BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Dengan layanan canggih yang tersedia di platform teknologi informasi, orang dapat dengan mudah berkomunikasi dan berinteraksi satu sama lain. Bahkan dengan teknologi informasi berasis internet proses bisnis dapat dilakukan dengan mudah. Namun penggunaan teknologi informasi media dan komunikasi telah menguah perilaku masyarakat dan peradaan manusia dalam skala global[1]. Dengan segala perkembangan teknologi informasi dan komunikasi yang sangat cepat dan luas pemakaian dan jangkauannya terutama di Indonesia yang dapat mempermudah masyarakat dalam mengakses internet guna mendapatkan informasi dimana pun dan kapan pun mereka mau. Saat ini internet sudah menjadi kebutuhan pokok bagi hampir seluruh masyarakat Indonesia.

Meskipun perkembangan teknologi informasi sangat pesat, perkembangan yang ada tidak selalu digunakan untuk tujuan positif, tetapi sering diarahkan juga untuk tujuan negatif. Perkembangan teknologi informasi yang terkomputerisasi dan terhubung melalui internet sering digunakan sebagai sarana dan pendukung kejahatan. Misalnya, memfitnah seseorang atau mungkin transaksi bisnis prostitusi online yang sekarang banyak diberitakan[2]. Sebagai langkah awal yang dapat dilakukan untuk mengantisipasi terjadinya kejahatan cyber adalah memberikan pemahaman akan pentingnya informasi yang dimiliki seperti identitas dan privasi yang tidak boleh dipublis secara bebas.

Secara keseluruhan, organisasi menyadari bahwa keamanan informasi merupakan aspek penting untuk menjaga profitabilitas dan keunggulan kompetitif. Namun, organisasi cenderung lebih peduli dengan kerentanan terhadap ancaman eksternal. Dengan demikian, terjadinya peningkatkan biaya untuk kebutuhan dalam bidang profesional di keamanan informasi dan teknologi[3]. Banyak permasalahan yang terjadi berasal dari ketidaktahuan tentang serangan yang terjadi, sehingga dapat memberikan dampak berbahaya yang cukup besar bagi suatu instansi atau perusahaan. Dengan memberikan pemahaman akan pentingnya keamanan informasi terhadap pengguna, maka dapat mengurangi serangan yang

dapat memberikan dampak positif dan meminimalisir risiko serangan keamanan informasi.

Mengingat pentingnya informasi, instansi pemerintahan harus mengelola keamanan informasi. Salah satu standar yang digunakan untuk mengukur tingkat keamanan informasi dalam suatu organisasi adalah dengan menggunakan Indeks KAMI yang mengacu pada standar SNI ISO/IEC 27001:2013. ISO 27001 merupakan bentuk kerangka standar internasional yang memuat standar di bidang keamanan informasi . ISO 27001 menyediakan kerangka kerja untuk penggunaan teknologi dan manajemen aset yang membantu organisasi memastikan bahwa keamanan informasi efektif. Ini termasuk akses data yang berkelanjutan, keamanan dan integritas informasi yang dimilikinya.[4].

Informasi merupakan salah satu aset terpenting dan berharga bagi kelangsungan hidup organisasi, keamanan, integritas nasional, kepercayaan publik atau konsumen, sehingga Kerahasiaan, integritas, dan ketersediaan informasi harus dijaga. Seiring dengan perkembangan teknologi, penerapan manajemen teknologi informasi yang baik saat ini menjadi kebutuhan dan kebutuhan setiap organisasi. Dalam penerapan tata kelola teknologi, faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan karena tata kelola suatu organisasi akan terganggu jika informasi merupakan salah satu objek utama yang menghadapi ancaman[5]. Pengamanan informasi perlu dilakukan pada beberapa aspek keamanan informasi diantaranya Confidentiality, Integrity dan Avaibility. Confidentiality adalah keamanan informasi menjamin hak akses suatu informasi kepada pemilik akses informasi. Integrity adalah bagaimana menjamin kelengkapan informasi dan menjaga informasi tersebut dari kerusakan atau ancaman dari pihak-pihak yang tidak bertanggung jawab yang berakibat berubah dari aslinya. Avaibility adalah menjamin informasi dapat diakses kapanpun oleh pemilik atau pengguna informasi tanpa terjadi gangguan atau perubahan informasi tersebut.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan maka didapat sebuah permasalahan yaitu, bagaimana merancang indeks kami berbasis website serta penerapan pada Dinas Pertanian, Perikanan, dan Pangan Kab. Sleman.

1.3. Batasan Masalah

Agar permasalahan ini tidak menyimpang dari penelitian, maka ditentukan batasan-batasan masalah permasalahan sebagai berikut :

a. Penelitian ini dilakukan guna mengetahui hasil dari pengukuran atau evaluasi tingkat keamanan informasi menggunakan indeks KAMI berbasis website.
b. Penelitian perancangan Indeks KAMI berbasis website ini menggunakan Indeks KAMI versi 4.1.
c. Website yang dibangun masih berbentuk localhost.
d. Penelitian dilakukan dalam ruang lingkup Dinas Pertanian, Perikanan, dan Pangan Kab. Sleman.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah membuat sistem Indeks KAMI berbasis website untuk mengukur tingkat keamanan informasi pada Dinas Pertanian, Perikanan, dan Pangan Kab. Sleman.

1.5. Sistematika Penulisan

Skripsi ini terdiri dari 5 bab, masing - masing bab memiliki pembahasan yang ditulis secara sistematis sebagai berikut :

Bab I Pendahuluan, pada bab ini menjelaskan latar belakang keamanan informasi, rumusan masalah, batasan masalah, tujuan penelitian dan sistematika penelitian.

Bab II Landasan Teori, pada bab ini membahas tentang teori – teori pendukung penelitian.

Bab III Metodologi Penelitian, pada bab ini menjelaskan mengenai metode yang digunakan pada penelitian dan gambaran umum tentang penelitian tersebut.

Bab IV Pembahasan, pada bab ini mejelaskan tentang proses pengumpulan data dan pembahasan hasil akhir dari analisis penelitian yang dilakukan.

Bab V Penutup, pada bab ini berisi kesimpulan dari penelitian dan saran.