BAB II

TINJAUAN LITERATUR

2.1. Penelitian Terkait

Dalam penelitian ini, penulis sedikit banyak mengambil refrensi dari penelitian-penelitian sebelumnya yang berkaitan dengan topic pada penelitian ini:

1. Menurut Samsiana, dkk (2021) dengan judul "Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks Kami" studi kasus Dinas komunikasi dan Informatika Kota Pontianak. Dalam Penelitian ini penulis menyimpulkan bahwa penggunaan Indeks KAMI berhasil mengukur tingkat kematangan keamanan informasi di DISKOMINFO Kota Pontianak, mencakup kategori penting seperti Sistem Elektronik, Manajemen Keamanan Informasi, Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengendalian Aset Keamanan Informasi, dan Teknologi Keamanan Informasi (Rahayu et al., 2021).
2. Menurut Edo Rizky, Suprapto, dan Andi (2018) dengan judul "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur)". Dalam Penelitian ini mengevaluasi keamanan informasi di Dinas Komunikasi dan Informatika Provinsi Jawa Timur dengan menggunakan Indeks KAMI dan standar ISO 27001, serta merekomendasikan perlunya evaluasi berkala untuk meningkatkan kesiapan dan efektivitas pengelolaan keamanan informasi (Rizky Pratama & Reza Perdanakusuma, 2018).
3. Menurut Rendy Ismail, Rinaldi , dkk (2023) dengan judul "Analisis Tingkat Keamanan Sistem Informasi Madrasah Tsanawiyah Negeri 2 Lampung Utara Menggunakan Metode Indeks Kami". Dalam Penelitian ini menunjukkan bahwa tingkat keamanan sistem informasi di MTsN 2 Lampung Utara masih belum memadai, dengan beberapa kelemahan teridentifikasi dalam praktik keamanan, kurangnya audit teknis, dan kesadaran keamanan yang rendah, sehingga diperlukan peningkatan dalam

praktik keamanan, kontrol teknis, dan manajemen risiko untuk memperkuat sistem informasi di institusi tersebut (Ismail et al., 2023).

2.2 Landasan Teori

1. Evaluasi

Kata evaluasi merupakan kata serapan dari bahasa Inggris yaitu "evaluation" yang berarti penilaian atau penaksiran. Evaluasi dapat didefinisikan sebagai kegiatan terencana yang bertujuan untuk mengumpulkan informasi, mengukur, dan menilai keberhasilan suatu proses atau hasil pembelajaran

Kemudian evaluasi juga berkutat tentang sejauh mana suatu kegiatan tertentu telah dicapai, bagaimana perbedaan pencapaian itu dengan suatu standar tertentu untuk mengetahui apakah ada selisih di antara keduanya, serta bagaimana manfaat yang telah dikerjakan itu bila dibandingkan dengan harapan-harapan yang ingin diperoleh

2. Keamanan Informasi

Keamanan informasi merupakan sebuah bentuk perlindungan informasi dan unsur-unsur penting, termasuk sistem dan perangkat keras, penggunaan, penyimpanan, dan pengiriman informasi. Untuk dapat melakukan perlindungan diperlukan beberapa alat kerja seperti kebijakan, kesadaran, pelatihan, pendidikan, serta teknologi. Sedangkan konsep keamanan informasi menurut ISO adalah suatu upaya untuk melindungi aset informasi yang dimiliki organisasi atau perusahaan. Hal ini bertujuan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dimasa datang dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis .

Konsep kunci keamanan informasi merupakan sebuah nilai pedoman atau kunci karakteristik dalam melakukan penilaian terhadap keamanan informasi di sebuah organisasi atau perusahaan. The C.I.A Tringle yang merupakan dasar dari model CNSS (Committe On National Security System)

di Amerika, mengumumkan adanya standar karakteristik keamanan informasi menjadi delapan konsep yaitu

a. *Confidentiality*

   Karakteristik ini merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses informasi.

b. *Integrity*

   Karakteristik tentang keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.

c. *Avaibility*

   Menjamin pengguna yang valid selalu bisa mengakses informasi dan sumber daya miliknya sendiri. Untuk memastikan bahwa orang-orang yang memang berhak tidak ditolak untuk mengakses informasi yang memang menjadi haknya.

d. *Privacy*

   Karakteristik ini merupakan bentuk dari perlindungan penggunaan informasi yang dikumpulkan, diproses dan digunakan dalam sebuah organisasi sesuai dengan pemilik dari informasi tersebut.

e. *Identification*

   Karakteristik ini memungkinkan sebuah sistem informasi memiliki karakteristik identifikasi dan mampu mengenali pengguna individu yang menggunakan informasi tersebut.

f. *Authentication*

   Merupakan sebuah karakteristik keamanan informasi agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai
   informasi.

g. *Authorization*

Merupakan karakteristik informasi yang berada pada sistem jaringan agar informasi tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses

tersebut.

h. *Accountability*

Merupakan karakteristik dari informasi yang telah ada dimana terdapat kontrol penjaminan informasi yang ada (akuntabel).

3. Indeks Keamanan Informasi

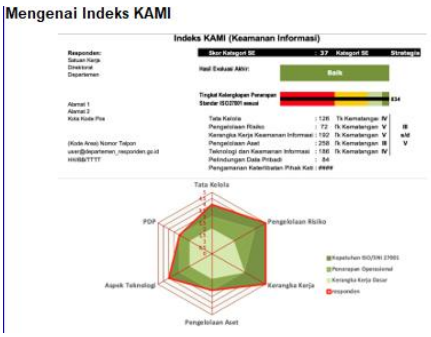
Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh Instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan *gambaran* indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Penilaian dapat dilakukan secara berkala sesuai dengan kebutuhan masing-masing institusi yang menerapkan. Wakil dari perusahaan akan menjawab pertanyaan yang diberikan dalam indeks KAMI dengan memilih status penerapan, yaitu:

a. Tidak Dilakukan
b. Dalam Perencanaan

c. Dalam Penerapan / Diterapkan Sebagian
d. Diterapkan Secara Menyeluruh



Gambar 2.1 Dashboard Indeks KAMI

Dashboard dari Indeks KAMI itu sendiri berisi nilai-nilai total dari setiap area yang ada di dalam Indeks KAMI dan memvisualisasikan nilai-nilai total tersebut dalam bentuk diagram radar dan diagram bar yang menunjukkan seberapa besar kematangan keamanan informasi tersebut.

Walau pengukuran tingkat kematangan dan kelengkapan keamanan informasi (melalui indeks KAMI) dalam penerapan SNI ISO/IEC 27001 ditujukan untuk instansi pemerintah, alat bantu tersebut juga dapat diterapkan pada perusahaan yang memberikan layanan kepada konsumen dalam skala besar. Dengan demikian usaha institusi dalam meningkatkan keamanan informasi dapat diukur dan terus diperbaiki sehingga mencapai suatu target yang diinginkan oleh intitusi sesuai dengan kebutuhannya masing-masing.

Dengan menggunakan indeks KAMI yang dilakukan secara berulang, maka suatu institusi dapat melakukan hal sebagai berikut:

a. Memantau langkah pembenahan atau peningkatan tingkat kelengkapan tata kelola keamanan informasi.
b. Mengevaluasi kesesuaian tata kelola keamanan setelah terjadinya perubahan yang signifikan dalam infrastruktur ataupun organisasi kerja yang ada dalam cakupan evaluasi.

c. Memastikan diterapkannya tata kelola keamanan informasi yang sesuai.
d. Sebagai bentuk pelaporan pelaksanaan tata kelola keamanan informasi kepada pimpinan.

4. Area Evaluasi Indeks KAMI

Indeks KAMI membantu institusi dalam melihat dan menilai tingkat kematangan penerapan SNI ISO/IEC 27001:2022. Indeks KAMI mengevaluasi area penting yang meliputi:

a. Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

b. Manajemen Keamanan Informasi

Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

c. Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

d. Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

e. Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

***f.* Visi dan Misi UPT TIK**

a) VISI

Menjadi unit yang unggul dalam menyediakan layanan syistem informasi dan konektivitas data dan komunikasi dalam mendukung pencapaian visi universitas muhammadiyah bengkulu tahun 2028.

b) MISI

1. Memperkuat insprastruktur teknologi informasi dan manajemen pengelolahanya untuk konektivitas yang tinggi.
2. Menggembangkan dan mengelolah system pemeliharaan data untuk menjamin ketersediaan data.
3. Melakukan dan mengerahkan pengembangan system informasi dengan menjaga integritas system dan data,baik untuk mendukung catur dharma maupun pengambilan keputusan eksekutif.

g. **Struktur Organisasi UPT TIK**