Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor

Hadiati Agus Pratiwi[1], Lily Wulandari[2]

[1,2] Magister Manajemen Sistem Informasi Universitas Gunadarma, Depok, Indonesia
Corresponding Authors : hadiahadiati@gmail.com

Abstract - *Communications and Informatics Office of Bogor Municipality is a government agency that has the task of assisting the Mayor of Bogor in carrying out Government Affairs in the field of Communication, Informatics, Statistics, and Encryption management that has implemented e-Government in its public services. The impact of the e-Government's implementation in public services with the increasing communication and exchange of data electronically causes vulnerabilities in information and communication system transactions which greatly affect the quality and security of information, so that the management of information security becomes very important for the Communications and Informatics Office of Bogor Municipality. This research was conducted to determine the level of readiness of information security management at the Communications and Informatics Office of Bogor Municipality using the Information Security Index (KAMI Index) Version 4.0 according to the security aspects defined by the ISO/IEC 27001:2013 standard made by the National Cyber and Crypto Board (BSSN). by evaluating various areas that are the target of the application of information security through the interview process. The evaluation result of the Electronic System Category obtained value of 35 and included in the Strategic Category illustrating that the use of electronic systems is an integral strategic part in supporting ongoing work processes. The evaluation result of the five areas of information security obtained a total score of 395 at the Basic Framework stage with Maturity Levels I+ to II. Based on the evaluation results, recommendations are prioritized at the lowest maturity level, namely the Information Security Risk Management area so that in the next evaluation there can be an increase in the level of information security maturity until it reaches the expected maturity level according to ISO 27001 compliance standards, which is at level III.*

Keywords: e-Government, information security management, KAMI Index

1. PENDAHULUAN

Kemajuan teknologi dimanfaatkan secara positif dalam proses penyelenggaraan pemerintahan melalui penerapan *e-Government.* Hal ini terjadi setelah adanya Instruksi Presiden (Inpres) Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan e-Government [1]. Pemanfaatan kemajuan teknologi ini untuk meningkatkan efisiensi, efektifitas, transparansi dan akuntabilitas pelayanan publik melalui layanan pemerintahan berbasis elektronik sesuai dengan Peraturan Presiden (Perpres) Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik [2].

Melalui penerapan *e-Government* dalam proses penyelenggaraan pemerintahan, pemerintah dapat mengoptimalkan perkembangan kemajuan teknologi informasi dalam proses birokrasi dengan membentuk jaringan sistem manajemen dan proses kerja yang terintegrasi. Hal ini menyebabkan antar instansi pemerintah dapat bekerja secara terpadu, memudahkan dan menyederhanakan dalam mengakses informasi dan layanan publik pemerintah sehingga masyarakat dan para pemangku kepentingan lainnya

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

dapat memanfaatkan informasi dan layanan publik pemerintah secara optimal melalui berbagai macam website dan aplikasi layanan publik untuk menarik investasi, memberikan informasi dan memperbaiki layanan publiknya. Dampak negatif yang ditimbulkan seiring dengan banyaknya jumlah aplikasi pelayanan masyarakat tersebut memunculkan kerawanan dalam transaksi sistem informasi dan komunikasi.

Keamanan informasi dan kewaspadaan terhadap bahaya bocornya informasi menjadi hal terpenting dalam penggunaan teknologi informasi, terutama informasi yang berklasifikasi dan bernilai strategis. Setiap informasi harus terjamin keamanan dan kerahasiaannya dari segala ancaman seperti akses, penggunaan, pengungkapan, gangguan, modifikasi atau perusakan dari pihak yang tidak memiliki otoritas. Maka apapun bentuk informasi yang digunakan, baik yang tersimpan atau disebarluaskan harus selalu terlindungi.

Sejalan dengan semakin banyaknya informasi yang disajikan pemerintah sebagai bagian dari pelayanan semakin besar pula tantangan terhadap keamanan informasi. Keamanan informasi menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Semua pihak terutama pejabat pemangku kebijakan harus mengerti arti pentingnya pengamanan informasi dan menyadari segala potensi kerawanan dalam transaksi sistem informasi dan komunikasi.

Pemerintah Kota Bogor dalam hal ini Dinas Komunikasi dan Informatika Kota Bogor melakukan penilaian mandiri (*self assessment*) terhadap aspek keamanan sistem informasi untuk mengetahui tingkat kesiapan dalam mengantisipasi ancaman terhadap keamanan informasi dan penyalahgunaan teknologi *informasi dalam penyelenggaraan layanan* e-Government. Penilaian mandiri ini menggunakan Indeks Keamanan Informasi (Indeks KAMI) berupa aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevalusi tingkat kesiapan (kelengkapan dan kematangan) penerapan keamanan informasi di sebuah organisasi sesuai aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013 yang dibuat oleh Badan Sandi dan Siber Nasional (BSSN).

2. TINJAUAN PUSTAKA

2.1. e-Government

*e-Governmen*t merupakan suatu proses layanan publik dari instansi pemerintah yang memanfaatkan teknologi informasi dan komunikasi. Manajemen pemerintahan dapat menjadi lebih efisien, dan memicu perubahan sosial di masyarakat dengan utilisasi teknologi informasi dan komunikasi ini. Implementasi e-government memperluas jangkauan layanan pemerintah karena tidak lagi dibatasi lokasi fisik dari instansi pemberi layanan [3].

e-Government memberikan peluang baru untuk meningkatkan kualitas pemerintahan, dengan cara ditingkatkannya efisiensi, layanan-layanan baru, peningkatan partisipasi warga dan adanya suatu peningkatan terhadap global information infrastructure. *e-government* akan meningkatkan kualitas pelayanan informasi publik sebagai jalan untuk mewujudkan good governance. Melalui *e-government*, pelayanan pemerintah akan berlangsung secara transparan, dapat dilacak prosesnya, sehingga dapat dianggap akuntabel. Unsur penyimpangan dapat dihindarkan dan pelayanan dapat diberikan secara lebih efektif dan efisien [4].

2.2. Keamanan Informasi

Menurut G. J. Simons, keamanan sistem informasi adalah bagaimana dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik [5]. Menurut ISO/IEC 27002 (2005) keamanan informasi

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

adalah perlindungan informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis, meminimalkan risiko bisnis, dan memaksimalkan laba atas investasi dan peluang bisnis. Pada ISO/IEC 27001 (2013) sistem manajemen keamanan informasi menjaga kerahasiaan, integritas dan ketersediaan informasi dengan menerapkan proses manajemen risiko dan meyakinkan pihak yang berkepentingan bahwa risiko dikelola dengan baik. Sistem manajemen keamanan informasi merupakan bagian dari dan terintegrasi dengan proses organisasi dan struktur manajemen secara keseluruhan [6].

2.3. Standar Nasional Indonesia (SNI) ISO/IEC 27001:2013

Standar Nasional Indonesia ISO/IEC 27001:2013 merupakan sebuah standar internasional keamanan informasi yang memuat persyaratan-persyaratan yang harus dipenuhi dalam usaha menggunakan konsep-konsep keamanan informasi yang berlaku secara internasional pada sebuah organisasi. SNI ISO/IEC 27001:2013 mensyaratkan penetapan sasaran kontrol dan kontrol keamanan informasi yang meliputi 14 area pengamanan sebagai berikut [7] :

a. Kebijakan keamanan informasi
b. Organisasi keamanan informasi
c. Sumber daya manusia menyangkut keamanan informasi
d. Manajemen asset
e. Akses control
f. Kriptografi
g. Keamanan fisik dan lingkungan
h. Keamanan operasi
i. Kemanaan Komunikasi
j. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
k. Hubungan dengan pemasok
l. Pengelolaan insiden keamanan informasi
m. Manajemen kelangsungan usaha (business continuity management)
n. Kepatuhan

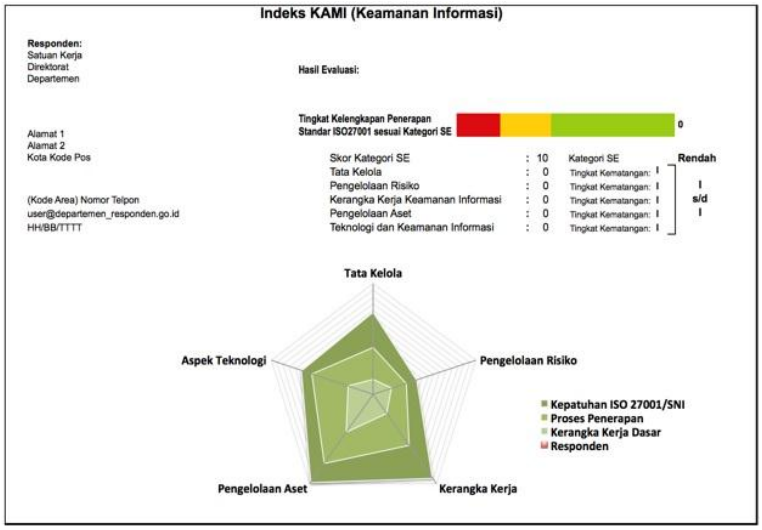
Merujuk pada Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN), menyebutkan bahwa BSSN mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan melakukan konsolidasi semua unsur yang terkait dengan keamanan siber. Terkait hal tersebut BSSN meneruskan program yang sebelumnya dilaksanakan oleh Kementerian Kominfo yakni penerapan indeks KAMI untuk menganalisa dan mengevalusi tingkat kesiapan (kelengkapan dan kematangan) penerapan keamanan informasi untuk seluruh instansi pemerintah pusat dan daerah sesuai dengan kriteria pada SNI ISO/IEC 27001 sebagai bahan perbaikan yang harus dilakukan oleh BSSN dan Instansi Pemerintah dalam mendukung penyelenggaraan SPBE atau e-Government [8].

2.4. Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 sebagai alat evaluasi

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di suatu organisasi. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh Standar ISO/IEC 27001:2013. Dashboard Penilaian Indeks KAMI Versi 4.0 dapat dilihat pada gambar 1 [9].



Gambar 1. Dashboard Penilaian Indeks KAMI Versi 4.0 *(Sumber : Badan Siber dan Sandi Negara, 2019)*

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan snapshot indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

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 (stakeholder).

Khusus untuk Instansi Pemerintah, penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggung jawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Pertukaran informasi dan diskusi dengan instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari *lesson learned* yang sudah dilalui.

Proses Evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area di bawah ini [9] :

a. Kategori Sistem Elektronik yang digunakan Instansi
b. Tata Kelola Keamanan Informasi
c. Pengelolaan Risiko Keamanan Informasi
d. Kerangka Kerja Keamanan Informasi
e. Pengelolaan Aset Informasi
f. Teknologi dan Keamanan Informasi
g. Suplemen : Area evaluasi untuk aspek pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan (Cloud Service) dan perlindungan data pribadi.

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

Pertanyaan dikelompokkan untuk 2 keperluan. Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Pengelompokkan kedua dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja CMMI (Capability Maturity Model for Integration). Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga. Korelasi antara skor akhir kategori sistem elektronik dengan status kesiapan area pengamanan dapat dilihat pada tabel 1.

Tabel 1. Tabel Korelasi terhadap Skor Kategori Sistem Elektronik

KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

(Sumber : Badan Siber dan Sandi Negara, 2019)

Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai [9] :

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

Sebagai awal penilaian semua responden akan dikategorikan ke dalam kategori kematangan tingkat I. Untuk penilaian yang lebih detil, tingkat kematangan tersebut diuraikan kembali dengan rentang tingkat kematangan seperti didefinisikan dalam tabel 2.

Tabel 2. Matrik Rentang Tingkat Kematangan

Tata Kelola Keamanan Informasi	I	I+	II	II+	III	III+	IV		
Pengelolaan Risiko Keamanan Informasi	I	I+	II	II+	III	III+	IV	IV+	V
Kerangka Kerja Keamanan Informasi	I	I+	II	II+	III	III+	IV	IV+	V
Pengelolaan Aset Informasi	I	I+	II	II+	III				
Teknologi dan Keamanan Informasi	I	I+	II	II+	III	III+	IV		

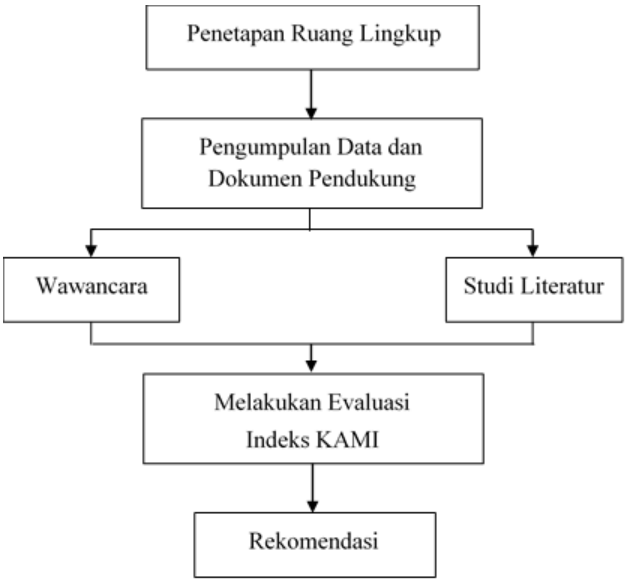
(Sumber : Badan Siber dan Sandi Negara, 2019)

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

3. METODE

3.1. Kerangka Penelitian

Kerangka penelitian merupakan langkah-langkah yang dibuat dalam suatu tahapan penelitian dan sangat diperlukan agar rangkaian penelitian dapat terarah, teratur dan sistematis. Langkah-langkah yang dilakukan dalam penelitian ini dapat dilihat pada gambar 2.



Gambar 2. Langkah-langkah yang dilakukan dalam penelitian

3.2. Penetapan Ruang Lingkup

Penetapan ruang lingkup dilakukan dengan mendefinisikan batasan penelitian dan penilaian yang sesuai dengan kepentingan penilaian Indeks KAMI. Penelitian dilakukan di Dinas Komunikasi dan Informatika Kota Bogor untuk mengevaluasi tingkat kesiapan pengamanan informasi menggunakan Indeks KAMI versi 4.0. Metode yang digunakan dalam penelitian ini adalah metode deskriptif dengan pendekatan kualitatif.

3.3. Pengumpulan data dan dokumen pendukung

3.3.1. Wawancara

Pengumpulan data dan informasi dilakukan melalui wawancara dilengkapi dengan dokumen-dokumen terkait sebagai bukti pendukung dalam bentuk Peraturan, Standar Operasional Prosedur (SOP), dan data-data terkait pelaksanaan kegiatan.

3.3.2. Studi literatur

Pengumpulan materi sebagai dasar untuk mencari teori-teori yang dibutuhkan dalam penelitian dilakukan dengan cara membaca dan merangkum melalui beberapa referensi penelitian terdahulu seperti

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

jurnal penelitian, text book yang membahas mengenai materi yang dipakai, serta e-book berkaitan dengan keamanan informasi sehingga diharapkan dapat menunjang dalam proses penelitian.

3.4. Penentuan Model Evaluasi

Model evaluasi yang digunakan untuk mengukur tingkat kesiapan pengamanan informasi menggunakan Indeks KAMI (Indeks Keamanan Informasi) Versi 4.0. dari Badan Siber dan Sandi Negara berdasarkan kesesuaian dengan kriteria pada SNI ISO/IEC 27001. Proses evaluasi dilakukan melalui pengisian sejumlah pertanyaan di masing-masing area yang telah disebutkan dalam tinjauan pustaka.

3.5. Rekomendasi

Berdasarkan hasil evaluasi dapat ditarik kesimpulan kondisi tingkat kesiapan dan kematangan pengamanan informasi pada Dinas Komunikasi dan Informatika Kota Bogor sehingga dibuat rekomendasi yang bermanfaat untuk mengetahui area mana yang masih perlu banyak peningkatan dan perbaikan dalam menunjang kesiapan pengamananan informasi baik berupa kelengkapan dokumen, ketersediaan prosedur operasional standar, peningkatan infrastruktur dan hal-hal pendukung lainnya. Apabila rekomendasi tersebut diimplementasikan maka pada periode evaluasi berikutnya dapat menghasilkan peningkatan nilai indeks yang berarti meningkat pula tingkat kesiapan dan kelengkapan pengamanan informasi pada Dinas Komunikasi dan Informatika Kota Bogor.

4. HASIL DAN PEMBAHASAN

4.1. Ruang Lingkup Objek Penelitian

Evaluasi tingkat kesiapan pengamanan informasi dilakukan di Dinas Komunikasi dan Informatika Kota Bogor menggunakan Indeks KAMI versi 4.0. Terdapat 194 (seratus sembilan puluh empat) pertanyaan yang terbagi ke dalam 7 bagian area evaluasi sebagai berikut :

1. Kategori Sistem Elektronik sebanyak 10 pertanyaan;
2. Tata Kelola Keamanan Informasi sebanyak 22 pertanyaan;
3. Pengelolaan Risiko Keamanan Informasi sebanyak 16 pertanyaan;
4. Kerangka Kerja Pengelolaan Keamanan Informasi sebanyak 29 pertanyaan;
5. Pengelolaan Aset Informasi sebanyak 38 pertanyaan;
6. Teknologi dan Keamanan Informasi sebanyak 26 pertanyaan;
7. Suplemen sebanyak 53 pertanyaan.

4.2. Pengumpulan Data dan Dokumen Pendukung

Pengumpulan data dilakukan melalui proses wawancara dalam Forum Grup Diskusi (FGD), dihadiri oleh Kepala Seksi Keamanan Informasi dan Persandian yang bertanggung jawab dan mempunyai tugas dan fungsi dalam penyiapan bahan perumusan kebijakan teknis, penyiapan bahan pelaksanaan kegiatan, serta pelaksanaan monitoring, evaluasi dan pelaporan kegiatan di bidang Keamanan Informasi dan Persandian.

FGD dihadiri pula oleh Kepala Bidang Teknologi Informasi, Kepala Seksi Infrastruktur Pusat Data dan Kepala Seksi Infrastruktur Jaringan yang membantu dalam memberikan penjelasan lebih detail terkait jawaban dari pertanyaan evaluasi, karena banyak pertanyaan dalam evaluasi ini membutuhkan penjelasan dari kepala seksi lain sesuai dengan tanggung jawab bidangnya masing-masing. Tahapan yang dilalui dalam penelitian, pembangunan konsep, atau penyelesaian kasus, dituliskan pada bagian metodologi.

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

4.3. Melakukan Evaluasi Indeks KAMI

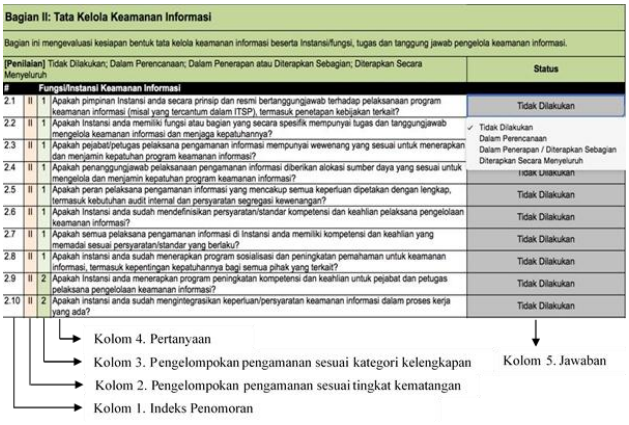
Penilaian evaluasi Indeks KAMI dilakukan dengan menjawab 194 (seratus sembilan puluh empat) pertanyaan yang tertera dalam aplikasi Indeks KAMI Versi 4.0 terdiri dari 7 bagian area evaluasi pertanyaan.

Karena memiliki metode penilaian evaluasi yang berbeda sehingga 7 bagian area evaluasi tersebut dikelompokkan menjadi 3 berdasarkan metode penilaian evaluasinya. Metode penilaian evaluasi yang pertama dilakukan untuk Bagian I yaitu Evaluasi Kategori Sistem Elektronik. Metode yang kedua digunakan dalam penilaian evaluasi Kelengkapan dan Kematangan Pengamanan Informasi, metode ini berlaku sama terhadap penilaian 5 area pengamanan informasi yang dimulai dari bagian II sampai bagian VI yaitu Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Pengelolaan Aset Informasi, dan Teknologi dan Keamanan Informasi. Metode penilaian ketiga dilakukan untuk Bagian VII yaitu evaluasi Suplemen.

Pertanyaan dan jawaban dalam evaluasi disajikan dalam bentuk tabel. Berdasarkan penomoran tabel yang tertera dalam Indeks KAMI Versi 4.0, kolom pertama di setiap pertanyaan menunjukkan indeks penomoran yang terdiri dari dua digit, digit pertama menunjukan bagian yang dievaluasi, digit kedua menunjukkan urutan pertanyaan. Indeks ini berlaku pada tabel bagian I sampai dengan VI.

Kolom kedua yang tertera pada tabel pertanyaan bagian II sampai bagian VI ditunjukkan dengan warna orange yang terdiri dari beberapa tingkatan warna yang diisi dengan angka romawi menunjukkan pengelompokkan pengamanan sesuai tingkat kematangan. Kolom ketiga ditunjukkan dengan warna hijau yang terdiri dari beberapa tingkatan warna yang diisi dengan angka 1 sampai 3 menunjukkan pengelompokan pengamanan sesuai kategori kelengkapan.

Kolom keempat yang tertera pada tabel pertanyaan bagian II sampai bagian VII berisi pertanyaan, kolom kelima merupakan kolom jawaban yang berisi pilihan jawaban berupa status yang sudah dilaksanakan sesuai kondisi yang ada, penjelasan setiap kolom pada tabel selengkapnya dapat dilihat pada gambar 3.

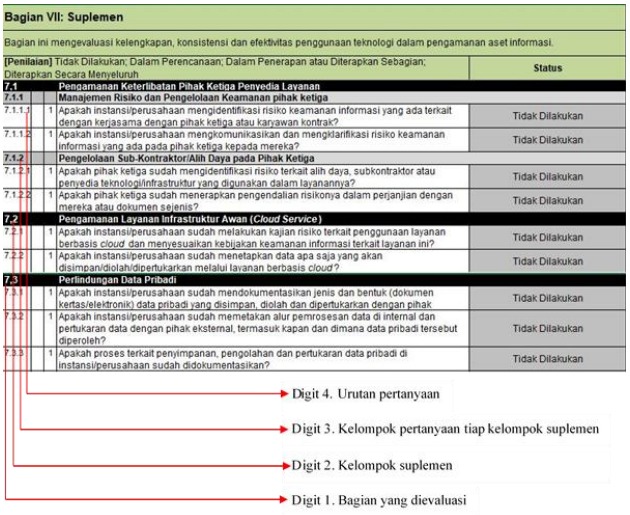


Gambar 3. Penjelasan kolom tabel pertanyaan

Untuk tabel bagian VII karena pertanyaan dibagi ke dalam beberapa sub kelompok pertanyaan maka pada kolom pertama indeks penomorannya terdiri dari empat digit, digit pertama menunjukan bagian yang dievaluasi, digit kedua menunjukkan kelompok suplemennya, digit ketiga menunjukkan kelompok

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

pertanyaan setiap kelompok suplemen, dan digit keempat menunjukkan urutan pertanyaan, selengkapnya dapat dilihat pada gambar 4. Untuk penjelasan kolom dua sampai dengan lima sama seperti dalam gambar 3.



Gambar 4. Penjelasan indeks penomoran tabel pertanyaan Bagian VII

4.3.1. Evaluasi Kategori Sistem Elektronik

Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan. Penilaian pada Kategori Sistem Elektronik terdiri dari 10 pertanyaan, setiap jawaban dari pertanyaan tersebut menunjukkan status sesuai kondisi yang ada pada institusi yang dinilai.

Berdasarkan penetapan skor yang tertera dalam Indeks KAMI Versi 4.0, perhitungan skor yang diperoleh dari setiap pertanyaan didefiniskan bahwa jika jawaban sesuai status pada poin A nilainya adalah 5, jika B nilainya adalah 2, dan jika C nilainya adalah 1.

Berdasarkan 10 pertanyaan yang diberikan maka didapatkan skor dari setiap jawaban, skor tersebut kemudian dijumlahkan dan hasil perhitungan total skor yang didapatkan dikategorikan hasilnya sesuai kategori yang telah didefiniskan dalam Indeks KAMI Versi 4.0. Terdapat tiga kategori hasil evaluasi yaitu Rendah, Tinggi, dan Strategis seperti yang tertera pada tabel 3.

Tabel 3. Kategori Sistem Elektronik

Skor	Kategori
10-15	Rendah
16-34	Tinggi
35-50	Strategis

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

Jawaban hasil wawancara untuk evaluasi kategori sistem elektronik dapat dilihat pada tabel 4.

Pada kategori ini Dinas Komunikasi dan Informatika mendapat total skor 35. Berdasarkan tabel 3, skor 35-50 termasuk ke dalam kategori Strategis, sehingga evaluasi sistem elektronik Dinas Komunikasi dan Informatika termasuk ke dalam kategori Strategis. Kategori ini menunjukkan bahwa penggunaan sistem elektronik menjadi bagian strategis yang tidak terpisahkan dalam mendukung proses kerja yang berjalan.

Tabel 4. Hasil evaluasi Kategori Sistem Elektronik

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

Bagian I: Kategori Sistem Elektronik			Skor
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**	
#	**Karakteristik Instansi/Perusahaan**		
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	B	2
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	B	2
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	B	2
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	B	2
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	A	5
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A	5
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/atau Terbatas [C] Biasa	B	2
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	A	5
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	A	5
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	A	5
	Skor penetapan Kategori Sistem Elektronik	**35**	
	Tingkat Ketergantungan	**Strategis**	

4.3.2. Evaluasi Kelengkapan dan Kematangan Pengamanan Informasi

Evaluasi kelengkapan dan tingkat kematangan pengamanan informasi dilakukan pada 5 area pengamanan informasi, yaitu:

a. Tata Kelola Keamanan Informasi;
b. Pengelolaan Risiko Keamanan Informasi;
c. Kerangka Kerja Pengelolaan Keamanan Informasi;

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

d. Pengelolaan Aset Informasi;
e. Teknologi dan Keamanan Informasi.

Setiap pertanyaan dijawab sesuai kondisi yang sudah diterapkan dengan skor sesuai dengan kategori pengamanan yang telah didefinsikan dalam Indeks KAMI Versi 4.0 seperti dalam tabel 5.

Tabel 5. Skor Tingkat Kematangan

Status Penerapan	Penetapan Skor		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Status penerapan pada tabel 5 merupakan pilihan jawaban dari setiap pertanyaan sesuai kondisi yang ada. Perhitungan penetapan skor pada tabel 5 setiap status penerapan dikategorikan menurut kelompok pengamanan sesuai kategori kelengkapan pada kolom 3 di setiap tabel pertanyaan seperti yang sudah dijelaskan pada gambar 3, sehingga pada status penerapan yang sama memiliki nilai yang berbeda sesuai kelompok pengamanannya.

Pengisian pertanyaan dengan label kategori pengamanan 3 dapat memberikan skor apabila semua pertanyaan pada label kategori pengamanan 1 dan 2 dijawab dengan status minimal “Dalam Penerapan atau Diterapkan Sebagian”. Skor pada setiap pertanyaan mengacu pada perhitungan dalam tabel 5.

Setiap pertanyaan terbagi ke dalam 3 kelompok pengamanan berdasarkan pewarnaan pada tabel seperti yang telah dijelaskan pada gambar 3. Pengelompokan pertanyaan tersebut mempengaruhi perhitungan skor dari setiap pertanyaan seperti yang didefinisikan dalam tabel 5. Total nilai evaluasi setiap area pengamanan diperoleh dari total skor seluruh pertanyaan.

Hasil evaluasi terhadap 5 area pengamanan informasi adalah sebagai berikut :

a. Hasil Evaluasi Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi tugas dan tanggung jawab pengelola keamanan informasi. Total nilai evaluasi area ini adalah 108.

b. Pengelolaan Risiko Keamanan Informasi

Bagian ini mengevaluasi tingkat kesiapan penerapan pengelolaan resiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Total nilai evaluasi area ini adalah 29.

c. Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Total nilai evaluasi area ini adalah 86

d. Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Total nilai evaluasi area ini adalah 91.

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

e. Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Total nilai evaluasi area ini adalah 81.

Contoh tabel hasil evaluasi terhadap 5 area pengaman informasi dengan menggunakan Indeks KAMI Versi 4.0 yang telah dilakukan pada Dinas Komunikasi dan Informatika Kota Bogor dapat dilihat pada tabel 6.

Tabel 6. Hasil Evaluasi Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi					Skor
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	
#			**Pengamanan Teknologi**		
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian	2
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Dalam Penerapan / Diterapkan Sebagian	2
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Dalam Penerapan / Diterapkan Sebagian	4
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Penerapan / Diterapkan Sebagian	4
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Dalam Penerapan / Diterapkan Sebagian	4
6.25	III	3	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Dalam Penerapan / Diterapkan Sebagian	6
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan	0
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**81**	

4.3.3. Evaluasi Suplemen

Bagian ini mengevaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan asset informasi. Evaluasi ini dilakukan untuk membahas aspek kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan (Cloud Service) dan Perlindungan Data Pribadi digunakan sesuai konteks atau cakupan yang ada.

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

Perhitungan skor setiap pertanyaan mengacu pada tabel 5, yang membedakan bagian ini dengan 6 area evaluasi sebelumnya adalah tidak adanya perhitungan total nilai evaluasi tetapi dihitung nilai rata-rata dari total nilai yang didapat pada setiap kelompok terhadap jumlah pertanyaan pada setiap kelompok.

Hasil evaluasi Suplemen didapatkan nilai rata-rata setiap aspek adalah sebagai berikut :

1. Pengamanan keterlibatan pihak ketiga penyedia layanan skor rata-rata 1,07;
2. Pengamanan layanan infrastruktur awan (Cloud Service) skor rata-rata 0;
3. Perlindungan data pribadi skor rata-rata 1,56.
4. Skor rata-rata tertera di baris bagian atas setiap kelompok pada tabel 4.10.

Skor yang didapat dari perhitungan bagian VII ini tidak mempengaruhi total skor dari bagian I sampai bagian VI dalam penilaian Indeks KAMI yang menunjukkan tingkat kesiapan dan kematangan pengamanan informasi. Berdasarkan Indeks KAMI penilaian bagian VII ini bertujuan untuk mendeteksi munculnya resiko keamanan informasi baru dengan adanya keterlibatan ketiga aspek tersebut.

Hasil evaluasi Suplemen dengan menggunakan Indeks KAMI Versi 4.0 yang telah dilakukan pada Dinas Komunikasi dan Informatika Kota Bogor dapat dilihat pada tabel 7.

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

Bagian VII: Suplemen					Skor
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	
7,1			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**		1,07
7.1.1			**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**		
7.1.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.5		1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.6		1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 7. Hasil Evaluasi Suplemen

4.4. Dashboard Indeks KAMI

Dashboard Indeks KAMI menampilkan hasil penilaian seluruh area evaluasi, yaitu skor 7 area evaluasi beserta tingkat kematangan dari masing-masing area, hasil evaluasi akhir status kesiapan pengamanan informasi, tingkat kelengkapan penerapan Standar ISO 27001, dan Radar Chart Indeks KAMI. Dashboard hasil evaluasi 7 area penilaian indeks KAMI pada Dinas Komunikasi dan Informatika Kota Bogor tertera pada gambar 5.

Dashboard hasil penilaian yang tertera pada gambar 5 menjelaskan sebagai berikut :

1. Skor Kategori Sistem Elektronik adalah 35 dan masuk ke dalam kategori Strategis ditampilkan dalam dashboard di bagian paling atas dengan latar warna hitam;
2. Skor Tata Kelola Keamanan Informasi adalah 108 berada pada kategori tingkat kematangan II, area ini dapat dilihat pada radar chart Indeks KAMI menunjukkan telah dalam tahap kepatuhan terhadap ISO 27001/SNI;

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

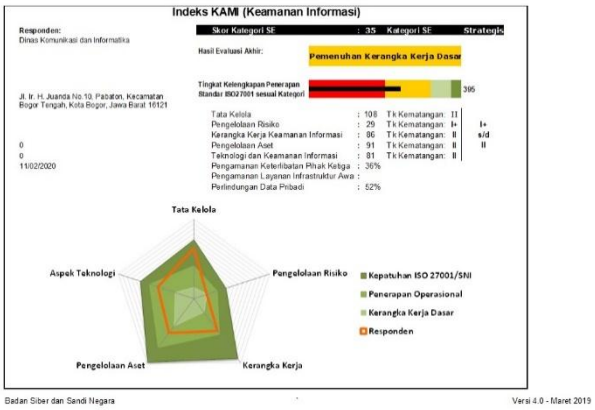
3. Skor Pengelolaan Risiko Keamanan Informasi adalah 29 berada pada kategori tingkat kematangan I+, area ini dapat dilihat pada radar chart Indeks KAMI menunjukkan berada dalam tahap kerangka kerja dasar;
4. Skor Kerangka Kerja Keamanan Informasi adalah 86 berada pada kategori tingkat kematangan II, area ini dapat dilihat pada radar chart Indeks KAMI menunjukkan berada dalam tahap penerapan operasional;
5. Skor Pengelolaan Aset Informasi adalah 91 berada pada kategori tingkat kematangan II, area ini dapat dilihat pada radar chart Indeks KAMI menunjukkan berada dalam tahap penerapan operasional;
6. Skor Teknologi dan Keamanan Informasi adalah 81 berada pada kategori tingkat kematangan II, area ini dapat dilihat pada radar chart Indeks KAMI menunjukkan berada dalam tahap penerapan operasional.
7. Skor Suplemen yang tertera pada dashboard ditampilkan dalam bentuk persentase total skor yang didapat pada setiap aspek terhadap total skor maksimal seluruh pertanyaan pada setiap kelompok. Untuk kelompok pengamanan keterlibatan pihak ketiga dalam dashboard tertera 36%, pengamanan perlindungan data pribadi dalam dashboard tertera 52%, dan untuk pengamanan layanan infrastruktur awan (cloud service) tidak dilakukan.

Radar chart pada gambar 5 menunjukkan sejauh mana respon Dinas Komunikasi dan Informatika Kota Bogor (warna orange) terhadap penerapan Sistem Manajemen Kemanan Informasi (SMKI). Pada lima area terlihat tingkat kematangan aspek tata kelola lebih baik dibandingkan aspek pengelolaan resiko, kerangka kerja, pengelolaan aset, dan aspek teknologi.

Berdasarkan skor yang diperoleh dari total nilai hasil evaluasi kelengkapan dan kematangan 5 area pengamanan informasi dengan total nilai 395, tingkat kelengkapan penerapan standar ISO 27001 berada pada tingkat I+ sampai dengan II seperti yang tertera dalam dashboard pada gambar 4.3 ditampilkan dalam bentuk garis horizontal berwarna hitam yang sudah mencapai warna kuning. Berdasarkan Indeks KAMI, pewarnaan tersebut menunjukkan tingkat kematangan yang dicapai, dimulai dari warna merah yang menunjukkan tingkat I, warna kuning menunjukkan tingkat II, warna hijau muda menunjukkan tingkat III, dan warna hijau tua menunjukkan tingkat IV.

Secara keseluruhan hasil evaluasi akhir Indeks KAMI yang memperoleh skor akhir 395 berdasarkan tabel 1 menunjukkan bahwa status kesiapan pengamanan informasi Dinas Komunikasi dan Informatika Kota Bogor termasuk dalam tahap Pemenuhan Kerangka Kerja Dasar, pada gambar 5 ditampilkan dalam dashboard di bagian atas dengan latar warna kuning.

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878



Gambar 5. Dashboard Penilaian Indeks KAMI pada Dinas Komunikasi dan Informatika Kota Bogor

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil evaluasi tingkat kesiapan dan kematangan keamanan informasi Dinas Komunikasi dan Informatika Kota Bogor menggunakan Indeks Keamanan Informasi (KAMI) Versi 4.0 dapat dibuat kesimpulan sebagai berikut :

1. Evaluasi Kategori Sistem Elektronik termasuk ke dalam kategori Strategis dengan skor 35 memberikan gambaran bahwa penggunaan sistem elektronik menjadi bagian strategis yang tidak terpisahkan dalam mendukung proses kerja Dinas Komunikasi dan Informatika Kota Bogor;
2. Evaluasi di 5 area pengamanan Dinas Komunikasi dan Informatika Kota Bogor mendapatkan total nilai 395 menunjukan status kesiapan pengamanan informasi berada pada tahap Pemenuhan Kerangka Kerja Dasar dengan tingkat kematangan level I+ sampai dengan II;
3. Pada area suplemen, evaluasi pengamanan dengan keterlibatan pihak ketiga mencapai 36%, evaluasi perlindungan data pribadi mencapai 52%, dan untuk pengamanan layanan infrastruktur awan (cloud service) karena tidak menggunakan layanan tersebut sehingga pencapaiannya 0%.

5.2. Saran

Dinas Komunikasi dan Informatika Kota Bogor agar memprioritaskan peningkatan hasil evaluasi pada area Pengelolaan Risiko Keamanan Informasi yang memiliki tingkat kematangan paling rendah yaitu level I+ untuk menyusun dokumen terkait manajemen pengelolaan risiko, mengevaluasi dan memperbaiki proses kerja, serta mewadahi proses kajian dan evaluasi yang mencakup aspek pengelolaan risiko keamanan informasi.

Melakukan evaluasi keamanan informasi menggunakan Indeks KAMI dua kali dalam setahun untuk melakukan tinjauan ulang tentang kesiapan keamanan informasi sekaligus mengukur keberhasilan terhadap perbaikan yang diterapkan dengan pencapaian tingkat kelengkapan dan kematangan sehingga tingkat kesiapan dan kematangan pengamanan informasi bisa mencapai tingkat III+ sebagai ambang batas minimum Standar ISO 27001.

Journal of Industrial Engineering & Management Research
Vol.2 No.5 DOI: https://doi.org/10.7777/jiemar
http://www.jiemar.org e-ISSN : 2722-8878

DAFTAR PUSTAKA

[1] Republik Indonesia. Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government.
[2] Republik Indonesia. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).
[3] Umar Yunan Kurnia Septo Hediyanto, "Penelitian E-Government di Propinsi Jawa Barat: Kajian Pustaka Sistematis", Jurnal Metris 19 (2018) 95–104. ISSN: 1411 – 3287, pp 96, 2018.
[4] Kantor Komunikasi dan Informatika Kota Bogor. "Perencanaan Induk Pengembangan e-Government Pemerintah Kota Bogor 2014-2018". Kota Bogor. Kantor Komunikasi dan Informatika Kota Bogor, 2013. pp 7.
[5] I Gede Putu Krisna Juliharta, "Analisa Tingkap Kesiapan Penerapan Keamanan Teknologi Informasi dalam Pelaksanaan e-Government Berbasis Indeks Keamanan Informasi (KAMI) Studi Kasus Pemerintah Kota Kediri", Jurnal Teknologi Informasi dan Komputer, Volume 5, Nomor 1, pp 22, Januari 2019.
[6] Yuni Cintia Yuzea, Yudi Priyadi, Candiwan, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001 : 2013 Serta Rekomendasi Model Sistem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi", Jurnal Sistem Informasi Bisnis 01, pp 39, 2016.
[7] Dicky Rutanaji, Sri Suning Kusumawardani, Wing Wahyu Winarno, "Penggunaan Kerangka Kerja SNI ISO/IEC 27001:2013 Untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI)", in Conference proceedings Seminar Nasional Geotik, ISSN: 2580-8796, 2018.
[8] Badan Siber dan Sandi Negara. "Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks KAMI bagi Pemerintah Daerah Provinsi". https://bssn.go.id/penerapan-sistem-manajemen-keamanan-informasi-berbasis-indeks-kami-bagi-pemerintah-daerah provinsi/, Oct 23, 2018 [Januari. 31, 2020].
[9] Badan Siber dan Sandi Negara, Aplikasi Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0, Maret 2019, 2019.