BAB 1 PENDAHULUAN

1.1 Latar Belakang

Peran Teknologi Informasi (TI) saat ini menjadi suatu kebutuhan dalam sebuah organisasi. Dengan adanya TI diharapkan mampu menunjang proses bisnis sehingga dapat mendukung dalam pencapaian visi, misi, dan tujuan organisasi. Hal ini penerapan TI tentu menjadi aset penting bagi keberlangsungan kehidupan di suatu organisasi dalam menjalankan strategi bisnisnya. Oleh karena itu dalam penerapan TI perlu adanya sebuah keamanan informasi agar terlindungi dari pihak yang tidak memiliki wewenang untuk mengetahui atau mengelolanya.

Keamanan informasi merupakan salah satu aspek penting yang harus diperhatikan oleh organisasi pada TI yang dimiliki [1]. Dimana keamanan informasi memiliki tiga aspek utama diantaranya *confidentiality* (kerahasiaan) yaitu data dan informasi hanya dapat diakses oleh orang yang berhak, *integrity* (integritas) yaitu perlindungan terhadap keaslian data dan informasi, dan *availability* (ketersediaan) yaitu melindungi ketersediaan data dan informasi sehingga data dapat diakses pada saat dibutuhkan.

Pada penelitian ini TI yang dimaksud dan dijadikan sebagai objek adalah *Enterprise Architecture* (EA). Menurut definisi, EA merupakan suatu pendokumentasian yang memuat elemen proses bisnis, teknologi, informasi data, dan aplikasi dengan sistem yang saling terintegrasi [2] . Di dalam EA terdapat data atau informasi yang terpusat sehingga dapat membantu organisasi dalam menyelaraskan antara strategi bisnis dengan strategi TI agar lebih optimal serta dapat membantu dalam pengambilan keputusan oleh pihak top *management* dalam menjalankan strategi nya. Dari hal tersebut maka dapat meningkatkan integritas, serta kualitas dari sebuah organisasi.

Institut Teknologi Telkom Surabaya (ITTelkom Surabaya) dengan beralamat di Jalan Ketintang No. 156, Surabaya yang baru berdiri pada tahun 2018 merupakan perguruan tinggi swasta dibawah naungan Yayasan Pendidikan Telkom (YPT) yang mempunyai visi menjadi perguruan tinggi berstandar internasional yang berbasis *Information and Communication Technology* (ICT). Di tahun 2021 hingga

saat ini, ITTelkom Surabaya memiliki 11 program studi yang terbagi dalam 2 fakultas yaitu Fakultas Teknologi Informasi dan Bisnis (FTIB) dan Fakultas Teknik Elektro dan Industri Cerdas (FTEIC). Adapun dari 11 program studi tersebut terbagi diantaranya 7 program studi berada di FTIB dan 4 program studi berada di FTEIC [3]. Hal tersebut menunjukkan bahwa EA sangat penting dalam menunjang dan mencapai strategi untuk kesuksesan terhadap visi institusi. Adapun objek yang diambil pada penelitian ini adalah EA ITTelkom Surabaya.

Dengan begitu data atau informasi pada EA sangat penting adanya dan harus dijaga karena terkait dengan kelangsungan proses bisnis. Didasari dengan EA yang merupakan penerapan dari TI tentu memiliki adanya ancaman dan risiko terhadap keamanan informasi. Dalam TI, risiko didefinisikan sebagai hasil dari kerentanan sistem terhadap ancaman yang ditimbulkannya bagi organisasi [4]. Risiko keamanan informasi yang memungkinkan seperti modifikasi data secara ilegal, maupun kesalahan manusia (sumber daya manusia), dan sebagainya [5].

Berdasarkan hasil wawancara dengan informan Wakil Dekan FTIB selaku pengembang EA yang terlampir pada Lampiran 4, EA dibangun pada awal tahun 2022, EA digunakan sebagai *blueprint* organisasi untuk menyelaraskan visi dan misi organisasi, serta proses bisnis. Saat ini EA ITTelkom Surabaya terbilang masih baru dan dalam pengembangannya masih dengan menggunakan kerangka kerja TOGAF – ADM kemudian di *generate* menjadi sebuah *HyperText Markup Language* (HTML) sehingga dapat berupa *website.* Namun saat ini data yang ada pada EA masih dapat terlihat secara keseluruhan tanpa adanya pembagian hak akses informasi. Selain itu ditambah dengan pernyataan informan lain selaku staf SPMP dan pengembang EA yang terlampir pada Lampiran 4 bahwa sejak dilakukan pengembangan EA belum pernah dilakukan penilaian risiko keamanan informasi. Sehingga hal tersebut memiliki potensi adanya risiko terhadap keamanan informasi yang ada pada EA.

Dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang sistem manajemen pengamanan informasi pasal 1 ayat 5 berbunyi sistem manajemen pengamanan informasi adalah peraturan keajiban bagi penyelenggara sistem elektronik dalam penerapan manajemen pengamanan

informasi berdasarkan asas risiko. Berdasarkan temuan *Accenture*, serangan *cybercrime* meningkat 67% selama lima tahun terakhir dan jumlah terbanyak nya adalah pada ancaman keamanan *website*. Berdasarkan hal tersebut sehingga perlunya untuk melakukan manajemen risiko keamanan informasi pada EA. Ada banyak cara untuk melakukan manajemen risiko salah satunya adalah dengan berpedoman pada persyaratan Standar Manajemen Keamanan Informasi (SMKI) ISO 27001:2013.

ISO 27001:2013 lebih menekankan pada persyaratan keamanan informasi yang dituangkan dalam 10 klausa umum dan detail 114 kendali (*control*) yang terbagi dalam 14 domain dan menggunakan pendekatan aset informasi (*Asset Approach*) dalam manajemen risikonya. ISO 27001:2013 merupakan prosedur terdokumentasi dan praktek - praktek *standard* untuk manajemen sistem, yang bertujuan menjamin keamanan informasi [6]. Manajemen risiko dapat digunakan untuk melihat risiko terkait keamanan, termasuk sumber risiko internal yang dapat berasal dari SDM (sumber daya manusia) yang dimiliki maupun risiko eksternal. Oleh karena itu, risiko keamanan informasi merupakan hal yang perlu diperhatikan oleh organisasi dan individu.

Penelitian ini menggunakan klausul utama pada ISO 27001:2013 yaitu klausul 6 (perencanaan) karena sesuai dengan persyaratan ISO 27001 adalah tentang perencanaan, dan khususnya perencanaan tindakan untuk mengatasi risiko dan peluang [7]. Klausul 7 (dukungan) sesuai dengan persyaratan ISO 27001 untuk menyediakan sumber daya yang cukup untuk penerapan, pemeliharaan, penetapan, dan peningkatan berkelanjutan dari sistem manajemen keamanan informasi [7]. Klausul 8 (operasi) sesuai dengan persyaratan ISO 27001:2013 untuk meminta organisasi melakukan perencanaan, penerapan dan pengendalian proses yang diperlukan untuk memenuhi persyaratan untuk menerapkan tindakan yang ditentukan dalam klausul 6 [7].

Penelitian ini dalam melakukan analisis risiko menggunakan metode *Failure Mode and Effect Analysis* (FMEA). FMEA merupakan proses yang terorganisasi untuk meningkatkan perlindungan terhadap aset informasi dalam mencegah terjadinya mode kegagalan, dampak, dan efek potensial yang dihasilkan dengan menganalisis dan mengelompokkan potensi risiko [8]. FMEA memiliki

perhitungan terkait *Risk Priority Number* (RPN) berdasarkan nilai *Severity* (keparahan), *Occurance* (kemungkinan), dan *Detection* (tingkat deteksi) kemudian dari hasil perhitungan dikelompokkan berdasarkan level risiko sehingga dari hal tersebut dapat diketahui potensi risiko paling tinggi dan memudahkan dalam pengambilan keputusan apakah perlu dimitigasi atau tidak [9]. Metode FMEA juga memiliki kelebihan yaitu dapat memastikan potensi kecacatan atau kegagalan dengan meninjau ulang desain, sistem, dari suatu produk maupun proses. Dalam penelitian ini juga dilakukan rencana penanganan / rekomendasi berdasarkan kontrol annex A ISO 27001:2013 yang nantinya disesuaikan dengan hasil risiko beserta penyebab potensial nya.

Berdasarkan beberapa dari hasil penelitian terdahulu, misalnya oleh Munaroh, Lailatul and Amrozi, Yusuf and Nurdian, Rizky Agung (2020) dengan judul "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013". Hasil Penelitian menunjukkan terdapat 22 *cause failure* yang menyebabkan terjadinya risiko pada keamanan aset TI di Bidang Perdagangan Dalam Negeri (PDN). Terdapat 11 *cause failure* yang memiliki level tinggi dengan rentan nilai 400 – 175 dari hasil perhitungan RPN dengan menggunakan metode FMEA serta dari hasil *cause failure* tersebut dilakukan mitigasi risiko berdasarkan ISO 27001:2013 agar tindakan mitigasi yang dilakukan sesuai dengan standar [10]. Selain itu juga terdapat penelitian oleh Naniek Utami Handayani, Mochammad Agung Wibowo, Diana Puspita Sari, Yoga Satria, Akbar Romadhona Gifari (2018) dengan judul "Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode *Failure Mode Effect And Analysis* Berbasis *Framework* ISO 27001". Hasil penelitian menunjukkan terdapat 25 *risk agent* pada SIFT UNDIP yang dikategorikan menjadi empat jenis aset. Risiko tertinggi pada kategori *High Level Risk* adalah risiko ketergantungan terhadap karyawan dengan nilai *Risk Priority Number* (RPN) sebesar 80 [11]. Penelitian lain oleh Eraldy Wardhanu, (2020) dengan judul "Analisis Risiko Sistem Manajemen Aset Berbasis ISO 27001:2013 Menggunakan Metode *Failure Mode and Effect Analysis* Pada PT. Tirta Investama". Hasil penelitian menunjukkan diperoleh 12 risiko dan 24 kejadian risiko. Terdapat risiko yang memiliki kejadian risiko lebih dari satu dikarenakan perbedaan penyebab dari hasil melakukan gap *analysis* berdasarkan annex klausul

ISO 27001:2013. Dan nilai risiko paling tinggi berdasarkan level risiko *very high* dengan nilai RPN 48 [12]. Sehingga dapat disimpulkan pada penelitian sebelumnya yaitu titik perbedaan pada objek penelitian dan klausul ISO 27001:2013 yang digunakan pada penelitian. Namun untuk keterkaitan penelitian yaitu menggunakan metode FMEA sebagai analisis risiko dan menggunakan standar ISO 27001:2013 sebagai proses penilaian risiko dan kontrol untuk penanganan risiko.

Berdasarkan dari uraian latar belakang diatas, maka penulis mengambil topik penelitian dengan judul "Penilaian Risiko Keamanan EA ITTelkom Surabaya Menggunakan Metode *Failure Mode Effect and Analysis* (FMEA) Berbasis ISO 27001". Hal ini diharapkan nantinya dapat berguna sebagai bahan perbaikan pada pengembangan EA ITTelkom Surabaya kedepannya berdasarkan dari hasil penilaian risiko sehingga dapat meminimalisir adanya risiko ancaman, serta EA ITTelkom Surabaya dapat terimplementasikan sesuai dengan standar ISO 27001:2013.

1.2 Rumusan Masalah

Berdasarkan dari hasil uraian latar belakang diatas, maka rumusan dalam penelitian ini adalah:

1. Apa saja risiko keamanan yang terdapat pada EA ITTelkom Surabaya?
2. Bagaimana hasil penilaian risiko keamanan EA ITTelkom Surabaya menggunakan metode FMEA yang berbasis ISO 27001:2013?
3. Bagaimana rekomendasi tindakan mitigasi / kontrol terhadap risiko keamanan pada EA ITTelkom Surabaya berdasarkan ISO 27001:2013?

1.3 Tujuan dan Manfaat

Berdasarkan dari rumusan masalah yang telah dijabarkan, tujuan dari penelitian ini yaitu :

1. Mengetahui apa saja risiko keamanan yang ada pada EA ITTelkom Surabaya.
2. Mengetahui hasil penilaian risiko keamanan informasi dengan berdasarkan metode FMEA yang berbasis ISO 27001:2013 pada EA ITTelkom Surabaya.
3. Memberikan rekomendasi tindakan mitigasi / kontrol terhadap risiko keamanan pada EA ITTelkom Surabaya berdasarkan ISO 27001:2013.

Adapun manfaat yang didapatkan dari penelitian ini yaitu:

Secara teoritis yaitu:

1. Dari hasil penelitian yang dilakukan diharapkan bisa menambah wawasan dan ilmu pengetahuan bagi peneliti maupun pembaca.
2. Hasil dari penelitian diharapkan dapat memberikan kontribusi bagi institusi mengenai implementasi manajemen risiko pada EA ITTelkom Surabaya, dan memungkinkan dapat dijadikan acuan untuk penelitian selanjutnya.

Secara praktis yaitu:

1. Bagi Pihak SPMP dan PUTI
   Hasil identifikasi dan penilaian risiko yang dihasilkan dapat dijadikan sebagai bahan perbaikan dan mencegah adanya risiko kedepannya yang ada pada EA.
2. Bagi Peneliti
   Dapat mengetahui dan memahami bagaimana cara melakukan penilaian risiko dan menganalisis risiko menggunakan metode FMEA berbasis ISO 27001 serta dapat menyelesaikan tugas akhir (skripsi) dengan tepat waktu.

1.4 Batasan Masalah

Berdasarkan rumusan masalah diatas, maka batasan pada penelitian ini, yaitu :

1. Pengembangan EA bukan bagian dalam penelitian ini melainkan hanya berfokuskan pada penilaian risiko.
2. ISO yang digunakan pada penelitian ini adalah ISO 27001:2013.
3. Klausul ISO 27001:2013 yang digunakan pada penelitian ini hanya mencakup 3 klausul yaitu klausul 6 : *planning*, klausul 7 : *support*, klausul 8 : *operation*.
4. Proses penilaian risiko berfokuskan pada klausul ISO 27001:2013 yaitu klausul 6 : *planning.*
5. Penelitian difokuskan pada bagian *software, hardware, people,* dan data terhadap risiko EA ITTelkom Surabaya.
6. Objek informan penelitian hanya difokuskan pada unit bagian PUTI, SPMP, dan Wakil Dekan FTIB ITTelkom Surabaya.