Evaluasi Keamanan Informasi pada Perusahaan Skincare DNY Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013

Ozilla Junior Pratomo[1], Mohammad Ulil Azmi Al Huraibi[2], Mujib Ridwan[3]

[1*,2,3] Sistem Innformasi; Universitas Islam Negeri Sunan Ampel; Surabaya; e-mail: ozijunior691@gmail.com, aazhmy1912@gmail.com, mujibrw@uinsa.ac.id

* Korespondensi: e-mail: ozijunior691@gmail.com

Diterima: 19 September 2025 ; Review: 28 November 2025; Disetujui: 04 Desember 2025

Cara sitasi: Pratomo OJ, Al Huraibi MUA, Ridwan M. 2025. Evaluasi Keamanan Informasi pada Perusahaan Skincare DNY Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013. Information System for Educators and Professionals. Vol 10(2): 117-126.

Abstrak: Peningkatan pemanfaatan teknologi digital dalam industri skincare menyebabkan perusahaan harus memastikan sistem keamanan informasi yang lebih kuat untuk melindungi data konsumen. Penelitian ini bertujuan mengevaluasi tingkat kematangan keamanan informasi pada Perusahaan DNY Skincare menggunakan Indeks Keamanan Informasi (KAMI) yang mengacu pada standar ISO/IEC 27001:2013. Evaluasi dilakukan dengan menganalisis tata kelola keamanan informasi, pengelolaan aset, manajemen risiko, serta efektivitas kontrol yang telah diterapkan perusahaan. Hasil penelitian menunjukkan bahwa aspek pelindungan data pribadi, pengelolaan aset informasi, dan teknologi keamanan telah diterapkan dengan cukup baik. Namun, beberapa komponen seperti validitas data, dokumentasi risiko, serta konsistensi implementasi kontrol keamanan masih memerlukan peningkatan. Temuan ini mengindikasikan bahwa perusahaan telah memiliki fondasi yang memadai untuk membangun sistem keamanan informasi yang berkelanjutan, tetapi masih membutuhkan penguatan pada area strategis tertentu. Penelitian ini menegaskan pentingnya peningkatan berkelanjutan dalam penerapan sistem manajemen keamanan informasi guna mendukung perlindungan optimal terhadap data konsumen dan memastikan kepatuhan terhadap standar keamanan informasi internasional.

Kata kunci: keamanan informasi, Indeks Keamanan Informasi, ISO/IEC 27001:2013, manajemen risiko, tata kelola sistem informasi

Abstract: *The increasing use of digital technology in the skincare industry requires companies to ensure a stronger information security system to protect consumer data. This study aims to evaluate the level of information security maturity at DNY Skincare using the Information Security Index (ISSI) based on the ISO/IEC 27001:2013 standard. The evaluation was conducted by analyzing information security governance, asset management, risk management, and the effectiveness of the company's implemented controls. The results indicate that aspects of personal data protection, information asset management, and security technology have been implemented quite well. However, several components such as data validity, risk documentation, and consistency of security control implementation still require improvement. These findings indicate that the company has an adequate foundation for building a sustainable information security system, but still needs strengthening in certain strategic areas. This study emphasizes the importance of continuous improvement in the implementation of an information security management system to support optimal protection of consumer data and ensure compliance with international information security standards.*

Keywords*: Information Security, KAMI Indeks, ISO/IEC 27001, Risk Management, Information System Governance*

1. Pendahuluan

Industri skincare berkembang pesat dalam satu dekade terakhir, didorong oleh meningkatnya kesadaran masyarakat mengenai pentingnya kesehatan dan perawatan kulit. Produk *skincare* kini menjadi bagian penting dari gaya hidup modern, bukan hanya sekadar kebutuhan tambahan. Pertumbuhan ini semakin kuat karena permintaan konsumen yang mengutamakan keamanan bahan, efektivitas produk, serta hasil yang dapat dibuktikan secara dermatologis [1].

Eksposur masyarakat terhadap tren kecantikan global, edukasi mengenai bahan aktif, dan rekomendasi rutinitas perawatan kulit turut dipengaruhi oleh media sosial serta peran influencer kecantikan. Informasi mengenai manfaat skincare kini tersebar luas di berbagai platform digital, membuat konsumen lebih sadar dan selektif dalam memilih produk [2]. Hal ini menyebabkan persaingan antar perusahaan semakin ketat dan menuntut adanya inovasi berkelanjutan.

Perkembangan teknologi memiliki dampak signifikan terhadap seluruh lini bisnis *skincare*. Penelitian dan pengembangan (R&D) kini memanfaatkan pendekatan berbasis data, analisis bioteknologi, serta pengujian produk yang lebih presisi dan ilmiah. Teknologi digital juga membantu perusahaan memahami kebutuhan konsumen melalui analisis pola penggunaan, preferensi bahan aktif, dan tren pasar [3].

Transformasi digital juga terlihat pada strategi pemasaran dan distribusi produk skincare. Perusahaan semakin mengandalkan platform *e-commerce*, media sosial, dan kampanye digital untuk menjangkau konsumen secara lebih luas dan efektif. Digitalisasi ini memungkinkan perusahaan mengumpulkan data konsumen dalam jumlah besar, termasuk perilaku belanja dan kebutuhan perawatan kulit.

Kecerdasan buatan (AI) dan *machine learning* bahkan telah menjadi teknologi kunci dalam memberikan rekomendasi produk personal, analisis kondisi kulit melalui foto, hingga layanan konsultasi virtual. Inovasi tersebut meningkatkan kenyamanan dan personalisasi layanan bagi konsumen sehingga berpotensi meningkatkan loyalitas pelanggan terhadap merek tertentu [4].

Namun, integrasi teknologi digital dalam bisnis *skincare* menimbulkan risiko keamanan informasi yang semakin kompleks. Pengumpulan data pribadi seperti identitas, riwayat konsultasi kulit, serta kebiasaan pembelian membutuhkan sistem perlindungan yang memadai. Tanpa pengamanan yang baik, data dapat berisiko mengalami kebocoran, pencurian, atau penyalahgunaan yang merugikan konsumen dan perusahaan [5].

Ancaman serangan siber, malware, dan potensi peretasan membuat perusahaan *skincare* harus memperkuat sistem keamanan informasi secara menyeluruh. Dampak dari insiden keamanan dapat mencakup kerugian finansial, hilangnya kepercayaan konsumen, menurunnya reputasi brand, hingga risiko hukum. Oleh karena itu, strategi manajemen keamanan informasi perlu direncanakan dengan matang dan mengikuti standar internasional [6].

Dalam konteks ini, standar *ISO/IEC 27001:2013* menjadi acuan global dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini memberikan kerangka kerja sistematis untuk mengidentifikasi, mengukur, dan memitigasi risiko keamanan informasi dalam organisasi. Penerapan *ISO/IEC 27001* terbukti meningkatkan efektivitas pengendalian keamanan dan kepatuhan perusahaan terhadap regulasi [7].

Selain ISO, penggunaan *Indeks Keamanan Informasi (KAMI)* menjadi metode evaluasi yang praktis untuk menilai tingkat kesiapan keamanan informasi di berbagai organisasi. Indeks KAMI membantu mengukur kelengkapan prosedur keamanan, implementasi kontrol teknis, serta kematangan kebijakan keamanan informasi secara menyeluruh. Alat ini telah banyak digunakan dalam analisis keamanan di berbagai institusi dan terbukti mendukung peningkatan keamanan yang terstruktur [8].

Berdasarkan kebutuhan perlindungan data yang semakin tinggi serta urgensi penerapan manajemen keamanan informasi dalam perusahaan skincare, penelitian ini dilakukan dengan judul "Evaluasi Keamanan Informasi pada Perusahaan *Skincare* DNY Berdasarkan *Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013".* Penelitian ini bertujuan mengevaluasi tingkat kesiapan keamanan informasi di perusahaan *skincare* DNY, mengidentifikasi potensi kelemahan, serta memberikan rekomendasi strategis untuk meningkatkan perlindungan data konsumen dan memperkuat tata kelola keamanan informasi [9].

Vol. 10, No. 2, Desember 2025, 117 - 126

2. Metode Penelitian

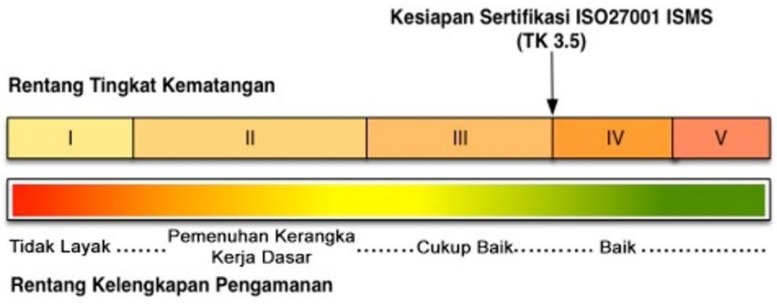
Penelitian ini menggunakan pendekatan deskriptif dengan tujuan utama untuk mengevaluasi tingkat kematangan Perusahaan DNY *Skincare* dalam mengelola sistem keamanan informasi yang diterapkan pada lingkungan operasionalnya. Pendekatan deskriptif dipilih karena mampu memberikan gambaran menyeluruh mengenai kondisi aktual organisasi, termasuk kebijakan, prosedur, serta mekanisme kontrol keamanan yang telah dijalankan. Melalui pendekatan ini, penelitian berfokus pada pengamatan, pengumpulan informasi, dan analisis data secara sistematis guna mengetahui sejauh mana perusahaan telah memenuhi standar keamanan informasi yang relevan, khususnya yang mengacu pada *ISO/IEC 27001:2013* dan *Indeks Keamanan Informasi (KAMI)* [10].

a. Wawancara

Wawancara dalam penelitian ini dilakukan dengan Kepala Bagian Teknologi Informasi (IT) di Perusahaan DNY *Skincare*. Narasumber tersebut merupakan individu yang memiliki peran strategis dalam pengelolaan serta implementasi tata kelola sistem keamanan informasi di lingkungan perusahaan. Sebagai pihak yang bertanggung jawab langsung terhadap pengembangan infrastruktur teknologi, pengawasan sistem informasi, serta penerapan kebijakan keamanan data, Kepala Bagian IT memiliki pemahaman mendalam mengenai kondisi aktual keamanan informasi perusahaan. Melalui wawancara ini, peneliti memperoleh informasi yang lebih komprehensif terkait prosedur keamanan yang diterapkan, tantangan yang dihadapi dalam menjaga keamanan data pelanggan, serta tingkat kesiapan perusahaan dalam memenuhi standar keamanan informasi seperti *ISO/IEC 27001:2013*. Wawancara tersebut juga menjadi sumber utama dalam menggali detail implementasi serta efektivitas pengendalian keamanan yang telah dijalankan di DNY *Skincare*.

b. Indeks *KAMI*

Pengisian indeks *KAMI* digunakan untuk mengumpulkan data sebagai bahan evaluasi. Data yang diperoleh akan diolah dan dianalisis untuk menilai kesiapan perusahaan dalam tata kelola keamanan informasi berdasarkan kerangka kerja indeks *KAMI*.



Sumber : *Indeks KAMI versi 5.0 ISO/IEC 27001:2003*

Gambar 1.Rentang tingkat kematangan dan Rentang kelengkapan pengamanan

Tingkat kesiapan dari sebuah organisasi dalam menerapkan sertifikasi *ISO 27001:2013* berada di disaran nilai III dan IV dengan T.K 3.5.

Evaluasi, menurut Arifin (2009), adalah proses yang dilakukan secara sistematis dan terus-menerus untuk menilai kualitas sesuatu berdasarkan kriteria tertentu guna mendukung pengambilan keputusan. Sementara itu, Arikunto (2008) menyatakan bahwa hasil evaluasi dapat mengarahkan kebijakan dalam empat opsi: menghentikan, merevisi, melanjutkan, atau menyebarluaskan program. Dalam praktiknya, pengelolaan keamanan informasi mencakup berbagai aspek penting yang saling terhubung, sehingga perlindungan sistem informasi memerlukan tata kelola yang baik dan mekanisme tanggap darurat. Hal ini bertujuan untuk

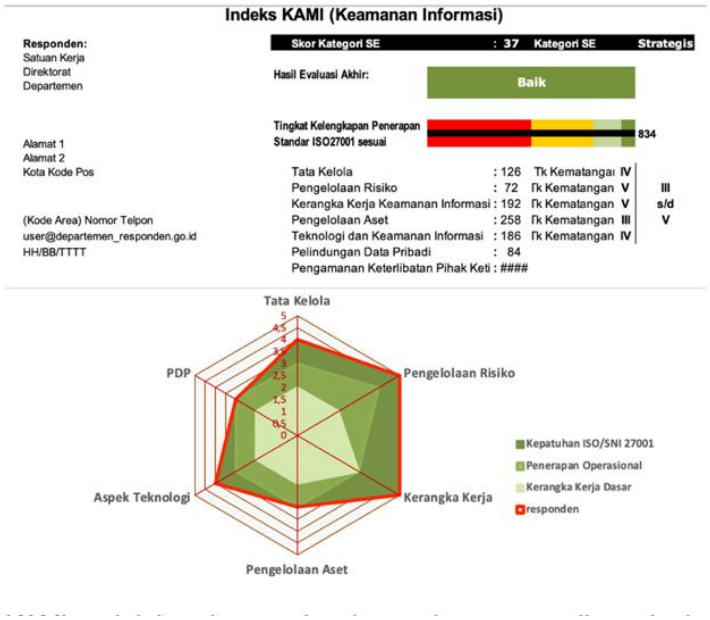
meminimalkan dampak dari gangguan atau kerusakan data yang dapat menghambat operasional suatu organisasi, dengan memastikan adanya rencana cadangan untuk menangani situasi tersebut.

Pengelolaan teknologi informasi menjadi sangat penting karena mencakup komponen utama organisasi seperti kepemimpinan, struktur, dan proses organisasi. Komponen-komponen ini harus saling terintegrasi dengan baik agar teknologi dapat mendukung kebutuhan organisasi secara optimal. Selain itu, tanggung jawab dalam pengelolaan informasi harus dijalankan dengan jelas, termasuk aturan spesifik dan pembagian tugas yang tepat. Menempatkan individu yang sesuai dengan keahlian mereka di posisi yang tepat dapat mengurangi risiko yang mungkin timbul akibat kurangnya pemahaman terhadap tugas tertentu.

Penelitian ini menggunakan indeks *KAMI* sebagai alat evaluasi untuk menilai tingkat kesiapan pengelolaan keamanan informasi dalam organisasi. Indeks *KAMI* memberikan gambaran terkait kesiapan kerangka kerja suatu organisasi dalam pengamanan informasi. Evaluasi ini mencakup berbagai area yang relevan dengan penerapan keamanan informasi dan sesuai dengan standar *ISO/IEC 27001:2013.*

Indeks *KAMI* dirancang agar dapat diterapkan oleh berbagai jenis organisasi untuk menghasilkan penilaian prioritas. Dengan adanya hasil perbandingan ini, organisasi dapat menyesuaikan diri dengan standar *ISO 27001:2013* sekaligus menentukan prioritas perbaikan. Penggunaan indeks KAMI secara berkala juga memberikan wawasan terkini mengenai kesiapan organisasi dalam menghadapi tantangan keamanan informasi, sekaligus meningkatkan kesadaran akan pentingnya pengelolaan keamanan informasi melalui tata kelola sistem informasi yang baik [11].

Evaluasi menggunakan indeks *KAMI* versi 5.0 saat ini dapat diterapkan untuk menilai berbagai jenis institusi di semua tingkat. Proses evaluasi dilakukan dengan menjawab sejumlah kategori pertanyaan yang terbagi ke dalam beberapa area, yaitu: Bagian I (Peran Teknologi Informasi dan Komunikasi), Bagian II (Tata Kelola Informasi yang Aman), Bagian III (Manajemen Risiko Keamanan Informasi), Bagian IV (Kerangka Kerja untuk Keamanan Informasi), Bagian V (Pengelolaan Aset Informasi), dan Bagian VI (Keamanan dan Teknologi Informasi).



Sumber : Indeks KAMI versi 5.0 *ISO/IEC 27001:2013*

Gambar 2. Contoh Dashboard Evaluasi Indeks KAMI

Dashboard yang ditampilkan menyajikan hasil evaluasi terhadap sebuah instansi, lembaga, atau stakeholder. Melalui dashboard ini, dapat terlihat gambaran tingkat kesiapan organisasi dalam mengimplementasikan tata kelola keamanan informasi berdasarkan setiap kategori yang ada, seperti tata kelola, aspek teknologi, pengelolaan aset, kerangka kerja, dan manajemen risiko. Semua informasi dalam diagram dashboard ini diselaraskan dengan standar *ISO/IEC 27001:2013*.

	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

Sumber : Indeks KAMI versi 5.0 *ISO/IEC 27001:2013*

Gambar 3. Skor Tingkat Kematangan

Setiap kategori dalam evaluasi ini terdiri dari sejumlah pertanyaan yang dikelompokkan ke dalam tiga bagian utama. Seluruh kategori telah disesuaikan dengan standar *ISO/IEC 27001:2013*, dengan rincian sebagai berikut:
Kategori 1: Berfokus pada kerangka dasar tata kelola untuk perlindungan keamanan informasi.
Kategori 2: Membahas efisiensi dan konsistensi dalam penerapan keamanan informasi.
Kategori 3: Bertujuan untuk meningkatkan performa sistem keamanan informasi.

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

Sumber : Indeks KAMI versi 5.0 ISO/IEC 27001:2003

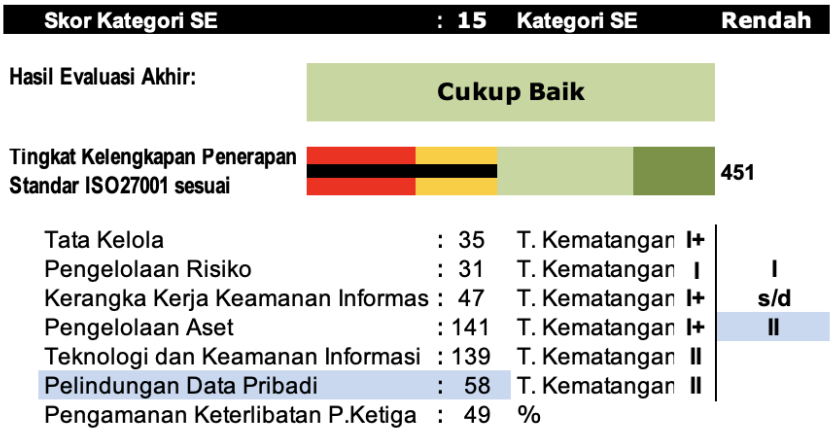
Gambar 4. Peran TIK dalam Instansi

3. Hasil dan Pembahasan

Hasil evaluasi penerapan tata kelola sistem informasi di Perusahaan DNY *Skincare*, dengan skor total 451, menunjukkan bahwa perusahaan telah mencapai tingkat kematangan yang cukup baik menurut standar *ISO/IEC 27001*. Penggunaan Indeks KAMI dalam evaluasi ini memberikan gambaran mendalam mengenai berbagai aspek tata kelola, seperti pengelolaan risiko, kerangka kerja keamanan, aset informasi, teknologi, dan peran TIK. Meskipun sebagian besar komponen telah diterapkan dengan baik, ada beberapa area yang masih memerlukan perhatian khusus agar tingkat kematangan bisa ditingkatkan ke level optimal. Misalnya, mungkin diperlukan penguatan dalam struktur kebijakan keamanan formal, mekanisme mitigasi risiko yang lebih detail, dan peningkatan kontrol akses pada aset-aset kritikal .

Hasil ini penting karena menunjukkan bahwa DNY *Skincare* sudah berada di jalur yang benar dalam mengimplementasikan sistem manajemen keamanan informasi (ISMS), tetapi masih

memiliki potensi perbaikan yang strategis. Dengan pemetaan area yang masih lemah, manajemen perusahaan dapat merancang roadmap perbaikan keamanan informasi yang lebih fokus dan berkelanjutan, termasuk persiapan menuju sertifikasi *ISO/IEC 27001* secara penuh .

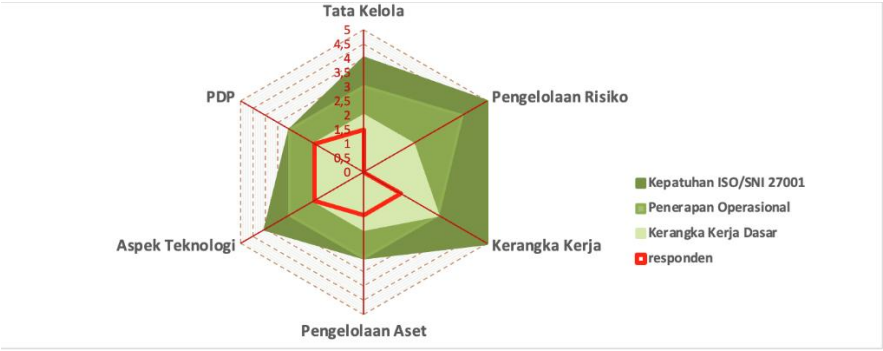


Sumber : Hasil indeks KAMI versi 5.0 ISO/IEC 27001:2013

Gambar 5. Hasil dari evaluasi akhir indeks KAMI versi 5.0 (diagram batang)

Pada aspek tata kelola, pengelolaan risiko, dan kerangka kerja keamanan informasi, tingkat kematangan berada pada kategori awal hingga menengah. Ini menunjukkan bahwa struktur tata kelola sudah mulai terbentuk, tetapi masih memerlukan peningkatan untuk mencapai tingkat kematangan yang lebih tinggi. Sementara itu, pengelolaan aset dan teknologi keamanan informasi menunjukkan hasil yang lebih baik, dengan tingkat kematangan yang mendekati standar yang diharapkan.

Komponen pelindungan data pribadi menjadi salah satu area yang menonjol dengan skor tertinggi, menandakan penerapan yang cukup matang dalam menjaga privasi dan keamanan informasi. Namun, pada aspek pengamanan keterlibatan pihak ketiga, meskipun telah menunjukkan hasil yang cukup baik, masih ada ruang untuk perbaikan, terutama dalam memastikan keamanan kerja sama dengan pihak eksternal.



Sumber : Hasil indeks KAMI versi 5.0 ISO/IEC 27001:2003

Gambar 6. Hasil dari evaluasi akhir indeks KAMI versi 5.0 (*spider chart*)

Spider chart mendukung analisis ini dengan menampilkan distribusi skor dari setiap aspek, menunjukkan kekuatan di beberapa area seperti teknologi dan pelindungan data, sekaligus mengidentifikasi kelemahan yang perlu diperbaiki, seperti pada kerangka kerja dasar dan pengelolaan risiko. Secara keseluruhan, hasil evaluasi ini memberikan gambaran komprehensif tentang kondisi tata kelola sistem informasi di Perusahaan DNY dan menjadi dasar perbaikan di masa mendatang.

Berdasarkan hasil evaluasi indeks *KAMI*, Perusahaan DNY telah menunjukkan komitmen terhadap tata kelola sistem informasi. Hal ini tercermin pada hampir seluruh kategori dalam indeks *KAMI*, sebagaimana dijelaskan dalam uraian berikut.

A. Bagian I : Kategori Sistem Elektronik

Evaluasi ini menunjukkan hasil yang cukup baik, karena perusahaan telah memenuhi sejumlah peraturan nasional yang berlaku terkait pengelolaan sistem elektronik dan perlindungan data pribadi. Hal ini menjadi indikator bahwa DNY *Skincare* memiliki kesadaran awal yang kuat dalam menerapkan tata kelola keamanan informasi. Selain itu, jumlah pengguna sistem elektronik yang berada pada kisaran 1.000 hingga 5.000 menunjukkan bahwa perusahaan sudah mengelola volume data yang cukup besar, sehingga penerapan sistem keamanan menjadi aspek krusial. Salah satu faktor penting yang turut berkontribusi terhadap tingginya skor pada bagian ini adalah adanya keterhubungan data pribadi yang dikelola oleh perusahaan dengan data pribadi lainnya, sehingga mencerminkan tingkat integrasi sistem yang cukup tinggi. Keterhubungan ini memberikan nilai tambah dalam evaluasi karena menunjukkan adanya proses bisnis yang terdigitalisasi dengan baik, meskipun di sisi lain hal tersebut juga menuntut penerapan kontrol keamanan yang lebih ketat untuk mencegah risiko kebocoran atau penyalahgunaan data.

Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa organisasi dengan jumlah pengguna sistem yang besar dan memiliki interkoneksi data pribadi cenderung memperoleh skor lebih tinggi pada evaluasi Indeks *KAMI*, sekaligus dituntut untuk menerapkan mekanisme perlindungan data yang lebih matang agar dapat memenuhi standar *ISO/IEC 27001* secara menyeluruh.

B. Bagian II : Tata Kelola Keamanan Informasi

Bagian ini berfokus pada aspek tata kelola keamanan informasi di instansi, khususnya terkait dengan pembagian peran serta tanggung jawab dalam pengelolaan data. Dalam konteks manajemen keamanan informasi, definisi fungsi dan tanggung jawab setiap unit kerja menjadi elemen yang sangat penting karena menentukan sejauh mana proses pengelolaan data dapat berjalan secara konsisten, aman, dan terukur. Pembagian tugas yang jelas juga membantu memastikan bahwa setiap aktivitas pengolahan data dilakukan oleh pihak yang memiliki kewenangan dan kompetensi yang tepat. Hal ini berkaitan langsung dengan prinsip akuntabilitas data, di mana organisasi harus mampu mempertanggungjawabkan keakuratan, keutuhan, dan keamanan informasi yang dikelolanya. Pengaturan struktur tersebut menjadi dasar bagi terciptanya tata kelola yang efektif, terutama dalam lingkungan operasional yang mengharuskan kepatuhan terhadap berbagai regulasi nasional mengenai perlindungan data pribadi.

Dari hasil evaluasi yang dilakukan, instansi memperoleh skor total 35, yang menunjukkan bahwa pengelolaan keamanan informasi pada bagian ini termasuk dalam kategori baik. Banyak indikator memperoleh nilai maksimal karena adanya penerapan standar pengelolaan data yang telah ditetapkan oleh Kementerian Pendidikan dan instansi terkait. Hal ini menunjukkan bahwa organisasi sudah berada pada jalur yang benar dalam menerapkan proses tata kelola data yang terstruktur dan terdokumentasi. Salah satu indikator yang menjadi contoh nyata adalah indikator 2.20, yang menilai kewajiban instansi dalam melaporkan status pengelolaan data kepada pimpinan secara berkala. Perolehan nilai maksimal pada indikator ini menunjukkan bahwa mekanisme pelaporan dan komunikasi internal telah berjalan dengan baik, yang pada akhirnya meningkatkan transparansi dan efektivitas dalam proses pengambilan keputusan terkait keamanan informasi.

C. Bagian III : Pengelolaan Risiko Keamanan Informasi

Hasil evaluasi pengelolaan risiko keamanan informasi menunjukkan bahwa Perusahaan DNY masih berada pada tahap awal dalam proses perencanaan dan implementasi manajemen risiko. Meskipun telah terdapat sejumlah langkah dasar yang mulai diterapkan, total skor pada tahap pertama hanya mencapai 30, yang mengindikasikan bahwa struktur manajemen risiko belum sepenuhnya matang atau terstandarisasi. Beberapa pertanyaan dalam instrumen *KAMI* juga dinyatakan tidak valid akibat keterbatasan data dan ketidaksesuaian antara kondisi aktual

dengan ketentuan pengisian. Hal ini menandakan adanya tantangan dalam proses dokumentasi, pencatatan, serta kurangnya bukti pendukung yang diperlukan untuk melengkapi proses evaluasi secara optimal.

Selain itu, penilaian tingkat kematangan yang dilakukan membantu memperjelas posisi perusahaan dalam aspek manajemen risiko, baik dari sisi kekuatan maupun kelemahan. Temuan ini mengindikasikan bahwa perusahaan perlu memperkuat proses identifikasi risiko, penilaian tingkat risiko, serta pengembangan mekanisme mitigasi yang lebih terstruktur dan terdokumentasi. Dalam kerangka *ISO/IEC 27001*, manajemen risiko merupakan komponen kritikal dalam menetapkan prioritas pengamanan aset informasi, sehingga DNY perlu meningkatkan konsistensi dan frekuensi evaluasi risiko secara berkala. Secara keseluruhan, diperlukan upaya berkelanjutan untuk memperbaiki prosedur, meningkatkan validitas data, serta memastikan bahwa seluruh kegiatan pengamanan informasi sesuai dengan standar internasional agar tingkat kesiapan keamanan informasi perusahaan dapat terus berkembang.

D. Bagian IV : Kerangka Kerja Pengelolaan Keamanan Informasi

Hasil evaluasi pengelolaan risiko keamanan informasi menunjukkan bahwa Perusahaan DNY memiliki total 12 pertanyaan pada tahap pertama, dengan capaian skor 36 dari maksimum 60. Nilai ini menggambarkan bahwa perusahaan telah memulai langkah-langkah penerapan manajemen risiko keamanan informasi, meskipun belum sepenuhnya optimal. Mayoritas indikator berada pada status “Diterapkan” atau “Dalam Perencanaan”, yang menandakan bahwa DNY Skincare telah memiliki kesadaran awal terhadap pentingnya pengelolaan risiko dalam menjaga keamanan data dan sistem informasi perusahaan. Namun demikian, masih terdapat beberapa jawaban yang dinyatakan tidak valid, yang mengindikasikan bahwa proses pengumpulan data internal belum sepenuhnya konsisten dan memerlukan evaluasi lebih lanjut. Ketidaksesuaian ini dapat berdampak pada representasi akurat mengenai kondisi sebenarnya di lapangan.

Lebih lanjut, penilaian tingkat kematangan menunjukkan adanya perbedaan signifikan antara skor minimal dan pencapaian aktual pada tiap tahap. Pada tahap II, DNY Skincare memperoleh skor 39, sedangkan pada tahap III total nilai meningkat hingga 108. Perbedaan skor ini menunjukkan adanya upaya penguatan dalam pengelolaan risiko, namun belum mencapai tingkat stabil dan terukur sesuai standar *ISO/IEC 27001:2013*. Secara keseluruhan, DNY *Skincare* masih berada dalam fase peningkatan berkelanjutan dan memerlukan perbaikan pada aspek validitas data, konsistensi implementasi kontrol risiko, serta dokumentasi yang lebih kuat. Perbaikan pada area tersebut akan membantu perusahaan mencapai tingkat kesiapan keamanan informasi yang lebih tinggi serta memastikan keberlanjutan perlindungan data di tengah meningkatnya ancaman keamanan digital.

E. Bagian V : Pengelolaan Aset Informasi

Hasil analisis data menunjukkan bahwa pada tahap 1 terdapat 27 pertanyaan dengan total skor penerapan mencapai 130. Meskipun skor maksimum yang dapat dicapai pada tahap ini adalah 81, hasil tersebut menggambarkan bahwa Perusahaan DNY telah mampu menerapkan sejumlah kebijakan keamanan informasi secara cukup konsisten. Tingginya skor pada beberapa indikator menunjukkan bahwa perusahaan memiliki fondasi yang baik dalam pengelolaan aset informasi dan penerapan kontrol dasar yang berhubungan dengan keamanan sistem. Namun demikian, adanya beberapa jawaban yang dinyatakan tidak valid mengindikasikan bahwa proses pengumpulan, pencatatan, maupun verifikasi data internal masih perlu ditingkatkan. Kesalahan atau ketidaksesuaian data seperti ini dapat memengaruhi objektivitas hasil evaluasi serta mengurangi ketepatan skor yang seharusnya mencerminkan kondisi aktual perusahaan.

Pada tahap penilaian tingkat kematangan, Perusahaan DNY memperoleh skor 75 pada tingkat kematangan II dan 111 pada tingkat kematangan III. Capaian tersebut menunjukkan bahwa perusahaan telah bergerak menuju tingkat kematangan yang lebih tinggi dalam pengelolaan keamanan informasi, terutama dari sisi dokumentasi, penerapan kontrol, serta prosedur manajemen. Meski begitu, kondisi ini juga menandakan bahwa perusahaan masih berada dalam fase transisi menuju tata kelola keamanan informasi yang sepenuhnya terstruktur dan berkelanjutan. Oleh karena itu, fokus utama ke depan adalah meningkatkan validitas data serta memperkuat integrasi prosedur keamanan di seluruh unit operasional. Dengan langkah tersebut, efektivitas pengelolaan risiko dan kualitas penerapan keamanan informasi di

Perusahaan DNY akan dapat meningkat secara signifikan dan selaras dengan standar *ISO/IEC 27001.*

F. Bagian VI : Teknologi dan Kemanan Informasi

Hasil analisis data menunjukkan bahwa pada tahap I terdapat 42 pertanyaan yang diajukan untuk menilai efektivitas pengelolaan keamanan informasi di Perusahaan DNY. Dari keseluruhan pertanyaan tersebut, perusahaan berhasil memperoleh total skor 130, yang secara umum mengindikasikan bahwa sebagian besar komponen kebijakan keamanan informasi telah diterapkan dengan baik. Meskipun demikian, skor maksimum yang mungkin diraih pada tahap ini adalah 81, sehingga terdapat ketidaksesuaian antara jumlah skor dengan rentang nilai dalam instrumen *KAMI*. Hal ini disebabkan oleh adanya beberapa pertanyaan yang dinilai tidak valid, yang menunjukkan bahwa proses pengisian atau dokumentasi pendukung belum sepenuhnya akurat. Ketidakvalidan data tersebut dapat memengaruhi objektivitas penilaian dan menunjukkan perlunya evaluasi ulang terhadap prosedur dokumentasi serta mekanisme verifikasi jawaban.

Pada tahap kematangan berikutnya, yaitu tahap II dan tahap III, perusahaan juga menunjukkan perkembangan yang cukup signifikan. Skor tahap II tercatat sebesar 75, sementara tahap III mencapai 111, yang mencerminkan bahwa sebagian besar aktivitas penguatan keamanan informasi sedang berlangsung dan mulai memperlihatkan hasil yang positif. Kendati demikian, temuan-temuan ini juga menegaskan bahwa masih terdapat ruang untuk peningkatan, terutama dalam hal validitas data dan konsistensi penerapan kontrol keamanan yang lebih ketat. Secara keseluruhan, meskipun perusahaan telah berada pada jalur yang benar dalam membangun tata kelola keamanan informasi yang efektif, fokus pada perbaikan kualitas data, peningkatan dokumentasi, serta validasi jawaban akan menjadi langkah penting untuk meningkatkan akurasi evaluasi dan mencapai tingkat kematangan yang lebih optimal di masa mendatang.

4. Kesimpulan

Penerapan sistem keamanan informasi di Perusahaan DNY *Skincare* menggunakan indeks *KAMI* sesuai dengan standar *ISO/IEC 27001* menunjukkan hasil yang menjanjikan. Hasil evaluasi menunjukkan bahwa perusahaan telah berhasil menerapkan kebijakan keamanan informasi dengan baik, meskipun terdapat beberapa area yang masih memerlukan perbaikan, terutama dalam hal validitas data dan pengelolaan risiko.

Evaluasi mengindikasikan bahwa tata kelola sistem informasi dan pengelolaan aset telah memperoleh skor yang memuaskan, dengan aspek pelindungan data pribadi menunjukkan penerapan yang cukup matang. Namun, pada aspek pengelolaan risiko dan kerangka kerja keamanan, perusahaan masih berada dalam tahap pengembangan, yang mencerminkan perlunya peningkatan berkelanjutan.

Indeks *KAMI* memberikan gambaran yang jelas mengenai kesiapan perusahaan dalam mengelola keamanan informasi, membantu dalam mengidentifikasi kekuatan serta kelemahan yang ada. Meskipun Perusahaan DNY telah menunjukkan kemajuan yang signifikan, masih ada kebutuhan mendesak untuk meningkatkan akurasi data dan memperbaiki langkah-langkah keamanan. Hal ini penting untuk memastikan perlindungan optimal terhadap informasi konsumen dan mendukung kepatuhan terhadap standar internasional di masa mendatang.

Referensi

[1] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, “The ISO / IEC 27001 Information Security Management Standard : How to Extract Value from Data in the IT Sector,” 2023.
[2] M. S. Khatami, N. M. Asnadi, and R. Anisyah, “ISO 27001 as Information Security Solution in Society 5 . 0 Era : Systematic Literature Review,” vol. 9, no. 1, pp. 484–492, 2025.
[3] A. Ferdinand, K. Naristi, R. Abdillah, S. D. Walujo, and L. Dica, “Pengukuran Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Metode FMEA dan Framework ISO 27001 : 2013 pada PT . ABC,” vol. 9, no. 1, pp. 23–33, 2024, doi: 10.33633/joins.v9i1.9059.
[4] A. L. Maryanto *et al.*, “EVALUATION OF INFORMATION SECURITY MANAGEMENT IN

TECHNOLOGY-BASED BEGINNING COMPANY USING THE KAMI INDEX," vol. 11, no. 1, pp. 1–12, 2022.

[5] M. Noor and H. Siregar, "Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO / IEC 27001," vol. 1, no. 2, pp. 58–64, 2025.

[6] M. Metode, F. Dan, and I. S. O. Pada, "MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI," vol. 2, no. 2, pp. 48–58, 2017.

[7] S. Resta *et al.*, "Cyber Security Risk Management Practices: Insights From an ISO 27001 Certified Organization," vol. 3, no. 2, 2024, doi: 10.26740/jdbim.v3i2.

[8] Y. C. Pradipta, Y. Rahardja, M. N. N. Sitokdana, U. Kristen, and S. Wacana, "TEKNOLOGI INFORMASI DAN KOMUNIKASI PENERBANGAN DAN ANTARIKSA (PUSTIKPAN) MENGGUNAKAN SNI ISO / IEC 27001 : 2013," pp. 352–358, 2013.

[9] S. Lvvq *et al.*, "Keywords : Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Malang adalah Perangkat untuk mendukung proses bisnis yang ada di dalam organisasi . Beberapa hasil yang didapatkan terjadi di Kominfo Kabupaten Malang .," vol. 3.

[10] J. S. Informasi, A. Amaliyah, P. T. Informatika, U. I. Nusantara, and S. P. Elektronik, "Evaluasi Mandiri Pada Sistem Penyelenggaraan Elektronik Berdasarkan Indeks Keamana Informasi (KAMI) Dan ISO 27001 (Studi Kasus : Sistem Litera Uninus)," vol. 05, pp. 87–97, 2023.

[11] A. S. Adung, P. T. Informatika, and S. T. T. P. Adi, "Evaluasi Indeks Keamanan Informasi (KAMI) Pada Pengamanan Penyelenggaraan Sistem Elektronik Berdasarkan ISO 27001 (Studi Kasus : STT Pratama Adi)," vol. 05, 2023.