CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 1, Mei 2024,, hlm. 42-49

Evaluasi Tingkat Kesiapan Keamanan Informasi Pada SMK XYZ Menggunakan Indeks KAMI Versi 4.2

Himawan Imtikhan Azmi[1], Muhammad Tulus Akbar[2], Bella Tasya Kumala Dewi[3], Bambang Sugiantoro[4]

[1,2,3,4]Program Studi Magister Informatika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga, Yogyakarta
Email: 22206051003@student.uin-suka.ac.id

Abstrak

Keamanan informasi penting untuk diperhatikan agar kerahasiaan informasi, data, manusia dan alat pendukung terlindungi. Namun, bahaya ancaman dalam bidang TI mengintai penyelenggara sistem elektronik (PSE), kejahatan yang timbul tidak hanya menyerang organisasi besar, melainkan menyerang berbagai tingkatan, ukuran, maupun tingkat kepentingan organisasi penyelenggara layanan TI. Oleh karena itu pentingnya melakukan evaluasi ke penyedia layanan informasi untuk memaksimalkan sumberdaya dalam menghadapi ancaman. Tujuan penelitian ini untuk melakukan evaluasi penyelenggaraan layanan TI menggunakan Indeks KAMI pada SMK XYZ. Proses evaluasi dilakukan dengan pendekatan kuantitatif. Data dikumpulkan dari hasil wawancara dan observasi dari PSE. Data yang terkumpul kemudian di analisis menggunakan aplikasi Indeks KAMI 4.2. Hasilnya, SMK XYZ termasuk kategori Rendah dengan skor SE 14, dengan status kesiapan Tidak Layak dengan skor Tingkat Penerapan Standar ISO27001 sesuai Kategori SE yaitu 314. Skor tiap area yang dievaluasi yaitu Tata Kelola memperoleh skor 72 dengan tingkat kematangan valid Tingkat II, Pengelolaan Risiko memperoleh skor 15 dengan tingkat kematangan valid Tingkat I, Kerangka Kerja Keamanan Informasi memperoleh skor 91 dengan tingkat kematangan valid Tingkat II, Pengelolaan Aset memperoleh skor 78 dengan tingkat kematangan valid Tingkat I+, Teknologi dan Keamanan Informasi memperoleh skor 58 dengan tingkat kematangan valid Tingkat II, dan bagian terakhir adalah Suplemen sebagai bagian tambahan pengukuran dengan tiga aspek di dalamnya yaitu aspek Pengamanan Keterlibatan Pihak Ketiga memperoleh nilai 33%, aspek Pengamanan Layanan Infrastruktur Awan memperoleh nilai 33%, dan aspek Perlindungan Data Pribadi memperoleh nilai 67%. Hasil evaluasi kesiapan (kelengkapan dan kematangan) yang telah dilakukan menjadi perhatian untuk meningkatkan keamanan informasi pada area dilakukan.

Kata kunci: Indeks KAMI, SMKI, Keamanan Informasi, ISO/IEC27001:2013.

Evaluation of Information Security Readiness Level at SMK XYZ Using the KAMI Index Version 4.2

Abstract

Ensuring information security is imperative to safeguard the confidentiality of data, individuals, and supporting tools. However, persistent threats in the realm of Information Technology (IT) pose a constant risk to electronic system providers. These threats target organizations of diverse sizes, levels, and interests within the IT service domain. Consequently, evaluating information service providers becomes crucial for optimizing resources in countering potential threats. This study focuses on assessing IT service delivery using the KAMI Index at SMK XYZ, employing a quantitative approach. Data is gathered through interviews and observations within the electronic system provider context. The collected data is then analyzed using the OUR Index 4.2 application. The evaluation reveals that SMK XYZ falls into the Low category, scoring 14 in the SE index, indicating an Unfit readiness status with an ISO27001 Standard Implementation Level score of 314, aligning with the SE Category. Further analysis of specific areas shows varying maturity levels. Governance scores 72 at Level II, Risk Management scores 15 at Level I, Information Security Framework scores 91 at Level II, Asset Management scores 78 at Level I +, and Technology and Information Security scores 58 at Level II. The Supplement section, addressing additional measurement aspects, records scores of 33% for Securing Third Party Involvement, 33% for Securing Cloud Infrastructure Services, and 67% for Personal Data Protection. These findings underscore the need for enhanced information security measures within the evaluated context.

***Keywords**: KAMI Index, SMKI, Information Security, ISO/IEC27001:2013.*

1. PENDAHULUAN

Topik mengenai cyber security selalu hangat untuk dibahas, topik keamanan informasi selalu menarik karena berkaitan dengan sensitivitas data yang berada pada cloud computing (Khan et al., 2022). Keamanan informasi adalah bentuk perlindungan informasi dan elemen pentingnya, termasuk sistem dan perangkat keras yang

menggunakan, menyimpan dan mengirimkan informasi (Whitman & Mattord, 2011).

Isu tentang keamanan cyber bukan menjadi tren dalam bidang IT melainkan hangat untuk dibahas dalam resiko bisnis, mestinya harus ditangani dengan hati-hati oleh pengatur regulasi, pasalnya kejahatan ini menyerang ke pebisnis kelas kecil karena memiliki keamanan yang rentan untuk diretas (Marican et al., 2023). Tercatat di Indonesia Cyber Security Report yang diterbitkan oleh ID-SIRTII merilis total serangan anomali pada tahun 2022 sebanyak 976.429.996 juta serangan, dilaporkan bahwa serangan paling banyak terjadi pada bulan januari yakni 272.962.734 anomali. Jumlah ini mengalami penurunan yang signifikan hingga 40% dari tahun sebelumnya, ini karena telah terpasang sensor di ISP dan penurunan jumlah Indicator of Compromise (IoC) yang terdeteksi. Serangan berasal dari MyloBot Botnet yang menargetkan untuk mengambil alih perangkat dan menjalankan operasi sistem (OS) (Ramadhani et al., 2020).

Indonesia melalui Badan Standarisasi Nasional (BSN) menetapkan ISO/IEC27001 sebagai Standar Nasional Indonesia (SNI) untuk mengatur regulasi keamanan informasi pada pemerintahan, perusahaan, komersil, organisasi non-profit dan usaha mikro dan multi Nasional (R.Y Rahman, 2023). Melalui Kementerian Komunikasi dan Informatika ditetapkan peraturan No. 4 Tahun 2016 tentang tools untuk merekayasa keamanan informasi agar dapat membenahi dan menerapkan pengamanan yang harus ditaati oleh Penyelenggara Sistem Elektronik (PSE), keamanan informasi yang harus di jaga ialah keamanan dalam kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara atau pertahanan dan keamanan negara (Khamil, 2022). Upaya yang dapat dilakukan agar terhindar dari ancaman kejahatan internet dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI) khususnya bagi penyedia layanan informasi publik yang berkategori tinggi dan strategis (Hambali & Musa, 2020). Selain itu penerapan SMKI bertujuan untuk memaksimalkan sumberdaya yang dimiliki dan menjadi sarana navigasi dalam pengendalian ancaman (Clarissa & Wang, 2023), dan juga dapat terhindar dan kerugian yang masif (Marican et al., 2023).

Indeks Keamanan Informasi (KAMI) merupakan sarana yang ditujukan untuk meninjau dan mengevaluasi tingkat kesiapan (kelengkapan dan kematangan penerapan keamanan informasi berdasarkan karakteristik SNI ISO/IEC27001 (BSSN, n.d.). Aktivitas evaluasi indeks KAMI dirancang agar dapat diterapkan oleh organisasi PSE baik pemerintah atau non-pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TI. Indeks KAMI diciptakan untuk mengukur tingkat kematangan manajemen keamanan layanan TI (Dewantara & Sugiantoro, 2021).

Evaluasi tingkat keamanan dilakukan dengan menggunakan Indeks KAMI versi 4.2 dengan melihat tingkat kematangan dan kesiapan dengan menerapkan standar ISO/IEC 27001:2013. Dalam perkembangannya, evaluasi pengelolaan keamanan informasi bagi penyelenggara keamanan didasarkan pada Panduan Penerapan Tata Kelola Keamanan Informasi Tahun 2011 dengan alat evaluasi berupa penggunaan Indeks Keamanan Informasi (KAMI) (Rahmah et al., 2019).

Tujuan dari penelitian ini untuk melakukan evaluasi penyelenggaraan layanan TI menggunakan Indeks KAMI pada SMK XYZ agar mengetahui gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi yang ada di SMK XYZ kemudian dapat menjadi perhatian bagi penyelenggara TI yang ada agar memperbaiki dan meningkatkan keamanan informasi pada area-area yang telah dievaluasi sesuai dengan standar ISO/IEC 27001:2013.

2. TINJAUAN PUSTAKA

Indeks KAMI telah banyak digunakan oleh beberapa peneliti dalam melakukan evaluasi terkait keamanan informasi. Hal ini akan digunakan sebagai tolak ukur peneliti dalam penlitian ini. Beberapa literatur yang membahas hal serupa diantaranya adalah penelitian yang dilakukan oleh (Khamil, 2022) dalam melakukan evaluasi tingkat kesiapan keamanan informasi menggunakan indeks KAMI 4.2 dan ISO/IEC 27001:2013 diperoleh hasil bahwa status tingkat kesiapan dinyatakan tidak layak berdasarkan standar yang diterapkan dengan tingkat kematangan tertinggi berada pada tingkat II+ dan terendah pada tingkat I. Hasil tersebut diperoleh berdasarkan korelasi skor akhir yang didapat pada kategori sistem elektronik yang tergolong tinggi sebesar 34 dan kategori keamanan Informasi sebesar 190.

Penelitian yang dilakukan oleh (Paramita et al., 2022) dalam melakukan analisis manajemen risiko keamanan data sistem informasi berdasarkan indeks KAMI 4.0 diperoleh hasil skor sebesar 340 dengan predikat Cukup Baik pada tingkat kematangan yang diterapkan berdasarkan 6 kriteria penilaian. 6 kriteria penilaian tersebut meliputi: kategori sistem elektronik dengan hasil rendah, kategori tata Kelola keamanan informasi dengan hasil kurang atau perlu dilakukan perbaikan, kategori pengelolaan risiko keamanan informasi dengan hasil cukup baik, kategori kerangka kerja pengelolaan keamanan informasi dengan kategori belum atau kurang memadai, kategori pengelolaan asset informasi dengan hasil cukup memadai, serta kategori teknologi dan keamanan informasi dengan hasil perlu dilakukan perbaikan.

Sedangkan pada penelitian yang dilakukan oleh (Sugiarto & Suryanto, 2022) menggunakan index

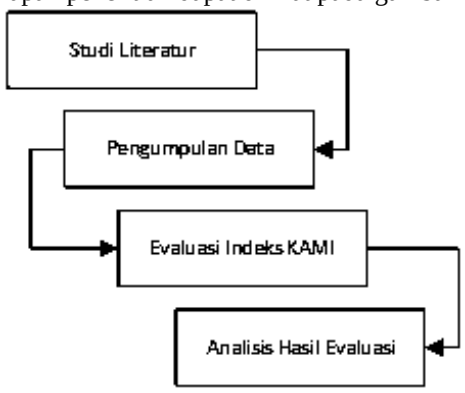
KAMI diperoleh hasil yang menyatakan bahwa keamanan pada sistem informasi memiliki kategori tidak layak dengan skor 164. Dari 5 kategori penilaian diperoleh tingkat kesiapan I+ pada kategori tata Kelola dan pengelolaan aset, dan tingkat kesiapan I pada kategori manajemen risiko, kerangka manajemen, dan teknologi keamanan informasi.

Penelitian yang dilakukan oleh (Kornelia & Irawan, 2021) dalam melakukan analisis keamanan informasi menggunakan tools indeks KAMI ISO 4.1 diperoleh hasil bahwa sistem yang diteliti memiliki teingkat kematangan III dengan status cukup baik dalam melaksanakan sertifikasi ISO/IEC27001:2013. Hasil tersebut diperoleh karena sebagian kelengkapan berdasarkan indeks KAMI belum dilengkapi oleh sistem sehingga memiliki status dalam perencanaan.

Hasil yang diperoleh dari penelitian yang dilakukan oleh (Khusna & Sugiantoro, 2023) dalam melakukan pengukuran tingkat keamanan informasi berdasrakan indeks keamanan informasi (KAMI) versi 4.2 yakni bahwa tingkat kesiapan keamanan informasi sistem tergolong dalam kategori tinggi berdasarkan skor kategori elektronik yang diperoleh sebesar 29. Sedangkan pada tingkat kelengkapan yang diterapkan berdasarkan standar ISO/IEC 27001 diperoleh hasil akhir cukup baik dengan nilai 480 yang dapat diartikan bahwa sistem telah memenuhi standar minimal bersasarkan ISO/IEC 27001.

3. METODOLOGI

Penelitian ini dilaksanakan berdasarkan tahapan penelitian yang telah dirancang. Tahapan-tahapan penelitian dapat dilihat pada gambar 1.



Gambar 1. Tahapan Penelitian

Gambar 1 merupakan tahapan-tahapan penelitian yang diawali dengan studi literatur sampai dengan analisis hasil evaluasi.

3.1. Studi Literatur

Studi literatur dilakukan untuk menentukan metode yang tepat terkait penanganan permasalah yang ada di dalam penelitian. Studi literatur dilakukan melalui aktivitas studi terhadap berbagai macam sumber referensi seperti jurnal ilmiah, buku, dan artikel lainnya.

3.2. Pengumpulan Data

Pengumpulan data dilakukan untuk mendapatkan data yang berhubungan dengan penelitian. Pengumpulan data dilakukan melalui teknik wawancara dan observasi terhadap SMK XYZ sebagai objek penelitian.

3.3. Evaluasi Indeks KAMI

Evaluasi indeks KAMI dilakukan dengan menggunakan aplikasi indeks KAMI versi 4.2 yang disediakan oleh Badan Siber dan Sandi Negara (BSSN). Aplikasi indeks KAMI 4.2 terdiri dari sejumlah pertanyaan di beberapa area yaitu:

1. Kategori Sistem Elektronik yang digunakan
2. Tata Kelola Keamanan Informasi
3. Pengelolaan Risiko Keamanan Informasi
4. Kerangka Kerja Keamanan Informasi
5. Pengelolaan Aset Informasi
6. Teknologi dan Keamanan Informasi

Suplemen (Tambahan pengukuran untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan (Cloud Service) dan Perlindungan Data Pribadi).

Pertanyaan yang ada pada Indeks KAMI 4.2 dikelompokkan untuk dua kepentingan. Pengelompokan pertama berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Area dalam pertanyaan ini diberi label 1 sampai 3. Pertanyaan dengan label 1 terkait dengan bentuk kerangka kerja dasar keamanan informasi. Pertanyaan dengan label 2 terkait dengan efektifitas dan konsistensi penerapannya. Pertanyaan dengan label 3 terkait dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi dimana tingkat ini sesuai dengan kesiapan minimum sertifikasi standar ISO/IEC 27001:2013. Skor kategori pengamanan berdasarkan status pengamanan dapat dilihat pada gambar 2.

	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. Skor Status Pengamanan untuk Kategori Pengamanan

Gambar 2 merupakan skor kategori pengamanan yang diukur dari tiap status pengamanan yang diterapkan. Status pengamanan dikelompokkan menjadi empat macam yaitu: Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan atau Diterapkan Sebagian, dan Diterapkan secara Menyeluruh.

Pengelompokan kedua berdasarkan tingkat kematangan penerapan pengamanan yang berpedoman pada tingkat kematangan yang ada dalam kerangka kerja COBIT (Control Objectives

for Information and Related Technology) atau CMMI (Capability Maturity Model Integration). Tingkat kematangan tersebut dikategorikan 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

Tingkat kematangan yang telah disebutkan sebelumnya juga ditambahkan beberapa tingkatan lagi untuk memberikan uraian yang lebih detail yaitu tingkatan antara I+, II+, III+, dan IV+. Kondisi awal untuk semua responden adalah pada Tingkat I . Ambang batas minimum tingkat kematangan yang diharapkan agar sesuai dengan standar ISO/IEC 27001:2013 adalah pada Tingkat III+.

3.4. Analisis Hasil Evaluasi

Analisis hasil evaluasi adalah tahapan terakhir dari penelitian ini. Aktivitas tersebut bertujuan untuk menganalisis hasil evaluasi yang dilakukan dengan menggunakan Indeks KAMI 4.2. Hasil analisis akan digunakan sebagai kesimpulan untuk selanjutnya dapat dijadikan pertimbangan oleh penyelenggara TIK di SMK XYZ.

4. PEMBAHASAN

Hasil dari penelitian yang dilakukan dengan menggunakan Indeks KAMI 4.2 dijelaskan dalam bab ini.

4.1. Bagian I: Kategori Sistem Elektronik

Kategori sistem elektronik digunakan untuk mengevaluasi tingkat atau kategori sistem elektronik yang digunakan. Kategori sistem elektronik memiliki tiga kriteria status penilaian tingkat ketergantungan yaitu rendah, tinggi, dan strategis. Penilaian dalam kategori sistem elektronik terdiri dari 10 pertanyaan untuk karakteristik instansi/perusahaan.

Hasil evaluasi dari kategori sistem elektronik mendapatkan skor penetapan kategori sistem elektronik yaitu 14.

Tabel 1. Korelasi Kategori SE dengan Status kesiapan

Kategori SE				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Tabel 1 merupakan korelasi antara Kategori Sistem Elektronik dengan Status Kesiapan. Berdasarkan hasil evaluasi dari Indeks KAMI 4.2 terhadap SMK XYZ mendapatkan skor penetapan Kategori SE 14. Maka, dapat disimpulkan bahwa Status Kesiapan dari SMK XYZ adalah Tidak Layak.

4.2. Bagian II: Tata Kelola Keamanan Informasi

Tata kelola keamanan informasi merupakan bagian yang berfungsi untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Tata kelola keamanan informasi diukur dengan empat kriteria status penilaian yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Bagian ini memiliki total 22 pertanyaan terkait fungsi/organisasi keamanan informasi yang terdiri dari 8 pertanyaan kategori pengamanan 1 dengan tingkat kematangan II, 5 pertanyaan kategori pengamanan 2 dengan tingkat kematangan II, 3 pertanyaan kategori pengamanan 2 dengan tingkat kematangan III, dan 6 pertanyaan kategori pengamanan 3 dengan tingkat kematangan IV.

Hasil evaluasi pada bagian ini mendapat total nilai evaluasi tata kelola yaitu 72.

Tabel 2. Nilai Evaluasi Tata Kelola Keamanan Informasi

Kategori Pengamanan	**Jumlah Pertanyaan**	**Nilai**
1	8	21
2	8	36
3	6	15
Total	22	72

Tabel 2 merupakan hasil evaluasi bagian tata kelola keamanan informasi. Hasil evaluasi menunjukkan nilai yang diperoleh adalah 72. Berdasarkan hasil evaluasi tingkat kematangan yang dicapai oleh SMK XYZ pada bagian ini adalah valid pada Tingkat II (Penerapan Kerangka Kerja Dasar). Hal tersebut menunjukkan bahwa bagian ini belum mampu mencapai ambang batas minimum tingkat kematangan untuk standar ISO/IEC 27001:2013 yaitu pada Tingkat III+.

4.3. Bagian III: Pengelolaan Risiko Keamanan Informasi

Pengelolaan risiko keamanan informasi adalah bagian ketiga yang digunakan untuk mengevaluasi

kesiapan penerapan pengelolaan risiko kemanan informasi sebagai dasar penerapan strategi keamanan informasi. Kriteria hasil penilaian pada bagian ini terdiri dari empat kriteria status penilaian yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Bagian ini memiliki total 16 pertanyaan terkait kajian risiko keamanan informasi yang terdiri dari 10 pertanyaan kategori pengamanan 1 dengan tingkat kematangan II, 2 pertanyaan kategori pengamanan 2 dengan tingkat kematangan III, 2 pertanyaan kategori pengamanan 2 dengan tingkat kematangan IV, dan 2 pertanyaan kategori pengamanan 3 dengan tingkat kematangan V.

Hasil evaluasi pada bagian ini mendapatkan total nilai evaluasi pengelolaan risiko keamanan informasi yaitu 15.

Tabel 3. Nilai Pengelolaan Risiko Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	10	7
2	4	8
3	2	0
Total	16	15

Tabel 3 adalah rincian nilai pengelolaan risiko keamanan informasi. Total nilai yang diperoleh pada bagian ini adalah 15. Berdasarkan hasil evaluasi yang diperoleh pada bagian ini hanya valid di kategori kematangan Tingkat I (Kondisi Awal). Artinya bagian ini belum mampu mencapai ambang batas minimum untuk standar ISO/IEC 27001:2013.

4.4. Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Kerangka kerja pengelolaan keamanan informasi menjadi bagian keempat yang dievaluasi. Bagian ini berfungsi untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan dan prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Bagian ini terdiri dari 29 pertanyaan dengan empat kriteria status penilaian yang digunakan yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh.

Pertanyaan-pertanyaan yang ada dibagi menjadi dua kategori utama. Kategori pertama dengan total 19 pertanyaan terkait penyusunan dan pengelolaan kebijakan & prosedur keamanan informasi terdiri dari 7 pertanyaan kategori pengamanan 1 dengan tingkat kematangan II, 2 pertanyaan kategori pengamanan 2 dengan tingkat kematangan II, 6 pertanyaan kategori pengamanan 2 dengan tingkat kematangan III, 2 pertanyaan kategori pengamanan 3 dengan tingkat kematangan III, dan 2 pertanyaan kategori pengamanan 3 dengan tingkat kematangan IV. Kategori kedua dengan total 10 pertanyaan terkait dengan pengelolaan strategi dan program keamanan informasi terdiri dari 2 pertanyaan kategori pengamanan 1 dengan tingkat kematangan II, 3 pertanyaan kategori pengamanan 1 dengan tingkat kematangan III, 2 pertanyaan kategori pengamanan 2 dengan tingkat kematangan III, 1 pertanyaan kategori pengamanan 3 dengan tingkat kematangan IV, dan 2 pertanyaan kategori pengamanan 3 dengan tingkat kematangan V.

Hasil evaluasi pada bagian ini mendapatkan total nilai evaluasi kerangka kerja yaitu 91.

Tabel 4. Nilai Kerangka Kerja Pengelolaan Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	12	24
2	10	40
3	7	27
Total	29	91

Tabel 4 adalah rincian nilai evaluasi bagian kerangka kerja pengelolaan keamanan informasi yang telah digabungkan dari dua kategori utama dengan mendapatkan total nilai 91. Berdasarkan hasil evaluasi yang diperoleh pada bagian ini mendapatkan kategori tingkat kematangan valid pada Tingkat II (Penerapan Kerangka Kerja Dasar). Sehingga bagian ini belum mampu mencapai ambang batas minimum tingkat kematangan yang setara dengan standar ISO/IEC 27001:2013.

4.5. Bagian V: Pengelolaan Aset Informasi

Pengelolaan aset informasi merupakan bagian kelima dalam evaluasi Indeks KAMI 4.2. Bagian ini digunakan untuk mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Bagian ini terdiri dari 38 pertanyaan dengan empat kriteria status penilaian yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Pertanyaan-pertanyaan tersebut dibagi menjadi dua kategori utama. Kategori pertama yaitu 27 pertanyaan terkait pengelolaan aset informasi yang terdiri dari 18 pertanyaan kategori pengamanan 1 dengan tingkat kematangan II, 1 pertanyaan kategori pengamanan 2 dengan tingkat kematangan II, 5 pertanyaan kategori pengamanan 2 dengan tingkat kematangan III, dan 3 pertanyaan kategori pengamanan 3 dengan tingkat kematangan III. Kategori kedua yaitu 11 pertanyaan terkait pengamanan fisik yang terdiri dari 6 pertanyaan kategori pengamanan 1 dengan tingkat kematangan II, 4 pertanyaan kategori pengamanan 2 dengan tingkat kematangan II, dan 1 pertanyaan

kategori pengamanan 3 dengan tingkat kematangan III.

Hasil evaluasi pada bagian ini mendapatkan total nilai evaluasi pengelolaan aset yaitu 78.

Tabel 5. Nilai Pengelolaan Aset Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	24	42
2	10	36
3	4	0
Total	38	78

Tabel 5 adalah rincian nilai untuk bagian pengelolaan aset informasi yang berasal dari dua kategori utama dengan total nilai yang didapatkan yaitu 78. Kategori tingkat kematangan yang diperoleh bagian ini yaitu Tingkat I+ (Kondisi Awal). Artinya bagian ini belum mampu mencapai ambang batas minimum yang setara dengan standar ISO/IEC 27001:2013.

4.6. Bagian VI: Teknologi dan Keamanan Informasi

Teknologi dan keamanan informasi adalah bagian yang mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Pertanyaan pada bagian ini berjumlah 26 pertanyaan yang dinilai dengan empat kriteria status penilaian yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Secara keseluruhan pertanyaan-pertanyaan tersebut terkait dengan pengamanan teknologi. Secara rinci dari 26 pertanyaan yang ada dibagi menjadi 14 pertanyaan kategori pengamanan 1 dengan tingkat kematangan II, 10 pertanyaan kategori pengamanan 2 dengan tingkat kematangan III, 1 pertanyaan kategori pengamanan 3 dengan tingkat kematangan III, dan 1 pertanyaan kategori pengamanan 3 dengan tingkat kematangan IV.

Hasil evaluasi pada bagian ini mendapatkan total nilai evaluasi teknologi dan keamanan informasi yaitu 58.

Tabel 6. Nilai Teknologi dan Keamanan Informasi

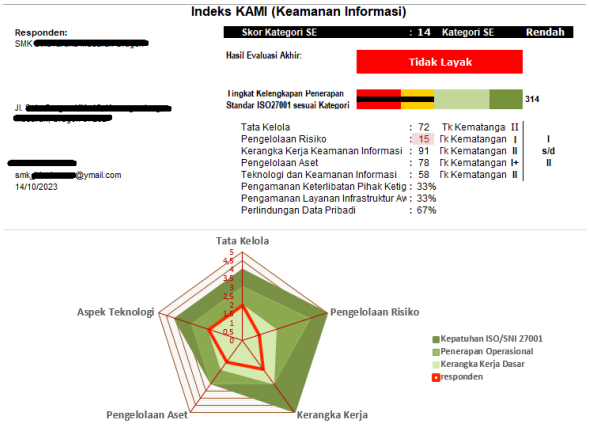
Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	14	
2	10	
3	2	
Total	26	58

Tabel 6 adalah rincian nilai pada bagian teknologi dan keamanan informasi dengan total nilai yang diperoleh adalah 58. Bagian ini mendapatkan kategori tingkat kematangan yang valid pada Tingkat II (Penerapan Kerangka Kerja Dasar). Perolehan tingkat tersebut menunjukkan bahwa bagian ini belum mampu mencapai ambang batas minimum tingkat kematangan yang setara dengan standar ISO/IEC 27001:2013.

4.7. Bagian VII: Suplemen

Suplemen merupakan bagian ke delapan sekaligus bagian akhir yang digunakan untuk mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Bagian ini terdiri dari 53 pertanyaan yang dinilai dengan empat kriteria status penilaian yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Pertanyaan-pertanyaan pada bagian ini dibagi atas kategori dan sub-kategori yaitu kategori pengamanan keterlibatan pihak ketiga penyedia layanan dengan sub-kategori manajemen risiko dan pengelolaan keamanan pihak ketiga, pengelolaan sub-kontraktor/alih daya pada pihak ketiga, pengelolaan layanan dan keamanan pihak ketiga, pengelolaan perubahan layanan dan kebijakan pihak ketiga, penanganan aset, pengelolaan insiden oleh pihak ketiga, rencana kelangsungan pihak ketiga, kategori pengamanan layanan infrastruktur awan (cloud service), dan kategori perlindungan data pribadi.

Hasil evaluasi pada bagian ini mendapatkan nilai untuk aspek Pengamanan Keterlibatan Pihak Ketiga 33%, aspek Pengamanan Layanan Infrastruktur Awan 33%, dan aspek Perlindungan Data Pribadi 67%. Berdasarkan hasil tersebut menunjukkan bahwa aspek Perlindungan Data Pribadi cukup diperhatikan dalam status penerapannya. Berbeda dengan dua aspek yang lain yaitu aspek Pengamanan Keterlibatan Pihak Ketiga dan aspek Pengamanan Layanan Infrastruktur Awan yang dalam statusnya belum diterapkan dengan baik atau masih dalam perencanaan.



Gambar 3. Dashboard Indeks KAMI 4.2

Gambar 3 merupakan rangkuman hasil dari evaluasi Indeks KAMI 4.2 yang dilakukan pada SMK XYZ. Gambar tersebut menunjukkan hasil evaluasi akhir untuk SMK XYZ mendapatkan skor Kategori Sistem Elektronik 14 dan mendapatkan predikat Rendah. Kemudian, hasil evaluasi akhir dinyatakan status kesiapannya Tidak Layak dengan total skor 314 untuk Tingkat Kelengkapan

Penerapan Standar ISO 27001 sesuai Kategori SE. Hasil evaluasi tiap bagian penilaian juga disebutkan kembali pada Dashboard ini. Grafik yang ada pada gambar 3 menunjukkan bagian yang menjadi fokus responden terhadap kepatuhan ISO/SNI 27001, penerapan operasional, dan kerangka kerja dasar. Responden memiliki fokus yang cukup baik terhadap area Tata Kelola, Kerangka Kerja, dan Aspek Teknologi. Karena ketiga area tersebut mendapatkan tingkat kematangan yang cukup bagus yaitu Tingkat II (Penerapan Kerangka Kerja Dasar).

5. KESIMPULAN

Berdasarkan hasil dan pembahasan penelitian yang telah dijelaskan pada bab sebelumnya, maka dapat diperoleh kesimpulan sebagai berikut:

1. Hasil evaluasi akhir terhadap SMK XYZ memperoleh skor Kategori SE 14 yang masuk ke dalam Kategori SE Rendah. Selain itu, SMK XYZ mendapatkan hasil status kesiapan Tidak Layak dengan skor Tingkat Penerapan Standar ISO27001 sesuai Kategori SE yaitu 314.
2. Skor tiap area yang dievaluasi yaitu Tata Kelola memperoleh skor 72 dengan tingkat kematangan valid Tingkat II, Pengelolaan Risiko memperoleh skor 15 dengan tingkat kematangan valid Tingkat I, Kerangka Kerja Keamanan Informasi memperoleh skor 91 dengan tingkat kematangan valid Tingkat II, Pengelolaan Aset memperoleh skor 78 dengan tingkat kematangan valid Tingkat I+, Teknologi dan Keamanan Informasi memperoleh skor 58 dengan tingkat kematangan valid Tingkat II, dan bagian terakhir adalah Suplemen sebagai bagian tambahan pengukuran dengan tiga aspek di dalamnya yaitu aspek Pengamanan Keterlibatan Pihak Ketiga memperoleh nilai 33%, aspek Pengamanan Layanan Infrastruktur Awan memperoleh nilai 33%, dan aspek Perlindungan Data Pribadi memperoleh nilai 67%.
3. Hasil evaluasi Indeks KAMI 4.2 terhadap SMK XYZ dapat menjadi gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi yang ada di SMK XYZ dan kemudian dapat menjadi perhatian bagi penyelenggara TIK yang ada untuk memperbaiki dan meningkatkan keamanan informasi pada area-area yang telah dievaluasi sesuai dengan standar ISO/IEC 27001:2013.

DAFTAR PUSTAKA

BSSN. (n.d.). *Konsultasi dan Assesment Indeks KAMI*. https://www.bssn.go.id/indeks-kami/

Clarissa, S., & Wang, G. (2023). Assessing Information Security Management Using ISO 27001:2013. *Jurnal Indonesia Sosial Teknologi*, *4*(9), 1361–1371. https://doi.org/10.59141/jist.v4i9.739

Dewantara, R., & Sugiantoro, B. (2021). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *8*(6), 1137. https://doi.org/10.25126/jtiik.2021863123

Hambali, H., & Musa, P. (2020). Analysis of Governance Security Management Information System Using Index Kami in Central Government Institution. *Angkasa: Jurnal Ilmiah Bidang Teknologi*, *12*(1). https://doi.org/10.28989/angkasa.v12i1.563

Khamil, D. I. (2022). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 dan ISO/IEC 27001:2013 (Studi Kasus : Diskominfo Kabupaten Gianyar). *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *9*(3), 1948–1960. https://doi.org/10.35957/jatisi.v9i3.2310

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022). Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach. *IEEE Access*, *10*, 65044–65054. https://doi.org/10.1109/ACCESS.2022.3179822

Khusna, T. N., & Sugiantoro, B. (2023). Pengukuran Tingkat Keamanan Informasi Pada Upt-Psi Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (Kami) Versi 4.2. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(3), 847–856. https://doi.org/10.29100/jipi.v8i3.3720

Kornelia, A., & Irawan, D. (2021). Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1. *Jurnal Pengembangan Sistem Informasi Dan Informatika*, *2*(2), 78–86. https://doi.org/10.47747/jpsii.v2i2.548

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*(January), 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Paramita, S., Siregar, S. A., Damanik, R. A., & ... (2022). Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013. *Bulletin of Information …*, *3*(4), 374–379. https://journal.fkpt.org/index.php/BIT/article/view/421%0Ahttps://journal.fkpt.org/index.php/BIT/article/download/421/263

R.Y Rahman, M. . H. (2023). EVALUASI KEAMANAN INFORMASI PADA SMAN 1 TANGGAMUS MENGGUNAKAN INDEKS

KAMI VERSI 4.2. *JURNAL FASILKOM*, *13*(2), 181–187.

Rahmah, Y., Hayuhardika, W., & Dwi herlambang, A. (2019). Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto menggunakan Indeks Keamanan Informasi (KAMI). *Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(6), 840–846.

Ramadhani, N. D., Putra, W. H. N., & Herlambang, A. D. (2020). Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *4*(5), 1490–1498. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7259

Sugiarto, P., & Suryanto, Y. (2022). Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001:2013. *International Journal of Mechanical Engineering*, *7*(2), 974–5823.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.