

SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)

Piski Sundari¹, Wella²

^{1,2}Program Studi Sistem Informasi, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara, Tangerang, Indonesia
²wella@umn.ac.id

Diterima 06 Juli 2020

Disetujui 11 November 2021

Abstract—Pusdatin of the Ministry of Public Works and Public Housing is an institution that manages data and information to support management within the ministry of public works. This research was conducted to evaluate the maturity of agencies prior to conducting an external audit of ISO 27001: 2013 certification. The method used in this research is PDCA (Plan-Do-Check-Act) using our index and ISO 27001, the technicality of this research starts from a check for analysis of current conditions, Act is carried out for assessment of the WE index, Plan compares our index results with ISO 27001, and Do control recommendations for improvement. The results of this evaluation show that PUSDATIN stopped at level I + in yellow area and overall PUSDATIN stated, "Needs improvement". In conclusion, Pusdatin is not ready for an external audit of ISO 27001: 2013 certification. The aforementioned results form the basis for the recommendations made from the findings of the WE index and compared with the ISO 27001 control.

Index Terms—audit keamanan informasi; indeks KAMI; ISO 27001:2013; tingkat kematangan SMKI

I. PENDAHULUAN

Peraturan yang diterbitkan pemerintah mengenai keamanan informasi yang tertera pada Permen No.82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dengan merujuk pada standar sistem manajemen keamanan informasi, yang mengharuskan instansi penyelenggaraan publik menetapkan tata kelola keamanan informasi secara andal dan aman serta tanggung jawab yang sesuai dengan permen yang sudah ditetapkan [1][2]. Tata kelola teknologi informasi dapat diartikan sebagai upaya menjamin pengelolaan teknologi informasi agar mendukung bahkan selaras dengan strategi bisnis yang dilakukan oleh pemimpin instansi mengenai manajemen teknologi informasi [2].

Instansi Pusdatin merupakan salah satu balai yang memiliki tugas pokok dan fungsi mengelola dan menyediakan data yang menunjang manajemen dilingkungan Kementerian Pekerjaan Umum dan Perumahan Rakyat, dalam pelaksanaannya untuk menunjang tugas dan fungsi, pusdatin didukung dengan alat teknologi yang canggih untuk melindungi

aset informasi yang dikelola. Dalam pelaksanaannya banyak ancaman risiko yang mungkin terjadi pada instansi Pusdatin. Dengan menyadari adanya risiko-risiko yang dapat menyebabkan terganggunya pelayanan publik baik risiko pelanggaran yang disengaja dan tidak disengaja oleh pihak yang kurang bertanggungjawab, serta bentuk kejahatan lainnya dalam rangka mencapai target yang telah ditetapkan segingga dibutuhkan adanya evaluasi terhadap keamanan informasi [3].

Berdasarkan wawancara, Pusdatin belum pernah melakukan evaluasi Tata Kelola Keamanan Informasi dan menerapkan standarisasi keamanan informasi. Padahal sebagai lembaga pemerintahan, pusdatin seharusnya melakukan evaluasi untuk dapat menilai sudah sejauh mana instansi ini menjalankan keamanan informasi sebagai instansi penyelenggara publik. Sebelum standarisasi diterapkan, Pusdatin perlu dilakukan evaluasi keamanan informasi di unit kerja untuk mendapatkan kondisi kesiapan dan kematangan keamanan informasi sebelum melakukan sertifikasi ISO 27001:2013.

Tujuan dari penelitian ini adalah untuk mengetahui sejauh mana kesiapan dan kematangan Pusdatin dalam rangka menuju Sertifikasi ISO 27001:2013 sambil memberikan rekomendasi perbaikan manajemen keamanan sistem informasi yang dapat diterapkan di Pusdatin.

Penelitian ini dilakukan dengan menggunakan alat evaluasi Indeks KAMI yang dikeluarkan oleh DISKOMINFO [1], menggunakan metode siklus PDCA, namun pada penelitian ini siklus yang terlebih dahulu dilakukan dimulai dari (*Check-Action-Plan-Do*).

II. TINJAUAN PUSTAKA

A. Peran Sistem Informasi

Teknologi informasi adalah suatu teknologi yang berhubungan dengan pengolahan data menjadi informasi dan proses penyaluran data atau informasi tersebut dalam batas-batas ruang dan waktu. Teknolgi

informasi sebagai perangkat lunak ataupun keras yang digunakan sistem informasi. Sistem informasi adalah sekumpulan *hardware, software, brainware, procedure* dan atau aturan yang diorganisasikan secara integral untuk mengolah data menjadi informasi yang bermanfaat guna memecahkan masalah dan pengambilan keputusan. Teknologi informasi ini sangat berperan dalam berbagai bidang baik itu bidang pendidikan, pemerintahan, perbankan atau pun perdagangan. Dalam suatu teknologi informasi baik peranan untuk bidang apa pun tidak akan lepas dengan apa yang namanya suatu sistem dan informasi [5].

B. Keamanan Informasi

Keamanan informasi merupakan upaya untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis [6]. Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan dalam kombinasi satu dengan yang lainnya. Strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Aspek-aspek keamanan informasi dalam suatu organisasi dapat dilihat pada Gambar 1 di bawah ini:



Gambar 1. Aspek keamanan informasi [7]

1. *Availability* = ketersediaan data
2. *Integrity* = menjamin kelengkapan informasi dari kerusakan
3. *Confidentiality* = menjamin kerahasiaan data

C. ISO/IEC 27001 Sebagai Standar SMKI

Standar yang merupakan standar nasional ini dibuat sebagai model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan, dan perbaikan. Sistem Manajemen Keamanan Informasi (SMKI). Desain dan penerapan SMKI dari suatu perusahaan dipengaruhi oleh kebutuhan dan sasaran perusahaan. Standar ini dan sistem pendukungnya diperkirakan akan berubah dari waktu ke waktu. Penerapan SMKI disesuaikan pula dengan kebutuhan perusahaan. Standar ini dapat

digunakan untuk menilai kesesuaian oleh pihak terkait baik internal maupun eksternal [4].

SMKI merupakan sebuah pendekatan yang bersifat sistematis yang bertujuan untuk mengelola informasi penting maupun informasi perusahaan yang bersifat sensitif agar tetap aman. SMKI ini juga memberikan panduan untuk mengelola unsur yang termasuk dalam melakukan pengelolaan informasi penting seperti manusia, proses dan sistem teknologi informasi dengan menerapkan proses manajemen risiko yang telah sesuai standar [8].

D. Indeks Keamanan Informasi (KAMI) tools SMKI

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001 [9].

Indeks KAMI membagi menjadi 2 proses, yang pertama mengetahui Tingkat Kepentingan TIK pada instansi untuk mengukur seberapa tinggi tingkat ketergantungan menggunakan TIK instansi untuk mendukung kegiatan proses bisnis yang dilakukan instansi dan yang ke dua adalah mengukur 5 area Kematangan Keamanan Informasi. Gambar 2 ini merupakan contoh radar *chart* 5 area Indeks KAMI.



Gambar 2. Contoh diagram radar *chart* indeks KAMI

Gambar 2 adalah Radar *Chart* dari jumlah (nilai) yang dihasilkan kemudian dipetakan sesuai dengan tingkat kepentingan TIK terhadap cakupan instansi tersebut. Status Kesiapan yang dicapai merupakan kondisi yang dilaporkan.

Peran TIK		Indeks (Skor Akhir)		Status Kesiapan
Rendah		0	124	Tidak Layak
0	12	125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang		Skor Akhir		Status Kesiapan
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		Skor Akhir		Status Kesiapan
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik/Cukup
Kritis		Skor Akhir		Status Kesiapan
37	48	0	333	Tidak Layak
		334	453	Perlu Perbaikan
		454	588	Baik/Cukup

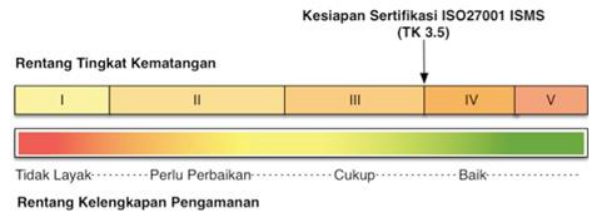
Gambar 3. Matriks peran dan status kesiapan [9]

Gambar 3 menggambarkan bahwa semakin tinggi ketergantungan terhadap TIK atau semakin penting peran TIK terhadap tugas instansi tersebut, maka semakin banyak bentuk pengamanan yang diperlukan, dan yang harus diterapkan sampai tahap tertinggi. Dengan menggunakan gambar matriks diatas, Status Kesiapan atau Kelengkapan dapat ditampilkan dengan instrumen *Bar Chart* seperti terlihat pada Gambar 4 di bawah ini:



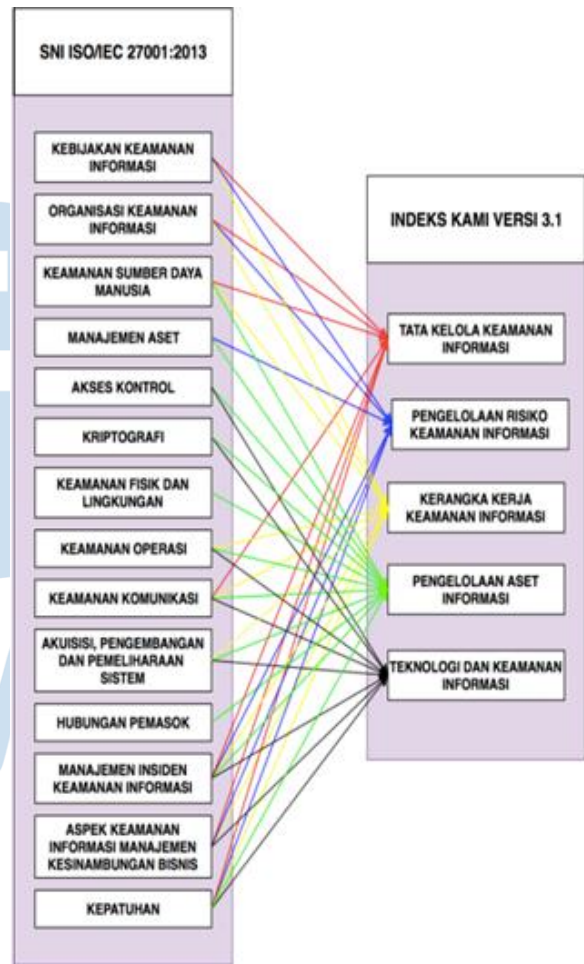
Gambar 4. Contoh hasil evaluasi tingkat kelengkapan [9]

Gambar 4 menjelaskan pencapaian yang masih ada di area berwarna merah masih dalam status kesiapan “Tidak Layak”, kemudian pencapaian di area warna kuning masih “Memerlukan Perbaikan”, sedangkan pencapaian warna hijau menunjukkan bahwa status kesiapan sudah “Baik/Cukup”. Sebagai contoh, untuk instansi yang peran/ketergantungan terhadap TIK dinilai sebagai “Rendah” dan total jumlah nilai kelengkapan 234. Gambaran rentang kelengkapan pengmanana atau level yang dicapai dapat dilihat pada Gambar 5 di bawah ini:



Gambar 5. *Bar chart* tingkat kelengkapan penerapan standar ISO 27001:2013 pada indeks KAMI [9]

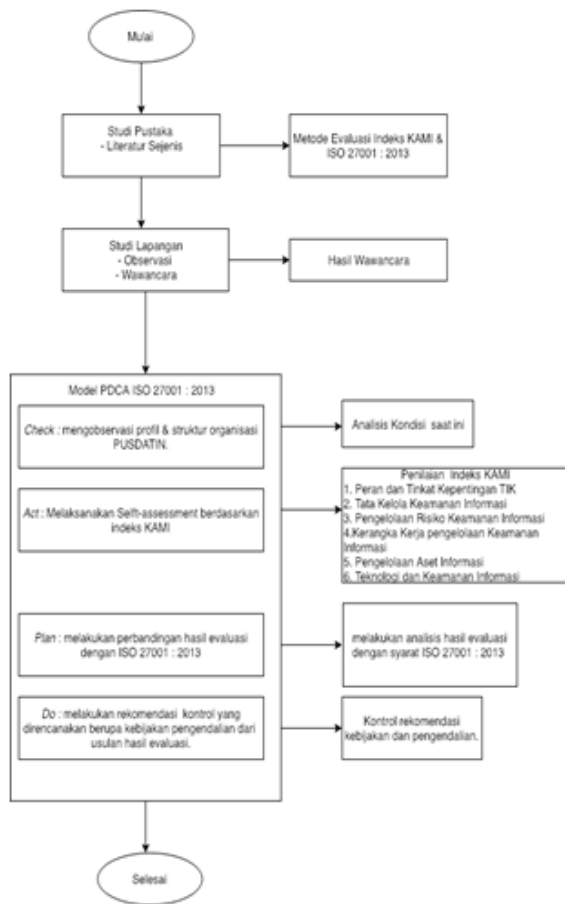
E. Keterkaitan Indeks KAMI dengan ISO 27001 : 2013



Gambar 6. Korelasi indeks KAMI dengan ISO 27001 : 2013 [9]

Gambar 6 ini menjelaskan korelasi antara Indeks KAMI dengan ISO 27001:2013, area yang digunakan dalam indeks KAMI untuk mengevaluasi atau mengukur tingkat sasaran pengendalian yang ada di ISO 27001:2013 ke dalam 5 area evaluasi.

III. METODOLOGI PENELITIAN



Gambar 7. Metodologi penelitian

Metodologi merupakan tahapan-tahapan atau alur yang akan digunakan untuk melakukan penelitian. Didalam penelitian ini dilakuka nenerapa tahap awal untuk melakukan studi literatur, melkakukan pengumpulan data, melakukan observasi serta menganalisa kondisi dilapangan.

Tahap pertama pada proses diatas yaitu melakukan studi pustaka dan literatur yang sejenis dengan penelitian yang sedang dilakukan. Selanjutnya dilakukan studi lapangan dimana tahap ini dilakukan untuk melihat kondisi instansi saat ini dan melakukan wawancara tahap 1 sebelum assesment. Tahap selanjutnya melakukan pendekatan proses penelitian menggunakan PDCA (*Plan – Do – Check – Act*). Namun pada peelitian ini PDCA dilakukan dengan proses acak yang dimulai dari *Check – Act – Plan – Do*, metode ini digunakan dengan menyesuaikan kondisi perusahaan.

Proses *Check* dilakukan untuk melihat kondisi instansi terkini dengan menganalisa dari profil perusahaan, struktur organisasi dan TUSI (Tugas dan Fungsi), *Action* dimana dilakukannya *Self-Assesment* berdasarkan Indeks KAMI.

Plan dimana proses lanjutan dari tahapan sebelumnya hasil evaluasi dari *assessment* dianalisa dan dibandingkan dengan kontrol ISO 27001.

Tahap terakhir *Do* adalah melakukan rekomendasi kontrol kebijakan dan pengendalian yang direncanakan berdasarkan hasil perbandingan dari hasil *assesment* dan kontrol ISO 27001.

IV. ANALISIS DAN PEMBAHASAN

Dari hasil Tingkat Ketergantungan TIK pada instansi berdasarkan penilaian Indeks KAMI, Kategori area ini instansi Pusdatin mendapatkan skor sebesar 39 dimana skor tersebut masuk kategori “KRITIS”. Arti dari kategori yang didapatkan pada area tersebut adalah kepentingan instansi dalam menggunakan TIK bisa diartikan sebagai bagian yang tidak dapat dipisahkan, artinya TIK merupakan bagian penting dalam pelaksanaan kegiatan operasional arau proses kerja yang berjalan di instansi Pusdatin.

Berdasarkan hasil pengumpulan data *Assesment* Indeks KAMI, status kesiapan Pusdatin Kementerian Pekerjaan Umum dan Perumahan Rakyat hasil akhir berdasarkan Indeks KAMI adalah “Tidak Layak”. Hal ini dapat dijelaskan bahwa Pusdatin “Perlu Perbaikan” pada sejumlah area keamanan informasi.

A. Hasil Indeks Tata Kelola Keamanan Informasi

Pada bagian ini dilakukan evaluasi kesiapan bentuk tata kelola keamanan informasi, dalam penilaian skor kelengkapan yang didapatkan tata kelola keamanan informasi dari 20 pertanyaan yang dibagi menjadi 3 kategori yaitu kategori I = 8 pertanyaan, kategori II = 8, dan kategori II = 6 pertanyaan. Nilai yang diperoleh adalah 73 (64%) dari nilai maksimal area ini yaitu 114. Nilai tersebut didapatkan karena terdapat 1 pertanyaan pada Tingkat kematangan II yang disrespon dengan status “Tidak Dilakukan” dan 4 skor untuk pertanyaan yang dijawab dengan status “Dalam Perencanaan”. Berdasarkan Assesment yang dilakukan dalam area Tata Kelola Keamanan Informasi dengan menggunakan Indeks KAMI hasil yang diperoleh adalah sebagai berikut:

Tabel 1. Skor kematangan area tata kelola

Keterangan	Skor
Total Nilai Evaluasi Tata Kelola	73
Jumlah pertanyaan tahap 1 = 8 Pertanyaan	14
Jumlah Pertanyaan Tahap 2 = 6 Pertanyaan	26
Jumlah Pertanyaan Tahap 3 = 6 Pertanyaan	33
Batas Skor Min untuk Skor Tahap Penerapan 3	40
Total Skor Tahap Penerapan 1 & 2	40
Status Penilaian Tahap Penerapan 3	Tidak Valid

Berdasarkan Tabel 1 diatas pertanyaan kategori 1 memiliki sebanyak 8 pertanyaan mendapat skor 14,

pertanyaan kategori 2 mendapat skor 26, dan pertanyaan kategori 3 mendapat skor 33.

Minimal skor untuk kategori penerapan 3 dan total skor tahap penerapan 1 & 2 memiliki nilai 40, hal tersebut diperoleh dari rumus yang sudah ditetapkan oleh Indeks KAMI. Status penilaian tahap penerapan 3 memiliki hasil “Tidak Valid” disebabkan karena tidak memenuhi nilai minimal yang dipersyaratkan untuk kategori 3.

B. Hasil Indeks Pengelolaan Risiko Keamanan Informasi

Pada bagian ini dilakukan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi. Dalam penilaiannya terdapat 15 pertanyaan yang terdapat pada area ini. Pertanyaan tersebut dibagi menjadi 3 kategori I = 9 pertanyaan, kategori II = 4 pertanyaan, dan kategori III = 2 pertanyaan. Nilai yang diperoleh pada area ini adalah 32 (46%) dari nilai maksimal area ini yaitu 69. Berdasarkan *Assesment* yang dilakukan dalam area Pengelolaan Risiko Keamanan Informasi dengan menggunakan Indeks KAMI hasil yang diperoleh adalah sebagai berikut:

Tabel 2. Skor kematangan area pengelolaan risiko keamanan informasi

Keterangan	Skor
Total Nilai Evaluasi Pengelolaan Risiko Keamanan	32
Jumlah pertanyaan tahap 1 = 9 Pertanyaan	16
Jumlah Pertanyaan Tahap 2 = 4 Pertanyaan	16
Jumlah Pertanyaan Tahap 3 = 2 Pertanyaan	0
Batas Skor Min untuk Skor Tahap Penerapan 3	34
Total Skor Tahap Penerapan 1 & 2	32
Status Penilaian Tahap Penerapan 3	Tidak Valid

Berdasarkan Tabel 2 pertanyaan kategori 1 sebanyak 9 pertanyaan memiliki skor 16, jumlah pertanyaan kategori 2 sebanyak 16, dan kategori 3 sebanyak 0.

Minimal skor untuk kategori penerapan 3 memiliki nilai skor 34, nilai tersebut sudah ditetapkan oleh Indeks KAMI sebelum jawaban kuesioner terjawab. Rumus tersebut berdasarkan dari nilai pemetaan skor “Dalam Penerapan/Diterapkan Sebagian” pada kategori pengamanan 1 dikalikan dengan jumlah pertanyaan kategori 1, ditambah nilai “Dalam Penerapan/Diterapkan Sebagian” pada kategori pengamanan 2 dikalikan jumlah pertanyaan kategori 2. Maha hasil penilaian status kategori penerapan 3 yang dihasilkan padatable diatas area pengelonaan Risiko Keamanan Informasi adalah “Tidak Valid”, karena tidak memenuhi nilai minimal yang dipersyaratkan untuk kategori 3.

C. Hasil Indeks Kerangka Kerja Pengelolaan Keamanan

Pada bagian ini dilakukan evaluasi kesiapan penerapan Kerangka Kerja Pengelolaan. Dalam penilaiannya terdapat 26 pertanyaan yang terdapat pada area ini. Pertanyaan tersebut dibagi menjadi 3: kategori I = 11 pertanyaan, kategori II = 8 pertanyaan, dan kategori III = 7 pertanyaan. Nilai yang diperoleh pada area ini adalah 95 (83%) dari nilai maksimal area ini yaitu 144. Berdasarkan *Assesment* yang dilakukan dalam area Kerangka Kerja Keamanan Informasi dengan menggunakan Indeks KAMI hasil yang diperoleh adalah sebagai berikut:

Tabel 3. Skor kematangan kerangka kerja pengelolaan risiko

Keterangan	Skor
Total Nilai Evaluasi Kerangka Kerja	95
Jumlah pertanyaan tahap 1 = 11 Pertanyaan	26
Jumlah Pertanyaan Tahap 2 = 8 Pertanyaan	30
Jumlah Pertanyaan Tahap 3 = 7 Pertanyaan	39
Batas Skor Min untuk Skor Tahap Penerapan 3	54
Total Skor Tahap Penerapan 1 & 2	56
Status Penilaian Tahap Penerapan 3	Valid

Berdasarkan Tabel 3 total nilai evaluasi kerangka kerja keamanan informasi memiliki nilai 95. Jumlah pertanyaan kategori 1 sebanyak 11 pertanyaan memiliki skor 26, jumlah pertanyaan kategori 2 memiliki skor sebanyak 30, dan jumlah pertanyaan kategori 3 memiliki skor sebanyak 39.

Nilai minimal skor untuk kategori tahap 3 yang dipersyaratkan bernilai 54, nilai tersebut sudah ditentukan dengan rumus yang sudah ditetapkan oleh Indeks KAMI dan sudah terisi sebelum pertanyaan kuesioner terjawab.

Hasil status penilaian tahap penerapan 3 memiliki status “Valid” dimana hal tersebut disebabkan karena sudah memenuhi nilai minimal yang dipersyaratkan untuk kategori 3, dimana skor tahap penerapan 1 & 2 memiliki skor yang lebih besar dari skor minimal tahap penerapan 3.

D. Hasil Indeks Pengelolaan Aset

Pada bagian ini dilakukan evaluasi kesiapan penerapan area pengelolaan aset. Dalam penilaiannya terdapat 34 pertanyaan yang terdapat pada area ini. Pertanyaan tersebut dibagi menjadi 3 kategori I = 21 pertanyaan, kategori II = 9 pertanyaan, dan kategori III = 4 pertanyaan. Nilai yang diperoleh pada area ini adalah 112 (73%) dari nilai maksimal area ini yaitu 153. Berdasarkan *Assesment* yang dilakukan dalam area Pengelolaan Aset Keamanan Informasi dengan menggunakan Indeks KAMI hasil yang diperoleh adalah sebagai berikut:

Tabel 4. Skor pengelolaan aset

Keterangan	Skor
Total Nilai Evaluasi Pengelolaan Aset	112
Jumlah pertanyaan tahap 1 = 21 Pertanyaan	50
Jumlah Pertanyaan Tahap 2 = 9 Pertanyaan	44
Jumlah Pertanyaan Tahap 3 = 4 Pertanyaan	18
Batas Skor Min untuk Skor Tahap Penerapan 3	78
Total Skor Tahap Penerapan 1 & 2	94
Status Penilaian Tahap Penerapan 3	Valid

Berdasarkan Tabel 4 ini total nilai evaluasi. Pengelolaan Aset keamanan informasi memiliki nilai 112. Jumlah pertanyaan kategori 1 sebanyak 21 pertanyaan memiliki skor 50, jumlah pertanyaan kategori 2 memiliki skor sebanyak 44, dan jumlah pertanyaan kategori 3 memiliki skor sebanyak 18.

Nilai minimal skor untuk kategori tahap 3 yang dipersyaratkan bernilai 78, nilai tersebut sudah ditentukan dengan rumus yang sudah ditetapkan oleh Indeks KAMI dan sudah terisi sebelum pertanyaan kuesioner terjawab.

Hasil status penilaian tahap penerapan 3 memiliki status "Valid" dimana hal tersebut disebabkan karena sudah memenuhi nilai minimal yang dipersyaratkan untuk kategori 3, dimana skor tahap penerapan 1 & 2 memiliki skor yang lebih besar dari skor minimal tahap penerapan 3.

E. Hasil Indeks Teknologi dan Keamanan Informasi

Pada bagian ini dilakukan evaluasi kesiapan penerapan area Teknologi dan Keamanan Informasi. Dalam penilaiannya terdapat 24 pertanyaan yang terdapat pada area ini. Pertanyaan tersebut dibagi menjadi 3 kategori I = 13 pertanyaan, kategori II = 10 pertanyaan, dan kategori III = 1 pertanyaan. Nilai yang diperoleh pada area ini adalah 82 (76%) dari nilai maksimal area ini yaitu 108. Berdasarkan *Assesment* yang dilakukan dalam area Teknologi dan Keamanan Informasi dengan menggunakan Indeks KAMI hasil yang diperoleh adalah sebagai berikut:

Tabel 5. Skor kematangan teknologi dan keamanan informasi

Keterangan	Skor
Total Nilai Evaluasi Kematangan Teknologi dan Keamanan Informasi	82
Jumlah pertanyaan tahap 1 = 13 Pertanyaan	32
Jumlah Pertanyaan Tahap 2 = 10 Pertanyaan	44
Jumlah Pertanyaan Tahap 3 = 1 Pertanyaan	6
Batas Skor Min untuk Skor Tahap Penerapan 3	66
Total Skor Tahap Penerapan 1 & 2	76
Status Penilaian Tahap Penerapan 3	Valid

Berdasarkan Tabel 5, total nilai evaluasi kerangka kerja keamanan informasi memiliki nilai 112. Jumlah

pertanyaan kategori 1 sebanyak 13 pertanyaan memiliki skor 32, jumlah pertanyaan kategori 2 memiliki skor sebanyak 44, dan jumlah pertanyaan kategori 3 memiliki skor sebanyak 6.

Nilai minimal skor untuk kategori tahap 3 yang dipersyaratkan bernilai 66, nilai tersebut sudah ditentukan dengan rumus yang sudah ditetapkan oleh Indeks KAMI dan sudah terisi sebelum pertanyaan kuesioner terjawab.

Hasil status penilaian tahap penerapan 3 memiliki status "Valid" dimana hal tersebut disebabkan karena sudah memenuhi nilai minimal yang dipersyaratkan untuk kategori 3, dimana skor tahap penerapan 1 & 2 memiliki skor 76 yang artinya lebih besar dari skor minimal tahap penerapan 3 yaitu 66.

F. Hasil Pengukuran Peran dan Tingkat Kepentingan TIK

Tabel 6. Hasil pengukuran peran dan tingkat kepentingan TIK

Peran dan Tingkat Kepentingan TIK di instansi Pusdatin		Skor
Skor	Tingkat	
0 - 12	Rendah	39 KRITIS
13 - 14	Sedang	
25 - 36	Tinggi	
37 - 48	Kritis	

Tabel 6 menunjukkan hasil untuk area Peran dan Tingkat Kepentingan TIK di instansi Pusdatin menunjukkan TIK memegang peran yang sangat penting di Pusdatin, hal ini ditunjukkan oleh perhitungan indeks KAMI, untuk area peran TIK Pusdatin memiliki Skor 39 yang berarti masuk dalam kategori nilai "KRITIS".

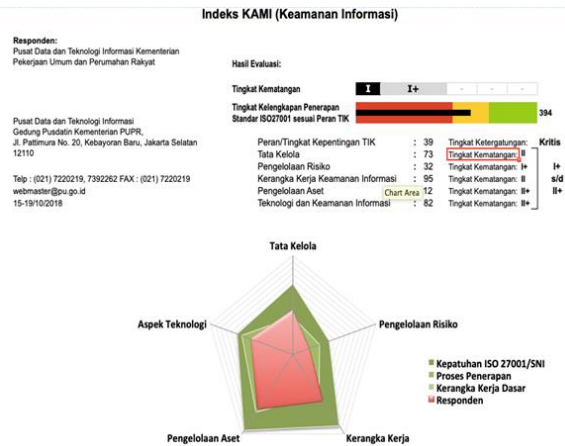
G. Hasil Pengukuran 5 Area Keamanan Informasi

Tabel 7. Hasil pengukuran 5 area keamanan informasi

Indeks KAMI	Skor	Tingkat Kematangan
Bagian II : Tata Kelola Keamanan Informasi	73	II
Bagian III : Pengelolaan Risiko Keamanan Informasi	32	I+
Bagian IV : Kerangka Kerja Pengelolaan Keamanan Informasi	95	II
Bagian V : Pengelolaan Aset Informasi	112	II+
Bagian VI : Teknologi dan Keamanan Informasi	82	II+
Total Skor (II+III+IV+V+VI)	394	I+ s/d II +

Pada Tabel 7 menunjukkan hasil pengukuran bagian II, IV, V, dan VI menunjukkan bahwa tingkat kematangan keamanan informasi di Pusdatin berada pada level II dan II+ yaitu Penerapan Kerangka Kerja

Dasar, sementara bagian III berada pada tingkat kematangan keamanan informasi di Pusdatin berada pada Kondisi Awal. Rangkuman evaluasi area keamanan informasi serta radar *chart* tingkat kelengkapan standar SNI ISO/IEC 27001 ditunjukkan pada gambar dibawah ini:



Gambar 8. Diagram radar hasil tingkat kelengkapan area keamanan informasi

Dilihat dari hasil penilaian indeks KAMI (keamanan informasi), dimana tingkat kematangan keamanan informasi berada pada kategori I+ yaitu kondisi awal yang berarti penerapan langkah pengamanan masih bersifat reaktif. Pusdatin memerlukan perbaikan untuk dapat mencapai kematangan minimum III+, agar mampu mendapatkan sertifikasi ISO 27001:2013.

H. Rekomendasi

Rekomendasi yang diberikan didasarkan oleh Standar SNI ISO 27001:2013 dengan melakukan perbandingan. Perbandingan dilakukan dengan melihat kekurangan apa saja yang ada pada setiap area dan membandingkannya dengan kontrol ISO 27001:2013 yang berkaitan dengan area tersebut. Berikut ini adalah tabel rekomendasi dari masing-masing:

Tabel 8. Rekomendasi area tata kelola keamanan informasi

No.	Saat ini	Rekomendasi	Kontrol ISO
1.	Belum ada pendefinisian standar kompetensi dan keahlian SMKI	Membuat dokumen /prosedur standar kompetensi pelaksana	Klausul (6.2) (7.2)
2.	Belum ada jadwal pemantauan rutin perubahan konfigurasi	Pembuatan jadwal pemantauan dokumentasi	A.9.2.3 A.12.1.1
3.	Belum adanya kegiatan analisa	Dilakukannya analisa atau	A.14.1.1 Klausul

No.	Saat ini	Rekomendasi	Kontrol ISO
	rutin atas konfigurasi. Hanya SOP standar	dokumen analisa kepatuhan mengenai keamanan pelaksanaan	9.3

Tabel 9. Rekomendasi area risiko keamanan informasi

No.	Saat ini	Rekomendasi	Kontrol ISO
1.	Dokumen masih dalam proses perencanaan untuk penanggung jawab risiko	Menentukan serta mengalokasikan peran dan tanggung jawab	A.6.1.1
2.	Tidak ada daftar identifikasi dan kepemilikan asset, masih dalam proses perencanaan	Menentukan kontrol pengendalian yang sesuai dengan kepemilikan asset dan penggunaannya	A.8.1.2

Tabel 10. Rekomendasi area kerangka kerja

No.	Saat ini	Rekomendasi	Kontrol ISO
1.	Belum ada kebijakan secara rinci dan menjelaskan tanggung jawab dan wewenang penerapan SMKI	Membuat dokumen kebijakan dan prosedur keamanan informasi.	A.6.1.1 A.6.1.2
2.	Belum mengidentifikasi seluruh peraturan yang menyangkut keamanan informasi	Melakukan pengidentifikasian dan daftar peraturan yang perundangan yang berlaku dan persyaratannya.	A.9.2.3 A.12.1.1
3.	Tidak ada Kegiatan rutin untuk mengevaluasi tingkat kepatuhan keamanan informasi yang sudah ditetapkan	Menetapkan keberlanjutan keamanan informasi.	Kalusul 10.2 A.17.1.3 A.5.1.2

Tabel 11. Rekomendasi area pengelolaan aset keamanan informasi

No.	Saat ini	Rekomendasi	Kontrol ISO
1.	Belum ada	Membuat	A.18.1.2

No.	Saat ini	Rekomendasi	Kontrol ISO
	peraturan pengamanan dan pengamanan asset instansi terkait HAKI	dokumen /prosedur standar kompetensi pelaksana	
2.	Belum adanya peraturan kebijakan penggunaan data pribadi	Membuat peraturan batasan penggunaan data dalam lingkungan pekerjaan	A.9.2.6
3.	Tidak ada prosedur pelaporan insiden terhadap pihak berwajib	Membuat prosedur pelaporan insiden terhadap pihak ke3	A.6.1.3

V. SIMPULAN

Kesimpulan yang dapat diperoleh dari penelitian ini adalah terkait penilaian Tingkat Kematangan atau kesiapan Manajemen Keamanan Informasi pada Pusdatin dengan menggunakan Indeks Keamanan Informasi (KAMI) adalah sebagai berikut:

1. Hasil dari penilaian Tingkat Kepentingan TIK di instansi adalah sebesar 39. Hal ini menunjukkan bahwa institusi Pusdatin termasuk dalam kategori "KRITIS". Dalam penggunaan TIK pada kegiatan operasional instansi merupakan hal yang tidak bisa dipisahkan, artinya semakin tinggi tingkat ketergantungan TIK oleh instansi semakin banyak anacam risiko yang mungkin terjadi dan perlu adanya keamanan informasi yang ekstra.
2. Hasil evaluasi pada 5 area yaitu (Tata Kelola, pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi Informasi) Indeks KAMI diketahui bahwa pusdatin berada pada level atau tingkat kematangan I+, dimana artinya pusdatin

perlu melakukan "Perbaikan" keamanan informasi. Untuk dapat melakukan sertifikasi ISO 27001:2013, minimal level kematangan yang harus dicapai pusdatin adalah level III+.

Berdasarkan hasil yang sudah disebutkan, dalam hal ini instansi belum layak atau "Perlu Perbaikan" untuk dapat melindungi asset yang dimiliki, sehingga instansi masih rentan terhadap tindak kejahatan yang mungkin dapat mengakibatkan terganggunya pelayanan sistem informasi di instansi Pusdatin.

DAFTAR PUSTAKA

- [1] DISKOMINFO. (2017). Panduan Penerapan SMKI Berbasis Indeks KAMI. Panduan Penerapan SMKI, 1.0.
- [2] Permen 15 pasal 1321. (2015, April 21). Peraturan pemerintah kementerian PUPR , 267.
- [3] Hidayat, N. (2014). Kajian Tata Kelola IT Berdasarkan Indeks KAMI pada Universitas Pakuan Bogor. Jurnal Paradigma, 16 (2), 1.
- [4] ISO/IEC 27001. (2013). International Standar ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements.
- [5] PUSDATIN. (2018). Dokumen Sejarah. PUSDATIN, Jakarta.
- [6] Tri Yani Akhirina, S. M. (2016). Evaluasi Keamanan Teknologi Informasi Pada Pt.Indotama Partner Logistics Menggunakan Indeks Keamanan Informasi (KAMI). TEKNOSI, 02, 53.
- [7] Rosmiati, i. R. (2016, februari). Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal dan Operasional Mengkombinasikan Standar ISO 27001:2013 dengan Maturity Level. Seminar Nasional Teknologi Informasi dan Multimedia.
- [8] IBM Certification. (2019). Sumber : www.ibm.com.
- [9] Basyarahil, F. A. (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. Jurnal Teknik ITS, 6.
- [10] DISKOMINFO. (2017). Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi. Panduan Penerapan SMKI, 1.0.