN

1.1. Latar Belakang

Perguruan tinggi sekarang sudah banyak memanfaatkan teknologi untuk mengelola data dan informasi dari mahasiswa, dosen, maupun staf perguruan tinggi. Universitas XYZ merupakan salah satu perguruan tinggi yang meluncurkan aplikasi untuk menunjang perkuliahan dan memenuhi kebutuhan bagian sumber daya manusia pada lingkungan Universitas XYZ. Aplikasi ini memiliki beberapa fitur untuk mahasiswa sebagai pengguna, seperti media presensi mahasiswa, nilai mahasiswa, jadwal mahasiswa, *timeline*, berita dan fitur lainnya. Sebagai aplikasi pastinya memiliki aset dan menyimpan data yang banyak serta cenderung sensitif. Oleh karena itu, perlu diperhatikan akan keamanan data yang tersimpan pada aplikasi.

Tim internal aplikasi XYZ mengatakan bahwa, aplikasi XYZ baru diluncurkan pada tahun 2021. Pengembangan aplikasi ini terus dilakukan baik dari sisi pengalaman pengguna maupun sisi keamanan informasi aplikasi. Keamanan informasi merupakan tindakan perlindungan terhadap kepentingan krusial individu, organisasi, maupun negara, yang mencakup melindungi informasi yang tidak lengkap, tidak konsisten, dan tidak sesuai [1]. Berdasarkan hasil wawancara dengan tim internal XYZ, pada perubahan ke versi 1.5.7 ada beberapa perbaikan yang dilakukan. Perubahan-perubahan ini dilakukan seperti, pada *coding* ketika pengambilan data pengguna, tampilan antarmuka, serta pembaruan API ke versi 2 yang lebih *secure* daripada versi sebelumnya. Dalam sisi pemenuhan terhadap standar keamanan informasi seperti ISO 27001 belum dilaksanakan, namun dalam menjaga keamanan informasi aplikasi, tim internal XYZ selalu melakukan *testing* setelah melakukan *development.* Karena aplikasi ini belum pernah melakukan audit keamanan informasi khususnya dengan standar ISO 27001:2022, maka pada penelitian ini dilakukan evaluasi keamanan informasi memanfaatkan standar ISO 27001:2022 serta pemberian rekomendasi mitigasi risiko untuk menjaga keamanan pada aplikasi.

Berdasarkan studi literatur pada penelitian terdahulu, ditemukan bahwa terdapat beberapa penelitian yang menggunakan standar ISO 27001 sebagai acuan

untuk manajemen keamanan informasi. Selain itu terdapat juga penelitian yang menggabungkan standar ISO 27001 dan metode *Failure Mode and Effect Analysis* (FMEA) yang bertujuan untuk mendefinisikan, mengidentifikasi kegagalan sistem, serta penilaian risiko. Berdasarkan hasil analisis menggunakan metode FMEA dan standar ISO/EIC 27001:2013, terdapat 22 *cause failure* yang berpotensi terjadinya risiko terhadap keamanan aset TI di Bidang Perdagangan Dalam Negeri (PDN) Dinas Perdagangan dan Perindustrian Pemerintah Provinsi XYZ [2]. Standar ISO 27001 dapat digunakan pada proses penilaian kelayakan aplikasi, seperti yang dilakukan pada aplikasi tiket bioskop [3]. Dalam studi kasus Perguruan Tinggi X juga mengadopsi ISO 27001 dan ISO 27002, serta metode FMEA untuk melakukan analisis komprehensif mengenai risiko keamanan informasi pada situs web repositori perpustakaan digitalnya [4].

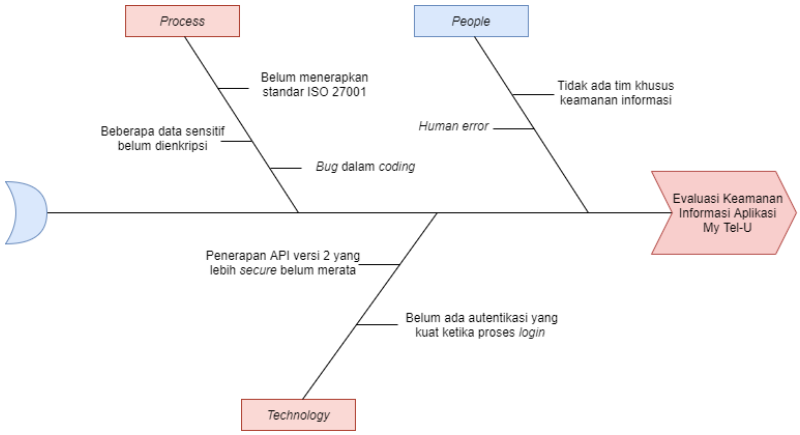
Metode *Failure Mode and Effect Analysis* (FMEA) dapat digunakan sebagai metode menganalisis potensi kesalahan atau kegagalan dalam sebuah proses atau sistem [4]. Dengan menerapkan metode FMEA, dilakukan identifikasi risiko potensial, serta penilaian RPN (*Risk Priority Number*) secara sistematis. Penilaian risiko dengan FMEA dilakukan berdasarkan tiga faktor yaitu *severity* (tingkat keparahan), *occurrence* (frekuensi terjadi), dan *detection* (kemudahan terdeteksi). Dari ketiga nilai faktor tersebut akan menghasilkan nilai RPN dan digunakan untuk mengukur tingkat prioritas risiko kegagalan. Sehingga, risiko akan mendapat prioritas mitigasi berdasarkan level risiko dan nilai RPN.

Selain mengidentifikasi risiko terhadap aplikasi XYZ dengan menggunakan metode FMEA, hal penting lain yang dilakukan adalah menerapkan standar ISO/IEC 27001:2022 dalam konteks aplikasi XYZ. ISO/IEC 27001: 2022 adalah sebuah standar internasional dalam menangani aspek kegiaatan dari teknis tertentu [5]. ISO/IEC 27001:2022 digunakan sebagai panduan dalam mengelola keamanan informasi secara terstruktur, sehingga dapat membantu pencapaian tujuan bisnis suatu organisasi. Pemanfaatan ISO/IEC 27001:2022 pada penelitian ini sebagai panduan penyusunan pertanyaan audit serta pemberian rekomendasi kontrol keamanan informasi pada aplikasi XYZ terhadap risiko potensial. Sehingga, dengan menggunakan standari ISO 27001:2022 dapat membantu dalam meningkatkan keamanan informasi aplikasi XYZ.

Proses evaluasi dan analisis keamanan informasi dengan menggabungkan metode FMEA dengan standar ISO/EIC 27001:2022, akan mendorong untuk merancang saran mitigasi keamanan informasi terhadap aplikasi XYZ. Melalui penerapan ISO/EIC 27001:2022 pada aplikasi XYZ, diharapkan dapat melindungi serta memelihara kerahasiaan, integritas, dan ketersediaan informasi [5]. Dari tim internal XYZ juga mengharapkan *feedback* terkait kondisi keamanan informasi XYZ saat ini. Sehingga penelitian ini mendorong pentingnya implementasi keamanan informasi berdasarkan standar ISO/EIC 27001:2022 pada aplikasi XYZ, agar aset informasi yang ada terjaga dan aman dari risiko yang mungkin terjadi. Serta penerapan rekomendasi kontrol berdasarkan ISO 27002:2022.

1.2. Identifikasi Masalah

Hubungan antara *people, technology,* dan *process* yang selaras dapat menghasilkan keamanan informasi yang baik dalam sebuah perusahaan. Tiga kategori ini membantu dalam menganalisis potensi solusi untuk masalah keamanan. Oleh karena itu, dengan mengklasifikasi ancaman dalam ketiga kategori ini dapat membantu mengatasi masalah keamanan [6]. Untuk mengetahui kondisi keamanan informasi aplikasi XYZ dilakukan wawancara untuk identifikasi masalah berdasarkan *people, technology,* dan *process.* Proses identifikasi masalah ini, akan dianalisis menggunakan *fishbone diagram* untuk mengidentifikasi faktor penyebab masalah [7]. Identifikasi masalah berdasarkan *people, technology,* dan *process* dapat dilihat pada Gambar 1.1 yang menggambarkan *fishbone diagram*.



Gambar 1. 1. *Fishbone diagram* identifikasi masalah

Berdasarkan diagram *fishbone* yang terlihat pada Gambar 1 masalah dibagi menjadi tiga ketegori, yaitu *people, technology,* dan *process.* Berikut penjelasan mengenai ketiga kategori tersebut:

a. *People* (orang)

   Berdasarkan kategori ini terdapat hasil identifikasi masalah seperti, tidak ada tim secara spesifik dalam hal keamanan aplikasi. Tim pengembang aplikasi XYZ belum memiliki tim khusus dalam mengawasi keamanan secara teknis, yang memungkinkan dapat menyebabkan terjadinya celah dalam proses pengembangan aplikasi. Dalam kategori *people* juga teridentifikasi masalah *human error.* Kesalahan manusia atau *human error* juga pernah terjadi ketika proses pengembangan aplikasi, sehingga terjadi masalah pada aplikasi. Masalah akibat *human error* pada saat pengembangan atau pemeliharaan aplikasi dapat berdampak pada keamanan aplikasi dan data pengguna.

b. *Technology* (teknologi)

   Dalam kategori ini ditemukan masalah, seperti implementasi API versi 2 yang lebih aman belum merata. Pada aplikasi XYZ, penerapan API versi 2 ini belum sepenuhnya, sehingga masih terdapat bagian yang rentan terhadap ancaman atau risiko yang terjadi. Proses *login* ke aplikasi XYZ belum ada penerapan autentikasi yang kuat dan hanya memasukkan *username* dan *password* saja. Hal ini dapat memungkinkan terjadinya risiko akses tidak sah, sehingga dapat terjadi pencurian data pengguna.

c. *Process* (proses)

   Untuk ketegori proses terdapat beberapa hasil identifikasi masalah seperti, beberapa data krusial atau sensitif belum dienkripsi, terjadinya *bug* dalam *coding,* serta belum ada penerapan standar keamanan informasi seperti ISO 27001. Data-data yang belum terenkripsi ini menjadi lebih rentan terhadap akses yang tidak sah, sehingga dapat menimbulkan risiko atau ancaman lainnya. Adanya *bug* dalam proses pengembangan aplikasi XYZ menandakan masih terdapat kelemahan yang perlu ditangani untuk menjaga keamanan dan stabilitas aplikasi.

1.3. Tujuan Penelitian

Dalam proses penelitian ini ada beberapa tujuan yang ingin terpenuhi, diantaranya sebagai berikut:

1. Mengevaluasi kondisi keamanan informasi terhadap aplikasi XYZ dengan menggunakan metode FMEA (*Failure Mode and Effect Anlysis*) dan standar ISO 27001: 2022.
2. Memberikan rekomendasi kontrol keamanan informasi berdasarkan standar ISO 27002: 2022.

1.4. Pertanyaan Penelitian

Berlandaskan identifikasi masalah yang sudah dijelaskan pada poin sebelumnya, terdapat beberapa pertanyaan penelitian yang dapat menjadi fokus pembahasan penelitian ini. Pertanyaan penelitian ini dirumuskan sebagai berikut:

1. Bagaimana evaluasi keamanan informasi berdasarkan metode FMEA dan ISO 27001:2022 pada aplikasi XYZ?
2. Bagaimana rekomendasi kontrol keamanan informasi berdasarkan standar ISO 27002:2022?

1.5. Ruang Lingkup Penelitian

Pada penelitian ini, terdapat beberapa ruang lingkup yang ditetapkan sebagai berikut:

1. Penelitian ini mengevaluasi keamanan informasi pada aplikasi XYZ versi 1.5.7.
2. Menggunakan standar ISO 27001:2022 yang berfokus pada manajemen keamanan informasi.
3. Memanfaatkan standar ISO 27002:2022 sebagai panduan praktis untuk menerapkan kontrol keamanan dan mengatasi risiko.

Penelitian ini menggunakan metode *Failure Mode and Effect Analysis* (FMEA) untuk melakukan proses penilaian risiko yang mungkin terjadi pada aplikasi XYZ.

1.6. Sistematika Penelitian

Dalam konteks keamanan informasi saat ini aplikasi XYZ hanya melakukan *testing* setelah proses *development* dan belum menerapkan standar keamanan seperti ISO 27001:2022 yang merupakan standar berfokus pada manajemen keamanan informasi. Sehingga pada penelitian ini berfokus pada evaluasi keamanan informasi aplikasi XYZ dengan memanfaatkan metode FMEA (*Failure*

Mode and Effect Analysis) serta standar ISO 27001:2022. Metode dan standar yang digunakan bertujuan untuk membantu dalam mengidentifikasi, mengklasifikasi, dan memberi rekomendasi mitigasi risiko keamanan. Penelitian ini dimulai dari penentuan objek penelitian, kemudian dilanjut dengan studi literatur untuk memperkuat teori penelitian serta merancang metodologi penelitian secara sistematis.

Kemudian pada tahap selanjutnya membuat dokumen *audit checklist* serta dokumen penilaian RPN. Pengisian dokumen-dokumen ini dilakukan dengan tim internal XYZ, dan hasil dari dokumen-dokumen tersebut dimanfaatkan sebagai data untuk penelitian ini. Setelah melakukan pengumpulan data dengan pengisian dokumen tersebut, selanjutnya dilakukan penyusunan rekomendasi mitigasi terhadap risiko yang sudah diidentifikasi serta melakukan validasi kepada tim internal XYZ terhadap rekomendasi yang diberikan. Tahapan terakhir pada penelitian ini adalah penarikan kesimpulan serta saran bagi organisasi maupun pada penelitian selanjutnya.