BAB I

PENDAHULUAN

1.1 Latar Belakang

Universitas Airlangga (UA) adalah salah satu perguruan tinggi di Indonesia yang mengembangkan sumber daya manusia untuk menunjang dunia pendidikan. Selain itu Universitas Airlangga memiliki moto *excellence with morality* dan mempunyai visi menjadi universitas yang mandiri, inovatif, terkemuka ditingkat nasional dan berupaya untuk berkembang menjadi *world class university*. Salah satu cara untuk menjadi *world class university* dengan memaksimalkan penggunaan sistem informasi yang mendukung kegiatan belajar-mengajar dan melingkupi semua sivitas akademik yang terintregasi antara pihak rektorat, fakultas, mahasiswa hingga wali mahasiswa.

Proses akademika UA ditunjang oleh sebuah organisasi yang bertanggung jawab dalam mengembangkan teknologi informasi untuk mengelola sistem yang digunakan baik untuk mahasiswa, pegawai, rektorat maupun dosen. Direktorat Sistem Informasi (DSI) sebagai organisasi internal yang bertujuan mengoptimalkan pelayanan akademik juga membantu pihak rektorat dalam hal penyelenggaraan sistem informasi. DSI memiliki banyak aset Teknologi Informasi (TI) yang dipakai untuk menunjang proses bisnis DSI.

DSI dibagi dalam menjadi empat seksi yaitu seksi *Informatics Brandings*, *Networking*, *Data Security*, dan Seksi Integrasi Sistem dan Pengembangan Aplikasi. Seksi *Informatics Brandings* bertanggung jawab dalam pengelolaan dan layanan informasi. Seksi *Networking* bertanggung jawab dalam tata kelola jaringan, hingga rekomendasi tentang penggunaan jaringan atau *bandwith*. Seksi *Security Data* bertanggung jawab dalam memastikan seluruh tata kelola keamanan data sistem berjalan baik, hingga dokumentasi terhadap hal yang dianggap penting terkait dengan pengamanan data. Seksi Integrasi Sistem dan Pengembangan Aplikasi bertanggung jawab dalam mengembangkan aplikasi sistem untuk mencapai tujuan organisasi, melakukan pengawalan terhadap Integrasi Sistem, memenuhi permintaan fakultas unit sehubungan dengan pembuatan dan atau pengembangan aplikasi program, hingga dokumentasi terhadap hasil pengembangan aplikasi.

Setiap seksi yang telah disebutkan memiliki aset yang berbeda sesuai dengan kebutuhan. Beberapa aset yang dimiliki oleh DSI yaitu, *hardware* seperti komputer, laptop, server dan *storage*, aset s*oftware* seperti Microsoft, Kaspersky, Ncomputing dan sebagainya, aset sumber daya manusia seperti keahlian. Aset informasi kontrak hukum dan topologi, aset s*ervices* seperti, *supplier* atau *vendor* yang melakukan *maintanance*, *Intangible* aset yang tidak terwujud reputasi organisasi dan *brand*.

DSI mulai mempelajari manajemen risiko pada tahun 2012 dan mulai menerapkan pada tahun 2013 dengan menggunakan standar ISO 31000. Manajemen risiko akan dievaluasi ketika audit *internal,* rapat tinjauan manajemen dan audit *external*. Namun meskipun sudah menerapkan pengelolaan risiko masih ditemukan

risiko yang muncul seperti ketika DSI mendapatkan suatu aset baru maka pihak DSI melakukan dokumentasi yang bertujuan untuk mencatat aset DSI yang akan dilaporkan kepada pihak *top level management.* Permasalahan timbul ketika perpindahan kepemilikan tanggung jawab dari DSI yang menyebabkan hilangnya aset tersebut, contohnya perpindahan notebook dari DSI ke bidang lain, saat dilakukan pengecekan atau kontrol terhadap notebook tersebut tidak ditemukan dimana posisi notebook tersebut saat ini, hal itu dikarenakan pada saat notebook dipindahkan ke bidang lain pencatatan aset tidak dilakukan dengan benar. DSI sebagai organisasi internal yang telah menerapkan teknologi informasi tentu saja akan menemukan risiko-risiko yang apabila terjadi bisa berdampak terhadap aset-aset TI. Oleh karena itu, pihak DSI membutuhkan sebuah kerangka kerja mengenai manajemen risiko yang berfungsi sebagai acuan pengelolaan risiko di DSI.

Manajemen risiko adalah mengurangi terjadinya hal-hal diluar dugaan dengan melakukan pendekatan terorganisasi untuk menentukan risiko-risiko yang potensial. Selanjutnya risiko-risiko potensial tersebut dapat diketahui akibat buruknya yang tidak diharapkan dan dapat dikembangkan rencana respon yang sesuai dengan risiko tersebut (Pressman, 2005). Dalam mengelola risiko yang ada dibutuhkan sebuah kerangka kerja yang digunakan sebagai pedoman. Salah satu pedoman yang digunakan adalah COBIT (*Control Objective for Information and Related Technology*). Menurut Campbell (2005), COBIT merupakan suatu cara untuk menerapkan tata kelola TI. COBIT berupa kerangka kerja yang harus digunakan oleh suatu organisasi bersamaan dengan sumber daya lainnya untuk membentuk suatu standar yang umum berupa panduan pada

lingkungan yang lebih spesifik. Secara terstruktur, COBIT terdiri dari seperangkat *management practices* untuk bidang teknologi informasi yang dirancang untuk memungkinkan tahapan bagi audit.

Kerangka kerja COBIT 5 terdiri dari lima domain yaitu *Evaluate, Direct and Monitor (EDM); Align, Plan and Organise (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); Monitor, Evaluate and Asses (MEA).* Salah satu proses yang menjelaskan terkait manajemen risiko adalah proses *Risk Manage* pada domain *Align, Plan and Organise*.

Proses APO12 merupakan sebuah proses dimana secara terus-menerus mengidentifikasi, menilai dan mengurangi risiko yang berhubungan dengan IT sesuai dengan batas atau level toleransi yang dibuat oleh manajemen eksekutif perusahan yang bertujuan mengintegrasikan manajemen yang berkaitan dengan risiko perusahaan dengan *Enterprise Risk Management* secara keseluruhan dan menyeimbangkan biaya dan keuntungan dari pengelolaan TI yang berhubungan dengan risiko perusahaan. Di dalam proses APO12 *Manage Risk* ini terdapat pembahasan mengenai seberapa besar tingkat kesadaran manajemen dalam mengelola risiko dan mengukur kematangan pengelolaan risiko berdasarkan *capability model* yang didasarkan pada ISO.IEC 27001:2005, ISO/IEC 27002:2011, ISO/IEC 3100.

Untuk memenuhi pengukuran tingkat pengelolaan risiko teknologi informasi yang efektif, perlu dilakukan penilaian terhadap tingkat kesadaran manajemen dalam mengelola risiko dan menganalisis tingkat kapabilitas di DSI UA menggunakan kuesioner yang mengacu pada COBIT 5 proses APO12, sehingga dapat di identifikasi

tingkat kesadaran manajemen dan tingkat kapabilitas DSI UA. Kuesioner I dibuat untuk mengukur tingkat kesadaran manajemen, butir pertanyaan dibuat mengacu pada KMP proses APO12 dan Kuesioner II dibuat untuk mengukur tingkat kapabilitas kondisi saat ini dan lima tahun kedepan yang diharapkan. Hasil dari kuesioner dibuat untuk merancang saran dan rekomendasi untuk acuan yang tepat dalam melakukan perbaikan pengelolaan risiko TI di DSI UA.

Berdasarkan latar belakang uraian tersebut, penelitian ini mengukur serta menganalisis pengelolaan risiko di DSI UA dengan menggunakan kerangka kerja COBIT 5. Dengan demikian penelitian ini diangkat dengan judul "Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 *Manage Risk"*.

1.2 Rumusan Masalah

Berikut merupakan rumusan masalah yang didapat dari penulisan skripsi ini adalah:

1. Bagaimana mengidentifikasi dan menganalisis tingkat kesadaran manajemen dalam pengelolaan risiko di DSI UA?
2. Bagaimana mengidentifikasi dan menganalisis *capability level* saat ini (*as-is*) dengan yang diharapkan (*to-be*) DSI Universitas Airlangga dalam mengelola risiko sesuai dengan acuan COBIT 5 proses APO12?
3. Bagaimana merancang strategi pengelolaan risiko yang efektif berdasarkan hasil analisis?

1.3 Tujuan Penelitian

Tujuan dari penelitian skripsi ini adalah sebagai berikut:

1. Mengetahui tingkat kesadaran manajemen dalam pengelolaan risiko di DSI.
2. Mengidentifikasi kesadaran dan menganalisis *Capability level* kondisi (*as-is*) saat ini dan (*to-be*) harapan yang ada pada proses APO12 Risk Management di DSI Universitas Airlangga.
3. Mendefinisikan suatu rancangan saran dan rekomendasi sehingga diperoleh acuan yang tepat dalam melakukan perbaikan mengelola risiko TI di DSI Universitas Airlangga.

1.4 Manfaat Penelitian

1. Hasil penelitian dapat digunakan sebagai panduan untuk mengetahui tingkat kesadaran DSI UA dalam pengelolaan risiko TI.
2. Hasil dari penelitian ini dapat digunakan sebagai masukan untuk DSI Universitas Airlangga dalam mencapai kondisi operasionalnya yang ideal terkait mengelola risiko TI yang akan berdampak pada proses bisnis.

1.5 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Pengerjaan penelitian ini berdasarkan data yang diberikan oleh pihak DSI Universitas Airlangga terkait dampak risiko yang mengancam jaringan.
2. Pemilihan responden untuk pengisian kuesioner dan wawancara dilakukan berdasarkan RACI *chart* yang disesuaikan dengan struktur organisasi DSI Universitas Airlangga.

3. Pengukuran manajemen risiko hanya dilakukan pada bagian networking yang meliputi jaringan, perangkat lunak dan perangkat keras.