EVALUASI KEAMANAN PENERAPAN SISTEM INFORMASI BERDASARKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA SMK N 1 NANGGULAN

Retno Widyarti, Yuli Praptomo Pamungkas Hari Sungkowo*
Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer El Rahma Yogyakarta
Jalan Sisingamangaraja No.76, Brotokusuman, Kec. Mergangsan, Kota Yogyakarta, D.I.Yogyakarta 55671
y.praptomo@gmail.com

ABSTRAK

Pemanfaatan sistem informasi di lingkungan pendidikan semakin meningkat, sehingga kebutuhan akan keamanan informasi menjadi semakin penting. SMK Negeri 1 Nanggulan telah menggunakan berbagai aplikasi untuk mendukung proses administrasi dan akademik, namun penguatan keamanan informasi belum dilakukan secara menyeluruh. Beberapa insiden seperti infeksi malware, kerusakan file, dan penggunaan akun bersama tanpa otorisasi menunjukkan adanya kerentanan yang perlu dievaluasi lebih lanjut. Penelitian ini bertujuan untuk menilai tingkat kesiapan dan kematangan keamanan informasi di SMK Negeri 1 Nanggulan serta mengidentifikasi area yang memerlukan peningkatan. Evaluasi dilakukan menggunakan Indeks Keamanan Informasi (KAMI) versi 3.1 dari BSSN, yang mengacu pada standar ISO/IEC 27001:2013. Metode penelitian meliputi observasi, wawancara, dan pengisian kuesioner oleh pihak sekolah. Hasil penilaian menunjukkan bahwa tingkat kematangan keamanan informasi berada pada Level 3 (Standar) dengan capaian keseluruhan 44,07%. Nilai ini mengindikasikan bahwa sekolah telah memiliki beberapa kontrol dasar keamanan, namun belum didukung oleh kebijakan, prosedur, dan dokumentasi yang memadai. Berdasarkan temuan tersebut, direkomendasikan penguatan tata kelola keamanan, peningkatan kerangka kerja keamanan, serta penyusunan SOP sesuai kontrol ISO/IEC 27001:2013 agar pengelolaan keamanan informasi dapat berjalan lebih efektif dan berkelanjutan.

Kata kunci : *Perlindungan Informasi, IndeksKAMI,Evaluasi Sistem, SMK, BSSN, Sistem Informasi*

1. PENDAHULUAN

Pemanfaatan teknologi informasi dan komunikasi (TIK) di lingkungan pendidikan semakin berkembang seiring meningkatnya kebutuhan akan layanan administrasi dan akademik yang cepat, akurat, dan transparan. Sistem informasi kini menjadi bagian penting dalam mendukung efektivitas kegiatan sekolah, mulai dari pengelolaan data peserta didik hingga pemantauan proses pembelajaran. Hal ini menunjukkan bahwa digitalisasi telah menjadi fondasi utama dalam peningkatan mutu tata kelola pendidikan. SMK Negeri 1 Nanggulan merupakan salah satu sekolah yang telah mengintegrasikan berbagai aplikasi dalam operasionalnya, seperti e-Rapor, Dapodik, E-Prima, ASN Memayu, dan sistem informasi internal lainnya. Pemanfaatan berbagai aplikasi tersebut membantu sekolah mempercepat proses administrasi serta memastikan data yang dikelola lebih mudah dianalisis dan digunakan untuk pengambilan keputusan. Implementasi ini juga menjadi langkah strategis untuk mendukung efisiensi manajemen sekolah.

Namun, penggunaan sistem informasi yang semakin luas membawa konsekuensi berupa meningkatnya risiko keamanan informasi. Ancaman seperti malware, akses tidak sah, kerusakan file, dan kebocoran data berpotensi mengganggu kelancaran layanan pendidikan. Beberapa insiden yang ditemukan, seperti file rusak akibat malware dan penggunaan akun bersama tanpa otorisasi, menunjukkan bahwa penerapan keamanan informasi di sekolah masih belum sepenuhnya terkelola dengan baik.

Permasalahan tersebut diperkuat oleh belum adanya evaluasi formal yang menilai tingkat kesiapan dan kematangan keamanan informasi di SMK Negeri 1 Nanggulan. Ketiadaan evaluasi membuat sekolah belum memiliki gambaran yang jelas mengenai prioritas perbaikan keamanan yang harus dilakukan. Kondisi ini dapat menimbulkan celah keamanan yang lebih besar jika sistem terus berkembang tanpa penguatan kontrol yang memadai.

Untuk menjawab kebutuhan tersebut, penelitian ini menggunakan Indeks Keamanan Informasi (KAMI) yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN). Instrumen ini dipilih karena mampu menilai kesiapan pengelolaan keamanan informasi secara sistematis, sekaligus mengukur tingkat kematangan berdasarkan prinsip dan kontrol yang mengacu pada ISO/IEC 27001:2013. Pendekatan ini memungkinkan penilaian yang lebih terukur terhadap kondisi keamanan informasi di sekolah.

Tujuan utama dari penelitian ini adalah menilai tingkat kesiapan keamanan informasi, mengidentifikasi kelemahan yang masih muncul, serta mengetahui tingkat kematangan keamanan informasi yang telah dicapai oleh SMK Negeri 1 Nanggulan. Evaluasi dilakukan melalui observasi, wawancara, dan pengisian kuesioner Indeks KAMI oleh pihak terkait, sehingga hasil yang diperoleh mencerminkan kondisi aktual penerapan keamanan informasi di lingkungan sekolah.

Sebagai rencana penyelesaian masalah, hasil evaluasi akan digunakan untuk menyusun rekomendasi perbaikan yang diselaraskan dengan kontrol pada ISO/IEC 27001:2013. Rekomendasi

tersebut diharapkan dapat membantu sekolah memperkuat kebijakan keamanan, meningkatkan prosedur operasional, membentuk struktur pengelolaan keamanan informasi, serta meningkatkan kesadaran keamanan siber bagi seluruh pengguna. Dengan demikian, pengelolaan sistem informasi di sekolah dapat berlangsung secara lebih aman, andal, dan berkelanjutan.

2. TINJAUAN PUSTAKA

2.1. Keamanan Informasi

Keamanan informasi merupakan rangkaian usaha sistematis yang ditujukan untuk menjaga data terhadap berbagai bentuk ancaman yang berpotensi menimbulkan kerugian, baik berupa kehilangan, kerusakan, maupun kebocoran informasi. Perlindungan ini mencakup proses, kebijakan, dan kontrol yang dirancang untuk memastikan bahwa data tetap terlindungi selama proses pengolahan, penyimpanan, maupun distribusinya. Dalam konteks organisasi modern, *keamanan informasi* telah menjadi aspek fundamental karena setiap aktivitas semakin bergantung pada sistem elektronik dan jaringan digital [3]. Tanpa mekanisme proteksi yang memadai, risiko penyalahgunaan data, manipulasi informasi, dan serangan *siber* akan meningkat, terutama pada sistem yang menjadi tulang punggung layanan operasional.

Prinsip dasar perlindungan informasi umumnya merujuk pada tiga konsep utama, yaitu *Confidentiality, Integrity, and Availability (CIA)*. *Confidentiality* mengacu pada upaya menjamin bahwa informasi hanya dapt diakses oleh pihak yang memiliki hak atau otorisasi; *Integrity* menjaga agar data tidak diubah, dihapus, atau dimanipulasi oleh pihak yang tidak berwenang; sedangkan *Availability* memastikan informasi dan sistem pendukungnya tetap tersedia ketika dibutuhkan oleh pengguna yang sah [9]. Ketiga prinsip tersebut merupakan fondasi dari berbagai kerangka kerja keamanan informasi dan menjadi landasan penyusunan kontrol teknis maupun kebijakan organisasi [4]. Dengan menerapkan kontrol yang sejalan dengan *CIA Triad*, organisasi dapat meminimalkan potensi ancaman terhadap aset informasi.

Dalam konteks pendidikan, keamanan informasi semakin penting karena sekolah mengelola data sensitif, seperti identitas peserta didik, arsip nilai, dokumen akademik, dan data administrasi internal. Jika tidak dilindungi, data tersebut berpotensi menjadi sasaran serangan, baik melalui *malware*, peretasan akun, maupun gangguan pada sistem aplikasi. Penelitian sebelumnya menunjukkan bahwa institusi pendidikan kerap menghadapi tantangan keamanan akibat lemahnya kontrol akses, belum adanya prosedur penanganan insiden, serta rendahnya kesadaran keamanan di lingkungan pengguna [8], [12]. Oleh sebab itu, dibutuhkan pendekatan keamanan yang menyeluruh agar pengelolaan informasi di sekolah dapat berjalan aman, andal, dan berkelanjutan.

2.2. Sistem Manajemen Keamanan Informasi *(ISO/IEC 27001:2013)*

Sistem Manajemen Keamanan Informasi atau *Information Security Management System (ISMS)* merupakan sebuah kerangka kerja yang disusun untuk mengatur, mengelola, dan menjaga keamanan informasi secara menyeluruh melalui penerapan kebijakan, prosedur, dan kontrol yang terstandarisasi [6]. Standar internasional yang menjadi acuan utama dalam pengaturan keamanan informasi adalah *ISO/IEC 27001:2013*, yang menekankan bahwa perlindungan informasi harus berbasis risiko dan dilakukan secara berkesinambungan melalui proses yang terdokumentasi dan dapat diaudit [10]. Melalui pendekatan tersebut, organisasi tidak hanya diharapkan mampu mencegah terjadinya insiden keamanan, tetapi juga mampu merespons dan memulihkan layanan dengan cepat ketika insiden terjadi.

ISO/IEC 27001:2013 menerapkan model *Plan–Do–Check–Act (PDCA)*, yang digunakan untuk memastikan keamanan informasi berjalan secara dinamis dan berkelanjutan. Tahap *Plan* mencakup penilaian risiko dan penyusunan kebijakan keamanan, *Do* berfokus pada penerapan kontrol, *Check* melakukan evaluasi dan audit berkala, sedangkan *Act* digunakan untuk melakukan perbaikan terhadap kelemahan yang ditemukan [9]. Selain kerangka proses tersebut, standar ini juga diperkuat dengan *Annex A* yang berisi daftar kontrol keamanan, meliputi pengendalian akses, keamanan jaringan, proteksi aset, pengelolaan insiden, serta kebijakan penggunaan sistem [5].

Penerapan *ISO/IEC 27001:2013* pada lingkungan pendidikan, termasuk sekolah, dinilai relevan karena dapat membantu institusi dalam membangun pengelolaan keamanan informasi yang lebih tertata serta terarah. Melalui adanya standar ini, sekolah dapat meningkatkan perlindungan terhadap aset informasi seperti data pribadi siswa, arsip akademik, maupun dokumen administrasi, sekaligus memperbaiki tata kelola keamanan secara menyeluruh [8]. Selain itu, standar ini juga mendorong organisasi untuk menyesuaikan kontrol keamanan dengan tingkat risiko yang dihadapi, sehingga pengelolaan keamanan informasi tidak hanya bersifat responsif, tetapi juga preventif [11].

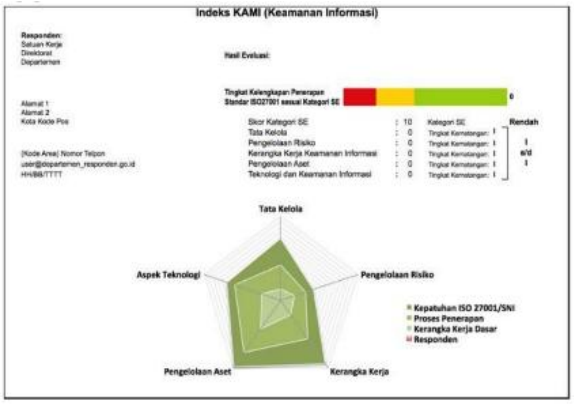
2.3. *Indeks Keamanan Informasi (KAMI) Versi 3.1*

Indeks Keamanan Informasi (KAMI) adalah instrumen penilaian yang dibuat oleh *Badan Siber dan Sandi Negara (BSSN)* untuk menilai tingkat kesiapan serta kematangan penerapan keamanan informasi suatu instansi dalam mengelola sistem elektronik secara aman, terarah, dan berkesinambungan [1]. Penilaian ini tidak dimaksudkan untuk mengaudit kontrol teknis secara mendalam, melainkan menilai sejauh mana kebijakan, prosedur, serta implementasi keamanan informasi telah diterapkan oleh organisasi

sesuai prinsip pengamanan yang diterapkan dalam standar *ISO/IEC 27001:2013* [4].

Pada Versi 3.1**,** *KAMI* menilai level kematangan pengamanan informasi melalui lima area utama, meliputi: (1) Tata Kelola Keamanan Informasi, (2) Manajemen Risiko Keamanan Informasi, (3) Kerangka Kerja Keamanan Informasi, (4) Pengelolaan Aset Informasi, serta (5) Teknologi dan Keamanan Informasi [5]. Kelima area ini merepresentasikan aspek kebijakan, proses, hingga kontrol teknis yang menjadi fondasi utama untuk membangun tata kelola keamanan informasi yang terstruktur dan terukur.

Struktur lima area penilaian tersebut dapat dilihat pada Gambar 1 dibawah ini..



Gambar 1. Dashboard penilaian indeks KAMI (*Sumber: Badan Siber dan Sandi Negara, 2019*)

Untuk memastikan hasilnya bisa ditindaklanjuti, *Indeks KAMI* memetakan setiap area penilaian kedalam kontrol yang tercantum pada *Annex A ISO/IEC 27001:2013*, sehingga usulan perbaikan yang dihasilkan dapat diterapkan secara operasional dan selaras dengan standar keamanan internasional [10], [11]. Dengan demikian, *KAMI* berperan sebagai alat *assessment* kematangan, sedangkan *ISO/IEC 27001* menjadi pedoman implementasi kontrol. Hubungan antara kedua kerangka kerja tersebut ditampilkan pada *Gambar 2* berikut.

Gambar 2. Tampilan dashboard penilaian indeks KAMI

Penggunaan *Indeks KAMI* semakin relevan untuk organisasi pendidikan karena banyak sekolah telah bergantung pada sistem elektronik dalam pengelolaan data akademik, administrasi, dan layanan pembelajaran. Melalui penilaian ini, sekolah dapat mengetahui posisi kematangannya, sekaligus memperoleh gambaran prioritas peningkatan keamanan informasi yang perlu dilakukan [8], [12].

2.4. *Kategori Sistem Elektronik (SE)* pada Indeks *KAMI* Edisi 3.1

Dalam proses evaluasi pada *Keamanan Informasi (KAMI)* Versi 3.1**,** langkah awal yang dilakukan adalah menentukan *Kategori Sistem Elektronik (SE)*. Tahap ini bertujuan mengukur seberapa besar ketergantungan organisasi terhadap sistem elektronik yang digunakan dalam operasionalnya [5]. Penentuan kategori *SE* diperlukan agar hasil penilaian dapat diinterpretasikan secara tepat, karena semakin tinggi ketergantungan suatu instansi pada sistem elektronik, semakin tinggi pula tingkat keamanan yang wajib diterapkan [6], [9].

Proses klasifikasi *SE* mempertimbangkan beberapa indikator, seperti jenis layanan yang dikelola sistem, keterlibatan data sensitif, jumlah pengguna, ruang lingkup layanan, serta dampak yang mungkin terjadi apabila sistem mengalami gangguan. Secara umum, *Indeks KAMI* Versi 3.1 mengelompokkan *SE* dibagi ke dalam empat kategori, yakni *Rendah*, *Sedang*, *Tinggi*, dan *Sangat Tinggi*, sebagaimana ditunjukkan pada *Gambar 3* berikut.

Gambar 3. Ilustrasi kategori Sistem Elektronik (SE) – BSSN Versi 3.1

Berdasarkan pedoman *Indeks KAMI* edisi 3.1, penentuan *Kelas Sistem Elektronik (SE)* dilakukan dengan memperhatikan tingkat ketergantungan organisasi terhadap sistem yang digunakan. Klasifikasi tersebut dibedakan ke dalam empat tingkatan, yakni *Rendah*, *Sedang*, *Tinggi*, dan *Sangat Tinggi*, sebagaimana ditampilkan pada Tabel 1 berikut.

Tabel 1. Klasifikasi Kategori Sistem Elektronik (SE)

Kategori SE	Rentang Nilai	Karakteristik Utama
Rendah	0–15	Gangguan tidak berdampak signifikan pada layanan
Sedang	16–25	Gangguan berpengaruh pada layanan operasional internal
Tinggi	26–34	Gangguan menghentikan layanan inti organisasi
Sangat Tinggi	35–50	Gangguan berdampak luas pada layanan publik

2.5. *Rumus Perhitungan Indeks KAMI* Edisi 3.1

Proses penilaian pada *Indeks Keamanan Informasi (KAMI* Versi 3.1) dilakukan melalui tiga tahapan utama, yaitu perhitungan *Kategori Sistem Elektronik (SE)*, pengukuran skor per area evaluai, serta penentuan level kematangan keamanan informasi

(level I–V). Tahapan ini memberikan gambaran kuantitatif mengenai kesiapan keamanan informasi pada sebuah instansi dan menjadi landasan dalam menetapkan prioritas perbaikan [6], [9].

Tahap pertama adalah menghitung skor *S*E berdasarkan total jawaban pada bagian kuesioner *SE*

$$Skor\ SE = \sum \text{ Nilai Jawaban} \quad (1)$$

Interpretasi semakin tinggi skor *SE*, semakin tinggi kategori sistem elektronik dan semakin besar kebutuhan kontrol keamanan.

Tahap berikutnya adalah menghitung persentase skor pada masing-masing area penilaian *KAMI*

$$Skor\ Area\ (\%) = \left(\frac{Nilai\ Diperoleh}{Nilai\ Maksimum}\right) x100\% \quad (2)$$

Persentase ini menunjukkan kondisi kesiapan keamanan informasi pada setiap area yang dinilai, meliputi Tata Kelola, Manajemen Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi Informasi.

Selanjutnya, untuk memperoleh keseluruhan gambaran tingkat kesiapan organisasi, skor tiap area dijumlahkan sehingga diperoleh skor total

$$Skor\ Total = \sum \text{ Skor Area} \quad (3)$$

Berdasarkan *Indeks KAMI* edisi 3.1, hasil penilaian kemudian dipetakan ke dalam lima tingkat kematangan keamanan informasi yang menggambarkan sejauh mana penerapan kontrol keamanan telah dijalankan oleh organisasi. Klasifikasi lengkapnya ditampilkan pada Tabel 2 berikut.

Tabel 2. Level keamanan Informasi Indeks KAMI

Level	**Kategori Kematangan**	**Deskripsi Utama**
Level I	Inisiasi	Penerapan keamanan belum memadai
Level II	Dasar	Kebijakan awal tersedia tetapi belum konsisten
Level III	Standar	Kontrol dasar berjalan meskipun belum sepenuhnya efektif
Level IV	Terkelola	Prosedur diterapkan secara konsisten dan terdokumentasi
Level V	Optimal	Pengelolaan keamanan berjalan efektif dan berkelanjutan

Nilai persentase tiap area kemudian digunakan pada bagian analisis untuk menentukan area mana yang menjadi prioritas perbaikan [8], [12].

2.6. Penelitian Terdahulu

Penelitian mengenai penilaian keamanan informasi berbasis *Indeks KAMI* yang merujuk pada *ISO/IEC 27001:2013* telah banyak dilaksanakan pada berbagai institusi, terutama di sektor pendidikan dan instansi pemerintah. Penelitian yang dilakukan oleh Anggraeni menyimpulkan bahwa kesiapan keamanan informasi sangat dipengaruhi oleh keberadaan kebijakan dan struktur tata kelola, namun implementasinya sering belum konsisten di lapangan [1]. Temuan tersebut sejalan dengan hasil penelitian Fitriana, yang menunjukkan bahwa institusi pendidikan umumnya berada pada tingkat kematangan menengah karena lemahnya dokumentasi keamanan dan tidak meratanya penerapan prosedur keamanan informasi [3].

Dalam konteks yang lebih luas, penelitian Ningrum et al. menekankan pentingnya penguatan kontrol akses dan perlindungan infrastruktur, terutama pada sistem akademik yang digunakan oleh banyak pengguna [8]. Sementara itu, Putra dan Nasution menegaskan bahwa pemetaan *Indeks* KAMI dengan *ISO/IEC 27001* dapat membantu organisasi menyusun rencana perbaikan yang lebih terukur, karena rekomendasi yang dihasilkan dapat langsung dikaitkan dengan kontrol yang relevan pada *Annex A* [10]. Penelitian lain oleh Ramdani dan Septiani menemukan bahwa banyak sekolah telah mengadopsi sistem elektronik, tetapi masih kurang memiliki mekanisme formal untuk mengelola keamanan informasi, sehingga risiko gangguan layanan masih tinggi [11].

Dari sisi pengelolaan risiko, Paramita et al. menunjukkan bahwa proses identifikasi risiko sering dilakukan, namun langkah mitigasi dan pengawasan jarang dijalankan secara konsisten [9]. Selain itu, Salsabila dan Karim menemukan bahwa serangan berupa *malware* dan gangguan sistem masih menjadi ancaman nyata pada sekolah yang belum menerapkan kontrol teknis secara menyeluruh [12]. Hal ini diperkuat oleh penelitian Wulandari dan Rakhman, yang menyatakan bahwa lemahnya prosedur penanganan insiden menyebabkan organisasi lambat merespons ketika terjadi gangguan pada *sistem informasi* [14].

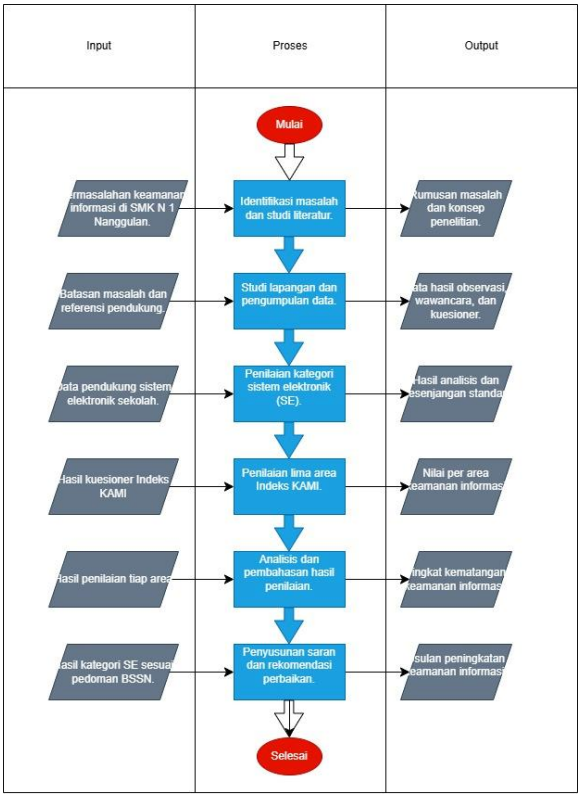
Melihat rangkaian temuan dari penelitian-penelitian tersebut, dapat disimpulkan bahwa tiga pola masalah paling dominan pada institusi pendidikan adalah lemahnya kontrol teknis, kurangnya dokumentasi kebijakan, dan rendahnya kesadaran keamanan informasi pengguna sistem [1], [3], [8], [12]. Pola ini menunjukkan bahwa penerapan keamanan informasi tidak cukup hanya mengandalkan infrastruktur, tetapi membutuhkan tata kelola yang kuat, prosedur yang jelas, serta peningkatan kompetensi pengguna agar keamanan informasi dapat berjalan berkelanjutan.

3. METODE PENELITIAN

Pada bagian ini dijelaskan mengenai metode penelitian yang digunakan, sehingga tahapan pengerjaan menjadi lebih sistematis dan terkelola dengan baik. Penelitian ini menggunakan pendekatan *kuantitatif deskriptif*, di mana data diperoleh dari hasil pengisian *kuesioner* dari kepala sekolah, guru, dan staf *IT* di SMK Negeri 1 Nanggulan**.**

Tujuan dari pendekatan ini adalah untuk menggambarkan kondisi keamanan informasi berdasarkan nilai numerik yang dihasilkan dari setiap area penilaian *Indeks KAMI*. Hasil pengukuran tersebut kemudian dianalisis untuk mengetahui tingkat kematangan pengamanan informasi serta kesesuaiannya dengan standar *ISO/IEC 27001:2013*.

Tahapan metodologi penelitian yang digunakan pada studi ini disajikan pada Gambar 4 berikut



Gambar 4. Tahapan metodologi penelitian

Langkah-langkah yang ditempuh dalam penelitian ini dapat dijelaskan sebagai berikut:

a. Melakukan Identifikasi Masalah dan Studi Literatur
   Langkah awal dilakukan dengan mengidentifikasi masalah keamanan informasi yang terjadi di sekolah serta meninjau referensi terkait, seperti panduan *Indeks KAMI BSSN* serta standar *ISO/IEC 27001:2013*, untuk membentuk dasar teori penelitian.
b. Melakukan kegiatan studi lapangan dan proses pengumpulan data
   Informasi diperoleh melalui instrument kuesioner *Indeks KAMI* versi 3.1 dan wawancara dengan pihak sekolah. Setiap jawaban *kuesioner* memiliki bobot skor yang menunjukkan kondisi nyata penerapan keamanan informasi.
c. Melakukan Penilaian Kategori Tingkat *Sistem Elektronik (SE)*
   Tahap ini menentukan kategori sistem elektronik sekolah berdasarkan nilai total yang diperoleh, mengacu pada skala BSSN yang membagi kategori menjadi *Rendah (0–15), Sedang (16–25), Tinggi (26–34)*, dan *Sangat Tinggi (35–50).*
d. Melakukan Penilaian Lima Area *Indeks KAMI*
   Lima area yang dinilai meliputi Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, serta Teknologi dan Keamanan Informasi. Nilai pada tiap area dihitung dan dikonversikan menjadi persentase tingkat kematangan.
e. Melakukan Analisis dan Pembahasan Data
   Hasil penilaian dari tiap area kemudian dianalisis menggunakan metode *kuantitatif deskriptif* untuk mengetahui posisi tingkat kematangan sekolah. Data divisualisasikan melalui tabel dan diagram untuk memperjelas hasil.
f. Penyusunan Saran dan Perningkatan Mengacu pada *ISO/IEC 27001:2013* Berdasarkan temuan analisis, dibuat rekomendasi peningkatan keamanan informasi yang diselaraskan dengan kontrol keamanan dalam *Annex A ISO/IEC 27001:2013*, agar sekolah dapat memperkuat kebijakan, prosedur, dan sistem pengamanan datanya.

4. HASIL DAN PEMBAHASAN

4.1. Nilai Kepentingan Penggunaan *Sistem Elektronik (SE)* pada SMK Negeri 1 Nanggulan

Berdasarkan ouput penilaian terkait tingkat kepentingan penggunaan *Sistem Elektronik (SE)* pada SMK Negeri 1 Nanggulan, diperoleh skor total sebesar 20. Berdasarkan pedoman *Indeks KAMI* edisi 3.1, nilai ini termasuk dalam kategori *Sedang*, yaitu pada rentang skor 16 hingga 25. Rincian dari penilaian tersebut ditampilkan pada Tabel 3 berikut.

Tabel 3. Rekap penilaian penggunaan Sistem Elektronik SMK Negeri 1 Nanggulan

No	Aspek Penilaian	Nilai	Ket
1	Sistem elektronik digunakan untuk kegiatan akademik dan administrasi sekolah	5	A
2	Data pribadi siswa dan guru disimpan dalam sistem	4	B
3	Ketergantungan terhadap sistem tinggi (digunakan setiap hari)	4	B
4	Sistem digunakan lebih dari satu unit kerja (kurikulum, tata usaha, kepegawaian)	3	C
5	Terdapat pengaruh terhadap layanan operasional sekolah bila sistem terganggu	4	B
Total Skor		**20**	**Kategori Sedang**

Kategori *Sedang* menunjukkan bahwa *sistem elektronik* di SMK Negeri 1 Nanggulan telah menjadi bagian penting dari proses operasional sekolah,

terutama untuk kegiatan administrasi, pengelolaan data akademik, serta kepegawaian. Namun, sistem belum sepenuhnya masuk kategori *tinggi* karena cakupan pengguna dan dampak gangguan masih terbatas pada lingkungan internal sekolah.

Penggunaan *sistem elektronik* di SMK Negeri 1 Nanggulan menunjukkan tingkat ketergantungan yang cukup relative tinggi terhadap data digital. Dengan adanya pengelolaan data siswa, guru, dan kegiatan pembelajaran secara *daring* maupun lokal, keberadaan *sistem elektronik* menjadi komponen penting yang perlu dijaga dari risiko kehilangan data, gangguan operasional, atau ancaman keamanan digital.

4.2. Evaluasi Kesiapan 5 Area Keamanan Informasi di SMK Negeri 1 Nanggulan

Penilaian lima area utama pengamanan informasi dilakukan dengan menggunakan *Indeks Keamanan Informasi (KAMI)* versi 3.1 yang dikeluarkan oleh *Badan Siber dan Sandi Negara (BSSN).* Lima area yang dinilai meliputi Tata Kelola Keamanan Informasi, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, serta Teknologi dan Keamanan Informasi**.**

Hasil penilaian memperlihatkan variasi level kesiapan di tiap area dengan rata-rata keseluruhan sebesar 44,07%**.** Nilai ini menempatkan sekolah pada *Level 3 (Standar),* yang berarti penerapan keamanan informasi sudah dilakukan namun belum sepenuhnya terdokumentasi dan terintegrasi dengan *sistem manajemen keamanan informasi berbasis ISO/IEC 27001:2013.*Visualisasi hasil evaluasi tersebut disajikan pada table 4 berikut.

Tabel 4. Rekapitulasi Penilaian Indeks KAMI

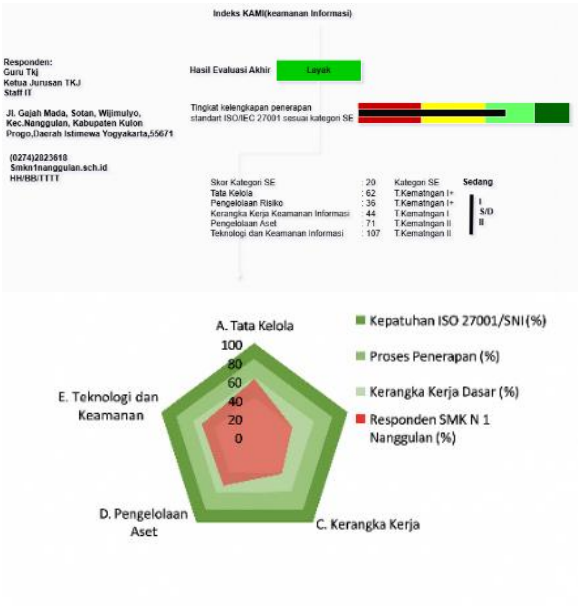
Area Penilaian	Skor Maks	Skor Diperoleh	(%)	Tingkat Kematangan
Tata Kelola Keamanan Informasi	150	62	41,3	Standar
Pengelolaan Risiko Keamanan Informasi	90	36	40,0	Standar
Kerangka Kerja Keamanan Informasi	130	44	33,8	Dasar
Pengelolaan Aset Informasi	150	71	47,3	Standar
Teknologi dan Keamanan Informasi	210	107	50,9	Cukup
Total	**720**	**320**	**44,07%**	**Level 3 (Standar)**

Berdasarkan data pada table tersebut, dapat ditegaskan bahwa Tata Kelola Keamanan Informasi**,** Pengelolaan Risiko, dan Pengelolaan Aset berada pada level *Standar*, sementara Kerangka Kerja Keamanan Informasi masih pada tingkat Dasar, dan Teknologi serta Keamanan Informasi sudah mencapai *Cukup*.

Perbedaan capaian antararea menunjukkan bahwa implementasi keamanan informasi di SMK Negeri 1 Nanggulan telah berjalan secara fungsional, namun belum memiliki sistem dokumentasi dan kebijakan yang konsisten di semua lini. Area dengan nilai tertinggi yaitu Teknologi dan Keamanan Informasi, mengindikasikan bahwa sekolah telah melakukan pengamanan pada *level* teknis seperti *antivirus*, autentikasi pengguna, dan kontrol akses. Sebaliknya, area Kerangka Kerja menunjukkan perlunya peningkatan pada aspek kebijakan dan *SOP* formal sebagai dasar tata kelola keamanan informasi.

4.3. Analisis Hasil Akhir Evaluasi *Indeks KAMI*

Bagian ini memaparkan hasil evaluasi *Indeks KAMI* yang telah dilakukan di SMK Negeri 1 Nanggulan menggunakan versi 3.1 dari *Badan Siber dan Sandi Negara (BSSN).* Penilaian dilaksanakan melalui proses wawancara, observasi, serta *kuesioner* terhadap pihak sekolah. Hasil akhir divisualisasikan dalam bentuk *dashboard* untuk menunjukkan tingkat kematangan pada lima area pokok, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset, serta Teknologi dan Keamanan Informasi. Visualisasi hasil tersebut dapat ditampilkan pada Gambar 5 berikut.



Gambar 5. Hasil Dashboard Indeks KAMI SMK Negeri 1 Nanggulan

Dashboard di atas menggambarkan capaian tingkat kematangan keamanan informasi pada SMK Negeri 1 Nanggulan yang berada dalam kisaran *Level I* hingga *Level II* dengan perolehan rata-rata keseluruhan 44,07%. Temuan ini menjelaskan bahwa sebagian besar kegiatan pengelolaan keamanan informasi telah berjalan namun masih berada pada tahap penerapan awal dan belum sepenuhnya

terdokumentasi selaras dengan standar *ISO/IEC 27001:2013.*

Adapun hasil tingkat kematangan untuk masing-masing area keamanan informasi dapat ditampilkan pada Tabel 4 berikut.

Tabel 5. Rekapitulasi penilaian per area Indeks KAMI

Area	Skor	Tingkat Kematangan
Tata Kelola	62	I+ (Penerapan Awal)
Pengelolaan Risiko	36	I+ (Penerapan Awal)
Kerangka Kerja Keamanan Informasi	44	I (Dasar)
Pengelolaan Aset	71	II (Cukup Terstruktur)
Teknologi dan Keamanan Informasi	107	II (Cukup Terstruktur)

Berdasarkan data tersebut, dapat dilihat bahwa dua bagian dengan skor tertinggi adalah Pengelolaan Aset dan Teknologi serta Keamanan Informasi, yang mengindikasikan bahwa penerapan kontrol teknis sudah cukup baik. Sementara itu, nilai terendah terdapat pada Kerangka Kerja Keamanan Informasi, yang menandakan bahwa aspek kebijakan dan dokumentasi keamanan informasi masih perlu diperkuat.

Secara keseluruhan, tingkat kematangan keamanan informasi di SMK Negeri 1 Nanggulan termasuk pada *Tingkat II (Penerapan Kerangka Kerja Dasar).* Kondisi ini berarti organisasi telah memiliki dasar keamanan informasi namun perlu meningkatkan konsistensi, dokumentasi, dan pengukuran kinerja agar dapat mencapai *Tingkat III+ (Terdefinisi dan Konsisten)* sesuai standar *ISO/IEC 27001:2013.*

4.4. Rekomendasi peningkatan pada 5 Area Keamanan Informasi

Sesudah dilakukan proses penilaian menggunakan *Indeks KAMI* versi 3.1 dan diketahui tingkat kematangan di tiap area, maka dilakukan penyusunan saran perbaikan yang difokuskan pada dua area dengan nilai terendah, yaitu Tata Kelola Keamanan Informasi dan Kerangka Kerja Keamanan Informasi. Kedua bagian ini memerlukan peningkatan karena masih berada pada tingkat kematangan *I* dan *I+*. Rincian saran perbaikan yang disusun berdasarkan standar *ISO/IEC 27001:2013* ditampilkan pada Tabel berikut.

Tabel 6. Saran dan Pebaikan

Area	Pertanyaan	Status
Tata Kelola Keamanan Informasi	Apakah sekolah memiliki kebijakan keamanan informasi yang terdokumentasi dan disosialisasikan kepada seluruh guru serta staf administrasi?	Tidak dilaksanakan
Saran Perbaikan: Control A.5.1 – Information Security Policies Sekolah perlu menyusun *Information Security Policy* yang disahkan oleh kepala sekolah dan mengatur aspek perencanaan, penggunaan, penyimpanan, dan perlindungan data sekolah. Dokumen ini perlu disosialisasikan kepada guru dan staf agar seluruh pengguna mengetahui aturan dan batasan dalam mengakses serta mengelola informasi sekolah.		
Kerangka Kerja Keamanan Informasi	Apakah sekolah telah menetapkan struktur organisasi yang menangani dan bertanggung jawab dalam pengelolaan keamanan informasi?	Tidak dilaksanakan
Saran Perbaikan: Control A.6.1.2 – Segregation of Duties Sekolah perlu menetapkan pemisahan tugas antara admin IT, guru operator, dan pihak manajemen untuk mengurangi risiko kesalahan, penyalahgunaan akses, serta konflik kepentingan. Selain itu, perlu dibentuk penanggung jawab keamanan informasi yang mengatur pengelolaan data dan penggunaan sistem secara lebih terkontrol.		

5. KESIMPULAN DAN SARAN

Berdasarkan temuan penelitian yang dilakukan di SMK Negeri 1 Nanggulan menggunakan *Indeks Keamanan Informasi (KAMI)* versi 3.1, dapat disimpulkan bahwa tingkat kematangan pengelolaan keamanan informasi sekolah masih berada pada tahap awal penerapan, dengan total nilai 320 dari 720 atau sekitar 44,07 persen yang menempatkan sekolah pada *level III (standar dasar penerapan).* Hasil ini menunjukkan bahwa *sistem elektronik* di sekolah sudah menjadi bagian penting dalam kegiatan akademik dan administrasi, namun tata kelola serta manajemen risiko keamanan informasi masih perlu diperkuat agar sejalan dengan standar *ISO/IEC 27001:2013*. Area yang capaian tertinggi terdapat pada Teknologi dan Keamanan Informasi, sementara area dengan capaian terendah adalah Kerangka Kerja Keamanan Informasi yang menandakan perlunya pembenahan kebijakan, *SOP*, dan struktur tanggung jawab keamanan. Untuk penelitian selanjutnya, disarankan dilakukan evaluasi lanjutan dengan melibatkan lebih banyak responden dari berbagai unit kerja, serta memperluas kajian terhadap efektivitas implementasi kontrol keamanan informasi agar dapat memberikan gambaran lebih komprehensif tentang kesiapan sekolah dalam mencapai tingkat kematangan keamanan yang lebih tinggi

.

DAFTAR PUSTAKA

[1] M. Anggraeni, "Audit Keamanan Informasi Menggunakan Indeks KAMI dan IT Governance," Jurnal IT Governance dan Sistem Informasi, vol. 6, no. 2, pp. 90–100, 2024.

[2] R. F. Fikri, "Implementasi Teknologi Proteksi Data dan Indeks KAMI di SMK Negeri," Jurnal Informatika Edukasi, vol. 4, no. 1, pp. 19–26, 2023.

[3] L. Fitriana, "Tingkat Kematangan Keamanan Informasi di SMA Negeri Menggunakan Indeks KAMI," Jurnal Teknologi dan Informasi Pendidikan, vol. 8, no. 1, pp. 14–23, 2022.

[4] M. H. Z. Hidayatullah, W. Y. Sulistyo, and S. A. Pratiwi, "Evaluasi Tingkat Keamanan Informasi SIA UIN SUKA Berdasarkan Indeks KAMI (Information Security) 4.0," JITU: Journal Informatic Technology and Communication, vol. 9, no. 1, pp. 83–91, May 2025.

[5] D. I. Khamil, G. M. A. Sasmita, and A. A. N. H. Susila, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.2 dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)," Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 3, pp. 1948–1960, Sep. 2022.

[6] N. Kusuma and Z. Latifah, "Analisis Kesiapan Sekolah Digital Menggunakan Model KAMI dan ISO 27001," Jurnal Ilmiah Rekayasa dan Sistem Informasi, vol. 10, no. 2, pp. 55–64, 2024.

[7] A. H. Nadanta, H. Farisi, and D. W. Brata, "Analisis Evaluasi Indeks KAMI (Keamanan Informasi) 5.0 dalam Pengelolaan Keamanan Informasi di SMK Telkom Purwokerto," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 9, no. 8, Aug. 2025.

[8] F. A. S. Ningrum, Y. Riwanto, I. Y. R. Pratiwi, and M. A. Fikri, "Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI," JIP (Jurnal Informatika Polinema), vol. 10, no. 3, pp. 437–442, May 2024.

[9] S. Paramita, S. A. Siregar, R. A. Damanik, and M. D. Irawan, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013," Bulletin of Information Technology (BIT), vol. 3, no. 4, pp. 374–379, Dec. 2022.

[10] D. Putra and R. Nasution, "Integrasi ISO/IEC 27001 dengan Indeks KAMI untuk Evaluasi Sistem Informasi Pemerintahan," Jurnal Sistem Informasi dan Teknologi, vol. 10, no. 3, pp. 102–111, 2022.

[11] A. Ramdani and N. Septiani, "Pemanfaatan Indeks KAMI untuk Evaluasi Infrastruktur TI pada Sekolah," Jurnal Sistem dan Teknologi Informasi, vol. 8, no. 1, pp. 39–46, 2023.

[12] D. Salsabila and Y. Karim, "Evaluasi Keamanan Informasi SMK XYZ Menggunakan Indeks KAMI dan ISO/IEC 27001:2013," Jurnal Cyber Security dan Forensik Digital, vol. 7, no. 1, pp. 43–49, May 2024.

[13] I. Sukmawati and D. Wibowo, "Evaluasi Keamanan Informasi Menggunakan Indeks KAMI di Dinas Pendidikan Kota Semarang," Jurnal Teknologi Informasi dan Komputer, 2025.

[14] T. Wulandari and Y. Rakhman, "Indeks KAMI sebagai Alat Audit Keamanan Informasi Pendidikan Menengah," Jurnal Ilmu Komputer dan Informatika, vol. 7, no. 3, pp. 101–110, 2022.