

## EVALUASI KEAMANAN INFORMASI PADA SMAN 1 TANGGAMUS MENGGUNAKAN INDEKS KAMI VERSI 4.2

Rizky Yulizar Rahman<sup>1</sup>, Muhammad Said Hasibuan<sup>2</sup>

<sup>1</sup>Jurusan Ilmu Komputer, Prodi Magister Teknik Informatika, Institut Bisnis dan Informatika Darmajaya Lampung

<sup>2</sup>Jurusan Ilmu Komputer, Prodi Magister Teknik Informatika, Institut Bisnis dan Informatika Darmajaya Lampung

e-mail: [rizky.2121210009@mail.darmajaya.ac.id](mailto:rizky.2121210009@mail.darmajaya.ac.id), [msaid@darmajaya.ac.id](mailto:msaid@darmajaya.ac.id)\*

### Abstract

*The importance of the process of evaluating information system security for an organization or company whose goal is to carry out early detection of information leaks and even disruption of information systems. This research was conducted at SMAN 1 Tanggamus. The research conducted was to determine the level of information security readiness based on ISO/IEC 27001:2013 standardization by using a tool, namely the KAMI Index Version 4.2. In this research, the method used to carry out the data collection process is by direct observation of the research object and questions and answers with the IT section that handles related information systems. Based on the research conducted, it was found that at the level of need for electronic devices, they get a score of 20 points which is in line with the high KAMI index and is still Level I to Level II. Although the results of the readiness assessment have a score of 245, this is a safety level of 1 that applies to SMAN 1 Tanggamus. To achieve the expected level of qualification SMAN 1 Tanggamus must improve information security internally and externally and carry out security assessments on an ongoing and continuous basis, Prepare a Road Map for an overview of the Information Security Management System clearly, Compile and publish to all existing employees the related list Assets and risk management that are always updated at any time, Compile and complete standard operating procedures for each existing management process, Complete documentation of activity implementation so that it has guidelines for holding documents when needed, Pay attention to and prioritize improvements to the level of security in the implementation of existing information systems.*

**Keywords:** Index KAMI version 4.2, Security, Information Technology, Evaluation, Information,

### Abstrak

Pentingnya proses evaluasi keamanan sistem informasi bagi suatu organisasi maupun perusahaan yang tujuannya adalah untuk melakukan deteksi dini dari bocornya informasi bahkan terganggunya sistem informasi. Dalam riset ini dilakukan pada SMAN 1 Tanggamus. Riset yang dilakukan adalah untuk mengetahui tingkat kesiapan keamanan informasi berdasarkan standarisasi ISO/IEC 27001:2013 dengan penggunaan alat bantu yaitu Indeks KAMI Versi 4.2. Pada riset ini metode yang digunakan untuk melakukan proses pengumpulan data adalah dengan melakukan pengamatan langsung pada objek riset serta tanya jawab dengan bagian IT yang menangani terkait sistem informasi. Berdasarkan riset yang dilakukan didapati bahwa pada level kebutuhan perangkat elektronik mendapatkan nilai 20 poin yang selaras dengan indeks KAMI yang tinggi dan masih Level I sampai Level II. Meskipun hasil asesmen kesiapan memiliki nilai 245, ini adalah tingkat keamanan 1 yang berlaku untuk SMAN 1 Tanggamus. Untuk mencapai tingkat kualifikasi yang diharapkan SMAN 1 Tanggamus harus meningkatkan keamanan informasi secara intern maupun ekstern serta melakukan penilaian keamanan secara berkelanjutan dan terus-menerus, Menyusun Road Map gambaran umum Sistem Manajemen Keamanan Informasi dengan jelas, Menyusun dan mempublikasikan kepada seluruh pegawai yang ada terkait daftar Aset dan manajemen risiko yang selalu di update setiap saat, Menyusun dan melengkapi standar operasional prosedur dari setiap proses pengelolaan yang ada, Melengkapi dokumentasi pelaksanaan kegiatan sehingga memiliki pedoman dokumen poegangan pada saat dibutuhkan, Memperhatikan serta memprioritaskan perbaikan tingkat keamanan pada pemnerapan sistem informasi yang ada.

**Kata Kunci:** Indeks KAMI versi 4.2, Keamanan, Teknologi Informasi, Evaluasi, Informasi

©This work is licensed under a Creative Commons Attribution - ShareAlike 4.0 International License

## 1. Pendahuluan

Tata kelola dari sebuah penerapan teknologi yang dilakukan dengan sistematis menjadi suatu keharusan bagi setiap fasilitator layanan internet. Dengan pesatnya perkembangan teknologi informasi, sangat berbanding lurus dengan tingkat resiko dari penerapan teknologi informasi. Luasnya penerapan teknologi informasi pada dunia pendidikan dapat memberikan dampak baik guna menambah nilai kepraktisan dan produktivitas. tidak dapat disangkal bahwa dalam penerapan teknologi informasi akan menghasilkan level kerentanan keamanan informasi [1] Oleh karena itu, tingkat keamanan pada sistem informasi yang baik sangat diharapkan. Keamanan dari suatu sistem informasi adalah suatu proses yang memiliki hubungan antara ketertutupan, integritas data dan kesiapan sumber daya informasi dalam wujud pengerjaan, pencadangan dan distribusi [2]. Keamanan sistem informasi dapat dipahami sebagai sejenis kekayaan yang sangat penting dan berharga untuk diamankan oleh suatu perusahaan atau organisasi. Perusahaan perlu memperhatikan keamanan aset yang dapat menimbulkan dampak berupa kehilangan data, kebocoran data, dan kegagalan sistem, serta dapat memicu dampak kerugian yang sangat kompleks baik dari sudut pandang finansial ataupun operasional [3].

Penilaian keamanan sistem informasi adalah sebuah cara yang dapat dilakukan dalam mengurangi ancaman atau resiko dari sensitivitas penerapan sistem informasi dari pihak yang tidak mempunyai hak [4], Acuan yang dipakai untuk mengerjakan proses pemeriksaan atau evaluasi terhadap sebuah perlindungan yaitu dengan menerapkan indeks KAMI yang mengacu atas dasar standarisasi ISO/IEC 27001:2013, didalam acuan indeks KAMI tersebut bisa dipakai dalam menganalisa dan penilaian terhadap kesiapan dari suatu sistem informasi pada lembaga, instansi pemerintahan serta organisasi berdasarkan standar yang sudah ada didalam SNI ISO/IEC 27001:2013 [5]. Indeks KAMI yang didasari pada standar ISO/IEC 27001:2013 adalah sebuah tools yang dipakai dalam proses analisa terhadap kesiapan suatu organisasi, perusahaan, maupun instansi pemerintahan sebagai deskripsi keadaan dari suatu ketelitian dalam memilih *Framework* keamanan informasi, yang dapat diterapkan oleh sebuah perusahaan, organisasi, dan instansi pemerintahan sekalipun [6].

Indeks KAMI memiliki 3 ruang lingkup penilaian antara lain. Pertama adalah mengelompokkan bagian dari sistem elektronik suatu perusahaan, instansi pemerintahan, atau organisasi. kemudian yang kedua yaitu melakukan pemeriksaan terhadap wilayah yang mencakup manajemen pengelolaan dari Keamanan Informasi, Manajemen Risiko Keamanan Informasi, *Framework* Keamanan Informasi, Manajemen Aset

Informasi, Teknologi Informasi dan Keamanan serta Integritas dari Pengamanan Informasi. untuk bagian pemeriksaan yang Selanjutnya ketiga yaitu melakukan penilaian terhadap aspek yang dapat menciptakan dampak terhadap keamanan informasi diantaranya pemeriksaan terhadap kesiapan dari campur tangan pihak lain, Layanan Infrastruktur *Cloud Computing*, dan Penjagaan terhadap Data Pribadi [7].

Standarisasi ISO/IEC 27001 adalah suatu acuan dari standarisasi keamanan informasi yang diterbitkan oleh International Organization for Standardization dan Electronics Engineering Committee (ISO/IEC), yang diperuntukan untuk membantu organisasi, perusahaan, maupun instansi pemerintahan untuk mengamankan aset berupa informasi [8]. ISO/IEC 27001 mendefinisikan berbagai syarat untuk memastikan, melaksanakan, memantau, mengawasi, dan menyimpan *Information Security Management System* (ISMS) [9], Standarisasi ISO/IEC bersifat berdiri sendiri terhadap keluaran berupa teknologi informasi, dengan memakai kebijakan manajemen berlandaskan risiko, serta dibuat untuk menetapkan kontrol keamanan yang ada dapat melakukan pengamanan aset informasi [10].

Terdapat sebagian riset yang dilakukan oleh peneliti terdahulu yang relevan dengan riset ini yaitu riset dengan judul “Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)” [11] tujuan dari riset ini adalah untuk melakukan penilaian dengan memakai Indeks KAMI 4.0 untuk mendapatkan hasil level kesiapan keamanan informasi pada instansi pemerintah. Hasil riset yang dilakuakn menghasilkan tingkat integritas dengan skor 195 dan pada umumnya level kesiapan keamanan informasi berada pada level I dan level I+. dari hasil riset yang sudah diperoleh dapat diberikan sebuah rekomendasi yaitu perlu melakukan peningkatan terhadap kelayakan keamanan informasi

Kemudian riset yang berjudul “Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus : UIN Sunan Kalijaga Yogyakarta)” [12] riset ini bertujuan untuk memaksimalkan proses keamanan informasi sesuai dengan standarisasi yang digunakan, Hasil riset ini menampilkan proses terjadi peningkatan skor sebesar 25, setelah diterapkan OSSIM dari sebelumnya sebesar 407 menjadi 432. Penerapan indeks KAMI membantu meningkatkan aspek tata kelola, pengelolaan kekayaan serta teknologi, untuk kelayakan keamanan informasi masih di level I+ sampai dengan II+ hal demikian menunjukkan bahwa keamanan informasi tidak layak dan dibutuhkan sebuah perbaikan

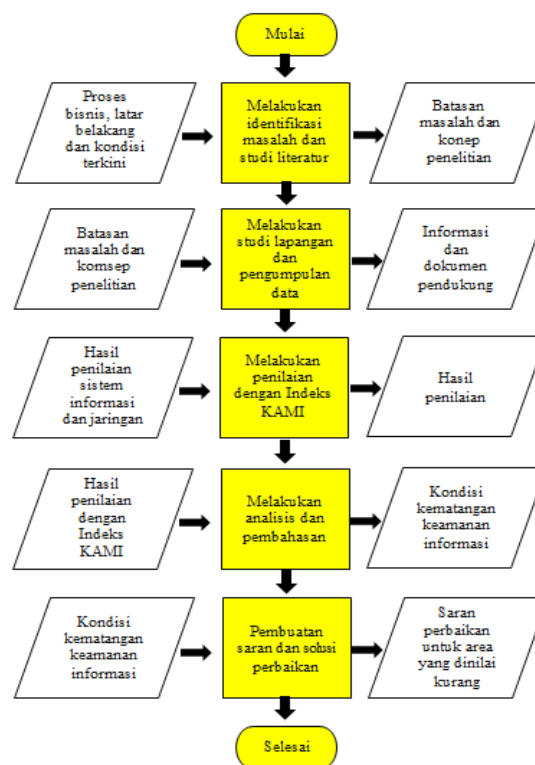
Kemudian riset selanjutnya berjudul “Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)” [13] Riset ini memiliki tujuan untuk melakukan penilaian terhadap kerentanan informasi dengan memanfaatkan tools Indeks KAMI untuk membantu melakukan penilaian evaluasi kesiapan pengamanan informasi guna terjaganya kerahasiaan, keaslian, keutuhan, dan kenirsangkalan informasi. Penelitian dilakukan menggunakan versi terbaru Indeks KAMI yaitu Versi 4.2. Hasil penilaian menghasilkan Skor Akhir sebesar 190 dengan Status Tingkat Kesiapan “Tidak Layak” dan tidak memenuhi Standar ISO/IEC 27001. Rekomendasi perbaikan yang diberikan dapat meningkatkan efektivitas kinerja Pengamanan Informasi Diskominfo Kabupaten Gianyar.

Berdasarkan hasil kajian pustaka didapatkan bahwa kajian terkait penilaian keamanan informasi menggunakan indeks KAMI versi 4.2 dapat dikatakan sangat minim jumlahnya, Indeks KAMI veris 4.2 adalah sebuah tools atau software yang digunakan dalam melakukan penilaian kesiapan keamanan informasi berdasarkan kriteria dari standarisasi SNI ISO/IEC 27001 [14], .maka dari uraian diatas riset ini memanfaatkan indeks KAMI versi 4.2 untuk melakukan penilaian dari kesiapan keamanan informasi pada SMAN 1 Tanggamus. Tujuan dilakukannya riset ini adalah untuk mengetahui dan memperoleh informasi terkait level kesiapan keamanan informasi.

## 2. Metode Penelitian

Adapun alur riset dalam pelaksanaan penilaian terhadap kerentanan sistem informasi memakai indeks KAMI versi 4.2 berdasarkan acuan standarisasi ISO/IEC 27001: 2013. Riset ini diawali dengan proses pengenalan terhadap masalah serta melakukan kajian literatur terkait penilaian keamanan sistem dan informasi untuk mencari acuan dari penelitian lain yang telah dilakukan oleh peneliti lain serta memperkuat teori sebagai bahan acuan untuk melakukan riset, Kemudian dilanjutkan dengan studi lapangan untuk mengumpulkan data dengan melakukan wawancara dengan tenaga ahli IT yang bertanggung jawab atas subjek tersebut dalam hal ini pada SMAN 1 Tanggamus serta dengan melakukan pengamatan dari proses penerapan teknologi informasi pada SMAN 1 Tanggamus dan melakukan tinjauan literature dari penelitian yang telah dilakukan sebelumnya oleh peneliti lain. Dokumen yang diperoleh dari *literature review* dapat dijadikan sebagai mekanisme untuk penilaian Indeks KAMI dengan standarisasi ISO/IEC 27001:2013. kemudian setelah data terkumpul selanjutnya adalah melakukan proses analisa dari data yang diperoleh menggunakan Indeks KAMI Versi 4.2 untuk mengetahui keadaan sebenarnya dari tingkat keamanan informasi pada SMAN 1 Tanggamus agar mampu dipelajari dan di analisa untuk diangkat menjadi pedoman atau rekomendasi perbaikan untuk

sistem keamanan informasi kepada SMAN 1 Tanggamus dengan acuan standarisasi ISO/IEC 27001 untuk dijadikan sebagai acuan perbaikan dimasa yang akan datang. Adapun tahapan dari riset ini dapat dilihat pada Gambar 1 berikut:



Gambar 1. Tahapan Riset

### 2.1. Metode Pengumpulan Data

Metode pengumpulan data dalam riset ini yaitu dengan mengutamakan pendekatan kuantitatif, yaitu :

#### a. Metode observasi

Melaksanakan pemantauan secara langsung pada objek riset yang ditentukan dalam hal ini SMAN 1 Tanggamus dengan tujuan untuk memantau dan mempelajari terkait proses penerapan teknologi informasi yang ada dan berjalan pada SMAN 1 Tanggamus.

#### b. Metode wawancara

Melaksanakan wawancara atau tanya jawab kepada tenaga ahli IT yang bertanggung jawab atas penerapan fasilitas mengenai informasi elektronik pada SMAN 1 Tanggamus dengan melalui proses mengemukakan perbincangan sesuai dengan instrument yang ada pada indeks KAMI versi 4.2.

### 2.2. Metode Analisa Data

Kegiatan awal sebelum melaksanakan proses penilaian, adalah dengan melakukan pengelompokan data berupa data elektronik yang bertujuan untuk mengklasifikasikan serta mengelompokkan data elektronik menjadi bentuk tertentu dengan tujuan agar data dapat dengan mudah untuk dianalisa dan diambil sebuah kesimpulan kemudian dari hasil kesimpulan tersebut selanjutnya dipelajari dan dianalisa untuk

dijadikan sebuah rekomendasi perbaikan. Terdapat hubungan antara bagian sistem elektronik dengan kedudukan dari kematangan suatu keamanan informasi yang didasari oleh indeks keamanan informasi (KAMI) yang terdefiniskan pada tabel berikut:

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

Gambar 2. Pengelompokan Kategori Sistem Elektronik

Penggolongan data elektronik menjadi bentuk tertentu yang dilakukan sesuai dengan ketentuan atau acuan dari tingkat kematangan keamanan informasi dengan dasar acuan yang mengacu dari COBIT (*Control Objectives for Information and Related Technologies*) atau CMMI (*Capability Maturity Model Integration*) [15]. Terdapat 5 kategori atau tingkatan dari sebuah level kematangan keamanan informasi yang terdapat didalam indeks KAMI versi 4.2 antaralain:

- Level I - Keadaan awal
- Level II - Implementasi kerangka kerja dasar
- Level III- Terdefinisi serta Selaras
- Level IV- Dikelola dan Terhitung
- Level V - Ideal

Berdasarkan tingkat kematangan diatas masih Terdapat 4 kategori yang telah ditambahkan ke level kematangan untuk penjelasan secara rinci, yaitu level I+, II+, III+ dan IV+. Standar keamanan informasi menurut standar ISO/IEC 27001:2013 dengan level kematangan keamanan informasi minimal harus berada pada level III+. Penilaian yang dilakukan dengan menggunakan indeks KAMI versi 4.2 dapat memberikan hasil berupa level kesiapan keamanan informasi seperti pada gambar berikut :



Gambar 3. Level kematangan ISO 27001

Syarat memperoleh poin dari sebuah proses penilaian level kesiapan keamanan informasi yang mengacu pada Indeks KAMI Versi 4.2 yaitu dengan cara mendistribusikan soal berupa pertanyaan yang ditujukan kepada responden terkait yang dibagi menjadi tujuh kelompok antaralain aspek kategori sistem elektronik dimana aspek ini bertujuan untuk

menilai sejauh mana ketergantungan terhadap sebuah sistem elektronik, aspek pengelolaan kewan informasi dimana pada aspek ini menekankan terhadap proses penilaian kesiapan tata kelola keamanan informasi serta fungsi tugas dan tanggung jawab, aspek pengelolaan resiko keamanan informasi dimana didalam aspek ini menekankan pada proses penilaian tingkat kesiapan penerapan pengelolaan resiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi, aspek kerangka kerja yang digunakan dalam proses pengelolaan keamanan informasi dimana didalam aspek ini menekankan pada penilaian terhadap kesiapan dari penggunaan kerangka kerja yang meliputi kebijakan serta prosedur dalam proses pengelolaan keamanan informasi serta strategi dalam hal penerapannya, aspek pengelolaan aset keamanan informasi, aspek teknologi informasi dimana didalam aspek ini menekankan keutuhan, stabilitas dan keberhasilan dari proses penggunaan teknologi untuk melakukan perlindungan terhadap aset informasi, kemudian aspek penilaian terakhir adalah aspek suplemen dimana dalam aspek ini bertujuan untuk memonitor munculnya ancaman yang mengancam keamanan informasi baru dengan adanya keterlibatan pihak ketiga dari beberapa aspek yang ada. terdapat poin untuk masing-masing mode keamanan tergantung tingkat kematangannya. Berikut ini ringkasan tanggapan penilaian berupa kerangka kedudukan dan pengelompokan keamanan:

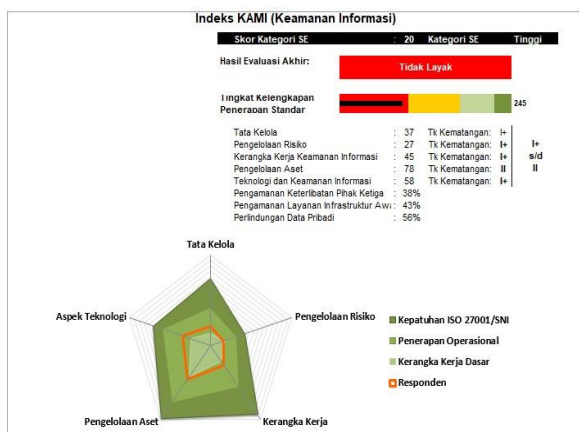
Tabel 1. Skor level kematangan

Status	Level Kematangan		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan Atau Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

Penyelesaian soal Kategori 3 dapat menghasilkan skor jika semua soal Kategori 1 dan Kategori 2 dalam aplikasi dapat dijawab minimal atau diterapkan sebagian. Jika ketergantungan lembaga, instansi pemerintahan ataupun perusahaan terhadap peran sistem elektronik semakin besar, hal ini dapat menyebabkan tumbuhnya berbagai bentuk implementasi keamanan informasi. [15]

### 3. Hasil dan Pembahasan

Berdasarkan proses penilaian level kematangan keamanan informasi pada SMAN 1 Tanggamus dapat diklasifikasikan kedalam 7 golongan yang telah disesuaikan dengan indeks KAMI versi 4.2, berikut merupakan hasil evaluasi keamanan informasi dilihat pada Gambar dibawah:



Gambar 4. Dashboard penilaian indeks KAMI versi 4.2

### 3.1. Kategori sistem elektronik

Dalam bagian ini menilai sejauh mana sistem elektronik yang digunakan SMAN 1 Tanggamus pada bagian ini memperoleh skor tertinggi yaitu 20. Skor ini didapatkan dari 10 butir soal pertanyaan indeks dengan skor maksimal 50 poin. Didalam kategori ini hanya akibat kegagalan sistem elektronik yang dilakukan penilaian dan memiliki skor tertinggi.

Konsekuensi yang didapat pada penilaian sistem elektronik dengan rating yang memuaskan untuk proses penerapan sistem elektronik di SMAN 1 Tanggamus, dimana permintaan sistem elektronik cenderung tinggi sehingga dapat dikatakan sangat ketergantungan pada sistem elektronik yang ada dan dapat menciptakan celah keamanan pada informasi yang terdapat pada penerapan teknologi informasi dalam lingkup SMAN 1 Tanggamus sehingga perlu menjadi perhatian yang lebih ketat untuk memastikan keamanan informasi pada penerapan teknologi informasi di SMAN 1 Tanggamus.

### 3.2. Tata Kelola Keamanan Informasi

Pada bagian selanjutnya merupakan proses melakukan penilaian terhadap kesiapan bentuk tata kelola keamanan informasi serta fungsi tugas dan tanggung jawab pengelola keamanan informasi yang meliputi proses penilaian manajemen keamanan informasi yang dapat mempengaruhi kualitas informasi yang dihasilkan oleh SMAN 1 Tanggamus. Skor tertinggi kategori Manajemen Keamanan Informasi adalah 126 poin. Hasil penilaian manajemen keamanan informasi yang disajikan pada tabel di bawah

Tabel 2. Hasil penilaian manajemen keamanan informasi

Status	Level Kematangan					Total
	1	Skor	2	Skor	3	
Tidak Dilakukan	0	0	0	0	0	0
Dalam Perencanaan	1	0	2	12	3	0
Dalam Penerapan Atau Sebagian	2	14	4	8	6	0
Diterapkan Secara Menyeluruh	3	3	6	0	9	0
Total Nilai Evaluasi Kemanan Informasi						37

Untuk bagian penilaian manajemen keamanan informasi atau sering disebut tata kelola didapatkan nilai skor 37 poin, menempatkan kategori ini ke level kesiapan I+. dimana proses manajemen keamanan informasi dapat dikatakan tidak layak dan perlu dilakukan perbaikan hal tersebut disebabkan karena banyaknya fungsi pengelolaan dari suatu sistem informasi pada area ini yang tidak dilakukan ditambah kurangnya dokumen pendukung yang memperkuat bahwa beberapa fungsi telah dilakukan pada SMAN 1 Tanggamus sehingga perlunya sebuah perbaikan dari segi pengelolaan sistem informasi yang ada serta melengkapi dokumentasi dari setiap aktivitas yang dilakukan dalam konteks tata kelola sistem informasi.pada SMAN 1 Tanggamus

### 3.3. Manajemen Resiko Keamanan Informasi

Langkah bagian ketiga adalah proses penilaian tingkat kesiapan penerapan pengelolaan resiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi pada SMAN 1 Tanggamus., yang meliputi berbagai risiko yang mungkin muncul dan mempengaruhi data maupun informasi di SMAN 1 Tanggamus. Hasil penilaian manajemen resiko keamanan informasi dSisajikan dalam tabel berikut:

Tabel 3. Penilaian manajemen resiko keamanan informasi

Status	Level Kematangan					Total
	1	Skor	2	Skor	3	
Tidak Dilakukan	0	0	0	0	0	0
Dalam Perencanaan	1	3	2	6	3	0
Dalam Penerapan Atau Sebagian	2	14	4	4	6	0
Diterapkan Secara Menyeluruh	3	0	6	0	9	0
Total Nilai Evaluasi Kemanan Informasi						27

Hasil penilaian di SMAN 1 Tanggamus menerima total 27 poin dan mendapat predikat level kesiapan I+. dimana proses manajemen resiko keamanan informasi dapat dikatakan tidak layak hal tersebut disebabkan karena banyaknya fungsi dari kegiatan pengelolaan resiko yang ada pada area ini yang sedang dalam tahap perencanaan dan sedang menunggu persetujuan dan anggaran untuk selanjutnya direalisasikan serta ditambah dengan kurangnya dokumen pendukung dari setiap proses pengelolaan resiko keamanan informasi yang telah dilakukan hal tersebut sangat menghambat dari proses evaluasi untuk dilakukan perbaikan.

### 3.4. Kerangka Kerja Keamanan Informasi

Proses tinjauan kerangka kerja manajemen keamanan informasi merupakan sebuah proses penilaian terhadap kelengkapan maupun kesiapan dari penggunaan kerangka kerja yang meliputi kebijakan serta prosedur dalam proses pengelolaan keamanan informasi serta strategi dalam hal penerapannya.. Langkah ini merupakan realisasi dan evaluasi dari langkah sebelumnya. Hasil pengukuran kerangka manajemen keamanan informasi disajikan pada tabel berikut:

Tabel 4. Evaluasi kerangka manajemen keamanan informasi

Status	Level Kematangan						Total
	Sko 1	Sko 2	Sko 3	Sko 4	Sko 5	Sko 6	
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	7	2	12	3	0	19
Dalam Penerapan Atau Sebagian	2	10	4	16	6	0	26
Diterapkan Secara Menyeluruh	3	0	6	0	9	0	0
Total Nilai Evaluasi Kemanan Informasi							45

Hasil penilaian kerangka kerja pengelolaan keamanan informasi di SMAN 1 Tanggamus dengan skor 45 tergolong maturity level I+. Skor ini diperoleh karena dalam proses evaluasi yang dilakukan banyak komponen yang berada dalam status perencanaan dan banyak dari proses yang dilakukan tanpa adanya dokumen yang mendukung sehingga mempengaruhi nilai yang didapat pada saat proses evaluasi dilakukan.

### 3.5. Manajemen aset informasi

Proses penilaian manajemen pengamanan aset informasi, termasuk didalam keutuhan peredaran pemakaian aset yang dipakai serta kelengkapan pengamanan aset informasi, termasuk keseluruhan alur penggunaan aset informasi yang ada pada SMAN 1 Tanggamus, berikut hasil penilaian dapat dilihat pada tabel dibawah:

Tabel 5. Penilaian manajemen aset informasi

Status	Level Kematangan						Total
	Sko 1	Sko 2	Sko 3	Sko 4	Sko 5	Sko 6	
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	5	2	14	3	0	19
Dalam Penerapan Atau Sebagian	2	26	4	12	6	0	38
Diterapkan Secara Menyeluruh	3	15	6	6	9	0	21
Total Nilai Evaluasi Kemanan Informasi							78

Hasil penilaian di proses ini memperoleh skor sebesar 78 poin dari total skor maksimal sebesar 168 poin sehingga termasuk kedalam level kesiapan II yang masih tergolong rendah dan perlu adanya perbaikan hal tersebut disebabkan oleh kurangnya dokumen yang mendukung pembuktian dari proses yang telah dilakukan sehingga perlu melengkapi dari dokumen terkait yang dapat mendukung bukti bahwa beberapa proses telah dilakukan dengan baik sesuai dengan prosedur yang berlaku seperti pembuatan daftar aset sistem informasi yang terdapat pada SMAN 1 Tanggamus yang dibagikan kepada seluruh pegawai untuk mencegah adanya penyelewengan aset informasi dari pihak yang tidak bertanggungjawab,

### 3.6. Teknologi Informasi dan Keamanan

Proses penilaian ini menekankan terhadap keutuhan, stabilitas dan keberhasilan dari proses penggunaan teknologi untuk melakukan perlindungan terhadap aset informasi yang terdapat pada SMAN 1 Tanggamus, hasil penilaian dapat dilihat pada tabel berikut:

Tabel 6. Hasil penilaian teknologi informasi dan keamanan

Status	Level Kematangan						Total
	Sko 1	Sko 2	Sko 3	Sko 4	Sko 5	Sko 6	
Tidak Dilakukan	0	0	0	0	0	0	0

Dalam Perencanaan	1	8	2	12	3	3	23
Dalam Penerapan Atau Sebagian	2	10	4	4	6	0	14
Diterapkan Secara Menyeluruh	3	3	6	18	9	0	21
Total Nilai Evaluasi Kemanan Informasi							58

Hasil penilaian Teknologi dan Keamanan Informasi SMAN 1 Tanggamus mendapatkan skor 58 poin dan mendapat level kesiapan I+ atau lebih rendah. Skor yang dicapai karena kurangnya penerapan keamanan informasi yang dilakukan SMAN 1 Tanggamus serta dokumen pendukung yang kurang terdokumentasi dengan baik sehingga mempersulit dalam mendapatkan nilai yang cukup baik pada area ini.

### 3.7. Suplemen

Tahapan terakhir adalah tahapan suplemen merupakan suatu proses evaluasi yang menilai keikutsertaan pihak luar kedalam kaitan penyampaian layanan dari instansi pemerintahan, lembaga atau perusahaan, yang dapat menghasilkan ancaman terkait keberadaan pihak luar tersebut, Nilai yang diperoleh dari proses evaluasi pada bagian Suplemen tidak akan mempunyai pengaruh terhadap total nilai dari keseluruhan kategori yang telah didapatkan nilainya dengan proses evaluasi dengan menggunakan Indeks KAMI yang dapat memperlihatkan level kesiapan dari proses pengamanan informasi dari ancaman resiko yang mengintai keberlangsungan penerapan teknologi informasi pada SMAN 1 Tanggamus. Berdasarkan acuan dari Indeks KAMI Versi 4.2 bahwa penilaian dari kategori suplemen ini memiliki tujuan untuk memonitor munculnya ancaman yang mengancam keamanan informasi baru dengan adanya keterlibatan pihak ketiga dari beberapa aspek yang ada.

Hasil evaluasi tahap terakhir didapatkan nilai untuk perlindungan keamanan informasi dari keterlibatan pihak luar diberi tingkat kematangan 38% dari presentase yang didapat tersebut menunjukkan bahwa terdapat cukup besar ketergantungan terhadap campur tangan pihak ketiga untuk melakukan proses penerapan sistem informasi pada SMAN 1 Tanggamus hal ini dapat berdampak buruk bagi keberlangsungan keamanan informasi sehingga perlu diperhatikan terkait campur tangan pihak ketiga didalam penerapan keamanan informasi yang ada. Kemudian terkait keamanan layanan infrastruktur *cloud computing* sebesar 43% hal ini perlu ditingkatkan untuk mencapai nilai presentase yang baik guna menghindari kebocoran data atau informasi dalam penggunaan fasilitas *cloud computing* yang sangat bermanfaat dalam proses penerapan sistem informasi pada SMAN 1 Tanggamus, Kemudian penilaian terakhir dari kategori suplemen adalah pengamanan data pribadi dengan hasil 56% hal ini sudah baik tetapi perlu ditingkatkan untuk kedepannya agar lebih kuat dari segi pengamanan terhadap data pribadi yang diterapkan oleh SMAN 1 Tanggamus agar dapat memperkecil resiko yang mengintai dari penerapan teknologi informasi pada SMAN 1 Tanggamus.

#### 4. Kesimpulan

Dari hasil penilaian level kematangan keamanan informasi menggunakan indeks KAMI versi 4.2, dapat ditarik sebuah kesimpulan bahwa pada level kebutuhan perangkat elektronik mendapatkan nilai 20 poin yang selaras dengan indeks KAMI yang tinggi dan masih Level I sampai Level II. Meskipun hasil asesmen kesiapan memiliki nilai 245, ini adalah tingkat keamanan 1 yang berlaku untuk SMAN 1 Tanggamus. Untuk mencapai tingkat kualifikasi sesuai dengan standarisasi ISO/IEC 27001:2013, SMAN 1 Tanggamus harus meningkatkan keamanan informasi secara intern maupun ekstern dalam hal ini pihak luar serta melakukan penilaian keamanan secara berkelanjutan dan terus-menerus. Menyusun Road Map gambaran umum Sistem Manajemen Keamanan Informasi dengan jelas, Menyusun dan mempublikasikan kepada seluruh pegawai yang ada terkait Daftar Aset dan Manajemen Risiko yang selalu di update setiap saat, Menyusun dan melengkapi SOP dari setiap proses pengelolaan yang ada, Melengkapi dokumentasi pelaksanaan kegiatan yang penting, sehingga memiliki pedoman dokumen poegangan pada saat dibutuhkan, Memperhatikan serta memprioritaskan perbaikan tingkat keamanan pada pemnerapan sistem informasi yang ada.

#### Daftar Pustaka

- [1] S. Paramita, Sandy Akbar Siregar, R. A. Damanik, and M. D. Irawan, "Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013," *Bull. Inf. Technol.*, vol. 3, no. 4, pp. 374–379, 2022, doi: 10.47065/bit.v3i1.421.
- [2] I. W. Wulandari and H. Hwihanus, "Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan," *J. Kaji. dan Penal. Ilmu Manaj.*, vol. 1, no. 1, pp. 11–25, 2023.
- [3] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network ( Literature Review Sim )," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: <https://doi.org/10.31933/jemsi.v3i5>.
- [4] D. Darwis, N. Y. Solehah, and Dartono, "Penerapan Framework COBIT 5 untuk audit tata kelola keamanan informasi pada Kantor Wilayah Kementerian Agama Provinsi Lampung," *TELEFORTECH J. Telemat. Inf. Technol.*, vol. 1, no. 2, pp. 38–45, 2021.
- [5] A. L. Maryanto, M. N. Al Azam, and A. Nugroho, "EVALUASI MANAJEMEN KEAMANAN INFORMASI PADA PERUSAHAAN PEMULA BERBASIS TEKNOLOGI MENGGUNAKAN INDEKS KAMI," in *Jurnal SimanteC*, Nov. 2022, vol. 11, no. 1, pp. 173–177.
- [6] R. A. P. P. Gala, R. Sengkey, and C. Punusingon, "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI," vol. 15, no. 3, pp. 189–198, 2020.
- [7] D. D. Prasetyowati, I. Gamayanto, S. Wibowo, and Suharnawi, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," *JOINS (Journal Inf. Syst.*, vol. 4, no. 1, pp. 65–75, 2019, doi: 10.33633/joins.v4i1.2429.
- [8] R. C. Annisyah, A. Budiono, and R. Fauzi, "ANALISIS DAN PERANCANGAN MANAJEMEN KEAMANAN INFORMASI DIREKTORAT SISTEM INFORMASI UNIVERSITAS TELKOM DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA AREA PENGELOLAAN ASET INFORMASI, TEKNOLOGI DAN KEAMANAN INFORMASI," *e-Proceeding Eng.*, vol. 8, no. 2, pp. 2663–2677, 2021.
- [9] F. Nasher, "Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (Lpse) Di Dinas Komunikasi Dan Informatika Kabupaten Cianjur Dengan Menggunakan Sni Iso/Iec 27001:2013," *Media J. Inform.*, vol. 10, no. 1, pp. 1–16, 2020, doi: 10.35194/mji.v10i1.465.
- [10] A. R. Riswaya, A. Sasongko, and A. Maulana, "EVALUASI TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI MENGGUNAKAN INDEKS KAMI UNTUK PERSIAPAN STANDAR SNI ISO/IEC 27001 (STUDI KASUS: STMIK MARDIRA INDONESIA)," *J. Comput. Bisnis*, vol. 14, no. 1, pp. 10–18, 2020.
- [11] N. D. Ramadhani, W. H. N. Putra, and A. D. Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 5, pp. 1490–1498, 2020.
- [12] R. Dewantara and B. Sugiantoro, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 8, no. 6, p. 1137, 2021, doi: 10.25126/jtiik.2021863123.
- [13] D. I. Khamil, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.
- [14] Biro Hukum dan Komunikasi Publik, "Konsultasi dan Assessment Indeks KAMI," *Badan Siber dan Sandi Negara*, 2021. <https://bssn.go.id/indeks-kami/>. (accessed Jun. 02, 2023).
- [15] F. A. Basyarahil, H. M. Astuti, and B. C. Hidayanto, "Evaluasi Manajemen Keamanan Informasi pada DPTSI ITS Surabaya," *J. Tek. Its*, vol. 6, no. 1, pp. 122–128, 2017.