Jurnal SimanteC
Vol. 11, No. 1 Desember 2022
P-ISSN : 2088-2130
E-ISSN : 2502-4884

EVALUASI MANAJEMEN KEAMANAN INFORMASI PADA PERUSAHAAN PEMULA BERBASIS TEKNOLOGI MENGGUNAKAN INDEKS KAMI

EVALUATION OF INFORMATION SECURITY MANAGEMENT IN TECHNOLOGY-BASED BEGINNING COMPANY USING THE KAMI INDEX

Aprilian Lisa Maryanto[1)], Moh Noor Al Azam[2)], Aryo Nugroho[3)]
[1,2,3] Prodi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
Jl. Arief Rachman Hakim No.51, PO BOX 60117 Sukolilo, Surabaya
E-mail: [1*]lisapratama5@gmail.com, [2]noor.azam@narotama.ac.id,
[3]aryo.nugroho@narotama.ac.id

ABSTRAK

Penelitian ini dilakukan pada perusahaan yang bergerak di penjualan *online* dan juga sebagai distributor produk parfum baju pertama di Indonesia. Perusahaan yang berjalan secara *online* pasti berkaitan dengan proses bisnis perusahaan yang bergantung dengan teknologi serta data-data perusahaan juga tersimpan secara *online*. Data-data yang tersimpan *online* sangat rentan terhadap kebocoran dan pencurian. Pihak perusahaan menyatakan bahwa perusahaan ini pernah mengalami kehilangan data berupa akun Instagram yang diretas, dan belum pernah menggunakan evaluasi kemanan informasi sejak pertama kali menerapkan digitalisasi untuk proses bisnisnya. Pengukuran tingkat kematangan dan kelengkapan manajemen informasi dengan Indeks KAMI Versi 4.0 yang mengacu pada ISO 27001:2013 adalah salah satu cara dalam meningkatkan kualitas manajemen keamanan informasi pada perusahaan tersebut. Penelitian dilakukan sesuai kebutuhan dengan menentukan area yang akan dievaluasi dengan Analisis *SWOT*. Area Tata Kelola Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Teknologi dan Keamanan Informasi merupakan area yang dievaluasi Dari total skor 50 didapatkan hasil evaluasi tingkat penggunaan kategori sistem elektronik sebesar 23, sehingga termasuk dalam Kategori Tinggi. Hasil evaluasi tingkat kematangan pengamanan informasi pada 3 area yaitu sebesar 63 dari total skor 645 mendapat Kategori Tidak Layak dengan Tingkat Kematangan I hingga I+. Berdasarkan hasil evaluasi tersebut, peneliti memberikan rekomendasi berdasarkan Kontrol ISO 27002:2013, salah satunya yaitu membuat prosedur pertukaran informasi yang aman antara pengelola keamanan informasi dengan pihak Internal maupun Eksternal Instansi.

Kata kunci: *Indeks KAMI, ISO 27001, Kontrol ISO 27002, Manajemen Keamanan Informasi*

ABSTRACT

This research was conducted among companies engaged in online sales and also as the first distributor of fabric perfume products in Indonesia. Businesses that run online are certainly related to the business processes of the company, which depend on technology, and company data is also stored online. The data stored online is very vulnerable to leakage and theft. The company stated that it had experienced data loss in the form of a hacked Instagram account and had never used information security evaluation since it first implemented digitization for its business processes. Measuring the maturity level and completeness of information management with the Information Security Index version 4.0 that references ISO 27001:2013 is a way to improve the quality of information security management in the company. The survey is conducted as needed by determining area to be evaluated with a SWOT analysis. Areas of information security governance, information security framework, technology, and information security are under evaluation. Out of a total score of 50, the results of the evaluation of the electronic systems category are 23, meaning that they fall into the high category. The results of the maturity level

evaluation of information security in 3 areas, namely 63 out of a total score of 645, were given an unattainable category with maturity levels of I to I+. Based on the results of the evaluation, the researcher makes recommendations based on ISO 27002:2013 Control, including creating a secure procedure for information exchange between information security managers and internal and external agencies.

Keywords: *Information Security Index, ISO 27001, ISO Control 27002, Information Security Management*

PENDAHULUAN

Seiring berkembangnya teknologi informasi, informasi sangat mudah didapat dan disebarluaskan sehingga menjadi aset yang membantu memudahkan pekerjaan bagi individu, pemerintah dan sektor swasta [1]. Negara Indonesia masih perlu adanya wawasan mengenai pentingnya sebuah informasi. Dikutip dari hasil penelitian pada tahun 2021 yang dipublikasikan oleh *International Telecommunication Union* (ITU) menjelaskan bahwa *Global Cyber Security Index* adalah pendasaran yang valid sebagai tolak ukur komitmen beberapa negara anggota terhadap keamanan siber tingkat dunia. Pada tahun 2020 Indonesia ada pada peringkat ke-24 dari 194 negara, hal tersebut merupakan kabar baik karena pada tahun 2018 Indonesia berada di peringkat ke-41 [2].

Tetapi hal tersebut tidak dapat digunakan sebagai pembenaran bahwa Indonesia telah baik dalam perlindungan keamanan informasi sehingga tidak perlu adanya tindakan pencegahan lagi. Jika dilihat dari data tersebut, maka sebaiknya perlu untuk meningkatkan keamanan informasi meskipun tanpa dinilai seperti itu, karena keamanan informasi sangatlah penting. Tujuan dari keamanan informasi adalah untuk menjaga dan memperhatikan faktor keamanan dari semua perangkat pendukung, jaringan dan fasilitas lainnya yang secara langsung maupun tidak langsung berhubungan dengan proses pengolahan informasi [3]. Keamanan informasi merupakan suatu Tindakan pencegahan dari berbagai ancaman penyalahgunaan informasi dan perlindungan terhadap aset informasi [4]. Keamanan informasi adalah aspek penting yang harus diatur dan diterapkan untuk Informasi yang didapatkan secara *real-time* dan akurat dari sistem perusahaan, dapat membuat para pemimpin memberikan keputusan bisnis dengan baik [5].

Hal ini perlu diterapkan serta diperhatikan oleh Perusahaan Pemula berbasis Teknologi di Surabaya. Perusahaan tersebut bergerak pada bidang *online shop* dan juga sebagai Distributor Produk Parfum Baju Pertama di Indonesia. Perusahaan perdagangan *online* pasti berkaitan dengan proses bisnis perusahaan seperti data transaksi, data keluar masuk barang, dan data target pasar yang tersimpan secara *online* [6]. Data-data yang tersimpan *online* sangat rentan terhadap kebocoran dan pencurian [7]. Pihak perusahaan menyatakan bahwa perusahaan ini pernah mengalami kehilangan data berupa akun Instagram yang diretas sehingga tidak dapat digunakan. Perusahaan tersebut juga belum pernah menggunakan evaluasi kemanan informasi sejak pertama kali menerapkan digitalisasi untuk proses bisnis mereka sehingga perusahaan tersebut kurang mengetahui seberapa matang tingkat kesiapan penerapan keamanan informasi pada perusahaan.

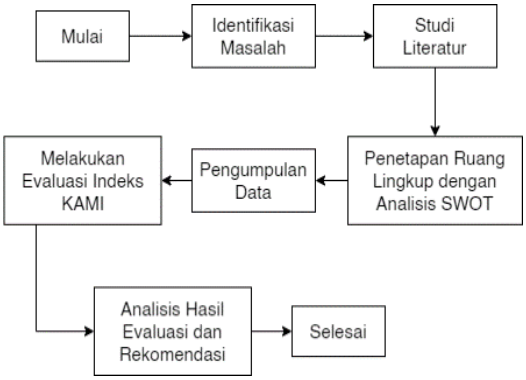
Pengukuran tingkat kematangan dan kelengkapan manajemen informasi dibantu dengan suatu alat yang disebut Indeks KAMI (Keamanan Informasi). Indeks KAMI adalah salah satu cara dalam meningkatkan kualitas sistem manajemen keamanan informasi pada perusahaan [8]. Sistem Manajemen Keamanan Informasi perlu diterapkan pada suatu perusahaan agar dapat mencegah hal-hal yang berkaitan dengan kebocoran informasi sehingga merugikan perusahaan. ISO/IEC 27001 adalah Standar Internasional Sistem Manajemen Keamanan Informasi yang paling terkenal. Pengukuran tingkat keamanan

informasi yang akurat melalui proses yang diterapkan dapat menggunakan standar tersebut [9]. Kumpulan peraturan dan tata cara dalam memanajemen data sensitif instansi secara terstruktur adalah pengertian Sistem Manajemen Keamanan Informasi (SMKI). SMKI bertujuan untuk memastikan berjalannya proses bisnis dengan melakukan pembatasan akibat pelanggaran keamanan informasi dan meminimalkan risiko [10].

Indeks KAMI mengacu pada ISO 27001 yang berisi tentang keamanan informasi [11]. Spesifikasi kebutuhan untuk sistem manajemen keamanan informasi merupakan ISO/IEC 27001. Standar internasional ini digunakan sebagai dasar untuk sertifikasi terakreditasi [12]. ISO 27001:2013 adalah bagian dari sistem manajemen dalam suatu organisasi berdasarkan pendekatan risiko bisnis yang bertujuan untuk membangun, menerapkan, mengoperasikan, mengamati, memelihara, dan meningkatkan keamanan informasi. Aplikasi dari ISO/IEC 27001 memungkinkan organisasi atau perusahaan untuk mengukur kinerja dan memberikan informasi yang relevan tentang Keamanan Informasi [13]. Dengan adanya evaluasi tersebut, perusahaan dapat memastikan bahwa kondisi tingkat kesiapan penerapan keamanan informasi dan dapat menggunakannya sebagai bahan evaluasi dan pengembangan manajemen keamanan informasi.

METODE

Penelitian ini dilakukan dengan menerapkan langkah-langkah yang sistematis sehingga pengerjaan lebih terorganisir. Langkah-langkah dalam penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Langkah-langkah penelitian

Gambar 1 menjelaskan Langkah-langkah penelitian ini yang dimulai dari Identifikasi Masalah, Studi Literatur, Penetapan Ruang Lingkup dengan Analisis *SWOT*, Pengumpulan Data, Melakukan Evaluasi Indeks KAMI, dan yang terakhir Analisis Hasil Evaluasi dan Rekomendasi.

a. Identifikasi Masalah

Identifikasi masalah dilakukan pada Perusahaan Pemula berbasis Teknologi di Surabaya. Perusahaan tersebut merupakan Pusat Distributor Parfum Baju Pertama di Indonesia yang semua proses bisnisnya dilakukan secara digital (*online*) seperti penerimaan bahan baku sampai penjualan ke pelanggan. Perusahaan ini belum pernah menggunakan evaluasi kemanan informasi sejak pertama kali menerapkan digitalisasi untuk proses bisnis mereka sehingga perusahaan tersebut kurang mengetahui seberapa matang tingkat kesiapan penerapan keamanan informasi pada perusahaan.

b. Studi Literatur

Pada tahap studi literatur dilakukan pengumpulan konsep dan teori sebagai dasar untuk mendapatkan beberapa landasan pemikiran dalam mendukung proses penelitian dengan cara mencari, membaca, dan merangkum beberapa referensi penelitian terdahulu seperti jurnal penelitian dan *e-book* yang sesuai dengan topik penelitian ini.

c. Penetapan Ruang Lingkup dengan Analisis *SWOT*

Penetapan ruang lingkup penelitian ini dengan melalukan analisis *SWOT* terhadap tingkat kepentingan penilaian

pada ketujuh area Indeks KAMI. Setiap area pada Indeks KAMI dianalisis apakah telah sesuai dengan kebutuhan Perusahaan kemudian dikelompokkan ke salah satu *SWOT* itu sendiri (*Strength, Weakness, Opportunities, Threat*). Untuk Area yang masuk ke dalam kategori *Weakness* dan *Treat* merupakan area yang akan dievaluasi dengan Indeks KAMI.

d. Pengumpulan Data

Pada tahap pengumpulan data ini yaitu dengan melakukan wawancara dan observasi lapangan. Wawancara dan Observasi lapangan dilakukan dengan menanyakan beberapa pertanyaan yang telah tercantum pada pedoman Indeks KAMI, dan juga melengkapi dokumen pendukung sebagai bukti dalam bentuk peraturan dan data-data terkait alur proses bisnisnya. Pertanyaan-pertanyaan pada proses wawancara diajukan kepada *CEO* (*Chief Executive Officer*), *CTO* (*Chief Technology Officer*), dan *HRD* Perusahaan. Narasumber yang dipilih tersebut merupakan petinggi perusahaan yang mengetahui semua alur proses bisnis yang dilakukan secara digitalisasi sehingga informasi yang didapatkan benar adanya dan bisa menghasilkan rekomendasi yang tepat sesuai dengan apa yang diperlukan oleh perusahaan terkait pengelolaan kemanan informasi.

e. Melakukan Evaluasi Indeks KAMI

Tahap penilaian ini dilakukan dengan mengevaluasi tingkat keamanan informasi menggunakan pedoman Indeks KAMI (Indeks Keamanan Informasi) Versi 4.0 berdasarkan kriteria ISO/IEC 27001. Indeks Keamanan Informasi (KAMI) adalah aplikasi yang digunakan sebagai alat untuk mengevaluasi dan menilai kesiapan (kelengkapan dan kematangan) suatu aplikasi keamanan informasi terhadap kriteria SNI ISO/IEC 27001. Indeks KAMI tidak dimaksudkan untuk menganalisis kelayakan atau efektivitas bentuk keamanan yang ada, tetapi lebih sebagai alat untuk memberikan pemahaman kepada instansi mengenai tingkat kesiapan kerangka kerja keamanan informasi [14].

Terdapat 3 bagian evaluasi pada Indeks KAMI. Bagian Evaluasi Pertama yaitu mengklasifikasikan Kategori Sistem Elektronik pada instansi. Bagian Evaluasi Kedua yaitu mengevaluasi area Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi Tingkat Kematangan dan Kelengkapan yang termasuk pada 5 area Pengamanan Informasi. Kemudian Bagian Evaluasi Ketiga yaitu mengevaluasi tiga aspek yang dapat mendeteksi munculnya risiko terhadap keamanan informasi diantaranya evaluasi kesiapan Keterlibatan Pihak Ketiga, Layanan Infrastruktur Awan, dan Perlindungan Data Pribadi dalam keamanannya [15].

f. Analisis Hasil Evaluasi dan Rekomendasi

Berdasarkan analisis hasil evaluasi dapat ditarik kesimpulan terkait tingkat keamanan informasi perusahaan sehingga bermanfaat sebagai pembahasan dan saran rekomendasi untuk area yang masih perlu peningkatan dan perbaikan, agar memiliki kerangka kerja yang lebih baik untuk keamanan informasi di alur proses bisnisnya yang tentu akan berisiko dengan adanya data penting seperti data pribadi, data pelanggan, dan keuangan.

HASIL DAN PEMBAHASAN

Evaluasi tingkat kematangan dan kelengkapan manajemen keamanan informasi di Perusahaan ini menggunakan Indeks KAMI Versi 4.0 dilakukan sesuai kebutuhan perusahaan, sehingga perlu adanya penetapan ruang lingkup dari kelima area pada Indeks KAMI yang sebaiknya perlu di evaluasi. Penetapan ruang lingkup ini menggunakan metode Analisis *SWOT*. Bahan untuk menganalisis kebutuhan perusahaan telah didapatkan melalui Proses Wawancara yang dilakukan dengan pihak yang berwenang dan bertanggung jawab dalam sistem teknologi dan digitalisasi perusahaan yaitu *CTO* (*Chief Technology Officer*).

Berikut hasil yang didapatkan dari Analisis *SWOT*.

[1] Area yang termasuk ***Strength*** yaitu Pengelolaan Aset Keamanan Informasi. Berdasarkan hasil wawancara mengenai area tersebut, didapatkan banyak hal yang telah diatur dan sebagian diterapkan menurut pedoman Indeks KAMI diantaranya sudah terdapat tata tertib penggunaan aset perusahaan, daftar inventaris perusahaan, dan aturan mengenai HAKI terhadap Si Peniru.

[2] Area yang termasuk ***Weakness*** yaitu Kerangka Kerja Keamanan Informasi & Teknologi dan Keamanan Informasi. Berdasarkan hasil wawancara. Area Kerangka Kerja Keamanan Informasi belum menerapkan otoritas untuk melakukan *download* data dan pengolahan data pada *Microsoft Excel* belum diatur dengan jelas. Sedangkan pada area Teknologi dan Keamanan Informasi masih dalam lingkup kecil dan sederhana, sehingga teknologi yang digunakan tidak memiliki aturan dan sistem secara detail.

[3] Area yang termasuk ***Opportunity*** yaitu Pengelolaan Risiko Keamanan Informasi. Dari hasil wawancara yang didapatkan untuk area tersebut telah diatur dengan baik meskipun belum terdapat aturan yang tertulis contohnya yaitu penyelasaian dari masalah Akun Instagram yang diretas dan memiliki kekuatan hukum untuk HAKI *Brand* Perusahaan.

[4] Area yang termasuk ***Threat*** yaitu Tata Kelola Keamanan Informasi. Pada area tersebut belum memiliki aturan dan pemegang khusus untuk bagian Pengelolaan Keamanan Informasi di Perusahaan ini, meskipun beberapa sistem telah memiliki SOP.

Berdasarkan Analisis *SWOT* didapatkan area yang akan dievaluasi dengan menggunakan Pedoman Indeks KAMI. Area tersebut yaitu area yang termasuk ke dalam kategori *Weakness* dan *Threat*, karena dianggap lemah dan dapat menyebabkan ancaman bagi perusahaan. Sehingga kesimpulannya terdapat 3 (tiga) area yang akan dievaluasi untuk mengetahui tingkat kematangan dan kelengkapan manajemen keamanan informasi di perusahaan tersebut diantaranya Kerangka Kerja Keamanan Informasi, Teknologi dan Keamanan Informasi, dan Tata Kelola Keamanan Informasi.

a. Evaluasi Indeks KAMI

Penilaian untuk mengevaluasi manajemen keamanan informasi dilakukan dengan menjawab 140 pertanyaan menggunakan Indeks KAMI dari 194 pertanyaan yang terdapat pada 7 bagian area evaluasi. Penelitian ini ditujukan untuk mengevaluasi bagian yang paling dibutuhkan oleh perusahaan, sehingga beberapa pertanyaan memang tidak ditanyakan saat wawancara evaluasi Indeks KAMI.

Kategori Sistem Elektronik, Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi, dan Suplemen termasuk dalam 7 bagian area evaluasi tersebut. Kemudian, dikelompokkan menjadi 3 bagian karena memiliki metode penilaian evaluasi yang berbeda. Metode Penilaian evaluasi pertama dilakukan pada bagian Kategori Sistem Elektronik. Metode penilaian evaluasi kedua digunakan untuk menilai Tingkat Kematangan Manajemen Keaman Informasi yang terdiri dari 5 area pengamanan informasi. Agar sesuai dengan kebutuhan perusahaan, maka dilakukan penilaian hanya terhadap 3 area pengamanan informasi yang telah melewati proses Analisis *SWOT*. Tiga area tersebut diantaranya Tata Kelola Keamanan Informasi, Kerangka Kerja Keamanan Informasi Teknologi dan Keamanan Informasi. Metode penilaian evaluasi ketiga dilakukan pada bagian Suplemen.

a) Evaluasi Kategori Sistem Elektronik

Penilaian pada area Kategori Sistem Elektronik terdapat 10

pertanyaan. Setiap pertanyaan memiliki 3 jawaban yang dapat dipilih sesuai status kondisi pada perusahaan. Setiap poin jawaban memiliki skor yang telah ditentukan dalam Pedoman Indeks KAMI Versi 4.0. Kemudian skor dari setiap jawaban dijumlah dan menghasilkan total skor yang selanjutnya dapat dikategorikan sesuai pilihan kategori yang terdapat pada Indeks KAMI Versi 4.0. Terdapat tiga kategori hasil Evaluasi Sistem Elektronik yaitu Rendah, Tinggi, dan Strategis seperti yang tertera pada Tabel 1.

Tabel 1. Kategori sistem elektronik

Skor	Kategori
10 - 15	Rendah
16 - 34	Tinggi
35 - 50	Strategis

Dari hasil wawancara, Evaluasi Kategori Sistem Elektronik didapatkan total skor 23. Berdasarkan Tabel 1, skor yang berjumlah 23 termasuk pada rentang 16 – 34 dengan Kategori Tinggi. Definisi dari Kategori Tinggi disini adalah penggunaan sistem elektronik pada perusahaan memiliki pengaruh yang tinggi dalam mendukung proses bisnis yang berjalan.

b) Evaluasi 3 Area Pengamanan Informasi

Penilaian pada bagian ini yaitu mengevaluasi tingkat kematangan dan kelengkapan pengamanan informasi pada 3 dari 5 area Indeks KAMI Versi 4.0 diantaranya Tata Kelola Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Teknologi dan Keamanan Informasi. Pada penelitian ini ditetapkan 3 area saja yang akan dievaluasi karena disesuaikan dengan kebutuhan perusahaan melalui proses Analisis *SWOT*.

Setiap status pengamanan dari pertanyaan pada area Indeks KAMI Versi 4.0 memiliki nilai skor yang telah ditentukan sebagai berikut.

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Gambar 2. Pemetaan skor indeks KAMI versi 4.0

Berdasarkan Gambar 2 pada kolom Kategori Pengamanan memiliki 3 jenis kategori. Kategori pengamanan 1 merupakan area untuk mengukur kerangka kerja dasar kemanan informasi. Kategori Pengamanan 2 merupakan area untuk mengukur efektivitas dan konsistensi penerapannya. Kemudian, Kategori Pengamanan 3 merupakan area untuk mengukur kemampuan peningkatan kinerja keamanan informasi. Kategori Pengamanan tersebut tertera pada kolom ketiga tabel evaluasi Indeks KAMI Versi 4.0. Sehingga setiap status pengamanan dari kategori pengamanan yang berbeda memiliki nilai skornya masing-masing. Pengisian pertanyaan dengan kategori pengamanan 3 dapat dinilai jika kategori pengamanan 1 dan 2 telah diisi minimal dengan posisi “Dalam Penerapan atau Diterapkan Sebagian”.

Analisis hasil evaluasi 3 area pengamanan informasi dijelaskan sebagai berikut :

a) Evaluasi Tata Kelola Keamanan Informasi

Status Penerapan	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	0	0	0	-	0
Dalam Perencanaan	9	0	0	-	9
Dalam Penerapan / Diterapkan Sebagian	0	0	0	-	0
Diterapkan Secara Menyeluruh	0	0	0	-	0
Total	9	0	0	-	9
Skor Minimum	12	8	24	-	Tidak Mencapai
Skor Pencapaian	36	14	54	-	Tidak Mencapai
Total Skor Area	126				

Gambar 3. Skor area tata kelola keamanan informasi

Berdasarkan hasil wawancara, pada Gambar 3 total skor evaluasi area Tata Kelola Keamanan Informasi sebesar 9 dari nilai total area 126, sehingga persentase yang didapatkan yaitu 7%. Skor tersebut bernilai kecil disebabkan karena pertanyaan kategori pengamanan 1 dan 2 diisi dalam posisi “Dalam Perencanaan”, sedangkan selebihnya “Tidak Dilakukan”. Pertanyaan kategori pengamanan 3 tidak dapat diisi karena kategori pengamanan 1 dan 2 tidak

memenuhi skor minimum menuju pertanyaan kategori pengamanan 3 yaitu 48. Evaluasi area Tata Kelola Keamanan Informasi berada pada Tingkat Kematangan I. Hal itu berdasarkan perbandingan total skor hasil evaluasi dengan skor minimal setiap kategori pengamanan yang telah ditetapkan Indeks KAMI Versi 4.0. Didapat bahwa skor 9 tidak melampaui skor minimum Tingkat Kematangan II pada area ini.

b) Evaluasi Kerangka Kerja Pengelolaan Keamanan Informasi

Status Penerapan	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	0	0	0	-	0
Dalam Perencanaan	9	3	0	-	12
Dalam Penerapan / Diterapkan Sebagian	0	0	0	-	0
Diterapkan Secara Menyeluruh	3	9	0	-	12
Total	12	12	0	-	**24**
Skor Minimum	15	45	15	12	Tidak Mencapai
Skor Pencapaian	24	62	27	18	Tidak Mencapai
Total Skor Area	**159**				

Gambar 4. Skor area kerangka kerja pengelolaan keamanan informasi

Berdasarkan hasil wawancara, pada Gambar 4 total skor evaluasi area Kerangka Kerja Keamanan Informasi sebesar 24 dari nilai total area 159, sehingga persentase yang didapatkan yaitu 15%. Skor tersebut bernilai kecil disebabkan karena pertanyaan kategori pengamanan 1 dan 2 diisi dalam posisi "Dalam Perencanaan", sedangkan selebihnya "Tidak Dilakukan", dan terdapat 3 pertanyaan yang diisi dalam posisi "Diterapkan Secara Menyeluruh". Pertanyaan kategori pengamanan tidak dapat diisi karena kategori pengamanan 1 dan 2 tidak memenuhi skor minimum menuju pertanyaan kategori pengamanan 3 yaitu 64. Evaluasi area Kerangka Kerja Keamanan Informasi berada pada Tingkat Kematangan I. Hal itu berdasarkan perbandingan total skor hasil evaluasi dengan skor minimal setiap kategori pengamanan yang telah ditetapkan Indeks KAMI Versi 4.0. Didapat bahwa skor 24 tidak melampaui skor minimum Tingkat Kematangan II pada area ini.

c) Evaluasi Teknologi dan Keamanan Informasi

Status Penerapan	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	0	0	0	-	0
Dalam Perencanaan	4	5	0	-	9
Dalam Penerapan / Diterapkan Sebagian	0	0	0	-	0
Diterapkan Secara Menyeluruh	15	6	0	-	21
Total	19	11	0	-	**30**
Skor Minimum	18	40	6	-	I+
Skor Pencapaian	28	62	9	-	Tidak Mencapai
Total Skor Area	**120**				

Gambar 5. Skor area teknologi dan keamanan informasi

Berdasarkan hasil wawancara, pada Gambar 5 total skor evaluasi area Teknologi dan Keamanan Informasi sebesar 30 dari nilai total area 120, sehingga persentase yang didapatkan yaitu 25%. Skor tersebut bernilai kecil disebabkan karena pertanyaan kategori pengamanan 1 dan 2 diisi dalam posisi "Dalam Perencanaan", sedangkan selebihnya "Tidak Dilakukan", dan terdapat 6 pertanyaan yang diisi dalam posisi "Diterapkan Secara Menyeluruh". Pertanyaan kategori pengamanan 3 pada Tingkat Kematangan IV tidak dapat diisi karena kategori pengamanan 1 dan 2 tidak memenuhi skor minimum yaitu 68. Evaluasi area Teknologi dan Keamanan Informasi berada pada Tingkat Kematangan I+. Hal itu berdasarkan perbandingan total skor hasil evaluasi dengan skor minimal setiap kategori pengamanan yang telah ditetapkan Indeks KAMI Versi 4.0. Didapat bahwa skor 30 telah melampaui skor pencapaian Tingkat Kematangan II pada area ini.

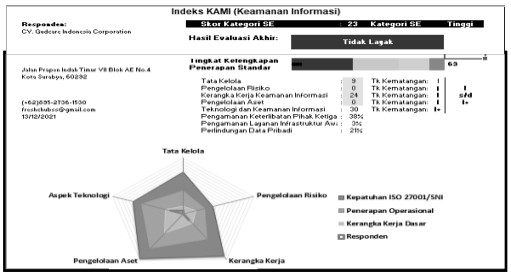
c) Evaluasi Suplemen

Penilaian pada area Suplemen memiliki 3 aspek pertanyaan untuk dievaluasi diantaranya evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastruktur Awan, dan Perlindungan Data Pribadi. Sama seperti bagian evaluasi sebelumnya, jawaban dari setiap pertanyaan memiliki status pengamanan dengan perhitungan nilai skor mengacu pada Gambar 2. Perbedaan area Suplemen ini dengan kelima area evaluasi yaitu tidak adanya perhitungan total skor evaluasi dan bukan merupakan indikator untuk menilai Evaluasi Tingkat Kematangan dan Kelengkapan Keamanan Informasi pada Indeks KAMI. Berdasarkan pedoman Indeks KAMI, area Suplemen bertujuan melibatkan

ketiga aspek tersebut agar perusahaan mengetahui akan adanya risiko terhadap keamanan informasi.

Dari hasil wawancara Evaluasi Suplemen dapat diketahui bahwa perhitungan skor dilakukan dengan menghitung rata-rata dari total skor terhadap jumlah pertanyaan di setiap aspek. Didapatkan skor rata-rata aspek Pengamanan Keterlibatan Pihak Ketiga yaitu 1,15 (38%), skor rata-rata aspek Pengamanan Layanan Infrastruktur Awan yaitu 0,10 (3%), dan skor rata-rata aspek Perlindungan Data Pribadi yaitu 0,63 (21%). Nilai Persentase setiap aspek didapatkan dari skor rata-rata dibagi dengan 3 aspek area Suplemen.

b. Analisis Hasil Akhir Evaluasi Indeks KAMI



Gambar 4. *Dashboard* hasil evaluasi indeks KAMI

Dashboard hasil evaluasi Indeks KAMI Perusahaan *Online Shop* dan Distributor Parfum Baju ditunjukkan pada Gambar 6. *Dashboard* tersebut tertera hasil evaluasi akhir status kesiapan pengamanan informasi, hasil evaluasi tingkat kematangan masing-masing area, dan tingkat kelengkapan penerapan sesuai standar ISO 27001 dengan *Radar Chart*. Berdasarkan Gambar 6, skor kategori untuk sistem elektronik ditetapkan menjadi 23 yang termasuk dalam kategori Tinggi. Kemudian, dari hasil evaluasi akhir Tingkat Kematangan Dan Kelengkapan Keamanan Informasi, statusnya "Tidak Layak" dengan skor 63, dan Tingkat Kelengkapan Penerapan Sesuai Standar ISO 27001 pada Level I hingga I+. Skor 63 berasal dari total skor akhir dari tiga area yang dievaluasi, diantaranya area Tata Kelola Keamanan Informasi sebesar 9 dengan Tingkat Kematangan I, Kerangka Keamanan Informasi sebesar 24 dengan Tingkat Kematangan I, Teknologi Informasi dan Keamanan mendapat skor 30 dengan Tingkat Kematangan I+. Untuk area Pengelolaan Risiko Keamanan Informasi dan Pengelolaan Aset Informasi, nilainya 0 karena area tersebut tidak dievaluasi pada penelitian ini. *Radar Chart* pada *Dashboard* menunjukkan bahwa tiga area pengamanan informasi yang telah dievaluasi masih dalam tahap pemenuhan Kerangka Kerja Dasar sesuai kepatuhan terhadap ISO 27001.

Secara keseluruhan Hasil Akhir Evaluasi Indeks Kami Perusahaan ini menunjukkan bahwa besarnya pengunaan sistem elektronik pada instansi tidak mendukung penerapan manajemen keamanan informasi yang memadai. Sehingga mendapatkan hasil evaluasi dengan status "Tidak Layak" dan berada pada Tingkat Kematangan I sampai dengan I+. Dimana untuk pengukuran Indeks KAMI, tingkat kematangan tersebut berada pada Tahap Kondisi Awal.

c. Rekomendasi

Pemberian rekomendasi dilakukan terhadap bagian penting yang kurang pada setiap area yang telah dievaluasi berdasarkan Kontrol ISO/IEC 27002:2013. Dengan memberikan rekomendasi ini diharapkan dapat menjadi media evaluasi perbaikan untuk Manajemen Keamanan Informasi di Perusahaan yang menjadi objek penelitian ini. Rekomendasi untuk setiap area yang telah dievaluasi dijelaskan sebagai berikut.

d) Rekomendasi Tata Kelola Keamanan Informasi

Berikut rekomendasi yang diberikan untuk beberapa kondisi yang kurang pada Area Tata Kelola Kemanan Informasi Perusahaan. Pada Tabel 2 menjelaskan tentang kekurangan pada Area Tata Kelola Kemanan Informasi. Sehingga berdasarkan Kontrol ISO 27002:2013, masalah tersebut dapat diatasi dengan cara yang tertera pada Tabel 2.

Tabel 2. Rekomendasi tata kelola keamanan informasi

No	Kondisi yang Kurang	Rekomendasi berdasarkan Kontrol ISO 27002:2013
1.	Belum memiliki kebijakan dalam pelaksanaan program keamanan informasi	**A.5.1.1 Kebijakan untuk Keamanan Informasi** Membuat serangkaian prosedur dalam pelaksanaan program keamanan informasi
2.	Belum mendefinisikan tanggung jawab keberlangsungan Layanan TIK	**A.6.1.1 Peran dan Tanggung Jawab Keamanan Informasi** Instansi harus mendefinisikan serta mengalokasikan untuk Langkah-langkah keberlangsungan Layanan TIK
3.	Belum adanya kompetensi keahlian pelaksana dan pemahaman keamanan informasi bagi semua pihak yang terkait pada Instansi	**A.7.2.2 Kepedulian, Pendidikan, dan Pelatihan Keamanan Informasi** Mengadakan program pelatihan pengelolaan keamanan informasi untuk semua pihak instansi yang terkait
4.	Belum diterapkan koordinasi pengelolaan keamanan informasi dengan pihak Internal maupun Eksternal Instansi dalam pertukaran informasi	**A.13.2.2 Perjanjian Perpindahan Informasi** Menciptakan proses pertukaran informasi yang aman antara manajer keamanan informasi dan lembaga internal dan eksternal

e) Rekomendasi Kerangka Kerja Pengelolaan Keamanan Informasi

Berikut rekomendasi yang diberikan untuk beberapa kondisi yang kurang pada Area Kerangka Kerja Pengelolaan Kemanan Informasi Perusahaan. Pada Tabel 3 menjelaskan tentang kekurangan pada Area Kerangka Kerja Pengelolaan Kemanan Informasi. Sehingga berdasarkan Kontrol ISO 27002:2013, masalah tersebut dapat diatasi dengan cara yang tertera pada Tabel 3.

Tabel 3. Rekomendasi kerangka kerja pengelolaan keamanan informasi

No	Kondisi yang Kurang	Rekomendasi berdasarkan Kontrol ISO 27002:2013
1.	Belum terdapat serangkaian kebijakan dan prosedur untuk mengatur keamanan informasi	**A.5.1.1 Kebijakan untuk Keamanan Informasi** Mewujudkan serangkaian prosedur dalam pelaksanaan program keamanan informasi
2.	Belum melibatkan aspek keamanan informasi dalam lingkup manajemen proyek	**A.6.1.5 Keamanan Informasi dalam Manajemen Proyek** Instansi harus melibatkan aspek keamanan informasi dalam lingkup manajemen proyek, tanpa memperhatikan tipe proyeknya
3.	Belum menerapkan manajemen penanggulangan risiko dalam perubahan sistem	**A.12.1.2 Manajemen Perubahan** Membuat prosedur penanggulangan risiko dari suatu perubahan yang mempengaruhi keamanan informasi pada Instansi.
4.	Belum memiliki kebijakan pengembangan sistem yang aman (*Secure SDLC*)	**A.14.2.1 Kebijakan Pengembangan yang Aman** Membuat aturan untuk diterapkan pada pengembangan perangkat lunak dan sistem
5.	Belum memiliki kerangka kerja untuk mengelola perencanaan keberlangsungan keamanan informasi	**A.17.1.1 Perencanaan Keberlangsungan Keamanan Informasi** Mewujudkan prosedur untuk keberlangsungan manajemen keamanan informasi

f) Rekomendasi Teknologi dan Keamanan Informasi

Berikut rekomendasi yang diberikan untuk beberapa kondisi yang kurang pada Area Teknologi dan Kemanan Informasi Perusahaan. Pada Tabel 4 menjelaskan tentang kekurangan pada Area Teknologi dan Kemanan Informasi. Sehingga berdasarkan Kontrol ISO 27002:2013, masalah tersebut dapat diatasi dengan cara yang tertera pada Tabel 4.

Tabel 4. Rekomendasi teknologi dan keamanan informasi

No	Kondisi yang Kurang	Rekomendasi berdasarkan Kontrol ISO 27002:2013
1.	Belum menerapkan program pengecekan untuk mengidentifikasi kelemahan konfigurasi terhadap jaringan, sistem, aplikasi yang digunakan secara rutin	**A.11.2.4 Pemeliharaan Peralatan** Instansi harus menerapkan program pemeliharaan dengan mengecek semua jaringan, sistem, aplikasi yang digunakan.
2.	Belum menerapkan *logging* untuk merekam upaya akses oleh yang tidak berhak	**A.12.4.1 Pencatatan Kejadian (*Event Logging*)** Membuat dan menerapkan pencatatan kejadian yang merekam aktivitas.
3.	Belum menerapkan enkripsi untuk melindungi aset informasi penting	**A.10.1.2 Manajemen Kunci** Menerapkan kunci enkripsi terhadap penggunaan dan perlindungan aset informasi penting pada Instansi.
4.	Belum menerapkan penggantian *password* secara otomatis pada sistem dan aplikasi	**A.9.4.3 Sistem Manajemen Kata Kunci (*password*)** Membuat sistem manajemen kata kunci seperti penggantian *password* otomatis
5.	Sistem belum memiliki mekanisme sinkronisasi waktu yang akurat	**A.12.4.4 Sinkronisasi Waktu** Menerapkan sinkronisasi waktu yang akurat untuk semua sistem pengolahan informasi
6.	Belum memiliki pengamanan untuk mengelola akses jaringan	**A.13.1.2 Keamanan Layanan Jaringan** Melakukan pengelolaan untuk mengamankan layanan jaringan dari yang tidak berhak
7.	Belum menentukan spesifikasi dan fitur keamanan selama pengembangan dan pengujian aplikasi	**A.14.2.8 Pengujian Keamanan Sistem** Instansi harus melakukan tes fungsi keamanan selama pengembangan aplikasi

SIMPULAN

Hasil evaluasi tingkat kematangan dan kelengkapan manajemen keamanan informasi Perusahaan *Online Shop* dan Distributor Parfum Baju dari penelitian ini dilakukan pada 3 Area Pengamanan Informasi mendapat hasil "Tidak Layak" dengan tingkat kematangan pada level I hingga I+ yaitu masih dalam tahap Kondisi Awal Penerapan Manajemen Keamanan Informasi. Kondisi tersebut dikarenakan terdapat banyak pertanyaan yang diajukan berada dalam status "Tidak Dilakukan" dan "Dalam Perencanaan", serta hanya beberapa yang diisi dengan status "Diterapkan Secara Menyeluruh". Berdasarkan hal tersebut, penulis memberikan rekomendasi berdasarkan Kontrol ISO 27002:2013, salah satunya yaitu membuat prosedur pertukaran informasi yang aman antara pengelola keamanan informasi dengan pihak Internal maupun Eksternal Instansi.

SARAN

Diharapkan rekomendasi perbaikan untuk Perusahaan *Online Shop* dan Distributor Parfum Baju dari penelitian ini dapat diterapkan agar tidak ada lagi hal yang merugikan instansi mengenai keamanan informasi. Selain itu, Instansi dapat melakukan dua kali Evaluasi Keamanan Informasi dengan Indeks KAMI selama setahun untuk menilai kesiapan keamanan informasi dan mengukur keberhasilan perbaikan yang dilakukan, sehingga tingkat kesiapan dan kematangan keamanan informasi dapat mencapai level III+ sebagai ambang batas minimal ISO 27001.

DAFTAR PUSTAKA

[1] R. Setyawan, A. Nugroho, K. E.

Susilo, B. Web, P. Gunung, and D. I. Mojokerto, "Metode Prototype Perancangan Smart Mountain Berbasis Web Studi Kasus Gunung Di Mojokerto," vol. XII, no. 2, pp. 80–89, 2021.

[2] Ayp, "BSSN: Indeks Keamanan Siber RI Peringkat 24 dari 194 Negara," *CNN Indonesia*, 2021. https://www.cnnindonesia.com/teknologi/20210907150335-185-690926/bssn-indeks-keamanan-siber-ri-peringkat-24-dari-194-negara (accessed Oct. 18, 2021).

[3] A. P. Galih, "Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan IPusnas," *AL Maktab.*, vol. 5, no. 1, p. 10, 2020, doi: 10.29300/mkt.v5i1.3086.

[4] B. Rahardjo, *Keamanan Informasi & Jaringan*. 2017.

[5] A. Nugroho, D. Rizaludin, S. Soebandhi, L. Junaedi, S. Winardi, and M. N. Al-Azam, "Automatic Sign of Commencement of Work from Enterprise Resource Planning," *Proceeding - ICoSTA 2020 2020 Int. Conf. Smart Technol. Appl. Empower. Ind. IoT by Implement. Green Technol. Sustain. Dev.*, 2020, doi: 10.1109/ICoSTA48221.2020.1570590248.

[6] B. W. Suhanjoyo and N. Aryo, "Perancangan Aplikasi Gugus Penjualan Terintegrasi Erp," *Conf. Innov. Appl. Sci. Technol. (CIASTECH 2020)*, no. Ciastech, pp. 461–470, 2020.

[7] P. Widodo and D. Gunawan, "Efektivitas keamanan informasi dalam menghadapi ancaman social engineering effectiveness of information security threats facing social engineering," *Ef. Keamanan Inf. Dalam Menghadapi Ancaman Soc. Eng.*, pp. 73–90, 2017.

[8] B. A. Firzah, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Berdasarkan Iso / Iec 27001 : 2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (Dptsi) Its Surabaya Evaluating Information Security Management Using Ind," vol. 6, no. 1, 2017.

[9] R. A. Syarif and A. Nugroho, "Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur Dengan Menggunakan Indeks Keamanan Informasi (Studi Kasus: Aplikasi Span)," *J. Info Artha*, vol. 4, pp. 69–80, 2016, [Online]. Available: http://www.jurnal.stan.ac.id/index.php/JIA/article/view/46.

[10] ITGID, "Information Security Management System (ISMS) : ISO 27001," *IT Governance Indonesia*, 2021. https://itgid.org/information-security-management-system-isms-iso-27001/ (accessed Nov. 04, 2021).

[11] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[12] B. Kenyon, *ISO 27001 Controls – A guide to implementing and auditing*. IT Governance Ltd, 2019.

[13] I. M. Lopes, T. Guarda, and P. Oliveira, "Implementation of ISO 27001 Standards as GDPR Compliance Facilitator Implementation of ISO 27001 Standards as GDPR Compliance Facilitator," no. December, 2019,

doi: 10.29333/jisem/5888.

[14] BSSN, "Konsultasi dan Assessment Indeks KAMI," *Badan Siber dan Sandi Negara Indonesia*, 2021. https://bssn.go.id/indeks-kami/ (accessed Nov. 05, 2021).

[15] F. Husin, H. F.Wowor, and S. D.S Karouw, "Implementasi Indeks Kami Di Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 12, no. 1, 2017, doi: 10.35793/jti.12.1.2017.17869.