BAB IV

HASIL DAN PEMBAHASAN

4.1. Objek Penelitian

4.1.1 Profil Perusahaan

PT Kano Teknologi Utama adalah perusahaan yang menyediakan produk dan layanan berupa *ERP & Business App Implementation, Big Data and Machine Learning, Specialized Stack and Mobile Development, Cloud Transformation*.

4.1.2 Sejarah Umum

PT Kano Teknologi Utama (Kano Solution) didirikan oleh sekelompok profesional berpengalaman di bidang teknologi informasi. Kano Solution berfokus pada solusi teknologi untuk berbagai industri, termasuk manufaktur, keuangan, dan telekomunikasi. Layanan Kano Solution meliputi konsultansi, pengembangan aplikasi, dan implementasi sistem ERP. Kano Solution berkomitmen untuk membantu kliennya mencapai tujuan bisnis mereka dengan memanfaatkan teknologi terkini.

4.1.3 Logo Perusahaan

Gambar 4. 1 Logo PT Kano Teknologi Utama

4.1.4 Visi dan Misi

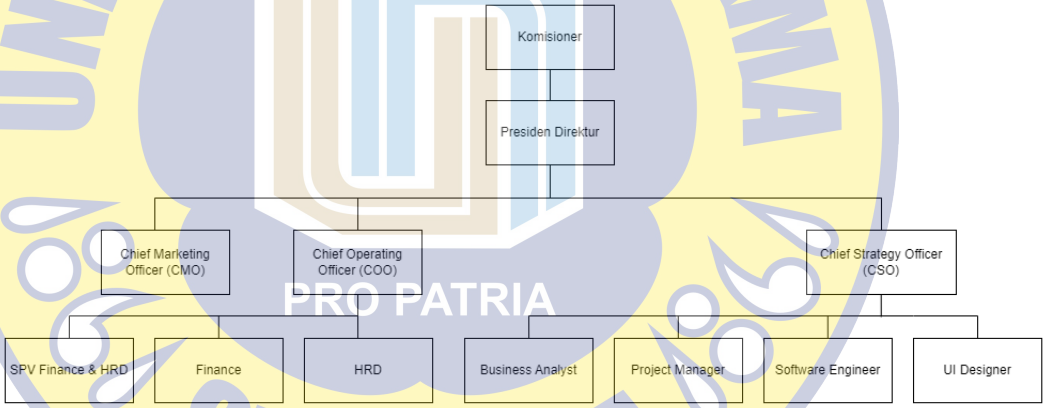
a. Visi

Become leader on Indonesia to deliver ERP, BigData, Business Enablement Software, Machine Learning and Analytic and Cloud Journey for enterprise

b. Misi

To become technology partner to our client by enable solution to deliver business insight and increase enterprise value

4.1.5 Struktur Organisasi



Gambar 4. 2 Struktur Organisasi PT Kano Teknologi Utama

4.1.6 Pembagian Tugas dan Tanggung Jawab

1. Komisioner

a. Bertanggung jawab atas pengawasan umum perusahaan sesuai anggaran dasar.

b. Mengawasi dan mengevaluasi kinerja direksi.

2. Presiden Direktur:

a. Mengidentifikasi dan memanfaatkan peluang bisnis.

b. Menyusun strategi dan program yang sejalan dengan visi dan misi.

3. *Chief Marketing Officer* (CMO):

a. Menetapkan target pemasaran yang tepat

b. Mengoptimalkan strategi pemasaran dengan anggaran yang tersedia

4. *Chief Operating Officer* (COO):

a. Mengawasi fungsi administrasi dan operasional perusahaan.

b. Memantau jalannya fungsi teknis operatif.

5. *Chief Strategy Officer* (CSO):

a. Membuat, mengembangkan, dan mengomunikasikan strategi perusahaan.

b. Mengembangkan visi untuk memastikan perusahaan terus berkembang.

4.1.7 Lokasi Perusahaan

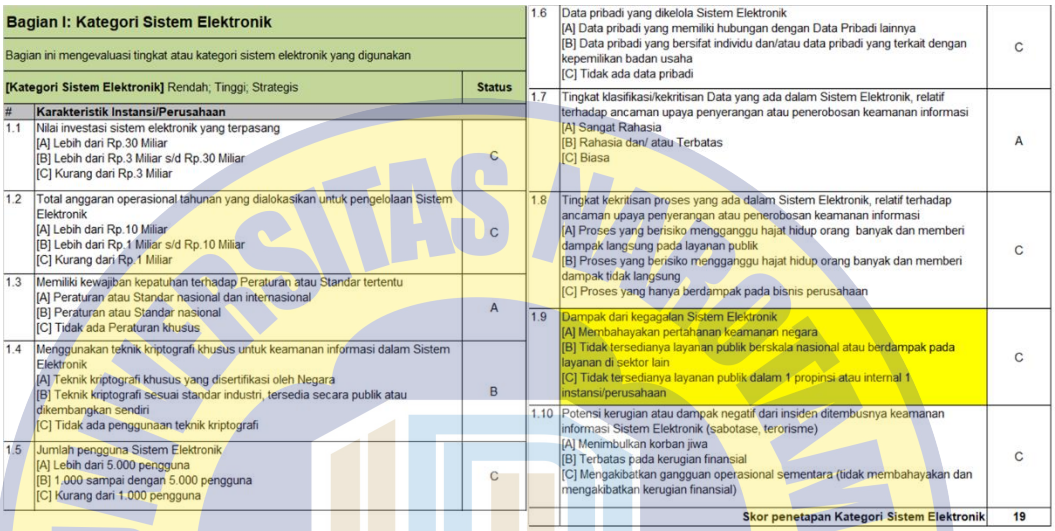
Lokasi PT Kano Teknologi Utama berada di Ruko Klampis Jaya, Jl. Klampis Jaya No.132, Klampis Ngasem, Kec. Sukolilo, Surabaya, Jawa Timur 60116.

4.2 Analisis Indeks Keamanan Informasi (KAMI)

4.2.1 Analisis Kategori Sistem Elektronik

Pada kategori sistem elektronik terdapat 10 pertanyan dengan 3 pilihan jawaban pada setiap pertanyaan. Pertanyaan yang diajukan seputar penggunanan sistem elektronik di perusahaan. Pertanyaan ini bertujuan untuk mengetahui tingkat ketergantungan perusahaan pada penggunaan teknologi informasi. Setiap pilihan

jawaban memiliki bobot skor masing masing. Kemudian skor tersebut akan diakumulasikan dan menghasilkan nilai akhir serta kategori sistem elektronik. Hasil penilaian kategori sistem elektronik ada pada gambar 4.3.



Bagian I: Kategori Sistem Elektronik

Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan

	[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	**Status**
#	**Karakteristik Instansi/Perusahaan**	
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	C
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	A
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	B
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	C
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	C
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	A
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	C
1.9	Dampak dari kegagalan Sistem Elektronik [A] Membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik berskala nasional atau berdampak pada layanan di sektor lain [C] Tidak tersedianya layanan publik dalam 1 propinsi atau internal 1 instansi/perusahaan	C
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	C
	Skor penetapan Kategori Sistem Elektronik	**19**

Gambar 4. 3 Penilaian Kategori Sistem Elektronik

Gambar 4.3 menunjukkan skor kategori sistem elektronik yang mencapai 19, termasuk dalam kategori tinggi. Hal ini menandakan bahwa sistem elektronik perusahaan memiliki pengaruh besar dalam kelancaran proses bisnis. [23].

4.2.2 Penilaian Enam Area Keamanan Informasi

Penilaian enam area informasi Indeks KAMI dilakukan dengan cara mengisi kuisioner yang telah disediakan. Kuisioner diisi sesuai hasil wawancara sebelumnya. Penilaian enam area keamanan informasi meliputi tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, perlindungan data pribadi. Tiap area memiliki jumlah pertanyaan yang berbeda yang dimana setiap pertanyaan memiliki 4 pilihan jawaban yang sama yaitu “Tidak Dilakukan”, “Dalam Perancanaan”, “Dalam Penerapan Atau Diterapkan Sebagian” dan “Diterapkan Secara Menyeluruh”.

Penilaian ini terbagi menjadi tiga tahap. Tahap 1 dan 2 harus diselesaikan dan dinyatakan valid terlebih dahulu sebelum lanjut ke tahap 3.

Penilaian enam area keamanan informasi bertujuan untuk mengetahui kesiapan perusahaan dalam hal tata kelola, pengelolaan risiko, dan kerangka kerja keamanan informasi. Selain itu, penilaian ini juga akan mengukur kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dan kontrol keamanan dalam pengamanan aset informasi dan data pribadi. Hasil penilaian ini akan membantu perusahaan dalam mengidentifikasi area yang perlu diperkuat dan meningkatkan postur keamanan informasi secara keseluruhan. Hasil penilaian yang telah dilakukan disajikan pada Tabel 4.1.

Tabel 4. 1 Tabel Penilaian 6 Area Keamanan Informasi

Area	Tahap 1				Tahap 2				Tahap 3				Total Nilai
	TD	DP	DP /DS	DM	TD	DP	DP /DS	DM	TD	DP	DP /DS	DM	
Tata Kelola Keamanan Informasi	-	-	1	7	-	-	4	4	-	2	2	2	99
Pengelolaan Risiko Keamanan Informasi	-	-	5	5	-	-	1	3	-	-	-	-	47
Kerangka Kerja Pengelolaan Keamanan Informasi	1	1	-	6	-	1	-	10	-	-	-	-	89
Pengelolaan Aset Informasi	1	-	3	23	-	2	-	17	-	-	-	-	181
Teknologi dan Keamanan Informasi	-	-	-	14	-	-	-	15	-	-	-	6	186
Perlindungan Data Pribadi	-	2	-	2	-	1	2	9	-	-	-	-	72

Keterangan :

TD : Tidak Dilakukan

DP : Dalam Perencanaan

DP/DS : Dalam Penerapan Atau Diterapkan Sebagian

DM : Diterapkan Secara Menyeluruh

4.2.3 Penilaian Suplemen

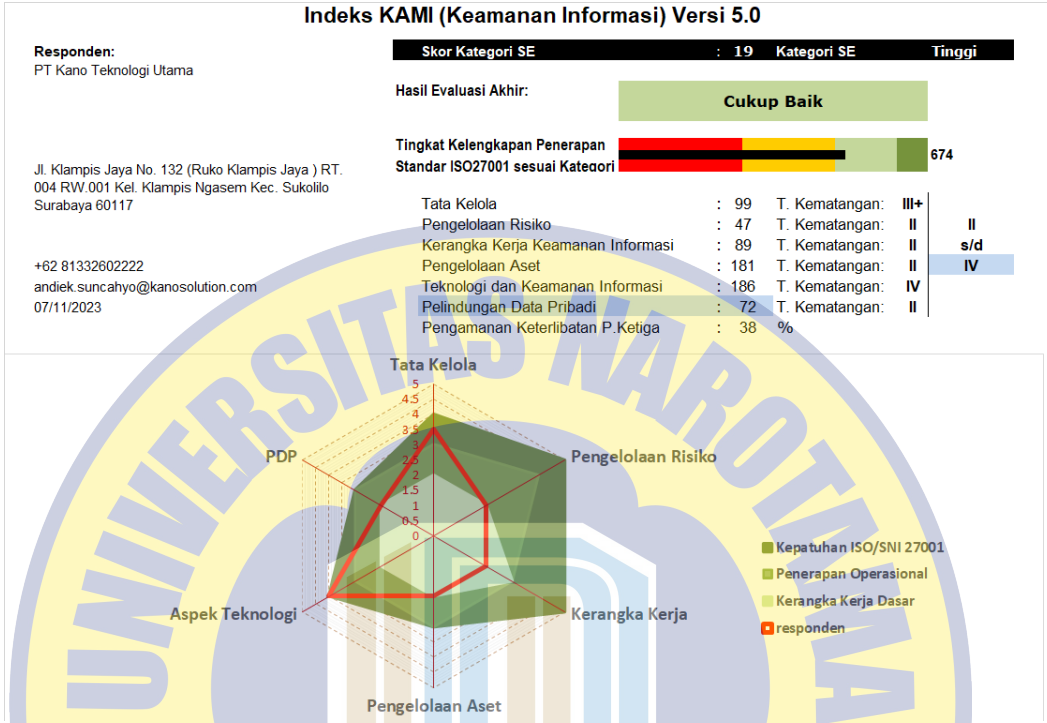
Penilaian kategori suplemen bertujuan untuk menilai kelengkapan, konsistensi dan efektivitas mekanisme keamanan yang digunakan untuk mengantisipasi risiko dari pihak ketiga eksternal yang terlibat dalam operasional layanan instansi/perusahaan. Penilaian suplemen dilakukan sama seperti penilaian enam area keamanan informasi. Namun dalam penilaian suplemen tidak ada tahapan dan nilai yang hasilkan dalam bentuk persentase. Hasil penilaian suplemen disajikan pada Tabel 4.2.

Tabel 4. 2 Penilaian Suplemen

Jawaban	**Jumlah**
Tidak Dilakukan	15
Dalam Perancanaan	2
Dalam Penerapan Atau Diterapkan Sebagian	1
Diterapkan Secara Menyeluruh	9
Total Skor	38%

4.3 Hasil Evaluasi dan Rekomendasi

4.3.1 Hasil Evaluasi Indeks Keamanan Informasi (KAMI)



Gambar 4. 4 Dashboard Hasil Evaluasi Menggunakan Indeks KAMI 5.0

Gambar 4. 4 menampilkan hasil evaluasi menggunakan Indeks Keamanan Informasi (KAMI). Dashboard ini menyajikan informasi lengkap terkait keamanan informasi, meliputi skor kategori sistem informasi dan elektronik, hasil evaluasi akhir kesiapan pengamanan, tingkat kematangan di setiap area, dan tingkat kelengkapan penerapan standar ISO 27001, semua ditampilkan dengan visualisasi Radar Chart yang mudah dipahami.Berdasarkan gambar 4.18 dapat diketahui bahwa skor kategori sistem elektronik adalah 19 dan termasuk dalam kategori tinggi. Sedangkan hasil evaluasi akhir adalah "Cukup Baik" dengan skor akhir 674 dan tingkat kelengkapan penerapan sesuai standar ISO 27001 berada pada tingkat II sampai dengan IV.

4.3.2 Rekomendasi Perbaikan

Rekomendasi perbaikan manajemen keamanan informasi PT. Kano Teknologi Utama didapatkan dari hasil penilaian yang telah dilakukan dengan Indeks KAMI versi 5.0. Penilaian tersebut dilakukan dengan menggunakan instrumen yang mengacu pada standar ISO/IEC 27001:2022. Hasil penilaian menunjukkan bahwa PT. Kano Teknologi Utama telah memenuhi sebagian besar persyaratan ISO/IEC 27001:2022, namun masih terdapat beberapa syarat yang belum terpenuhi.

Rekomendasi perbaikan diberikan pada syarat-syarat yang belum terpenuhi tersebut. Pemberian rekomendasi dilakukan dengan memperhatikan kondisi dan kebutuhan PT. Kano Teknologi Utama. Rekomendasi perbaikan yang telah dipaparkan diharapkan dapat menjadi acuan dalam melakukan evaluasi untuk meningkatkan kualitas manajemen keamanan informasi. PT. Kano Teknologi Utama. Evaluasi perbaikan ini penting dilakukan untuk memastikan bahwa PT. Kano Teknologi Utama dapat memenuhi semua persyaratan ISO/IEC 27001:2022.

Selain itu, rekomendasi perbaikan tersebut juga diharapkan dapat meningkatkan status penerapan pada syarat yang belum terpenuhi. Peningkatan status penerapan ini dapat dilakukan dengan menerapkan kontrol-kontrol keamanan informasi yang sesuai dengan rekomendasi. Kontrol-kontrol keamanan informasi tersebut dapat berupa kontrol teknis, administratif, atau organisasional. Dengan demikian, rekomendasi yang diberikan adalah sebagai berikut.

Tabel 4. 3 Rekomendasi Sesuai ISO/IEC 27001:2022

No	Kondisi yang Kurang	Rekomendasi Sesuai ISO/IEC 27001:2022
1	Perusahaan belum memiliki dokumentasi resmi mengenai pembagian tanggung jawab	A 5.2 *Information Security Roles and Responsibilities* Perusahaan perlu mendefinisikan dan menetapkan peran dan tanggung jawab sehingga semua pihak dapat mengetahui dengan jelas kewajiban yang harus dilakukan.
2	Perusahaan belum memiliki kebijakan transfer data.	A 5.14 *Information Transfer* Perusahaan perlu memiliki kebijakan dalam transfer data yang mencakup pengendalian, pelacakan, kontak dan tanggung jawab, pelabelan, ketersediaan, pedoman dan dampak hukum sehingga tranfer data menjadi aman.
3	Perusahaan belum memiliki kebijakan yang mengatur keamanan informasi dalam lingkup *cloud* komersial.	A 5.23 *Information security for use of cloud services* Perusahaan perlu memiliki prosedur terkait penggunaan layanan *cloud*. Prosedur yang dibuat setidaknya mencakup bagaiamana menetapkan proses untuk akuisisi, penggunaan, pengelolaan dan keluar dari layanan cloud, melakukan penilaian risiko keamanan informasi, melakukan pemantauan dan pengendalian terhadap layanan cloud.
4	Perusahaan belum memiliki prosedur untuk mengatasi insiden keamanan informasi.	A 5.24 *Information Security Incident Management Planning and Preparation* Perusahaan perlu memiliki prosedur untuk mengatasi insiden keamanan informasi dengan begitu dapat meminimalkan kerusakan operasional yang disebabkan oleh insiden keamanan informasi. Prosedur yang dibuat meliputi peran dan tanggung jawab, pedoman manajemen insiden dan pedoman pelaporan.
5	Perusahaan belum memiliki dokumentasi operasional secara resmi	A 5.37 *Documented Operating Procedures* Perusahaan perlu memiliki dokumentasi prosedur operasional terkait keamanan informasi. Contoh prosedur operasional yang perlu didokumentasikan seperti pembuatan cadangan data, penghapusan media, pembaruan perangkat lunak.
6	Perusahaan belum memiliki prosedur pelaporan kejadian keamanan informasi.	A 6.8 *Information Security Event Reporting* Perusahaan perlu memiliki prosedur pelaporan kejadian keamanan informasi sehingga kejadian keamanan informasi dapat dilaporkan secara tepat waktu, konsisten, efektif dan efisien. Prosedur yang dibuat mencakup jenis kegiatan yang dilaporkan, cara melaporkan kejadian, cara menyelidiki kejadian, cara belajar dari kejadian.

Dengan menerapkan rekomendasi di atas, diharapkan skor Indeks KAMI PT. Kano Teknologi Utama dapat meningkat secara signifikan. Hal ini akan meningkatkan tingkat kesiapan pengamanan informasi dan meminimalisir risiko terjadinya insiden keamanan informasi. Berikut adalah tabel perbandingan nilai Indeks KAMI PT. Kano Teknologi Utama saat ini dan nilai yang diharapkan setelah implementasi rekomendasi:

Tabel 4. 4 Perbandingan Skor Saat Ini dan Skor Yang DIharapkan

Area	Skor Saat Ini	Skor Yang Diharapkan
kerangka kerja keamanan informasi	89	92
tata kelola keamanan informasi	99	111
perlindungan data pribadi	72	74
pengelolaan aset informasi	181	192