BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era digital ini, sistem informasi digunakan sebagai sarana penunjang aktivitas yang digunakan di berbagai bidang pekerjaan. Sistem informasi dibutuhkan untuk memudahkan alur kerja dengan sistem pengambilan keputusan yang lebih akurat, efektif dan efisien. Sistem informasi pendidikan atau dapat pula disebut sistem informasi akademik menghimpun berbagai data dan informasi civitas akademik yang saling terintegrasi sehingga dapat mendukung proses bisnis pendidikan yang terjadi di dalamnya. Di dalam sistem informasi akademik tentunya banyak melibatkan aset data dan informasi civitas akademik yang krusial dan sensitif sehingga membutuhkan pengelolaan keamanan sistem informasi. Keamanan informasi didefinisikan sebagai bentuk upaya perlindungan bagi informasi dengan membuat langkah untuk menjaga aspek CIA yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) (A. Ključnikov, dkk 2019).

Keamanan sistem informasi dijalankan dari berbagai sisi keamanan mulai dari fisik, lingkungan, hingga sumber daya manusia. Penerapan keamanan dari ketiga sisi tersebut tentunya diupayakan berdasarkan risiko yang berpotensi timbul dan berdampak pada kinerja sistem yang dimiliki. Menurut Setyadi (2016) risiko merupakan tantangan yang pasti dihadapi di masa yang akan datang tanpa diketahui wujudnya secara pasti. Dalam upaya mengurangi dan memperkecil risiko tersebut dibutuhkan manajemen risiko yang efektif dan efisien sebagai pengendalian risiko yang berkesinambungan.

Adapun penelitian mengenai keamanan internet yang telah dilakukan sebelumnya oleh lembaga ID SIRTII/CC pada tahun 2018. Lembaga ID SIRTII/CC atau *Security Incident Response Team on Internet Infrastructure/Coordination Center* merupakan lembaga resmi yang melakukan analisis data mengenai insiden serangan pada infrastruktur internet di Indonesia. Pada laporan ID SIRTII/CC menyatakan bahwa Indonesia menerima sebanyak

122.435.215 serangan *malware*, 16.939 kejadian pada website dan 2.885 kejadian dari masyarakat. Berdasarkan fakta tersebut Indonesia dinyatakan sebagai sasaran serangan *cybercrime* terbanyak (ID SIRTII/CC, 2018). Selain itu terdapat penelitian lain yang menjelaskan bentuk serangan *cybercrime* dapat terjadi pada pengguna atau sumber daya manusia yang menjadi titik terlemah keamanan data pada sistem informasi (Safianu, 2016). Penelitian tersebut juga menyebutkan bahwa tipe serangan kepada sistem informasi memiliki tingkat keberhasilan yang lebih tinggi dibandingkan tipe serangan fisik terhadap sistem informasi itu sendiri. Hal ini menunjukkan diperlukannya upaya pencegahan kejahatan sistem informasi. Maka dari itu, berdasarkan keterlibatan aset data dan informasi pada sistem informasi pendidikan, dibutuhkan penerapan keamanan informasi sebagai langkah pencegahan risiko keamanan.

Berdasarkan identifikasi risiko keamanan informasi yang didapatkan, adapun bentuk pencegahan kejahatan keamanan sistem informasi yang diupayakan pemerintah yaitu membentuk peraturan khususnya di dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) Pasal 32 Ayat (1) yang mengatur tentang larangan bagi setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak dokumen elektronik milik orang lain atau milik publik. Selain dengan undang-undang perlindungan ITE, bentuk perlindungan kejahatan keamanan khususnya pada sistem informasi akademik juga dapat diupayakan dengan penerapan kontrol kerangka kerja pelaksanaan keamanan sistem informasi.

Sistem Informasi Akademik (SIAK) Universitas Pendidikan Indonesia menjadi sistem informasi akademik yang dipilih sebagai studi kasus dalam penelitian ini. Pada proses upaya identifikasi masalah penelitian dilakukan studi pendahuluan dengan melakukan wawancara guna menemukan permasalahan keamanan sistem informasi pada lokasi penelitian yang dituju. Di dalam wawancara tersebut tergambarkan bahwa belum adanya kerangka kerja yang diterapkan sebagai manajemen risiko keamanan informasi pada sistem informasi yang digunakan. Hal tersebut menunjukkan adanya kebutuhan penerapan

manajemen risiko berdasarkan kerangka kerja yang dapat disesuaikan pada sistem informasi akademik.

Penerapan sistem keamanan sistem informasi akademik tersebut disesuaikan dengan kebutuhan perlindungan aset-aset yang dimiliki oleh organisasi terkait. Analisis penerapan kerangka kerja dilakukan dengan harapan dapat menjadi bentuk upaya pencegahan kejahatan sistem informasi sekaligus manajemen risiko keamanan sistem informasi yang konsisten atas aset dan proses pada lembaga pendidikan yang dituju.

Pada penelitian ini dilakukan analisis penerapan keamanan sistem informasi akademik pada SIAK UPI berdasarkan kontrol kerangka kerja NIST SP 800-30. Pada kerangka kerja NIST SP 800-30 berisi pembahasan mengenai model proses yang dapat dilakukan mengenai siklus hidup suatu pengembangan sistem SDLC *(system development life cycle)* secara rinci. Pada kerangka kerja NIST SP 800-30 terdapat tiga tahapan manajemen risiko yaitu penilaian risiko *(risk assessment)*, mitigasi risiko *(risk mitigation)*, dan evaluasi risiko *(risk evaluation).* Ketiga tahapan tersebut menghasilkan rekomendasi berupa tahapan manajemen yang harus dilakukan oleh sasaran penelitian sebagai praktik penerapan manajemen risiko keamanan sistem informasi.

Adapun penelitian terdahulu yang dilakukan oleh Juliasari, Y., & Zulfikar, D. H. (2022), digunakan kerangka kerja NIST SP 800-30 dengan keenam tahapan penilaian risiko (*risk assessment*) guna mendapatkan analisis manajemen risiko. Berdasarkan penelitian tersebut, pada Sistem Informasi Pendidik dan Tenaga Kependidikan atau SIMPATIKA didapatkan 3 risiko level tinggi, 2 risiko level sedang dan 2 risiko level rendah yang dijadikan acuan proses mitigasi risiko (*risk mitigation*). Selain itu, dilakukan pula pencarian total biaya proses mitigasi dari setiap pencegahan risiko yang dilakukan.

Berdasarkan latar belakang di atas, digunakan jenis penelitian kualitatif dengan desain penelitian studi kasus guna pengumpulan serta analisis data penelitian. Teknik pengumpulan data dilakukan melalui tahapan observasi, wawancara serta dokumentasi. Observasi Direktorat STI Universitas Pendidikan Indonesia sebagai lokasi utama diterapkannya Sistem Informasi Akademik (SIAK) UPI. Selain itu wawancara dilakukan kepada tiga jenis partisipan dengan

latar belakang *IT Security* dari lembaga berbeda guna memperoleh data dan fakta mengenai kondisi lapangan dalam menerapkan keamanan informasi. Setelah itu dilakukan dokumentasi dibutuhkan sebagai instrumen pendukung dalam pengumpulan dan analisis data. Pada proses analisis data digunakan metode OCTAVE *(Operationally Critical Threat, Asset and Vulnerability)* sebagai langkah identifikasi, analisa dan pengawasan terhadap pengelolaan risiko keamanan informasi pada lokasi penelitian.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka rumusan masalah yang didapatkan yaitu:

1. Bagaimana hasil identifikasi risiko pada Sistem Informasi Akademik (SIAK) Universitas Pendidikan Indonesia berdasarkan kerangka keamanan informasi?
2. Bagaimana hasil penilaian risiko pada Sistem Informasi Akademik (SIAK) Universitas Pendidikan Indonesia berdasarkan kerangka keamanan informasi?
3. Bagaimana rekomendasi manajemen risiko pada Sistem Informasi Akademik (SIAK) Universitas Pendidikan Indonesia berdasarkan kerangka keamanan informasi?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang didapatkan maka diperlukan batasan pada permasalahan yang akan diteliti diantaranya:

1. Terdapat berbagai jenis sistem informasi, pada penelitian ini sistem informasi yang diteliti merupakan sistem informasi akademik
2. Terdapat berbagai macam kerangka kerja keamanan informasi, pada penelitian ini digunakan NIST SP 800-30
3. Terdapat tiga tahapan besar manajemen risiko dari kerangka kerja NIST SP 800-30 yaitu penilaian, mitigasi dan evaluasi. Pada penelitian ini tahapan yang dilakukan terbatas pada tahapan penilaian risiko

1.4 Tujuan Penelitian Skripsi

Berdasarkan rumusan masalah yang telah didapatkan, maka tujuan penelitian diantaranya sebagai berikut:

1. Memberikan hasil identifikasi risiko pada Sistem Informasi Akademik (SIAK) Universitas Pendidikan Indonesia berdasarkan kerangka keamanan informasi
2. Memberikan hasil penilaian risiko berdasarkan kerangka kerja keamanan pada Sistem Informasi Akademik (SIAK) Universitas Pendidikan Indonesia
3. Memberikan rekomendasi manajemen risiko pada Sistem Informasi Akademik (SIAK) Universitas Pendidikan Indonesia berdasarkan kerangka keamanan informasi

1.5 Manfaat Penelitian Skripsi

Pada penelitian ini terdapat manfaat teoretis dan praktis diantaranya sebagai berikut:

1.5.1 Secara Teoretis

Pada penelitian ini secara teoritis diharapkan dapat menjadi sumbangsih pemikiran dan referensi bagi para pengembang sistem informasi, khususnya sistem informasi akademik untuk meningkatkan kesadaran terhadap keamanan sistem informasi dengan menciptakan berbagai model keamanan sistem informasi dari acuan kerangka kerja yang dapat disesuaikan dengan kebutuhan.

1.5.2 Secara Praktis

Pada penelitian ini secara praktis diharapkan agar sasaran penelitian dapat mendapatkan informasi mengenai risiko yang dapat terjadi pada sistem informasi akademik yang dimilikinya. Selain itu dokumen hasil penelitian diharapkan dapat digunakan sebagai rekomendasi manajemen risiko ataupun langkah dasar terhadap pengendalian kesadaran keamanan informasi.