Analisa Tingkat Kematangan Penerapan Keamanan Informasi Pemerintah Kota Bitung Menggunakan Indeks KAMI (Studi Kasus : Dinas Komunikasi dan Informatika Kota Bitung)

Aryani C. D. Tinungki[1)], Steven R. Sentinuwo[)], Stanley D.S. Karouw [3)]
Teknik Elektro Fakultas Teknik Univesitas Sam Ratulangi Manado, Jl. Kampus Bahu-Unsrat Manado, 95115
E-mail : 13021106197@student.unsrat.ac.id[1)], steven@unsrat.ac.id [2)], stanley.karouw@unsrat.ac.id [3)]

Abstract* – *The National Cyber and Crypto Agency, in the annual report of the Government Computer Security Incident Response Team (Gov-CSIRT) Indonesia, received 237 reports of total cyber attacks in 2019 and vulnerabilities were the most complained of cyber complaints. (Annual Report, GOV-CSIRT Indonesia, 2019). Many government agencies provide electronic services in order to carry out the mandate of an Electronic-Based Government System but have not implemented an Information Security Management System (ISMS). (GOV-CSIRT INDONESIA Services, 2019). Bitung City is a city that is currently working on technology-based government management. According to research conducted by the Manado Information and Communication Research and Development Center (BPPKI), regarding the management of information architecture planning in one of the government agencies, namely the Bitung City Information and Communication Agency, the Bitung City Government does not yet have a standardization for the use of information and communication technology system governance. (ICT). Information Security Index (WE Index) as a tool compiled by the Information Security Directorate Team of the Ministry of Communication and Information Technology to measure, analyze and evaluate the level of readiness for implementing information security based on compliance with the criteria in SNI ISO / IEC 27001. This evaluation tool is a tool to provide a description of the conditions of readiness (completeness and maturity) of the information security framework at the head of the agency. The results of the measurement obtained a score of information security maturity level in the Bitung City Government, which can be used as an evaluation to improve the level of information security of the Bitung City Government in the future.

Keywords: Index KAMI Information Security, ISMS.

Abstrak — Badan Siber dan Sandi Negara dalam laporan tahunan Government Computer Security Incident Response Team (Gov-CSIRT) Indonesia, mendapat laporan 237 total serangan siber ditahun 2019 dan kerentanan menjadi aduan siber yang paling banyak diadukan. (Laporan Tahunan, GOV-CSIRT Indonesia, 2019). Banyak instansi pemerintah yang memberikan layanan elektronik dalam rangka menjalankan amanat Sistem Pemerintah Berbasis Elektronik tetapi belum menerapkan Sistem Manajemen Keamanan Informasi (SMKI). (Layanan GOV-CSIRT INDONESIA, 2019). Kota Bitung adalah kota yang sementara mengupayakan pengelolaan pemerintahan berbasis teknologi. Menurut penelitian yang dilakukan Balai pengkajian dan pengembangan komunikasi dan informatika (BPPKI) manado, tentang tata kelola perencanaan arsitektur informasi pada salah satu instansi pemerintah yaitu Dinas Komunikasi dan Informatika Kota Bitung, Pemerintah Kota Bitung belum memiliki standarisasi untuk penggunaan tata kelola sistem teknologi informasi dan komunikasi (TIK). Indeks Keamanan Informasi (Indeks KAMI) sebagai alat bantu yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika untuk mengukur, menganalisa dan mengevaluasi tingkat kesiapan penerapan keamanan informasi berdasarkan kesesuaian dengan kriteria pada SNI ISO/IEC 27001. Alat evaluasi ini sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada pimpinan instansi. Hasil dari pengukuran didapatkan skor tingkat kematangan keamanan informasi di Pemerintah Kota Bitung, yang bisa digunakan sebagai evaluasi untuk meningkatkan tingkat keamanan informasi Pemerintah Kota Bitung kedepannya.

Kata kunci— Indeks Kami, Keamanan Informasi, SMKI

I. PENDAHULUAN

Bagi organisasi pemerintah, menerapkan teknologi informasi dan komunikasi yang baik dan optimal adalah harapan dalam upaya untuk mengembangkan penyelenggaraan pemerintahan berbasiskan elektronik, meningkatkan transparansi dan kualitas pelayanan kepada masyarakat. Informasi menjadi hal yang sangat penting apalagi untuk instansi/organisasi yang bergerak dalam bidang pelayanan publik, maka menjadi hal yang perlu diperhatikan juga adalah keamanan dari informasi itu sendiri.

Badan Siber dan Sandi Negara dalam laporan tahunan *Government Computer Security Incident Response Team (Gov-CSIRT)* Indonesia, mendapat laporan 237 total serangan siber ditahun 2019 dan kerentanan menjadi aduan siber yang paling banyak diadukan. (Laporan Tahunan, GOV-CSIRT Indonesia, 2019). Banyak instansi pemerintah yang memberikan layanan elektronik dalam rangka menjalankan amanat Sistem Pemerintah Berbasis Elektronik tetapi belum menerapkan Sistem Manajemen Keamanan Informasi (SMKI). (Layanan GOV-CSIRT INDONESIA, 2019).

Kota Bitung adalah kota yang sementara mengupayakan pengelolaan pemerintahan berbasis teknologi. Saat ini pemerintah kota Bitung lebih berfokus kepada membuat inovasi-inovasi dalam bidang teknologi informasi untuk menunjang pelayanan pemerintahan. Menurut penelitian yang dilakukan Balai pengkajian dan pengembangan komunikasi dan informatika (BPPKI) manado, tentang tata kelola perencanaan arsitektur informasi pada salah satu instansi pemerintah yaitu Dinas Komunikasi dan Informatika Kota Bitung, didapati bahwa pemerintah Kota Bitung belum memiliki standarisasi untuk penggunaan tata kelola sistem teknologi informasi dan komunikasi (TIK). Beberapa instansi yang ada di pemerintahan kota Bitung harus berupaya meningkatkan kinerja mereka dalam mengelola TIK secara baik dan benar. Sebelum standarisasi diterapkan, perlu dilakukan evaluasi keamanan sistem informasi di lingkup kerja demi mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi dengan menggunakan Indeks Keamanan Informasi.

Indeks Keamanan Informasi (Indeks KAMI) sebagai alat bantu yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika untuk mengukur, menganalisa dan mengevaluasi tingkat kesiapan penerapan keamanan informasi berdasarkan kesesuaian dengan kriteria pada SNI ISO/IEC 27001, yang fungsinya sebagai indikator penerapan keamanan informasi secara nasional di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan dan efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada pimpinan instansi. Hasil dari pengukuran ini akan didapatkan skor tingkat kematangan keamanan informasi di Pemerintah Kota Bitung, yang nantinya bisa digunakan sebagai evaluasi untuk meningkatkan tingkat keamanan informasi Pemerintah Kota Bitung kedepannya.

A. Penelitian Terkait

1. I Gede Putu K. J Program Studi Sistem Informasi STMIK Primakara (2019). Analisa Tingkat Kesiapan Penerapan Keamanan Teknologi Informasi Dalam Pelaksanaan e-Government Berbasis Indeks Keamanan Informasi (KAMI) Studi Kasus Pemerintahan Kota Kediri. Tujuan dari penelitian ini yaitu mengukur ketiga aspek dalam sistem seperti aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*), guna meningkatkan pengelolaan sistem yang dimiliki oleh pemerintahan Kota Kediri. Perbedaan penelitian ini dengan penelitian saya terletak pada studi kasus yang diambil. Pada penelitian ini mengambil studi kasus di pemerintahan Kota Kediri sedangkan saya mengambil penelitian dengan studi kasus di pemerintahan Kota Bitung. [5]
2. Muh. Faturachman Husin, Hans F. Wowor, Stanley D.S. Karouw (2017). Implementasi Indeks KAMI di Universitas Sam Ratulangi. Penelitian ini bertujuan untuk mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi dengan mengevaluasi keamanan sistem informasi pada unit kerja Universitas Sam Ratulangi yang mempunyai tugas dan kewajiban untuk mengelola dan memberikan informasi. Perbedaan penelitian ini dengan penelitian saya yaitu terletak pada studi kasus dan versi Indeks KAMI yang digunakan. Penelitian ini mengambil studi kasus di Universitas Sam Ratulangi dan menggunakan Indeks KAMI versi 2.5. Sedangkan pada penelitian saya mengambil studi kasus pada pemerintahan Kota Bitung dengan menggunakan Indeks KAMI versi 4.1. [2]
3. Albar Agista (2018). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi studi kasus Sekretariat DPRD Kota Cimahi. Tujuan dari penelitian ini adalah untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Dengan memberikan hasil seperti sebuah usulan perbaikan bagi bagian IT dan Multimedia Sekretariat DPRD Kota Cimahi berdasarkan hasil penilaian menggunakan Indeks KAMI dan usulan dari ISO27002. Penelitian ini sama-sama menggunakan tools Indeks KAMI versi 3.1 perbedaanya adalah pada studi kasus yakni pada skretariat DPRD Kota Cimahi sedangkan penelitian saya pada Pemerintah Kota Bitung. [6]
4. Mark Wolden, Raul Valverde, Malleswara Talla (2015). *"The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System". BAE System, Saudi Arabia, John Molson School of Business, Concordia University, Montreal.* Pada penelitian ini menjelaskan bahwa penulis menggunakan COBIT 5 untuk memberikan kerangka kerja langkah-langkah penerapan keamanan sistem informasi yang bisa dilakukan oleh suatu organisasi dalam mengamankan sistem informasi yang ada. Sama halnya dengan penelitian ini, penelitian saya pun bertujuan memberikan gambaran tingkat kematangan serta gambaran kerangka kerja penerapan keamanan informasi pada suatu instansi/organisasi, tetapi menggunakan alat ukur lain yaitu Indeks Keamanan Sistem Informasi (KAMI). [4]
5. Tedi Agoan, Hans F. Wowor dan Stanley D.S. Karouw (2017). Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi dan Informatika Kota

Manado Menggunakan Framework COBIT 5 Domain Evaluate, Direct, Monitor (EDM) dan Deliver, Service, and Support (DSS). Penelitian ini bertujuan untuk mengukur kematangan Teknologi Informasi berdasarkan COBIT 5 serta Rekomendasi yang dapat ditindaklanjuti dalam instansi untuk melakukan perbaikan dimasa yang akan datang. Perbedaan penelitian ini dengan penelitian saya terletak pada alat ukur yang digunakan. Pada penelitian ini menggunakan alat ukur COBIT 5. Sedangkan pada penelitian saya menggunakan alat ukur Indeks KAMI. Persamaan penelitian ini dengan penelitian saya adalah melakukan penelitian tentang audit atau analisa. [1]

6. Novita Ester Wowor, Steven R. Sentinuwo, Stanley D.S. Karouw (2018). Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks KAMI. Tujuan dari penelitian ini yaitu mengukur, menganalisa, dan mengevaluasi keamanan informasi di seluruh unit-unit kerja demi mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi. Persamaan penelitian ini dengan penelitian saya adalah sama-sama melakukan penelitian tentang audit atau analisa, sama-sama menggunakan tools indeks KAMI versi 3.1 sebagai alat ukur evaluasi keamanan informasi tetapi berbeda studi kasus yakni pada pemerintahan Kota Manado sedangkan saya pada pemerintahan Kota Bitung. [3]

B. Keamanan Informasi

Keamanan sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

Keamanan sistem informasi memiliki 4 tujuan yang mendasar yaitu :

a). Kerahasiaan (*Confidentiality*)

Keamanan informasi menjamin bahwa hak akses suatu informasi hanya dapat diakses oleh pemilik akses informasi, keutuhan serta konsistensi data pada sistem tersebut tetap terjaga.

b). Ketersediaan (*Availability*)

Menjamin pengguna yang sah untuk selalu dapat mengakses informasi dimanapun dan kapanpun oleh pemilik atau pengguna informasi tanpa terjadi gangguan atau perubahan informasi tersebut.

c). Integritas (*Integrity*)

Menjamin konsistensi dan kelengkapan informasi tersebut sesuai aslinya dari kerusakan atau ancaman pihak-pihak yang tidak bertanggungjawab yang berusaha merubah data tersebut.

d). Pengguna yang sah (*Legitimate Use*).

Menjamin kepastian bahwa sumberdaya tidak dapat digunakan oleh orang yang tidak berhak.

C. Sistem Manajemen Keamanan Informasi (SMKI)

Sistem keamanan informasi adalah kumpulan dari prosedur dan kebijakan yang terkait dengan risiko – risiko. SMKI bertujuan untuk meminimalisir resiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak yang akan ditimbulkan dari pelanggaran keamanan. Sejak tahun 2005, International Organization for Standardization (ISO) atau Organisasi Internasional untuk Standarisasi telah mengembangkan sejumlah standar tentang Information Security Management Systems (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan. Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah ISO/IEC 27001.

ISO 27001 adalah sebuah dokumen standar sistem manajemen keamanan informasi (SMKI) atau *information security manajemen system (ISMS)* yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi atau instansi dalam mengimplementasikan konsep-konsep keamanan informasi. Dengan kata lain ISO 27001 memberikan spesifikasi atau persyaratan yang harus dipenuhi untuk membangun sistem manajemen keamanan informasi.

Keuntungan mengimplementasikan standar ISO/IEC 27001 adalah :

1) Mengurangi kemungkinan pelanggaran keamanan di lingkungan teknologi informasi, karena standar ini menyediakan model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan informasi dan seluruh infrastruktur atau sistem sarana parasarana yang berkaitan langsung dengan pertukaran atau penyimpan data atau informasi penting tersebut.
2) Menunjukkan komitmen kerahasiaan data.
3) Meminimalisir resiko dan konsekuensi yang berdampak pada biaya yang harus dikeluarkan apabila terjadi bencana atau ancaman.
4) Menjadi nilai tambah bagi organisasi sehingga dapat memberi pengaruh positif dalam hal citra perusahaan, nilai, dan persepsi yang baik dari pihak lain.
5) Meningkatkan kepercayaan pelanggan, pihak ketiga dan seluruh stakeholder yang ada terhadap pelayanan yang diberikan oleh organisasi.
6) Dengan sertifikasi ISO 27001 itu artinya sebuah organisasi telah menunjukkan tata kelola yang baik dalam penanganan informasi dan dianggap telah

sesuai dengan peraturan hukum dan undang-undang yang berlaku dalam suatu negara. Seperti undang-undang ITE dan permen kominfo no 4 tahun 2016 tentang sistem manajemen pengamanan informasi.

7) Salah satu standar pengamanan informasi yang diakui diseluruh dunia dan dapat diintegrasikan dengan sistem manajemen atau framework tata kelola lainnya seperti : ISO 9000, ISO 14000, ISO 20000, ISO 38500, ITIL, COBIT, dan yang lainnya.
8) Membantu organisasi mendeteksi celah kerentanan yang dapat mengancam kebocoran informasi.
9) Membuat pelaksanaan setiap proses menjadi lebih sistematis dan merubah budaya kerja organisasi. Ini adalah tujuan dari sebuah sistem manajemen.
10) Menjadi lebih mudah bagi organisasi karena memiliki kontrol terkait keamanan informasi terhadap lingkungan dan proses bisnis.

ISO 27001 menjadi acuan pengambilan keputusan untuk keberlangsungan bisnis jangka panjang dengan mendapatkan pengakuan bahwa sebuah organisasi layak dalam mengolah aset berharga yaitu informasi.

D. Indeks Keamanan Informasi

1. Pengertian Indeks KAMI

Indeks Keamanan Informasi (Indeks KAMI) adalah sebagai alat bantu yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika untuk mengukur, menganalisa dan mengevaluasi tingkat kesiapan penerapan keamanan informasi berdasarkan kesesuaian dengan kriteria pada SNI ISO/IEC 27001, yang fungsinya sebagai indikator penerapan keamanan informasi secara nasional di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan dan efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada pimpinan instansi/perusahaan.

Alat evaluasi Indeks KAMI ini dapat digunakan oleh organisasi dengan skala nasional, maupun yang berukuran kecil. Penggunaan di Instansi pemerintah dapat dilakukan di tingkat pusat maupun satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggungjawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya

Gambar 1. *Radar chart Indeks KAMI*

Untuk proses penilaian menggunakan Indeks KAMI versi 4.1 dilakukan melalui sejumlah pertanyaan di masing-masing area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013 dibawah ini :

a. Kategori Sistem Elektronik yang digunakan Instansi.
b. Tata Kelola Keamanan Informasi.
c. Pengelolaan Risiko Keamanan Informasi.
d. Kerangka Kerja Keamanan Informasi.
e. Pengelolaan Aset Informasi.
f. Teknologi dan Keamanan.
g. Suplemen.

Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran. Pertanyaan dikelompokkan untuk 2 keperluan :

1) Berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Responden diminta untuk memberi tanggapan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan diberi label "1"), efektifitas dan konsistensi penerapannya (label "2"), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label "3"). Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2013.

2) Berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga. Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai:

- Tingkat I - Kondisi Awal
- Tingkat II - Penerapan Kerangka Kerja Dasar
- Tingkat III - Terdefinisi dan Konsisten
- Tingkat IV - Terkelola dan Terukur
- Tingkat V – Optimal

Indeks KAMI sebaiknya digunakan 2X dalam setahun untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan

yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu.

II. METODE PENELITIAN

Pada bab ini menjelaskan alur penelitian dimana terdapat rincian tentang bahan atau materi, alat, urutan langkah-langkah yang dibuat secara sistematis, logis sehingga dapat dijadikan pedoman yang jelas dan mudah untuk menyelesaikan permasalahan, analisis hasil dan kesulitan-kesulitan yang dihadapi. Untuk lokasi penelitian dilakukan di Pemerintahan Kota Bitung. Urutan langkah-langkah penelitian penyelesaian masalah dapat dilihat pada tabel dibawah ini (Novita Ester Wowor *et al., 2018 :5*) :

TABEL 1. ALUR PENELITIAN

No	Tahap	Input	Proses	Output
1.	Persiapan	a. Telaah Dokumen bisnis b. Wawancara Kabid. Pengembangan Sistem Informatika dari Dinas Kominfo Kota Bitung c. Asistensi dengan Dosen Pembimbing	Studi Literatur	Identifikasi masalah Pemerintah Kota Bitung
2.	Desain Penelitian	a. Identifikasi Organisasi: Visi, Misi, Struktur Organisasi Renstra TIK Pemerintah Kota Bitung b. Asistensi dengan Dosen Pembimbing	a. Studi Literatur b.Wawancara	Batasan Masalah
3.	Pengumpulan Data	a. Populasi dan Sampel b. Asistensi dengan Dosen Pembimbing	Kuisioner dan Wawancara	Data Mentah
4.	Analisa Data	a. Analisa Data Kuisioner b. Asistensi dengan Dosen Pembimbing	a. Data Cleansing b. Analisa Tingkat Kematangan	Skor Akhir dan Grafik Tingkat Kematangan
5.	Penyusunan Laporan	a. Grafik Tingkat Kematangan b. Asistensi dengan Dosen Pembimbing untuk area yang dinilai kurang	Kesimpulan dan Saran Perbaikan	a. Laporan Hasil Penelitian b. Presentasi Hasil Penelitian

Pada tahap pertama persiapan, salah satu cara mengumpulkan informasi yaitu peneliti melakukan telaah dokumen bisnis dengan mengumpulkan dan mempelajari dokumen renstra TIK yang berisi visi, misi, tujuan, kebijakan, dan program dan kegiatan yang menyangkut TIK pada Pemerintah Kota Bitung. Kemudian bertemu dan wawancara dengan kepala bidang Pengembangan Sistem Informatika di Dinas Kominfo Kota Bitung dan Dosen Pembimbing untuk proses penelitian. Meninjau kembali paper penelitian yang pernah dilakukan sebelumnya untuk menemukan teori-teori dasar yang terkait dengan permasalahan sehingga output yang didapat yaitu identifikasi masalah TIK pada Pemerintah Kota Bitung khususnya pada Dinas Komunikasi dan Informatika Kota Bitung.

Pada tahap kedua, peneliti melakukan identifikasi organisasi yang berisi tentang visi, misi , renstra TIK Pemerintah Kota Bitung. Melakukan wawancara dengan dosen pembimbing untuk mendapatkan desain penelitian yang akan dilakukan dalam penelitian ini dan melakukan kembali studi literatur. Hasil yang didapatkan dalam tahap desain penelitian yaitu batasan masalah agar penelitian tidak terlalu luas dan mengarah pada objek penelitian.

Tahapan selanjutnya yaitu tahap pengumpulan data, dimana populasi dalam penelitian ini adalah seluruh penyelenggara layanan TIK di SKPD Pemerintah Kota Bitung khususnya pada Dinas Komunikasi dan Informatika Bitung. Untuk sampel menggunakan *accidental sampling* dimana menjalankan kuesioner dan melakukan wawancara kepada responden yang berada dilokasi pada saat penelitian berlangsung.

Tahapan keempat yaitu tahap analisa data, dimana akan dilakukan analisa data kuesioner dari data-data hasil penyebaran kuesioner dikumpulkan dan dilakukan evaluasi terkait gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi di Pemerintah Kota Bitung khususnnya Dinas Komunikasi dan Informatika Kota Bitung yang nantinya akan di proses menjadi data cleansing yaitu proses analisa kualitas dari suatu data dengan cara mengubah, mengoreksi data-data yang salah guna menghasilkan data berkualitas tinggi. Kemudian akan dilakukan analisa tingkat kematangan untuk mendapatkan hasil tingkat kelengkapan dan tingkat kematangan keamanan informasi pada Pemerintah Kota Bitung.

Pada tahap kelima yaitu penyusunan laporan, berdasarkan grafik tingkat kematangan yang diperoleh pada tahap sebelumya akan diberikan kesimpulan sebagai pernyataan singkat tentang hasil analisis deskripsi dan pembahasan tentang hasil tes hipotesis tersebut. Kesimpulan

berisi jawaban atas pertanyaan yang tercantum dalam bagian rumusan masalah. Dan juga akan diberikan saran perbaikan untuk area yang dinilai kurang dari penelitian yang telah dilakukan. Kemudian Saran hanya berisi rekomendasi yang dirumuskan oleh peneliti namun bukan untuk menjawab permasalahan dalam pokok penelitian. Saran dirumuskan berdasarkan penelurusan yang menurut penulis dapat bermanfaat secara praktis maupun bermanfaat bagi pengembangan ilmu pengetahuan.

III. HASIL DAN PEMBAHASAN

Penelitian tingkat kematangan keamanan informasi pada pemerintah Kota Bitung (Dinas Komunikasi dan Informatika Kota Bitung) dilakukan berdasarkan Indeks KAMI versi 4.1. Alat ukur ini terdiri dari 194 (seratus sembilan puluh empat) pertanyaan yang dibagi menjadi 7 Bagian. Bagian I responden diminta untuk mendefinisikan tentang kategori sistem elektronik yang ada dan pada bagian II – bagian VII responden diminta untuk menjawab tentang tingkat pengelolaan kematangan pengelolaan informasi.

TABEL 2. REKAPITULASI DATA HASIL KUESIONER

AREA	SKOR
Kategori Sistem Elektronik	15
Tata Kelola Keamanan Informasi	35
Pengelolaan Risiko Keamanan Informasi	18
Kerangka Kerja Pengelolaan Keamanan Informasi	34
Pengelolaan Aset Informasi	54
Teknologi dan Keamanan Informasi	59

Gambar 2. Tingkat Kelengkapan Penerapan SMKI

Berdasarkan informasi pada gambar 2 dapat disimpulkan bahwa :

1) Dari tingkat kelengkapan penerapan SMKI, Pemerintah Kota Bitung (Dinas Komunikasi dan Informatika) berada pada level "Tidak Layak", dengan total skor 200, yang merupakan jumlah dari seluruh skor rata-rata disetiap area keamanan informasi yang dievaluasi. Itu artinya sistem manajemen keamanan informasi di pemerintah Kota Bitung (Dinas Komunikasi dan Informatika) masih sangat kurang.

2) Berdasarkan hasil pengumpulan data, tingkat kematangan SMKI pemerintah Kota Bitung (Dinas Komunikasi dan Informatika) adalah Tk.Kematangan I yaitu pada Pengelolaan risiko keamanan informasi dan kerangka kerja keamanan informasi dan untuk Tk.Kematangan I+ pada bagian tata kelola keamanan informasi, pengelolaan aset dan teknologi keamanan informasi.

Gambar 3. Radar Tingkat Kelengkapan Penerapan SMKI

Pada diagram radar gambar 3, diagram yang membentuk pola garis orange merupakan kondisi SMKI Pemerintah Kota Bitung (Dinas Komunikasi dan Informatika Kota Bitung) berdasarkan hasil pengisian kuesioner oleh para informan, yaitu :

1) Dari kelima area keamanan informasi yang diamati, terlihat bahwa Pemerintah Kota Bitung memiliki aspek teknologi dan tata kelola yang lebih baik dibanding area keamanan lainnya (mendekati standar penerapan operasional).
2) Area kerangka kerja mencapai kerangka kerja dasar. Kecuali pada area pengelolaan aset dan pengelolaan risiko terlihat bahwa Pemerintah Kota Bitung tidak mencapai kerangka kerja dasar. Hal ini perlu diperbaiki untuk meningkatkan pengamanan informasi.

Skor tata kelola keamanan informasi yaitu 35 dengan tingkat kematangan I+. Dari total 22 pertanyaan yang diajukan pada area tata kelola keamanan informasi, 0 diantaranya direspon "Tidak Dilakukan", 8 diantaranya direspon "Dalam Perencanaan", 8 direspon "Dalam penerapan atau diterapkan sebagian", dan 6 direspon "Diterapkan secara menyeluruh".

Skor pengelolaan risiko keamanan informasi yaitu 18 dengan tingkat kematangan I. Dari total 16 pertanyaan yang diajukan, 0 diantaranya direspon "Tidak dilakukan", 10 direspon "Dalam perencanaan", 4 direspon "Dalam penerapan

atau diterapkan sebagian" dan 2 direspon "Diterapkan secara menyeluruh".

Skor kerangka kerja pengelolaan keamanan informasi yaitu 34 dengan tingkat kematangan I. Dari total 29 pertanyaan yang diajukan, 0 direspon"Tidak dilakukan", 12 direspon "Dalam perencanaan", 10 direspon "Dalam penerapan atau diterapka sebagian", dan 7 direspon "diterapkan secara menyeluruh".

Skor pengelolaan aset informasi yaitu 54 dengan tingkat kematangan I+. Dari total 38 pertanyaan yang diajukan, 0 direspon " Tidak dilakukan", 24 direspon "Dalam perencanaan", 10 direspon "Dalam penerapan atau diterapkan sebagian", dan 4 direspon " Diterapkan secara menyeluruh".

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian yang sudah dilakukan untuk mengetahui tingkat kematangan penerapan keamanan informasi pada pemerintah Kota Bitung dalam hal ini Dinas Komunikasi dan Informatika Kota Bitung maka kesimpulan dari penelitian ini adalah :

1. Indeks Keamanan Informasi (Indeks KAMI) memberikan gambaran kesiapan (kelengkapan dan kematangan) kerangka kerja informasi pada pemerintah Kota Bitung dan bisa digunakan untuk meningkatkan tingkat keamanan informasi pada pemerintah Kota Bitung (Dinas Komunikasi dan Informatika Kota Bitung).
2. Dalam Kategori Sistem Elektronik, tingkat ketergantungan pemerintah Kota Bitung (Dinas Komunikasi dan Informatika Kota Bitung) terhadap TIK adalah tergolong tinggi tetapi tingkat kematangan dalam menerapkan keamanan informasi justru tergolong rendah. Pada aspek teknologi dan tata kelola jauh lebih baik dan untuk beberapa area lainnya perlu adanya perbaikan yaitu pada aspek pengelolaan risiko, pengelolaan aset dan kerangka kerja pengelolaan keamanan informasi.
3. Skor akhir Indeks KAMI di pemerintah Kota Bitung (Dinas Komunikasi dan Informatika Kota Bitung) adalah 200 dari skor maksimum 645 atau 31,1%. Dengan skor ini, pemerintah Kota Bitung lebih khusus Dinas Komunikasi dan Informatika Kota Bitung tergolong belum mencapai standar keamanan yang baik.

B. Saran

Berikut adalah saran yang dapat disampaikan dalam tugas akhir ini:

1. Membuat perencanaan program untuk meningkatkan keamanan informasi secara keseluruhan baik dalam area kerangka kerja, tata kelola, pengelolaan aset, pengelolaan risiko, dan teknologi keamanan informasi dan diberlakukan terus menerus.
2. Melaksanakan program sosialiasi, seminar dan juga pelatihan kepada sumber daya manusia yang ada tentang keamanan informasi dan betapa pentingnya sistem manajemen dari keamanan informasi tersebut.
3. Mengambil langkah yang pasti untuk dilakukan dengan mulai menerapkan pengamanan meski baru dalam area teknis sekalipun.

V. KUTIPAN

[1] T. S. Agoan, H. Wowor, S. D. Karouw. 2017. 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).. *E-Journal Teknik Informatika*, Vol 10, No.1

[2] M. F.Husin, H. Wowor, S. D. Karouw. 2017. Implementasi Indeks KAMI di Universitas Sam Ratulangi. *E-Journal Teknik Informatika* Vol 12, No.1.

[3] N. E. Wowor, S. R. Sentinuwo, S. D. Karouw. 2018. Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks KAMI. *Jurnal Teknik Informatika* Vol 13, No.4

[4] *Mark Wolden, Raul Valverde, Malleswara Talla. 2015.*

[5] I Gede P. K.Juliharta. 2019. Analisa Tingkat Kesiapan Penerapan Keamanan Teknologi Informasi Dalam Pelaksanaan e-Government Berbasis Indeks Keamanan Informasi (KAMI). *Jurnal Teknologi Informasi dan Komputer*, Vol .5 No.1.

[6] A. Agista. 2018. Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI). Studi Kasus Sekretariat DPRD Kota Cimahi.

Sekilas tentang penulis, nama Aryani Cintia Devi Tinungki lahir di Siau pada tanggal 12 Maret 1996, anak pertama dari dua bersaudara dari pasangan suami/istri Bapak Abram Irfan Tinungki dan Ibu Litsly Megrits Manguntika. Adapun riwayat pendidikan penulis yaitu Sekolah Dasar di SD St.Stephanus Aertembaga (2001 - 2007), lalu melanjutkan pendidikan Sekolah Menengah Pertama di SMP Negeri 7 Bitung (2007 - 2010), kemudian melanjutkan pendidikan di Sekolah Menengah Kejuruan Yaitu SMK Negri 1 Bitung (2010 - 2013). Pada tahun 2013 penulis melanjutkan pendidikan ke salah satu perguruan tinggi yang berada di Kota Manado yaitu Universitas Sam Ratulangi Manado dengan mengambil Program Studi Strata Satu (S-1) Teknik Informatika di Jurusan Teknik Elektro Fakultas Teknik. Penulis pernah mengambil bagian dalam organisasi dan kepanitiaan yang ada yaitu pernah menjadi anggota Himpunan Mahasiswa Elektro (HME), Tim kerja Unit Pelayanan Kerohanian Kristen Fakultas Teknik Unsrat, dan Anggota Paduan Suara Blue Choir Fakultas Teknik Unsrat.

Penulis membuat Skripsi demi memenuhi syarat Sarjana (S1) dengan judul penelitian “Analisa Tingkat Kematangan Penerapan Keamanan Informasi Pemerintah Kota Bitung Menggunakan Indeks KAMI (Studi kasus : Dinas Komunikasi dan Informatika Kota Bitung)”, yang dibimbing oleh Bapak Dr. Eng. Steven R. Sentinuwo, ST.,MTI dan Bapak Stanley D.S. Karouw, ST,. MTI.