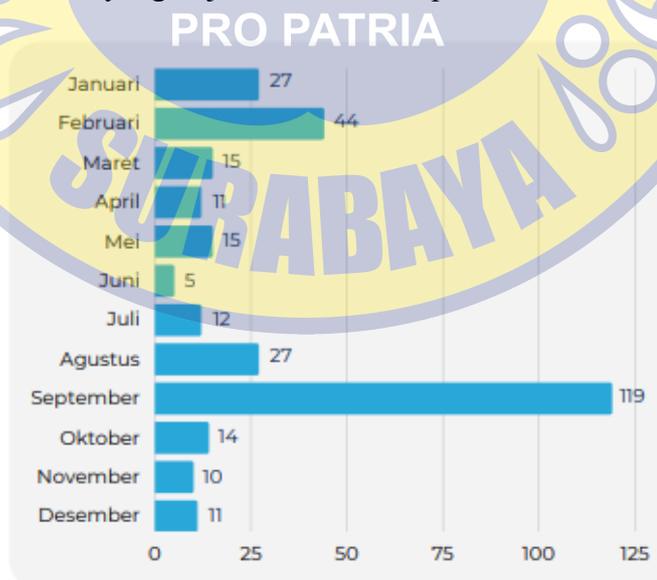


BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan pesat teknologi informasi membuka peluang baru bagi individu, pemerintah, dan sektor swasta untuk menyelesaikan pekerjaan dengan lebih mudah [1]. Perusahaan menggunakan teknologi informasi untuk mengolah data yang kemudian akan diolah menjadi informasi berharga untuk mengambil keputusan [2]. Dengan demikian data merupakan aset penting dalam perusahaan. Data harus dijaga supaya terhindar dari ancaman terhadap keamanan informasi [3]. Salah satu ancaman keamanan informasi yang merugikan adalah kebocoran data. Menurut Lanskap Keamanan Siber Indonesia 2022, sebanyak 311 insiden kebocoran data yang terjadi di Indonesia [4]. Gambar 1.1 dibawah ini menyajikan rekapitulasi data terkait kebocoran data yang terjadi di Indonesia pada Tahun 2022.



Gambar 1. 1 Rekapitulasi Insiden Kebocoran Data di Indonesia Tahun 2022

Kerentanan sistem teknologi informasi disebabkan oleh lemahnya sistem keamanan informasi [4]. Aspek penting dalam menjaga keamanan informasi ada tiga yaitu kerahasiaan, keutuhan, dan ketersediaan [5]. Melakukan evaluasi pada tiga aspek tersebut dapat membantu mengidentifikasi risiko keamanan informasi. Evaluasi yang dilakukan harus sesuai dengan standar nasional ataupun internasional [6]. Indeks KAMI merupakan alat bantu untuk mengukur tingkat keamanan informasi suatu organisasi berdasarkan standar internasional SNI ISO/IEC 27001. [7].

Indeks KAMI dapat membantu mengetahui kelengkapan dan kematangan keamanan informasi perusahaan yang menggunakan teknologi informasi dalam aktivitas sehari-hari. Dengan demikian, organisasi tersebut memiliki gambaran mengenai kondisi keamanan informasi dan dapat melakukan evaluasi sehingga keamanan menjadi lebih baik. PT. Kano Teknologi Utama merupakan salah satu perusahaan yang mengintegrasikan teknologi informasi dalam aktivitas sehari-harinya.

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*. Saat ini PT. Kano Teknologi Utama belum melakukan sertifikasi audit ISO 27001. Penelitian ini memilih Indeks KAMI sebagai alat bantu karena dapat membantu untuk mengevaluasi keamanan dan kematangan teknologi informasi, guna membantu organisasi dalam meningkatkan keamanan dan mencapai kepatuhan terhadap standar ISO 27001.

1.2 Perumusan Masalah

Penelitian ini akan membahas mengenai:

- 1) Bagaimana hasil akhir yang diperoleh oleh PT Kano Teknologi Utama setelah dilakukan evaluasi dengan Indeks KAMI 5.0?
- 2) Bagaimana level kematangan dan kelengkapan keamanan PT. Kano Teknologi Utama?
- 3) Apa saja rekomendasi yang diberikan untuk meningkatkan keamanan informasi pada PT. Kano Teknologi Utama berdasarkan ISO 27001?

1.3 Batasan Masalah

Batasan yang akan diterapkan dalam penelitian meliputi:

- 1) Penelitian dilakukan di PT. Kano Teknologi Utama yang berlokasi di Ruko Klampis Jaya, Jl. Klampis Jaya No.132, Klampis Ngasem, Kec. Sukolilo, Surabaya.
- 2) Penelitian menggunakan data yang diambil melalui wawancara dengan direktur PT. Kano Teknologi Utama.
- 3) Penelitian ini menggunakan Indeks KAMI 5.0.
- 4) Rekomendasi yang diberikan berdasarkan ISO 27001:2022.

1.4 Tujuan penelitian

Berikut adalah tujuan penelitian ini:

- 1) Mengetahui hasil penilaian menggunakan Indeks KAMI pada PT. Kano Teknologi Utama.

- 2) Mengetahui tingkat kematangan dan kesiapan keamanan informasi PT. Kano Teknologi Utama.
- 3) Memberikan rekomendasi untuk meningkatkan keamanan informasi pada PT. Kano Teknologi Utama berdasarkan ISO 27001:2022.

1.5 Manfaat Penelitian

1. Manfaat Teoritis

Secara teoritis, penelitian ini dapat bermanfaat seperti:

- a. Berkontribusi dalam penelitian ilmiah yang berfokus pada penerapan evaluasi keamanan informasi.
- b. Menjadi rujukan bagi penelitian selanjutnya yang berfokus pada evaluasi keamanan informasi.

2. Manfaat Praktis

Secara praktis, penelitian ini dapat bermanfaat seperti:

- a. Bagi penulis, meningkatkan pemahaman dan kemampuan dalam evaluasi keamanan informasi.
- b. Bagi pihak PT Kano Teknologi Utama, mengetahui kondisi keamanan informasi dan menerapkan rekomendasi berdasarkan ISO 27001:2022 untuk meningkatkan ketahanan dan kepercayaan dalam menghadapi berbagai ancaman siber.

BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Penelitian Terdahulu

Peneliti memiliki beberapa referensi dari penelitian sebelumnya yang menggunakan Indeks KAMI, diantaranya adalah sebagai berikut :

- 1) Reynaldo Adi Putra Pratama Gala, dkk (2020) dengan judul “Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI” yang terbit di Jurnal Teknik Informatika vol.15 UNSRAT. Penelitian ini dilakukan di Kabupaten Minahasa Tenggara untuk mengetahui tingkat keamanan informasi pemerintah. Penelitian ini menggunakan Indeks KAMI versi 4.0. Hasil dari penelitian ini menunjukkan bahwa tingkat kematangan informasi pemerintah Kabupaten Minahasa Tenggara masih rendah atau “Tidak Layak” dan berada di area merah dengan total skor 264 [8].
- 2) Silvia Paramita, dkk (2022) dengan judul "Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013" yang terbit di Jurnal Bulletin of Information Technology (BIT) Vol 3, No 4. Penelitian ini dilakukan di SMA Negeri 6 Medan. Penelitian ini menggunakan Indeks KAMI versi 4.0. Hasil dari penelitian ini menunjukkan bahwa tingkat kematangan dan kesiapan teknologi informasi di SMA Negeri 6 Medan cukup baik dengan total skor 340 [9].
- 3) Rendy ismail, dkk (2023) dengan judul "Analisis Tingkat Keamanan Sistem Informasi Madrasah Tsanawiyah Negeri 2 Lampung Utara Menggunakan

Metode Indeks KAMI" yang terbit di Jurnal informasi dan Komputer Vol: 11 No:2. Penelitian ini dilakukan di Madrasah Tsanawiyah Negeri 2 Lampung Utara untuk meninjau kesiapan implementasi keamanan sistem informasi. Hasil penelitian menunjukkan bahwa tingkat kewananan informasi Madrasah Tsanawiyah Negeri 2 Lampung Utara belum memadai [10].

- 4) Tachiyya Nailal, dkk (2023) dengan judul "Pengukuran Tingkat Keamanan Informasi Pada UPT-PSI Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (KAMI) Versi 4.2" yang terbit di Jurnal JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Vol. 8, No. 3. Penelitian ini dilakukan di Unit Pelaksana Teknis-Pusat Sistem Informasi (UPT-PSI) Universitas Sunan Muria Kudus untuk mengetahui tingkat pengamanan yang sudah dicapai. Penelitian ini menggunakan Indeks KAMI versi 4.2. Hasil penelitian menunjukkan bahwa kelengkapan pada UPT-PSI Universitas Muria Kudus cukup baik dengan skor 480 dan tingkat kematangan berada di level II sampai dengan III [11].
- 5) Dicky Insan Khamil, dkk (2022) dengan judul "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)" yang terbit di Jurnal Teknik Informatika dan Sistem Informasi ISSN 2407-4322 Vol. 9, No. 3. Penelitian ini dilakukan Diskominfo Kabupaten Gianyar dengan tujuan evaluasi pengamanan informasi. Penelitian ini menggunakan Indeks KAMI 4.2. Penelitian ini menunjukkan bahwa status tingkat kesiapan Diskominfo

Kabupaten Gianyar “Tidak Layak dengan skor akhir 190 [12].

Tabel 2. 1 Penelitian Terdahulu

| No | Penulis | Judul | Tempat Penelitian | Hasil Penelitian |
|----|---|--|-----------------------------------|--|
| 1 | Reynaldo Adi Putra Pratama Gala, dkk (2020) | Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI | Kabupaten Minahasa Tenggara | Hasil dari penelitian ini menunjukkan bahwa tingkat kematangan informasi pemerintah Kabupaten Minahasa Tenggara masih rendah atau “Tidak Layak” dan berada di area merah dengan total skor 264 |
| 2 | Silvia Paramita, dkk (2022) | Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013 | SMA Negeri 6 Medan | Hasil dari penelitian ini menunjukkan bahwa tingkat kematangan dan kesiapan teknologi informasi di SMA Negeri 6 Medan cukup baik dengan total skor 340 |

Tabel 2. 2 Lanjutan

| No | Penulis | Judul | Tempat Penelitian | Hasil Penelitian |
|----|--------------------------------|---|--|--|
| 3 | Rendy ismail, dkk (2023) | Analisis Tingkat Keamanan Sistem Informasi Madrasah Tsanawiyah Negeri 2 Lampung Utara Menggunakan Metode Indeks KAMI | Madrasah Tsanawiyah Negeri 2 Lampung Utara | Hasil penelitian menunjukkan bahwa tingkat kewanaman informasi Madrasah Tsanawiyah Negeri 2 Lampung Utara belum memadai |
| 4 | Tachiyya Nailal, dkk (2023) | Pengukuran Tingkat Keamanan Informasi Pada UPT-PSI Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (KAMI) Versi 4.2 | Unit Pelaksana Teknis-Pusat Sistem Informasi (UPT-PSI) Universitas Sunan Muria Kudus | Hasil penelitian menunjukkan bahwa kelengkapan pada UPT-PSI Universitas Muria Kudus cukup baik dengan skor 480 dan tingkat kematangan berada di level II sampai dengan III |
| 5 | Dicky Insan Khamil, dkk (2022) | Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar) | Diskominfo Kabupaten Gianyar | Penelitian ini menunjukkan bahwa status tingkat kesiapan Diskominfo Kabupaten Gianyar “Tidak Layak dengan skor akhir 190 |

2.2 Teori – Teori Dasar

2.2.1 Keamanan Informasi

Keamanan informasi adalah usaha untuk melindungi aset informasi dari segala ancaman yang merugikan perusahaan [13]. Keamanan informasi memiliki tiga tujuan yang ingin dicapai yaitu aspek kerahasiaan, integritas dan ketersediaan informasi [14]. Masing masing aspek dapat dijelaskan sebagai berikut [15]:

1. Kerahasiaan : informasi hanya dapat diakses oleh pihak yang berwenang.
2. Integritas : informasi hanya dapat diubah oleh pihak berwenang dan menjaga akurasi data.
3. Ketersediaan : informasi dapat diakses ketika dibutuhkan.

Keamanan informasi juga bertujuan untuk mencegah kerusakan, kehilangan dan kebocoran informasi ke pihak lain [14]. Selain itu keamanan informasi bertujuan untuk menjaga keberlangsungan bisnis dan meminimalisir kerugian [16]. Oleh karena itu, perusahaan harus menjaga dan meningkatkan keamanan informasi untuk melindungi perusahaan dari ancaman yang merugikan.

2.2.2 Sistem Keamanan Manajemen Informasi

Manajemen keamanan informasi merupakan alat, kebijakan dan prosedur untuk melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi oleh perusahaan. Kegiatan utama manajemen keamanan informasi adalah asesmen dan evaluasi risiko untuk melindungi aset perusahaan [17]. Sebuah organisasi perlu mengimplementasikan sistem untuk mencegah ancaman keamanan informasi salah satunya adalah sistem manajemen keamanan informasi. Sistem manajemen

keamanan informasi merupakan sistem manajemen dengan pendekatan risiko bisnis untuk membentuk, menerapkan, memantau, mengoperasikan, meninjau, menjaga, dan mengembangkan keamanan informasi [18].

2.2.3 The International Organization for Standardization (ISO)

The International Organization for Standardization atau ISO adalah organisasi internasional yang beranggotakan 167 badan standar nasional dunia. ISO mengumpulkan anggotanya untuk berbagi pengetahuan kemudian dikembangkan menjadi sebuah standar internasional untuk pasar dunia. Tujuan berdirinya ISO adalah membuat standar internasional agar perusahaan dapat bersaing dengan pasar global [19]. ISO 27001 merupakan salah satu standar yang dibuat oleh ISO yang sudah diakui dan diadopsi oleh seluruh dunia termasuk Indonesia [20]. ISO 27001 berdasar pada manajemen risiko keamanan informasi dan dirancang untuk melindungi aset informasi dari ancaman yang merugikan dan membantu meningkatkan keamanan perusahaan [21]. Dengan demikian ISO 27001 dapat dikatakan sebagai dasar yang harus diperhatikan untuk membuat sistem Manajemen keamanan informasi suatu perusahaan.

2.2.4 Indeks KAMI 5.0

Dalam proses evaluasi ISO 27001 alat bantu yang dapat digunakan adalah Indeks KAMI. Indeks KAMI adalah alat bantu untuk menganalisis tingkat kematangan dan kesiapan keamanan informasi perusahaan yang dirancang sesuai standar ISO 27001 versi 2013. Indeks KAMI dirancang agar dapat digunakan oleh seluruh perusahaan atau instansi untuk mendukung terlaksananya proses teknologi informasi [22]. Dengan adanya Indeks KAMI perusahaan dapat memiliki gambaran

mengenai kesiapan keamanan informasi sehingga perusahaan dapat meningkatkan keamanan informasi sesuai kebijakan yang telah ditentukan.

Indeks KAMI pertama kali diterbitkan pada tahun 2009 untuk versi 1 kemudian mengalami perbaikan dan revisi hingga versi 5.0 pada Maret 2023 dengan adanya perubahan dari versi sebelumnya yaitu versi 4.2. Perubahan yang terjadi antara lain [7] :

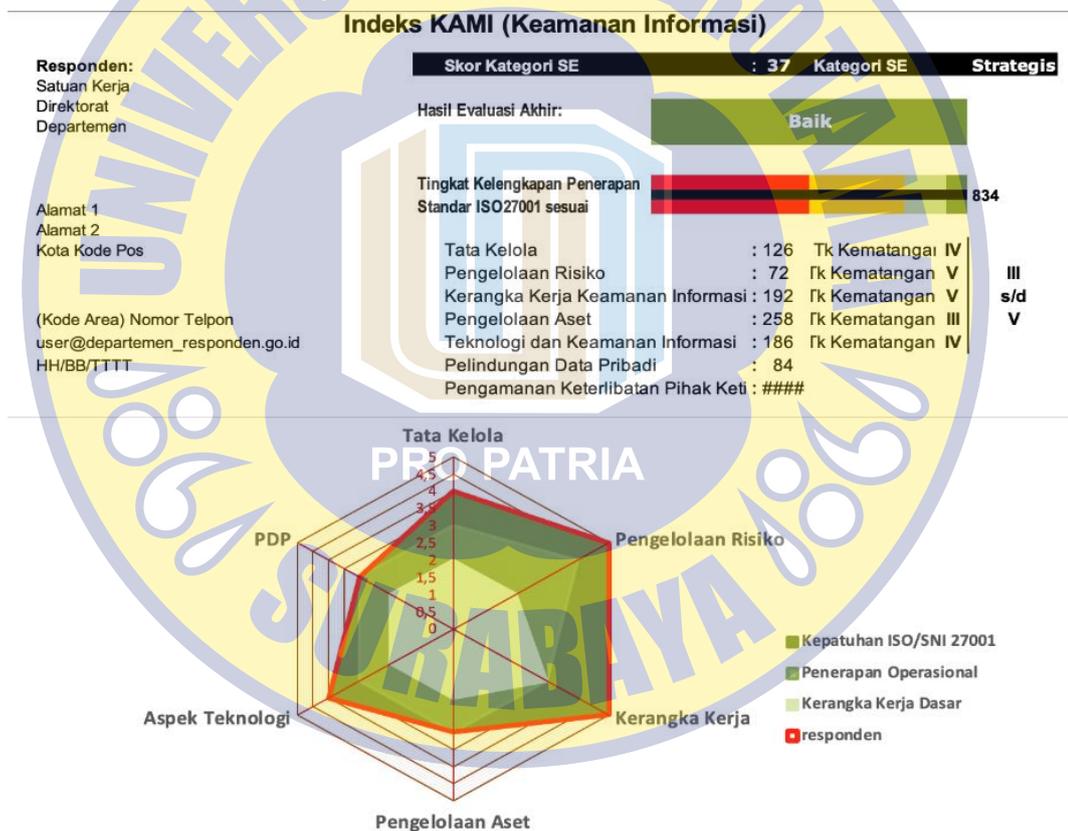
- 1) Penambahan area evaluasi sesuai ISO 27001:2022, pada Kerangka Kerja, Pengelolaan Aset dan Teknologi.
- 2) Pemindahan area evaluasi Suplemen - Penggunaan Infra Layanan Awan ke area evaluasi utama (Pengelolaan Aset).
- 3) Memisahkan area evaluasi Suplemen - Pelindungan Data Pribadi menjadi area sendiri/terpisah.
- 4) Penyesuaian rumus perhitungan skor dan dashboard.
- 5) Penambahan opsi kondisi ""Tidak Berlaku/Relevan"" pada sejumlah pertanyaan apabila area evaluasi memang tidak relevan dengan ruang lingkup
- 6) Revisi kriteria pada Kategori SE agar lebih konsisten.

Evaluasi yang dilakukan oleh Indeks KAMI meliputi [7] :

- 1) Kategori sistem elektronik
- 2) Tata kelola keamanan informasi
- 3) Pengelolaan risiko keamanan informasi
- 4) Kerangka kerja keamanan informasi
- 5) Pengelolaan aset informasi

- 6) Teknologi dan keamanan informasi
- 7) Perlindungan data pribadi
- 8) Pengamanan keterlibatan pihak ketiga

Hasil evaluasi kemudian akan direpresentasikan dalam Radar Chart dengan enam area utama. Nilai Indeks KAMI dengan standar ISO/IEC 27001:2013 juga akan terlihat di Radar Chart. Hasil evaluasi menggunakan Indeks KAMI 5.0 ditunjukkan pada gambar 2.1.



Gambar 2. 1 Dashboard Indeks KAMI 5.0

Sumber : BSSN

Nilai akhir dari hasil evaluasi memiliki korelasi dengan skor kategori sistem elektronik. Korelasi dapat dijelaskan pada gambar 2.2.

| KATEGORI SISTEM ELEKTRONIK | | | | |
|-----------------------------------|----|-------------------|-----|--------------------------------|
| Rendah | | Skor Akhir | | Status Kesiapan |
| 10 | 15 | 0 | 247 | Tidak Layak |
| | | 248 | 443 | Pemenuhan Kerangka Kerja Dasar |
| | | 444 | 760 | Cukup Baik |
| | | 761 | 916 | Baik |
| Tinggi | | Skor Akhir | | Status Kesiapan |
| 16 | 34 | 0 | 387 | Tidak Layak |
| | | 388 | 646 | Pemenuhan Kerangka Kerja Dasar |
| | | 647 | 828 | Cukup Baik |
| | | 829 | 916 | Baik |
| Strategis | | Skor Akhir | | Status Kesiapan |
| 35 | 50 | 0 | 472 | Tidak Layak |
| | | 473 | 760 | Pemenuhan Kerangka Kerja Dasar |
| | | 761 | 864 | Cukup Baik |
| | | 865 | 916 | Baik |

Gambar 2. 2 Kategori Sistem Elektronik

(Sumber : BSSN)

Kemudian dilakukan pengukuran tingkat kematangan yang mengacu pada kerangka kerja COBIT atau CMMI. Tingkat kematangan ini dapat digunakan untuk melaporkan pemetaan dan pemringkatan kesiapan informasi di lembaga. Tingkat kematangan didefinisikan sebagai berikut :

- 1) Tingkat I - Kondisi Awal
- 2) Tingkat II - Penerapan Kerangka Kerja Dasar
- 3) Tingkat III - Terdefinisi dan Konsisten
- 4) Tingkat IV - Terkelola dan Terukur
- 5) Tingkat V – Optimal

Rentang tingkat kematangan dapat dilihat pada gambar 2.3.



Gambar 2. 3 Rentang Tingkat Kematangan

