Evaluasi Manajemen Keamanan Informasi menggunakan Indeks KAMI 4.2 pada Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ

Flourensia Sapty Rahayu*[1], Putri Nastiti[2], Cyril Saulnier Mikanen Gultom[3]

[1-3]Program Studi Sistem Informasi, Universitas Atma Jaya Yogyakarta

E-mail: sapty.rahayu@uajy.ac.id*[1], putri.nastiti@uajy.ac.id[2], 171709524@students.uajy.ac.id[3]

Abstrak. Manajemen keamanan informasi adalah salah satu upaya untuk melindungi aset informasi yang dimiliki oleh sebuah instansi dari potensi ancaman. Salah satu aktivitas untuk meyakinkan bahwa praktek pengamanan informasi telah dilakukan dengan benar adalah dengan melakukan evaluasi terhadap keamanan informasi. Di Indonesia, instansi-instansi pelayanan publik diwajibkan untuk melakukan praktek pengamanan informasi. Dinas Komunikasi, Informatika dan Persandian (Diskominfosandi) Kabupaten XYZ adalah salah satu instansi pemerintah yang wajib melakukan praktek pengamanan informasi. Selama ini Diskominfosandi Kabupaten XYZ telah menerapkan praktek pengamanan informasi dan telah melakukan evaluasi tahunan dengan menggunakan indeks Keamanan Informasi (KAMI) versi 4.2. Namun hasil evaluasi sebelumnya menunjukkan masih adanya kelemahan terutama di area kerangka kerja keamanan informasi. Upaya perbaikan telah dilakukan namun belum diketahui apakah sudah ada perbaikan dalam indeks KAMInya. Berdasarkan hal tersebut, penelitian ini dilakukan dengan tujuan untuk mengevaluasi kembali praktek pengamanan informasi yang dilakukan dengan Indeks KAMI 4.2. Hasil evaluasi menunjukkan bahwa praktek pengamanan informasi telah mengalami peningkatan, dari skor tingkat kelengkapan 389 pada evaluasi sebelumnya ke 435. Tingkat kematangan indeks KAMI juga meningkat dari I+ sampai dengan II+ menjadi II sampai dengan III. Berdasarkan hasil tersebut diberikan beberapa rekomendasi untuk meningkatkan skor dan level pengamanan informasi.

Kata kunci: Keamanan Informasi; Indeks KAMI 4.2; SNI ISO/IEC 27001

Abstract. *Information security management is one of the efforts to protect an institution's information assets from potential threats. One of the activities to ensure that information security practices have been carried out properly is to evaluate the information security implementation. In Indonesia, public service agencies are required to implement information security practices. Dinas Komunikasi, Informatika dan Persandian (Diskominfosandi) of XYZ regency is a government agency that must implement information security practices. So far, Diskominfosandi of XYZ regency has implemented information security practices and has conducted annual evaluations using the Indeks Keamanan Informasi (KAMI) version 4.2. However, the results of the previous evaluation showed some weaknesses, particularly in the information security framework. Improvement efforts*

have been made, but it is not yet known whether there has been an improvement in the KAMI index. Based on this, this study was conducted to re-evaluate the information security practices with the KAMI index 4.2. The evaluation results showed that the KAMI index had increased, from a completeness score of 389 in the previous evaluation to 435. The maturity level of the KAMI index also increased from I+ to II+ to II to III. Based on these results, several recommendations are provided to improve the score and level of information security.

Keywords: *Information security; KAMI Index 4.2; SNI ISO/IEC 27001*

1. Pendahuluan

Penerapan tata kelola TIK saat ini merupakan kebutuhan dan juga merupakan tuntutan bagi setiap instansi penyelenggara pelayanan publik, dikarenakan peran TIK menjadi semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu perwujudan dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola TIK, penerapan keamanan informasi sangatlah penting karena kinerja tata kelola TIK akan terganggu jika informasi yang merupakan salah satu objek utama tata kelola TIK mengalami masalah keamanan. Masalah keamanan informasi tersebut menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) [1].

Keamanan informasi merupakan salah satu cara untuk mengamankan aset informasi dari ancaman yang ada. Keamanan informasi dapat menjamin kebelangsungan bisnis, mengurangi risiko yang dapat terjadi, dan mengoptimalkan pengembalian investasi secara tidak langsung. Ketika informasi yang disimpan, dikelola, dan dibagikan suatu organisasi semakin banyak, maka risiko terjadinya kerusakan data, kehilangan data, maupun terekspos nya data ke pihak yang tidak berwenang akan semakin besar [2]. Beralihnya sistem pemerintahan dengan memanfaatkan kemajuan dalam bidang teknologi informasi dan komunikasi tentu saja akan memunculkan permasalahan baru yang lebih kompleks. Salah satu permasalahan adalah timbulnya kerawanan dan ancaman keamanan bidang informasi. Berkaca dari hal ini maka tugas penyelenggaraan persandian dan keamanan informasi sangatlah berat karena harus menangkal segala bentuk ancaman dan kerawanan terhadap pencurian informasi daerah.

Salah satu upaya yang telah dilakukan oleh Kementerian Komunikasi dan Informatika untuk meningkatkan tingkat keamanan informasi dari instansi pemerintahan yaitu dengan menciptakan alat yang digunakan untuk menilai tingkat kematangan serta kelengkapan dalam penerapan keamanan informasi yang disebut Indeks Keamanan Informasi (KAMI) [3]. Indeks KAMI merujuk pada ISO 27001 yang berisi mengenai standar keamanan informasi. ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi informasi dan pengelolaan aset yang dapat membantu suatu organisasi untuk memastikan bahwa keamanan informasi yang mereka terapkan sudah efektif [2].

Diskominfosandi Kabupaten XYZ sebelumnya sudah melakukan evaluasi mandiri pada tahun 2019. Berdasarkan evaluasi sebelumnya, nilai kematangan Indeks KAMI Diskominfosandi Kabupaten XYZ adalah pada level II dari maksimal level V, sedangkan skor kelengkapannya adalah 389. Nilai kematangan minimal yang disyaratkan untuk dapat menerapkan ISO/IEC 27001 adalah III+, sedangkan nilai kematangan indeks KAMI di Diskominfosandi Kabupaten XYZ masih II sehingga belum memenuhi syarat minimal untuk menerapkan ISO/IEC 27001. Skor kelengkapan 389 bermakna bahwa status kesiapan pengamanan informasi Diskominfosandi Kabupaten XYZ masih dalam status "Pemenuhan kerangka kerja dasar". Hasil evaluasi mandiri sebelumnya juga menunjukkan Diskominfosandi Kabupaten XYZ memiliki kategori sistem elektronik "strategis". Sistem Elektronik "strategis" merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, Pelayanan Publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara. Kewajiban untuk instansi yang memiliki sistem elektronik strategis diatur dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi pasal 7 ayat 1, yang berbunyi "Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis harus menerapkan standar SNI ISO/IEC 27001 dan

ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya" [4]. Kewajiban untuk memiliki sertifikat Sistem Manajemen Pengamanan Informasi (SMPI) diatur dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi Pasal 10 ayat 1, yang berbunyi "Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi wajib memiliki Sertifikat Sistem Manajemen Pengamanan Informasi". Peraturan-peraturan ini yang mendasari Diskominfosandi Kabupaten XYZ untuk menerapkan standar SNI ISO/IEC 27001 dan memiliki sertifikat SMPI. Dalam peraturan yang sama pasal 21 juga disebutkan bahwa "Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi dapat melakukan Penilaian Mandiri berdasarkan standar SNI/ISO IEC 27001" [4]. Lebih lanjut, Peraturan Badan Siber dan Sandi Negara Nomor 8 tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik Pasal 12 ayat 1 yang berbunyi "Untuk mempersiapkan penerapan SNI ISO/IEC 27001 sebagaimana dimaksud dalam Pasal 9, Penyelenggara Sistem Elektronik dapat melakukan penilaian berdasarkan Indeks KAMI" [5]. Aturan-aturan ini yang mendasari Diskominfo Kabupaten XYZ untuk melakukan penilaian mandiri menggunakan Indeks KAMI yang merupakan turunan dari standar SNI/ISO IEC 27001.

Dalam rangka memenuhi standar SNI/ISO IEC 27001, pihak Diskominfosandi Kabupaten XYZ harus melakukan penilaian mandiri kembali untuk menilai kecukupan sistem manajemen pengamanan informasinya. Penelitian ini dilakukan untuk mengevaluasi SMPI pada Diskominfosandi Kabupaten XYZ dengan alat indeks KAMI 4.2. Hasil penilaian diharapkan dapat memberikan rekomendasi perbaikan terkait praktek pengamanan informasi pada Diskominfosandi Kabupaten XYZ.

2. Dasar Teori

2.1. Pengamanan Informasi

Pengamanan Informasi merupakan suatu upaya untuk mencegah agar aset informasi aman dari berbagai macam ancaman yang dapat terjadi untuk meminimalisir risiko negatif yang diterima [6]. Kegiatan ini dilakukan untuk melindungi aset informasi, mengurangi risiko, meminimalisir dampak yang terjadi akibat adanya ancaman, dan memastikan keberlangsungan bisnis [7][8]. Pengamanan informasi terdiri dari 3 aspek, yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA). *Confidentiality* (kerahasiaan) merupakan aspek keamanan informasi yang menjamin bahwa data dan informasi hanya dapat diakses oleh pihak yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan. *Integrity* (integritas) merupakan aspek keamanan informasi yang menjamin bahwa data tidak dapat dirubah tanpa izin pihak yang berwenang, keakuratan dan keutuhan sebuah informasi harus terjaga. *Availability* (ketersediaan) merupakan aspek keamanan informasi yang menjamin bahwa data dan informasi akan tersedia kapanpun untuk diakses oleh pengguna yang memiliki hak akses [9].

2.2. Indeks KAMI 4.2

Indeks KAMI adalah sebuah alat yang menggabungkan berbagai aspek pengamanan informasi untuk mengevaluasi status terkini pengamanan informasi dan tingkat kematangan program keamanan informasi yang diterapkan oleh suatu organisasi [10]. Indeks KAMI berfungsi sebagai alat yang digunakan untuk menilai tingkat kematangan dan kelengkapan penerapan standar, serta memberikan gambaran tentang tata kelola keamanan informasi dalam organisasi tersebut [11]. Tujuannya adalah untuk memungkinkan organisasi, baik pada tingkat nasional maupun yang lebih kecil, untuk menilai dan membandingkan kondisi keamanan informasi mereka, mengidentifikasi area perbaikan, dan menetapkan prioritas. Evaluasi menggunakan Indeks KAMI ini sebaiknya dilakukan secara rutin oleh pejabat yang memiliki tanggung jawab dalam pengelolaan keamanan informasi di seluruh bagian organisasi. Indeks KAMI 4.2 merupakan pembaharuan dari indeks KAMI 4.1 di mana indeks KAMI 4.1 mengacu pada standar ISO/IEC 27001:2009, sedangkan indeks KAMI 4.2 mengacu pada versi standar ISO yang lebih baru yaitu ISO/IEC 27001:2013.

Dalam konteks instansi pemerintahan, penggunaan Indeks KAMI penting untuk menjalankan evaluasi tahunan yang diwajibkan. Penggunaan indeks KAMI oleh instansi pemerintah juga dapat membantu meningkatkan tingkat keamanan informasi mereka. Penilaian dalam Indeks KAMI dilakukan dengan mengevaluasi semua persyaratan keamanan yang dijelaskan dalam standar ISO/IEC 27001:2013, yang telah diorganisir menjadi lima area utama yaitu Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset informasi, Teknologi dan Keamanan Informasi.

2.2.1. Penilaian dalam Indeks KAMI 4.2

Sebelum melakukan evaluasi, terlebih dahulu dilakukan pengklasifikasian terhadap kategori Sistem Elektronik. Pemilihan kategori Sistem Elektronik ini bertujuan untuk mengkategorikan instansi ke dalam tingkat tertentu [12]. Kategori sistem elektronik ini terdiri dari tiga tingkat, yaitu rendah, tinggi, dan strategis. Pertanyaan dalam Indeks KAMI dibagi menjadi dua kategori berdasarkan kebutuhan. Pertama, pertanyaan diklasifikasikan berdasarkan tingkat kesiapan implementasi keamanan sesuai dengan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Dalam kategori ini, responden diminta memberikan tanggapan tentang tiga aspek: kerangka kerja dasar keamanan informasi (ditandai sebagai "1"), efektivitas dan konsistensi implementasinya (ditandai sebagai "2"), serta kemampuan untuk terus meningkatkan kinerja keamanan informasi (ditandai sebagai "3"). Tingkat terakhir ini sesuai dengan kesiapan minimum yang dibutuhkan untuk proses sertifikasi standar ISO/IEC 27001. Setiap jawaban akan dinilai dengan skor yang nantinya akan diolah untuk menghasilkan indeks, dan hasil evaluasi akan ditampilkan dalam *dashboard* pada akhir proses ini. Panduan pemberian skor untuk setiap pertanyaan dapat dilihat pada Tabel 1. Sebagai contoh pemberian skor, misalnya jika jawaban untuk pertanyaan tertentu adalah “Dalam Perencanaan” dan pertanyaan tersebut masuk dalam aspek/kategori pengamanan “1” maka skor yang didapatkan adalah “1”.

Tabel 1. Matriks Bobot Penilaian Status Penerapan [13]

	Kategori Pengamanan		
Status Pengamanan	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

Hasil evaluasi untuk setiap area akan direpresentasikan dalam diagram radar yang menampilkan tingkat kesiapan pada setiap area. Diagram ini memungkinkan perbandingan kondisi kesiapan dari evaluasi dengan tingkat kesiapan yang telah ditetapkan sebagai acuan. Dengan mengamati diagram tersebut, para pimpinan instansi dapat mengidentifikasi kebutuhan perbaikan yang diperlukan dalam berbagai area penerapan keamanan informasi. Korelasi antara kategori sistem elektronik, skor kelengkapan yang diperoleh, dan status kesiapan dapat dilihat pada Tabel 2. Tabel 2 memetakan status kesiapan untuk penerapan ISO/IEC 27001 berdasarkan kategori sistem elektronik yang dimiliki serta skor kelengkapan yang diperoleh. Sebagai contoh, jika instansi memiliki kategori sistem elektronik “strategis” dan memiliki skor kelengkapan 550, maka status kesiapannya adalah “Cukup baik”.

Tabel 2. Matriks Kategori Sistem Elektronik dan Status Kesiapan [13]

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
Stategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak layak
		334	535	Pemenuhan kerangka kerja dasar
		536	609	Cukup baik
		610	645	Baik

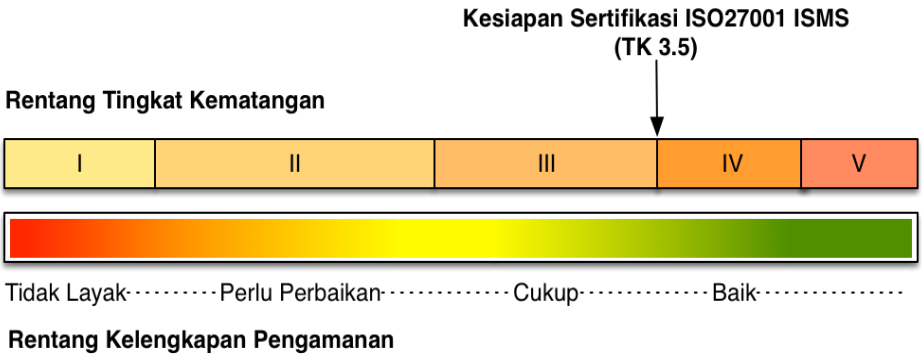
Pengelompokkan pertanyaan yang kedua dilakukan berdasarkan tingkat kematangan implementasi keamanan dengan kategori yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja *Control Objective for Information Technologies* (COBIT) atau *Capability Maturity Model Integration* (CMMI) [13]. Tingkat kematangan ini akan digunakan sebagai sarana untuk melaporkan pemetaan dan peringkat kesiapan keamanan informasi di Kementerian/ Lembaga.
Dalam Indeks KAMI, tingkat kematangan ini didefinisikan sebagai berikut [13]:

1. Tingkat I – Kondisi Awal
2. Tingkat II – Penerapan Kerangka Kerja Dasar
3. Tingkat III – Tedefinisi dan Konsisten
4. Tingkat IV – Terkelola dan Terukur
5. Tingkat V - Optimal

Untuk memberikan penjelasan yang lebih rinci, tingkatan ini diperluas dengan tambahan tingkatan I+, II+, III+, dan IV+, sehingga secara total ada 9 tingkatan kematangan. Awalnya, semua responden akan diberikan kategori kematangan pada Tingkat I, Sebagai standar yang setara dengan ISO/IEC 27001:2013, tingkat kematangan yang diinginkan untuk standar minimum sertifikasi adalah tingkat III+.

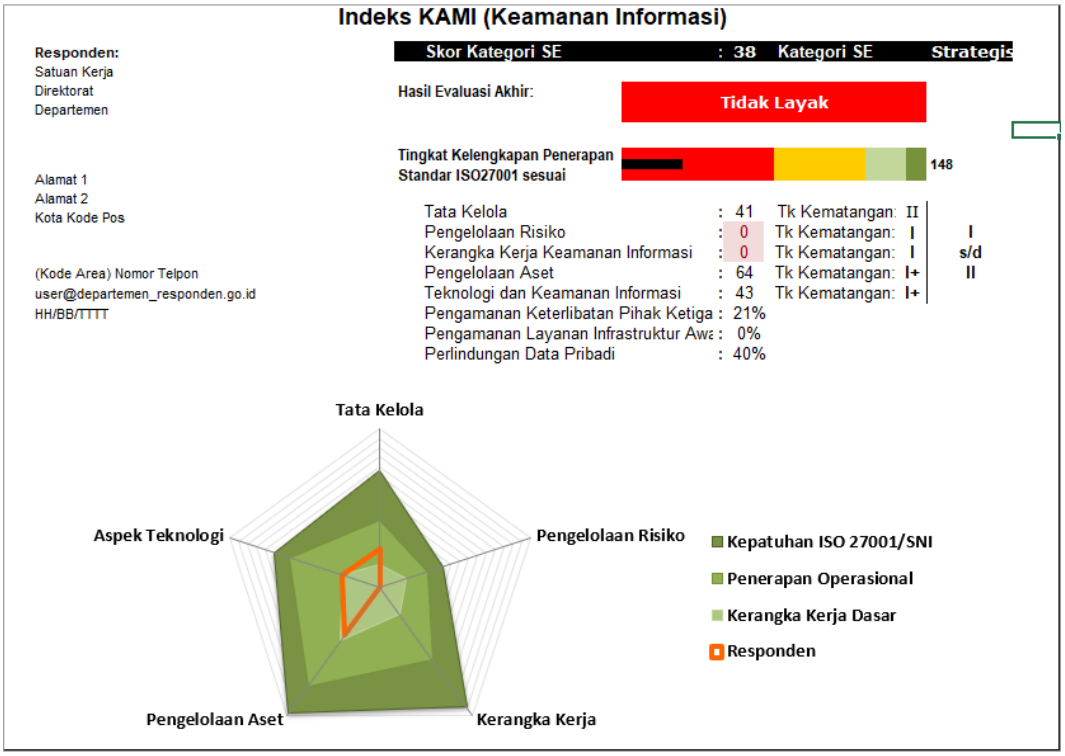
Kedua pengelompokkan pertanyaan dapat dipetakan untuk memberikan dua sudut pandang yang berbeda yaitu dari sudut pandang tingkat kelengkapan keamanan dan tingkat kematangan pengamanan. Pengelompokkan yang dipetakan tersebut dapat dilihat pada

Gambar ***1***.



Gambar 1. Rentang Tingkat Kematangan [13]

Hasil evaluasi dari Indeks KAMI versi 4.2 akan ditampilkan ke dalam sebuah diagram yang berbentuk seperti jaring laba-laba (*spider chart*) dengan 5 area utama. Diagram tersebut juga akan menunjukkan perbandingan antara nilai Indeks KAMI yang diperoleh dengan kepatuhan terhadap ISO 27001:2013. Contoh skor akhir yang disesuaikan dengan status kesiapan dari instansi terkait mengenai keamanan informasinya dapat dilihat pada Gambar 2.



Gambar 2. Contoh *Dashboard* Hasil Evaluasi Indeks KAMI [13]

3. Metodologi Penelitian

Ruang lingkup penelitian ini mencakup 5 area evaluasi dalam indeks KAMI, yaitu: (1) Tata Kelola Keamanan Informasi, (2) Pengelolaan Risiko Keamanan Informasi, (3) Kerangka Kerja Pengelolaan Keamanan Informasi, (4) Pengelolaan Aset Informasi, dan (5) Teknologi Keamanan Informasi. Tahapan penelitian dalam evaluasi indeks KAMI di Diskominfosandi Kabupaten XYZ terdiri dari 3 tahap, yaitu: (1)

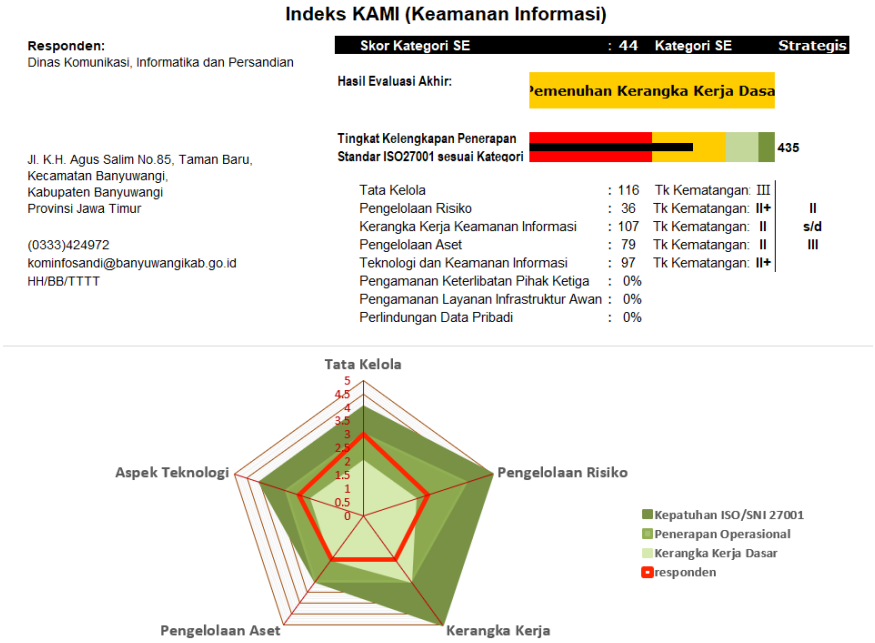
pengumpulan informasi, (2) penilaian dan analisis, (3) dan pembuatan rekomendasi. Pada tahap pengumpulan informasi, penulis mengumpulkan berbagai informasi mengenai proses layanan Diskominfosandi Kabupaten XYZ, sistem informasi yang berjalan, *supplier*/ vendor dan *customer*, dan standar/aturan yang diimplementasikan. Metode pengumpulan data yang digunakan adalah studi dokumen dan kuesioner. Alat indeks KAMI berupa kuesioner yang perlu diisi oleh responden. Narasumber yang mengisi kuesioner merupakan pihak yang ditunjuk Kepala Seksi Persandian dari Diskominfosandi Kabupaten XYZ. Setelah hasil kuesioner dan dokumen-dokumen pendukung didapatkan, dilakukan analisis informasi dan dokumentasi berdasarkan hasil perhitungan indeks KAMI. Untuk memperoleh informasi lebih lanjut, penulis melakukan wawancara guna menguji dan mengkonfirmasi kebenaran dari isi kuesioner indeks KAMI yang diisi oleh pihak Diskominfosandi Kabupaten XYZ.

Penilaian yang dilakukan menggunakan alat ukur indeks KAMI 4.2. Penilaian tersebut dimulai dari penetapan kategori Sistem Elektronik dari Diskominfosandi Kabupaten XYZ, lalu dilanjutkan dengan melakukan penilaian terhadap aspek Tata Kelola Pengamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi dan Teknologi Keamanan Informasi. Proses penilaian akan menghasilkan berbagai temuan dan bukti-bukti pendukung yang telah dikonfirmasi. Temuan tersebut didiskusikan dengan pihak Diskominfosandi Kabupaten XYZ guna menyusun rekomendasi yang tepat bagi Diskominfosandi Kabupaten XYZ. Rekomendasi berupa saran perbaikan atau peningkatan terhadap prosedur atau aktivitas/ proses bisnis disusun berdasarkan dari hasil penilaian Indeks KAMI.

4. Hasil dan Pembahasan

4.1. Dashboard Hasil Penilaian Indeks KAMI

Gambar 3 menunjukkan *dashboard* hasil penilaian akhir indeks KAMI. Dari hasil pengisian kuesioner, sistem elektronik dari Diskominfosandi Kabupaten XYZ termasuk dalam kategori “strategis”. Dari Gambar 3 dapat dilihat juga bahwa skor kelengkapan penerapan ISO/IEC 27001 yang diperoleh adalah 435. Nilai ini lebih tinggi dari hasil penilaian sebelumnya yaitu 389. Sedangkan tingkat kematangan untuk semua area berkisar di level II sampai III. Nilai ini juga meningkat dari hasil penilaian sebelumnya yang masih berkisar di level I+ sampai II+. Diagram radar pada Gambar 3 menunjukkan hasil penilaian untuk 5 area utama dari indeks KAMI. Dari 5 area utama, 3 area telah masuk dalam tahap “Penerapan Operasional”, yaitu aspek Teknologi, Tata Kelola, dan Pengelolaan Risiko. Sedangkan 2 area yang lain yaitu Pengelolaan Aset dan Kerangka Kerja ada dalam tahap “Kerangka Kerja Dasar”. Hasil evaluasi akhir berdasarkan pemetaan skor kelengkapan yang diperoleh (skor=435) sesuai dengan Tabel 2 menunjukkan bahwa pengamanan informasi pada Diskominfosandi Kabupaten XYZ masih dalam status “Pemenuhan Kerangka Kerja Dasar”.



Gambar 3. *Dashboard* Penilaian Indeks KAMI 4.2 Diskominfosandi Kabupaten XYZ

4.2. Tata Kelola Keamanan Informasi

Hasil penilaian pada area Tata Kelola Keamanan Informasi menunjukkan terdapat peningkatan pada beberapa poin. Namun masih ada beberapa bagian yang perlu ditingkatkan lagi dikarenakan dapat berdampak negatif pada kegiatan tata kelola pengamanan informasi. Selain ada beberapa poin yang masih kurang, terdapat beberapa poin yang tidak ditemukan dokumen pendukungnya saat evaluasi. Sebagai contoh, pada poin 14 yang berisi pertanyaan "Apakah tanggung jawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?", tidak ada dokumen pendukungnya sehingga skor yang diberikan adalah 2 (dalam perencanaan). Contoh bukti dokumen yang harus tersedia untuk poin 14 adalah dokumen yang berisi definisi dan tanggung jawab untuk mengelola *business continuity* dan *disaster recovery plan*. Kekurangan yang lain adalah belum didefinisikannya kebijakan dan langkah-langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum pidana maupun perdata.

4.2.1. Pengelolaan Risiko Keamanan Informasi

Pengelolaan risiko terkait keamanan informasi sudah dilaksanakan, namun untuk pengawasan dan evaluasi terhadap penerapan pengelolaan risiko terkait keamanan informasi tersebut belum dilaksanakan. Terdapat penurunan nilai pada poin 12, 13 dan 14 dikarenakan tidak ada dokumen yang dapat membuktikan bahwa aktivitas pada poin tersebut dilakukan pada saat penilaian dilakukan, sedangkan pada penilaian sebelumnya dokumen bukti aktivitas pada poin tersebut tersedia. Penurunan pada poin-poin tersebut yang menunjukkan bahwa proses pengawasan dan evaluasi terhadap penerapan pengelolaan risiko terkait keamanan informasi tersebut belum dilaksanakan. Dokumentasi dan pencatatan terkait status penyelesaian langkah mitigasi risiko, evaluasi penyelesaian langkah mitigasi yang sudah diterapkan, dan hasil kaji ulang profil risiko beserta mitigasinya tidak ditemukan. Keberadaan dokumen pendukung sangat penting untuk memastikan penyelesaian atau kemajuan proses mitigasi risiko tersebut, memastikan konsistensi dan efektivitas dari langkah mitigasi tersebut, juga memastikan akurasi dan validitas termasuk merevisi profil risiko yang ada apabila terjadi perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan yang baru.

4.2.2. Kerangka Kerja Keamanan Informasi

Bagian Kerangka Kerja Pengamanan informasi mengalami peningkatan jika dibandingkan dengan penilaian sebelumnya. Peningkatan tersebut terdapat pada poin 1, 3, 6, 7, 11, 13, 24, 25, 27, 28 dan 29. Namun pada bagian ini juga terdapat penurunan nilai pada poin 4, 5, 9, 10, 12, 14, dan 19. Penurunan tersebut terjadi karena tidak ada dokumen yang dapat membuktikan bahwa aktivitas pada poin tersebut dilakukan pada saat penilaian dilakukan, sedangkan pada penilaian sebelumnya dokumen bukti aktivitas pada poin tersebut tersedia. Dokumen pendukung untuk bagian Kerangka Kerja Pengamanan Informasi ini sangat penting sebagai pedoman dalam mengatur layanan TIK mulai dari kebijakan, standar, prosedur, sampai dengan personil yang melaksanakan masing-masing kegiatan layanan TIK tersebut.

4.2.3. Pengelolaan Aset Keamanan Informasi

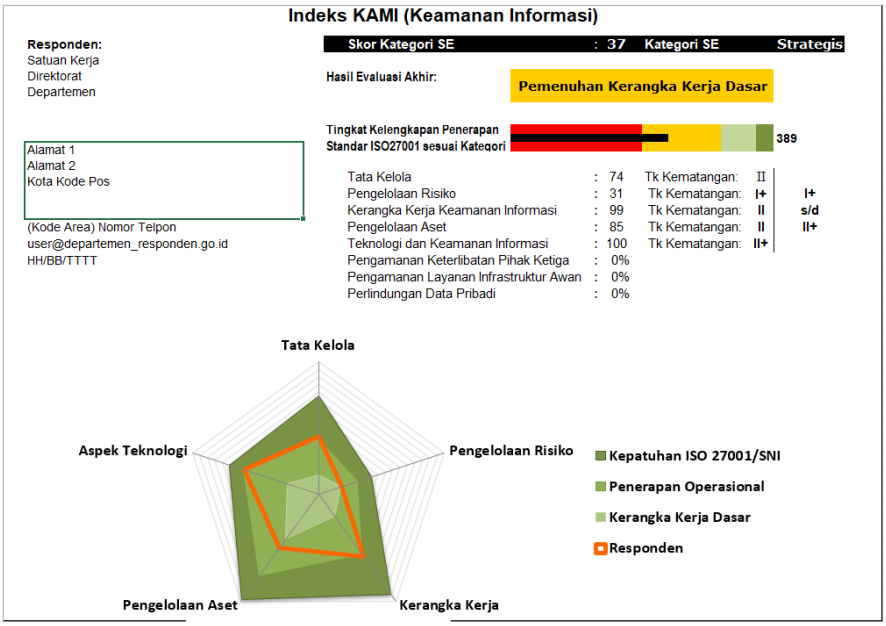
Terdapat penurunan nilai pada poin 4, 6, 7, 9, 10, 11, 18, 19, 20, 24, 25, 26, 27 dan 38 dikarenakan tidak ada dokumen yang dapat membuktikan bahwa aktivitas pada poin tersebut dilakukan pada saat penilaian dilakukan, sedangkan pada penilaian sebelumnya dokumen bukti aktivitas pada poin tersebut dilakukan tersedia. Poin 6, 7, 9, 10, 11, 18, 19, 20 dan 24 berada dalam tahap "Dalam Perencanaan" dikarenakan pihak Diskominfosandi Kabupaten XYZ sedang menyusun dokumen yang berisi terkait poin-poin tersebut. Untuk poin 25 dan 26 seharusnya mendapatkan skor 9, poin 27 dan 38 seharusnya mendapatkan skor 3. Namun karena total skor dari tahap penerapan 1 dan 2 tidak melebihi batas skor minimal untuk skor tahap penerapan 3 maka skor pada tahap penerapan 3 tidak dihitung dan tampil sebagai '0' pada alat ukur indeks KAMI 4.2. Batas skor minimal yang dijumlahkan dari nilai tahap 1 dan tahap 2 adalah 88, namun total tahap penerapan 1 dan 2 tidak mencapai batas skor minimal dan hanya mendapatkan nilai 79.

4.2.4. Teknologi dan Keamanan Informasi

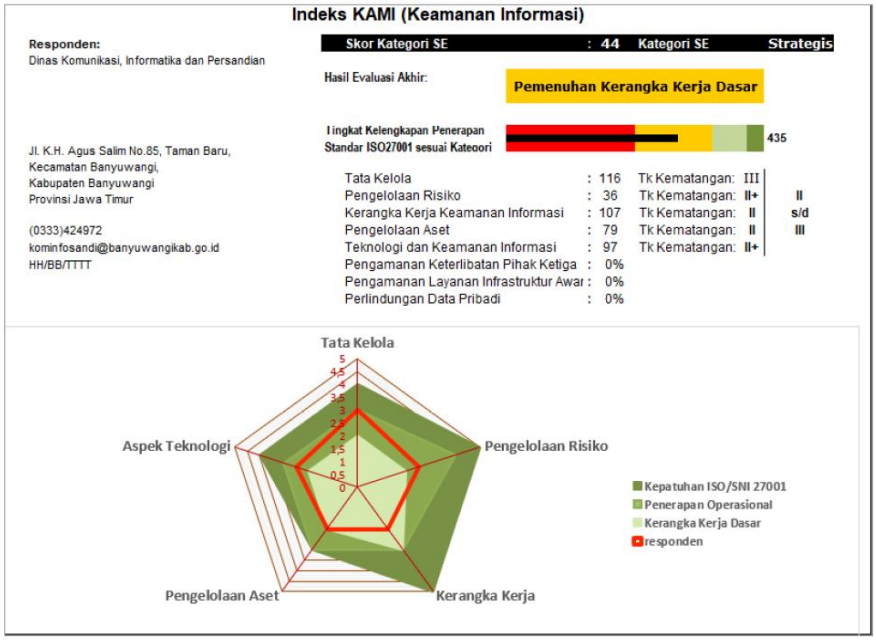
Terdapat penurunan nilai pada poin 14, 15, 24 dan 25 dikarenakan tidak ada dokumen yang dapat membuktikan bahwa aktivitas pada poin tersebut dilakukan pada saat penilaian dilakukan, sedangkan pada penilaian sebelumnya dokumen bukti aktivitas pada poin tersebut dilakukan tersedia. Dampak dari tidak dilakukannya poin 25 cukup besar. Tidak diterapkannya lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun (poin 25), dapat memiliki dampak yang serius pada keamanan dan kualitas sistem yang dihasilkan.

4.3. Perbandingan Hasil Penilaian

Hasil evaluasi sebelumnya ditunjukkan pada Gambar 4 sedangkan hasil evaluasi yang dilakukan pada penelitian ini ditunjukkan pada Gambar 5.



Gambar 4. *Dashboard Hasil* Penilaian Indeks KAMI Tahun 2019



Gambar 5. *Dashboard* Hasil Penilaian Indeks KAMI Tahun 2023

Dari Gambar 4 dan Gambar 5 dapat dilihat bahwa untuk area Tata Kelola, Pengelolaan Risiko, dan Kerangka Kerja Keamanan Informasi mengalami peningkatan. Area Tata Kelola yang sebelumnya memiliki skor 74 (Tingkat Kematangan II) telah naik menjadi 116 (Tingkat Kematangan III), area Pengelolaan Risiko yang sebelumnya memiliki skor 31 (Tingkat Kematangan I+) telah naik menjadi 36 (Tingkat Kematangan II+), area Kerangka Kerja Keamanan Informasi yang sebelumnya memiliki skor 99 (Tingkat Kematangan II) telah naik menjadi 107 (Tingkat Kematangan II). Namun area Pengelolaan Aset mengalami penurunan, yang sebelumnya memiliki skor 85 (Tingkat Kematangan II) telah turun menjadi

79 (Tingkat Kematangan II). Area Teknologi dan Keamanan Informasi juga mengalami penurunan dari skor 100 (Tingkat Kematangan II+) menjadi 97 (Tingkat Kematangan II+). Secara keseluruhan, tingkat kelengkapan Penerapan Standar ISO 27001 sesuai kategori telah meningkat secara signifikan dari skor 389 ke 435 dan juga jangkauan (*range*) tingkat kematangan Indeks KAMI telah meningkat dari I+ sampai dengan II+ menjadi II sampai dengan III.

4.4. Rekomendasi Perbaikan

Berdasarkan temuan yang didapatkan, dirancang rekomendasi perbaikan yang dapat dilakukan oleh Diskominfosandi Kabupaten XYZ. Rekomendasi disusun berdasarkan kebutuhan yang tercantum pada masing-masing pertanyaan. Rekomendasi untuk seluruh domain disajikan pada Tabel 3.

Tabel 3. Rekomendasi Perbaikan

No	Domain	Permasalahan	Rekomendasi
1	Tata Kelola Keamanan Informasi	1. Belum ditetapkannya personel yang bertanggung jawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plan*) 2. Belum didefinisikannya kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)	1. Menetapkan personel yang bertanggung jawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plan*) 2. Menyusun kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)
2	Pengelolaan Risiko Keamanan Informasi	1. Belum dilaksanakannya pemantauan status penyelesaian langkah mitigasi risiko secara berkala 2. Belum dilaksanakannya evaluasi melalui proses yang objektif/ terukur terhadap penyelesaian langkah mitigasi yang sudah diterapkan 3. Belum dilaksanakannya kaji ulang secara berkala terhadap bentuk mitigasi dari profil risiko 4. Belum dilaksanakannya kaji ulang secara berkala terhadap kerangka kerja pengelolaan risiko 5. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian objektif kinerja efektivitas pengamanan	1. Menetapkan kebijakan dan prosedur terkait pemantauan atas status penyelesaian langkah mitigasi risiko secara berkala dan melaksanakannya 2. Melaksanakan evaluasi terhadap penyelesaian langkah mitigasi yang sudah diterapkan melalui proses yang objektif/ terukur 3. Melaksanakan kaji ulang bentuk mitigasi dari profil risiko secara berkala 4. Melaksanakan kaji ulang kerangka kerja pengelolaan risiko secara berkala 5. Melaksanakan penilaian objektif kinerja efektivitas pengamanan dan menjadikan pengelolaan risiko sebagai salah satu dari kriteria-kriteria proses penilaian tersebut
3	Kerangka Kerja Pengelolaan Keamanan informasi	1. Belum ditetapkannya kebijakan keamanan informasi secara formal 2. Belum dipublikasikannya kebijakan keamanan informasi kepada semua staf/ karyawan termasuk pihak terkait 3. Belum dipastikannya kemudahan kebijakan keamanan informasi diakses oleh pihak yang membutuhkannya	1. Menyusun, menetapkan dan menerapkan kebijakan dan prosedur keamanan informasi secara formal serta mempublikasikannya kepada semua staf/ karyawan termasuk pihak terkait dan dipastikan kemudahan aksesnya agar dapat diakses oleh pihak yang membutuhkannya. Pastikan kebijakan dan prosedur keamanan informasi merefleksikan

No	Domain	Permasalahan	Rekomendasi
		4. Belum tersedia prosedur (mencakup pelaksana, mekanisme, jadwal, materi dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga 5. Kebijakan dan prosedur keamanan informasi yang ada belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/ objektif tertentu yang ditetapkan oleh Kepala Dinas Komunikasi Informatika dan Persandian 6. Belum tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindaklanjuti sesuai prosedur yang diberlakukan 7. Belum tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindaklanjuti konsekuensi dari kondisi tersebut 8. Belum diterapkannya kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya 9. Belum diterapkannya proses mengevaluasi risiko terkait rencana pembelian/ implementasi sistem baru dan menanggulangi permasalahan yang muncul 10. Belum ada proses untuk menanggulangi penerapan suatu sistem yang mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya 11. Belum memiliki perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sehingga belum diatur terkait pelaksanaan uji coba dan tim pemulihan bencana terhadap layanan TIK tersebut 12. Belum dilaksanakannya evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala	kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/ objektif tertentu yang ditetapkan oleh Kepala Dinas Komunikasi Informatika dan Persandian 2. Menyusun dan menetapkan prosedur (mencakup pelaksana, mekanisme, jadwal, materi dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga 3. Menyesuaikan kebijakan dan prosedur keamanan informasi yang ada dengan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/ objektif tertentu yang ditetapkan oleh Kepala Dinas Komunikasi Informatika dan Persandian 4. Menyusun, menetapkan dan menerapkan prosedur penanganan permasalahan/ insiden keamanan informasi yang di dalamnya memiliki proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindaklanjuti 5. Menyusun, menetapkan dan menerapkan prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindaklanjuti konsekuensi dari kondisi tersebut 6. Menyusun, menetapkan dan menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya 7. Menyusun, menetapkan dan menerapkan proses mengevaluasi risiko terkait rencana pembelian/ implementasi sistem baru dan menanggulangi permasalahan yang muncul 8. Menerapkan proses untuk menanggulangi penerapan suatu sistem yang mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya

No	Domain	Permasalahan	Rekomendasi
			9. Menyusun, menetapkan dan menerapkan perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) 10. Melaksanakan evaluasi kelayakan kebijakan dan prosedur keamanan informasi secara berkala
4	Pengelolaan Aset Informasi	1. Daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi telah dibuat, namun belum termasuk dengan kepemilikan asetnya 2. Belum tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya 3. Belum ditetapkannya tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut 4. Belum tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten 5. Belum tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi 6. Belum memiliki dan menerapkan tata tertib terkait penggunaan komputer, email, internet dan intranet 7. Belum memiliki dan menerapkan tata tertib pengamanan dan penggunaan aset instansi terkait HAKI 8. Belum memiliki dan menerapkan peraturan terkait instalasi piranti lunak di aset TI milik instansi 9. Ketentuan terkait identitas elektronik dan proses autentikasi (*username & password*) termasuk kebijakan terhadap pelanggarannya telah dimiliki namun untuk penerapannya baru diterapkan sebagian belum secara menyeluruh 10. Belum memiliki dan menerapkan persyaratan dan prosedur pengelolaan/ pemberian akses, autentikasi dan autorisasi untuk menggunakan aset informasi 11. Belum memiliki dan menerapkan ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data 12. Belum memiliki dan menerapkan prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala 13. Belum memiliki dan menerapkan ketentuan pengamanan fisik yang disesuaikan dengan	1. Memperbarui daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi dengan menambahkan kepemilikan dari masing-masing aset yang telah terdata, dan menambahkan aset yang belum terdata dalam daftar inventaris tersebut 2. Menyusun, menetapkan dan menerapkan proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya 3. Menetapkan tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut (*user access matrix*) 4. Menyusun, menetapkan dan menerapkan proses pengelolaan konfigurasi yang diterapkan secara konsisten (Kebijakan dan prosedur pengelolaan konfigurasi perangkat keras dan perangkat lunak) 5. Menyusun, menetapkan dan menerapkan proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi 6. Menyusun, menetapkan dan menerapkan tata tertib terkait penggunaan komputer, email, internet dan intranet dalam rangka melaksanakan pengamanan informasi 7. Menyusun, menetapkan dan menerapkan tata tertib pengamanan dan penggunaan aset instansi terkait HAKI 8. Menyusun, menetapkan dan menerapkan peraturan terkait instalasi piranti lunak di aset TI milik instansi 9. Menerapkan ketentuan terkait identitas elektronik dan proses autentikasi (*username & password*) termasuk kebijakan terhadap pelanggarannya secara menyeluruh 10. Menyusun, menetapkan dan menerapkan persyaratan dan prosedur pengelolaan/ pemberian akses, autentikasi dan autorisasi untuk menggunakan aset informasi

No	Domain	Permasalahan	Rekomendasi
		definisi zona dan klasifikasi aset yang ada di dalamnya 14. Belum memiliki dan menerapkan proses pengecekan latar belakang SDM 15. Belum memiliki dan menerapkan prosedur penghancuran data/ aset yang sudah tidak diperlukan 16. Belum memiliki dan menerapkan prosedur untuk *user* yang mutasi/ keluar atau tenaga kontrak/ *outsource* yang habis masa kerjanya 17. Belum memiliki dan menerapkan prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/ *vendor*) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan 18. Belum tersedia peraturan pengamanan perangkat komputasi milik instansi apabila digunakan di luar lokasi kerja resmi (kantor) 19. Belum tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga 20. Belum tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya (misal larangan penggunaan telepon genggam di dalam ruang server, menggunakan kamera, dll) 21. Belum tersedia proses untuk mengamankan lokasi kerja dari keberadaan/ kehadiran pihak ketiga yang bekerja untuk kepentingan instansi	11. Menyusun, menetapkan dan menerapkan ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data 12. Menyusun, menetapkan dan menerapkan prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala 13. Menyusun, menetapkan dan menerapkan ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya 14. Menyusun, menetapkan dan menerapkan proses pengecekan latar belakang SDM [Menyusun, menetapkan dan menerapkan prosedur penghancuran data/ aset yang sudah tidak diperlukan 15. Menyusun, menetapkan dan menerapkan prosedur untuk user yang mutasi/ keluar atau tenaga kontrak/ *outsource* yang habis masa kerjanya 16. Menyusun, menetapkan dan menerapkan 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 17. Menyusun, menetapkan dan menerapkan peraturan pengamanan perangkat komputasi milik instansi apabila digunakan di luar lokasi kerja resmi/ kantor (kebijakan, standar dan prosedur *remote access control*). 18. Menyusun, menetapkan dan menerapkan mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga 19. Menyusun, menetapkan dan menerapkan peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya (misal larangan penggunaan telepon genggam di dalam ruang server, menggunakan kamera, dll) 20. Menyusun, menetapkan dan menerapkan proses untuk mengamankan lokasi kerja dari keberadaan/ kehadiran pihak ketiga yang bekerja untuk kepentingan instansi (misal pembatasan akses masuk ke dalam lokasi kerja, dll)

No	Domain	Permasalahan	Rekomendasi
5	Teknologi Keamanan Informasi	1. Sistem dan aplikasi belum secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/ panjangnya dan penggunaan kembali *password* lama 2. Akses yang digunakan untuk mengelola sistem (administrasi sistem) belum menggunakan bentuk pengamanan khusus yang berlapis 3. Setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/ validasi pada saat proses pengembangan dan uji coba namun belum terdapat dokumentasi atas hal tersebut 4. Belum diterapkannya lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun	1. Menerapkan otomatisasi pada sistem dan aplikasi agar dapat secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/ panjangnya dan penggunaan kembali *password* lama 2. Memberi pengamanan khusus yang berlapis pada akses untuk mengelola sistem (administrasi sistem) 3. Menerapkan dan mendokumentasikan spesifikasi dan fungsi keamanan yang diverifikasi/ validasi pada saat proses pengembangan dan uji coba setiap aplikasi yang ada dan yang akan ada 4. Membuat dan menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun

5. Kesimpulan

Berdasarkan hasil pengukuran indeks KAMI, skor kelengkapan pengamanan informasi memperoleh skor 435 yang bermakna pengamanan informasi pada Diskominfosandi Kabupaten XYZ masih dalam status "Pemenuhan Kerangka Kerja Dasar". Tingkat kematangan pengamanan informasi Diskominfosandi Kabupaten XYZ berada pada tingkat kematangan II sampai III. Hal tersebut menunjukkan bahwa tingkat kematangan keamanan informasi Diskominfosandi Kabupaten XYZ masih berada di bawah dari standar yang dibutuhkan untuk sertifikasi ISO/IEC 27001 yaitu tingkat kematangan III+. Namun jika dibandingkan dengan hasil pengukuran pada evaluasi sebelumnya, pengamanan informasi pada Diskominfosandi Kabupaten XYZ telah mengalami peningkatan baik itu pada skor kelengkapan maupun tingkat kematangannya. Berdasarkan temuan pada tiap-tiap area, direkomendasikan beberapa hal untuk peningkatan terutama pada bagian Kerangka Kerja Keamanan Informasi dan Pengelolaan Aset Informasi yang masih berada pada tingkat kematangan II. Adapun rekomendasi telah diberikan pada pihak Diskominfosandi Kabupaten XYZ dan akan ditindaklanjuti sebagai langkah perbaikan.

Referensi

[1] R. Budiarto, "Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA dan ISO 27001 Pada Organisasi Xyz," *CESS (Journal Comput. Eng. Syst. dan Sci.*, vol. 2, no. 2, pp. 48–58, 2017.

[2] Y. Rahmah, W. H. N. Putra, and A. D. Herlambang, "Evaluasi Tingkat Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan Menggunakan Indeks KAMI," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 3, pp. 840–847, 2020, Accessed: Oct. 13, 2021. [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7067

[3] D. Dwi Prasetyowati, I. Gamayanto, and S. wibowo, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," *J. Inf. Syst.*, vol. 4, no. 1, pp. 65–75, 2019.

[4] Menteri Komunikasi dan Informatika Republik Indonesia, "Peraturan Menteri Komunikasi dan

Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi." 2016.
[5] Badan Siber dan Sandi Negara, "Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik." 2020.
[6] R. A. Syarif and A. Nugroho, "Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur dengan Menggunakan Indeks Keamanan Informasi (Studi Kasus: Aplikasi Span)," *J. Info Artha*, vol. 4, pp. 69–80, 2016, doi: 10.31092/jia.v4i4.46.
[7] B. Lembah Mahersmi, F. Artowini Muqtadiroh, and B. Cahyo Hidayanto, "Pada Dishubkominfo Kabupaten Tulungagung," *Semin. Nas. Sist. Inf. Indones.*, no. November, pp. 181–194, 2016.
[8] A. Ramadhani, "KEAMANAN INFORMASI," *JILS J. Inf. Libr. Stud.*, vol. 1, no. 1, 2018, Accessed: Nov. 03, 2021. [Online]. Available: http://103.66.199.204/index.php/JILS/article/view/249/332
[9] E. Kurniawan, "Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 1, pp. 139–147, 2018, Accessed: Oct. 30, 2021. [Online]. Available: https://dspace.uii.ac.id/handle/123456789/5665
[10] A. B. Setiawan, "Kajian Kesiapan Keamanan Informasi Instansi Pemerintah Dalam Penerapan E-Government," *J. Masy. Telemat. dan Inf.*, vol. 4, no. 2, pp. 109–126, 2013.
[11] N. Arman, W. Hayuhardhika, N. Putra, and A. Rachmadi, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI)," vol. 3, no. 6, pp. 5750–5755, 2019, [Online]. Available: http://j-ptiik.ub.ac.id
[12] T. E. Wijatmoko, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Kantor Wilayah Kementerian Hukum dan HAM DIY," *csecurity*, vol. 3, no. 1, pp. 1–6, 2020, doi: https://doi.org/10.14421/csecurity.2020.3.1.1951.
[13] BSSN, "Website BSSN yang mengandung Indeks KAMI [," 2023. https://www.bssn.go.id/indeks-kami/
[14] M. Maidiana, "Penelitian Survey," *ALACRITY J. Educ.*, vol. 1, no. 2, pp. 20–29, 2021, doi: 10.52121/alacrity.v1i2.23.
[15] J. W. Creswell and J. D. Creswell, *Mixed Methods Procedures*. 2018.
[16] Ardiansyah, Risnita, and M. S. Jailani, "Teknik Pengumpulan Data Dan Instrumen Penelitian Ilmiah Pendidikan Pada Pendekatan Kualitatif dan Kuantitatif," *J. IHSAN J. Pendidik. Islam*, vol. 1, no. 2, pp. 1–9, 2023, doi: 10.61104/ihsan.v1i2.57.