

Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI

Reynaldo Adi Putra Pratama Gala ¹⁾, Rizal Sengkey ²⁾, Charles Punusingon ³⁾,

Teknik Elektro Prodi Informatika, Universitas Sam Ratulangi Manado, Jl. Kampus Bahu-Unsrat Manado, 95115

dede.gala87@gmail.com, rizalsengkey@gmail.com, charlespunuhsingon@yahoo.com,

Diterima: Juni 2020; direvisi: Agustus 2020; disetujui: Agustus 2020

Abstract – Southeast Minahasa Regency is a regency that has maximized the benefits of Information and Communication Technology in supporting Southeast Minahasa programs towards a smart city. But unfortunately there is no information security framework that meets the SNI ISO/IEC 27001 standards. Therefore, it must be done in the field of security using the Information Security Management System (SMKI) method, namely the Information Security Index (KAMI). The level of information security maturity of the MITRA Regency Government is still very low or "Ineligible" and is in the "Red" area with a total score is 264 which is the result of all the average scores in each of the evaluated Information Security areas.

Keywords — Indeks KAMI; Information Security; SMKI; Smart city.

Abstrak — Kabupaten Minahasa Tenggara adalah kabupaten yang telah memaksimalkan manfaat Teknologi Informasi dan Komunikasi dalam mendukung program-program Minahasa Tenggara menuju kota layak huni atau *the smart city*. Tapi sayangnya tidak diterapkan kerangka kerja keamanan informasi yang memenuhi standar SNI ISO/IEC 27001. Oleh karena itu, harus dilakukan didalam bidang keamanan dengan menggunakan metode (SMKI) Sistem Manajemen Keamanan Informasi yaitu Indeks Keamanan Informasi yang (KAMI). Tingkat kematangan keamanan informasi Pemerintah Kabupaten MITRA masih tergolong sangat rendah atau "Tidak Layak" dan berada di area "Merah" dengan total skor yaitu berjumlah 264 yang merupakan hasil jumlah dari seluruh skor rata-rata di setiap area Keamanan Informasi yang dievaluasi.

Kata kunci — Indeks KAMI; Keamanan Informasi; SMKI; Smart city.

I. PENDAHULUAN

Keamanan informasi merupakan hal penting yang masih sangat jarang diperhatikan oleh pemerintahan, perusahaan, atau organisasi sebagai pemilik informasi tersebut. Hasil survey *ESET Asia Cyber Savviness Report 2015* mengungkap fakta bahwa negara Indonesia menempati urutan terendah pengetahuan masyarakatnya terhadap resiko kejahatan *cyber*. Selain itu, masyarakat Indonesia juga tercatat santai saja terhadap ancaman *cybercrime* dan dinilai yang paling tidak khawatir terhadap kejahatan di dunia *online*. Maka dari itu harus dilindungi dari berbagai bentuk ancaman dan serangan. Secara garis besar, ancaman terhadap sistem informasi bisa dibagi menjadi dua kategori yaitu ancaman aktif, seperti kejahatan atau kecurangan yang dilakukan dengan sengaja oleh seseorang, dan ancaman pasif yang berupa kegagalan sistem, kesalahan manusia yang tidak disengaja dan faktor bencana alam [1]. Kabupaten minahasa tenggara adalah

kabupaten yang telah memaksimalkan pemanfaatan Teknologi Informasi dan Komunikasi. dalam mendukung program-program Minahasa Tenggara menuju kota layak huni, efisien dan berkesinambungan, serta yang berwawasan lingkungan, sering disebut sebagai Kota Cerdas atau *The Smart City* (mitrakab.go.id). Visi Dinas Komunikasi dan Informatika Kabupaten Minahasa Tenggara, Terwujudnya efektifitas dan efisiensi komunikasi dan informatika dalam penyelenggaraan pemerintahan daerah untuk mencapai Kabupaten Minahasa Tenggara yang berdikari berdaulat dan berkepribadian. Dengan visi tersebut, Dinas Komunika dan Informatika di harapkan dapat memberikan kontribusi melalui upaya mewujudkan Kabupaten Minahasa Tenggara yang berpengetahuan, mandiri, dan berdaya saling tinggi melalui pemanfaatan TIK. Institusi yang memiliki kewajiban dan kewenangan serta tanggung jawab mewujudkan masyarakat informasi yang berpengetahuan, inovatif, komunikatif, mandiri, sejahtera, berdaya saing Guna mewujudkan Visi tersebut di atas ditetapkan misi sebagai berikut :

- 1) Meningkatkan Sumber Daya Manusia (SDM) aparatur bidang teknologi informasi dan komunikasi (TIK)
- 2) Meningkatkan Sarana dan Prasarana Teknologi Komunikasi dan Informatika (TIK)
- 3) Melaksanakan Pelayanan Informasi dan Komunikasi Kepada Masyarakat [2].

Indeks KAMI sebagai alat yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika untuk mengukur dan menganalisis tingkat kesiapan atau kematangan pengamanan informasi yang ada di suatu instansi. Hasil pengukuran ini akan menghasilkan tingkat kematangan keamanan informasi di setiap Satuan Kerja Perangkat Daerah (SKPD) di Pemerintah Kabupaten Minahasa Tenggara, yang nantinya akan dievaluasi dan digunakan sebagai referensi untuk meningkatkan tingkat keamanan informasi dimasa mendatang [3]. Hasil penelitian ini nantinya akan menghasilkan skor dari tingkat kematangan keamanan informasi Pemerintah Kabupaten Minahasa Tenggara, yang nantinya akan mendapatkan bahan pertimbangan pengambilan keputusan atau kebijakan bidang keamanan informasi di Pemerintah Kabupaten Minahasa Tenggara untuk kedepannya.

A. Penelitian Terkait

Mustaqim, Susanto, dan Hidayanto (2014) Evaluasi Manajemen Keamanan Informasi menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur. Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh

nopember (ITS) Surabaya. Berdasarkan KMK No. 479/KMK.01/2010 maka kebijakan dan standar sistem manajemen keamanan informasi di lingkungan Kementerian Keuangan mengacu kepada ISO/IEC 27001:2005. ISO/IEC 27001:2005 merupakan dokumen standar internasional tentang sistem manajemen keamanan informasi atau Information *Security Management Sistem* (ISMS) Dalam pelaksanaannya ada sejumlah aspek yang biasanya tidak dapat terpenuhi oleh instansi dalam rangka penerapan keamanan informasi berdasarkan indeks KAMI. Faktor penyebab inilah yang kemudian menjadi aspek penentu penilaian secara krusial tentang penerapan indeks KAMI dalam institusi pemerintahan. Selain faktor penyebab, beberapa faktor kesuksesan juga diukur sebagai masukan bagi pihak manajerial dan organisasi secara keseluruhan demi meningkatkan tingkat kematangan organisasi dalam rangka pengelolaan keamanan informasi pada institusinya. Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. 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 ISO/IEC 27001:2005 Hasil dari penelitian ini adalah mendapatkan penilaian mengenai pengelolaan keamanan TI, mengetahui tingkat kematangan pengelolaan keamanan teknologi informasi dan mendapatkan rekomendasi atas hasil analisis faktor penyebab dan faktor pendukung dalam pengelolaan keamanan informasi. Perbedaan penelitian ini dengan penelitian saya pada studi kasus yang di ambil. Pada penelitian ini mengambil studi kasus di Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur. Sedangkan pada penelitian saya mengambil studi kasus di setiap SKPD Minahasa Tenggara. dan persamaan penelitian ini dengan saya sama – sama menggunakan indeks KAMI versi 3.1 [4].

Winda Septilia Kusumaningrum, dan Budi Widjajanto (2016) Kelengkapan Dan Kematangan Sistem Keamanan Informasi Berdasarkan Indeks KAMI Pada Divisi Sampling Dan Pengujian BBPOM Kota Semarang. Fakultas Ilmu Komputer, Universitas Dian Nuswantoro (UDN) Semarang. Pentingnya peran Teknologi Informasi dan Komunikasi (TIK) dalam upaya meningkatkan kualitas layanan demi terwujudnya tata kelola pemerintah yang baik (*Good Corporate Governance*) sehingga peranan tata kelola Teknologi Informasi dalam suatu instansi penyelenggara pelayanan publik sangat dibutuhkan. Berdasarkan penelitian sebelumnya terkait pengelolaan keamanan informasi di BBPOM maka diperlukan sebuah kegiatan evaluasi Sistem Manajemen Keamanan Informasi dalam menjamin keamanan informasi para penyedia barang/jasa. Dengan adanya pengukuran ini nantinya dapat menghasilkan temuan dan rekomendasi yang dapat digunakan BBPOM Kota Semarang sebagai referensi untuk meningkatkan pengelolaan keamanan informasi agar kedepannya dapat mendukung tujuan bisnis organisasi dengan lebih baik. Dari hasil studi dokumen wawancara dan kuesioner menggunakan pedoman Indeks KAMI maka diperoleh skor hasil Tingkat Kematangan yaitu 381 dengan Level II+, yang meliputi Tata Kelola dengan skor 75 pada Level II+, Pengelolaan Risiko dengan skor 42 pada Level II, Kerangka Kerja dengan skor 95 pada Level II+, Pengelolaan Aset dengan skor 94 pada Level II, dan Teknologi dengan skor 75 pada Level II+. Dan untuk meningkatkan tingkat Kematangan dan Kelengkapan BBPOM

Kota Semarang dapat melakukan strategi perbaikan yang dilakukan secara bertahap dari masing-masing area pengamanan. Perbedaan penelitian ini dengan saya terletak pada kelengkapan dan kematangan sistem keamanan informasi, sedangkan penelitian saya menganalisa atau mengukur tingkat kematangan disetiap SKPD Minahasa Tenggara [5].

Rahmat Hidayat, Mohammad Suyanto, dan Andi Sunyoto (2018) Indeks Penelitian Keamanan Informasi Untuk Mengukur

Kematangan Manajemen Keamanan Layanan TI (Studi Kasus BPMP Kabupaten Gresik). Teknik Informatika Universitas AMIKOM Yogyakarta. Penelitian ini berisi hasil pengukuran kematangan Sistem Manajemen Keamanan Informasi (ISMS) di Kabupaten Gresik Hasil pengukuran kelengkapan dan kematangan ISMS di BPMP Kabupaten Gresik masih tergolong rendah, yaitu pada level I sampai II yang berarti tingkat kematangannya dinyatakan dalam kondisi awal hingga implementasi kerangka dasar, masih di bawah standar ISO 27001: 2009. Dan untuk evaluasi tingkat kelengkapan implementasi lima area dengan skor pencapaian tahun 207, maka menurut Indeks KAMI berarti status kesiapan dianggap "Tidak Layak". Penyebab tingkat kematangan yang rendah dari SMKI termasuk tingkat kesadaran yang rendah dari kepemimpinan dan karyawan terkait SMKI, kurangnya dokumentasi kegiatan dan juga untuk pengembangan aplikasi dan infrastruktur yang ada reaktif. Peneliti menyarankan hal-hal yang perlu untuk meningkatkan kesadaran kepada para pemimpin dan karyawan tentang pentingnya ISMS, dan untuk mengembangkan Cetak Biru TIK yang memungkinkan pengembangan aplikasi BPMP dan infrastruktur harus dilakukan secara terencana dan komprehensif. Dan meningkatkan SOP di lingkungan BPMP untuk mendukung pergeseran proses bisnis dari berbasis kertas ke administrasi berbasis teknologi serta menumbuhkan dokumentasi data dan informasi di BPMP Kabupaten Gresik. Perbedaan dan Persamaan dalam penelitian ini ada pada studi kasus yang di ambil yaitu beliau di BPMP Kabupaten Gresik kalau saya di Kabupaten MITRA (Minahasa Tenggara). dan juga sama – sama menggunakan Indeks KAMI 3.1 [6].

Muh. Faturachman Husin, Hans F. Wowor, dan Stanley D.S. Karouw (2017) Implementasi Indeks KAMI di Universitas Sam Ratulangi.. Teknik Informatika, Universitas Sam Ratulangi Manado. Penelitian ini untuk mendapatkan tingkat kematangan keamanan informasi di Universitas Sam Ratulangi ternyata masih tergolong rendah dan butuh perbaikan walaupun peran/tingkat ketergantungan akan teknologi informasi dan komunikasi tergolong tinggi.

Perbedaan dengan penelitian saya terletak pada alat ukur Indeks KAMI. beliau menggunakan Indeks KAMI versi 2.3 sedangkan saya menggunakan Indeks Kami versi 3.1 dan perbedaan ini berada pada kuesionernya, alat ukur evaluasi ini terdapat 131 pertanyaan sedangkan Indeks KAMI versi 3.1 memiliki 141 pertanyaan [7].

Chalifa Chazar, (2015) Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. Informasi merupakan salah satu aset penting bagi perusahaan. Oleh karena itu kemampuan untuk menyediakan informasi secara cepat dan akurat merupakan hal yang esensial. Pengelolaan informasi sering kali melibatkan peran Sistem Informasi (SI) dan Teknologi Informasi (TI). Akan tetapi seiring perkembangannya, TI seringkali dimanfaatkan oleh beberapa pihak yang tidak bertanggung jawab yang dapat menimbulkan

ancaman dan resiko yang dapat merugikan perusahaan. Masalah keamanan seringkali kurang mendapatkan perhatian dari pihak *stakeholder*. "*Prevention is better than cure*". Seri ISO/IEC 27000 menawarkan satu set spesifikasi, kode etik dan pedoman praktik terbaik (*best practise*) untuk memastikan manajemen layanan TI (Teknologi Informasi). ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu confidentiality, integrity dan availability. Kata kunci: Keamanan Sistem Informasi, ISMS, SMKI, ISO/IEC 27000, ISO/IEC 27001. Perbedaan dengan penelitian saya yaitu (SMKI) Sistem Manajemen Keamanan Informasi ini menggunakan ISO/IEC 27001:2005. Sedangkan saya menggunakan ISO/IEC 27000:2013 [8].

B. Keamanan Informasi

Keamanan informasi adalah upaya melindungi aset informasi dari berbagai ancaman baik yang dilakukan secara sengaja maupun tidak sengaja yang terjadi dengan meningkatnya ancaman gangguan/ insiden yang terkait dengan penggunaan Teknologi Informasi dan Komunikasi (TIK) yang dapat mengganggu aspek kerahasiaan, keutuhan, dan ketersediaan layanan.

Junian Dani (2008) Keamanan informasi telah dibangun atas 3 kunci dasar dari prinsip kunci keamanan informasi yaitu, *Confidentiality* (Kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

1) Confidentiality

Junian Dani (2008) *Confidentiality* atau kerahasiaan berfokus pada upaya untuk menghindari pengungkapan secara tidak sah terhadap informasi yang bersifat rahasia maupun sensitive. Pengungkapan informasi tersebut dapat terjadi secara disengaja, seperti pemecahan sandi untuk membaca informasi, atau dapat terjadi secara tidak disengaja, dikarenakan kecerobohan dari individu dalam menangani informasi.

2) Integrity

Junian Dani (2008) *Integrity* (integritas atau keutuhan) berarti bahwa data tidak dapat dibuat, diganti, atau dihapus tanpa proses otorisasi. Dengan kata lain, *integrity* merupakan prinsip yang ditujukan untuk menjaga keakuratan suatu informasi. Sebagai contoh, data yang disimpan pada salah satu bagian dari sistem database telah melewati persetujuan dengan data terkait yang tersimpan pada bagian lain dari sistem database.

3) Availability

Junian Dani (2008) *Availability* atau ketersediaan menjamin bahwa pengguna sistem yang berhak memiliki akses tanpa interupsi terhadap sistem dan jaringan. Hal tersebut memastikan bahwa informasi atau sumber data akan selalu tersedia ketika dibutuhkan [9].

C. Sistem Manajemen Keamanan Informasi (SMKI)

KOMINFO (2017) Standar ISO (*International Organization for Standardization*) atau Organisasi Internasional untuk Standardisasi sejak tahun 2005 telah

mengembangkan sejumlah standar tentang *Information Security Management Systems* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan. Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

- 1) ISO/IEC 27000:2009 – *ISMS Overview and Vocabulary*
- 2) ISO/IEC 27001:2005 – *ISMS Requirements*
- 3) ISO/IEC 27002:2005 – *Code of Practice for ISMS*
- 4) ISO/IEC 27003:2010 – *ISMS Implementation Guidance*
- 5) ISO/IEC 27004:2009 – *ISMS Measurements*
- 6) ISO/IEC 27005:2008 – *Information Security Risk Management*
- 7) ISO/IEC 27006: 2007 – *ISMS Certification Body Requirements*
- 8) ISO/IEC 27007 – *Guidelines for ISMS Auditing*

Dari standar seri ISO 27000 ini, hingga September 2011, baru ISO/IEC 27001:2005 yang telah diadopsi Badan Standardisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001:2009.

D. ISO/IEC 27001:2013

KOMINFO (2017) Standar ISO 27001:2013 telah mengadopsi format terkini dari standar sistem manajemen yang bertujuan menjaga konsistensi, keselarasan dan kompatibilitas dari sistem manajemen organisasi yang dibangun dengan merujuk pada standar-standar yang dikembangkan ISO, seperti ISO 9001, ISO 14001, ISO 27001, dan lainnya. (KOMINFO,2017). Beberapa konsep baru yang dikenalkan atau di pertajam dalam ISO 27001:2013.

E. Indeks KAMI

KOMINFO (2017) 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 27001:2009. Hasil evaluasi indeks KAMI menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di instansi pemerintah [10].

Menurut Badan Siber Dan Sandi Negara (BSSN) Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru. Keterlibatan pihak ketiga dalam rantai pasok (*supply chain*) layanan suatu instansi/perusahaan menimbulkan risiko terkait keberadaan/keterlibatan pihak eksternal tersebut. Layanan berbasis infrastruktur awan (*Cloud*) memberikan peluang efisiensi dan peningkatan kinerja yang sangat signifikan bagi instansi/perusahaan, akan tetapi risiko terkait data yang berada pada pengendalian pihak ketiga (penyelenggara layanan) perlu dimitigasi. Sedangkan dengan disahkannya peraturan terkait perlindungan data pribadi oleh banyak negara memerlukan kerangka kerja yang secara spesifik membahas bagaimana data pribadi yang ada / digunakan dalam



Gambar 1 Dashboard Indeks KAMI

TABEL I
ALUR PENELITIAN

No	Tahap	Input	Proses	Output
1	Persiapan	<ul style="list-style-type: none"> Telaah Dokumen Bisnins Bertemu dan Wawancara kabid pengembangan sistem dinas kominfo Kab. MITRA 	Studi Literatur	Identifikasi masalah di pemerintahan Kab.MITRA
2	Desain Penelitian	Identifikasi Organisasi visi, misi Renstra TIK Pemerintah Kab. MITRA	<ul style="list-style-type: none"> Studi Literatur Wawancara 	Batasan Masalah
3	Pengumpulan Data	Populasi dan Sampel	Kuisoner dan wawancara	Data Kasar
4	Analisa Data	Analisa Data Kuisoner	<ul style="list-style-type: none"> Data Cleansing Analisa tingkatan kematangan 	Skoe akhir dan grafik tingkat kematangan
5	Penyusunan Laporan	Grafik tingkat kematangan	Kesimpulan dan saran rekomendasi	<ul style="list-style-type: none"> Laporan Hasil Penelitian Presentasi Penelitian

Bagian II: Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi			
[Penilaian] Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan atau Diterapkan Sebagian, Diterapkan Secara Menyeluruh	Status	Skor	
#	Fungsi/Instansi Keamanan Informasi		
2.1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Tidak Dilakukan	0
2.2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Tidak Dilakukan	0
2.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	0
2.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	0
2.5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan	0
2.6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0

Gambar 2 Pertanyaan Indeks KAMI

instansi/perusahaan diamankan sesuai dengan persyaratan hukum. Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan potret indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembandingan dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui Bimbingan Teknis, Asesmen, dan Konsultasi.

Dengan perkembangan sekarang Indeks KAMI diberikan pada BSSN (Badan Siber Dan Sandi Negara) dan ditingkatkan lagi toolsnya menjadi Indeks KAMI versi 4.0 BSSN, Untuk menilai kesiapan instansi/perusahaan dalam mengelola risiko di 3 (tiga) area baru ini, pada revisi 4.0 disediakan modul suplemen yang membahas aspek kesiapan pengamanan untuk ketiga aspek tersebut. Penggunaan modul suplemen untuk evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastruktur Awan (*Cloud Service*) dan Perlindungan Data Pribadi digunakan sesuai konteks atau cakupan yang ada [11].

II. METODE PENELITIAN

A. Kerangka Berpikir

Urutan langkah-langka penelitian masalah dapat di lihat pada tabel 1 yang dimana urutan langkah-langkahnya yang dibuat secara sistematis, logis sehingga dapat dijadikan pedoman yang jelas dan mudah untuk menyelesaikan permasalahan, analisis hasil akhir Pemerintah Kabupaten Minahasa Tenggara dan kesulitan-kesulitan yang dihadapi.

B. Persiapan

Tahap persiapan, peneliti akan melakukan telaah dokumen bisnis dengan dokumen yang akan dipelajari ada pada Dokumen Renstra TIK Kabupaten Minahasa Tenggara yang berisi tentang pedoman arah pembangunan di bidang penyelenggaraan Komunikasi dan Informatika dalam kurung waktu 2 (dua) tahun 2018 s/d 2019.

Kemudian studi literatur dilakukan dengan mengumpulkan data – data atau dari sumber dan penemuan dari penelitian yang telah dilakukan sebelumnya. Teori -teori yang terkait dengan permasalahan penelitian Indeks KAMI dan penelitian yang menggunakan Indeks KAMI versi lainnya atau penelitian yang menggabungkan beberapa model evaluasi. Studi literatur dilakukan dengan membaca, merangkum, dan kemudian menuliskan kembali dengan metode yang sudah ditentukan

Identifikasi masalah yang didapat :

- 1) Bertemu dengan kepala bidang kominfo Kab. MITRA dan membahas tentang permasalahan di bidang sistem manajemen keamanan informasi.

- 2) Mempersiapkan kuesioner yang ada pada Indeks KAMI untuk melakukan wawancara di berbagai SKPD di kabupaten Minahasa Tenggara.
- 3) Mengumpulkan data – data kasar atau data yang belum diolah dari hasil wawancara di setiap SKPD Kab. MITRA dan membuat video wawancara dari berbagai responden yang ada di setiap SKPD Kab. MITRA.

C) *Desain Penelitian*

Teknik wawancara akan digunakan untuk mendapatkan informasi tentang pengamanan keamanan informasi di seluruh SKPD Pemerintah Kabupaten Minahasa Tenggara. Wawancara dilakukan dengan metode interview dimana penulis

mengajukan pertanyaan dan informan memberikan jawaban dan penulis mencatat setiap jawaban yang nantinya akan digunakan untuk membuat laporan hasil wawancara.

Batasan masalah agar penelitian tidak terlalu luas dan mengarah pada objek penelitian, maka diberikan batasan masalah sebagai berikut:

- 1) Penelitian ini menggunakan Random accidental sampling dengan menemukan keterangan informan sebagai narasumber.
- 2) Penelitian ini menggunakan Indeks Keamanan Informasi (KAMI) sebagai alat ukur.

D) *Pengumpulan Data*

Tahap populasi dimana dalam penelitian ini adalah seluruh penyelenggara layanan TIK atau operator TIK di Satuan Kerja Perangkat Daerah (SKPD) Pemerintah Kabupaten Minahasa Tenggara.

Menurut (Endang Mulyatiningsih, 2011) Teknik pengambilan sampel, Setiap jenis penelitian membutuhkan teknik pengambilan sampel (teknik sampling) yang tepat sesuai dengan populasi sasaran yang akan diteliti. Populasi penelitian bersifat heterogen dan homogen. Manusia merupakan jenis populasi yang heterogen, sedangkan benda dan tumbuhan merupakan jenis populasi yang relatif homogen. Sampel penelitian yang diambil dari populasi yang heterogen harus representatif atau mewakili semua karakteristik yang terdapat pada populasi. Demikian juga bila populasi memiliki cakupan wilayah luas, sampel yang diambil juga harus mewakili setiap bagian wilayah yang berbeda. Sampel yang representatif adalah sampel yang diambil secara acak sehingga semua anggota populasi berpeluang untuk dipilih. Sampel acak menjadi syarat utama pada penelitian yang hasilnya akan digeneralisasikan ke seluruh populasi. Sampel non acak hanya diperbolehkan untuk penelitian yang memiliki karakteristik populasi homogen atau apabila hasil penelitian hanya berlaku untuk sampel yang diteliti [12]. Dan pada tahap ini penelitian pengambilan sampel menggunakan accidental sampling.

Menurut (Sugiyono, 2009) Accidental sampling adalah Teknik penentuan sampel berdasarkan kebetulan, yaitu konsumen yang secara kebetulan/incidental bertemu dengan peneliti dapat digunakan sebagai sampel, bila dipandang orang yang kebetulan ditemui itu cocok sebagai sumber data. Jumlah sampel yang akan diambil adalah 30 orang informan dari berbagai SKPD di Pemerintah Kabupaten Minahasa Tenggara.

Kuisoner dan wawancara untuk mengumpulkan data-data terkait kesiapan Pemerintah Kabupaten MITRA dalam menerapkan SMKI sesuai standar ISO 27001. Kuisoner yang

akan digunakan peneliti adalah Indeks Keamanan Informasi (Indeks KAMI) versi 3.1 yang disusun utamanya untuk membantu penyelenggara pelayanan publik dalam menyusun sistem dokumentasi SMKI yang memadai dan memenuhi persyaratan standar SNI ISO:IEC 27001:2013. Responden adalah pembuat kebijakan (Pegawai) atau pelaksana kebijakan (operator) yang bertanggung jawab atau bertugas menangani teknologi keamanan informasi terhadap masing-masing area yang akan dievaluasi.

Data Kasar adalah sebuah kondisi dimana data yang dikumpulkan tidak ada perubahan apapun. Data kasar dapat berdiri sendiri dan tidak menjadi subjek untuk diproses atau dimanipulasi inilah mengapa data mentah disebut data primer. Data kasar yang digunakan dalam penelitian ini yaitu data hasil dari kegiatan wawancara dan kuisoner yang belum diolah.

E) *Pengumpulan Data*

Analisa data dapat dengan cara manual atau bantuan perangkat lunak komputer tergantung kemampuan peneliti dan kesulitan dalam pengolahan data. Bantuan perangkat komputer paling sering digunakan karena sangat membantu peneliti mengolah data dan menghemat waktu. Hal yang harus diperhatikan adalah komputer tidak dapat memahami esensi penelitian kita, jadi peneliti harus secara benar dan teliti melakukan pengolahan data dengan baik dan benar mulai dari tahapan awal hingga akhir.

Analisa data kuisoner dari yang sudah di sebarakan lalu dikumpulkan serta dilakukan evaluasi kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi di Pemerintah Kabupaten Minahasa Tenggara. Pada tahap data cleansing proses analisa kualitas dari suatu data dengan cara mengubah, mengoreksi, atau menghapus data-data yang salah, tidak lengkap, tidak akurat, atau memiliki format yang salah dalam basis data guna menghasilkan data berkualitas tinggi. Proses data cleansing terkadang dilakukan dengan perpaduan antara proses otomatisasi dan proses manual.

Analisa tingkat kematangan keamanan informasi dikelompokkan untuk 2 keperluan yaitu:

1) Tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Dalam pengelompokkan ini responden diminta untuk memberi tanggapan mulai dari area terkait dengan bentuk kerangka kerja dasar kemanana informasi (pertanyaan diberi (label “1”), efektifitas dan konsistensi penerapannya (label “2”), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label “3”). Setiap jawaban diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka indeks sekaligus digunakan untuk menampilkan hasil evaluasi dalam dashboard di akhir proses ini.

Untuk keseluruhan area pengamanan, pengisian pertanyaan dengan label “3” hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan label “1” dan “2” sudah diisi dengan status minimal “Diterapkan Sebagian”.

2) 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 ukur untuk melaporkan pemetaan dan pemingkatan kesiapan keamanan informasi di Kementerian/Lembaga.



Gambar 3 Diagram Radar Grafik Hasil Penilaian SMKI

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

Untuk membantu memberikan uraian yang lebih detail, tingkatan ini ditambah dengan tingkatan antara -I+, II+, III+, IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. sebagai padanan terhadap standar ISO/IEC 27001:2013, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah tingkat III+.

Untuk Grafik hasil penelitian dapat dilihat di gambar 3 yaitu mengacu pada Diagram Radar yang menunjukkan sejauh mana kelengkapan pengamanan sudah mendekati atau mencapai tingkat kelengkapan yang diharapkan pada diagram radar.

F) Penyusunan Laporan

Kesimpulan dari penelitian ini adalah berisi tentang jawaban dan permasalahan dalam bentuk resume atau ikhtisar dari permasalahan.

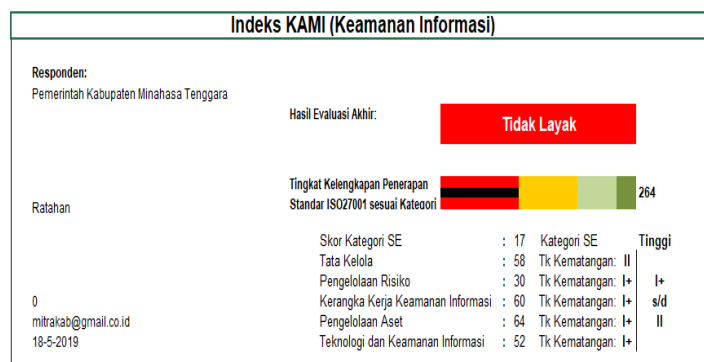
Saran merupakan sebuah solusi yang ditujukan untuk menyelesaikan permasalahan yang dihadapi. Saran harus bersifat membangun, mendidik, dan secara objektif serta sesuai dengan topik yang dibahas. Saran hanya berisi rekomendasi yang dirumuskan oleh peneliti namun bukan untuk menjawab permasalahan dalam pokok penelitian.

Rekomendasi adalah memberitahukan kepada seseorang atau lebih bahwa sesuatu yang dapat dipercaya, dapat juga merekomendasikan diartikan sebagai saran yang sifatnya menganjurkan, membenarkan, atau menguatkan mengenai sesuatu

III. HASIL DAN PEMBAHASAN

A. Hasil Analisa Tingkat Kematangan Sistem Keamanan Informasi Pemerintah Kab. MITRA

Berdasarkan tabel III rekapitulasi data hasil observasi di dapat di simpulkan bahwa penelitian tingkat kematangan sistem keamanan informasi pada Kabupaten Minahasa Tenggara ini dilakukan berdasarkan INDEKS KAMI versi 3.1. Alat ukur



Gambar 4 Tingkat Kelengkapan Penerapan SMKI

TABEL II
REKAPITULASI DATA HASIL OBSERVASI

Area	Skor
Kategori Sistem Elektronik	17
Tata Kelola Keamanan Informasi	58
Pengelolaan Risiko Keamanan Informasi	30
Kerangka Kerja Keamanan Informasi	60
Pengelolaan Aset Informasi	64
Teknologi dan Keamanan Informasi	52

evaluasi ini terdapat 141 pertanyaan yang dibagi menjadi 6 bagian yaitu untuk Bagian I 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.

Hasil pengumpulan data penelitian dapat dilihat pada gambar 4 yang dimana dilakukan analisis tingkat kelengkapan penerapan standar manajemen keamanan informasi (SMKI) dan hasil evaluasi akhir di gambar 5 yaitu dapat disimpulkan :

- Kategori Sistem Elektronik yang ada di Pemerintah Kabupaten Minahasa Tenggara berada pada level Tinggi dengan Skor 17.
- Sementara itu dari tingkat kelengkapan penerapan SMKI, Pemerintah Kabupaten Minahasa Tenggara berada pada level "Tidak Layak", area "Merah" dengan total skor yaitu berjumlah 264, skor tersebut merupakan hasil jumlah dari seluruh skor rata-rata di setiap area Keamanan Informasi yang dievaluasi.

Pada gambar 5 radar diagram berwarna merah muda merupakan kondisi dari Sistem Manajemen Keamanan Informasi di Pemerintah Kabupaten Minahasa Tenggara. berdasarkan hasil pengisian kuesioner oleh peneliti. Dapat

disimpulkan bahwa:

- Dari kelima area keamanan informasi, tampak bahwa Pemerintah Minahasa Tenggara telah memiliki Pengolahan Aset dan Aspek Teknologi yang lebih baik dibanding area keamanan lainnya meskipun belum mendekati standar yang ditetapkan dalam Proses Penerapan.
- Sedangkan untuk Area Kerangka Kerja, Area Tata Kelola dan Area Pengelolaan Risiko tampak bahwa Pemerintah Minahasa Tenggara tergolong tidak mencapai kerangka kerja dasar ini sangat perlu diperbaiki untuk meningkatkan pengamanan informasi.

B. Pembahasan Tingkat Kelengkapan Penerapan SMKI

Pemerintah Kabupaten Minahasa Tenggara untuk Tingkat Kelengkapan SMKI berdasarkan hasil dari pengumpulan data berdasarkan Indeks KAMI menunjukkan hasil kelengkapan penerapan SMKI pada gambar 6. Dan pada gambar 6 juga menunjukkan area merah pada bar chart terlihat pencapaian Tingkat Kelengkapan Penerapan SMKI memerlukan perbaikan pada sejumlah aspek yang ada.

Hasil dari pencapaian skor dari para responden Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset, Teknologi dan Keamanan Informasi.

1) Tata Kelola Keamanan Informasi

Hasil kalkulasi di area Tata Kelola Keamanan Informasi dari semua instansi Pemerintah Kabupaten Minahasa Tenggara sebelumnya terdapat skor 58 dengan tingkat kematangan II. Hasil ini disebabkan oleh beberapa hal.

Dari total 22 pertanyaan yang diajukan pada area Tata Kelola Keamanan informasi ini, 6 diantaranya direspon “Tidak Dilakukan” 1 diantaranya direspon “Dalam Perencanaan”, 8 diantaranya direspon “Dalam Penerapan/Diterapkan Sebagian”, dan sisanya 7 diantaranya direspon “Diterapkan Secara Menyeluruh”.

Berdasarkan tingkat kelengkapan penerapan SMKI di area Tata Kelola Keamanan Informasi dari Pemerintah Kabupaten Minahasa Tenggara sementara proses perencanaan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggung jawab untuk mengelola keamanan informasi dan kepatuhannya,

Pemerintah Kabupaten Minahasa Tenggara sementara melakukan penerapan atau diterapkan sebagian dari instansi



Gambar 5 Radar Diagram Hasil Penilaian SMKI

pemerintahan untuk meningkatkan kelengkapan penerapan SMKI di area Tata Kelola Keamanan Informasi diantaranya. Pimpinan Instansi secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait, Pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi. Semua pelaksana pengamanan informasi di Instansi memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku.

Sementara itu Pemerintah Kabupaten Minahasa Tenggara sudah menerapkan secara menyeluruh tingkat kelengkapan SMKI di area Tata Kelola Keamanan Informasi diberbagai instansi pemerintahan sudah menerapkan secara menyeluruh pengamanan informasi yang diberikan alokasi sumber daya yang sesuai untuk mengelola menjamin kepatuhan program keamanan informasi dan disetiap instansi sudah menerapkan keseluruhan pelaksana pengamanan informasi yang mencakup semua keperluan yang dipetakan dengan lengkap.

Akan tetapi Pemerintah Kab MITRA untuk di area Tata Kelola Keamanan Informasi dengan skor akhir 58 dengan tingkat kematangan II (Penerapan Kerangka Kerja Dasar) masih tergolong Rendah dengan status kesiapan “Tidak Layak”.

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area Tata Kelola Keamanan Informasi, maka Pemerintah Kabupaten Minahasa Tenggara perlu melakukan perbaikan diantaranya:

- Pimpinan harus menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.
- Disetiap Instansi sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, pemantauannya dan eskalasi pelaporannya.
- Menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanaannya.
- Menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi.
- Mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya.
- Mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

Hasil Evaluasi Akhir:

Tidak Layak

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori



264

Gambar 6 Tingkat Kelengkapan Penerapan SMKI

2) *Pengelolaan Risiko Keamanan Informasi*

Hasil kalkulasi di area Pengelolaan Risiko Keamanan Informasi dari semua instansi Pemerintah Kabupaten Minahasa Tenggara sebelumnya terdapat skor 30 dengan tingkat kematangan I+. Hasil ini disebabkan oleh beberapa hal diantaranya;

Dari total 16 pertanyaan yang diajukan pada area Pengelolaan Risiko Keamanan Informasi ini, 2 diantaranya direspon “Tidak Dilakukan”. 7 diantaranya direspon “Dalam Perencanaan”, 6 diantaranya direspon “Dalam Penerapan/Diterapkan Sebagian”, dan sisanya 1 diantaranya direspon “Diterapkan Secara Menyeluruh”.

Berdasarkan tingkat kelengkapan penerapan SMKI di area Pengelolaan Risiko Keamanan Informasi dari Pemerintah Kabupaten Minahasa Tenggara sementara dalam proses perencanaan menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan.

Pemerintah Kabupaten Minahasa Tenggara sementara melakukan penerapan atau diterapkan sebagian dari instansi pemerintahan untuk meningkatkan kelengkapan penerapan SMKI di area Pengelolaan Risiko Keamanan Informasi dan

disetiap instansi sementara melakukan program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.

Sementara itu Pemerintah Kabupaten Minahasa Tenggara sudah menerapkan secara menyeluruh langkah mitigasi risiko yang disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK dari tingkat kelengkapan SMKI di area Pengelolaan Risiko Keamanan Informasi diberbagai instansi pemerintahan.

Akan tetapi Pemerintah Kabupaten Minahasa Tenggara untuk di area Pengelolaan Risiko Keamanan Informasi dengan skor akhir 30 dengan tingkat kematangan I+ (Kondisi Awal) masih tergolong Rendah dengan status kesiapan “Tidak Layak”.

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area Pengelolaan Risiko Keamanan Informasi, maka Pemerintah Kabupaten Minahasa Tenggara perlu melakukan perbaikan diantaranya:

- a) Membuat kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya.
- b) Membuat pengelola risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan

3) *Kerangka Kerja Pengelolaan Keamanan Informasi*

Hasil kalkulasi di area Keangka Kerja Pengelolaan Keamanan Informasi dari semua instansi Pemerintah Kabupaten Minahasa Tenggara sebelumnya terdapat skor 60 dengan tingkat kematangan I+. Hasil ini disebabkan oleh beberapa hal.

Dari total 29 pertanyaan yang diajukan pada area Kerangka Kerja Pengelolaan Keamanan Informasi ini, 7 diantaranya direspon “Tidak Dilakukan”. 11 diantaranya direspon “Dalam Perencanaan”, 5 diantaranya direspon “Dalam Penerapan/Diterapkan Sebagian”, dan sisanya 6 diantaranya direspon “Diterapkan Secara Menyeluruh”.

Berdasarkan tingkat kelengkapan penerapan SMKI di area Kerangka Kerja Pengelolaan Keamanan Informasi dari Pemerintah Kabupaten Minahasa Tenggara sementara dalam proses perencanaan Merencanakan kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.

Pemerintah Kabupaten Minahasa Tenggara sementara melakukan penerapan atau diterapkan sebagian dari instansi pemerintahan untuk meningkatkan kelengkapan penerapan SMKI di area Kerangka Kerja Pengelolaan Keamanan Informasi dalam penerapan kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya.

Sementara itu Pemerintah Kabupaten Minahasa Tenggara sudah menerapkan secara menyeluruh tingkat kelengkapan SMKI di area Kerangka Kerja Pengelolaan Keamanan Informasi diberbagai instansi pemerintahan Sementara menerapkan secara keseluruhan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan.

Akan tetapi Pemerintah Kabupaten Minahasa Tenggara untuk di area Kerangka Kerja Pengelolaan Keamanan Informasi dengan skor akhir 60 dengan tingkat kematangan I+ (Kondisi

Awal) masih tergolong Rendah dengan status kesiapan “Tidak Layak”.

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area Kerangka Kerja Pengelolaan Keamanan Informasi, maka Pemerintah Kabupaten Minahasa Tenggara perlu melakukan perbaikan diantaranya:

- a) Melakukan perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk.
- b) Membuat uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal.
- c) Melakukan perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada.
- d) Melaksanakan kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala.
- e) Perlu merevisi kebijakan dan prosedur yang berlaku ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya.
- f) menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif.
- g) Melaksanakan rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten

4) *Pengelolaan Aset Informasi*

Hasil kalkulasi di area Pengelolaan Aset Informasi dari semua instansi Pemerintah Kabupaten Minahasa Tenggara sebelumnya terdapat skor 64 dengan tingkat kematangan I+. Hasil ini disebabkan oleh beberapa hal diantaranya:

Dari total 38 pertanyaan yang diajukan pada area Pengelolaan Aset Informasi ini, 6 diantaranya direspon "Tidak Dilakukan". 19 diantaranya direspon "Dalam Perencanaan", 8 diantaranya direspon "Dalam Penerapan/Diterapkan Sebagian", dan sisanya 5 diantaranya direspon "Diterapkan Secara Menyeluruh".

Berdasarkan tingkat kelengkapan penerapan SMKI di area Pengelolaan Aset Informasi dari Pemerintah Kabupaten Minahasa Tenggara sementara dalam proses perencanaan Membutuhkan rencana proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya, Rencananya definisi dari tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut, Merencanakan proses pengelolaan konfigurasi yang diterapkan secara konsisten, dan Merencanakan peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.

Pemerintah Kabupaten Minahasa Tenggara sementara melakukan penerapan atau diterapkan sebagian dari instansi pemerintahan untuk meningkatkan kelengkapan penerapan SMKI di area Pengelolaan Aset Informasi sudah diterapkan sebagian definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda, diterapkan sebagian proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten, Melakukan penerapan proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi, diterapkan proses peraturan terkait instalasi piranti lunak di aset TI milik instansi

Sementara itu Pemerintah Kabupaten Minahasa Tenggara sudah menerapkan secara menyeluruh tingkat kelengkapan SMKI di area Pengelolaan Aset Informasi diberbagai instansi pemerintahan sementara menerapkan secara menyeluruh tata tertib penggunaan komputer, email, dan intranet yang baik.

Akan tetapi Pemerintah Kabupaten Minahasa Tenggara untuk di area Pengelolaan Aset Informasi dengan skor akhir 64 dengan tingkat kematangan I+ (Kondisi Awal) masih tergolong Rendah dengan status kesiapan "Tidak Layak".

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area Pengelolaan Aset Informasi, maka Pemerintah Kabupaten Minahasa Tenggara perlu melakukan perbaikan diantaranya:

- a) Menerapkan daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? termasuk kepemilikan aset.
- b) Membuat definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku.
- c) Menyediakan daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya.

- d) Menyediakan daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
- e) Menyediakan 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.
- g) Melakukan proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda.

5) *Teknologi Dan Keamanan Informasi*

Hasil kalkulasi di area Teknologi dan Keamanan Informasi dari semua instansi Pemerintah Kabupaten Minahasa Tenggara sebelumnya terdapat skor 52 dengan tingkat kematangan I+. Hasil ini disebabkan oleh beberapa hal diantaranya:

Dari total 26 pertanyaan yang diajukan pada area Teknologi Dan Keamanan Informasi ini, 1 diantaranya direspon "Tidak Dilakukan". 18 diantaranya direspon "Dalam Perencanaan", 6 diantaranya direspon "Dalam Penerapan/Diterapkan Sebagian", dan sisanya 1 diantaranya direspon "Diterapkan Secara Menyeluruh".

Berdasarkan tingkat kelengkapan penerapan SMKI di area Teknologi Dan Keamanan Informasi ini dari Pemerintah Kabupaten Minahasa Tenggara sementara dalam proses perencanaan diantaranya:

- a) Membutuhkan rancangan perbaikan jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll).
- b) Perencanaan proses konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
- c) Disetiap instansi perlu proses secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada.
- d) Sementara dalam perbaikan jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
- e) Merencanakan proses keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.
- f) Merencanakan proses keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
- g) Perubahan dalam sistem informasi secara otomatis yang terekam di dalam log.
- h) Perlu membuat upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log.
- i) Dalam perencanaan semua upaya akses dalam log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
- j) Disetiap Instansi harus menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
- k) Disetiap instansi harus membuat perencanaan mempunyai standar dalam menggunakan enkripsi.

Pemerintah Kabupaten Minahasa Tenggara sementara melakukan penerapan atau diterapkan sebagian dari instansi

pemerintahan untuk meningkatkan kelengkapan penerapan SMKI di area Teknologi Dan Keamanan Informasi sedang melaksanakan semua sistem dan aplikasi secara otomatis sudah diterapkan mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama, Melakukan penerapan sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini, Disetiap instansi komputer *desktop* dan *server* masih dalam merepkan atau diterapkan sebagian untuk melindungi dari penyerangan virus (*malware*), Diharuskan menerapkan seluruh jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.

Sementara itu Pemerintah Kabupaten Minahasa Tenggara sudah menerapkan secara menyeluruh layanan TIK (sistem komputer) yang menggunakan internet dan sudah dilindungi dengan lebih dari 1 lapis pengamanan tingkat kelengkapan SMKI di area Teknologi Keamanan Informasi dibagi berbagai instansi pemerintahan.

Akan tetapi Pemerintah Kabupaten Minahasa Tenggara untuk di area Teknologi dan Keamanan Informasi dengan skor akhir 52 dengan tingkat kematangan I+ (Kondisi Awal) masih tergolong Rendah dengan status kesiapan “Tidak Layak”.

Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area Teknologi dan Keamanan Informasi, maka Pemerintah Kabupaten Minahasa Tenggara perlu melakukan perbaikan pada pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

IV. KESIMPULAN DAN SARAN

A Kesimpulan

Dari hasil penelitian tentang Tingkat Kematangan Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara dengan Menggunakan Indeks KAMI, dapat diketahui bahwa untuk kategori Sistem Elektronik tingkat ketergantungan TIK tergolong tinggi, Sayangnya Pemerintah Kab. MITRA tentang pengelolaan keamanan informasi masih tergolong sangat rendah dengan skor akhir yang di dapat dengan menggunakan Indeks KAMI yaitu 264 dari skor maksimum 645 dan tidak memenuhi standar SNI ISO/IEC 27001:2013, maka dari itu diperlukan perbaikan pada semua aspek yang ada yaitu pada tata kelola keamanan informasi, pengelolaan risiko keamanan, kerangka kerja keamanan informasi, pengelolaan aset, teknologi dan keamanan informasi.

B Saran

Berdasarkan kesimpulan diatas maka peneliti dapat memberikan saran-saran sebagai berikut. Pemerintah Kabupaten Minahasa Tenggara harus membuat kebijakan umum sistem manajemen keamanan informasi, Membuat kebijakan sistem manajemen keamanan informasi terkait prosedur pengendalian hak akses, Sarana untuk kedepan Pemerintahan Kabupaten Minahasa Tenggara harus melakukan peningkatan Tingkat Kelengkapan penerapan standar ISO27001 (SMKI) di area. Tata Kelola Keamanan Informasi,, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Pengelolaan Aset Informasi,

Teknologi Keamanan Informasi

V KUTIPAN

- [1] *ESET Asia Cyber-Savviness Report 2015*, 2015, *Cyber Serutity : User Knowledge, Behaviour and Attitudes In Asia*.
- [2] Dinas Kementrian Informasi Kabupaten Minahasa Tenggara (2017).
- [3] Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika. (2011). “Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik”. Jakarta, Indonesia
- [4] *Mustaqim Siga, Tony Dwi Susanto, Bakti Cahyo Hidayanto (2014) “Evaluasi Manajemen Keamanan Informasi menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur”* Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS) Surabaya.
- [5] Winda Septilia Kusumaningrum, Budi Widjanto (2016) “*Kelengkapan Dan Kematangan Sistem Keamanan Informasi Berdasarkan Indeks KAMI Pada Divisi Sampling Dan Pengujian BBPOM Kota Semarang*” Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
- [6] Rahmat Hidayat, Mohammad Suyanto, Andi Sunyoto (2018) “*Indeks Penilaian Keamanan Informasi Untuk Mengukur Kematangan Manajemen Keamanan Layanan TI (Studi Kasus : BPMP Kabupaten Gresik)*” Teknik Informatika Universitas AMIKOM Yogyakarta.
- [7] Muh. Faturachman Husin, Hans F. Wowor, Stanley D.S. Karouw (2017) “*Implementasi Indeks KAMI di Universitas Sam Ratulangi*” Teknik Informatika Universitas Sam Ratulangi.
- [8] Chalifa Chazar (2015). “*Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005*”.
- [9] Junian Dani (2008). “*Pengembangan Kebijakan Keamanan*”, FASILKOM UI, 2018
- [10] (KOMINFO, 2017). Tim Direktorat Keamanan Informasi kementerian Komunikasi dan Informatika RI. 2017. “Panduan Penerapan Sistem Manajemen Keamanan”
- [11] BSSN Badan Siber Sandi Negara, 2019. *Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)*”.
- [12] Endang Mulyatiningsih (2011). “*Riset Terapan Bidang Pendidikan & Teknik*”

TENTANG PENULIS



Penulis bernama lengkap Reynaldo Adi Putra Pratama Gala, lahir di Manado pada tanggal 22 Desember 1996 dari pasangan Bapak Marten Gala dan Ibu Jetje Maringka. Penulis merupakan anak empat dari empat bersaudara. Penulis menyelesaikan pendidikan Sekolah Dasar di SD Negeri 124 Manado pada tahun 2007, kemudian melanjutkan pendidikan di SMP Negeri 7 Manado lulus pada tahun 2011, dan pendidikan Sekolah Menengah Atas di SMK Negeri 1 Manado pada tahun 2014. Setelah lulus SMK, penulis melanjutkan pendidikan di salah satu perguruan tinggi Manado yaitu Universitas Sam Ratulangi dengan mengambil Program Studi Teknik Informatika Jurusan Teknik Elektro dan menyelesaikan studi S1 pada tahun 2019.