Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks KAMI

Novita Ester Wowor[1], Steven R. Sentinuwo[2], Stanley D.S. Karouw[3]
Teknik Elektro Universitas Sam Ratulangi. Manado, Jl. Kampus Unsrat Bahu, Manado 95115
14021106072@student.unsrat.ac.id[1], steven@unsrat.ac.id[2], stanley.karouw@unsrat.ac.id[3]

Abstrak – **Penetrasi pengguna internet di Indonesia setiap tahun selalu bertambah, oleh karena itu berdampak pula pada peningkatan ancaman dan serangan siber di Indonesia. Meskipun sampai saat ini tidak ada sistem keamanan informasi yang dapat menjamin 100% keamanannya. Salah satu kebijakan yang dapat diambil oleh organisasi untuk mencegah/mengurangi gangguan keamanan informasi adalah dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI). Pemerintah Kota Manado memiliki unit-unit kerja yang mempunyai kewajiban sebagai pengelola semua informasi yang ada di Kota Manado. Sayangnya Pemerintah Kota Manado belum pernah menerapkan, memiliki, atau menyusun kerangka kerja keamanan informasi yang memenuhi standar SNI ISO/IEC 27001. Oleh karena itu perlunya dilakukan *self-assessment* bidang keamanan dengan menggunakan metode SMKI yaitu Indeks KAMI sebagai alat bantu untuk mengukur, menganalisa, dan mengevaluasi keamanan informasi di seluruh unit-unit kerja demi mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi. Indeks KAMI disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika. Hasil pengukuran tingkat kematangan keamanan informasi Pemerintah Kota Manado bahwa untuk kategori Sistem Elektronik tingkat ketergantungan TIK tergolong tinggi, namun untuk pengelolaan keamanan informasi masih tergolong sangat rendah atau "Tidak Layak" dan masih sangat dibutuhkan perbaikan di setiap aspek yang ada. Oleh karena itu akan diberikan suatu saran perbaikan pada kekurangan yang ditemukan pada sistem keamanan informasi.**

Kata kunci - **Indeks KAMI, Keamanan Informasi, Smart City, SMKI.**

Abstract - **The penetration of Indonesian internet users has increased every year, therefore having an impact to improvement of cyber threat and offense in Indonesia. Even now, there is no information security system than can ensure 100%. One of the policy that some organization can take to decrease or preventing the interference of information security is applying Sistem Manajemen Keamanan Informasi (SMKI). The government of Manado city has job units that responsible to manage all the information in the whole city. Unfortunately the government of Manado city never applies, having, or establish their information security framework according to SNI ISO/IEC 27001. Therefore the government need to self-assessment their security sector with SMKI method, Indeks KAMI as a tool to measure, analyze, and evaluate the information security in the all jobs unit to see the description and maturity the information security. Index Kami arranged by group of Direktorat Keamanan Informasi Kementerian Komunikasi Dan Informatika. The result of the maturity of the information security measures of the government of Manado city says that the dependency of information and communication technology in electronic system classified as high, but the management of the information security was classified as low or not feasible and need to be repaired in every aspect. Therefore, there will be suggestion for improving the information security system deficiency.**

Keywords - **Information Security, Index KAMI, Smart City, SMKI.**

I. PENDAHULUAN

Penetrasi pengguna internet di Indonesia yaitu 143,26 juta jiwa dari total populasi penduduk Indonesia sebanyak 262 juta orang, itu berarti 54,68% [1]. Oleh karena itu berdampak pula pada peningkatan ancaman dan serangan siber di Indonesia. Indonesia S*ecurity Incident Response Team of Internet Infrastructure (ID-SIRTII)* menemukan data total jumlah serangan pada tahun 2017 sebanyak 205,502,159 (terjadi peningkatan jumlah total serangan dari tahun 2016 sebanyak 135,672,948) dengan total insiden Website 15,483 (domain peringkat tertinggi insiden website go.id 24,4%), total kebocoran data pada domain .ID 98,787 (domain peringkat tertinggi kebocoran data go.id 80,1%), total *Phishing Site* pada domain .ID 132, Total celah keamanan Website pada domain.ID 4,219, laporan insiden 2,260 (peringkat insiden terbanyak yang dilaporkan Fraud (61%), dan Ancaman Siber tertinggi pada tahun 2017 adalah Malware dengan 36,423,773 total aktivitas malware yang termonitor. Berdasarkan laporan The Global Cybersecurity index 2017 yang dirilis oleh The UN International Telecommunication Union (ITU), Indonesia termasuk dalam negara dengan keamanan siber yang lemah dari 195 negara, Indonesia menempati peringkat ke-70 dengan skor 0,424 [2].

Meskipun sampai saat ini tidak ada keamanan Sistem Informasi yang dapat menjamin 100% keamanannya. Walaupun demikian salah satu kebijakan yang dapat diambil oleh organisasi untuk mengatasi gangguan keamanan informasi adalah dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI).

Kota Manado adalah kota yang telah memaksimalkan pemanfaatan teknologi informasi dan komunikasi dalam mendukung program–program kota menuju kota layak huni, efisien dan berkesinambungan, serta yang berwawasan lingkungan atau green based environment sering disebut sebagai Kota Cerdas atau the Smart City [3]. Pemerintah Kota Manado memiliki unit-unit kerja yang mempunyai tugas dan kewajiban untuk mengelola dan memberikan informasi yang berbeda-beda. Dari hasil wawancara dengan Kabid. Pengembangan Sistem Informatika, Dinas Kominfo Kota Manado, bahwa Pemerintah Kota Manado belum pernah menerapkan, memiliki, atau menyusun kerangka kerja keamanan informasi yang memenuhi standar SNI ISO/IEC 27001. Maka dari itu perlunya dilakukan *self-assessment* bidang keamanan untuk evaluasi keamanan sistem informasi di seluruh unit-unit kerja demi mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi dengan menggunakan 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 [4].

Hasil dari pengukuran ini nantinya akan didapatkan skor tingkat kematangan keamanan informasi di Pemerintah Kota Manado, yang nantinya digunakan sebagai evaluasi untuk meningkatkan tingkat keamanan informasi Pemerintah Kota Manado kedepannya.

A. *Keamanan Informasi*

Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik [5]. Keamanan informasi sebetulnya adalah usaha mengamankan suatu asset yang meliputi keamanan elemen sistem hardware dan *software* seperti, komputer, jaringan, aplikasi, bahkan data dan informasi.

Keamanan informasi bertujuan untuk tercapainya CIA yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) informasi suatu organisasi dari masalah ancaman dan kelemahan sistem [6].

B. *CIA*

Keamanan informasi memiliki beberapa aspek yang wajib dipahami dalam penerapannya. Beberapa aspek tersebut sering dipahami sebagai C.I.A yang terdiri dari *confidentiality*, *integrity*, dan *availability*. CIA ini digunakan untuk menentukan apakah aman atau tidaknya suatu jaringan atau informasi. Informasi yang bernilai adalah informasi yang dapat disajikan pada waktu yang tepat, lengkap, serta akurat, juga harus konsisten [6].

Confidentiality atau kerahasiaan adalah aspek yang biasa dipahami tentang keamanan. Aspek *confidentiality* menyatakan bahwa data hanya dapat diakses atau dilihat oleh orang yang berhak. Aspek ini dikenal dengan istilah *privacy*, serangan terhadap aspek *confidentiality* dapat berupa penyadapan data (melalui jaringan), memasang *key logger*, dan pencurian fisik mesin / disk yang digunakan untuk menyimpan data. Perlindungan terhadap aspek *confidentialit*y dapat dilakukan dengan menggunakan kriptografi, dan membatasi akses (segmentasi jaringan) [6].

Aspek *integrity* atau integritas mengatakan bahwa data tidak boleh berubah tanpa izin dari yang berhak. Serangan terhadap aspek integrity dapat dilakukan oleh *man-in-the-middle*, yaitu menangkap data di tengah jalan kemudian mengubahnya dan meneruskannya ke tujuan. Data yang disampaikan di tujuan (*misalkan aplikasi di web server*) tidak tahu bahwa data sudah diubah di tengah jalan. Perlindungan untuk aspek *integrity* dapat dilakukan dengan menggunakan *message authentication code* [6].

Availability atau ketersediaan adalah ketergantungan kepada sistem yang berbasis teknologi informasi menyebabkan sistem (beserta datanya) harus dapat diakses ketika dibutuhkan. Jika sistem tidak tersedia, *not available*, maka dapat terjadi masalah yang menimbulkan kerugian finansial atau bahkan nyawa. Serangan terhadap aspek *availabilit*y dilakukan dengan tujuan untuk meniadakan layanan atau membuat layanan menjadi sangat lambat sehingga sama dengan tidak berfungsi. Serangannya disebut *Denial of Service (DOS).* Perlindungan terhadap aspek *availability* dapat dilakukan dengan menyediakan redundansi. [6].

C. *Sistem Keamana Informasi (SMKI)*

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 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 [7]. 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.

Gambar 1. Struktur Dokumentasi SMKI

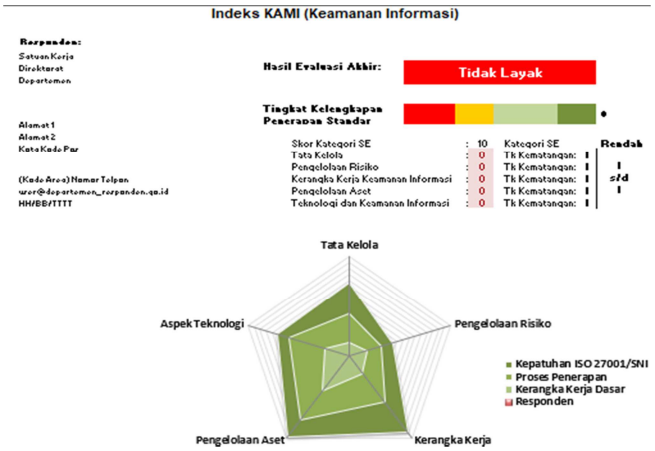
Tingkat 1 merupakan dokumen dengan hirarki tertinggi dalam struktur dokumentasi SMKI. Dokumen tingkat 1 bersifat strategis yang memuat komitmen yang dituangkan dalam bentuk kebijakan, standar, sasaran dan rencana terkait pengembangan *(development),* penerapan *(Implementation)* dan peningkatan *(improvement*) sistem manajemen keamanan Informasi [7].

Tingkat 2 merupakan dokumen yang umumnya meliputi prosedur dan panduan yang dikembangkan secara internal oleh instansi/Lembaga penyelenggara pelayanan publik dan memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan. Dokumen ini sifatnya operasional [7].

Tingkat 3 merupakan dokumen yang meliputi petunjuk teknis, instruksi kerja dan formulir yang digunakan untuk mendukung pelaksanaan prosedur tertentu sampai ke tingkatan teknis. Instruksi kerja tidak selalu diperlukan untuk setiap prosedur. Sepanjang prosedur sudah menguraikan langkah-langkah aktivitas yang jelas dan mudah dipahami penanggung jawab kegiatan, petunjuk teknis/instruksi kerja tidak diperlukan lagi [7].

D. Indeks Keamanan Informasi

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2013 [4].



Gambar 2. Dasboard Indeks KAMI

Bentuk evaluasi dari Indeks KAMI dirancang agar bisa digunakan untuk kepentingan organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya suatu proses yang ada di organisasi

Untuk proses evaluasi yang dilakukan dengan menggunakan Indeks KAMI versi 3.1 menggunakan sejumlah pertanyaan di masing-masing area di bawah ini:

1) Kategori Sistem Elektronik yang digunakan Instansi
2) Tata Kelola Keamanan Informasi
3) Pengelolaan Risiko Keamanan Informasi
4) Kerangka Kerja Keamanan Informasi
5) Pengelolaan Aset Informasi, dan
6) Teknologi dan Keamanan Informasi

Alat evaluasi ini dianjurkan untuk dilakukan pejabat yang secara langsung bertanggung jawab dan mempunyai wewenang mengelola keamanan infomasi yang ada di semua area instansinya.

Sebelum mulai menjawab pertanyaan terkait kesiapan pengamanan informasi, responden diminta untuk mendefinisikan Kategori Sistem Elektronik di Instansinya. Definisi ini bisa dijabarkan untuk tingkat Satuan Kerja baik di tingkat Kementerian/Lembaga, ataupun untuk satuan kerja yang lebih kecil, sampai ke Unit Eselon III. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan Sistem Elektronik yang digunakan instansi ke "tingkat" tertentu: Rendah, Tinggi dan Strategis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik Sistem Elektornik yang sama.

Pertanyaan dikelompokkan untuk 2 keperluan.

1) Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Dalam pengelompokan ini responden diminta untuk memberi tanggapan mulai dari area yang terkait

dengan bentuk kerangka kerja dasar keamanan informasi, efektifitas dan konsistensi penerapannya, sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi .Tingkat terakhir ini sesuai dengan kesiapan yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2013. Setiap jawaban diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka indeks sekaligus digunakan untuk menampilkan hasil evaluasi dalam *dashboard* di akhir proses ini

2) Pengelompokan kedua dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh keangka 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

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (*stakeholders*).

E. Penelitian Terkait

Terdapat bebrapa penelitian sebelumnya yang menjadi tinjauan dalam keamanan informasi. Ini sebagai bahan tinjauan dalam penelitian yang dilakukan dan akan dicantumkan beberapa hasil penelitian sebelumnya yang dilakukan oleh beberapa peneliti.

Fiezah a. Basyarahil, Hanim Maria Astuti, Bekti Cahyo Hidayanto (2017) [8]. Evaluasi Manajemen Keamanan Informasi menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. Perbedaan penelitian ini dengan penelitian saya terletak pada studi kasus yang diambil. Pada penelitian ini mengambil studi kasus di Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. Sedangkan pada penelitian saya mengambil studi kasus di Pemerintah Kota Manado.

Muh. Faturachman Husin, Hans F. Wowor, Stanley D.S. Karouw (2017) [9]. Implementasi Indeks KAMI di Universitas Sam Ratulangi. 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. Sedankan pada penelitian saya mengambil studi kasus di Pemerintah Kota Manado dan menggunakan Indeks KAMI versi 3.1.

Endi Lastyono Putra, Bekti Cahyo Hidyanto, Hanim Maria Astuti (2014) [10]. Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan menggunakan Indeks Keamanan Informasi (KAMI). Perbedaan penelitian ini dengan penelitan saya terletak pada studi kasus yang diambil. Pada penelitian ini mengambil studi kasus di Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Sedangkan pada penelitia saya mengambil studi kasus di Pemerintah Kota Manado.

Farroh Sakinah, Bambang Setiawan (2014) [11]. Indeks Penilaian Kematangan *(Maturity)* Manajemen Keamanan Layanan TI. Perbedaan Penelitian ini dengan penelitian saya terletak pada alat ukur yang digunakan. Pada penelitian ini menggunakan alat ukur yaitu COBIT 4.1. Sedangkan pada penelitian saa menggunakan alat ukur Indeks KAMI.

Tedi Agoan, Hans F. Wowor dan Stanley D.S. Karouw (2017) [12]. 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). Perbedaan penelitian ini dengan penelitian saya terletak pada lat 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.

Linda Jayanti, Steven R. Sentinuwo, Oktavian A. Lantang, Agustinus Jacobus (2016) [13]. Analisa Pola Penyalahgunaan *Facebook* Sebagai Alat Kejahatan *Trafficking* Menggunakan *Data Mining*. Perbedaan penelitian ini dengan penelitian saya yaitu, penelitian ini bertujuan untuk menganalisa pola penyalahgunaan facebook sebagai alat kejahatan trafficking menggunakan data mining. Sedangkan pada penelitian saya berfokus kepada keamanan informasi di Pemerintah Kota Manado. Persamaan penelitian ini dengan penelitian saya adalah melakukan penelitian tentang audit atau analisa.

Brian Gamaliel, Yaulie Rindengan, Stanley Karouw (2017) [14]. Pengukuran Tingkat Keselarasan Tata Kelola Teknologi Informasi Menggunakan Cobit 5 Pada Pemerintah Sulawesi Utara. Perbedaan penelitian ini dengan penelitian saya terletak pada studi kasus yang diambil. Pada penelitian ini menggunakan alat ukur COBIT 5 untuk mengetahui tingkat keselarasan TI. Sedangkan pada penelitian saya menggunakan alat ukur Indeks KAMI untuk mengukur tingkat kematangan keamanan informasi. Persamaaan penelitian ini dengan penelitian saya yaitu, sama sama melakukan analisa untuk teknologi informasi.

II. METODOLOGI PENELITIAN

Pada bagian ini menejelaskan 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 Manado. Dan untuk urutan langkah-langkah penelitian penyelesaian masalah dapat dilihat pada tabel 1.

TABEL 1. ALUR PENELITIAN

No.	Tahap	Input	Proses	Output
1	Persiapan	a. Telaah Dokumen Bisnis b. Bertemu dan Wawancara Kabid. Pengembangan Sistem Informatika di Dinas Kominfo Kota Manado c. Bertemu dan Wawancara dengan Dosen Pembimbing	Studi Literatur	Identifikasi Masalah di Pemerintah Kota Manado
2	Desain Penelitian	a. Identifikasi Organisasi: Visi, Misi, Renstra TIK Pemerintah Kota Manado. b. Bertemu dan Wawancara dengan Dosen Pembimbing	a. Studi Literatur b. Wawancara	Batasan Masalah
3	Pengumpulan Data	a. Populasi dan Sampel b. Bertemu dan Wawancara dengan Dosen Pembimbing	Kuesioner dan Wawancara	Data Mentah
4	Analisa Data	a. Analisa Data Kuesioner b. Bertemu dan Wawancara dengan Dosen Pembimbing	a. Data Cleansing b. Analisa tingkat kematangan	Skor akhir dan grafik tingkat kematangan
5	Penyusunan Laporan	a. Grafik Tingkat Kematangan b. Bertemu dan Wawancara dengan Dosen Pembimbing	Kesimpulan dan Saran	a. Laporan Hasil Penelitian b. Presentasi Hasil Penelitian

Pada tahapan pertama yaitu persiapan, peneliti melakukan telaah dokumen bisnis yaitu dengan mengumpulkan dan mempelajari dokumen Renstra TIK Pemerintah Kota Manado yang berisi tentang visi, misi, tujuan, kebijakan, program yang menyangkut dengan TIK yang ada di Pemerintah Kota Manado. Kemudian bertemu dan wawancara dengan kabid. Pengembangan Sistem Informatika di Dinas Kominfo Kota Manado dan Dosen Pembimbing untuk proses penelitian. Mempelajari studi literatur dengan mengumpulkan data-data atau sumber-sumber dan penemuan dari penelitian yang dibutuhkan untuk penelitian ini. Output yang didapat dari tahap perdiapan yaitu identifikasi masalah TIK di Pemerintah Kota Manado.

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

Tahapan ketiga yaitu tahap pengumpulan data, dimana populasi dalam penelitian ini adalah seluruh penyelenggara layanan TIK di SKPD Pemerintah Kota Manado yaitu 55 SKPD. Untuk sampel menggunakan accidental sampling dimana menjalankan kuesioner dan melakukan wawancara kepada responden yang kebetulan berada dilokasi pada saat penelitian berlangsung, jumlah sampel yang akan diambil adalah 55 informan. Untuk kuesioner digunakan untuk mengumpulkan data-data terkait kesiapan Pemerintah Kota Manado dalam menerapkan SMKI sesuai standar ISO 27001. Kusesioner yang digunakan adalah Indeks KAMI versi 3.1 yang disusun utamanya untuk membantu pengelenggara pelayanan publik dalam menyusun sistem dokumentasi SMKI yang memadai dan memenuhi persyaratan SNI ISO:IEC 27001:2013. Responden yang akan diwawancarai dan dimintakan data yaitu pembuat kebiakan (pejabat) atau pelaksana kebijakan (operator) yang bertanggungjawab atau bertugas menangani teknologi keamanan informasi terhadap masing-masing area yang akan dievaluasi. Keluarannya akan didapatkan data mentah yaitu hasil dari kegiatan wawancara dan penyebaran kuesioner yang belum diolah.

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 Manado 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. Selanjutnya akan dilakukan analisa tingkat kematangan untuk mendapatkan hasil tingkat kelengkapan dan

tingkat kematangan keamanan informasi pada Pemerintah Kota Manado. Keluarannya akandidapatkan skor akhir dan grafik tingkat kematangan.

Tahapan kelima yaitu tahap penyusunan laporan, dimana dari grafik tingkat kematangan akan akan diberikan kesimpulan dan saran dari penelitian yang telah dilakukan dan keluaran pada tahap ini yaitu laporan hasil penelitian dan dilaksanakan presentasi hasil penelitian.

III. HASIL DAN PEMBAHASAN

Penelitian tingkat kematangan keamananinformasi pada Pemerintah Kota Manado dilakukan berdasarkan INDEKS KAMI versi 3.1. alat ukur ini terdiri dari 141 pertanyaan yang dibagi menjadi 6 bagian yaitu bagian 1 Kategori Sistem Elektronik terdapat 10 pertanyaan, Bagian II Tata Kelola Keamanan Informasi 22 pertanyaan, Bagian III Pengelolaan Risiko Keamanan Informasi 16 pertanyaan, Bagian IV Kerangka Kerja Keamanan Informasi 29 pertanyaan, Bagian V Pengelolaan Aset Informasi 38 pertanyaan, dan Bagian VI Teknologi dan Keamanan Informasi 26 pertanyaan. Bagian I responden diminta untuk mendefinisikan tentang Kategori Sistem Elektronik yang ada dan untuk Bagian ke II s/d Bagian ke VI responden diminta untuk menjawab tentang tingkat pengelolaan kematangan keamanan informasi. Rekapitulasi data hasil kuesioner dapat dilihat pada tabel 2.

TABEL 2. REKAPITULASI DATA HASIL KUESIONER

AREA	SKOR
Kategori Sistem Elektronik	18
Tata Kelola Keamanan Informasi	33
Pengelolaan Risiko Keamanan Informasi	18
Kerangka Kerja Pengelolaan Keamanan Informasi	34
Pengelolaan Aset Informasi	50
Teknologi dan Keamanan Informasi	37

Gambar 3. Tingkat Kelengkapan Penerapan SMKI

Gambar 4. Radar Hasil Penilaian SMKI

Berdasarkan informasi pada Gambar 3 tingkat kelengkapan penerapan SMKI dan hasil akhir dapat disimpulkan bahwa:

1) Kategori Sistem Elektronik yang ada di Pemerintah Kota Manado berada pada level Tinggi dengan Skor 18.
2) Sementara itu dari tingkat kelengkapan penerapan SMKI, Pemerintah Kota Manado berada pada level "Tidak Layak", area "Merah" dengan totalskor yaitu berjumlah 172, skor tersebut merupakan hasil jumlah dari seluruh skor rata-rata di setiap area keamanan informasi yang dievaluasi. "Tidak Layak" Maksudnya penerapan sistem manajemen keamanan informasi di Pemerintah Kota Manado masih sangat kurang.
3) Tingkat kematangan SMKI Pemerintah Kota Manado berdasarkan hasil pengumpulan data adalah Tk. Kematangan I meliputi Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan informasi dan Teknologi Keamanan informasi, Sedangkan untuk Tk. Kematangan I+ hanya pada Pengelolaan Aset Informasi.

Pada Gambar 4, dapat dilihat untuk diagram berwarna merah muda merupakan kondisi dari Sistem Manajemen Keamanan Informasi di Pemerintah Kota Manado berdasarkan hasil pengisian kuesioner olehpara informan dan dapat dicermati bahwa:

1) Dari kelima area keamanan informasi yang diamati, tampak bahwa Pemerintah Kota Manado telah memiliki Pengolahan Aset dan Aspek teknologi yang lebih baik disbanding area Tata Kelola Keamanan Informasi, Kerangka Kerja Keamanan Informasi dan Pengelolaan Risiko Keamanan Informasi, meskipun belum mendekati standar yang ditetapkan dalam proses penerapan.
2) Sedangkan untuk area Kerangka Kerja, Tata Kelola dan Pengelolaan Risiko tampak bahwa Pemerintah Kota Manado tergolong tidak mencapai kerangka kerja dasar ini dangat perlu

diperbaiki untuk meningkatkan pengamanan informasi.

Tingkat kelengkapan penerapan SMKI berdasarkan hasil dari pengmpulan data berdasarkan Indeks KAMI pada bar chart area merah Gambar 2 menunjukan Tingkat Kelengkapan Penerapan SMKI masih dangat rendah, dan memerlukan perbaikan pada sejumlah aspek yag ada yaitu pada Tata Kelola Keamanan informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset, Teknologi dan Keamanan Informasi.

Skor tata kelola keamanan informasi yaitu 33 dengan tingkat kematangan I. Dari total 22 pertanyaan yang diajukan pada area tata kelola keamanan informasi ini, 8 (38%) diantaranya direspon "Tidak Dilakukan", 14(64%) diantaranya direspon "Dalam Perencanaan", 0 diantaranya direspon "Dalam Penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh".

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, Pemerintah Kota Manado perlu melakukan perbaikan diantaranya:

1) Semua pelaksana baik operator maupun pimpinan yang bertanggung jawab sebagai pengelola pengamanan informasi harus memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar kompetensi untuk pengelolaan keamanan informasi.
2) Menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhan keamanan informasi bagi semua pihak yang terkait.
3) Menerapkan target dan sasaran pengelolaan keamanan informasi yang berguna untuk berbagai area keamanan informasi, mengevaluasi pencapaiannya secara rutin, dan menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya.
4) Pengelolaan keamanan informasi harus berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan, dll) dan kepada pihak eksternal yang berkepentingan (regulator, aparat keamanan seperti polisi) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak.
5) Mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi, misalnya previloge attack yaitu sebuah sistem yang dapat menyusup masuk kedalam komputer dan mengambil ahli komputer tersebut untuk memantau apa yang dikerjakan oleh pengguna sebenarnya, dan yang menyangkut pelanggaran hukum (pidana dan perdata) misalnya seseorang dengan sengaja dan tanpa hak akses melakukan penyadapan atas informasi elektronik / dokumen / sistem elektronik. Dikenakan Pasal 31 UU ITE N0 19 Tahun 2016.
6) Menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu baik itu pejabat dan petugas pelaksana (operator/pejabat pengelola keamanan informasi).
7) Pimpinan harus menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggung jawabnya.

Skor pengelolaan risiko keamanan informasi yaitu 18 dengan tingkat kematangan I. Dari total 22 pertanyaan yang diajukan pada area pengelolaan risiko keamanan informasi ini, 7(44%) diantaranya direspon "Tidak Dilakukan", 9(56%) diantaranya direspon "Dalam Perencanaan", 0 diantaranya direspon "Dalam Penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh".

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, Pemerintah Kota Manado perlu melakukan perbaikan diantaranya:

1) Membuat program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
2) Menetapkan penanggung jawab manajemen risiko dan pelaporan status pengolahan risiko keamanan informasi sampai kepada tingkat pimpinan.
3) Harus membuat kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
4) Menyusun langkah mitigasi dan penanggulangan risiko keamanan informasi
5) Mengidentifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama misalnya data atau informasi yang paling penting.
6) Menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi). Contoh: Gedung kantor, dengan ancaman bencana alam, kelemahannya kondisi kantor di lereng bukit, dan dampaknya gedung dan server utama mengalami kerusakan.
7) Menetapkan dan mendefinisikan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama.

Skor kerangka kerja pengelolaan keamanan informasi yaitu 34 dengan tingkat kematangan I. Dari total 29 pertanyaan yang diajukan pada area kerangka kerja keamanan informasi ini, 7(24%) diantaranya direspon "Tidak Dilakukan", 22(76%) diantaranya direspon "Dalam Perencanaan", 0 diantaranya direspon "Dalam Penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh".

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, Pemerintah Kota Manado perlu melakukan perbaikan diantaranya:

1) Membuat kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.
2) Menetapkan kebijakan keamanan informasi secara formal, dan dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.
3) Menyediakan mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
4) Menyediakan proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
5) Menyediakan proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjut sesuai prosedur yang diberlakukan.
6) Aspek keamanan informasi harus mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan tik tercantum dalam kontrak dengan pihak ketiga.
7) Mendefinisikan, mengomunikasikan, dan menegakkan konsekuensi dari pelanggaran kebijakan keamanan informasi.
8) Menyediakan prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjut konsekuensi dari kondisi yang ada.
9) Menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch yaitu perangkat lunak yang didesain untuk memperbaiki kelemahan atau celah keamanan yang ada, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya.
10) Menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.
11) Menerapkan proses pengembangan sistem yang aman (*Secure SLDC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan.
12) Menyediakan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) maksudnya dimana kondisi bisnis harus dapat terus berjalan pasca terjadinya bencana, yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji cobannya.
13) Mengevaluasi seluruh kebijakan dan prosedur keamanan informasi terutama kelayakannya secara berkala.
14) Membuat strategi penerapan keamanan informasi sesuai hasil analisa risiko.
15) Membuat rencana dan program peningkatan keamanan informasi untuk jangka menengah/Panjang (1-3-5 tahun) yang harus direalisasikan secara konsisten.
16) Melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku).
17) Membentuk tim serta mendefinisikan komposisi, peran, wewenang dan tanggungjawab dan membuat perencanaan pemulihan bencana terhadap layanannya TIK (*disaster recovery plan*).

Skor kerangka kerja pengelolaan aset informasi yaitu 50 dengan tingkat kematangan I+. Dari total 29 pertanyaan yang diajukan pada area pengelolaan aset informasi ini, 5(13%) diantaranya direspon "Tidak Dilakukan", 30(79%) diantaranya direspon "Dalam Perencanaan", 3(8%) diantaranya direspon "Dalam Penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh".

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, Pemerintah Kota Manado perlu melakukan perbaikan diantaranya:

1) Membuat daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset).
2) Membuat definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku.
3) Membuat proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset dan keperluan pengamanannya.
4) Mendefinisikan tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut.
5) Menyediakan proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten).
6) Menyediakan proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
7) Mendefinisikan tanggungjawab pengamanan informasi secara individual untuk semua staf/karyawan.
8) Menerapkan tata tertib pengamanan dan penggunaan aset instansi terkait HAKI.

9) Menerapkan peraturan penggunaan data pribadi yang mensyaratkan pemberian izin tertulis oleh pemilik data pribadi.
10) Melakukan proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
11) Melakukan proses pengecekan latar belakang SDM, karena untuk mencari karyawan yang jujur untuk proses pengelolaan aset informasi.
12) Membuat proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
13) Membuat prosedur penghancuran data/aset yang sudah tidak diperlukan.
14) Membuat prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) dan langkah pembenahan apabila terjadi ketidak sesuaian (non-conformity) terhadap kebijakan yang berlaku.
15) Membuat prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
16) Menyediakan daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya.
17) Membuat prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan.
18) Membuat peraturan pengamanan perangkat komputasi milik instansi apabila digunakan diluar lokasi kerja resmi (kantor).
19) Membuat tata tertib penggunaan komputer, email, internet dan intranet.

Skor teknologi keamanan informasi yaitu 37 dengan tingkat kematangan I. Dari total 29 pertanyaan yang diajukan pada area teknologi keamanan informasi ini, 4(15%) diantaranya direspon "Tidak Dilakukan", 21(81%) diantaranya direspon "Dalam Perencanaan", 1(4%) diantaranya direspon "Dalam Penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh". Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, Pemerintah Kota Manado perlu melakukan perbaikan diantaranya:

1) Menyediakan konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
2) Layanan TIK (sistem komputer) yang menggunakan internet harus dilindungi dengan lebih dari 1 lapis pengamanan.
3) Semua log harus dianalisa secara berkala untuk memastikan akurasi, validitas, dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
4) Membuat dan menerapkan standar dalam menggunakan enkripsi.
5) Menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi.
6) Menerapkan penggantian password secara berkala dan mengatur kompleksitas/panjangnya.

IV. PENUTUP

A. *Kesimpulan*

Kesimpulan dari penelitian ini yaitu:

1) Kategori sistem elektronik tingkat ketergantungan TIK Pemerintah Kota Manado tergolong tinggi, akan tetapi untuk kesadaran Pemerintah Kota Manado tentang pengelolaan keamanan informasi masih tergolong sangat rendah, maka dari itu diperlukan perbaikan pada semua aspek yang ada yaitu pada tata kelola keamanan infromasi, pengelolaan risiko keamanan, kerangka kerja keamanan informasi, pengelolaan aset, teknologi dan keamanan informasi.
2) Skor akhir Indeks KAMI di seluruh unit kerja yang mempunyai pengelola keamanan di Pemerintah Kota Manado adalah 172 dari skor maksimum 645 atau 26,66% dan tidak memenuhi standar keamanan yang baik.

B. *Saran*

Berdasarkan kesimpulan diatas maka peneliti dapat memberikan saran-saran sebagai berikut:

1) Meningkatkan kemampuan SDM dengan menerapkan program-program untuk peningkatan pemahaman tentang pentingnya keamanan informasi, seperti melaksanakan program sosialisasi, *workshop*, dan menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi, termasuk kepentingan kepatuhannya di semua SKPD yang terkait.
2) Langkah-langkah yang dapat dilakukan untuk memenuhi standar keamanan yang Baik, yaitu:
   1) Membuat rencana dan program peningkatan keamanan informasi untuk tata kelola keamanan infromasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset, teknologi dan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) dan direalisasikan secara konsisten.
   2) Membuat kebijakan dan prosedur yang diperlukan untuk mengelola keamanan informasi yang disusun dan dituliskan dengan jelas, dan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya.

DAFTAR REFERENSI

[1] APJII.(2018). *"Hasil Survey Penetrasi dan Perilaku Pengguna Internet Indonesia 2017"* Diambil dari https://apjii.or.id/survey2017.

[2] Kompas, (2017). *"Keamanan SIber Indonesia Tak Lebih Baik Dibandingkan Malaysia dan Singapura".* Diambil dari : https://nasional.kompas.com/read/2017/11/21/20480051/keamanan-siber-indonesia-tak-lebih-baik-dibandingkan-malaysia-dan-singapura

[3] Pemerintah Kota Manado, *"Visi dan Misi Kota Manado"* Diambil dari : http://manadokota.go.id/site/visi_misi

[4] Direktorat Keamanan Informasi, Direktorat Jendral Aplikasi Informatika, (2017). *"Panduan Penerapan Sistem Manajemen Keamanan Informasi berbasi Indeks Keamanan Informasi (KAMI)".* Jakarta. Indonesia.

[5] G.J Simson, dan gene Spafford (1996), Partical UNIX & Internet Security, O'Reily & Associates, Inc,2nd edition.

[6] Budi Rahardjo (2017). *"Keamanan Informasi",* PT Insan Infonesia, Bandung, Indonesia.

[7] Direktorat Keamanan Informasi, Kementrian Komunikasi dan Informatika. (2011). *"Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik".* Jakarta. Indonesia.

[8] Firzah A. Basyarahil, Hanim Maria Astuti, dan Bekti Cahyo Hidayanto *"Evaluasi Manajemen Keamanan Informasi menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya",* Jurnal Teknik ITS Vol. 6, No 1, 2017. Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS) Surabaya.

[9] Muh. Faturachman Husin, Hans F. Wowor, Stanley D. S. Karouw, *"Implemetasi Indeks KAMI di Universitas Sam Ratulangi"*, E-Journal Teknik Informatika Vol 12, No.1, 2017. Teknik Informatika Universitas Sam Ratulangi.

[10] Endi Lastyono Putra, Bekti Cahyo Hidyanto, Hanim Maria Astuti, *"Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI)"*, JURNAL TEKNIK POMITS Vol 3, No 2, 2014. Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS), Surabaya, Indonesia.

[11] Farroh Sakinah, Bambang Setiawan, *"Indeks Penilaian Kematangan (Maturity) Manajemen Keamana Layanan TI",* Jurnal Teknik POMITS, Vol 3, No.2, 2014, Institut Teknologi Sepuluh Nopember (ITS).

[12] Tedi Agoan, Hans F. Wowor dan Stanley Karouw "*Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan Framework COBIT 5 Domain Evaluate, Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS)*", E-Journal Teknik Informatika, Vol 10, No 1, 2017. Universitas Sam Ratulangi. Manado, Indonesia.

[13] Linda Jayanti, Steven R. Sentinuwo, Oktavian A. Lantang, Agustinus Jacobus, "Analisa Pola Penyalahgunaan *Facebook* Sebagai Kejahatan *Trafficking* Menggunakan *Data Mining*", E-Journal Teknik Informatika, Volume 8, No 1, 2016. Teknik Informatika Universitas Sam Ratulangi Manado, Indonesia.

[14] Brian Gamaliel, Yaulie Rindengan, Stanley Karouw, *"Pengukuran Tingkat Keselarasan Tata Kelola Teknologi Informasi Menggunakan COBIT 5 Pada Pemerintah Sulawesi Utara,* E-Journal Teknik Informatika, Vol 11, No.1, 2017. Universitas Sam Ratulangi Manado, Indonesia.

SEKILAS TENTANG PENULIS

Novita Ester Wowor adalah nama lengkap dari penulis. Dilahirkan di Manado pada 7 November 1996. Saya merupakan anak ke-2 dari pasangan Steren Wowor dan Shirley Lumintang.

Saya menempuh pendidikan dimulai dari SD GMIM 1 Pakuure (2002-2008). Saya melanjutkan pendidikan di SMP Negeri 2 Tenga (2008-2011), pada jenjang menengah atas saya melanjutkan pendidikan di SMK N 1 Amurang (2011-2014).

Di tahun 2014 penulis lulus dari bangku SMK kemudian melanjutkan pendidikan S1 di salah satu perguruan tinggi yang ada di Sulawesi Utara yaitu Universitas Sam Ratulangi dengan mengambil Program Studi Teknik Informatika di Jurusan Elektro Fakultas Teknik. Selama berada di bangku kuliah saya sangat bersyukur karena dapat tergabung dalam organisasi kemahasiswaan yaitu Himpunan Mahasiswa Elektro (HME), menjadi bagian dari POSITIVISME, dan UPK Kr-FT Unsrat. Hingga akhirnya pada Oktober 2018 saya dapat menyelesaikan studi S1 dengan hasil yang baik.