BAB II
TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Studi sebelumnya mengenai perencanan pengelolaan keamanan informasi berbasis ISO 27001 menggunakan Indeks KAMI dilakukan oleh Firdani dan Perdanakusuma [11]. Objek penelitian ini adalah Dinas Kominfo Kabupaten Rembang[11]. Penelitian ini bertujuan untuk merancang pengelolaan keamanan informasi pada Dinas Kominfo Kabupaten Rembang, penelitian ini juga menggunakan Indeks KAMI sebagai metode untuk mengetahui kondisi saat ini keamanan informasi pada Dinas Kominfo Kabupaten Rembang serta mengindetifikasi risiko untuk mengetahui seberapa besar dan risiko apa saja yang diterima oleh Dinas Kominfo Kabupaten Rembang[11]. Temuan dari penelitian tersebut adalah sistem elektronik pada Dinas Kominfo Kabupaten Rembang adalah 25 sehingga berada pada kategori tinggi dengan skor tingkat kelengkapan penerapan standar ISO 27001 sebesar 161 dimana masih menunjukkan posisi area merah sehingga berada pada level “Tidak Layak”. Dari kelima area keamanan informasi, masing masing berada pada level I dan I+ dengan nilai terendah berada pada area pengelolaan risiko dengan skor 17 dan nilai tertinggi pada area teknologi dan keamanan informasi dengan skor 43. Dengan demikian, pada penelitian ini berfokus pada perencanaan pengelolaan keamanan informasi berdasarkan analisis risiko[11].

Mahersmi,dkk [12] melakukan penelitian yang membahas tentang analisis risiko yang bertujuan untuk mengidentifikasi risiko terkait asset teknologi informasi penting organisasi. Penelitian ini menggunakan OCTAVE untuk menganalisis risiko keamanan informasi karena menilai terjadinya risiko dari berbagai perspektif organisasi[12]. Hasil dari penelitian ini adalah identifikasi Potential cause, identifikasi risikko, dan penilaian risiko. Pada tahapan penilaian risiko dilakukan untuk mendeskripsikan informasi secara mendalam terhadap risiko yang telah diidentifikasi yang nantinya akan menghasilkan nilai severity,

Commented [V18]:

Commented [EMSM19]: Jika penulis ada dua, tulis kedua nama belakang penulis.
Jika penulis lebih dari 2 gunakan dkk
Contoh:
2 penulis: Wirayudha dan Haryanto
Lebih dari 2 penulis: Wirayudha, dkk.

Cek untuk semua sitasi!

Commented [V20]:

occurrence, dan detection. Nilai tersebut akan digunakan untuk menghitung RPN (Risk Priority Number) parameter dari level severity, occurrence, dan detection.

Firmana,dkk [13] melakukan penelitian yang membahas penggunaan indeks KAMI sebagai evaluasi keamanan informasi pada PT.PLN DISTRIBUSI JATIM. Dengan menyediakan keamanan yang relevan untuk menjaga keamanan informasi yang telah ditetapkan oleh pemerintah, sehingga perlu adanya evaluasi yang berkaitan dengan keamanan informasi yang sesuai ISO 27001 berupa Indeks Keamanan Informasi (KAMI). Untuk menganalisa seberapa penting tingkat kepentingan penggunaan TIK yang dilakukan oleh PT. PLN Distribusi Jatim yang diharapkan dapat memberikan rekomendasi yang lebih baik lagi untuk menjaga keamanan informasi. Temuan dari penelitian inihasil evaluasi berada pada level I+ dengan total skor 190 dari total keseluruhan skor 588. Level I+ merupakan level yang masuk pada tahapan kondisi awal untuk tingkat kematangan dari total lima level. Tingkat kematangan I+ menunjukkan bahwa empat bentuk pengamanan TKII-Tahap 1 dengan status “Dalam Penerapan/Diterapkan Sebagian” dan sisa jumlah pengamanan TKII-Tahap 1 yang ada dengan status “Sedang Direncanakan”.

Commented [V21]:

Husin,dkk [14] melakukan sebuah penelitian yang membahas implementasi indeks KAMI di Universitas Sam Ratulangi. Sebagai instansi pendidikan haruslah memiliki standar keamanan sehingga penelitian ini berfokus pada evaluasi keamanan informasi di unit kerja Universitas Sam Ratulangi dimana output dari penelitian ini adalah hasil tingkat kematangan keamanan informasi di Universitas Sam Ratulangi dan nantinya dijadikan bahan evaluasi lanjutan untuk meningkatkan keamanan informasi dimasa mendatang[14].

Commented [V22]:

Prasetyowati,dkk[15] dalam penelitian nya yang membahas evaluasi manajemen keamanan informasi menggunakan indeks KAMI berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Layanan Semarang dimana terjadi peretasan pada website PIP Semarang Hal tersebut membuat terjadinya beberapa masalah salah satunya yaitu hilangnya data-data penting dan tampilan website PIP Semarang menjadi berantakan karena diretas oleh pihak yang tidak bertanggung jawab, sehingga pihak unit teknologi informatika harus melakukan input data dari awal. Hasil keseluruhan dari penilaian kelima area dalam Indeks KAMI adalah sebesar

Commented [V23]:

238 dari jumlah total keseluruhan sebesar 645 dan berada pada level I-I+ dimana level ini masih berada pada “ Kondisi Awal ” penerapan keamanan informasi. Berdasarkan penjelasan diatas perbandingan dan ringkasan penelitian sebelumnya dapat dilihat pada Tabel 2.1

Commented [EMSM24]: Penulisan tabel diawali huruf kapital. Tabel 2.1
Cek ejaan!

Commented [EMSM25]: Buat table dalam bentuk landscape uapya lebih mudah dibaca

Tabel 2.2. Tabel Perbandingan

NO	1	2	3	4	5
Peneliti	Anindhita Firdani,Andi Reza Perdanakusuma	Balqis Lembah Mahersmi, dkk.	Roodhin Firmana, dkk.	Muh. Faturachman Husin, dkk.	Desy Dwi Prasetyowati, dkk.
Tahun	2019	2016	2013	2017	2019
Tujuan	Melakukan perencanaan pengelolaan keamanan informasi	Identifikasi risiko pada Dishubkominfo terkait aset teknologi informasi	Melakukan evaluasi keamanan informasi pada PT.PLN Distribusi Jatim	Melakukan evaluasi keamanan informasi pada unit kerja Univeritas Sam Ratulangi.	Melakukan evaluasi manajemen keamanan informasi menggunakan indeks KAMI pada Politeknik Ilmu Layanan (PIP) Semarang

Metode	Analisis deskriptif dengan metode pengumpulan data wawancara dan kuesioner	Analisis deskriptif dengan metode pengumpulan data wawancara	Analisis deskriptif dengan metode pengumpulan data studi lapangan dan literatur	Analisis deskriptif dengan metode pengumpulan data kuesioner	Analisis deskriptif dengan metode pengumpulan data wawancara
Hasil	Sistem elektronik pada dinas kominfo kabupaten rembang adalah 25 sehingga berada pada kategori tinggi dengan skor tingkat kelengkapan penerapan standar ISO 27001 sebesar 161 dimana masih menunjukkan posisi area merah sehingga berada pada level “Tidak Layak” dan memerlukan perencanaan pengelolaan keamanan informasi.	Dari proses identifikasi risiko terhadap layanan teknologi informasi pada Dinas Perhubungan Komunikasi dan Informatika kabupaten Tulungagung diperoleh 13 risiko dan 31 kejadian risiko dengan demikian terdapat risiko yang memiliki kejadian risiko lebih dari satu dikarenakan perbedaan penyebab.	Tingkat kematangan keamanan informasi PT.PLN Distrbusi Jatim serta rekomendasi perbaikan	Tingkat kematangan keamanan informasi Universitas Sam Ratulangi yang nantinya akan menjadi bahan evaluasi lanjutan untuk meningkatkan keamanan informasi dimasa datang.	Tingkat kematangan keamanan informasi PIP Semarang serta saran dan rekomendasi perbaikan

2.2. Dasar Teori

2.2.1. Keamanan Informasi

Keamanan informasi menjadi salah satu usaha yang krusial dalam sebuah organisasi untuk menjaga informasi penting yang dimiliki terhadap risiko-risiko yang berpotensi muncul dan berbahaya bagi organisasi[12]. Terdapat 3 aspek penting dalam sebuah informasi yaitu [11][16]:

1. Kerahasiaan

   Kerahasiaan berari informasi hanya bisa diakses oleh orang yang memiliki wewenang dan menjamin kerahasiaan informasi yan dikirim, diterima, dan disimpan.
2. Keutuhan

   Keutuhan berarti informasi yang ada tidak mengalami pengurangan nilai tanpa ada izin dari pihak yang berwenang atau utuh secara informasi
3. Ketersediaan

   Ketersediaan berarti menjamin pengguna dapat mengakses informasi tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Pengguna dalam hal ini bisa berarti manusia atau system yang mempunyai hak untuk mengakses informasi tersebut

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang berupa kebijakan (*policy*), pedoman kerja (*guidance work* atau SOP), struktur organisasi hingga perangkat lunak Didalam keamanan informasi terdapat berbagai macam risiko yang akan dihadapi baik itu dari berbagai sisi yaitu internal, eksternal, alamiah dan alam seperti bencana alam seperti banjir, kebakaran, dan lain-lain[5][17]. Terdapat banyak hal lain yang mengancam keaman informasi suatu organisasi seperti malware. Malware terdiri atas program-program lengkap atau segmen-segmen kode yang dapat menyerang suatu *system* dan melakukan fungsi-fungsi yang tidak diharapkan oleh pemiliki *system*[18][17].

Commented [V26]:
Commented [V27]:
Commented [V28]:
Commented [V29]:

2.2.2. ISO/IEC 27001

Seri ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality*, *integrity* dan *availability*. Adanya tata kelola data pemerintahan yang efisien, transparan, inovatif dan patisipatif dalam hal ini keamanan data dan informasi akan memiliki peran penting dalam mewujudkan penyelenggaraan pemerintahan yang baik dan bersih. Oleh karena itu kemampuan untuk menyediakan informasi secara cepat dan akurat merupakan hal yang esensial[17]. ISO/IEC 27001 adalah *framework* yang menyediakan panduan dalam penerapan SMKI dan memberikan sertifikat internasional melalui pihak ketiga untuk memastikan bahwa control keamanan informasi beroperasi telah sesuai dengan kriteria standar keamanan informasi (ISO/IEC 27001:2013). SMKI memiliki lingkup pada semua bagian struktur organisasi, tanggung jawab, kegiatan perencanaan, kebijakan, proses, prosedur, praktik dan sumber daya[19][6]. Pada standar ISO/IEC 27001 ini memiliki 7 *mandatory* klausul yaitu [20]:

Commented [V30]:
Commented [V31]:
Commented [V32]:
Commented [V33]:
Commented [V34]:

1. Klausul 4 konteks Organisasi
2. Klausul 5 Kepemimpinan
3. Klausul 6 Perencanaan
4. Klausul 7 Pendukung
5. Klausul 8 Operasi
6. Klausul 9 Evaluasi Kinerja
7. Klausul 10 Peningkatan

Dalam ISO/IEC 27001:2013 terdiri dari 114 kontrol yang terbagi menjadi 14 domain antara lain[21] :

A.5 Kebijakan keamanan informasi - kontrol tentang bagaimana kebijakan ditulis dan ditinjau

A.6 Organisasi keamanan informasi - kontrol tentang bagaimana tanggung jawab diberikan; juga mencakup kontrol untuk perangkat seluler dan teleworking

A.7 Keamanan sumber daya manusia - kontrol sebelum bekerja, selama, dan setelah bekerja

A.8 Manajemen aset - pengendalian yang berkaitan dengan inventaris aset dan penggunaan yang dapat diterima; juga untuk klasifikasi informasi dan penanganan media

A.9 Kontrol akses - kontrol untuk pengelolaan hak akses pengguna, sistem dan aplikasi, dan untuk pengelolaan tanggung jawab pengguna

A.10 Kriptografi - kendali yang terkait dengan enkripsi dan manajemen kunci

A.11 Keamanan fisik dan lingkungan - kendali yang menentukan area aman, kendali masuk, perlindungan terhadap ancaman, keamanan peralatan, pembuangan yang aman, Kebijakan Meja Jernih dan Layar Jernih, dll.

A.12 Keamanan operasional - banyak kontrol yang terkait dengan manajemen produksi TI: manajemen perubahan, manajemen kapasitas, malware, backup, logging, pemantauan, instalasi, kerentanan, dll.

A.13 Keamanan komunikasi - kontrol yang terkait dengan keamanan jaringan, pemisahan, layanan jaringan, transfer informasi, perpesanan, dll.

A.14 Akuisisi, pengembangan dan pemeliharaan sistem - kontrol yang menentukan persyaratan keamanan, dan keamanan dalam proses pengembangan dan dukungan

A.15 Hubungan pemasok - kontrol tentang apa yang harus disertakan dalam perjanjian, dan cara memantau pemasok

A.16 Manajemen insiden keamanan informasi - pengendalian untuk melaporkan kejadian dan kelemahan, mendefinisikan tanggung jawab, prosedur respons, dan pengumpulan bukti

A.17 Aspek keamanan informasi dari manajemen kelangsungan bisnis - pengendalian yang memerlukan perencanaan kelangsungan bisnis, prosedur, verifikasi dan peninjauan, dan redundansi TI

A.18 Kepatuhan - kontrol yang memerlukan identifikasi hukum dan peraturan yang berlaku, perlindungan kekayaan intelektual, perlindungan data pribadi, dan tinjauan keamanan informasi

2.2.3. Indeks KAMI

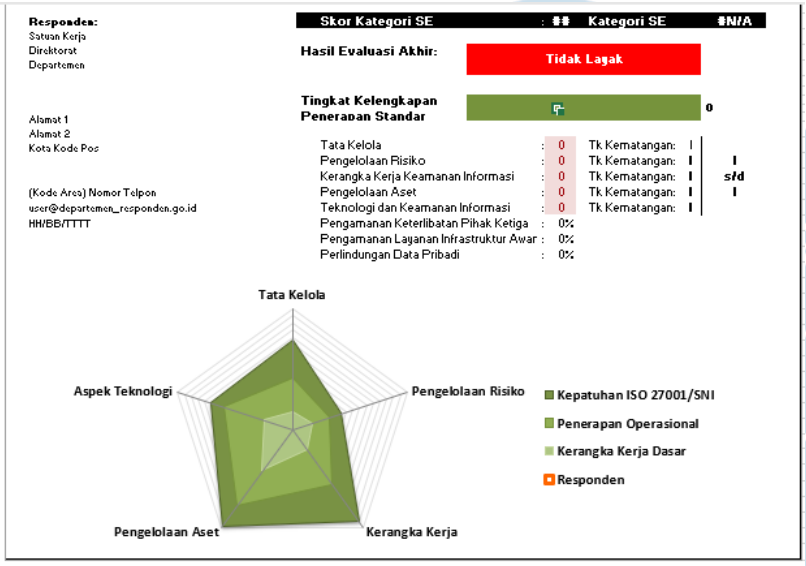
Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Aspek Teknologi dengan suplemen Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan dan Perlindungan Data Pribadi. Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi.

Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2013, yang disusun kembali menjadi 5 (lima) area di bawah ini[22]:

Commented [V35]:

- Tata Kelola Keamanan Informasi – Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
- Pengelolaan Risiko Keamanan Informasi – Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
- Kerangka Kerja Keamanan Informasi – Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
- Pengelolaan Aset Informasi – Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
- Teknologi dan Keamanan Informasi – Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Sebagai gambaran hasil evaluasi dapat dilihat pada Gambar 2.2.



Gambar 2.1. Dashboard Hasil Evaluasi Indeks KAMI

Sebelum dilakukan penilaian secara menyeluruh maka dilakukan proses klasifikasi terlebih dahulu terhadap kategori Sistem Elektronik. Hal ini bertujuan untuk mengelompokkan instansi kedalam ukuran tertentu pada Tabel 2.2.

Commented [V36]:

Tabel 2.2. Nilai kategori Sistem Elektronik.

Batas Bawah	Batas Atas	Klasifikasi
10	15	Rendah
16	34	Tinggi
35	50	Strategis

Jika skor yang didapatkan oleh instansi kisaran 10 sampai 15 akan masuk pada kategori “Rendah” yang berarti penggunaan TIK mendukung proses kerja yang berjalan, walaupun tidak pada tingkatan yang signifikan. Jika mendapatkan

Commented [V37]:

skor kisaran 16 sampai 34 maka instansi tergolong pada kategori “Tinggi” yang berarti TIK merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan. Jika mendapatkan skor kisaran 35 sampai 50 instansi akan termasuk pada kategori “Strategis” dimana penggunaan TIK merupakan satu-satunya cara untuk menjalankan proses kerja yang bersifat strategis atau berskala nasional.

Pada penilaian kategori Sistem Elektronik terdapat uraian secara rinci kaitan nilai kategori sistem elektronik pada Tabel 2.2 dengan tingkat kelengkapan dan keamanan informasi yang bisa dilihat pada Tabel 2.3.

Commented [V38]:

Tabel 2.3. Kaitan Sistem Elektronik dan status kesiapan indeks KAMI 4.1

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

Pada penilaian kelima area keamanan informasi memiliki nilai skor berbeda. Pada Tabel 2.4 berikut adalah pemetaan skor indeks KAMI berdasarkan masing masing kategori:

Tabel 2.4. Matriks Bobot Penilaian Status Penerapan.

	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

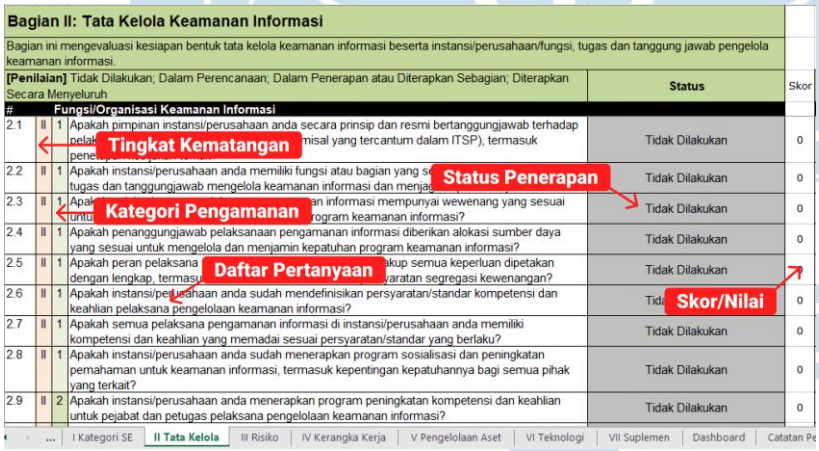
Berikut pada Tabel 2.5 merupakan cuplikan tampilan Kategori Sistem Elektronik pada Indeks KAMI

Tabel 2.5. Cuplikan Kategori Sistem Elektronik pada Indeks KAMI

Bagian I: Kategori Sistem Elektronik		
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	C
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	C

Pada Tabel 2.5 di atas, memiliki Status Penilaian A, B, dan C dengan bobot nilainya masing-masing. A memiliki nilai 5, B memiliki nilai 2, sedangkan C memiliki nilai 1. Setelah pengisian pada semua poin pertanyaan, nilai akan dijumlahkan secara keseluruhan sehingga memperoleh tingkat keterkaitan instansi terhadap sistem elektronik. Untuk kategori tingkat keterkaitan dapat dilihat secara detail pada Tabel 2.3.

Pada masing-masing area, penilaian dengan Indeks KAMI memuat hal yang berguna untuk tercapainya tujuan pada setiap area pengamanan yang ada. Untuk melakukan sertifikasi standar SNI ISO/IEC 27001 : 2013, diperlukan pemenuhan persyaratan minimum dari pengamanan Indeks KAMI. Di bawah ini Gambar 2.2 merupakan contoh tampilan pertanyaan di area Tata Kelola Keamanan Informasi dalam Indeks KAMI.



Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

#			[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	Status	Skor
			Fungsi/Organisasi Keamanan Informasi		
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelak… misal yang tercantum dalam ITSP), termasuk pene…	Tidak Dilakukan	0
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang s… tugas dan tanggungjawab mengelola keamanan informasi dan menja…	Tidak Dilakukan	0
2.3	II	1	Apak… an informasi mempunyai wewenang yang sesuai untu… rogram keamanan informasi?	Tidak Dilakukan	0
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	0
2.5	II	1	Apakah peran pelaksana … akup semua keperluan dipetakan dengan lengkap, termasu… yaratan segregasi kewenangan?	Tidak Dilakukan	0
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tida…	0
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan	0
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan	0
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0

… | I Kategori SE | II Tata Kelola | III Risiko | IV Kerangka Kerja | V Pengelolaan Aset | VI Teknologi | VII Suplemen | Dashboard | Catatan Pe

Gambar 2.2. Cuplikan pertanyaan Area Tata Kelola Keamanan Informasi

Di setiap pilihan jawaban memiliki bobot penilaiannya masing-masing. Berikut pada Tabel 2.4 pemetaan skor untuk penilaian Status Penerapan instansi yang digunakan pada pertanyaan di seluruh bagian atau area.

Adapun untuk keperluan Indeks KAMI tingkat kematangan keamanan informasi tersebut didefinisikan sebagai berikut:

Commented [V39]:

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

Untuk membantu memberikan uraian yang lebih detail ditambahkan tingkatan antara I+,I I+, III+, dan IV+. Sehingga keseluruhan ada 9 tingkatan kematangan.Tingkat kematangan keamanan informasi yang diharapkan adalah III+.