BAB 1
PENDAHULUAN

1.1 Latar Belakang

Berkembangnya teknologi informasi yang sangat pesat saat ini, menuntut hampir sebagian besar instansi pendidikan Indonesia bersaing kuat menciptakan pemanfaatan teknologi informasi. Teknologi informasi merupakan aset penting dalam mengelola dan menghasilkan informasi [1] yang bisa membuat perusahaan memiliki daya saing dan nilai tambah. Dengan memanfaatkan teknologi informasi, atas dasar prinsip penerapan ICT *(Information Communication Technologies)* dalam proses pembelajaran memungkinkan segala kegiatan yang berhubungan dengan informasi menjadi lebih mudah dan praktis. Namun seiring dengan manfaat yang diperoleh, teknologi informasi dalam penyelenggaraannya mengandung berbagai risiko.

Risiko adalah tantangan yang harus dihadapi di masa yang akan datang karena wujudnya yang belum diketahui secara pasti. Namun usaha untuk mengurangi atau memperkecil dampak yang ditimbulkan risiko tetap dapat dilakukan dengan melakukan pengendalian risiko terhadap ketidakpastian [2]. Dikutip dari antaranews.com pada November 2014 lalu, *Cisco Midyear Security Report* memaparkan temuannya terkait ancaman keamanan teknologi informasi di kalangan perusahaan. Diantaranya risiko infeksi *malware*, menyebar melalui situs-situs yang sengaja mendistribusikannya. 94 persen jaringan milik pelanggannya teridentifikasi memiliki lalu lintas ke situs tersebut. Pada pertengahan pertama tahun 2014 *Cisco Midyear Secuirty Report* juga menemukan adanya peningkatan kecil yang tidak wajar pada *malware* yang memiliki risiko keamanan TI. Sancoyo Setiabudi, *Country Manager* untuk *Cisco* Indonesia berkata, "Tantangan dan risiko merupakan hal yang tidak dapat dihindari, terutama ketika berbicara mengenai kemajuan, pertumbahan, dan inovasi." Oleh

sebab itu diperlukan penerapan manajemen risiko dalam menjalankan suatu proses bisnis utama dan pendukung.

Agar dapat mengimplementasikan manajemen risiko yang esfisien dan efektif, diperlukan adanya keterlibatan dan pengawasan semua *stakeholder* dalam penyusunan penerapan kebijakan dan prosedur penggunaan teknologi informasi yang baik dan benar serta pengukuran untuk pengendalian dari risiko teknologi informasi yang berkesinambungan. Ada banyak kerangka kerja yang dapat digunakan perusahaan dalam penerapan manajemen risiko. Salah satu diantara banyak kerangka kerja yang ada dipilih *Operationally Critical Threat, Asset and Vulnerability Evaluation* (OCTAVE) sebagai kerangka kerja yang dapat mengidentifikasi, menganalisa dan mengawasi pengelolaan risiko keamanan informasi [3]. Untuk melengkapi proses analisa dari risiko TI, dipilih FMEA (*Failure Mode and Effect Analysis*) sebagai prosedur dalam penilaian risiko TI yang akan dan mungkin dihadapi, dengan memberitahukankan tentang informasi dasar mengenai kendala risiko, proses, dan desain.

Universitas Dian Nuswantoro mempunyai banyak aktivitas utama dengan membagi aktivitas tersebut kedalam 2 bagian besar aktifitas utama, pertama yang dilakukan oleh PT. Dian Nuswantoro Teknologi dan Informasi (Dinustek) yang bertanggungjawab pada bagian *hardware*, dan *network* sedangkan pada PSI (Pusat Sistem dan Informasi) bertanggung jawab pada bagian *software* dan *Data*. Pada dinustek aktifitas utama yang dilakukan yaitu *maintenance*, jika terjadi gangguan pada semua jaringan yang ada di Universitas Dian Nuswantoro baik yang sifatnya internal maupun eksternal. Dinustek tidak hanya melakukan *maintenance* terhadap jaringan saja tetapi juga melakukan *maintenance* terhadap *hardware* yang ada didalam proses bisnis utama yang ada di Universitas Dian Nuswantoro seperti *server*, komputer, *router, switch* dll. Sedangkan untuk bagian Pusat Sistem dan Informasi (PSI) yaitu yang menangani *software* dan juga *data* yang ada di Universitas Dian Nuswantoro. Aktifitas utama PSI ini melakukan *coding, maintenance* dan juga melakukan *education*.

Disadari betul oleh pihak PT. Dian Nuswantoro Teknologi dan Informasi (Dinustek) dan PSI adanya risiko TI dan dampak risiko TI yang mungkin muncul dalam penyelenggaraan unit pelaksanaan teknis jaringan komputer dan fasilitas pendukung yang ada di Universitas Dian Nuswantoro. Karena seringnya terjadi kegagalan pada jaringan terutama pada bagian *server* yang sering mengalami *down* pada saat *input* KRS dan sering terjadi kegagalan atau kerusakan sistem dikarenakan *human error*. Dan di Dinustek dan PSI belum ada prosedur yang memiliki standar keamanan dalam mengelola aset-aset TI. Sehingga dalam kegiatan operasional, manajamen jaringan komputer dan fasilitas pendukung yang ada pada Universitas Dian Nuswantoro perlu dilakukan pengelolaan risiko teknologi informasi. Pengelolaan risiko TI pada jaringan komputer dan fasilitas pendukung Dinustek dan PSI dengan menggunakan kerangka kerja OCTAVE diharapkan dapat memberi idenfikasi yang jelas terkait aset kritis TI dan ancaman yang menimbulkan risiko TI, analisa dan evaluasi dari risiko TI yang mungkin muncul sehingga dapat memberi usulan strategi dan rencana implementasi manajemen risiko yang baik sesuai standar ISO 27001 dan 27002 dalam mengidentifikasi setiap *control* yang diperlukan untuk mengurangi risiko dan sejauh mana harus diterapkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan di atas, berikut adalah rumusan masalah yang akan diselesaikan dalam penelitian ini:

1. Bagaimana analisa risiko aset kritis terhadap risiko-risiko teknologi informasi pada Universitas Dian Nuswantoro?
2. Bagaimana evaluasi risiko yang terkait dengan aset teknologi informasi pada Universitas Dian Nuswantoro?
3. Bagaimana hasil penilaian mitigasi risiko aset teknologi informasi yang dimiliki Universitas Dian Nuswantoro?

1.3 Batasan Masalah

Dalam pengerjaan penelitian ini, terdapat beberapa batasan masalah yang perlu diperhatikan, yaitu sebagai berikut:

1. Metode penelitian yang dilakukan adalah observasi atau pengamatan peneliti dengan menggunakan kerangka kerja FMEA dan OCTAVE.
2. Penilaian terhadap analisa risiko yang digunakan adalah kerangka kerja FMEA.
3. Dalam perencanaan dan pengembangan analisa risiko aset TI menggunakan standar ISO 27001 dan 27002.
4. *Interview protocol* dilakukan pada Sistem Administrator / Network Admin Dinustek dan Sistem Administrator PSI Universitas Dian Nuswantoro.

1.4 Tujuan Penelitian

Tujuan pengerjaan penelitian ini adalah sebagai berikut:

1. Mengetahui aset kritis teknologi infomasi dan ancaman pada Universitas Dian Nuswantoro yang sering muncul terhadap aset tersebut.
2. Menghasilkan hasil analisa evaluasi risiko terhadap teknologi informasi pada Universitas Dian Nuswantoro.
3. Mengetahui langkah-langkah rencana mitigasi yang tepat terhadap aset TI Universitas Dian Nuswantoro.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat antara lain:

1. Universitas Dian Nuswantoro mendapatkan informasi mengenai risiko yang mungkin terjadi serta tingkat kerawanan pada aset teknologi informasi yang dimiliki oleh organisasi.
2. Pihak Universitas Dian Nuswantoro juga mengetahui evaluasi efektivitas dari tindakan yang diambil dari risiko yang mungkin terjadi dari penggunaan TI.