BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Pada era globalisasi ini semua elemen kehidupan sudah terintegrasi dengan teknologi dan juga sistem yang mana membawa banyak perubahan bagi kehidupan masyarakat sehari-hari. Dengan adanya hal tersebut maka diperlukan sebuah sistem yang memiliki keamanan informasi yang baik, salah satunya yaitu dalam bidang pendidikan di ranah Universitas. Lembaga pendidikan biasanya mempunyai sebuah sistem informasi akademik yang dibuat dengan tujuan memudahkan entitas yang saling berkaitan untuk mengakses data lebih mudah sehingga hal tersebut dapat membuat pekerjaan lebih efektif dan efisien. Di dalam sistem informasi akademik memuat beberapa hal seperti data civitas akademik, info perkuliahan, riwayat tagihan, dan lain-lain, Hal tersebut memuat data-data penting dan krusial. Dengan diterapkannya keamanan informasi merupakan bentuk upaya perlindungan data-data dan juga informasi yang ada dalam sistem. Menurut pendapat ahli pada (Hermawan, 2022), penerapan keamanan informasi dapat diterapkan dengan menjaga aspek CIA yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

Adanya keamanan sistem informasi mendorong beberapa organisasi atau perusahaan untuk menerapkan hal tersebut untuk mengurangi beberapa risiko yang terjadi salah satunya ancaman siber, menurut (Lokobal, 2014) risiko merupakan sesuatu yang belum pasti dan terjadi selama selang waktu tertentu yang dapat menyebabkan suatu kerugian, baik itu kerugian kecil yang tidak terlalu berdampak maupun kerugian besar yang berpengaruh terhadap keberlangsungan suatu perusahaan.

Adapun berdasarkan penelitian sebelumnya oleh (Hapsari & Pambayun, 2023). Mengenai ancaman *Cyber Crime* di Indonesia dijelaskan bahwa teknologi digital yang berkembang pesat memiliki dampak positif dalam hal akses informasi, keterlibatan sosial, dan pemberdayaan ekonomi. Akan tetapi juga

berisiko terhadap penyebaran informasi palsu dan ketergantungan pada teknologi. Perkembangan teknologi digital juga telah meningkatkan ancaman *cybercrime* secara signifikan, termasuk serangan malware, hacking, dan pencurian data pribadi. Serangan *cybercrime* juga berdampak pada pencurian identitas, kehilangan pekerjaan, kerugian finansial, kebocoran data. Masyarakat pada umumnya kurang sadar akan risiko *cybercrime* dan tidak memahami cara melindungi diri mereka sendiri secara efektif. Menurut (Riskiyadi, 2021) perlu adanya tindakan antisipatif untuk menanggulangi ancaman *cybercrime* salah satunya yaitu dengan meningkatkan pemahaman mengenai *cybersecurity* dan tindakan pemulihan *cybercrime*. Adanya kemajuan teknologi yang berkembang juga mempengaruhi sistem keamanan yang ada dan membuat pelaku *cybercrime* semakin aktif dan mudah melakukan tindakan kejahatan. Oleh karena itu penelitian dilakukan agar memberikan pemahaman dan juga pengetahuan mengenai penanggulangan *cybercrime* dengan menyiapkan keamanan informasi yang berkualitas.

Laporan *National Cyber Security Index* (NCSI) skor indeks keamanan siber Indonesia sebesar 38,96 poin dari 100 pada 2022 sehingga menempatkan Indonesia pada peringkat ke-3 terendah diantara seluruh negara G20. Sementara itu masih dalam laporan yang sama, secara global Indonesia menempati peringkat ke-83 dari 160 negara. Menurut (Daeng, 2023) dari kejadian pada beberapa tahun ke belakang, Indonesia merupakan negara yang lemah *cyber-security* nya. Hal ini dapat diketahui dari maraknya berbagai kejadian, salah satunya yaitu pada jurnal (Saputra et al., 2023) kejadian penyerangan yang dilakukan oleh peretas dengan inisial “bjorka” yang berhasil meretas data milik kementrian komunikasi dan informatika (kominfo) dan menjual data rekamanan komisi pemilihan umum (KPU) sebanyak 105 juta rekaman, 1,3 miliar rekaman registrasi kartu SIM prabayar Indonesia yang memuat NIK, dan juga nomor telepon, selain itu peretasan data juga terjadi pada Pusat Data Nasional (PDN) yang terserang *Ransomware*, Badan Siber dan Sandi Negara menyebutkan bahwa faktor utama dari kejadian tersebut yaitu pengelolaan tata kelola dan juga manajemen risiko pada PDN tidak dicadangkan (Putranto Saptohutomo, 2024).

Berdasarkan penelitian dan juga survei mengenai kejahatan keamanan informasi yang telah diketahui, maka pemerintah membentuk suatu kebijakan dalam bentuk peraturan khususnya dalam Undang-Undang Pasal 32 ayat 1 UU No 11/2008 tentang Informasi dan Transaksi Elektronik (ITE), yang berbunyi (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik. Selain hal itu pencegahan kejahatan keamanan sistem informasi dapat diupayakan dengan penerapan control kerangka kerja pada unit keamanan sistem informasi.

Sistem Informasi Akademik (SIAK) UPI menjadi tujuan dalam penelitian kemanan sistem informasi ini. Proses identifikasi dan perumusan masalah dilakukan menggunakan studi literatur penelitian terdahulu mengenai keamanan sistem informasi akademik (SIAK-UPI) menggunakan NIST 800-30 masih ada celah dan belum terindikasinya sistem menggunakan indeks KAMI yang berpedoman pada ISO 27001 dikarenakan penerapan security assessment yang masih berkala (Sekar Putri, 2023). Hal tersebut menandakan bahwa perlu dilakukan penerapan keamanan sistem informasi yang berpedoman pada *Information Security Management* ISO 27001:2022 Menggunakan indeks KAMI. Dari beberapa kerangka keamanan informasi yang ada seperti NIST, OCTAVE,COBIT, dan juga ISO 27001. Dari hasil observasi pada DSTI UPI didapatkan temuan bahwa pernah terjadi ancaman *malware* dengan jenis serangan *ransomware* pada SIAK UPI. Penerapan Indeks KAMI yang diadaptasi dari ISO/IEC 27001:2022 merupakan penerapan tingkat keamanan yang sudah disesuaikan dengan standar nasional dan internasional untuk mengukur tingkat kesiapan dan juga kepatuhan terhadap keamanan informasi, maka dari itu pemilihan Indeks KAMI relevan bagi organisasi di Indonesia, seperti Universitas Pendidikan Indonesia (UPI), karena alat ini telah disesuaikan dengan konteks regulasi dan kebutuhan lokal.

Adapun penelitian terdahulu yang dilakukan oleh (Sekar Putri, 2023). digunakan kerangka kerja NIST SP 800-30, Pada penelitian tersebut. Pada Sistem Informasi Akademik (SIAK-UPI) didapatkan 2 risiko yaitu *high level*, 2 risiko

medium level serta 4 risiko *low level* , Berdasarkan penelitian sebelumnya risiko high level meliputi serangan *browser hijacking* dan beberapa distribusi data yang tidak terdeteksi. Sedangkan risiko medium level meliputi serangan *ramsomware* dan jaringan server *down,* lalu pada risiko *low level* meliputi serangan virus, kesalahan yang terjadi pada sistem, listrik yang padam seperti pada kerusakan bencana alam.

Berdasarkan latar belakang yang sudah dijelaskan, Dapat disimpulkan bahwa pentingnya penerapan kemananan informasi pada sistem informasi akademik (SIAK-UPI) menggunakan pedoman INDEKS KAMI ISO 27001 maka penulis tertarik melakukan penelitian mengenai "Manajemen Sistem Keamanan Informasi berdasarkan ISO/IEC 27001:2022 Pada SIAK UPI". Proses pengumpulan data dan identifikasi yang dilakukan penulis menggunakan metode kuantitatif dengan pendekatan studi deskriptif melalui tahapan wawancara, observasi dan juga angket. Peneliti melakukan wawancara kepada pengelola penanggung jawab keamanan informasi dan melakukan observasi di Direktorat STI Universitas Pendidikan Indonesia sebagai tempat pengelolaan Sistem Informasi Akademik (SIAK-UPI).

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat disimpulkan bahwa, rumusan masalah yang didapatkan yaitu :

1. Apakah keamanan informasi pada Sistem Informasi Akademik (SIAK) UPI sudah memenuhi aspek keamanan informasi berdasarkan ISO/IEC 27001:2022 ?.
2. Bagaimana rekomendasi berdasarkan hasil analisis sistem keamanan informasi berdasarkan ISO/IEC 27001:2022?.

1.3 Batasan Masalah

Berdasarkan latar belakang di atas, maka dapat disimpulkan bahwa, batasan masalah yang didapatkan yaitu :

1. Penelitian ini dilakukan pada sistem Informasi Akademik (SIAK-UPI)
2. Terdapat beberapa kerangka kerja keamanan informasi, pada penelitian ini penulis berpedoman pada Indeks KAMI ISO/IEC 27001:2022

1.4 Tujuan Penelitian

Adapun Tujuan dari Penelitian ini yaitu :

1. Mengetahui keamanan informasi pada Sistem Informasi Akademik (SIAK) UPI, apakah sudah memenuhi aspek keamanan informasi berdasarkan ISO/IEC 27001:2022
2. Memberikan rekomendasi berdasarkan hasil analisis ssitem keamanan informasi berdasarkan ISO/IEC 27001:2022.

1.5 Manfaat Penelitian

Adapun manfaat yang dihasilkan dari penelitian ini yaitu :

1.5.1 Secara Teoritis

Jika dilihat secara teoritis, penelitian ini bisa dijadikan untuk referensi dan pengembangan sistem informasi bagi peneliti selanjutnya khususnya bagi peneliti atau pengembang sistem informasi agar dapat meningkatkan kesadarannya mengenai pentingnya keamanan sistem informasi untuk menghindari kebocoran data.

1.5.2 Secara Praktis

Secara Praktis, penelitian ini diharapkan agar apa yang menjadi sasaran penulisa bisa tercapai dan mendapatkan informasi mengenai tingkat keamanan yang dilakukan oleh instansi pada sistem akademik.

1.6 Struktur Organisasi Skripsi

Struktur organisasi skripsi pada penelitian "Manajemen Keamanan Sistem Informasi (KAMI) terhadap Indeks KAMI ISO/IEC 27001:2022" terdapat 5 BAB yang mana berisi BAB I hingga BAB V, memuat Pendahuluan, Kajian Pustaka, Metode Penelitian, Hasil dan Pembahasan, dan pada bab terakhir berisi Simpulan, Implikasi dan juga rekomendasi yang mana disusun secara sistematis dengan urutan sebagai berikut :

1) Bab I: Pendahuluan

   Pada Bab ini dijelaskan mengenai latar belakang penulis mengambil penelitian tersebut, Rumusan masalah dan juga batasan masalah yang menjadi tolak ukur pengambilan data, serta adanya tujuan dari sebuah penelitian yang akan dilakukan, dan terakhir dijelaskan mengenai manfaat penelitian.

2) Bab II: Kajian Pustaka

   Bab ini berisi tentang kajian pustaka, yang mana menggambarkan teori-teori yang berkaitan dengan penelitian ini seperti seperti sistem informasi, sistem informasi akademik, ISO 27001:2022, dan juga Indeks KAMI.

3) Bab III: Metode Penelitian

   Bab ini berisi tentang bagaimana tata cara pengambilan data dalam penelitian ini, seperti uraian mengenai jenis penelitian, desain penelitian hingga menjelaskan bagaimana teknik pengumpulan data yang sesuai dengan prosedur penelitian yang sudah dibuat.

4) Bab IV: Temuan dan Pembahasan

   Bab ini berisi tentang hasil dan pembahasan mengenai penilaian evaluasi keamanan sistem informasi menggunakan Indeks KAMI ISO 27001:2022 yang mana pada Bab ini juga dijelaskan hasil temuan penelitian serta rekomendasi untuk kedepannya seperti apa.

5) Bab V: Simpulan, Implikasi, serta Rekomendasi

   Bab ini berisi simpulan, implikasi, dan juga rekomendasi yang didasarkan pada data dari hasil penelitian yang sudah dilakukan.