Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 3, No. 10, Oktober 2019, hlm. 9552-9559 http://j-ptiik.ub.ac.id

Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI

Marinda Yunella[1], Admaja Dwi Herlambang[2], Widhy Hayuhardhika Nugraha Putra[3]

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]marindayunella@student.ub.ac.id, [2]herlambang@ub.ac.id, [3]widhy@ub.ac.id

Abstrak

Teknologi informasi menekankan pada konsep penyebaran informasi untuk menunjang pelayanan publik. Informasi sendiri merupakna aset berharga yang perlu dilindungi melalui pengelolaan keamanan informasi. Saat ini pengelolaan keamanan informasi pada Dinas Komunikasi dan Informatika (KOMINFO) Kota Malang belum dilakukan secara optimal. Hal tersebut dapat dilihat dari permasalahan teknis terkait dengan kemananan informasi yang terjadi secara berulang. Pada penilaian Sistem Pemerintahan Berbasis Elektronik tahun 2018, KOMINFO memperoleh hasil yang kurang maksimal. Keamanan menjadi salah satu aspek penting dalam penilaian SPBE. Selain itu instansi juga belum melakukan sertifikasi sistem manajemen pengamanan informasi yang diwajibkan oleh Pemerintahan Pusat. Tujuan dilakukan penelitian ini adalah untuk melakukan evaluasi keamanan informasi menggunakan Indeks KAMI versi 4.0. Hasil evaluasi tersebut digunakan sebagai dasar rekomendasi perbaikan untuk menunjang peningkatan keamanan informasi sesuai dengan kelengkapan standar SNI/ISO 27001:2013. Hasil evaluasi diperoleh tingkat kelengkapan sebesar 246 dan tingkat kematangan berada pada level I+. Berdasarkan hasil evaluasi akhir KOMINFO dikategorikan sebagai belum layak terhadap kelengkapan penerapan standar SNI/ISO 27001:2013. Sehingga terdapat 9 rekomendasi pada area tata kelola, 13 rekomendasi area pengelolaan risiko, 12 rekomendasi area kerangka kerja, 16 rekomendasi area pengelolaan aset, 9 rekomendasi area teknologi dan keamanan dan 9 rekomendasi area suplemen yang diajukan untuk melengkapi kelengkapan penerapan keamanan informasi.

Kata kunci: *Keamanan Informasi, Indeks KAMI, SNI/ISO 27001:2013*

Abstract

The information technology was emphasized on concept of information share which aimed to support public service. This information was referred as valuable asset which needed to the government protection through the management of information security. Currently, the management of information security in Dinas Komunikasi dan Informatika (KOMINFO) Kota Malang has not been optimally implemented. This condition due to some technical problems related to information security issue which have been occurred repeatedly. On the evaluation of Electronic-Based Government System in 2018, KOMINFO has achieved less maximal result. The security was an important aspect in this valuation. Besides, the institution did not have certification on information security management system which was required by the Central Government. Therefore, this research aimed to evaluate the information security by means of KAMI index 4.0 version. Based on the evaluation, the result was exerted as a basic of improvement recommendation which functioned to support the process of information security improvement in appropriate to standard equipment SNI/ISO 27001:2013. Further, according to this evaluation result, it showed the Level of Completeness 246 and maturity level on level I+. Thus, from this last evaluation result, KOMINFO was categorized as not feasible to the completeness of standard implementation SNI/ISO 27001:2013. As the consequence, it resulted to 9 recommendations on governance area, 13 recommendation on risk management area, 12 recommendation on framework area, 16 recommendations on asset management area, 9 recommendations on technology and security area, and 9 recommendations on supplementary area which were proposed to complete the equipment of information security implementation.

Keywords: *Information Security, KAMI Index, SNI/ISO 27001:2013*

1. PENDAHULUAN

Penerapan teknologi informasi berfokus terhadap penyebaran informasi kepada setiap unit organisasi guna menunjang kebutuhan dan pencapaian tujuan organisasi. Informasi memiliki peran penting dalam memandu setiap keputusan yang dibuat oleh pimpinan organisasi. Oleh karena itu informasi sendiri dapat disebut sebagai suatu aset berharga yang memiliki nilai lebih dan dapat dijadikan sebagai keunggulan kompetitif bagi organisasi.

E-government merupakan salah satu contoh penerapan teknologi informasi pada sektor pemerintah yang dimanfaatkan sebagai wadah penyediaan layanan publik bagi masyarakat luas, di mana interaksi dan transaksi yang dilakukan tidak terbatas pada lingkup bisnisnya tetapi juga melibatkan masyarakat dan pemangku kepentingan lainnya (Shareef, 2016). Selain itu terdapat juga program pemerintah yang disebut dengan Sistem Pemerintahan Berbasis Elektronik (SPBE). Sistem elektronik merupakan suatu perangkat teknologi informasi yang berfungsi untuk mengelola seluruh informasi elektronik dari pengumpulan hingga penyebaran informasi terhadap khalayak publik (Kementrian Komunikasi dan Informatika, 2016). Semakin banyaknya penggunaan teknologi pada ranah Pemerintahan semakin besar pula ancaman terhadap keamanan informasi yang dikelola.

Keamanan informasi sendiri merupakan metode yang digunakan dalam melakukan perlindungan terhadap data, informasi dan sistem informasi dari kegiatan-kegiatan yang bersifat mengubah dan merusak tanpa otoritas yang telah di izinkan (Kementrian Komunikasi dan Informatika, 2008). Jika suatu informasi yang berharga mengalami masalah keamanan informasi, dapat memunculkan ancaman yang sangat berbahaya bagi organisasi. Selain itu penerapan keamanan informasi juga dapat menunjang upaya dalam meningkatkan kualitas pelayanan yang diberikan oleh pemerintah dan mengukur seberapa baik tata kelola pada pemerintah.

Berdasarkan hasil wawancara yang telah dilakukan pada Dinas Komunikasi dan Informatika Kota Malang sering terjadi permasalahan-permasalahan teknis terkait dengan keamanan informasi yang terjadi secara berulang. Permasalahan tersebut seperti serangan terhadap data server, permasalahan pada domain, permasalahan pada API yang digunakan, permasalan terkait pihak pengembang dan lain-lain.

Kemudian saat ini KOMINFO Kota Malang bertanggung jawab pada proyek penyusunan Peraturan Walikota terkait dengan pengumpulan data. Kedepannya direncanakan akan ada satu server khusus (*Data Center*) yang akan menampung seluruh data pada lingkup Pemerintah Kota Malang. Pada *data center* tersebut dibutuhkan sebuah kebijakan khusus yang mengatur terkait manajeman keamanan data dan informasi yang berfungsi sebagai arahan dan pedoman dalam pelaksanaan pengelolaan data.

KOMINFO Kota Malang juga sedang melakukan perbaikan internal dalam rangka perbaikan penilaian Sistem Pemerintahan Berbasis Elektronik (SPBE). Merujuk pada Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Pemerintah wajib melaksanakan SPBE berdasarkan prinsip-prinsip yang telah ditentukan. Salah satunya prinsip yang tertera pada pasal 2 ayat 8 tentang keamanan yang mencakup kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya yang mendukung SPBE (Peraturan Presiden RI, 2018). Berdasarkan rekomendasi penilaian SPBE sebelumnya dikatakan bahwa KOMINFO Kota Malang perlu adanya kebijakan internal pengoperasian pusat Data yang dinilai dan dievaluasi secara berkala terhadap perubahan-perubahan di internal dan eksternal serta menerapkan manajemen perubahan.

Selain itu merujuk pada Peraturan Menteri Komunikasi dan Informatika No 4 Tahun 2016 tentang Sistem Manajemen Keamanan Informasi dalam penyelenggaraan Sistem Elektronik, disebutkan bahwa sistem elektronik yang telah beroprasi wajib memiliki Sertifikat Sistem Manajemen Pengamanan Informasi dalam jangka waktu paling lambat 2 (dua) tahun. Sedangkan KOMINFO Kota Malang sampai saat ini belum melakukan sertifikasi manajeman keamanan informasi.

Berdasarkan permasalahan yang telah dijelaskan maka kegiatan evaluasi perlu dilakukan untuk memastikan keamanan informasi sudah sesuai dengan standar yang berlaku dan untuk memberikan gambaran terkait manajemen keamanan informasi yang dikelola serta menjadi bahan pertimbangan dalam pembuatan kebijakan keamanan informasi di

Kota Malang. Selain itu hasil dari evaluasi dapat dijadikan rekomendasi perbaikan untuk menunjang peningkatan nilai pada evaluasi SPBE yang akan dilakukan oleh Dinas Komunikasi dan Informatika Kota Malang serta persiapan dalam melakukan sertifikasi keamanan informasi.

Evaluasi keamanan informasi dilakukan menggunakan alat evaluasi indeks KAMI yang memiliki tujuan untuk menganalisis tingkat kesiapan dari penerapan keamanan informasi di sebuah organisasi. Selain melakukan evaluasi menggunakan indeks KAMI, dilakukan juga peninjauan hasil dari evaluasi terhadap kontrol keamanan yang terdapat pada ISO *Annex A.* Hal ini bertujuan untuk mengetahui persyaratan yang belum terpenuhi pada Indeks KAMI dan tindakan apa yang harus dilakukan terkait pengelolaan keamanan informasi. Indeks KAMI dan ISO/IEC 27001 sendiri dipilih berdasarkan Peraturan Mentri Komunikasi dan Informatika no 4 tahun 2016.

2. LANDASAN KEPUSTAKAAN

Terdapat beberapa referansi yang digunakan dalam mendukung penelitian ini terkait dengan keamanan informasi. Salah satunya yaituPPenelitian yang dilakukan oleh Mufti Rizal dan Yudho Giri Sucahyo (2013) dengan judul *Studi Tentang Kesiapan Area Kerangka Keamanan Informasi Berdasarkan Penilaian Indeks Keamanan Informasi Di Kementerian XYZ.* Dilatarbelakangi oleh beberapa kejadian terkait ancaman pada sektor keamanan informasi sistem pemerintahan serta beberapa data yang menunjukkan bahwa keamanan informasi pada Pemerintahan Indonesia tergolong lemah. Penelitian tersebut meneliti terkait implementasi teknologi informasi dan komunikasi yang dianjurkan oleh salah satu kerangka kerja keamanan informasi yang dianggap sesuai dengan kondisi yang tampak, yaitu penilaian indeks keamanan informasi (KAMI). Penilaian dilakukan untuk mengukur kesiapan penerapan kerangka kerja keamanan informasi di Kementerian XYZ. Hasil penilaian menunjukkan bahwa tingkat kematangan kerangka kerja keamanan informasi Kementerian XYZ berada pada Level I+. Dimana untuk melakukan perbaikan berkelanjutan perlu didukung oleh suatu kebijakan keamanan informasi (Rizal dan Sucahyo, 2013).

Evaluasi adalah suatu proses untuk menentukan atau mengukur seberapa baik sebuah *artifact* bekerja pada suatu organisai yang mengimplementasikan (Cronholm dan Göbel, 2016) . *Artifact* pada ranah teknologi informasi mengarah pada suatu sistem berbasis komputer yang digunakan oleh organisasi dalam menjalankan proses bisnisnya. Tujuan dari dilakukannya evaluasi adalah untuk menghasilkan sebuah informasi dan berguna dalam menemukan solusi atas masalah yang terjadi atau melakukan perbaikan terhadap *artifact* yang ada saat ini.

Keamanan informasi merupakan sebuah metode yang digunakan dalam melakukan perlindungan terhadap data, informasi dan sistem informasi dari kegiatan-kegiatan yang bersifat mengubah dan merusak tanpa otoritas yang telah di izinkan(Kementrian Komunikasi dan Informatika, 2008).

Indeks KAMI adalah instrumen pertimbangan untuk penilaian tingkat ketersediaan dan kematangan yang digunakan untuk mengukur implementasi dari manajemen keamanan informasi pada suatu organisasi. Selain mengevaluasi juga dapat menganalisis kesamanaan dengan aspek pedoman pada standar SNI ISO 27001:2013 (Badan Siber dan Sandi Negara, 2019). Indeks KAMI versi 4.0 merupakan revisi terbaru yang dikeluarkan pada bulan Maret tahun 2019. Perbedaan indeks KAMI versi 4.0 dengan versi yang sebelumnya terletak pada penambahan modul suplemen yang membahas aspek risiko keamanan informasi terkait keterlibatan pihak ketiga atau pihak eksternal dalam rantai pasok (*Supply Chain)*, risiko terhadap layanan berbasis infrastruktur awan *(Cloud Service)*, dan risiko terkati perlindungan data pribadi yang hanya boleh digunakan sesuai dengan persyaratan hukum.

ISO/IEC 27001:2013 merupakan suatu metode khusus dalam melakukan standarisasi keamanan informasi yang diakui diseluruh dunia. Standar ini memiliki karakteristik berupa kriteria keamanan (kontrol) yang telah disusun sedemikian rupa yang harus dilakukan sebuah instansi atau organisasi dalam pembangunan sebuah Sistem Manajemen Keamanan Informasi (SMKI)(Kementrian Komunikasi dan Informatika, 2017). Risiko dijadikan bagian dari pertimbangan dan perhatian khusus dalam pembentukan kontrol-kontrol keamanan guna menunjang kesuksesan dan pencegahan terjadinya serangan terhadap aset berharga.

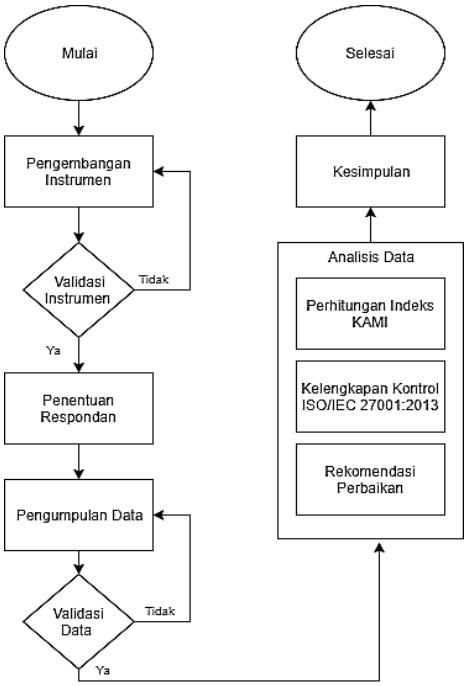
Seluruh area yang terdapat pada indeks KAMI didasarkan pada aspek keamanan yang

telah ditetapkan dalam standar ISO/IEC 27001:2013. Indeks KAMI merangkum 14 area kontrol keamanan informasi yang ada pada lampiran *Annex A* ISO/IEC 27001:2013 digambarkan pada Gambar 1.

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi	Suplemen
Security Policies	√	√	√			√
Organisation of Information Security	√	√	√			
Human Resource Security	√		√	√		√
Asset Management		√		√		√
Access Control				√	√	√
Cryptography				√	√	√
Physical and Environmental Security				√		
Operations Security			√	√	√	√
Communications Security	√		√	√	√	√
Systems Acquisition, Development and Maintenance			√	√	√	
Supplier Relationships				√		
Information Security Incident Management	√	√	√	√	√	√
Information Security Aspects of BCM	√	√	√		√	√
Compliance	√	√	√	√	√	√

Gambar 1. Hubungan ISO/IEC 27001:2013 dan Indeks KAMI versi 4.0

3. METODE PENELITIAN



Gambar 2. Metode Penelitian

Dalam Gambar 2. menunjukan alur metode penelitian dengan penjelasan yang pertama mulai melakukan pengembangan instrumen berdasarkan pertanyaan pada setiap area Indeks KAMI. Instrumen tersebut akan dijadikan sebagai pedoman wawancara untuk pengumumpulan data terkait keamanan informasi pada KOMINFO Kota Malang. Setelah melakukan pengembangan instrumen, dilakukan validasi instrumen kepada orang yang ahli pada bidang tata kelola teknologi informasi. Memilih responden yang sesuai dengan ranah keamanan informasi pada indeks KAMI dan menentukan area yang akan di evaluasi sesuai dengan persetujuan responden selaku pihak yang mengetahui kondisi tata kelola keamanan informasi saat ini. Melakukan pengumpulan data dengan cara melakukan wawancara tertutup pada responden yang sesuai dengan persyaratan. Melakukan verifikasi data melalui teknik *checklist*, dimana verifikasi ini digunakan untuk memastikan data yang diberikan sesuai dengan keadaan aslinya. Melakukan analisis data yang didapatkan melalui perhitungan hasil kuesioner memakai formula indeks KAMI, kemudian melakukan perbandingan hasil evaluasi dengan kontrol yang ada pada ISO 27001:2013 serta membuat rekomendasi. Memberikan kesimpulan dan saran untuk Dinas Komunikasi dan Informatika Kota Malang sebagai langkah perbaikan kedepannya.

4. HASIL DAN ANALISIS

Sebelum melakukan proses wawancara terkait penilaian keamanan informasi, dilakukan pendefinisian ruang lingkup penilaian. Ruang lingkup penilaian pada penelitian ini adalah data dan informasi yang dikelola oleh Dinas Komunikasi dan Informatika Kota Malang dan pengelolaan sistem informasi pelayanan yang terdapat pada Dinas Komunikasi dan Informatika Kota Malang.

Dalam kategori sistem elektronik dilakukan penilaian untuk memberikan gambaran terkait keadaan sistem elektronik yang digunakan.

Tabel 1. Data Penilaian Kategori Sistem Elektronik

Bagian I: Kategori Sistem Elektronik		
Total Pertanyaan		**10**
Hasil Jawaban Responden		
Pilihan Jawaban	**Hasil**	**Skor**
[A]	1	5
[B]	7	2
[C]	2	1
Total Skor Kategori Sistem Elektronik		**21**

Berdasarkan hasil penilaian yang ditunjukkan pada Tabel 1. didapatkan total skor yang didapat pada kategori sistem elektronik adalah sebesar 21 yang dapat dikategorikan sebagai “Tinggi”. Kemudian untuk hasil dari data penilaian pada area tata kelola keamanan informasi, area pengelolaan risiko keamanan informasi, area kerangka kerja keamanan informasi, area pengelolaan aset, area teknologi dan keamanan informasi dan area suplemen dapat dilihat pada tabel berikut.

Tabel 2. Penilaian Pengamanan Tata Kelola

Bagian II: Tata Kelola Keamanan Informasi			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Pengamanan**		
	KP 1	**KP 2**	**KP 3**
Tidak dilakukan	0	0	0
Dalam Perencanaan	0	4	0
Dalam penerapan atau diterapkan sebagian	6	3	0
Diterapkan secara menyeluruh	2	1	0
Total Nilai Tata Kelola			**44**

Tabel 3. Penilaian Pengamanan Pengelolaan Risiko

Bagian III: Pengelolaan Risiko			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Pengamanan**		
	KP 1	**KP 2**	**KP 3**
Tidak dilakukan	0	0	0
Dalam Perencanaan	7	0	0
Dalam penerapan atau diterapkan sebagian	2	4	0
Diterapkan secara menyeluruh	1	0	0
Total Nilai Pengelolaan Risiko			**22**

Tabel 4. Penilaian Pengamanan Kerangka Kerja

Bagian IV: Kerangka Kerja			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Pengamanan**		
	KP 1	**KP 2**	**KP 3**
Tidak dilakukan	0	0	0
Dalam Perencanaan	4	6	0
Dalam penerapan atau diterapkan sebagian	8	4	0
Diterapkan secara menyeluruh	1	0	0
Total Nilai Kerangka Kerja			**48**

Tabel 5. Penilaian Pengamanan Pengelolaan Aset

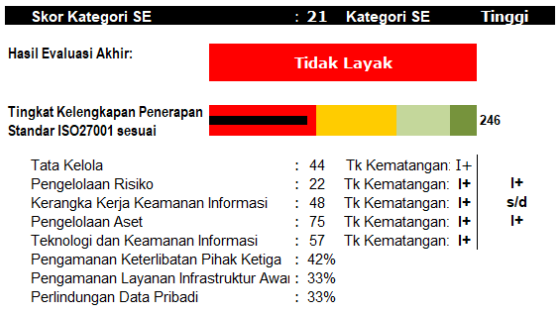
Bagian V: Pengelolaan Aset			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Pengamanan**		
	KP 1	**KP 2**	**KP 3**
Tidak dilakukan	0	0	0
Dalam Perencanaan	9	5	0
Dalam penerapan atau diterapkan sebagian	13	3	0
Diterapkan secara menyeluruh	2	2	0
Total Nilai Pengelolaan Aset			**75**

Tabel 6. Penilaian Pengamanan Teknologi dan keamanan

Bagian VI: Teknologi dan Keamanan			
Hasil Jawaban Responden			
Status Pengamanan	**Kategori Pengamanan**		
	KP 1	**KP 2**	**KP 3**
Tidak dilakukan	0	0	0
Dalam Perencanaan	2	5	0
Dalam penerapan atau diterapkan sebagian	11	5	0
Diterapkan secara menyeluruh	1	0	0
Total Nilai Teknologi dan keamanan			**57**

Tabel 7. Penilaian Pengamanan Teknologi dan keamanan

Bagian VII: Suplemen	
Hasil Jawaban Responden	
Status Pengamanan	**KP 1**
Tidak dilakukan	0
Dalam Perencanaan	46
Dalam penerapan atau diterapkan sebagian	7
Diterapkan secara menyeluruh	0



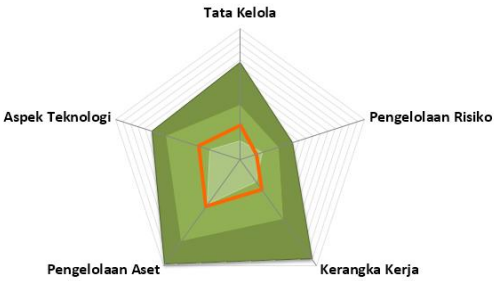
Gambar 3. Hasil Penilaian Kelengkapan dan Pengamanan

Dari hasil pada Gambar 3 dapat disimpulkan bahwa kategori sistem elektronik, Dinas Komunikasi dan Informatika mencapai skor 21 yang berarti bahwa sistem elektonik sudah menjadi bagian yang tidak terpisahkan dalam aktivitas organisai dan dikategorikan sebagai kategori **"Tinggi"**. Sedangkan untuk tingkat kelengkapan terhadap pemenuhan standar ISO/IEC 27001 sesuai dengan kategori SE mencapai total 246 masih tergolong **"Tidak Layak"**.

Tabel 8. Persentase Pencapaian Tingkat Kematangan

Keterangan	Area 1	Area 2	Area 3	Area 4	Area 5
Skor Responden	44	22	48	75	57
Presentase	34,6 %	30,6 %	30,2 %	44,6 %	47,5 %
Tingkat Kematangan	I+	I+	I+	I+	I+

Bedasarkan Tabel 8. pada area 1 yaitu area tata kelola keamanan informasi mendapatkan skor 44 dengan presentase pencapaian sebesar 34,6% dan mencapai tingkat kematangan level I+, pada area 2 yaitu area pengelolaan risiko mendapatkan skor 22 dengan presentase pencapaian sebesar 30,6% dan mencapai tingkat kematangan level I+, pada area 3 yaitu area kerangka kerja mendapatkan skor 48 dengan presentase pencapaian sebesar 30,2% dan mencapai tingkat kematangan level I+, pada area 4 yaitu area pengelolaan aset mendapatkan skor 75 dengan presentase pencapaian sebesar 44,6% dan mencapai tingkat kematangan level I+, pada area 5 yaitu area teknologi dan keamanan mendapatkan skor 57 dengan presentase pencapaian sebesar 47,5% dan mencapai tingkat kematangan level I+. Area yang terakhir adalah area suplemen dimana mendapatkan rincian pada aspek pengamanan pihak ketiga mendapat skor 1,26 dengan presentase sebesar 42%, aspek Aspek layanan infrastruktur awan (*cloud service*) mendapat skor 1,0 dengan presentase sebesar 33% dan aspek perlindungan data pribadi mendapat skor 1,0 dengan presentase sebesar 33%.



Gambar 4. Diagram Radar Tingkat Kelengkapan

Pada diagram radar yang disajikan pada Gambar 4. dapat diketahui cakupan penerapan keamanan informasi terhadap kerangka kerja dasar, penerapan operasional dan kepatuhan terdapat standar ISO/IEC 27001. Radar berwarna oren merupakan area cakupan responden yang menunjukkan bahwa kerangka kerja dasar pada aspek teknologi, pengelolaan aset dan kerangka kerja sudah terpenuhi. Namun untuk pengelolaan risiko Dinas Komunikasi dan Informatika belum memenuhi sepenuhnya. Untuk area yang paling baik diantara kelima area dan paling mendekati pemenuhan terhadap standar ISO 27001 adalah area tata kelola keamanan informasi.

5. PEMBAHASAN

Berdasarkan hasil penilaian maka dapat ditemukan beberapa aspek pertanyaan yang belum terpenuhi, belum diterapkan atau pun masih dalam proses perencanaan penerapan. Aspek-aspek tersebut tersebut diusulkan rekomendasi perbaikannya berdasarkan tinjauan analisis antara kontrol *Annex A*, pertanyaan pada Indeks KAMI dan ISO *Information Security Management System documentation checklist.*

Pada area tata kelola keamanan informasi secara garis besar, Dinas Komunikasi dan Informatika Kota Malang perlu membuat beberapa kebijakan, prosedur dan kerangka kerja terkait transfer informasi. Memasukkan pernyataan terkait peran dan tanggungjawab pengamanan informasi kedalam perjanjian kontrak. Menetapkan dan mendokumentasikan program kerja terkait dengan manajemen kesinambungan bisnis. Mendefinisikan dan mendokumentasikan seluruh peran dan tanggungjawab pengelola kepatuhan keamanan informasi. Mendefinisikan kebijakan, prosedur pengukuran kinerja keamanan. Menetapkan terget dan sasaran pencapaian keamanan informasi. Mendokumentasikan seluruh kepatuhan keamanan informasi terhadap persyaratan hukum. Mendefinisikan pengelolaan manajemen insiden yang terdokumentasi.

Pada area pengelolaan risiko informasi secara garis besar, Dinas Komunikasi dan Informatika Kota Malang perlu mendefinisikan sebuah program kerja tertulis terkait dengan pengelolaan risiko keamanan informasi yang terdokumentasi. Pengelolaan risiko mencakup peran dan tanggungjawab pengelola, kerangka kerja dan prosedur penanganan risiko, pengelompokan dan hubungan klasifikasi aset informasi, penetapan ambang batas risiko, program kajian risiko, penyusunan langkah mitigasi risiko, alokasi sumberdaya untuk penanganan risiko, evaluasi dan status penerapan pengelolaan risiko, kepatuhan terhadap pengelolaan risiko dan pengkajian secara berkala program pengelolaan risiko.

Pada area kerangka kerja keamanan informasi secara garis besar, Dinas Komunikasi dan Informatika Kota Malang perlu mendefinisikan prosedur terkait pengkomunikasian kebijakan instansi kepada seluruh pihak. Penambahan persyaratan pada dokumen kontrak terkait keamanan sumberdaya manusia. Mendefinisikan prosedur yang mengelola aspek pengecualian. Mendefinisikan prosedur dan pedoman mengenai kegiatan pengembangan perangkat lunak. Membuat prosedur terkait dengan akuisisi, pengembangan, dan pemeliharaan sistem. Mendefinisikan kerangka kerja terkait kontrol insiden keamanan informasi mencakup strategi kesinambungan bisnis. Melakukan tinjauan kelayakan terhadap prosedur dan kebijakan kemanan informasi. Mendefinisikan pelaksanaan program audit internal.

Pada area pengelolaan aset keamanan informasi secara garis besar, Dinas Komunikasi dan Informatika Kota Malang perlu mendefinisikan kebijakan terkait klasifikasi informasi. Mendefinisikan kebijakan kontrol akses yang lebih spesifik untuk setiap aset informasi. Mendokumentasikan seluruh prosedur operasi. Mendefinisikan proses pengelolaan konfigurasi. Membuat dokumentasi kebijakan klasifikasi informasi. Kebijakan mencakup aturan dan otorisasi waktu penyimpanan untuk klasifikasi data. Meningkatkan peran manajemen insiden. Menetapkan strategi pencadangan. Mendefinisikan prosedur keamanan serta batasan-batasan keamanan. Instansi harus memeriksa dan mendokumentasikan catatan identitas dan pemeriksaan latar belakang. Kebijakan tentang penghancuran data. Kebijakan, prosedur, pedoman dan aturan yang mendukung proses penghentian. Mendokumentasikan semua persyaratan kepatuhan eksternal terkait HKI. Mendefinisikan prosedur keamanan berkaitan dengan pengamanan transfer aset.

Pada area teknologi dan keamanan informasi secara garis besar, Dinas Komunikasi dan Informatika Kota Malang perlu mengimplementasi dan mendokumentasikan perlindungan berlapis pada jaringan. Melakukan pengelolaan catatan log dari berbagai kegiatan, peristiwa, dan insiden. Mendefinisikan kebijakan khusus terkait kontrol kriptografi. Dokumetasi terkait pengelolaan kontrol *malware*. Mendefinisikan strategi, kebijakan, prosedur dan pedoman mengenai kegiatan pengembangan perangkat lunak dan sistem. Mendefinisikan sebuah kebijakan tertulis terkait pengkajian keamanan informasi yang telah diterapkan.

Pada area suplemen secara garis besar, Dinas Komunikasi dan Informatika Kota Malang perlu memasukkan aspek kepatuhan keamanan informasi pada setiap dokumen kontrak pihak ketiga. Mendefinisikan sebuah kebijakan tertulis terkait pengelolaan subkontraktor atau alih daya pihak ketiga. Instansi perlu menetapkan sebuah kebijakan tertulis terkait proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau keamanan informasi dalam hubungan dengan pihak ketiga. Mendefinisikan prosedur kontrol bagi pihak ketiga terkait perubahan formal yang mencakup dokumen kebijakan dan pedoman pengendalian perubahan. Instansi perlu menetapkan sebuah kebijakan dan prosedur manajemen media atau aset yang dapat dipindahkan atau digunakan oleh pihak ketiga. Mendefinisikan peran manajemen insiden keamanan informasi dalam hubungannya dengan pihak ketiga. instansi perlu menetapkan perencanaan persyaratan dan program kerja yang berkaitan dengan manajeman kesinambungan bisnis dan kontrol keamanan informasi yang penting selama insiden. Mendefinisikan sebuah kebijakan tertulis terkait pengelolaan layanan infrastruktur awan (*Cloud Service*). Menetapkan program pengelolaan keamanan informasi terkait perlindungan data pribadi.

6. PENUTUP

Berdasarkan hasil penelitian yang telah dilakukan dapat disimpulkan bahwa hasil evaluasi akhir pada penilaian Indeks KAMI, Dinas Komunikasi dan Informatika Kota Malang mendapatkan status tidak layak dengan tingkat kelengkapan penerapan standar ISO 27001 yang sesuai mencapai skor 246. Untuk penilaian tingkat kematangan rata-rata berada pada level I+. Kemudian berdasarkan hasil analisis yang telah dilakukan, muncul beberapa rekomendasi yang dapat dipertimbangkan oleh Dinas Komunikasi dan Informatika Kota Malang untuk perbaikan penerapan kemanan informasi serta peningkatan pada penilaian Indeks KAMI. Pada area tata kelola keamanan informasi terdapat 9 rekomendasi, area pengelolaan risiko terdapat 13 rekomendasi, area kerangka kerja terdapat 12 rekomendasi, area pengelolaan aset terdapat 16 rekomendasi, area teknologi dan keamanan informasi terdapat 9 rekomendasi dan area

suplemen terdapat 9 rekomendasi yang diusulkan.

Berdasarkan penelitian yang telah dilakukan terdapat beberapa usulan yang dapat dipertimbangkan untuk penelitian selanjutnya yaitu melakukan pengembangan prosedur keamanan yang berikaitan dengan manajemen layanan teknologi informasi menggunakan kerangka kerja ITIL versi 4.0 praktik *Information Security Management* atau melakukan pengembangan prosedur analisis risiko keamanan informasi menggunakan kerangka kerja manajemen risiko yang dikembangkan oleh *National Institute of Standards and Technology*.

7. DAFTAR PUSTAKA

Cronholm, S. and Göbel, H., 2016. Evaluation of the Information Systems Research Framework : Empirical Evidence from a Design Science Research Project. *The Electronic Journal Information Systems Evaluation*, 19(3), pp.158–168.

Kementrian Komunikasi dan Informatika, 2008. Panduan Topologi dan Keamanan Sistem Informasi.

Kementrian Komunikasi dan Informatika, 2016. Peraturan Menteri Komunikasi dan Informatika RI nomor 4 Tahun 2016 tentang Sistem manajemen Pengamanan informasi. 4(1), p.29.

Kementrian Komunikasi dan Informatika, 2017. Panduan Penerapan Sistem Manajemen Keamanan Informasi (SMKI). (September).

Peraturan Presiden RI, 2018. Sistem Pemerintahan Berbasis Elektronik. p.Nomor 95 Tahun 2018.

Rizal, M. and Sucahyo, Y.G., 2013. A study on the preparedness of information security framework area based on the assessment of information security index in Ministry of XYZ. *2013 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2013*, (March), pp.55–59.

Shareef, S.M., 2016. Enhancing Security of Information in E- Government Enhancing Security of Information in E-Government. *Journal of Emerging Trends in Computing and Information Sciences*, 7(3), pp.139–146.