

BAB I

PENDAHULAN

1.1 Latar Belakang

Teknologi komputer telah menjadi bagian integral dari suatu organisasi memperbolehkan karyawan maupun orang lain untuk mengakses sistem informasi dari mana-mana, dengan kecanggihan ancaman keamanan yang semakin meningkat, kebutuhan untuk memberikan keamanan dianggap lebih penting. Sehingga aspek keamanan system informasi menjadi penting untuk dijaga dan lindungi. Keamanan informasi merupakan salah satu aspek penting yang harus diperhatikan. Keamanan informasi merupakan salah satu aspek penting yang harus diperhatikan oleh organisasi dan perusahaan. Informasi baik berupa teks, gambar, audio, maupun video yang menyimpan asset penting bagi perusahaan, wajib dilindungi dengan sistem manajemen keamanan informasi. Kebocoran, kerusakan atau hilangnya suatu informasi dapat menimbulkan kerugian baik secara finansial maupun produktivitas bagi organisasi dan perusahaan (Mufadhol, 2009).

Universitas Bina Insani Lubuklinggau telah menerapkan sistem informasi akademik yang digunakan Academic Management System (AMS). adalah sistem informasi akademik yang dalam kegiatan administrasi akademik kampus secara online, Sistem itu sendiri terbentuk dari sistem-sistem lainnya seperti sistem proses Penerimaan Mahasiswa Baru (PMB), pembuatan jadwal kuliah, pengisian Kartu Rencana Studi (KRS), pengisian nilai, pengelolaan data dosen & mahasiswa. Sistem ini juga dapat berfungsi sebagai pendukung untuk analisis data dalam

menentukan keputusan Kampus. Penggunaan sistem informasi akademik termaksud mahasiswa, dosen, dan admin.

Sistem Informasi Akademik pada Universitas Bina Insani Lubuklinggau yang digunakan sebagai kegiatan kampus yang terjadi saat ini kelemahan terhadap keamanan yang terdampak pada aset berupa data dan hardware pada SIA PMB, contoh incident pencurian data maupun pengambilalihan akses secara ilegal dari serangan. melalui risk assessmen pihak petugas dapat terbantu dalam mengetahui risiko-risiko apa saja yang dapat terjadi dan dampak kerentanan pada sistem PMB, mengukur seberapa mungkin risiko tersebut diulang , kemudian ditunjukkan hasil perhitungan risiko manakah yang menjadi prioritas yang dalam hal ini butuh penanganan segera dan manakah risiko yang dapat menemukan penanganan berikutnya.

Dari permasalahan diatas penting dilakukannya evaluasi resiko pada keamanan dan mengukur dampak potensi dari kerentanan yang terjadi pada sistem IT, tahapan analisis risiko dapat meminimalisir dan mengendalikan risiko sesuai peringkat nilai level risiko atau tingkat insiden sistem yang dialami di institusi perguruan tinggi dari ancaman keamanan risiko Universitas Bina Insani. Kegiatan penilaian risiko di sistem informasi akadekmin hanya berdasarkan pada pengalaman dan pengetahuan yang sebatas pada pengenalan teknologi informasi, belum dilaksanakan secara khusus. Semakin besar aset informasi yang dilayankan kepada petugas melalui teknologi web, semakin besar sumber ancaman yang akan mengganggu kelancaran sistem informasi pmb.

Kejadian *incident*, atau *vulnerability* yang terjadi diatas merupakan risiko yang dapat mengganggu proses bisnis contoh incident. Misalnya siber attack

berpura-pura sebagai pemakai yang lupa passwordnya dan minta agar diganti menjadi kata lain, dengan pertimbangan incident, dan vulnerability yang sering terjadi maka diperlukan penanganan risiko, dan penilaian risiko dilakukan dalam proses manajemen risiko keamanan informasi sehingga risiko yang ada bisa ditangani dan dikendalikan. Manajemen risiko keamanan informasi adalah metode untuk penilaian dan mitigasi risiko terhadap aspek kebutuhan keamanan informasi yang memuat 3 unsur penting yaitu: Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan). Tiga unsur penting dari aspek keamanan tersebut sangat rawan terhadap ancaman serangan-serangan yang mengancam keberadaannya baik serangan terhadap sumber-sumber informasi baik secara fisik dan melalui akses secara jaringan.(Mahardika 2017)

Pada penelitian ini. pentingnya evaluasi resiko dilakukan untuk membantu proses pengambilan keputusan berdasarkan hasil analisis risiko, proses evaluasi risiko akan menemukan seberapa besar kerusakan resiko yang menjadi kelemahan sistem informasi akademik PMB, dan bagaimana prioritas perlakuan atas resiko - risiko tersebut seperti dalam aktifitas ini perlu dilakukan penilaian untuk mengetahui level risiko dari risiko tinggi, sedang, dan rendah.. Dapat membantu mengidentifikasi risiko, mengurangi dampak ancaman risiko dengan level metode yang digunakan yaitu penilaian model-DREAD (*Damage Potential, Reproducibility, Exploitability, Affected User, Discoverability*) merupakan model yang digunakan untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko untuk sebuah ancaman yang terjadi (Meier et al. (2003).

Pada penelitian sebelumnya menurut (Suprihanto, Prahasto et al. 2013) dan (Saputra, Nelmiawati et al. 2017) DREAD dipilih sebagai acuan penilaian risiko dalam penggunaan sistem dan teknologi informasi di perguruan tinggi untuk mengetahui level atau peringkat risiko tersebut. Untuk membantu mengatasi masalah ini dan untuk menambah dimensi baru dalam menentukan dampak, tentang apakah ancaman keamanan web itu benar berarti, maka masalah ini dapat dilakukan proses penilaian risiko dengan model DREAD .Dengan adanya model DREAD diharapkan dapat membantu pemmasalahan diatas dan memberikan dan menghasilkan informasi peringkat risiko pada sistem informasi pada Universitas Bina Insani, Maka berdasarkan uraian tersebut, penulis tertarik untuk melakukan penelitian lebih lanjut lagi dengan judul; “EVALUASI RESIKO KEAMANAN MENGGUNAKAN MODEL DREAD TERHADAP SISTEM INFORMASI AKADEMIK DI UNIVERSITAS BINA INSAN LUBUKLINGGAU”.

1.3. Identifikasi Masalah

Menindak lanjuti masalah yang terdapat pada latar belakang diatas, maka identifikasi masalah yang akan diangkat pada penelitian ini adalah:

1. Mengalami kelemahan terhadap keamanan pada sistem aplikasi registrasi penerimaan mahasiswa baru resiko yang timbulkan seperti virus, hacker ataupun pencurian data dari database yang belum terintegasi pada *Academic Management System* (AMS) di Universitas Bina Insani Lubuklinggau.
2. Pihak universitas belum pernah melakukan penilaian risiko tingkat dampak ancaman pada implementasi sistem aplikasi registrasi

penerimaan mahasiswa baru (PMB) yang ada dengan menggunakan metode DREAD.

3. Penting dilakukannya analisis risiko dan mengukur potensi bahaya dari setiap tahapan pekerjaan yang berdampak pada aset IT dengan adanya tahapan analisis risiko dapat mengandilakan risiko atas dasar prioritas insiden AMS yang dialami di institusi perguruan tinggi dari ancaman keamanan risiko Universitas Bina Insani.

1.2 Batasan Masalah

Adapun penelitian ini difokuskan pada masalah no 2 yaitu tidak menyimpang dari permasalahan yang ada, maka perlu adanya batasan masalah.

1. Melakukan penilaian risiko pada tingkat dampak ancaman yang belum diketahui potensi bahaya pada sistem aplikasi registrasi pada penerimaan mahasiswa baru (PMB).
2. Memberikan perhatian tentang keamanan informasi serta risiko-risiko yang mungkin akan timbul.

1.4. Rumusan Masalah

Berdasarkan latar belakang diatas, maka penulis merumuskan permasalahan dalam penelitian ini yaitu sebagai berikut: Bagaimana risiko – risiko kelemahan pada keamanan sistem aplikasi regesitrasi penerimaan mahasiswa baru (PMB) yang mengalami kerentanan yang ditimbulkan?

1.5. Tujuan Masalah

Tujuan penelitian ini untuk mengetahui resiko-resiko yang mungkin terjadi dalam sistem informasi akademik, dapat dijabarkan sebagai berikut :

1. Mengetahui risiko yang menjadi dampak ancaman pada keamanan sistem informasi.
2. Mengetahui tingkat level risiko terhadap keamanan sistem informasi saat ini.
3. Memberikan rekomendasi meminimalisir risiko terhadap dampak keamanan sistem informasi.

1.6. Manfaat Penelitian

Adapun manfaat penelitian ini diambil oleh penulis dalam melakukan penelitian ini adalah:

1. Mengurangi risiko terhadap dampak ancaman keamanan sistem informasi.
2. Hasil dari pengukuran resiko dapat dimanfaatkan tim pengembangan aplikasi web terhadap peringkat level ancaman risiko.

1.7. Ruang Lingkup Penelitian

Dalam penulisan tesis ini, penulis akan membatasi ruang lingkup penelitian dengan menitik beratkan permasalahan yang akan dibahas, yaitu :

1. Penelitian ini hanya membahas proses penilain risiko untuk mengetahui level risiko keamanan sistem informasi.
2. Penelitian dilakukan terhadap keamanan sistem informasi akademik Universitas Bina Insani Lubuklinggau.
3. Objek Penelitian dilakukan pada Universitas Bina Insani Lubuklinggau.

1.8. Susunan dan Struktur Proposal Tesis

Susunan dan struktur proposal tesis ini maksudnya agar dapat memberikan garis besarnya secara jelas sehingga terlihat hubungan antara bab yang satu dengan

bab yang lainnya. Susunan dan struktur proposal tesis dijabarkan di bawah ini sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang, identifikasi masalah, batasan masalah, rumusan masalah, tujuan dan manfaat penelitian, ruang lingkup penelitian, serta susunan dan struktur tesis.

BAB II KAJIAN PUSTAKA

Pada bab ini membahas tentang kajian pustaka, penelitian terdahulu, dan hipotesis penelitian yang akan dilakukan.

BAB III METODOLOGI PENELITIAN

Pada bab ini pembahasannya yang terdiri dari metode penelitian yang digunakan, metode pengumpulan data serta jadwal penelitian.