

Penggunaan Indeks Keamanan Informasi (KAMI) 4.2 Sebagai Metode Evaluasi Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota XYZ

Muhammad Iqbal^{1*}, Dwi Arief Prambudi², I Putu Deny Arthawan Sugih Prabowo³

Program Studi Sistem Informasi, Jurusan Matematika dan Teknologi Informasi, Institut Teknologi Kalimantan

^{1*}10191056@student.itk.ac.id, ²dwiariefprambudi@lecturer.itk.ac.id, ³putudeny.asp@lecturer.itk.ac.id

Abstrak. Diskominfo Kota XYZ dibentuk pada awal tahun 2017 bersamaan dengan diterbitkannya Peraturan Walikota (Perwali) XYZ nomor 38 Tahun 2016 Tentang Susunan Organisasi dan Tata Kerja Diskominfo Kota XYZ. Terdapat bidang yang memiliki tanggung jawab terhadap keamanan informasi yaitu bidang Teknologi Informasi & Komunikasi dan bidang Persandian & Statistik. Berdasarkan wawancara yang dilakukan dengan karyawan Diskominfo Kota XYZ terdapat gangguan berupa peretasan sistem yang menyerang Diskominfo Kota XYZ, hal ini dapat terjadi dikarenakan lemahnya keamanan informasi pada Diskominfo Kota XYZ, saat ini Diskominfo Kota XYZ berfokus untuk memperluas jaringan *Fiber Optic* ke berbagai Organisasi Perangkat Daerah (OPD) sehingga kurang memperhatikan aspek keamanan informasi. Kemudian Diskominfo Kota XYZ juga belum mempunyai dokumen fisik mengenai manajemen risiko SMKI. Pada penelitian ini, akan dilakukan evaluasi keamanan informasi pada Dinas Komunikasi dan Informatika Kota XYZ menggunakan Indeks KAMI 4.2 dengan standar ISO/IEC 27001:2013 untuk mengetahui Tingkat Kesiapan keamanan informasi. Didapatkan hasil evaluasi dengan skor akhir keseluruhan sebesar 418 dan skor akhir pada kategori Sistem Elektronik (SE) sebesar 26 yang termasuk ke dalam kategori “Tinggi”, sehingga menunjukkan bahwa keamanan informasi saat ini berada pada status Tingkat Kesiapan “Tidak Layak” dengan Tingkat Kematangan pada tingkat I hingga tingkat II. Adapun saran dan rekomendasi perbaikan yang diberikan mengacu pada standar atau control ISO/IEC 27001:2013.

Kata Kunci : Evaluasi, Diskominfo Kota XYZ, Indeks Keamanan Informasi (KAMI) 4.2, ISO/IEC 27001:2013, SMKI.

1. PENDAHULUAN

Kemajuan teknologi informasi (TI) terus berkembang cepat hingga saat ini, membuat setiap organisasi atau perusahaan harus dapat beradaptasi terhadap perkembangan teknologi informasi. Berdasarkan survey oleh Badan Pusat Statistik (BPS), perkembangan teknologi di Indonesia pada tahun 2021 mempunyai nilai sebesar 62,10% meningkat tinggi dibandingkan pada tahun 2020 yang hanya sebanyak 53,73% [1]. Teknologi yang berkembang pesat tentunya terdapat informasi yang diolah dan disimpan didalamnya. Informasi menjadi data yang telah diproses sedemikian rupa sehingga bisa meningkatkan pengetahuan seseorang yang menggunakan data tersebut. Informasi memiliki siklus yang menggambarkan pengolahan data menjadi informasi untuk pengambilan keputusan, hingga akhirnya tindakan yang dihasilkan mengarah pada pengembalian data [2]. Oleh karena itu informasi merupakan salah satu hal terpenting yang harus dilindungi untuk mencegah penyalahgunaan dari informasi tersebut.

Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ merupakan salah satu instansi pemerintahan di Kota XYZ yang berfokus pada bidang Teknologi Informasi dan Komunikasi. Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ mempunyai tugas untuk membantu dan mendukung kelancaran tugas Kepala Daerah, menjalankan sebagian urusan pemerintah yang menjadi kewenangan pemerintah daerah dalam pelaksanaan kebijakan daerah yang bersifat spesifik khususnya perumusan, penetapan dan pelaksanaan kebijakan operasional di bidang pengelolaan dan pelayanan informasi, sarana komunikasi dan diseminasi informasi, teknologi informasi dan komunikasi aplikasi dan layanan publik, persandian dan statistik serta koordinasi pelaksanaan tugas, pembinaan, dan pemberian dukungan administrasi kepada seluruh organisasi di lingkungan dinas.

Berdasarkan hasil wawancara dengan pihak Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ, diketahui terdapat permasalahan yang menyerang sistem Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Hal ini dapat terjadi dikarenakan kurangnya pemahaman mengenai keamanan informasi, kemudian Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ hanya berfokus untuk memperluas jaringan *Fiber Optic* ke berbagai Organisasi Perangkat Daerah (OPD) seperti kecamatan, kelurahan, dan puskesmas, sehingga Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ belum pernah melakukan evaluasi keamanan informasi baik secara internal atau mandiri (*self assessment*) ataupun dengan pihak eksternal melalui Badan Siber & Sandi Negara (BSSN). Berdasarkan hal tersebut, maka diperlukan evaluasi keamanan informasi pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ untuk melihat kondisi keamanan informasi saat ini apakah sudah sesuai dengan standar yang berlaku atau belum.

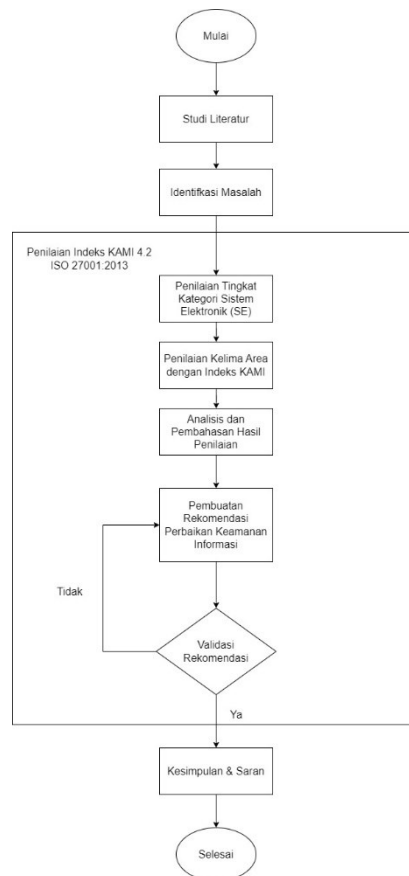
Evaluasi keamanan informasi merupakan suatu kegiatan untuk menilai tingkat kematangan dan kesiapan keamanan informasi pada suatu instansi atau perusahaan. Evaluasi keamanan informasi memiliki standar internasional yang dibentuk oleh Badan Siber dan Sandi Negara Republik Indonesia, yaitu Indeks Keamanan Informasi (KAMI). Berdasarkan peraturan oleh BSSN Nomor 8 tahun 2021, Indeks Keamanan Informasi (KAMI) digunakan untuk mengevaluasi tingkat

kematangan, tingkat kelengkapan penerapan pada ISO/IEC 27001 :2013 dan memberikan gambaran tata kelola keamanan informasi pada sebuah organisasi. Indeks KAMI 4.2 memiliki 7 area evaluasi berdasarkan ISO/IEC 27001:2013 seperti Kategori Sistem Elektronik, area Tata Kelola Keamanan Informasi, area Pengelolaan Risiko Keamanan Informasi, area Kerangka kerja Keamanan Informasi, area Pengelolaan Aset Informasi, area Aspek Teknologi dan *Suplemen* [3]-[4].

Diharapkan dengan adanya penelitian ini, dapat mengetahui dan menilai tingkat kesiapan serta kematangan keamanan informasi sehingga sesuai dengan standar SNI ISO/IEC 27001:2013 dan memberikan rekomendasi serta saran perbaikan yang diharapkan dapat meningkatkan tingkat keamanan informasi pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ.

2. METODE

Adapun tahapan yang dilakukan dalam penelitian ini terdiri atas 7 (tujuh) tahap, mulai dari tahap studi literatur hingga tahap kesimpulan dan saran. Rincian penjelasan dari setiap tahapan dalam melaksanakan penelitian, dapat dilihat pada Gambar 1 berikut.



Gambar 1. Diagram Alir Penelitian

2.1 Studi Literatur

Pada tahap ini melakukan studi literatur dengan mengumpulkan beberapa referensi dari buku, jurnal, dan tugas akhir mengenai keamanan informasi, SMKI, ISO/IEC 27001, Indeks Keamanan Informasi (KAMI), Area Penilaian Indeks KAMI Versi 4.2, dan Skor Penilaian Indeks KAMI Versi 4.2.

2.2 Identifikasi Masalah

Pada tahap ini melakukan identifikasi masalah dengan menggunakan metode wawancara kepada pihak instansi / organisasi yang dituju sehingga didapatkan pada Diskominfo XYZ belum memiliki dokumen evaluasi keamanan informasi menggunakan metode Indeks KAMI dan belum ada evaluasi yang dilakukan dari pihak instansi. Pada tahap ini juga dilakukan kajian, penetapan konsep serta metode, tools dan framework yang nantinya akan digunakan untuk permasalahan dari penelitian.

2.3 Penilaian Tingkat Kategori Sistem Elektronik (SE)

Pada tahap ini melakukan penilaian tingkat kategori sistem elektronik pada tahap ini akan dilakukan evaluasi sebelum menentukan penilaian pada kategori berdasarkan skor total sistem elektronik (SE) yang terdapat pada Diskominfo

XYZ, dimana hasil yang didapatkan akan dikategorikan menjadi tiga yaitu rendah, tinggi, dan strategis. Penilaian dilakukan kepada salah satu responden pada bidang yang memiliki peran dan tanggung jawab pada sistem elektronik, penilaian dilakukan dengan metode wawancara dengan memberikan 10 buah pertanyaan mengenai sistem elektronik yang telah disediakan oleh Indeks KAMI 4.2 pada *software Microsoft Excel*. Hasil yang didapatkan dari tahapan ini yaitu berupa klasifikasi tingkat karakteristik meliputi kategori rendah, tinggi, atau strategis berdasarkan skor total dari penilaian kategori sistem elektronik (SE) pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ.

2.4 Penilaian Kelima Area Indeks KAMI 4.2

Pada tahap ini melakukan penilaian kelima area keamanan informasi pada Diskominfo XYZ sesuai dengan metode KAMI 4.2 untuk menentukan nilai kematangan dan kesiapan dari keamanan informasi yang dijalankan pada pihak instansi. Dimana pada tahapan ini akan dilakukan sebuah penilaian kelima area secara menyeluruh menggunakan hasil pertanyaan meliputi area tata kelola, area risiko, area kerangka kerja, area pengelolaan aset, area teknologi dan suplemen yang telah ditentukan dengan rinci sesuai dengan Indeks KAMI 4.2 pada *software Microsoft Office Excel*. Penilaian juga dilakukan kepada responden yang merupakan penanggung jawab dari bidang terkait kemudian dilakukan metode wawancara atau observasi secara langsung. Hasil yang didapatkan dari tahapan ini yaitu berupa nilai kematangan dari skor total penilaian kelima area pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ.

2.5 Pembuatan Rekomendasi Perbaikan Keamanan Informasi

Tahap ini dilakukan untuk memberikan rekomendasi kepada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ dalam bentuk tabel yang berisikan kondisi instansi saat ini serta kondisi ideal hingga memberikan rekomendasi kepada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ agar dapat mencapai kondisi yang sesuai dengan standar ISO/IEC 27001:2013. Kemudian hasil dari rekomendasi akan diberikan kepada pihak Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ untuk divalidasi. Apabila kondisi telah sesuai, maka akan lanjut ke tahapan berikutnya. Namun apabila belum sesuai, maka akan kembali pada tahapan pembuatan rekomendasi hingga sesuai dengan instansi.

2.6 Kesimpulan dan Saran

Pada tahap ini dilakukan penarikan kesimpulan mengenai kesiapan serta kematangan dan pengambilan keputusan yang sesuai dengan hasil evaluasi, data dan dokumentasi. Kemudian memberikan saran perbaikan yang sesuai dengan hasil dari evaluasi beserta data yang telah dikumpulkan mengenai keamanan informasi pada pihak instansi terkait guna meningkatkan nilai pada area keamanan informasi untuk persiapan kegiatan evaluasi keamanan informasi pada Diskominfo XYZ.

3. HASIL DAN PEMBAHASAN

Bagian ini berisi penjelasan mengenai hasil dari penelitian evaluasi keamanan informasi menggunakan Indeks KAMI 4.2 pada Diskominfo Kota XYZ mulai dari tahapan penyusunan instrumen pengumpulan data hingga hasil dari penelitian.

3.1 Penilaian Tingkat Kategori Sistem Elektronik (SE)

Pada tahap ini akan dilakukan penilaian terhadap tingkat Kategori Sistem Elektronik (SE) yang dilakukan dengan metode wawancara bersama narasumber, adapun hasil penilaian dapat dilihat pada Tabel 1 berikut.

Tabel 1. Hasil Penilaian Tingkat Kategori Sistem Elektronik (SE)

Bagian I : Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
Jumlah Pertanyaan Sistem Elektronik (SE)			: 10
Hasil Jawaban Narasumber			
Status Penerapan	Jumlah Pertanyaan	Skor	Total Skor
[A]	3	5	15
[B]	4	2	8
[C]	3	1	3
Skor penetapan kategori Sistem Elektronik :			26

Didapatkan hasil skor penetapan Kategori Sistem Elektronik (SE) sebesar 26 dan masuk kedalam kategori "Tinggi" yang berarti kepentingan penggunaan sistem elektronik pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ.

3.2 Penilaian Kelima Area Indeks KAMI 4.2

Setelah dilakukan penilaian terkait penggunaan Sistem Elektronik (SE), selanjutnya dilakukan penilaian terhadap seluruh area Indeks KAMI 4.2 meliputi Area Tata Kelola Keamanan Informasi, Area Risiko Keamanan Informasi, Area Kerangka Kerja Keamanan Informasi, Area Pengelolaan Aset Informasi, Area Teknologi dan Keamanan Informasi serta Suplemen. Adapun penilaian terhadap area Indeks KAMI 4.2 pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ dapat dilihat pada subbab berikut.

3.2.1 Penilaian Area Tata Kelola Keamanan Informasi

Penilaian yang ditujukan pada area Tata Kelola Keamanan Informasi berikut berisikan pertanyaan yang berisikan status “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan / Diterapkan Sebagian”, dan “Dilakukan Secara Menyeluruh” oleh Dinas Komunikasi dan Informatika Kota XYZ. Penilaian dilakukan dengan metode wawancara bersama narasumber, adapun hasil penilaian dapat dilihat pada Tabel 2 berikut.

Tabel 2. Hasil Penilaian Area Tata Kelola Keamanan Informasi

Bagian II : Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.			
Jumlah Pertanyaan Tata Kelola Keamanan Informasi		:	22
Hasil Jawaban Narasumber			
Status Penerapan	Jumlah Pertanyaan		
Tidak Dilakukan	0		
Dalam Perencanaan	2		
Dalam Penerapan / Diterapkan Sebagian	15		
Diterapkan Secara Menyeluruh	5		
Total Nilai Evaluasi Tata Kelola Keamanan Informasi		:	87
Hasil Tingkat Kelengkapan Pengamanan			
Tingkat Kategori Pengamanan (KP)	Jumlah Pertanyaan	r Penerapan 1 dan 2	
KP 1	8	18	
KP 2	8	36	
KP 3	6	33	
Jumlah Pertanyaan / Skor Penerapan :		22	87
Hasil Tingkat Kematangan Pengamanan			
Tingkat Kategori Kematangan	Jumlah Pertanyaan	Skor	Tingkat Status Kematangan
II	13	40	II
III	3	14	No
IV	6	33	No
Total / Skor :		22	87
			II

Berdasarkan Tabel 2, dapat disimpulkan bahwa area Tata Kelola Keamanan Informasi Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ saat ini memiliki total nilai evaluasi sebesar 87 poin dan berada pada tingkat kematangan pengamanan II yang berarti dalam penerapan kerangka kerja dasar.

3.2.2 Penilaian Area Pengelolaan Risiko Keamanan Informasi

Penilaian yang ditujukan pada area Pengelolaan Risiko Keamanan Informasi berikut berisikan pertanyaan yang berisikan status “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan / Diterapkan Sebagian”, dan “Dilakukan Secara Menyeluruh” oleh Dinas Komunikasi dan Informatika Kota XYZ. Penilaian dilakukan dengan metode wawancara bersama narasumber, adapun hasil penilaian dapat dilihat pada Tabel 3 berikut.

Tabel 3. Hasil Penilaian Area Pengelolaan Risiko Keamanan Informasi

Bagian III : Risiko Keamanan Informasi			
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.			
Jumlah Pertanyaan Risiko Keamanan Informasi		:	16



Hasil Jawaban Narasumber

Status Penerapan	Jumlah Pertanyaan	
Tidak Dilakukan	0	
Dalam Perencanaan		16
Dalam Penerapan / Diterapkan Sebagian	0	
Diterapkan Secara Menyeluruh	0	
Total Nilai Evaluasi Risiko Keamanan Informasi	:	18
Hasil Tingkat Kelengkapan Pengamanan		

Tingkat Kategori Pengamanan (KP)	Jumlah Pertanyaan	Skor Penerapan 1 dan 2	
KP 1	10	10	
KP 2	4	8	
KP 3	2	0	
Jumlah Pertanyaan / Skor Penerapan :	16	18	
Hasil Tingkat Kematangan Pengamanan			
Tingkat Kategori Kematangan	Jumlah Pertanyaan	Skor	Tingkat Status Kematangan
II	10	10	No
III	2	4	No
IV	2	4	No
V	2	0	No
Total / Skor :	16	18	I

Berdasarkan Tabel 3, dapat disimpulkan bahwa area Risiko Keamanan Informasi Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ saat ini memiliki total nilai evaluasi sebesar 18 poin dan berada pada tingkat kematangan pengamanan I yang berarti dalam kondisi awal.

3.2.3 Penilaian Area Kerangka Kerja Pengelolaan Keamanan Informasi

Penilaian yang ditujukan pada area Kerangka Kerja Pengelolaan Keamanan Informasi berikut berisikan pertanyaan yang berisikan status “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan / Diterapkan Sebagian”, dan “Dilakukan Secara Menyeluruh” oleh Dinas Komunikasi dan Informatika Kota XYZ. Penilaian dilakukan dengan metode wawancara bersama narasumber, adapun hasil penilaian dapat dilihat pada Tabel 4 berikut.

Tabel 4. Hasil Penilaian Area Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV : Kerangka Kerja Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
Jumlah Pertanyaan Kerangka Kerja		:	29
Hasil Jawaban Narasumber			
Status Penerapan	Jumlah Pertanyaan		
Tidak Dilakukan	0		
Dalam Perencanaan	10		
Dalam Penerapan / Diterapkan Sebagian	12		
Diterapkan Secara Menyeluruh	7		
Total Nilai Evaluasi Kerangka Kerja		:	97
Hasil Tingkat Kelengkapan Pengamanan			
Tingkat Kategori Pengamanan (KP)	Jumlah Pertanyaan	Skor Penerapan 1 dan 2	
KP 1	12	23	
KP 2	10	47	
KP 3	7	27	
Jumlah Pertanyaan / Skor Penerapan :	29	97	
Hasil Tingkat Kematangan Pengamanan			
Tingkat Kategori Kematangan	Jumlah Pertanyaan	Skor	Tingkat Status Kematangan
II	11	23	I+
III	13	47	No
IV	3	12	No
V	2	15	No
Total / Skor :	29	41	I+

Berdasarkan Tabel 4, dapat disimpulkan bahwa area Kerangka Kerja Keamanan Informasi Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ saat ini memiliki total nilai evaluasi sebesar 97 poin dan berada pada tingkat kematangan pengamanan I+ yang berarti dalam kondisi awal.

3.2.4 Penilaian Area Pengelolaan Aset Informasi

Penilaian yang ditujukan pada area Pengelolaan Aset Informasi berikut berisikan pertanyaan yang berisikan status “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan / Diterapkan Sebagian”, dan “Dilakukan Secara Menyeluruh” oleh Dinas Komunikasi dan Informatika Kota XYZ. Penilaian dilakukan dengan metode wawancara bersama narasumber, adapun hasil penilaian dapat dilihat pada Tabel 5 berikut.

Tabel 5. Hasil Penilaian Area Pengelolaan Aset Informasi

Bagian V : Pengelolaan Aset Informasi			
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.			
Jumlah Pertanyaan Pengelolaan Aset Informasi		:	38
Hasil Jawaban Narasumber			
Status Penerapan	Jumlah Pertanyaan		
Tidak Dilakukan	3		
Dalam Perencanaan	0		
Dalam Penerapan / Diterapkan Sebagian	23		
Diterapkan Secara Menyeluruh	12		
Total Nilai Evaluasi Pengelolaan Aset Informasi		:	116
Hasil Tingkat Kelengkapan Pengamanan			
Tingkat Kategori Pengamanan (KP)	Jumlah Pertanyaan	r Penerapan 1 dan 2	
KP 1	24	54	
KP 2	10	44	
KP 3	4	18	
Jumlah Pertanyaan / Skor Penerapan :		38	116
Hasil Tingkat Kematangan Pengamanan			
Tingkat Kategori Kembangan	Jumlah Pertanyaan	Skor	Tingkat Status Kematangan
II	29	78	II
III	9	38	No
Total / Skor :		38	46
			II

Berdasarkan Tabel 5, dapat disimpulkan bahwa area Pengelolaan Aset Informasi Dinas Komunikasi dan Informatika Kota XYZ saat ini memiliki total nilai evaluasi sebesar 116 poin dan berada pada tingkat kematangan pengamanan II yang berarti dalam penerapan kerangka kerja dasar.

3.2.5 Penilaian Area Teknologi dan Keamanan Informasi

Penilaian yang ditujukan pada area Teknologi dan Keamanan Informasi berikut berisikan pertanyaan yang berisikan status “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan / Diterapkan Sebagian”, dan “Dilakukan Secara Menyeluruh” oleh Dinas Komunikasi dan Informatika Kota XYZ. Penilaian dilakukan dengan metode wawancara bersama narasumber, adapun hasil penilaian dapat dilihat pada Tabel 6 berikut.

Tabel 6. Hasil Penilaian Area Teknologi dan Keamanan Informasi

Bagian VI : Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

Jumlah Pertanyaan Teknologi		:	26
Hasil Jawaban Narasumber			
Status Penerapan	Jumlah Pertanyaan		
Tidak Dilakukan	1		
Dalam Perencanaan	1		
Dalam Penerapan / Diterapkan Sebagian	7		
Diterapkan Secara Menyeluruh	17		
Total Nilai Evaluasi Teknologi		:	100
Hasil Tingkat Kelengkapan Pengamanan			

Tingkat Kategori Pengamanan (KP)	Jumlah Pertanyaan	Skor Penerapan 1 dan 2	
KP 1	14	37	
KP 2	10	48	
KP 3	2	15	
Jumlah Pertanyaan / Skor Penerapan :	26	100	
Hasil Tingkat Kematangan Pengamanan			
Tingkat Kategori Kematangan	Jumlah Pertanyaan	Skor	Tingkat Status Kematangan
II	14	28	II
III	11	49	II+
IV	1	3	No
Total / Skor :	26	80	II

Berdasarkan Tabel 6, dapat disimpulkan bahwa area Teknologi dan Keamanan Informasi Dinas Komunikasi dan Informatika Kota XYZ saat ini memiliki total nilai evaluasi sebesar 100 poin dan berada pada tingkat kematangan pengamanan II+ yang berarti dalam penerapan kerangka kerja dasar.

3.2.6 Penilaian Suplemen

Penilaian terhadap Suplemen dilakukan untuk menjelaskan dan mengevaluasi mengenai kebijakan keterlibatan pihak ketiga atau pihak eksternal dalam supply chain mulai dari pengelolaan dan penanganan pada suatu layanan untuk manajemen risiko, penggunaan layanan berbasis infrastruktur awan (cloud) dan bentuk pengamanan serta perlindungan terhadap data pribadi pada Diskominfo Kabupaten Paser yang dilakukan dengan metode wawancara bersama narasumber, adapun hasil penilaian dapat dilihat pada Tabel 7 berikut.

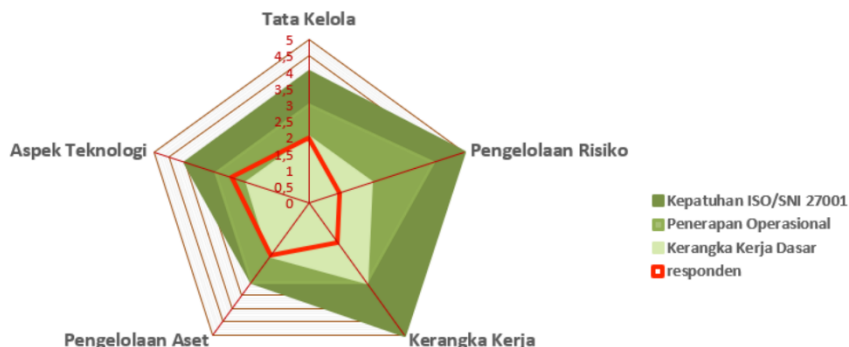
Tabel 7. Hasil Penilaian Suplemen

Bagian VII : Suplemen		
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.		
Jumlah Pertanyaan Suplemen	: 53	
Hasil Jawaban Narasumber		
Status Penerapan	Jumlah Pertanyaan	
Tidak Dilakukan	11	
Dalam Perencanaan	3	
Dalam Penerapan / Diterapkan Sebagian	16	
Diterapkan Secara Menyeluruh	23	
Hasil Tingkat Kelengkapan Pengamanan		
Tingkat Kategori Pengamanan (KP)	Jumlah Pertanyaan	Skor Penerapan 1
KP 1	53	53
Jumlah Pertanyaan / Skor Penerapan :	53	53

Berdasarkan Tabel 7, dapat disimpulkan bahwa Suplemen Dinas Komunikasi dan Informatika Kota XYZ saat ini memiliki total nilai evaluasi Suplemen bagian Pengamanan Keterlibatan Pihak Ketiga sebesar 2,00 atau 67%, Suplemen bagian Pengamanan Layanan Infrastruktur Awan sebesar 1,70 atau 57% dan Suplemen bagian Perlindungan Data Pribadi sebesar 2,06 atau 69%.

3.3 Analisis dan Pembahasan Hasil Penilaian Indeks KAMI 4.2

Pada tahap ini akan menampilkan hasil penilaian akhir dan analisis mengenai kelima area dan suplemen yang telah dilakukan penilaian menggunakan metode Indeks KAMI 4.2 pada Dinas Komunikasi dan Informasi (Diskominfo) Kota XYZ. Tahap ini dilakukan untuk menilai tingkat kematangan dan kelengkapan keamanan informasi untuk mengambil keputusan yang sesuai dengan hasil evaluasi. Adapun hasil evaluasi akhir akan ditampilkan melalui *dashboard* Indeks KAMI 4.2 yang meliputi ketujuh area berdasarkan tingkat kematangan dari setiap area, evaluasi akhir status kesiapan pengamanan informasi, tingkat kelengkapan dalam penerapan ISO/IEC 27001:2013 dan Radar *Chart* Indeks KAMI 4.2 yang dapat dilihat pada Gambar 2 berikut.



Gambar 2. Hasil *Dashboard* Indeks KAMI 4.2 Diskominfo Kota XYZ

Adapun hasil yang ditampilkan dapat diketahui bahwa tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ masih tergolong kurang, yaitu berada pada tingkat I / II+ dengan nilai sebesar 418. Nilai ini didapatkan dari total 5 area pada Indeks KAMI mulai dari area Tata Kelola dengan nilai 87, Pengelolaan Risiko dengan nilai 18, Kerangka Kerja Keamanan Informasi dengan nilai 97, Pengelolaan Aset dengan nilai 116, dan Teknologi dan Keamanan Informasi dengan nilai 100. Dapat diketahui pada *spider chart dashboard*, terdapat area yang dinilai dalam Indeks KAMI belum terpenuhi dan sesuai dengan kepatuhan ISO 27001. Hasil yang didapatkan dalam penilaian menunjukkan bahwa pada area Tata Kelola, Aspek Teknologi, dan Pengelolaan Aset tidak mencapai nilai yang diharapkan. Dapat dilihat pada gambar 3 berikut.



Gambar 3. Hasil Evaluasi Indeks KAMI 4.2 Diskominfo Kota XYZ

Hasil evaluasi dari tingkat kesiapan keamanan informasi yang telah dilakukan pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ mendapatkan skor Kategori Sistem Elektronik (SE) sebesar 26 yang mencapai tingkat ketergantungan “Tinggi” yang dapat dikatakan bahwa penggunaan Sistem Elektronik pada Dinas Komunikasi dan Informatika Kota XYZ merupakan bagian utama dari proses kerja yang berjalan. Adapun tingkat kelengkapan penerapan standar ISO/IEC 27001:2013 pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ mendapatkan skor sebesar 418 yang berarti status tingkat kesiapan amanan informasi atau hasil evaluasi akhir yaitu “Tidak Layak” dalam memenuhi standar ISO/IEC 27001:2013. Sedangkan untuk mendapatkan status kesiapan “Baik”, perusahaan atau instansi harus mendapatkan skor akhir diatas 583. Hasil akhir tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ berada pada tingkat I/II+.

3.4 Pembuatan Rekomendasi Perbaikan Keamanan Informasi

Tahapan pembuatan rekomendasi perbaikan dilakukan untuk memberikan rekomendasi serta saran perbaikan terhadap area yang memiliki status penerapan Tidak Dilakukan dan Dalam Perencanaan pada Dinas Komunikasi dan Informatika Kota XYZ.

3.4.1 Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi

Rekomendasi yang ditujukan pada area tata Kelola Keamanan Informasi berikut berisikan rekomendasi perbaikan yang dapat digunakan pada pertanyaan yang mendapatkan status “tidak dilakukan” dan “dalam perencanaan” oleh Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Rekomendasi berikut dilakukan berdasar pada ISO/IEC 27001:2013, adapun salah satu contoh rekomendasi perbaikan dapat dilihat pada Tabel 8 berikut.

Tabel 8. Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi

No.	Pertanyaan	Status Penerapan	Nilai Skor
2.22	Apakah instansi / perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Perencanaan	3
Rekomendasi Perbaikan ISO/IEC 27001:2013 (18.1 Kesesuaian dengan persyaratan hukum dan kontraktual)			
Menetapkan bahwa instansi / perusahaan membutuhkan penekanan terhadap kebijakan hukum seperti perundang-undangan yang dapat digunakan dan ditegakkan untuk mengatasi segala bentuk gangguan keamanan informasi terhadap aset yang dimiliki oleh instansi / perusahaan.			

3.4.2 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi

Rekomendasi yang terdapat pada area Pengelolaan Risiko Keamanan Informasi berisikan saran dan rekomendasi yang dapat digunakan pada area Pengelolaan Risiko Keamanan Informasi secara keseluruhan dikarenakan area berikut seluruh pertanyaan mendapatkan status “dalam perencanaan” oleh Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Rekomendasi berikut berdasar pada ISO/IEC 27001:2013, adapun salah satu contoh rekomendasi perbaikan dapat dilihat pada Tabel 9 berikut.

Tabel 9. Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi

No.	Pertanyaan	Status Penerapan	Nilai Skor
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan	3
Rekomendasi Perbaikan ISO/IEC 27001:2013 (6.5.1 Keamanan Informasi dalam manajemen proyek)			
Menetapkan bahwa penerapan <i>framework</i> , seperti ISO/IEC 27001 dan melakukan dokumentasi secara berkala. Dengan melakukan dokumentasi instansi / perusahaan dapat memantau insiden keamanan informasi yang terjadi kemudian dapat dilakukan evaluasi lebih lanjut mengenai hasil yang telah didapatkan.			

3.4.3 Rekomendasi Perbaikan Area Kerangka Kerja Keamanan Informasi

Rekomendasi yang ditujukan pada area Kerangka Kerja Pengelolaan Informasi berikut berisikan rekomendasi perbaikan yang dapat digunakan pada pertanyaan yang mendapatkan status “tidak dilakukan” dan “dalam perencanaan” oleh Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Rekomendasi berikut dilakukan berdasar pada ISO/IEC 27001:2013. Adapun salah satu contoh rekomendasi perbaikan dapat dilihat pada Tabel 10 berikut.

Tabel 10. Rekomendasi Perbaikan Area Kerangka Kerja Keamanan Informasi

No.	Pertanyaan	Status Penerapan	Nilai Skor
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (<i>disaster recovery plan</i>) sudah dilaksanakan sesuai jadwal?	Dalam Perencanaan	3

Rekomendasi Perbaikan ISO/IEC 27001:2013 (17.1.2 Mengimplementasikan keberlangsungan keamanan informasi)

Menetapkan bahwa setelah dilakukan penetapan kebijakan dan prosedur yang terdapat di dalam BCP dan DRP, selanjutnya pihak dari manajemen keamanan informasi dapat melakukan uji coba perencanaan pemulihan bencana terhadap layanan TIK berdasarkan penjadwalan yang telah disepakati bersama.

3.4.4 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi

Rekomendasi yang ditujukan pada area Pengelolaan Aset Informasi berikut berisikan rekomendasi perbaikan yang dapat digunakan pada pertanyaan yang mendapatkan status “tidak dilakukan” oleh Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Rekomendasi berikut dilakukan berdasar pada ISO/IEC 27001:2013, adapun salah satu contoh rekomendasi perbaikan dapat dilihat pada Tabel 11 berikut.

Tabel 11. Rekomendasi Perbaikan Area Pengelolaan Aset Informasi

No.	Pertanyaan	Status Penerapan	Nilai Skor
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi?	Tidak Dilakukan	0

Rekomendasi Perbaikan ISO/IEC 27001:2013 (9.2.2 Penyedia Akses Pengguna)

Menetapkan bahwa organisasi dapat membuat peraturan / tata tertib mengenai pemberian ijin tertulis oleh pemilik data pribadi, sehingga pemilik data pribadi dapat mengakses atau melihat data pribadinya.

3.4.5 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi

Rekomendasi yang ditujukan pada area Teknologi dan Keamanan Informasi berikut berisikan rekomendasi perbaikan yang dapat digunakan pada pertanyaan yang mendapatkan status “tidak dilakukan” dan “dalam perencanaan” oleh Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Rekomendasi berikut dilakukan berdasar pada ISO/IEC 27001:2013, adapun salah satu contoh rekomendasi perbaikan dapat dilihat pada Tabel 12 berikut.

Tabel 12. Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi

No.	Pertanyaan	Status Penerapan	Nilai Skor
6.22	Apakah adanya laporan penyerangan virus/ <i>malware</i> yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Perencanaan	2

Rekomendasi Perbaikan ISO/IEC 27001:2013 (12.2.1 Kendali terhadap *malware*)

Menetapkan bahwa instansi harus mempunyai pencatatan jejak rekam dari proses pendeteksian *malware* dan pemulihan yang dilakukan pada aplikasi wajib dilakukan secara rutin dan berkelanjutan.

3.4.6 Rekomendasi Perbaikan Suplemen

Rekomendasi yang ditujukan pada area Suplemen berisikan rekomendasi perbaikan yang dapat digunakan pada pertanyaan yang mendapatkan status “tidak dilakukan” dan “dalam perencanaan” oleh Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Rekomendasi berikut dilakukan berdasar pada ISO/IEC 27001:2013, adapun salah satu contoh rekomendasi perbaikan dapat dilihat pada Tabel 13 berikut.

Tabel 13. Rekomendasi Perbaikan Suplemen

No.	Pertanyaan	Status Penerapan	Nilai Skor
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Tidak Dilakukan	0
Rekomendasi Perbaikan ISO/IEC 27001:2013 (14.2.7 Pengembangan alih daya)			
Menetapkan bahwa pihak ketiga harus menerapkan pengendalian risiko mengenai alih daya untuk membantu mengurangi atau menghindari risiko yang akan menimpa pihak ketiga. Pengendalian risiko ini dapat berupa dokumen yang disetujui oleh pihak ketiga.			

4. KESIMPULAN

Kesimpulan yang dapat diperoleh dari penelitian terkait evaluasi keamanan informasi menggunakan Indeks KAMI 4.2 pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ yaitu penilaian pada kategori Sistem Elektronik (SE) sebesar 26 poin dari 50 yang termasuk ke dalam kategori “Tinggi”. Adapun hasil keseluruhan penilaian keenam area sebesar 418 poin dari total keseluruhan 645 poin, sehingga didapatkan hasil evaluasi akhir keamanan informasi pada Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ berada pada status Tingkat Kesiapan “Tidak Layak” dalam memenuhi standar atau kontrol ISO/IEC 27001:2013 dengan Tingkat Kematangan berada pada tingkat I/II+. Rekomendasi diberikan kepada seluruh area keamanan informasi yang mendapatkan penilaian “Dalam Perencanaan” dan “Tidak Dilakukan” oleh Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ. Pada Area Tata Kelola Keamanan Informasi terdapat 2 rekomendasi, pada Area Pengelolaan Risiko terdapat 16 rekomendasi, pada Area Kerangka Kerja Keamanan Informasi terdapat 10 rekomendasi, pada Area Pengelolaan Aset terdapat 3 rekomendasi, pada Area Teknologi dan Keamanan Informasi terdapat 2 rekomendasi, dan pada Area Suplemen terdapat 14 rekomendasi. Saran dan Rekomendasi perbaikan diberikan dengan mengacu pada standar atau klausul ISO/IEC 27001:2013.

DAFTAR PUSTAKA

- [1] Badan Pusat Statistik, “Statistik Telekomunikasi Indonesia 2021,” 2021.
- [2] Rahmawati, F. H., & Adityarini, E. (2021). Sistem Informasi Persediaan Barang pada CV. Anak Teladan. *Jurnal Sistem Informasi STMIK Antar Bangsa*, *X*, 2.
- [3] Badan Siber dan Sandi Negara Republik Indonesia, Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2021. 2021, pp. 10–27.
- [4] Badan Siber dan Sandi Negara Republik Indonesia, "Indeks KAMI Versi 4.2," diambil kembali dari "Indeks KAMI": <https://bssn.go.id/indeks-kami/>, 2019.