

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada saat ini banyak perguruan tinggi telah memanfaatkan teknologi web sebagai sarana untuk melayani mahasiswa dalam bidang akademik. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa perguruan tinggi memilihnya untuk pelayanan akademik. Teknologi web memberikan kemudahan untuk mengakses informasi cepat dan murah yang disediakan oleh website maupun pustaka digital. Dengan kelebihanannya tersebut maka banyak organisasi yang membangun sistem informasi berbasis web (Alhendawi & Baharudin, 2013; Nikolaidou & Anagnostopoulos, 2003). Meskipun demikian teknologi web rentan terhadap sabotase, serta tindak kejahatan (Suduc et al., 2010). Menurut Rao dan Pant (2010) aplikasi web memiliki sisi kerentanan yang dapat menjadi ancaman namun sisi lainnya teknologi web dapat mengatasi berbagai permasalahan seperti dapat digunakan dalam beberapa *platform* yang berbeda dan dapat dihubungkan dengan berbagai macam teknologi basis data.

Salah satu sisi kerentanan yang dapat dieksploitasi pada aplikasi berbasis web yaitu dari sisi penggunaan teknologi basis data, jenis serangan ini dikenal dengan istilah injeksi SQL (Doshi & Siddharth, 2010). Pada tahun 2014 injeksi SQL merupakan serangan yang paling banyak terjadi dengan persentase 8.1% (Ionescu, 2015), masih menurut Ionescu (2015) pada tahun yang sama malware menjadi penyumbang serangan terbesar kedua setelah DDos (Distributed denial-of-service). Selain itu, kesalahan konfigurasi juga menjadi salah satu jenis ancaman pada aplikasi berbasis web.

Ancaman pada sistem informasi tersebut yang apabila benar-benar terjadi dapat menyebabkan kerusakan sistem informasi sehingga menyebabkan gangguan terhadap operasional institusi dan pada akhirnya menimbulkan kerugian. Dampak kerusakan sistem informasi dapat menyebabkan kerugian secara finansial,

menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan (Maulana & Supangkat, 2006). Hal ini sejalan dengan apa yang diungkapkan oleh Suduc (2010) bahwa sistem informasi beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam, pencurian, kebakaran, lonjakan listrik dan perusakan. Risiko kerusakan logik mengacu kepada akses tidak sah, kerusakan secara sengaja maupun tidak disengaja pada sistem informasi dan data. Maulana & Supangkat (2006) mengungkapkan bahwa risiko adalah segala hal yang mungkin berdampak pada kemampuan organisasi dalam mencapai tujuannya.

Adanya risiko kerusakan sistem informasi yang mungkin berdampak bagi kelangsungan operasional organisasi dapat diantisipasi dengan mengelola risiko tersebut. Dengan manajemen risiko diharapkan dapat mengurangi dampak dari kerusakan sistem informasi yang diakibatkan oleh ancaman apabila terwujud (Maulana & Supangkat, 2006). Elky (2006) mengungkapkan bahwa dengan manajemen risiko diharapkan dapat memahami dan menanggapi faktor-faktor yang dapat menyebabkan kegagalan dalam hal kerahasiaan, integritas atau ketersediaan sistem informasi. Penilaian risiko merupakan bagian dari manajemen risiko (Maulana & Supangkat, 2006; Elky, 2006). Penilaian risiko dilakukan untuk mengukur seberapa besar risiko sering terjadi atau seberapa besar dampak dari risiko (Maulana & Supangkat, 2006). Penilaian risiko perlu dilakukan untuk mengetahui adanya ancaman serius yang dapat mengeksploitasi kerentanan baik yang diketahui maupun tidak diketahui (Radack, 2012).

Berkaitan dengan hal tersebut untuk maka perlu dilakukan penilaian risiko untuk mengetahui profil risiko, analisis terhadap risiko, kemudian melakukan respon terhadap risiko tersebut sehingga tidak terjadi dampak yang dapat ditimbulkan oleh risiko tersebut (Maulana & Supangkat, 2006). Penilaian risiko merupakan bagian penting dari keberhasilan mengelola strategi keamanan pada sistem informasi (Corland, 2014). Masih menurut Corland (2014) dengan penilaian risiko dapat membantu organisasi untuk mengidentifikasi aset sistem

informasi kritis dan membuat prioritas mitigasi. Proses penilaian risiko akan dilakukan pada sistem informasi akademik (SIMAK) yang terdapat di Universitas Negeri Siliwangi Tasikmalaya. SIMAK merupakan aplikasi berbasis web yang terhubung ke jaringan publik.

Metode OCTAVE Allegro akan dipilih sebagai kerangka kerja proses penilaian risiko yang akan dilakukan pada sistem informasi akademik (SIMAK). OCTAVE Allegro merupakan salah satu varian dari metode OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*). Menurut Woody (2006) OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamanan sistem informasi berbasis risiko. OCTAVE dikembangkan oleh *Software Engineering Institute (SEI)* Universitas Carnegie Mellon (Alberts et. al. 2009). OCTAVE Allegro merupakan metode yang disederhanakan dengan fokus pada aset informasi (Caralli, 2007).

Keating (2012) mengungkapkan bahwa OCTAVE Allegro menjadi salah satu pilihan metode penilaian risiko yang dapat digunakan di Perguruan Tinggi. Liu et. al (2009) dan West et. al (2002) menyatakan bahwa OCTAVE Allegro dan pendahulunya telah diterima secara luas oleh komunitas keamanan informasi sebagai alat praktis yang efektif terkait penilaian risiko sistem informasi. Terdapat sejumlah laporan tentang adaptasi metodologi ini dalam beberapa pekerjaan nyata berdasarkan pengamatan dan uji coba di lapangan (Goldman, 2009; Marek & Paulina, 2006).

1.2 Rumusan Masalah

Rumusan masalah untuk penelitian ini yaitu bagaimana menerapkan penilaian risiko dengan fokus pada layanan sistem informasi akademik di Perguruan Tinggi menggunakan metode OCTAVE Allegro.

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini yaitu penilaian risiko hanya dilakukan pada sistem informasi dengan fokus pada aset informasi kritis.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Mengidentifikasi, menganalisis dan mengelola risiko Sistem Informasi Akademik (SIMAK) di Perguruan Tinggi menggunakan metode OCTAVE Allegro.
2. Mengembangkan strategi untuk meningkatkan keamanan sistem informasi dengan tujuan mencegah dampak yang ditimbulkan akibat terganggunya aset informasi kritis.

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian ini adalah:

1. Mengurangi risiko terjadinya kerusakan pada sistem informasi akademik beserta asetnya.
2. Hasil dari penilaian risiko dapat dijadikan sebagai dasar pengambilan keputusan untuk membuat kebijakan yang terkait dengan keamanan sistem informasi.
3. Pihak institusi dapat membuat strategi mitigasi yang tepat jika ancaman yang menyebabkan kerusakan sistem informasi benar-benar terjadi.

1.6 Metodologi Penelitian

Penelitian akan dilakukan sesuai dengan langkah – langkah berikut:

a. Studi Literatur

Melakukan studi literature terhadap berbagai sumber referensi dengan pencarian data di internet dan buku – buku literatur tentang topik – topik yang sesuai.

b. Pengambilan Data

Pengambilan data antara lain dengan cara observasi lapangan serta wawancara dengan pihak atau bagian yang menangani sistem informasi akademik. Data yang diambil dapat berupa dokumen cetak biru pengembangan sistem informasi dan panduan pengguna.

c. Analisis dan Penilaian Risiko

Pada tahap ini dilakukan analisis risiko dan penilaian risiko pada Sistem Informasi dengan fokus pada aset – asetnya. Penilaian risiko dilakukan sesuai dengan langkah-langkah pada metode *OCTAVE Allegro*.

d. Pengambilan Kesimpulan

Tahap selanjutnya yaitu pengambilan kesimpulan dari hasil penilaian risiko dan pengembangan rekomendasi kebijakan manajemen risiko.

1.7 Sistematika Penulisan

Secara garis besar tesis ini terdiri dari lima bab dengan beberapa subbab, berikut ini sistematika penulisannya secara lengkap:

BAB I PENDAHULUAN

Pada bab ini dibahas latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan metodologi penelitian.

BAB II LANDASAN TEORI

Bab ini membahas tinjauan pustaka, teori – teori pendukung yang berkaitan seperti keamanan sistem informasi, ancaman keamanan sistem informasi, manajemen risiko dan penilaian risiko serta dibahas secara singkat metodologi manajemen risiko menggunakan *OCTAVE Allegro*.

BAB III METODOLOGI

Pada bab ini akan dibahas lebih lanjut penjabaran metodologi yang akan digunakan secara lebih rinci, meliputi metodologi dan langkah – langkah pengerjaan manajemen risiko menggunakan *OCTAVE Allegro*.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini dibahas mengenai hasil penilaian risiko menggunakan metode *OCTAVE Allegro* serta dibahas pula langkah – langkah pelaksanaan penilaian risiko sistem informasi. Pada bagian akhir dibahas pula strategi mitigasi yang dibuat berdasarkan hasil dari proses penilaian risiko.

BAB V KESIMPULAN DAN SARAN

Bab terakhir merupakan kesimpulan dari hasil penelitian yang telah dilakukan dan beberapa saran untuk penelitian lebih lanjut.