E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 9 No 6 Tahun 2025

IMPLEMENTASI INDEKS KAMI DI SMKN 2 BANDAR LAMPUNG

Teguh Sugiarto[1], R.Z. Abdul Aziz[2], Muhammad Said Hasibuan[3]

IIB Darmajaya Lampung
Teguh2421211027P@mail.darmajaya.ac.id, rz_aziz@darmajaya.ac.id, msaid@darmajaya.ac.id

ABSTRACT

Information stands as a pivotal strategic asset for all organizations, educational institutions included, making it a frequent objective of cyberattacks and exploitation. To secure these assets, information systems must guarantee the trhee foundational principt of information security: confidentiality, and availability. SMKN 2 Bandar Lampung, a vocational secondary school, relies on multiple work units for managing and conveying information, thus an evaluation of its information system security is imperative. This studing aim to gauge the readiness and maturity of inforrnation securities within SMKN 2 Bandar Lampung utilizing the Information Security Index (Indeks KAMI). This assessment tool, developed by Indonesia's Directorate of Inforrnation Security , Ministries of Comunication and Informatïon Technology, examines five key areas: governance, risk management, the security framework, aset management, and technology and procedures. The results demonstrate that SMKN 2 Bandar Lampung's information security maturity is currently low, despite a pronounced dependence on Information and Communication Technology (ICT) for its operational and service delivery processes. This situation reveals a significant discrepancy between the necessity for a robust information system and the existing, inadequate information security practices. Consequently, this research provides several recommendations intended to assist the institution in improving the worthy of its information security management system moving forward.

Keywords: *Information Security, KAMI Index, SMKN 2 Bandar Lampung, Information System, Information and Communication Technology, Security Maturity*

ABSTRAK

Informasi adalah aset krusial bernilai strategis bagi setiap entitas, tak terkecuali institusi pendidikan, yang menjadikannya target utama eksploitasi via serangan siber. Untuk mengamankannya, sistem informasi wajib menjamin tiga pilar fundamental: kerahasiaan, integritas, dan ketersediaan. SMKN 2 Bandar Lampung, sebagai lembaga pendidikan vokasi, memiliki beragam unit kerja yang bertanggung jawab atas pengelolaan serta penyampaian informasi, sehingga evaluasi terhadap keamanan sistem informasinya menjadi krusial. Penelitiaan dikhususkan untuk menilai tingkat kesiapsiagaan dan kedewasaan keamanan Informasi di lingkungan SMKN 2 Bandar Lampung. Penilaian dilakukan menggunakan Indeks Keamanan Informasi, sebuah instrumen yang dikembangkan Direktorat Keamanan Informasi, Kementrian Komunikasi dan Inforrnatika RI, dengan fokus pada lima perspektif: “tata kelola, manajemen risiko, kerangka kerja keamanan, manajemen aset, serta teknologi dan prosedur”. Hasil studi menunjukkan tingkat kematangan keamanan informasi di SMKN 2 Bandar Lampung yang masih rendah, meskipun ketergantungan pada Teknologi Informasi dan

Article History
Received: Juli 2025
Reviewed: Juli 2025
Published: Juli 2025

Plagiarism Checker No 235
Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

Kornunikasi (TIK) untuk operasïonal dan bantuan sangat tinggi. Temuan ini menyoroti adanya kesenjangan signifikan antara kebutuhan akan sistem informasi yang andal dengan implementasi praktik keamanan yang belum memadai. Lebih lanjut, penelitian ini menawarkan sejumlah rekomendasi perbaikan sebagai acuan bagi sekolah guna meningkatkan efektivitas sistem manajemen keamanan informasinya di masa depan.

Kata Kunci: Keamanan Informasi, Indeks KAMI, SMKN 2 Bandar Lampung, Sistem Informasi, Teknologi Informasi dan Komunikasi, Kematangan Keamanan

PENDAHULUAN

Bagi setiap entitas, termasuk lembaga pendidikan, informasi memegang peranan sebagai aset strategis yang sangat vital. Ketersediaan data yang akurat, kredibel, dan aman menjadi landasan esensial dalam mendukung pengambilan keputusan, kelancaran operasional sehari-hari, hingga formulasi rencana jangka panjang. Akan tetapi, pesatnya kemajuan teknologi informasi dan komunikasi turut menjadikan informasi sebagai objek incaran utama dalam serangan siber, yang bertujuan untuk dieksploitasi oleh pihak-pihak tidak bertanggung jawab [1].

Laporan Keamanan Siber Indonesia yang dirilis oleh ID-SIRTII mengindikasikan bahwa total serangan siber di Indonesia “pada tahun 2016 mencapai 136.672.948, sebuah lonjakan lebih dari 50% dibandingkan tahun 2015” yang mencatatkan 89.691.783 serangan. Serangan jenis Distributed Denial of Service (DDoS) mendominasi, dengan puncaknya terjadi waktu itu tahun 2016 sebanyak 46,338,965 serangan dasyat. Lebih lanjut, domain pemerintah berakhiran situs.go.id menjadikan target utama phishing, dengan kontribusi sekitar 17,73% dari total hos phishing, disusul oleh domain .id sebesar 13,64% [2]. Ragam serangan dan insiden ini menegaskan bahwa ruang siber (cyberspace) telah bertransformasi menjadi arena utama bagi pelaksanaan aksi-aksi yang mengancam keamanan informasi.

Menyadari urgensi proteksi informasi, setiap organisasi dituntut untuk mengimplementasikan kebijakan serta sistem yang mumpuni guna memelihara kerahasiaan, integritas, dan ketersediaan informasi. Salah satu pendekatan kebijakan yang relevan adalah adopsi Sistem Manajemen Keamanan Informasi (SMKI). Sistem tersebut dirancang untuk memastikan bahwa risiko terhadap informasi dapat terkelola secara efektif melalui serangkaian kebijakan, prosedur, dan kontrol yang presisi. Meskipun demikian, realitasnya menunjukkan bahwa belum ada, dan kemungkinan tidak akan pernah ada, sistem keamanan informasi yang sempurna, yang mampu memberikan perlindungan 100% terhadap segala bentuk ancaman [3]. Oleh sebab itu, pelaksanaan evaluasi secara periodik menjadi elemen krusial dalam upaya pemeliharaan dan peningkatan sistem keamanan informasi.

SMKN 2 Bandar Lampung, sebagai institusi pendidikan menengah kejuruan, menyelenggarakan berbagai kegiatan dan memanfaatkan sistem informasi untuk mendukung proses belajar-mengajar serta manajemen sekolah. Hingga kini, institusi tersebut belum mengadopsi standar sistem informasi yang terpadu dan terukur. Dengan demikian, sebelum melangkah ke penerapan standarisasi, menjadi penting untuk terlebih dahulu melakukan evaluasi terhadap kondisi keamanan informasi yang berada pada setiap zona di kawasan sekolah.

Tujuan dari evaluasi ini adalah untuk mendapatkan gambaran komprehensif mengenai tingkat kesiapsiagaan serta tindaklanjut dari keamanan informasi di lingkungan SMKN 2 Bandar Lampung. Salah satu instrumen yang dapat dimanfaatkan untuk evaluasi ini adalah Keamanan Informasi (Indeks KAMI), sebuah pengukuran yang dirancang oleh sekelompok tim Direktorat Keamanan Informasi, dari Kementerian Komunikasi Informatika. Instrumen ini berfungsi untuk menilai dan mengeavaluasi sejauh mana kesiapan dengan kata lain tindakan pengamanan

informasi dalam sebuah instansi, meliputi aspek kebijakan, tata kelola, manajemen risiko, hingga pengelolaan aset informasi [4].

Melalui pengukuran menggunakan Indeks KAMI, diharapkan akan teridentifikasi posisi atau tingkatan kematangan keamanan informasi di SMKN 2 Bandar Lampung. Hasil pengukuran ini selanjutnya akan dianalisis secara mendalam dan dijadikan landasan dalam penyusunan strategi peningkatan keamanan informasi di lingkungan sekolah. Dengan pendekatan ini, sekolah dapat mengambil langkah-langkah yang lebih terfokus dan efektif guna membangun sistem keamanan informasi yang lebih unggul di waktu mendatang.

METODE PENELITIAN

Semua Bagian ini menguraikan alur serta tahapan yang sistematis dalam pelaksanaan studi, dimulai dari fase persiapan hingga tahap penyusunan laporan akhir. Metodologi yang dipaparkan meliputi bahan atau materi yang digunakan, instrumen penelitian, serta serangkaian langkah yang dirancang secara logis. Tujuannya adalah untuk menjadi panduan dalam mengatasi permasalahan yang dikaji, melakukan analisis terhadap temuan, dan mengidentifikasi berbagai kendala yang mungkin muncul selama proses penelitian.

Tabel 1. Alur Penelitian

Tahapan	Kegiatan	Output
Persiapan	- Telaah dokumen seperti Renstra TIK dan hasil audit sistem informasi - Studi literatur terhadap teori dan penelitian terdahulu terkait Indeks KAMI	Identifikasi permasalahan TIK di instansi terkait
Desain Penelitian	- Identifikasi organisasi: visi-misi, distruktur organisasi, plan strategi TIK - Perumusan kuisïoner dan batasan masalah - Penyusunan kerangka kerja evaluasi menggunakan Indeks KAMI	Kuisioner, panduan wawancara, batasan masalah
Pengumpulan dan Analisis Data	- Menentukan populasi dan sampel - Melakukan pengisian kuisioner dan wawancara - Analisis data untuk menilai tingkat lanjuit keamanan Informasi	Nilai tingkat lanjutt dan rekomendasi peningkatan keamanan Informasi
Penyusunan Laporan	- Merangkum hasil analisis - Menyusun kesimpulan dan saran - Menyusun laporan akhir dan presentasi	Laporan penelitian, kesimpulan, saran dan rekomendasi

Bagian ini memaparkan alur penelitian secara detail, meliputi bahan atau materi, instrumen yang digunakan, serta serangkaian tahapan penelitian yang tersusun secara terstruktur dan logits. Tujuan penyusunan ini adalah untuk menyediakan kerangka acuan yang mudah dan jelas serta diikuti dalam niat menyelesaikan permasalahan, menganalisis temuan, serta mengidentifikasi potensi kendala selama proses penelitian. Rangkaian langkah penelitian ini disajikan dalam Tabel 1 (dalam dokumen asli).

- *Tahap Persiapan:*

Pada tahap pertama ini, peneliti melakkukan kajian mendalam terhadap dokumen internal institusi dan literatur yang relevan. Ini mencakup analisis dokumen seperti Rencana Strategis TIK SMKN 2 Bandar Lampung dan laporan audit sistem informasi sekolah. Selain itu, dilakukan penelusuran terhadap landasan teoretis dan temuan dari studi-studi sebelumnya, terutama yang memanfaatkan Indeks KAMI versi terdahulu atau model evaluasi sejenis. Teori-teori yang relevan kemudian diringkas sesuai dengan kebutuhan penelitian. Luaran dari fase

ini adalah teridentifikasinya permasalahan terkait Teknologi Informasi dan Komunikasi (TIK) di SMKN 2 Bandar Lampung.

- *Tahap Desain Penelitian:*

Dalam tahap ini, peneliti mengidentifikasi karakteristik organisasi dan merancang pelaksanaan penilaian menggunakan Indeks KAMI. Mencirikan lembaga meliputi pemahaman visi-misi, struktur lembaga, rencana strategi TIK SMKN 2 Bandar Lampung, serta laporan audit sebelumnya. Indeks KAMI digunakan sebagai instrumen evaluasi untuk menilai implementasi tata kelola keamanan informasi secara berkesinambungan. Jika terjadi perubahan pada pembangunan atau unit sejak evaluasi terakhir, dilakukan dikaji lagi untuk memastikan kematangan dan kelengkapan tata kelola yang ada. Hasil dari tahap ini berupa penyusunan kuesioner, pengembangan panduan wawancara, dan penetapan ruang lingkup masalah guna memastikan fokus pembahasan.

- *Tahap Pengumpulan dan Analisis Data:*

Pada fase ini, peneliti menetapkan sampel, populasi dan metode analis data yang akan digunakan. Populasi penelitian mencakup sebagian pengelola dan user layanan TIK di SMKN 2 Bandar Lampung, yang terdiri atas staff, guru dan siswa, dengan total populasi 2215 individu berdasarkan rata-rata pengguna layanan TIK sekolah. Untuk pengambilan data yang akan digunakan adalah sampling asidental, dimana sampel di pilih berdasarkan ketersediaan informan saat penelitian dilakukan. Jumlah sampel yang terlibat dalam penelitian ini adalah 18 informan. Luaran dari fase ini adalah perolehan nilai tingkat kewajaran keamanan informasi dan rumusan rekomen untuk meningkatkan lengkap atau tidaknya serta efektivitas sistem tersebut.

- *Tahap Penyusunan Laporan:*

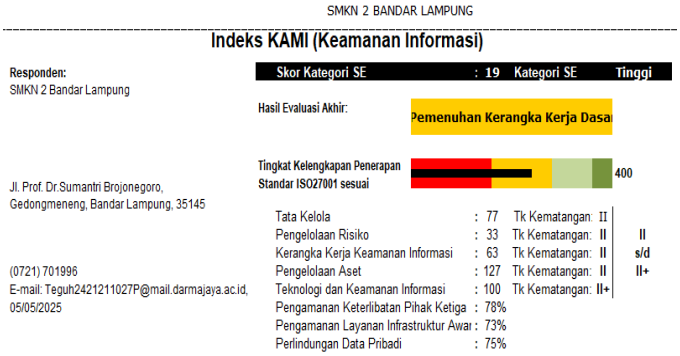
Tahap final ini adalah penyusunan laporan penelitian yang komprehensif. Laporan ini akan memuat saran, rekomendasi, serta tinjauan literatur yang mendukung temuan. Hasil dari fase ini berupa dokumen laporan akhir penelitian, simpulan, saran perbaikan, dan materi presentasi hasil dari penelitian.

HASIL DAN PEMBAHASAN

Implementasi penilaian menggunakan Indeks KAMI di SMKN 2 Bandar Lampung dilakukan dengan memakai Indeks KAMI rilis 4.2. Instrumen evaluasi ini terdiri atas total 131 (seratus tigapuluh satu) pertanyaan yang dikelompokkan ke dalam enam bagian. Pada Bagian satu, informan diminta untuk indefinisikan aspek Tata Kelola Keamanan Informasi diunit kerja masing - masing. lainnya itu, informan juga di minta untuk memberikan deskripsi mengenai Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Informasi Pengelolaan Keamanan, Pengelolaan Informasi Aset, Informasi Teknologi dan Keamanan, Pengamanan Pihak Luar, Pengamanan Infra-struktur, serta Perlindungan Data-data Pribadi melalui serangkaian pertanyaan yang berkaitan dengan Tingkat lanjutan dari informasi keamanan. Rekapitulasi dan pengolahan data obserrvasi dapat dicermati pada Tabel 2.

Tabel 2. Skor Area Evaluasi SMKN 2 B Lampung

AREA	SKOR
Tata Kelola Keamanan Informasi	77
Pengelolaan Resiko Keamanan Informasi	33
Kerangka Kerja Pengelolaan Keamanan Informasi	63
Pengelolaan Aset Informasi	127
Teknologi dan Keamanan Informasi	100
Pengamanan Pihak Ketiga	78%
Pengamanan Infrastruktur	73%
Perlindungan Data Pribadi	75%


SMKN 2 BANDAR LAMPUNG

Indeks KAMI (Keamanan Informasi)

Responden:
SMKN 2 Bandar Lampung

Skor Kategori SE : 19 Kategori SE Tinggi

Hasil Evaluasi Akhir: Pemenuhan Kerangka Kerja Dasa

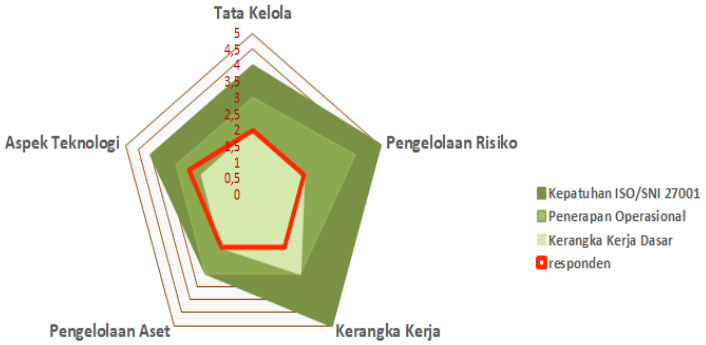
Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai 400

Jl. Prof. Dr.Sumantri Brojonegoro, Gedongmeneng, Bandar Lampung, 35145

(0721) 701996
E-mail: Teguh2421211027P@mail.darmajaya.ac.id,
05/05/2025

Tata Kelola	: 77	Tk Kematangan: II	II
Pengelolaan Risiko	: 33	Tk Kematangan: II	s/d
Kerangka Kerja Keamanan Informasi	: 63	Tk Kematangan: II	II+
Pengelolaan Aset	: 127	Tk Kematangan: II	
Teknologi dan Keamanan Informasi	: 100	Tk Kematangan: II+	
Pengamanan Keterlibatan Pihak Ketiga	: 78%		
Pengamanan Layanan Infrastruktur Awan	: 73%		
Perlindungan Data Pribadi	: 75%		

Gambar 2. Hasil Evaluasi Keamanan SMKN 2 B Lampung



Gambar 3. Diagram Radar Hasil Penilaian SMKI

Berdasarkan petunjuk yang disajikan pada Gambar 2 (dalam dokumen asli), dapat ditafsirkan bahwa meskipun dari perspektif tingkat kelengkapan penerapan Sistem Informasi Manajemen Keamanan (SMKI), SMKN 2 Bandar Lampung ada pada level "Pemenuhan Kerangka Kerja Dasar", terdapat area yang di indikasikan sebagai "Merah" dengan skor total 400. Skor ini adalah akumulasi dari seluruh poin rata - rata pada setiap zona Informasi Keamanan yang di evaluasi.

Tingkat lengkap atau tidaknya implementasi SMKI dapat juga diamati melalui Gambar 3. (dalam dokumen asli). Diagram dengna warna merah muda pada gambar tersebut merepresentasikan kondisi SMKI di SMKN 2 Bandar Lampung, berdasarkan pengisian hasil kuesioner dari para informan. Diagram tersebut, dapat dicermati beberapa poin:

- Dari kelima area utama informasi keamanan yang diobservasi, bahwa tampak SMKN 2 Bandar Lampung menunjukkan kondisi yang lebih baik pada Aspek Teknologi dan Tata Kelola dibandingkan lingkungan keamanan lainnya (sangat mendekati standar yang ditetapkan dalam Penerapan Proses).
- Pada Area Pengelolaan Aset dan Pengelolaan Risiko, terlihat bahwa SMKN 2 Bandar Lampung belum mencapai standar susunain kerja-dasar. Hal ini mengindikasikan perlunya perbaikan untuk meningkatkan informasi pengamanan di area tersebut.
- Demikian pula pada zona Susuan Kerja, capaiannya belum memenuhi Kerangka Kerja Dasar, yang menandakan bahwa SMKN 2 Bandar Lampung sangat memerlukan perbaikan guna meningkatkan pengamanan informasi di area ini.

Secara keseluruhan, tingkat kelengkapan SMKI di SMKN 2 Bandar Lampung, berdasarkan data yang terkumpul melalui Indeks KAMI dan divisualisasikan pada area merah dalam diagram batang pada Gambar 2, mengisyaratkan bahwa SMKI yang ada saat ini perlunya perbaikan pada berbagai ruang lingkupnya.

Utama perbaikan untuk aspek - aspek tersebut, dengan mengacu pada radar info diagram pada gambar 3, dan persent capaian skor informan ditabel 2, adalah sebagai berikut

(diurutkan berdasarkan prioritas): Susunan Kerja Pengelolaan Informasi Keamanan, Tata Kelola Keamanan Informasi, Pengelolaan Aset Informasi, Aspek Teknologi Informasi Keamanan, dan Pengelolaan Risiko Informasi Keamanan.

Area Susunan Kerja Informasi Keamanan mencatatkan poin sebesar 63, yang mengindikasikan tingkat keamanan pada level II. Dari pertanyaan yang berjumlah 29 butir yang diajukan dalam lingkup ini, distribusi respons adalah sebagai berikut:

- Tidak ada (0) pertanyaan yang direspons dengan "Tidak Dilakukan".
- Sebanyak 6 pertanyaan (sekitar 20,69%) direspons dengan "Dalam Perencanaan".
- Sebanyak 20 pertanyaan (sekitar 68,97%) direspons dengan "Dalam penerapan/Diterapkan Sebagian".
- Sisanya, 3 pertanyaan (sekitar 10,34%) direspons dengan " Diterapkan Secara Menyeluruh ".

Untuk menunjang peningkakan lingkup kelengkapan implementasi SMKI dalam domain ini, SMKN 2 Bandar Lampung disarankan untuk melakukan beberapa perbaikan, antara lain:

1) Formalisasi Kebijakan dan Prosedur: Menyusun dan mendokumentasikan kebijakan serta prosedur keamanan informasi secara jelas dan tertulis, dengan cara mencatat peran dan tanggungjawab pihak-pihak yang diberi kewewenangan untuk implementasinya.
2) Publikasi dan Aksesibilitas Kebijakan: Menetapkan kebijakan informasi keamanan sesuai kewajara, mempublikasikannya pada seluruh pihak yang ada dalam lingkup ini, dan memastikan kemudahan akses bagi pihak-pihak yang memerlukannya.
3) Manajemen Dokumen Kebijakan: Mengimplementasikan proses evaluasi untuk pengelolaan berkas prosedur dan kebijakan informasi keamanan, tercantum juga penggunaan daftar buku induk, pengaturan distribusi, mekanisme penarikan dari per-edaran, dan metode penyimpanannya.
4) Komunikasi Kebijakan: Menyediakan alur dalam menghubungkan kebijakan informasi keamanan (beserta data ubahnya) pada seluruh pihak yang relevan.
5) Refleksi Kebutuhan Mitigasi Risiko: Memastikan bahwa kebijakan dan prosedur informasi keamanan yang ada telah mencerminkan kebutuhan menjadi berkurang makna yang di identifikasi dari kajian risiko informasi keamanan.
6) Prosedur Penanganan Insiden dan Aset: Mencantumkan prosedur untuk pelaporan makna kejadian, penjagaan rahasiaa, hak kekayaan intelectual (HAKI), tatatertib penggunaan, dan pengamanan substansi.
7) Konsekuensi Pelanggaran Kebijakan: Menetapkan konsekuensi yang jelas atas pelanggaran kebijakan informasi keamanan yang telah di artikan, dibicarkan, dan dilaksanakan tegas.
8) Prosedur Pengecualian: Membuat prosedur secara resmi untuk mengolah setiap pengecualian pada penerapan kebijakan informasi keamanan.

Domain Pengelolaan Risiko Keamanan Informasi memperoleh skor 33. Dari pertanyaan berjumlah 16 butir yang dipaparkan untuk lingkungan ini, distribusi responsnya adalah sebagai berikut:

- Tidak ada (0) pertanyaan yang dijawab dengan "Tidak Dilakukan".
- Sebanyak 2 pertanyaan (12,5%) dijawab dengan "Dalam Perencanaan".
- Sebanyak 13 pertanyaan (81,25%) dijawab "Dalam penerapan / Diterapkan Sebagian".
- Satu pertanyaan sisanya (6,25%) dijawab "Diterapkan Secara Menyeluruh".

Guna meningkatkan tingkatan kelengkapan implementasi SMKI pada domain ini, SMKN 2 Bandar Lampung disarankan untuk mengambil langkah-langkah perbaikan berikut:

1) Formalisasi Kerangka Kerja Pengelolaan Risiko: Membuat kerangka kerja pengolah risiko informasi keamanan yang terdokumentasi secara baik dan digunakan sesuai harapan proses.
2) Definisi dan Hubungan dalam Kerangka Risiko: Memastikan kerangka kerja pengelolaan risiko ini mencakup tafsiran dan keterkaitan antara tingkat pembeda aset informasi, level warning, probabilitas terjadinya ancaman, serta dampak kerugian yang mungkin timbul bagi instansi.

3) Penetapan Ambang Batas Risiko: Menetapkan batasan bawah tingkat risiko yang di terima oleh institusi.
4) Identifikasi Kepemilikan dan Pengelola Aset: mentafsirkan pemimilikan dan pihak pengelola (cusstodian) untuk setiap aset informasi yang ada, termasuk aset utama dan proses kerja utama yang memanfaatkan alat ini tersebut.
5) Analisa Risiko integral: Menjalankan inisiatif analisa mengukur risiko informasi keamanan secara integral terhadap alat-alat informasi miliknya (dasar untuk identifikasi sebuah langkah mitigasi atau penanggulangan yang menjadi salah satu bagian dari si aplikasi pengelolaan informasi keamanan).
6) Pemantauan Status Risiko Mitigasi: Memantau status selesai adalah langkah mitigasi risiko secara berkesinambungan agar dipastikan progres atau penyelesaiannya.
7) Efektivitas Pengukur Mitigasi: Melakukan evaluasi/mengukur terhadap selesainya langkah mitigasi yang sudah diterapkan agar dipastikan konsisten dan efektif.
8) Evaluasi Profil Risiko Berkala Berkesinambugan: Mengkaji profil risiko dan bentuk mitigasi secara periodik untuk akut valid. Ini termasuk revisi atas profil risiko bila terdapat perubahan situasi dan kondisi yang tiba-tiba atau kebutuhan untuk menerapkan bentuk pengaman.
9) Evaluasi Risiko pada Sistem Baru: Menerapkan proses untuk mengukur risiko dalam perencanaan pembelian (implementasi) sistematis yang baru dan menanggulangi masalah yang mungkin ada.
10) Kerangka Kerja Rencana Progress Layanan TIK: diterapkannya susunan kerja pengelolaan rencana terapan layanan TIK (planning continuity) yang didefinisi persyaratan informasi keamanan, termasuk jadwal uji atau simulasinya.

Area Tata Kelola Informasi Keamanan mendapatkan skor 77. Dari pertanyaan sejumlah 22 butir yang lontarkan untuk domain ini, pola responsnya adalah sebagai berikut:

- Tidak ada (0) pertanyaan yang dijawab dengan "Tidak Dilakukan".
- Sebanyak 5 pertanyaan (sekitar 22,73%) dijawab dengan "Dalam Perencanaan".
- Sebanyak 13 pertanyaan (sekitar 59,09%) dijawab dengan "Dalam penerapan/Diterapkan Sebagian".
- Sisa 4 pertanyaan (sekitar 18,18%) dijawab dengan "Diterapkan Secara Menyeluruh".

Agar level kelengkapan implementasi SMKI dalam zona ini, SMKN 2 Bandar Lampung direkomendasikan untuk melakukan perbaikan-perbaikan berikut:

1) Definisi Standar Kompetensi dan Keahlian: Mendefinisikan secara jelas standar kompetensi serta keahliaan yang dibutuhkan oleh para pelaksana pengelolaan informasi keamanan.
2) Aplikasi Peningkatan Kompetensï: Menerapkan program berkelanjutan untuk peningkatan kompetensi dan keahlian bagi para pengurus secara struktur serta staff pelaksana pengelolaan informasi keamanan.
3) Koordinasi Proaktif Kepatuhan Pengamanan: Memastikan bahwa pengolah informasi keamanan secara proaktif menerapkan dan menjamin kepatuhan terhadap pengamanan ïnformasi melalui koordinasi dengan unit kerja terkait (seperti SDM, Legal/Hukum, Umum, Keuangan, dsb) serta pihak eksternal yang memiliki kepentingan (misalnya, satuan keamanan).
4) Definisi dan Alokasi Tanggung Jawab Keberlangsungan Layanan: Mendefinisikan dan mengalokasikan tanggung jawab secara jelas untuk proses pengambilan keputusan, perancangan, pelaksanaan, dan pengelolaan langkah-langkah keberlangsungan pelayan TIK (mencakup continuity business dan disaster plans recovery).

Domain Pengelolaan Perangkat Informasi Keamanan memperoleh skor 127. Dari pertanyaan 38 butir yang disajikan untuk zona ini, distribusi responsnya adalah sebagai berikut:

- Tidak ada (0) pertanyaan yang dijawab dengan "Tidak Dilakukan".
- Sebanyak 3 pertanyaan (sekitar 7,89%) dijawab dengan "Dalam Perencanaan".

- Sebanyak 20 pertanyaan (sekitar 52,63%) dijawab dengan "Dalam penerapan/Diterapkan Sebagian".
- Sisanya, 15 pertanyaan (sekitar 39,47%) dijawab dengan "'Diterapkan Secara Menyeluruh".

Untuk meningkatkan tingkat kelengkapan implementasi SMKI pada domain ini, SMKN 2 Bandar Lampung disarankan untuk mengambil langkah-langkah perbaikan berikut:

Pelaporan diproses Insiden kepada Pihak Berwajib: Membuat proses formal untuk pelaporan kejadian-kejadian informasi keamanan ke pihak yang berwenang.

1) Pengelompokkan dan Evaluasi Perangkat Berdasarkan Kepentingan: Mengelompokkan dan Mengevaluasi perangkat informasi dengan sesuai dengan tingkat kepentingan aset tersebut bagi instansi serta kebutuhan pengamanannya.
2) Penyediaan Tingkatan Aksess dan Matriks Alokasi: Menyediakan tingkatan akses yang berbeda-beda dan membuat matriks yang mencatat alokasi akses untuk setiap aset.
3) Pengelolaan Perubahan Sistem yang Konsisten: Menyediakan mekanisme pengolah rubahan terhadap sistem (perubahan konfigurasi di dalamnya) yang ditetapkan secara konsisten.
4) Pengelolaan dengan Konsisten terkait Konfigurasi: Menyediakan mekanisme pengolah konfigurasi yang ditetapkan dengan konsistensi tinggi.
5) Rilis berproses Perangkat Baru dan Pembaruan Inventaris: Membuat proses untuk merilis aset baru ke dalam lingkungan operasional dan simultan memutakhirkan inventaris perangkat informasi.
6) Definisi Tanggungjawab Pengamanan Individu: Mendefinisikan tanggungjawab informasi pengamanan secara individu untuk semua unit kerja.
7) Tata Tertib Pengamanan Aset dan Data Pribadi: Membuat tata tertib terkait pengamanan dan penggunaan aset instansi yang mencakup aspek HAKI (Hak atas Kekayaan Intelektual) dan peraturan pengamanan data pribadi.
8) Penetapan Waktu Penyimpanan dan Syarat Penghancuran Data: Menetapkan durasi waktu penyimpanan untuk setiap klasifikasi data yang ada serta syarat-syarat untuk penghancuran data.
9) Prosedur Penghancuran Data/Aset yang Tidak Diperlukan: Membuat prosedur formal untuk penghancuran data atau aset yang sudah tidak lagi diperlukan.
10) Prosedur Kajian Penggunaan Akses dan Pembenahan: Membuat prosedur untuk melakukan kajian penggunaan akses pengguna (user access review) dan langkah-langkah pembenahan apabila ditemukan ketidaksesuaian (non-conformity) dengan kebijakan yang berlaku.
11) Pengamanan Fasilitas Fisik Sesuai Klasifikasi Aset: Menerapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan atau klasifikasi aset informasi. Pengamanan ini harus berlapis dan mampu mencegah upaya akses oleh pihak yang tidak berwenang.
12) Proses Pengelolaan Alokasi Key Access Fisik dan Elektronik: Membuat proses untuk mengelola alokasi kunci masuk (baik fisik maupun elektronik) ke fasilitas fisik.
13) Rancang Ruang Penyimpanan yang Tahan Risiko Kebakaran: Menggunakan rancangan dan material yang mampu menanggulangi risiko kebakaran, serta dilengkapi dengan fasilitas pendukung (seperti deteksi kebakaran, alat pemadam api, dan kelembaban) yang sesuai untuk konstruksi ruang penyimpanan perangkat pengolah sangat penting.
14) Proses Inspeksian dan Perawatan Perangkat serta Fasilitas: Membuat proses untuk melakukan pemeriksaan (inspeksi) dan perawatan terhadap perangkat komputer, fasilitas pendukungnya, serta layak atau tidaknya keamanan lokasi kerja untuk penempatan perangkat informasi itu sangat penting.
15) Mekanisme Pengamanan Pengiriman Perangkat Informasi: Memberikan mekanisme pengamanan dalam proses pengiriman perangkat informasi (perangkat maupun dokumen) yang melibatkan pihak ketiga itu.

Area Teknologi Informasi Keamanan mencatatkan skor 100. Dari pertanyaan sebanyak 26 butir yang diajukan dalam domain ini, distribusi respons adalah sebagai berikut:

- Tidak ada (0) pertanyaan yang direspons dengan "Tidak Dilakukan".

- Tidak ada (0) pertanyaan yang direspons dengan "Dalam Perencanaan".
- Sebanyak 11 pertanyaan (sekitar 42,31%) direspons dengan "Dalam penerapan/Diterapkan Sebagian".
- Sisanya, 15 pertanyaan (sekitar 57,69%) direspons dengan "Diterapkan Secara Menyeluruh".

Demi meningkatkan tingkatan kelengkapan implementasian SMKI dalam lingkungan ini, SMKN 2 Bandar Lampung direkomendasikan untuk melakukan perbaikan-perbaikan berikut:

1) Implementasi Keamanan Berlapis (Defense in Depth) untuk Layanan TIK: Melindungi pelayan TIK (operasi komputer) yang terhubung ke jaringan dengan lebih dari satu lapisan pengamanan. SMKN 2 Bandar Lampung disarankan untuk mengadopsi pendekatan defense in depth, yaitu penggunaan beberapa lapisan keamanan secara bertingkat untuk meminimalkan risiko serangan baik dari luar maupun dalam. Langkah-langkah yang dapat diambil meliputi: penggunaan firewall eksternal dan internal, implementasi sistem deteksi dan pencegahan intrusi (IDS/IPS), segmentasi jaringan, pembatasan akses berdasarkan peran (role-based access control), dan otentikasi dua faktor (2FA) untuk login ke sistem-sistem penting.
2) Analisis Kepatuhan Konfigurasi Standar Secara Rutin: Menganalisis kepatuhan penerapan konfigurasi standar yang ada secara rutin. Perlu dilakukan audit berkala terhadap semua hardware dan software untuk memastikan bahwa konfigurasi sistem telah sesuai dengan praktik terbaik (best practice) dan standar keamanan (misalnya, CIS Benchmark). Langkah yang disarankan meliputi: menyusun dan menerapkan kebijakan baseline configuration, menggunakan alat bantu automated configuration assessment, menyusun laporan audit, dan melakukan tindak lanjut jika ditemukan deviasi.
3) Analisis Log Berkala untuk Audit dan Forensik: Menganalisa semua report secara kesinambungan untuk memastikan akurasi, validitas, dan kelengkapan isinya (demi kepentingan jejak auditnya dan forensik). Log dari server, firewall, dan endpoint harus dikumpulkan, disimpan, dan dianalisis secara terpusat untuk mendeteksi potensi insiden. Rekomendasi perbaikannya mencakup: menerapkan sistem SIEM (Security Information and Event Management), menentukan periode retensi untuk penyimpanan log, dan melakukan korelasi antar log dari berbagai sistem untuk mendeteksi anomali.
4) Penerapan Standar Enkripsi: Menerapkan standar dalam penggunaan enkripsi. Untuk melindungi data yang disimpan maupun yang dikirim, sekolah harus mengimplementasikan algoritma dan protokol enkripsi yang sesuai dengan standar industri (misalnya, AES-256, TLS 1.3). Peningkatannya dapat berupa: mengenkripsi seluruh data sensitif baik saat diam (at rest) maupun saat transit (in transit), mewajibkan penggunaan VPN saat melakukan akses jarak jauh ke sistem, dan memberikan pelatihan kepada staf terkait pentingnya penggunaan enkripsi.

Pengamanan Pengelolaan Kunci Enkripsi: Menerapkan pengamanan untuk mengelola kunci masuk ke dalam sistem (sertifikat elektronik didalamnya) yang digunakan, termasuk alur penggunaannya. Agar data tetap aman, tidak cukup hanya dengan enkripsi; pengelolaan kunci (key management) juga harus diperkuat. Langkah-langkah yang dapat diambil meliputi: menggunakan hardware security module (HSM) atau key management system (KMS), terutama untuk data kritikal, menerapkan kebijakan rotasi kunci secara berkala, dan membatasi akses terhadap kunci hanya kepada personel yang memiliki wewenang.

KESIMPULAN

Dari hasil penelitian yang sudah dilakukan di SMKN 2 Bandar Lampung guna mengukur Tingkat Informasi Keamanan dengan menggunakan Indeks Informasi Keamanan (KAMI) versi 4.2, dapat ditarik beberapa kesimpulan utama sebagai berikut:

1. Hasil evaluasi menggunakan Indeks KAMI menunjukkan bahwasanya tingkat kematangan keamanan informasi di SMKN 2 Bandar Lampung saat ini berada pada kategori "Diterapkan Secara Menyeluruh", dengan perolehan total skor keseluruhan sebesar 400 poin. Skor ini

mengindikasikan bahwa sistem manajemen keamanan informasi (SMKI) di lingkungan sekolah belum sepenuhnya dikembangkan dan diimplementasikan secara komprehensif. Di sisi lain, tingkat kepentingan TIK di SMKN 2 Bandar Lampung ini tergolong tinggi, dengan skor kepentingan tercatat sebesar 27. Adanya ketimpangan antara tingginya ketergantungan terhadap TIK dengan rendahnya tingkat penerapan keamanan informasi menyiratkan adanya risiko signifikan terhadap keberlangsungan layanan informasi serta potensi ancaman terhadap aspek kerahasiaan, integritas, dan ketersediaan data.

2. Penilaian melalui Indeks KAMI, yang mencakup lima area utama yang disederhanakan dari standar ISO/IEC 27001:2009, mengungkapkan bahwa hanya dua area yang menunjukkan performa relatif baik, yaitu: Teknologi dan Informasi Keamanan dengan skor 100 poin, serta Tata Kelola Informasi Keamanan dengan skor 77 poin. Sebaliknya, tiga area lainnya masih menunjukkan tingkat kematangan yang rendah. Area-area tersebut adalah Pengelolaan Risiko Informasi Keamanan (skor 33 poin), Kerangka Kerja Informasi Keamanan (skor 63 poin), dan Pengelolaan Aset Informasi (skor 127 poin). Khususnya pada area Pengelolaan Risiko dan Kerangka Kerja Informasi Keamanan, nilai yang rendah mencerminkan belum adanya pendekatan yang sistematis dalam mengidentifikasi, menganalisis, dan memitigasi risiko keamanan informasi. Selain itu, hal ini juga menunjukkan belum terbentuknya prosedur dan kebijakan keamanan yang terdokumentasi baik.

DAFTAR PUSTAKA

[1] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*. Pearson Educación, 2004.

[2] A. I. Saleh and M. D. Winata, “Indonesia’s Cyber Security Strategy: Problems and Challenges,” presented at the International Joint Conference on Arts and Humanities 2023 (IJCAH 2023), Atlantis Press, Dec. 2023, pp. 1675–1696. doi: 10.2991/978-2-38476-152-4_169.

[3] M. Whitman and H. Mattord, “Principles of Information Security, 2nd Edition,” *Fac. Artic.*, Dec. 2004, [Online]. Available: https://digitalcommons.kennesaw.edu/facpubs/1430

[4] E. R. Pratama, S. Suprapto, and A. R. Perdanakusuma, “Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur),” *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, Aug. 2018.

[5] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” *J. Inf. Secur.*, vol. 04, no. 02, pp. 92–100, 2013, doi: 10.4236/jis.2013.42011.

[6] M. E. Whitman and H. J. Mattord, *Management of information security*. Cengage Learning, 2019. Accessed: May 13, 2025. [Online]. Available: https://thuvienso.hoasen.edu.vn/handle/123456789/9285

[7] M. Li, “Construction of an Enterprise Information Network Security Management System Based on Artificial Intelligence,” *Procedia Comput. Sci.*, vol. 259, pp. 677–685, Jan. 2025, doi: 10.1016/j.procs.2025.04.018.

[8] T. N. Khusna and B. Sugiantoro, “PENGUKURAN TINGKAT KEAMANAN INFORMASI PADA UPT-PSI UNIVERSITAS MURIA KUDUS BERDASARKAN INDEKS KEAMANAN INFORMASI (KAMI) VERSI 4.2,” *JIPI J. Ilm. Penelit. Dan Pembelajaran Inform.*, vol. 8, no. 3, Art. no. 3, Aug. 2023, doi: 10.29100/jipi.v8i3.3720.

[9] T. Santoso, “Panduan Penerapan Tata Kelola KIPPP”, Accessed: May 14, 2025. [Online]. Available: https://www.academia.edu/9682761/Panduan_Penerapan_Tata_Kelola_KIPPP

[10] “Infosecurity Magazine - Strategy, Insight, Technology,” Infosecurity Magazine. Accessed: May 14, 2025. [Online]. Available: https://www.infosecurity-magazine.com/

[11] C. Chazar, “STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005,” 2015.

[12] L. Santi, "Standar Nasional Indonesia SNI ISO/IEC 27001:2009 Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Persyaratan Information technology - Security techniques - Information security management systems - Requirements", Accessed: May 14, 2025. [Online]. Available: https://www.academia.edu/4580114/Standar_Nasional_Indonesia_SNI_ISO_IEC_27001_2009_Teknologi_informasi_Teknik_keamanan_Sistem_manajemen_keamanan_informasi_Persyaratan_Information_technology_Security_techniques_Information_security_management_systems_Requirements

[13] I. N. Rohmawati, I. K. Gozali, and M. Mt, "EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)".

[14] T. S. Agoan, H. F. Wowor, and S. Karouw, "Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan Framework COBIT 5 Domain Evaluate, Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS)," J. Tek. Inform., vol. 10, no. 1, Art. no. 1, Apr. 2017, doi: 10.35793/jti.v10i1.15627.

[15] B. Gamaliel, Y. D. Y. Rindengan, and S. Karouw, "PENGUKURAN TINGKAT KESELARASAN TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 PADA PEMERINTAH SULAWESI UTARA," J. Tek. Inform., vol. 11, no. 1, Art. no. 1, Jun. 2017, doi: 10.35793/jti.v11i1.16747.

[16] M. Rizal and Y. G. Sucahyo, "A study on the preparedness of information security framework area based on the assessment of information security index in Ministry of XYZ," in 2013 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Sep. 2013, pp. 55–59. doi: 10.1109/ICACSIS.2013.6761552.

[17] N. Matondang, B. Hananto, and C. Nugrahaeni, "ANALISIS TINGKAT KESIAPAN PENGAMANAN SISTEM INFORMASI," J. Teknol. Inf. Dan Pendidik., vol. 12, no. 1, Art. no. 1, Mar. 2019, doi: 10.24036/tip.v12i1.176.

[18] A. Muhajirin and K. H. Santoso, "KAJIAN TINGKAT KEMATANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI STUDI KASUS: SUKU DINAS KOMUNIKASI DAN INFORMATIKA JAKARTA SELATAN," 2012.

[19] G. D. S. Barani, W. H. N. Putra, and B. S. Prakoso, "Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus : Dinas Komunikasi dan Informatika Provinsi Jawa Timur)".

[20] A. R. Rahmandini, B. T. Hanggara, and A. Rachmadi, "Analisis Tingkat Kesiapan Keamanan Informasi pada Badan Perencanaan Pembangunan, Penelitian dan Pengembangan Kabupaten Tapin menggunakan Indeks KAMI (Keamanan Informasi) 4.1," J. Pengemb. Teknol. Inf. Dan Ilmu Komput., vol. 5, no. 2, pp. 589–596, Feb. 2021.

[21] N. E. Wowor, S. R. Sentinuwo, and S. D. S. Karouw, "Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks KAMI," J. Tek. Inform., vol. 13, no. 3, Art. no. 3, Sep. 2018, doi: 10.35793/jti.13.3.2018.28081.

[22] A. Firdani, S. Suprapto, and A. R. Perdanakusuma, "Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 menggunakan Indeks KAMI Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang," J. Pengemb. Teknol. Inf. Dan Ilmu Komput., vol. 3, no. 6, pp. 6009–6015, Jul. 2019.

[23] "EVALUASI TINGKAT KEAMANAN INFORMASI SEBAGAI UPAYA PENINGKATAN KEAMANAN SISTEM INFORMASI AKADEMIK DI SEKOLAH TINGGI TEKNIK QOMARUDDIN GRESIK MENGGUNAKAN INDEKS KEAMANAN INFORMASI | Abidin | NJCA (Nusantara Journal of Computers and Its Applications)." Accessed: May 14, 2025. [Online]. Available: https://journal.csnu.or.id/index.php/njca/article/view/198/0

[24] R. Habibullah, M. T. Nuruzzaman, and A. Mulyanto, “Evaluasi Keamanan Sistem Informasi Dengan Indeks KAMI Dan COBIT 5 Di Pesantren,” Cyber Secur. Dan Forensik Digit., vol. 7, no. 2, pp. 69–80, Dec. 2024, doi: 10.14421/csecurity.2024.7.2.4576