



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB II

LANDASAN TEORI

2.1. 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. Teknologi 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 (Tri Yani Akhirina¹, 2016).

2.2. Keamanan Informasi

Keamanan informasi berkaitan dengan perlindungan aset berharga terhadap kehilangan, pengungkapan penyalahgunaan, atau kerusakan. Dalam konteks ini, "aset berharga" adalah informasi yang direkam, diproses, disimpan, dikirim atau diambil baik dari media elektronik atau non elektronik. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang

didapat dari investasi dan kesempatan bisnis. Menurut (Rosmiati, 2016), 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. 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 2.1** dibawah ini:



Gambar 2.1 Aspek Keamanan Informasi
Sumber : www.ibm.com (2018)

1. **Confidentiality** adalah keamanan informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu. *Confidentiality* adalah bahwa informasi tidak tersedia atau diungkapkan kepada

individu, entitas, atau proses yang tidak sah. Misalnya pengungkapan informasi pada pihak tidak berhak secara lisan, surat elektronik, menyalin, mencetak dokumen, dan sebagainya. Kita tahu bahwa informasi adalah sebuah kekuatan, dan di era informasi ini, akses menuju sebuah informasi menjadi lebih penting lagi. Akses tidak berwenang yang terjadi pada informasi yang rahasia (*confidential*) dapat memiliki konsekuensi yang sangat serius, tidak hanya pada aplikasi keamanan nasional, tapi juga berlaku pada industri/pabrik dan komersial. Terdapat beberapa cara mekanisme proteksi '*confidentiality*' untuk sistem informasi, antara lain adalah teknik kriptografi dan control akses. Maka ancaman-ancaman seperti *malware*, *intruders*, jaringan yang tak aman, dan sistem administrasi yang lemah dapat diatasi.

2. ***Integrity*** adalah keamanan informasi seharusnya menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan atau ancaman lain yang menyebabkan berubahnya informasi dari aslinya. *Integrity* adalah tindakan menjaga keakuratan dan kelengkapan asset. Integritas suatu data bukan hanya benar, tetapi juga terpercaya. Sebagai contoh, jika sebuah informasi disalin ke dalam USB atau mengupload ke email, maka informasi tersebut bukan hanya tidak rahasia lagi, tetapi telah diragukan integritasnya. Sebab, jika sebuah file/data telah digandakan, maka akan terbuka kemungkinan risiko untuk diubah atau mengalami modifikasi. Terdapat beberapa mekanisme proteksi pada '*Integrity*', yang dibagi menjadi dalam 2 kelompok, yaitu mekanisme pencegahan, seperti kontrol akses yang mencegah pemodifikasian informasi yang tak berwenang,

selain itu ada teknik pendeteksian, dimana diadakan sebuah pendeteksian pemodifikasian informasi yang tak berwenang setelah mekanisme pencegahan gagal dilakukan. Control yang menjaga ‘*integrity*’ termasuk prinsip antara lain *privilege* (hak), *separation* (pemisahan), dan *rotation* (perotasian) dalam pekerjaan.

3. **Availability** adalah keamanan informasi seharusnya menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Ketersediaan dapat diukur dengan sebagai contoh adalah dalam konteks bisnis memiliki web portal yang aman melawan serangan *Denial of Service* (DOS) atau bila ketersediaan infrastruktur komputer tidak dapat diyakini bekerja pada sistem organisasi, hal ini menyebabkan proses atau orang-orang tidak dapat bekerja pada saat itu. Jadi, *availability* juga merupakan hal yang penting disamping *confidentiality* dan *integrity*. Ancaman terhadap *availability* dikenal sebagai *denial of service* atau disingkat DoS. Musibah yang terjadi natural dan dibuat oleh manusia bisa mempengaruhi availabilitas. Maka, *disaster recovery* planning itu dibutuhkan untuk meminimalisir kehancuran/kehilangan data

2.3. Tata Kelola Keamanan Sistem Informasi

Pengertian tata kelola TI yaitu mencakup Sistem Informasi (SI), teknologi dan komunikasi, bisnis dan hukum serta isu-isu lain yang melibatkan hampir seluruh pemangku kepentingan (*stakeholder*), baik direktur, manajemen eksekutif, pemilik proses, supplier, pengguna TI bahkan pengaudit SI/TI. Pembentukan dan penyusunan tata kelola merupakan tanggung jawab dari jajaran direksi dan

manajemen eksekutif. (Sarno, 2009). Beberapa pengertian juga didapatkan untuk pengertian tata kelola ini, menurut (Surendro, 2009) Tata kelola TI merupakan bagian terintegrasi dari pengelolaan perusahaan yang memastikan bahwa teknologi informasi perusahaan dapat digunakan untuk mempertahankan dan memperluas strategi dan tujuan organisasi.

Dan menurut Sarno, fokus utama tata kelola TI dapat dibagi menjadi lima area yaitu:

1. *Penyelarasan Strategi (Strategic Alignment)*

Memfokuskan kepastian terhadap keterkaitan antara strategi bisnis dan TI serta penyelarasan antara operasional TI dengan bisnis.

2. *Penyampaian nilai (Value delivery)*

terkait dengan penyampaian nilai yang memastikan bahwa TI memenuhi manfaat yang dijanjikan dengan memfokuskan pada pengoptimalan biaya dan pembuktian nilai akan keberadaan TI.

3. *Pengelolaan sumber daya (Resource management)*

Berkaitan dengan pengoptimalan investasi yang dilakukan dan pengelolaan secara tepat dari sumber daya TI yang kritis mencakup: aplikasi, informasi, infrastruktur, dan sumber daya manusia (SDM). Isu kunci area ini berhubungan dengan pengoptimalan pengetahuan dan infrastruktur.

4. *Pengelolaan risiko (Risk management)*

Membutuhkan kepekaan akan risiko oleh manajemen senior, pemahaman yang jelas akan perhatian perusahaan terhadap keberadaan risiko,

pemahaman kebutuhan akan kepatutan, transparansi akan risiko yang signifikan terhadap proses bisnis perusahaan dan tanggung jawab pengelolaan risiko ke dalam perusahaan itu sendiri.

5. Pengukuran kinerja (*Performance measurement*)

Penelusuran dan pengawasan implementasi dari strategi, pemenuhan proyek yang berjalan, penggunaan sumber daya, kinerja proses dan penyampaian layanan dengan menggunakan kerangka kerja seperti *Balanced Scorecard* yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan terukur dibandingkan dengan akuntansi konvensional. Dan berbagai kerangka kerja tata kelola TI yang tersedia dan sudah dibakukan serta diakui oleh seluruh dunia yaitu, *Information Technology Infrastructure*.

2.4. Indeks KAMI

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, juga 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.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun

tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan *snapshot* indeks kesiapan- dari aspek kelengkapan maupun kematangan- kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembandingan dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya. Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (*stakeholders*). Khusus untuk Instansi Pemerintah, penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Pertukaran informasi dan diskusi dengan Instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari *lesson learned* yang sudah dilalui (Panduan Penerapan SMKI Berbasis Indeks KAMI, 2017; Panduan Penerapan SMKI Berbasis Indeks KAMI, 2017).

2.5. Metode Penilaian Indeks KAMI

Penilaian menggunakan metode ini untuk melakukan siklus *Act* yaitu melaksanakan *self-assessment* berdasarkan indeks KAMI. Penilaian dalam Indeks KAMI (Keamanan Informasi) dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001 (KEMINFO, 2012)

Menurut (Panduan Penerapan SMKI Berbasis Indeks KAMI, 2017), Alat evaluasi Indeks KAMI ini dapat digunakan oleh organisasi dengan skala nasional, maupun yang berukuran kecil. Penggunaan di Instansi pemerintah dapat dilakukan di tingkat pusat maupun satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijelankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggungjawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Proses evaluasi dilakukan melalui sejumlah pertanyaan di masingmasing area di bawah ini:

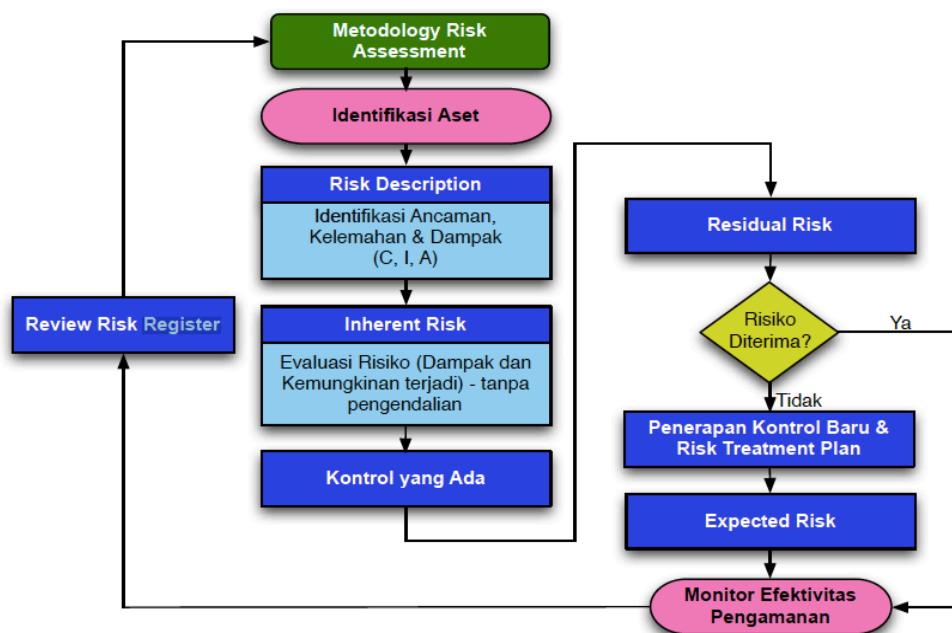
a. Tata Kelola Keamanan Informasi

Area tata kelola merupakan rangkuman penerapan kontrol yang ada pada KMK 479 tahun 2010 yaitu; sasaran pengendalian umum, organisasi, keamanan informasi dalam pengelolaan kelangsungan usaha dan kepatuhan. Penerapan kontrol dalam area ini meliputi kebijakan formal yang mendefinisikan peran, tanggung-jawab, kewenangan pengelolaan keamanan informasi, dari pimpinan unit kerja sampai ke pelaksana operasional. Termasuk dalam area ini juga adalah adanya program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.

b. Pengelolaan Risiko Keamanan Informasi

Area pengelolaan risiko merupakan rangkuman penerapan kontrol yang ada pada KMK 479 tahun 2010 yaitu; sasaran pengendalian organisasi, pengelolaan aset informasi, keamanan informasi dalam pengelolaan kelangsungan

usaha dan kepatuhan. Bentuk penerapan kontrol pada area pengelolaan risiko keamanan informasi ini sejalandengan strategi penerapan manajemen risiko yang terdapat pada Peraturan Menteri Keuangan Nomor: 191/PMK.01/2008 tentang, penerapan Manajemen Risiko di Lingkungan Departemen Keuangan. Salah satu strateginya adalah memastikan bahwa seluruh risiko telah teridentifikasi dan terdapat mitigasi yang terencana dan terukur untuk menjaga agar risiko tersebut berada pada tingkat yang sesuai dengan toleransi yang telah ditetapkan. Adapun proses pengelolaan risiko keamanan informasi dapat dilihat pada **Gambar 2.2** berikut:



Gambar 2.2 Proses Pengelolaan Risiko Keamanan Informasi
Sumber : Risk Management ISMS (2013)

1. *Methodology risk assessment* merupakan metode penilaian risiko asset informasi berdasarkan dampak dan kemungkinan terjadi risiko terhadap asset informasi.
2. Identifikasi aset merupakan proses mengidentifikasi, klasifikasi dan

membuat profil aset informasi.

3. *Risk description* merupakan proses mengidentifikasi acaman, kelemahan dan dampak terhadap kerahasiaan, integritas dan ketersediaan aset informasi.
4. *Inherent risk* merupakan proses mengevaluasi risikoterkait dampak dan kemungkinan terjadi pada aset informasi tanpa penerapan pengendalian.
5. Kontrol yang ada merupakan pengendalian yang diterapkan organisasi.
6. *Residual risk* adalah sisa risiko yang dihasilkan oleh adanya penerapan kontrol.
7. Penerapan kontrol baru dan *risk treatment plan* merupakan tindak lanjut dari risiko yang melebihi ambang batas dan opsi penanganan risiko yang terbaik yang dilanjutkan dengan pengembangan rencana mitigasi risiko.
8. *Expected risk* merupakan nilai risiko yang diharapkan dengan penerapan kontrol baru dan risk treatment plan.
9. Monitoring efektivitas pengamanan merupakan proses memantau efektivitas pengaman yang diterapkan.
10. *Review risk register* merupakan proses menelaah dan mengkaji pengelolaan risiko.

c. Kerangka Kerja Keamanan Informasi

Area kerangka kerja merupakan rangkuman penerapan kontrol yang ada pada KMK 479 tahun 2010 yaitu; sasaran pengendalian umum, organisasi, keamanan sumber daya manusia, pengelolaan komunikasi dan operasional, pengelolaan gangguan keamanan informasi, keamanan informasi dalam

pengelolaan kelangsungan usaha dan kepatuhan. Kelengkapan kontrol di area ini adalah kebijakan dan prosedur kerja operasional, kompetensi sumber daya manusia, termasuk strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikan.

d. Pengelolaan Aset Informasi

Area pengelolaan aset informasi merupakan rangkuman penerapan kontrol yang ada pada KMK 479 tahun 2010 yaitu; sasaran pengendalian pengelolaan aset informasi, keamanan sumber daya manusia, keamanan fisik dan lingkungan, pengendalian akses, dan keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi. Kontrol yang diperlukan dalam area ini adalah bentuk pengamanan terkait keberadaan aset informasi, termasuk keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.

e. Teknologi dan Keamanan Informasi

Area teknologi dan keamanan informasi merupakan rangkuman penerapan kontrol yang ada pada KMK 479 tahun 2010 yaitu; sasaran pengendalian akses, keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi, pengelolaan gangguan keamanan informasi, keamanan informasi dalam pengelolaan kelangsungan usaha dan kepatuhan.

2.5.1. Proses Penilaian Kelengkapan dan Kematangan Tata Kelola Keamanan Informasi

Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan

kondisi penerapan keamanan informasi sesungguhnya. Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan Sistem Elektronik yang digunakan instansi ke “tingkat” tertentu: Rendah, Tinggi dan Strategis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik Sistem Elektronik yang sama. Pertanyaan dikelompokkan untuk 2 keperluan.

a. Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013.

Pengelompokan kedua dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh keangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga. Untuk keperluan Indeks KAMI. Pemetaan dan pemeringkatan akan dilakukan Tim yang ditetapkan Kementerian Komunikasi dan Informatika (Kominfo) dan menjadi dasar bagi pemberian OPINI Kominfo tentang kondisi tata kelola keamanan informasi di Kementerian/Lembaga terkait.

Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai berikut:

Tingkat 0 – Tidak Diketahui (PASIF)

- Status kesiapan keamanan informasi tidak diketahui
- Pihak yang terlibat tidak mengikuti atau tidak melaporkan pemeringkatan Indeks KAMI.

Tingkat I - Kondisi Awal (REAKTIF)

- Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.
- Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
 - o Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik.
 - o Pihak yang terlibat tidak menyadari tanggung jawab mereka.

Tingkat II – Penerapan Kerangka Kerja Dasar (AKTIF)

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
- Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
- Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya.
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan

tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.

- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
- Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.

Tingkat III – Terdefinisi dan Konsisten (PRO AKTIF)

- Bentuk pengamanan yang baku sudah diterapkan secara konsisten dan terdokumentasi secara resmi.
- Efektivitas pengamanan dievaluasi secara berkala, walaupun belum melalui proses yang terstruktur.
- Pihak pelaksana dan pimpinan secara umum dapat menangani permasalahan terkait pengelolaan keamanan pengendalian dengan tepat, akan tetapi beberapa kelemahan dalam sistem manajemen masih ditemukan sehingga dapat mengakibatkan dampak yang signifikan.
- Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar atau persyaratan hukum yang terkait.
- Secara umum semua pihak yang terlibat menyadari tanggungjawab mereka dalam pengamanan informasi.

Tingkat IV – Terkelola dan Terukur (TERKENDALI)

- Pengamanan diterapkan secara efektif sesuai dengan strategi manajemen risiko.
- Evaluasi (pengukuran) pencapaian sasaran pengaman dilakukan secara

rutin, formal dan terdokumentasi.

- Penerapan pengamanan teknis secara konsisten dievaluasi efektivitasnya.
- Kelemahan manajemen pengamanan teridentifikasi dengan baik dan secara konsisten ditindaklanjuti pembenahannya.
- Manajemen pengamanan bersifat pro-aktif dan menerapkan pembenahan untuk mencapai bentuk pengelolaan yang efisien.
- Insiden dan ketidakpatuhan (*non-conformity*) diselesaikan melalui proses formal dengan pembelajaran akar permasalahan.
- Karyawan merupakan bagian yang tidak terpisahkan dari pelaksana pengamanan informasi.

Tingkat V – Optimal (OPTIMAL)

- Pengamanan menyeluruh diterapkan secara berkelanjutan dan efektif melalui program pengelolaan risiko yang terstruktur.
- Pengamanan informasi dan manajemen risiko sudah terintegrasi dengan tugas pokok instansi.
- Kinerja pengamanan dievaluasi secara terus menerus, dengan analisis parameter efektivitas kontrol, kajian akar permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja.
- Target pencapaian program pengamanan informasi selalu dipantau, dievaluasi dan diperbaiki.
- Karyawan secara proaktif terlibat dalam peningkatan efektivitas pengamanan.

(KOMINFO, 2011)

2.5.2. Petunjuk Penggunaan Alat Evaluasi Indeks KAMI

KAMI adalah perangkat untuk mengevaluasi penerapan tata kelola keamanan informasi yang dilakukan secara berkelanjutan, dan digunakan untuk memberikan gambaran kemajuan hasil penerapan secara berkala. Apabila terjadi perubahan pada infrastruktur atau unit kerja yang ada dalam lingkup awal evaluasi Indeks KAMI, pengkajian ulang bermanfaat untuk memastikan kelengkapan dan kematangan bentuk tata kelola yang diterapkan di awal. Untuk proyek pengadaan sistem aplikasi berskala besar dan strategis, Indeks KAMI dapat juga difungsikan sebagai *checklist* penerapan tata kelola bagi pengamanan sistem tersebut (KOMINFO, 2011).

Proses penilaian indeks KAMI (Keamanan Informasi) dilakukan dengan langkah-langkah sebagai berikut ini.

1. Ruang Lingkup

Langkah pertama yang harus dilakukan adalah mendefinisikan ruang lingkup penilaian. Ruang lingkup dapat dipilih sesuai dengan kepentingan penilaian Indeks KAMI, dan dapat dipilih sebagai suatu satuan kerja (di tingkat apapun) ataupun suatu sistem informasi. Di bawah ini diuraikan beberapa (contoh: Pusat Data dan Informasi

Kementerian X. Termasuk infrastruktur *Data Centre* dengan cakupan lokasi kerja di Jakarta (dan daerah lain). Penjelasan ruang lingkup (termasuk batasannya) sangat penting untuk dijabarkan secara lengkap dan jelas.

2. Peran dan Tingkat Ketergantungan TIK

Sebelum proses penilaian dilakukan secara kuantitatif, proses klasifikasi dilakukan terlebih dahulu terhadap sistem elektronik dalam instansi atau cakupan evaluasinya. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Strategis, Tinggi, dan Rendah. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik kepentingan TIK yang sama. Peran TIK dievaluasi dengan bahasan:

- Total anggaran tahunan yang dialokasikan untuk TIK
- Jumlah staf atau pengguna dalam instansi yang menggunakan infrastruktur TIK
- Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi instansi anda
- Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh instansi anda
- Dampak dari kegagalan sistem TIK utama yang digunakan instansi anda
- Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja instansi anda
- Dampak dari kegagalan sistem TIK instansi anda terhadap kinerja instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional
- Tingkat sensitifitas pengguna sistem TIK di instansi anda

- Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya
- Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK instansi anda
- Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK
- Tingkat klasifikasi/kekritisian sistem TIK di instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi
- Kategori Peran TIK dapat dijelaskan secara umum sebagai berikut ini :

| Peran TIK | |
|------------------|----|
| Rendah | |
| 0 | 12 |
| Sedang | |
| 13 | 24 |
| Tinggi | |
| 25 | 36 |
| Kritis | |
| 37 | 48 |

Gambar 2.3 Pemetaan Skor Peran Teknologi Informasi dan Komunikasi
Sumber : Indeks KAMI

Gambar 2.3 menjelaskan menjelaskan ketegori Peran TIK yang dimaksud disini secara umum dapat dijelaskan sebagai berikut ini:

- Minim

Penggunaan TIK dalam lingkup yang didefinisikan tidak signifikan, dan keberadaannya tidak berpengaruh proses kerja yang berjalan.

- Rendah

Penggunaan TIK mendukung proses kerja yang berjalan, walaupun tidak pada tingkatan yang signifikan.

- Sedang

Penggunaan TIK merupakan bagian dari proses kerja yang berjalan, akan tetapi ketergantungannya masih terbatas.

- Tinggi

TIK merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan.

- Kritis

Penggunaan TIK merupakan satu-satunya cara untuk menjalankan proses kerja yang bersifat strategis atau berskala nasional.

| Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi | | | | | |
|---|---|-------|---|--|--|
| Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda. | | | | | |
| [Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis | Status | Skor | | | |
| # | Karakteristik Instansi | | | | |
| 1.1 | Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis | | | | |
| 1.2 | Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis | | | | |
| 1.3 | Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi | Minim | 0 | | |
| 1.4 | Nilai kekayaan intelektual yang dimiliki dan dihasikan oleh Instansi anda | Minim | 0 | | |
| 1.5 | Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda | Minim | 0 | | |
| 1.6 | Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda | Minim | 0 | | |

Minim: hanya digunakan untuk mempermudah sejumlah kecil pekerjaan rutin, pencatatan, penyimpanan salinan dokumen, dll
Rendah: digunakan untuk menunjang kegiatan rutin
Sedang: digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi
Tinggi: digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi
Kritis: digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi yang bersifat nasional dan strategis

Gambar 2.4 Tampilan Evaluasi Peran TIK
 Sumber : Indeks KAMI

Gambar 2.4 merupakan perhitungan Peran Teknologi dan Komunikasi (TIK) dengan indeks KAMI (Keamanan Informasi) menggunakan skor untuk setiap pilihan jawaban kuesioner. Pemertan skor untuk Peran Teknologi Informasi dan Komunikasi (TIK) adalah sebagai berikut :

- Skor pilihan jawaban Minum adalah 0
- Skor pilihan jawaban Rendah adalah 1
- Skor pilihan jawaban sedang adalah 2
- Skor pilihan jawaban Tinggi adalah 3
- Skor pilihan jawaban Kritis adalah 4

2.5.3. Penilaian V (Lima) Arena Tingkat Kelengkapan Keamanan Informasi

Dalam pengelompokan ini responden diminta untuk memberi tanggapan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan diberi label “1”), untuk efektifitas dan konsistensi penerapannya dikategorikan (label “2”), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi dikategorikan (label “3”). Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyarkan oleh proses sertifikasi standar ISO/IEC 27001:2013. Setiap jawaban diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka indeks sekaligus digunakan untuk menampilkan hasil evaluasi dalam *dashboard* di akhir proses ini. Skor yang diberikan untuk jawaban pertanyaan sesuai tingkat kematangannya mengacu kepada:

| Status Pengamanan | Kategori 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 |

Gambar 2.5 Pemetaan Skor Kategori Pengamanan Indeks KAMI
Sumber : Indeks KAMI

Gambar 2.5 di atas merangkum seluruh jumlah jawaban penilaian mandiri dan bentuk matriks antara status pengamanan dan kategori. (Catatan: untuk keseluruhan area pengamanan, pengisian pertanyaan dengan label “3” hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan label “1” dan “2” sudah diisi dengan status minimal “Diterapkan Sebagian”). Hasil dari penjumlahan skor untuk masing-masing area ditampilkan dalam diagram radar dengan latar belakang area untuk tingkat maksimal kematangan 1 s/d 3.

| Bagian II: Tata Kelola Keamanan Informasi | | |
|--|---|-----------------|
| Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. | | |
| [Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh | | Status |
| # | Fungsi/Instansi Keamanan Informasi | |
| 2.1 | 1 Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi termasuk penetapan kebijakan terkait? | Tidak Dilakukan |
| 2.2 | 1 Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya? | Tidak Dilakukan |
| 2.3 | 1 Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi? | Tidak Dilakukan |
| 2.4 | 1 Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi? | Tidak Dilakukan |
| 2.5 | 1 Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan? | Tidak Dilakukan |
| 2.6 | 1 Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi? | Tidak Dilakukan |
| 2.7 | 1 Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku? | Tidak Dilakukan |
| 2.8 | 1 Apakah organisasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait? | Tidak Dilakukan |
| 2.9 | 2 Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi? | Tidak Dilakukan |
| 2.10 | 2 Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasi persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada? | Tidak Dilakukan |

Gambar 2.6 Evaluasi Kematangan Pengamanan Indeks KAMI

Sumber : Indeks KAMI

Penjelasan mengenai Ilustrasi **Gambar 2.6** tertera dibawah ini :

- (1) Kolom yang menunjukkan kategori kematangan terkait pertanyaan yang dibahas;
- (2) Kolom yang menunjukkan kategori tahap penerapan
- (3) Daftar pertanyaan
- (4) Pilihan jawaban

Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi SESUNGGUHNYA. Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran. Pada saat responden menjawab setiap pertanyaan dengan pilihan status penerapan seperti gambar diatas, setiap jawaban akan diberikan skor yang nilainya disesuaikan dengan tahapan penerapan (ketegori) bentuk pengamanan. Untuk tahapan awal nilainya lebih rendah dibandingkan tahapan berikutnya. Demikian halnya untuk status penerapannya, penerapan yang sudah berjalan secara menyeluruh memberikan nilai yang lebih tinggi dibandingkan bentuk penerapan lainnya (KEMINFO, 2012).

2.5.4. Penilaian Kelengkapan Keamanan Informasi Indeks KAMI

Penilaian kelengkapan kontrol menggunakan sejumlah aturan sesuai skala yang diberlakukan. Keseluruhan (rangkuman) penilaian, baik untuk aspek kelengkapan maupun kematangan dapat dilihat pada Gambar di bawah ini.

| | Tata Kelola | Manajemen Risiko | Kerangka Kerja | Pengelolaan Aset | Teknologi | |
|--|-------------|------------------|----------------|------------------|------------|--------------|
| Jumlah pertanyaan Tahap 1 | 8 | 9 | 11 | 21 | 13 | |
| Jumlah pertanyaan Tahap 2 | 6 | 4 | 8 | 9 | 10 | |
| Jumlah pertanyaan Tahap 3 | 6 | 2 | 7 | 4 | 1 | |
| Total jumlah pertanyaan | 20 | 15 | 26 | 34 | 24 | (119) |
| Jumlah skor maksimal | 114 | 69 | 144 | 153 | 108 | (588) |
| Batas Skor Min untuk Skor Tahap Penerapan 3* | 40 | 34 | 54 | 78 | 66 | |
| Jumlah Pertanyaan Tk Kematangan II | 11 | 9 | 10 | 26 | 13 | |
| <i>Jumlah pertanyaan Tahap 1</i> | 8 | 9 | 8 | 21 | 13 | |
| <i>Jumlah pertanyaan Tahap 2</i> | 3 | 0 | 2 | 5 | 0 | |
| Jumlah Pertanyaan Tk Kematangan III | 3 | 2 | 11 | 8 | 10 | |
| <i>Jumlah pertanyaan Tahap 1</i> | 0 | 0 | 3 | 0 | 0 | |
| <i>Jumlah pertanyaan Tahap 2</i> | 3 | 2 | 6 | 4 | 10 | |
| <i>Jumlah pertanyaan Tahap 3</i> | 0 | 0 | 2 | 4 | 0 | |
| Jumlah Pertanyaan Tk Kematangan IV | 6 | 2 | 3 | 0 | 1 | |
| <i>Jumlah pertanyaan Tahap 2</i> | 0 | 0 | 0 | 0 | 0 | |
| <i>Jumlah pertanyaan Tahap 3</i> | 6 | 2 | 3 | 0 | 1 | |
| Jumlah Pertanyaan Tk Kematangan V | 0 | 2 | 2 | 0 | 0 | |
| <i>Jumlah pertanyaan Tahap 3</i> | 0 | 2 | 2 | 0 | 0 | |

Gambar 2.7 Jumlah Pertanyaan dalam Indeks KAMI
Sumber : Indeks KAMI

Catatan: Skor Minimum adalah seluruh pengamanan Tahap 1 & 2 dalam kondisi "Dalam Penerapan/Diterapkan Sebagian.

2.5.5. Penghitungan Skor Indeks KAMI (Keamanan Informasi)

Penghitungan Skor Indeks KAMI ini dilakukan untuk 5 (lima) area kelengkapan informasi yang akan dijelaskan masing-masingnya sebagai berikut:

A. Penghitungan Skor Tata Kelola Keamanan Informasi

Untuk menghitung jumlah skor yang berada pada kolom paling kanan Indeks KAMI (Keamanan Informasi) menggunakan fungsi Index dan MatchMicrosoft excel. Penggabungan fungsi INDEX dan MATCH akan

menghasilkan solusi pencarian data yang baik dimana kita dapat mencari dari referensi berdasarkan kolom atau baris yang kita inginkan. Rumus fungsi INDEX dan MATCH untuk mendapatkan nilai Skor adalah sebagai berikut:

1. Untuk menghitung Skor kategori tingkat kematangan II dan III menggunakan fungsi *INDEX dan MATCH Microsoftexcel*

*=INDEX(array,MATCH(lookup_value,lookup_array,[match_type]),
column_num)*

2. Untuk menghitung Skor kategori kematangan IV menggunakan fungsi IF Microsoft excel2010

=IF(Logical_test, [value_if_true], [value_if_false])

3. Untuk menghitung Total evaluasi Tata Kelola Keamanan Informasi adalah dengan menjumlahkan skor yang ada pada kolom paling kanan dengan rumus fungsi Microsoft excel sebagai berikut:

=SUM(number 1:number 2:...)

4. Untuk menghitung jumlah pertanyaan tahap satu, dua, dan tiga menggunakan rumus fungsi *Countif Microsoft excel*. Fungsi *Countif Microsoft excel* adalah untuk menghitung jumlah data pada sebuah range(jarak) tabel yang memenuhi kriteria dari kondisi yang dipersyaratkan pada parameter fungsi. Rumus fungsi *Countif Microsoft*

excel sebagai berikut:

COUNTIF(range , criteria)

5. Untuk menghitung Batas Skor Minimum untuk Skor Tahap Penerapan III menggunakan rumus:

$= (2 * \text{hasil jumlah pertanyaan tahap 1}) + (4 * \text{hasil jumlah pertanyaan tahap 2})$

6. Untuk menghitung Total Skor Tahap Penerapan 1 dan 2 menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$=SUM(\text{number 1}:\text{number 2}:\dots)$

7. Untuk menentukan Status Penilaian Tahap Penerapan III menggunakan rumus fungsi *IF Microsoft excel*, Jika jumlah Total Skor Tahap Penerapan 1 dan 2 lebih besar dari Batas Skor Minimum untuk Skor Tahap Penerapan III maka Status Penilaian Tahap Penerapan III **VALID** tetapi jika tidak Status Penilaian Tahap Penerapan III **TIDAK VALID**. Rumus fungsi *IF Microsoft excel* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$=IF(\text{Logical_test}, [\text{value_if_true}], [\text{value_if_false}])$

8. Untuk menghitung Skor Tingkat Kematangan II menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan dengan rumus fungsinya sebagai berikut:

$=SUM(\text{number 1}:\text{number 2}:\dots)$

9. Untuk menghitung Skor Minimum Tingkat Kematangan II adalah dengan rumus $= (4 * 2) + (4 * 1)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan II sudah terisi sebelum pertanyaan pada kuesioner dijawab.

10. Untuk menghitung Skor Pencapaian Tingkat Kematangan II adalah

dengan rumus $= (8*2) + (3*4)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan II sudah terisi sebelum pertanyaan pada kuesioner dijawab.

11. Untuk menentukan Status Tingkat Kematangan II menggunakan rumus fungsi *IF Microsoft excel*, Jika skor tingkat kematangan II lebih besar atau sama dengan skor pencapaian tingkat kematangan II maka tingkat kematangan II mencapai minimal dan jika skor tingkat kematangan II lebih besar atau sama dengan skor minimum tingkat kematangan II maka tingkat kematangan I+ mencapai minimal. Rumus fungsi *IF Microsoftexcel* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

12. Untuk menghitung skor tingkat kematangan III menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor dengan rumus fungsinya sebagai berikut:

$$=SUM(number\ 1:number\ 2:...)$$

13. Untuk menentukan validitas tingkat kematangan III menggunakan rumus fungsi *IF Microsoft excel*, jika skor minimum tingkat kematangan II lebih besar sama dengan 80% ambang batas tingkat kematangan status validitas tingkat kematangan III adalah **YES** tetapi jika skor minimum tingkat kematangan II lebih kecil dari 80% ambang batas tingkat kematangan status validitas tingkat kematangan III adalah **NO**. Rumus fungsi *IF*

Microsoft excel untuk status validitas tingkat kematangan III adalah

$=IF(Logical_test, [value_if_true], [value_if_false])$

14. Untuk menghitung Skor Minimum Tingkat Kematangan III adalah dengan rumus $= (2*2) + (1*4)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan III sudah terisi sebelum pertanyaan pada kuesioner dijawab.

15. Untuk menghitung Skor Pencapaian Tingkat Kematangan III adalah dengan rumus $= (2*4) + (1*6)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan III sudah terisi sebelum pertanyaan pada kuesioner dijawab.

16. Untuk menentukan status tingkat kematangan III menggunakan rumus fungsi *IF Microsoft excel*, Jika validitas tingkat kematangan III berstatus YES maka secara otomatis tingkat kematangan III berstatus **YES**. Jika skor tingkat kematangan III lebih tinggi dari skor pencapaian tingkat kematangan III maka pencapaian tingkat kematangan III masuk kategori tingkat kematangan III dan jika skor tingkat kematangan III lebih besar atau sama dengan skor minimum tingkat kematangan III maka pencapaian tingkat kematangan III masuk kategori tingkat kematangan II+ dan berstatus **NO**.

17. Untuk menghitung skor tingkat kematangan IV menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor dengan

rumus fungsinya sebagai berikut:

$$=SUM(number\ 1:number\ 2:...)$$

18. Untuk menentukan validitas tingkat kematangan IV menggunakan rumus fungsi *AND Microsoft excel*, fungsi *AND* akan menghasilkan nilai *true* (benar) jika semua syarat atau argument yang diuji benar atau akan menghasilkan nilai *false* (salah) jika salah satu atau lebih argumen bernilai salah. Rumus fungsi *AND Microsoft excel* untuk Status validitas tingkat kematangan IV sebagai berikut:

$$=IF(AND([logical\ 1], [logical\ 2], [logical\ 3]))$$

19. Untuk menghitung Skor Minimum Tingkat Kematangan IV adalah dengan rumus $= (2*6) + (4*3)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan IV sudah terisi sebelum pertanyaan pada kuesioner dijawab.

20. Untuk menghitung Skor Pencapaian Tingkat Kematangan IV adalah dengan rumus $= 6*9$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan IV sudah terisi sebelum pertanyaan pada kuesioner dijawab.

21. Untuk menentukan status tingkat kematangan IV menggunakan rumus fungsi *AND Microsoft excel 2010*, fungsi *AND* akan menghasilkan nilai *true* (benar) jika semua syarat atau argumen yang diuji benar atau akan menghasilkan nilai *false* (salah) jika salah satu atau lebih argumen bernilai

salah. Rumus fungsi ANDMicrosoft excel2010 untuk Status tingkat kematangan IV sebagai berikut:

$$=IF(AND(logical, [logical 2], [logical 3])$$

B. Penghitungan Pengelolaan Risiko Keamanan Informasi

Untuk menghitung jumlah skor yang berada pada kolom paling kanan Indeks KAMI (Keamanan Informasi) menggunakan fungsi Index dan Match pada Microsoft excel. Penggabungan fungsi Index dan Match akan menghasilkan solusi pencarian data yang baik dimana kita dapat mencari referensi berdasarkan kolom atau baris yang kita diinginkan. Rumus fungsi INDEX dan MATCH untuk mendapatkan nilai skor adalah sebagai berikut:

1. Untuk menghitung skor kategori tingkat kematangan II, III dan IV menggunakan fungsi INDEX dan MATCH Microsoft excel.

$$=INDEX(array, MATCH(lookup_value, lookup_array, [match_type]), column_num)$$

2. Untuk menghitung skor kategori tingkat kematangan V menggunakan fungsi IF Microsoft excel.

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

3. Untuk menghitung Total Nilai Evaluasi Pengelolaan Risiko Keamanan

Informasi adalah dengan menjumlahkan skor yang ada pada kolom paling kanan dengan rumus fungsi Microsoft excel 2010 sebagai berikut:

$$=SUM(number 1: number 2: ...)$$

4. Untuk menghitung jumlah pertanyaan tahap satu, dua dan tiga menggunakan rumus fungsi Count if Microsoft excel. Fungsi Count if

Microsoft excel adalah untuk menghitung jumlah data pada sebuah *range* (jarak) tabel yang memenuhi kriteria dari kondisi yang dipersyaratkan pada parameter fungsi. Rumus fungsi *Count if Microsoft excel* adalah sebagai berikut:

$$=COUNTIF(range, criteria)$$

5. Untuk menghitung jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III pengelolaan risiko keamanan informasi adalah dengan menggunakan rumus sebagai berikut:

$$=(2*\text{hasil jumlah pertanyaan tahap 1}) + (4*\text{hasil jumlah pertanyaan tahap 2})$$

6. Untuk menghitung Total Skor Tahap Penerapan 1 dan 2 menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor, dengan rumus fungsinya sebagai berikut:

$$=SUM(number 1: number 2:...)$$

7. Untuk menetapkan Status Penilaian Tahap Penerapan III menggunakan rumus fungsi *IFMicrosoft excel 2010*, jika jumlah Total Skor Tahap Penerapan 1 dan 2 lebih besar atau sama dengan jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III maka Status Penilaian Tahap Penerapan III VALID. Tetapi jika tidak, Status Penilaian Tahap Penerapan

III menjadi TIDAK VALID. Rumus fungsi *IFMicrosoft excel 2010* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$$=IF(logical_test, [value_if_true], [value_if_false])$$

8. Untuk menghitung Skor Minimum Tingkat Kematangan II adalah dengan

rumus = $(4*2)+(5*1)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) KOMINFO. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan II sudah terisi sebelum pertanyaan pada kuesioner dijawab.

9. Untuk menghitung Skor Pencapaian Tingkat Kematangan II adalah dengan rumus = $(9*2)$ yang sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) KOMINFO. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan II sudah terisi sebelum pertanyaan pada kuesioner dijawab.

10. Untuk menghitung status Tingkat Kematangan II adalah dengan menggunakan rumus yang sudah ditetapkan oleh Indeks KAMI (keamanan informasi) yaitu = $0.8*9*3$ dengan ketentuan $> 80\%$ ambang batas tingkat kematangan dengan menggunakan rumus fungsi IFMicrosoft excel 2010, jika nilai Skor Tingkat Kematangan II maka tingkat kematangan pengelolaan risiko keamanan informasi termasuk dalam tingkat kematangan II. Tetapi, jika skor Tingkat Kematangan II lebih besar atau sama dengan Skor Minimum Tingkat Kematangan II maka tingkat kematangan pengelolaan risiko keamanan informasi termasuk dalam tingkat kematangan I. Rumus fungsi IFMicrosoft excel 2010 untuk Status

Penilaian Tahap Penerapan III sebagai berikut:

$=IF(Logical_test, [value_if_true], [value_if_false])$

11. Untuk menghitung Skor Tingkat Kematangan III menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor, dengan

rumus fungsinya sebagai berikut:

$=SUM (number\ 1: number\ 2: \dots)$

12. Untuk meningkatkan status validitas Tingkat Kematangan III dengan menggunakan rumus fungsi *IF Microsoft excel*, jika skor Tingkat Kematangan II jumlahnya lebih besar atau sama dengan dari hasil perhitungan status tingkat kematangan II maka validitas tingkat kematangan III = *YES*. Tetapi, jika skor Tingkat Kematangan II jumlahnya lebih kecil dari hasil perhitungan status tingkat kematangan II maka validitas tingkat kematangan III = *NO*. Rumus fungsi *IFMicrosoft excel* adalah sebagai berikut:

$=IF (Logical_test, [value_if_true], [value_if_false])$

13. Untuk menghitung Skor Minimum Tingkat Kematangan III adalah dengan rumus $= (2*2)+(0*4)$ yang sudah menjadi ketentuan dari Indeks KAMI (Keamanan informasi) KOMINFO. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan III sudah terisi sebelum pertanyaan pada kuesioner dijawab.

14. Untuk menghitung skor pencapaian Tingkat Kematangan III adalah dengan menggunakan rumus $2*4$ yang sudah menjadi ketentuan dari Indeks KAMI (keamanan informasi) KOMINFO. Angka yang ada pada kolom skor pencapaian Tingkat Kematangan III sudah terisi sebelum pertanyaan pada kuesioner dijawab.

15. Untuk menentukan status Tingkat Kematangan III yaitu jika status validitas tingkat kematangan III = *YES* maka secara otomatis status

Tingkat Kematangan III juga YES. Ketentuan berikutnya jika status validitas Tingkat Kematangan III= NO, maka syarat berikutnya adalah dengan melihat nilai skor tingkat kematangan III lebih besar atau sama dengan skor pencapaian tingkat kematangan III. Secara otomatis status tingkat kematangan III masuk ke dalam kategori tingkat kematangan III. Tetapi jika skor tingkat kematangan III jumlahnya lebih besar atau sama dengan skor minimum tingkat kematangan III secara otomatis status tingkat kematangan III masuk dalam kategori kematangan II+.

16. Untuk menghitung skor Tingkat Kematangan IV menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor dengan rumus fungsinya sebagai berikut:

$$=SUM (number 1: number 2:...)$$

17. Untuk menentukan tingkat validitas Tingkat Kematangan IV menggunakan rumus fungsi *AND Microsoft excel*, fungsi *AND* akan menghasilkan nilai *true* (benar) jika semua syarat atau argumen yang diuji benar atau akan menghasilkan nilai *false* (salah) jika salah satu atau lebih argumen bernilai salah. Rumus fungsi *AND Microsoft excel* untuk Status Validitas Tingkat Kematangan IV sebagai berikut:

$$=IF (AND(logical, [logical 2], [logical 3])$$

18. Skor Minimum Tingkat Kematangan IV sudah merupakan angka standar yang sudah menjadi ketetapan dari Indeks KAMI (Keamanan Informasi) KOMINFO. Angka yang ada pada kolom skor adalah Skor Minimum Tingkat Kematangan IV yang sudah terisi sebelum pertanyaan pada

kuesioner dijawab.

19. Untuk menghitung Skor pencapaian Tingkat Kematangan IV adalah dengan rumus $= 2*6$ yang sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) KOMINFO. Angka yang ada pada kolom Skor pencapaian Tingkat Kematangan IV sudah terisi sebelum pertanyaan pada kuesioner dijawab.

20. Untuk menentukan status Tingkat Kematangan IV menggunakan rumus yang sudah ditetapkan dan juga menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika status validitas kematangan IV = *YES* maka secara otomatis status Tingkat Kematangan IV juga *YES*. Ketentuan berikutnya jika skor Tingkat Kematangan II berjumlah 27 atau jika skor Tingkat Kematangan III berjumlah 12 atau jika skor Tingkat Kematangan IV lebih besar atau sama dengan skor pencapaian Tingkat Kematangan IV maka secara otomatis status Tingkat Kematangan IV masuk dalam kategori Tingkat Kematangan IV. Tetapi jika skor Tingkat Kematangan IV lebih besar atau sama dengan skor minimum Tingkat Kematangan IV, maka secara otomatis status Tingkat Kematangan III masuk dalam kategori Tingkat Kematangan III dan status Tingkat Kematangan IV belum mencapai minimal (*NO*).

21. Untuk menghitung Skor Tingkat Kematangan V menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, rumus fungsinya adalah sebagai berikut:
 $=SUM(number\ 1: number\ 2: \dots)$

22. Untuk menentukan validitas Tingkat Kematangan V menggunakan rumus fungsi *AND Microsoft excel*. Fungsi ini akan menghasilkan nilai *true*

(benar) jika semua syarat atau argumen yang diuji benar atau akan menghasilkan nilai false (salah) jika salah satu atau lebih argumen bernilai salah. Rumus fungsi *AND Microsoft excel* untuk Status validitas Tingkat Kematangan V adalah sebagai berikut:

$$=IF (AND(logical, [logical 2], [logical 3]))$$

23. Untuk menghitung Skor minimum Tingkat Kematangan V adalah dengan rumus $= 2*6$ yang sudah menjadi ketentuan Indeks KAMI (Keamanan Informasi) KOMINFO. Angka yang ada pada kolom skor pencapaian Tingkat Kematangan V sudah terisi sebelum pertanyaan pada kuesioner dijawab.

24. Untuk menghitung Skor pencapaian Tingkat Kematangan V adalah dengan rumus $= 2*9$ yang sudah menjadi ketentuan Indeks KAMI (Keamanan Informasi) KOMINFO. Angka yang ada pada kolom Skor pencapaian Tingkat Kematangan V sudah terisi sebelum pertanyaan pada kuesioner dijawab.

25. Untuk menentukan Status Tingkat Kematangan V menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika status validitas Tingkat Kematangan V = *YES* maka secara otomatis Status Tingkat Kematangan V juga *YES*. Ketentuan berikutnya jika skor Tingkat Kematangan V lebih

besar atau sama dengan skor pencapaian Tingkat Kematangan V maka status Tingkat Kematangan V secara otomatis masuk dalam kategori Tingkat Kematangan V. Tetapi jika skor Tingkat Kematangan V lebih besar atau sama dengan skor minimum Tingkat Kematangan V secara

otomatis status Tingkat Kematangan V masuk dalam kategori tingkat kematangan IV dan status Tingkat Kematangan V belum mencapai minimal (NO).

C. Perhitungan Kerangka Kerja Pengelolaan Keamanan Informasi

Untuk menghitung jumlah skor yang berada pada kolom paling kanan Indeks KAMI (Keamanan Informasi) menggunakan fungsi Index dan MatchMicrosoft excel. Penggabungan fungsi INDEX dan MATCH akan menghasilkan solusi pencarian data yang baik dimana kita dapat mencari dari referensi berdasarkan kolom / baris yang kita inginkan. Rumus fungsi INDEX dan MATCH untuk mendapatkan nilai Skor adalah sebagai berikut:

1. Untuk menghitung Skor kategori tingkat kematangan II dan III menggunakan fungsi INDEX dan MATCH Microsoft excel.

=INDEX(array, MATCH(lookup_value, lookup_array, [match_type]),
column_num)

2. Untuk menghitung Skor kategori kematangan IV dan V menggunakan fungsi IF Microsoft excel.

=IF(Logical_test, [value_if_true], [value_if_false])

3. Untuk menghitung Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi adalah dengan menjumlahkan skor kolom paling kanan dengan rumus fungsi Microsoft excel2010 sebagai berikut:

=SUM(number 1:number 2:...)

4. Untuk menghitung jumlah pertanyaan tahap satu, dua, dan tiga

menggunakan rumus fungsi *Countif Microsoft excel*. Fungsi *Countif Microsoft excel* adalah untuk menghitung jumlah data pada sebuah *range* (jarak) tabel yang memenuhi kriteria dari kondisi yang dipersyaratkan pada parameter fungsi. Rumus fungsi *Countif Microsoft excel* sebagai berikut:

$$=COUNTIF(range, criteria)$$

5. Untuk menghitung jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III kerangka kerja keamanan informasi adalah dengan menggunakan rumus sebagai berikut:
$$=(2 * \text{hasil jumlah pertanyaan tahap1}) + (4 * \text{hasil jumlah pertanyaan tahap 2})$$
6. Untuk menghitung Total Skor Tahap Penerapan 1 dan 2 menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number 1: number 2: ...)$$

7. Untuk menentukan Status Penilaian Tahap Penerapan III kerangka kerja pengelolaan keamanan informasi menggunakan rumus fungsi *IF Microsoft excel*, Jika jumlah Total Skor Tahap Penerapan 1 dan 2 lebih besar atau sama dengan jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III maka Status Penilaian Tahap Penerapan III *VALID* tetapi, jika jumlah Total Skor Tahap Penerapan 1 dan 2 kurang dari Batas Skor Minimum untuk Skor Tahap Penerapan III Status Penilaian Tahap Penerapan III *TIDAK VALID*. Rumus fungsi *IF Microsoft excel* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

8. Untuk menghitung Skor Tingkat Kematangan II menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number 1:number 2:...)$$

9. Untuk menghitung Skor Minimum Tingkat Kematangan II kerangka kerja pengelolaan keamanan informasi adalah dengan rumus $= (4*2) + (4*1)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Koinfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan II kerangka kerja pengelolaan keamanan informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

10. Untuk menghitung status tingkat kematangan II kerangka kerja pengelolaan keamanan informasi adalah dengan menggunakan rumus yang sudah ditetapkan oleh Indeks KAMI (keamanan informasi) yaitu $= 0.8 * ((8*3) + (2*6))$ dengan ketentuan $> 80\%$ ambang batas tingkat kematangan dan menggunakan rumus fungsi *IF Microsoft excel*, jika nilai Skor Tingkat Kematangan II lebih besar sama dengan nilai Skor Pencapaian Tingkat Kematangan II maka tingkat kematangan kerangka kerja pengelolaan keamanan informasi termasuk dalam tingkat kematangan II tetapi, jika Skor Tingkat Kematangan II lebih besar atau sama dengan Skor Minimum Tingkat Kematangan II maka tingkat kerangka kerja pengelolaan keamanan informasi termasuk dalam tingkat kematangan I+. Rumus fungsi *IF Microsoft excel* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

11. Untuk menghitung Skor Tingkat Kematangan III menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number\ 1:number\ 2:…)$$

12. Untuk menentukan status validitas tingkat kematangan III kerangka kerja pengelolaan keamanan informasi dengan menggunakan rumus fungsi *IF Microsoft excel*, jika Skor Tingkat Kematangan II jumlahnya lebih besar atau sama dengan dari hasil perhitungan status tingkat kematangan II maka validitas tingkat kematangan III kerangka kerja pengelolaan keamanan informasi *YES* tetapi, jika Skor Tingkat Kematangan II jumlahnya lebih kecil dari hasil perhitungan status tingkat kematangan II maka validitas tingkat kematangan III *NO*. Rumus fungsi *IF Microsoft excel* untuk status validitas tingkat kematangan III sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

13. Untuk menghitung Skor Minimum Tingkat Kematangan III kerangka kerja pengelolaan keamanan informasi adalah dengan rumus $= (3*3) + (2*2) + (4*4) + (1*3) + (1*6)$ rumus tersebut sudah menjadi ketetapan dari Indeks KAMI (Keamanan Informasi) Koinfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan III kerangka kerja pengelolaan keamanan informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

14. Untuk menghitung Skor Pencapaian Tingkat Kematangan III kerangka

kerja pengelolaan keamanan informasi adalah dengan rumus $= (3*3) + (2*4) + (4*6) + (2*6)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Koinfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan III kerangka kerja pengelolaan keamanan informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

15. Untuk menentukan status tingkat kematangan III kerangka kerja pengelolaan keamanan informasi menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika status validitas tingkat kematangan III *YES* maka secara otomatis status tingkat kematangan III kerangka kerja pengelolaan keamanan informasi juga *YES*. Ketentuan berikutnya jika status validitas tingkat kematangan III *NO*, maka syarat berikutnya adalah dengan melihat nilai skor tingkat kematangan III lebih besar atau sama dengan skor pencapaian tingkat kematangan III secara otomatis status tingkat kematangan III masuk dalam kategori tingkat kematangan III tetapi, jika skor tingkat kematangan III jumlahnya lebih besar atau sama dengan skor minimum tingkat kematangan III secara otomatis status tingkat kematangan III masuk dalam kategori tingkat kematangan II+.

16. Untuk menghitung Skor Tingkat Kematangan III menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number 1:number 2:...)$$

17. Untuk menentukan validitas tingkat kematangan IV kerangka kerja

pengelolaan keamanan informasi menggunakan rumus fungsi *AND Microsoft excel*, fungsi *AND* akan menghasilkan nilai *true* (benar) jika semua syarat atau argumen yang diuji benar atau akan menghasilkan nilai *false* (salah) jika salah satu atau lebih argumen bernilai salah. Rumus fungsi *AND Microsoft excel* untuk Status validitas tingkat kematangan IV sebagai berikut:

$$=IF(AND([logical 1], [logical 2], [logical 3]))$$

17. Untuk menghitung Skor Minimum Tingkat Kematangan IV kerangka kerja pengelolaan keamanan informasi adalah dengan rumus $=(2*6)+(1*3)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan IV kerangka kerja pengelolaan keamanan informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

18. Untuk menghitung Skor Pencapaian Tingkat Kematangan IV kerangka kerja pengelolaan keamanan informasi adalah dengan rumus $=(3*9)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan IV kerangka kerja pengelolaan keamanan informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

19. Untuk menentukan status tingkat kematangan IV kerangka kerja pengelolaan keamanan informasi menggunakan rumus yang sudah ditetapkan dari Indeks KAMI (Keamanan Informasi) Kominfo dan juga menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika

status validitas tingkat kematangan IV *YES* maka secara otomatis status tingkat kematangan IV juga *YES*. Ketentuan berikutnya jika skor tingkat kematangan II berjumlah 36 atau jika skor tingkat kematangan III berjumlah 63 atau jika skor tingkat kematangan IV lebih besar atau sama dengan skor pencapaian tingkat kematangan IV maka status tingkat kematangan IV secara otomatis status tingkat kematangan IV masuk dalam kategori tingkat kematangan IV tetapi jika skor tingkat kematangan IV lebih besar atau sama dengan skor minimum tingkat kematangan IV secara otomatis status tingkat kematangan III masuk dalam kategori tingkat kematangan III+ dan status tingkat kematangan IV belum mencapai minimal (*NO*).

D. Perhitungan Skor Pengelolaan Aset

Penghitungan Pengelolaan Aset Informasi dengan menggunakan alat evaluasi kelengkapan dan kematangan Indeks KAMI (Keamanan Informasi) menggunakan *Microsoft excel* dan rumus fungsi yang ada dalam *Microsoft excel*. Rumus fungsi *Microsoft excel* yang digunakan untuk menghitung tingkat kelengkapan pengelolaan aset informasi adalah sebagai berikut:

1. Untuk menghitung Skor kategori tingkat kematangan II dan III menggunakan fungsi *INDEX* dan *MATCH* *Microsoft excel*.
$$=INDEX(array, MATCH(lookup_value, lookup_array, [match_type]), colum_num)$$
2. Untuk menghitung skor kategori tingkat kematangan III tahap penerapan III menggunakan rumus fungsi *IF* *Microsoft excel*.

$=IF(Logical_test, [value_if_true], [value_if_false])$

3. Untuk menghitung Total Nilai Evaluasi Pengelolaan Aset Informasi adalah dengan menjumlahkan skor kolom paling kanan dengan rumus fungsi *Microsoft excel* sebagai berikut:

$=SUM(number\ 1:number\ 2:…)$

4. Untuk menghitung jumlah pertanyaan tahap satu, dua, dan tiga menggunakan rumus fungsi *Countif Microsoft excel*. Fungsi *Countif Microsoft excel* adalah untuk menghitung jumlah data pada sebuah *range* (jarak) tabel yang memenuhi kriteria dari kondisi yang dipersyaratkan pada parameter fungsi. Rumus fungsi *Countif Microsoft excel* sebagai berikut:

$=COUNTIF(range, criteria)$

5. Untuk menghitung jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III Pengelolaan Aset Informasi adalah dengan menggunakan rumus sebagai berikut:

$=(2 * \text{hasil jumlah pertanyaan tahap 1}) + (4 * \text{hasil jumlah pertanyaan tahap 2})$

6. Untuk menghitung Total Skor Tahap Penerapan 1 dan 2 menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$=SUM(number\ 1:number\ 2:…)$

7. Untuk menentukan Status Penilaian Tahap Penerapan III Pengelolaan Aset Informasi menggunakan rumus fungsi *IF Microsoft excel*, Jika jumlah Total Skor Tahap Penerapan 1 dan 2 lebih besar atau sama dengan jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III maka Status

Penilaian Tahap Penerapan III VALID tetapi, jika jumlah Total Skor Tahap Penerapan 1 dan 2 kurang dari Batas Skor Minimum untuk Skor Tahap Penerapan III Status Penilaian Tahap Penerapan III TIDAK VALID. Rumus fungsi *IF Microsoft excel* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

8. Untuk menghitung Total Skor tingkat kematangan II menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number\ 1:number\ 2:...)$$

9. Untuk menghitung Skor Minimum Tingkat Kematangan II Pengelolaan Aset Informasi adalah dengan rumus $= (4*2) + (17*1)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan II Pengelolaan Aset Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

10. Untuk menghitung Skor Pencapaian Tingkat Kematangan II Pengelolaan Aset Informasi adalah dengan rumus $= (21*2) + (5*4)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo.

Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan II Pengelolaan Aset Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

11. Untuk menghitung status tingkat kematangan II Pengelolaan Aset

Informasi adalah dengan menggunakan rumus yang sudah ditetapkan oleh Indeks KAMI (keamanan informasi) yaitu $=0.8*((21*3)+(5*6))$ dengan ketentuan $> 80\%$ ambang batas tingkat kematangan dan menggunakan rumus fungsi *IF Microsoft excel*, jika nilai Skor Tingkat Kematangan II lebih besar sama dengan nilai Skor Pencapaian Tingkat Kematangan II maka tingkat Pengelolaan Aset Informasi termasuk dalam tingkat kematangan II tetapi, jika Skor Tingkat Kematangan II lebih besar atau sama dengan Skor Minimum Tingkat Kematangan II maka tingkat kematangan Pengelolaan Aset Informasi termasuk dalam tingkat kematangan I+ dan tidak memenuhi validasi untuk tingkat kematangan III. Rumus fungsi *IF Microsoft excel* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

12. Untuk menghitung Total Skor tingkat kematangan III menggunakan rumus fungsi *SUM Microsoft excel 2010* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number\ 1:number\ 2:...)$$

13. Untuk menghitung status validitas tingkat kematangan III menggunakan Rumus fungsi *IF Microsoft excel*. Ketentuan dalam menentukan validitas

tingkat kematangan III adalah jika skor tingkat kematangan II lebih besar atau sama dengan skor status tingkat kematangan II maka validitas tingkat kematangan III berstatus *YES*, jika jika skor tingkat kematangan II lebih rendah dari skor status tingkat kematangan II maka validitas tingkat

kematangan III berstatus *NO*. Rumus fungsi *IF Microsoft excel* untuk status validitas tingkat kematangan III adalah sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

14. Untuk menghitung Skor Minimum Tingkat Kematangan III Pengelolaan Aset Informasi adalah dengan rumus $= (2*2) + (2*4) + (1*3) + (3*6)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan III Pengelolaan Aset Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

15. Untuk menghitung Skor Pencapaian Tingkat Kematangan III Pengelolaan Aset Informasi adalah dengan rumus $= (2*4) + (2*6) + (4*6)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan III Pengelolaan Aset Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

16. Untuk menentukan status tingkat kematangan III Pengelolaan Aset Informasi menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika status validitas tingkat kematangan III *YES* maka secara otomatis status tingkat kematangan III kerangka kerja pengelolaan

keamanan informasi juga *YES*. Ketentuan berikutnya jika status validitas tingkat kematangan III *NO* maka syarat berikutnya adalah dengan melihat nilai skor tingkat kematangan III lebih besar atau sama dengan skor pencapaian tingkat kematangan III secara otomatis status tingkat

kematangan III masuk dalam kategori tingkat kematangan III yang artinya tingkat kematangan III belum mencapai minimal (*NO*). Jika skor tingkat kematangan III jumlahnya lebih besar atau sama dengan skor minimum tingkat kematangan III secara otomatis status tingkat kematangan III masuk dalam kategori tingkat kematangan II+ yang artinya tingkat kematangan III belum mencapai minimal (*NO*).

E. Perhitungan Skor Teknologi dan Keamanan Informasi

Perhitungan Teknologi dan Keamanan Informasi dengan menggunakan alat evaluasi kelengkapan dan kematangan Indeks KAMI (Keamanan Informasi) menggunakan *Microsoft excel* dan rumus fungsi yang ada dalam *Microsoft excel*. Rumus fungsi *Microsoft excel* yang digunakan untuk menghitung tingkat kelengkapan Teknologi dan Keamanan Informasi adalah sebagai berikut:

1. Untuk menghitung Skor kategori tingkat kematangan II dan III

menggunakan fungsi *INDEX* dan *MATCH* *Microsoft excel*.

$$=INDEX(array, MATCH(lookup_value, lookup_array, [match_type]), column_num)$$

2. Untuk menghitung Skor kategori tingkat kematangan IV menggunakan fungsi *IF* *Microsoft excel*.

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

3. Untuk menghitung Total Nilai Evaluasi Teknologi dan Keamanan

Informasi adalah dengan menjumlahkan skor kolom paling kanan dengan rumus fungsi *Microsoft excel* sebagai berikut:

$$=SUM(number\ 1:number\ 2:...)$$

4. Untuk menghitung jumlah pertanyaan tahap satu, dua, dan tiga

menggunakan rumus fungsi *Countif Microsoft excel*. Fungsi *Countif Microsoft excel* adalah untuk menghitung jumlah data pada sebuah *range* (jarak) tabel yang memenuhi kriteria dari kondisi yang dipersyaratkan pada parameter fungsi. Rumus fungsi *Countif Microsoft excel* sebagai berikut:

$$=COUNTIF(range, criteria)$$

5. Untuk menghitung jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III Teknologi dan Keamanan Informasi adalah dengan menggunakan rumus sebagai berikut:

$$=(2 * \text{hasil jumlah pertanyaan tahap1}) + (4 * \text{hasil jumlah pertanyaan tahap 2})$$

6. Untuk menghitung Total Skor Tahap Penerapan 1 dan 2 menggunakan rumus fungsi *SUMMicrosoft excel2010* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number 1:number 2:...)$$

7. Untuk menentukan Status Penilaian Tahap Penerapan III Teknologi dan Keamanan Informasimenggunakan rumus fungsi *IF Microsoft excel*, Jika jumlah Total Skor Tahap Penerapan 1 dan 2 lebih besar atau sama dengan jumlah Batas Skor Minimum untuk Skor Tahap Penerapan III maka Status Penilaian Tahap Penerapan III VALID tetapi, jika jumlah Total Skor Tahap Penerapan 1 dan 2 kurang dari Batas Skor Minimum untuk Skor Tahap Penerapan III Status Penilaian Tahap Penerapan III TIDAK VALID.Rumus fungsi *IF Microsoft excel* untuk Status Penilaian Tahap Penerapan III sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

8. Untuk menghitung Total Skor tingkat kematangan II menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number\ 1:number\ 2:...)$$

9. Untuk menghitung Skor Minimum Tingkat Kematangan II Teknologi dan Keamanan Informasi adalah dengan rumus $= (4*2) + (9*1)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Koinfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan II Teknologi dan Keamanan Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

10. Untuk menghitung Skor Pencapaian Tingkat Kematangan II Teknologi dan Keamanan Informasi adalah dengan rumus $= 13*2$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Koinfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan II Teknologi dan Keamanan Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

11. Untuk menghitung status tingkat kematangan II Teknologi dan Keamanan Informasi adalah dengan menggunakan rumus yang sudah ditetapkan oleh Indeks KAMI (keamanan informasi) yaitu $= 0.8*13*3$ dengan ketentuan $> 80\%$ ambang batas tingkat kematangan dan menggunakan rumus fungsi *IF Microsoft excel*, jika nilai Skor Tingkat Kematangan II lebih besar sama dengan nilai Skor Pencapaian Tingkat Kematangan II maka

Teknologi dan Keamanan Informasi termasuk dalam tingkat kematangan II tetapi, jika Skor Tingkat Kematangan II lebih besar atau sama dengan Skor Minimum Tingkat Kematangan II maka tingkat kematangan Teknologi dan Keamanan Informasi termasuk dalam tingkat kematangan I+ dan status tingkat kematangan II Teknologi dan Keamanan Informasi belum mencapai minimum (NO). Rumus fungsi *IF Microsoft excel* untuk Status Penilaian Tahap Penerapan II sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

12. Untuk menghitung Total Skor tingkat kematangan III menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number\ 1:number\ 2:...)$$

13. Untuk menghitung status validitas tingkat kematangan III menggunakan Rumus fungsi *IF Microsoft excel*. Ketentuan dalam menentukan validitas tingkat kematangan III adalah jika skor tingkat kematangan II lebih besar atau sama dengan skor status tingkat kematangan II maka validitas tingkat kematangan III berstatus *YES*, jika jika skor tingkat kematangan II lebih rendah dari skor status tingkat kematangan II maka validitas tingkat kematangan III berstatus *NO*. Rumus fungsi *IF Microsoft excel* untuk status validitas tingkat kematangan III adalah sebagai berikut:

$$=IF(Logical_test, [value_if_true], [value_if_false])$$

14. Untuk menghitung Skor Minimum Tingkat Kematangan III Teknologi dan Keamanan Informasi adalah dengan rumus

$= (3*3) + (2*2) + (4*4) + (1*3) + (1*6)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan III Teknologi dan Keamanan Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

15. Untuk menghitung Skor Pencapaian Tingkat Kematangan III Teknologi dan Keamanan Informasi adalah dengan rumus $= (3*3) + (2*4) + (4*6) + (2*6)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan III Teknologi dan Keamanan Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

16. Untuk menentukan status tingkat kematangan III Teknologi dan Keamanan Informasi menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika status validitas tingkat kematangan III *YES* maka secara otomatis status tingkat kematangan III kerangka kerja pengelolaan keamanan informasi juga *YES*. Ketentuan berikutnya jika status validitas tingkat kematangan III *NO* maka syarat berikutnya adalah dengan melihat nilai skor tingkat kematangan III lebih besar atau sama dengan skor pencapaian tingkat kematangan III secara otomatis status tingkat kematangan III masuk dalam kategori tingkat kematangan III yang artinya tingkat kematangan III belum mencapai minimal (*NO*). Jika skor tingkat kematangan III jumlahnya lebih besar atau sama dengan skor minimum tingkat kematangan III secara otomatis status tingkat kematangan III masuk dalam kategori tingkat kematangan II+ yang artinya tingkat

kematangan III belum mencapai minimal (*NO*).

17. Untuk menghitung Skor tingkat kematangan IV menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number 1:number 2:...)$$

18. Untuk menentukan validitas tingkat kematangan IV Teknologi dan Keamanan Informasi menggunakan rumus fungsi *AND Microsoft excel*, fungsi *AND* akan menghasilkan nilai *true* (benar) jika semua syarat atau argumen yang diuji benar atau akan menghasilkan nilai *false* (salah) jika salah satu atau lebih argumen bernilai salah. Rumus fungsi *AND Microsoft excel* untuk Status validitas tingkat kematangan IV sebagai berikut:

$$=IF(AND([logical], [logical 2], [logical 3]))$$

19. Untuk menghitung Skor Minimum Tingkat Kematangan IV Teknologi dan Keamanan Informasi adalah dengan rumus $=(2*6)+(1*3)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan IV Teknologi dan Keamanan Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

20. Untuk menghitung Skor Pencapaian Tingkat Kematangan IV Teknologi dan Keamanan Informasi adalah dengan rumus $=(3*9)$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Kominfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan IV Teknologi dan Keamanan Informasi sudah terisi sebelum

pertanyaan pada kuesioner dijawab.

21. Untuk menentukan status tingkat kematangan IV menggunakan rumus yang sudah ditetapkan dari Indeks KAMI (Keamanan Informasi) Kominfo dan juga menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika status validitas tingkat kematangan IV *YES* maka secara otomatis status tingkat kematangan IV juga *YES*. Ketentuan berikutnya jika skor tingkat kematangan II berjumlah 36 atau jika skor tingkat kematangan III berjumlah 63 atau jika skor tingkat kematangan IV lebih besar atau sama dengan skor pencapaian tingkat kematangan IV maka status tingkat kematangan IV secara otomatis status tingkat kematangan IV masuk dalam kategori tingkat kematangan IV tetapi jika skor tingkat kematangan IV lebih besar atau sama dengan skor minimum tingkat kematangan IV secara otomatis status tingkat kematangan III masuk dalam kategori tingkat kematangan III dan status tingkat kematangan IV belum mencapai minimal (*NO*).

22. Untuk menghitung Total Skor tingkat kematangan V menggunakan rumus fungsi *SUM Microsoft excel* yaitu dengan menjumlahkan skor yang berada paling kanan, dengan rumus fungsinya sebagai berikut:

$$=SUM(number 1:number 2:...)$$

23. Untuk menentukan validitas tingkat kematangan V menggunakan rumus

fungsi *AND Microsoft excel*, fungsi *AND* akan menghasilkan nilai true (benar) jika semua syarat atau argumen yang diuji benar atau akan menghasilkan nilai false (salah) jika salah satu atau lebih argumen bernilai salah. Rumus fungsi *AND Microsoft excel* untuk Status validitas tingkat kematangan V sebagai berikut:

$$=IF(AND([logical 1], [logical 2], [logical 3]))$$

24. Untuk menghitung Skor Minimum Tingkat Kematangan V Teknologi dan Keamanan Informasi adalah dengan rumus $=2*6$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Koinfo. Angka yang ada pada kolom Skor Minimum Tingkat Kematangan V Teknologi dan Keamanan Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

25. Untuk menghitung Skor Pencapaian Tingkat Kematangan V Teknologi dan Keamanan Informasi adalah dengan rumus $=2*9$ rumus tersebut sudah menjadi ketentuan dari Indeks KAMI (Keamanan Informasi) Koinfo. Angka yang ada pada kolom Skor Pencapaian Tingkat Kematangan V Teknologi dan Keamanan Informasi sudah terisi sebelum pertanyaan pada kuesioner dijawab.

26. Untuk menentukan status tingkat kematangan V menggunakan rumus fungsi *IF Microsoft excel* dengan ketentuan jika status validitas tingkat kematangan V telah mencapai minimal (*YES*) maka secara otomatis status tingkat kematangan V juga telah mencapai minimal (*YES*). Ketentuan berikutnya jika skor tingkat kematangan V lebih besar atau sama dengan

skor pencapaian tingkat kematangan V maka status tingkat kematangan V secara otomatis status tingkat kematangan V masuk dalam kategori tingkat kematangan V tetapi jika skor tingkat kematangan V lebih besar atau sama dengan skor minimum tingkat kematangan V secara otomatis status tingkat kematangan V masuk dalam kategori tingkat kematangan IV+ dan status tingkat kematangan V belum mencapai minimal (NO).

2.5.6. Pengkajian Hasil Indeks KAMI

Hasil dari penjumlahan skor untuk masing-masing area ditampilkan dalam 2 (dua) instrumen di *dashboard* :

1. Tabel nilai masing-masing area;
2. *Radar Chart* dengan 5 (lima) sumbu sesuai dengan area pengamanan.

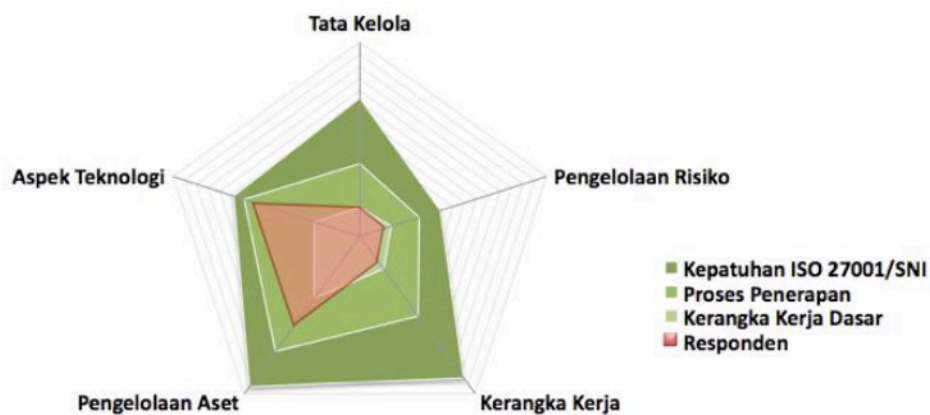
Kedua instrumen ini dapat dilihat pada gambar dibawah ini. Untuk nilai masing-masing area dirangkum dalam gambar pada tabel dibawah ini, institusi akan melihat seberapa besar tingkat kelengkapan masing-masing area yang telah dicapai.

| | |
|-----------------------------------|-----|
| Peran/Tingkat Kepentingan TIK | : 0 |
| Tata Kelola | : 0 |
| Pengelolaan Risiko | : 0 |
| Kerangka Kerja Keamanan Informasi | : 0 |
| Pengelolaan Aset | : 0 |
| Teknologi dan Keamanan Informasi | : 0 |

Gambar 2.8 Rangkuman Evaluasi Berdasarkan Area Keamanan Informasi
Sumber : Indeks KAMI

Sedangkan diagram radar pada gambar dibawah ini menunjukkan sejauh mana kelengkapan pengamanan sudah mendekati atau mencapai tingkat

kelengkapan yang diharapkan. Dalam diagram radar, latar belakang area menunjukkan ambang batas tingkat kelengkapan (kategori) 1 s/d 3 (hijau muda s/d hijau tua). Nilai dari masing-masing area ditampilkan dalam area merah. Dalam diagram ini bisa dilihat perbandingan antara kondisi kesiapan sebagai hasil dari proses evaluasi dengan acuan tingkat kelengkapan yang ada.



Gambar 2.9 Diagram Radar Tingkat Kelengkapan Masing-Masing Area
Sumber : Indeks KAMI

Gambar 2.9 diatas 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 | 12 | 0 | 124 | Tidak Layak |
| | | 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 2.10 Matriks Peran TIK dan Status Kesiapan
Sumber : Indeks KAMI

Gambar 2.10 diatas 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 dibawah ini :



U N I V E R S I T A S
M U L T I M E D I A
N U S A N T A R A

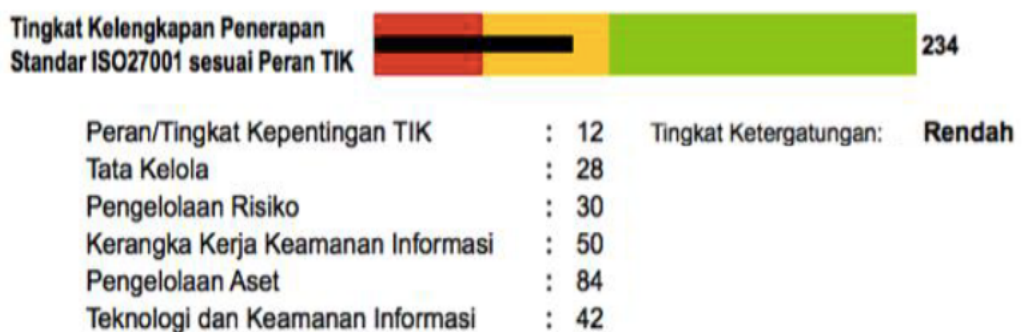


Rentang Kelengkapan Pengamanan

Gambar 2.11 Bar Chart Tingkat Kelengkapan Penerapan Standart ISO27001

Sumber : Indeks KAMI

Gambar 2.11 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/ketertanggung terhadap TIK dinilai sebagai “Rendah” dan total jumlah nilai kelengkapan 234, Maka *dashboard* akan menampilkan hasil seperti yang ada di **Gambar 2.12** dibawah ini.



Gambar 2.12 Contoh Hasil Evaluasi Tingkat Kelengkapan
Sumber : Indeks KAMI

M U L T I M E D I A
N U S A N T A R A

2.5.7. Mekanisme Penilaian Kematangan

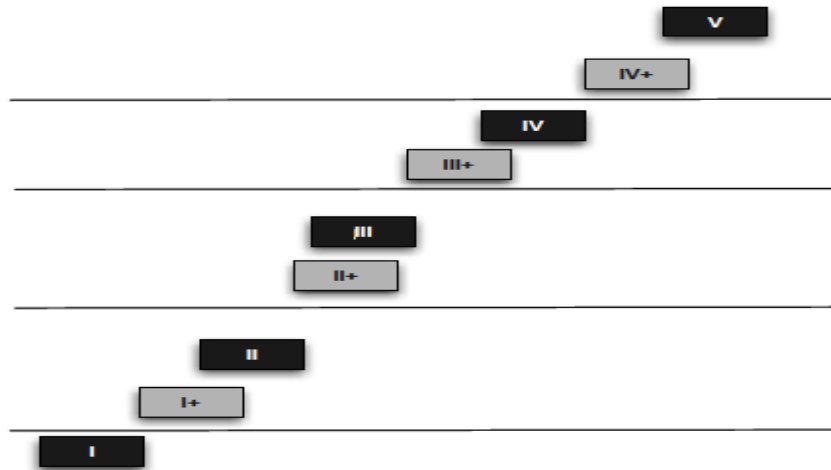
Penilaian kemudian dilakukan dengan menganalisis jumlah di masing-masing area dan menganalisis apakah jumlah tersebut sudah mencapai atau melewati ambang batas pencapaian tingkat kematangan (TK) tertentu.

Penghitungan dilakukan dengan menerapkan prinsip:

- Pencapaian Tingkat Kematangan dilakukan sesuai dengan kelengkapan dan (konsistensi + efektivitas) penerapannya.
- Tingkat Kematangan yang lebih tinggi mensyaratkan kelengkapan, konsistensi dan efektivitas pengamanan di level bawahnya.
- Pencapaian suatu Tingkat Kematangan II dan III hanya dapat dilakukan apabila sebagian besar di Tingkat Kematangan sebelumnya $[x-1]$ sudah “Diterapkan Secara Menyeluruh”.
- Khusus untuk pencapaian TKIV dan TKV mengharuskan seluruh bentuk pengamanan di tingkat-tingkat sebelumnya sudah “Diterapkan Secara Menyeluruh.” Hal ini memberikan efek kesulitan yang lebih tinggi untuk mencapai 2 (dua) tingkatan terakhir tingkat kematangan. Detail perhitungan ambang batas pencapaian Tingkat Kematangan I-V diuraikan di bagian lain dalam dokumen ini.
- Untuk membantu memberikan uraian yang lebih detail, tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar ISO/IEC 2700:2005, tingkat kematangan yang diharapkan untuk

ambang batas minimum kesiapan sertifikasi adalah Tingkat III+."

- Ambang batas pencapaian tingkat keamanan tertentu dapat didefinisikan sebagaimana ditunjukkan pada Gambar dibawah ini.



Gambar 2.13 Gambaran Definisi Evaluasi Tingkat Kematangan
Sumber : Panduan Penerapan Tata Kelola Keamanan Informasi (2011)

Gambar 2.13 menggambarkan penentuan ambang batas pencapaian suatu tingkat kematangan ditentukan berdasarkan perumusan di bawah ini (TK_x = Tingkat Kematangan x):

Tingkat Kematangan I: Tidak ada ambang batas minimum

- Diasumsikan semua responden diberikan status ini pada saat dimulainya evaluasi.

Tingkat Kematangan I+: Mencapai minimal

- 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.”

Tingkat Kematangan II: Mencapai minimal

- Seluruh bentuk pengamanan TKII-Tahap 1 dengan status “Dalam Penerapan/Diterapkan Sebagian”; dan
- Seluruh bentuk pengamanan TKII-Tahap 2 dengan status “Dalam Penerapan/Diterapkan Sebagian.”

Tingkat Kematangan II+: Mencapai minimal

- Prasyarat Dasar Tingkat Kematangan II+, yaitu mencapai nilai total bentuk pengamanan Tingkat Kematangan II > (80% dari nilai seluruh bentuk pengamanan Tingkat Kematangan II - Tahap 1 & 2 dengan status “Diterapkan Secara Menyeluruh”); dan
- Seluruh bentuk pengamanan Tingkat Kematangan III-Tahap 1 dengan status “Diterapkan Secara Menyeluruh”; dan
- Dua bentuk pengamanan Tingkat Kematangan III-Tahap 2 dengan status “Sedang Direncanakan”; dan
- Sisa jumlah pengamanan Tingkat Kematangan III-Tahap 2 yang ada dengan status “Dalam Penerapan/Diterapkan Sebagian”; dan
- Satu bentuk pengamanan Tingkat Kematangan III-Tahap 3 dengan status “Sedang Direncanakan.”
- Sisa jumlah pengamanan Tingkat Kematangan III-Tahap 3 dengan status “Dalam Penerapan/Diterapkan Sebagian.”

Tingkat Kematangan III: Mencapai minimal

- Prasyarat Dasar Tingkat Kematangan II+; dan
- Seluruh bentuk pengamanan Tingkat Kematangan III-Tahap 1 dengan

- status “Diterapkan Secara Menyeluruh”; dan
- Dua bentuk pengamanan Tingkat Kematangan III-Tahap 2 dengan status “Dalam Penerapan/Diterapkan Sebagian”; dan
- Sisa jumlah pengamanan Tingkat Kematangan III-Tahap 2 yang ada dengan status “Diterapkan Secara Menyeluruh”; dan
- Dua bentuk pengamanan Tingkat Kematangan III-Tahap 3 dengan status “Dalam Penerapan/Diterapkan Sebagian.”

Tingkat Kematangan III+: Mencapai minimal

- Persyaratan Dasar Tingkat Kematangan III+ yaitu mencapai nilai total lebih dari:
- Seluruh bentuk pengamanan Tingkat kematangan III - Tahap 1 dengan status “Diterapkan Secara menyeluruh”, dan
- Satu bentuk pengamanan Tingkat Kematangan III – tahap 2 dengan status “Dalam Penerapan/Diterapkan Sebagian”, dan
- Sisa jumlah pengamanan Tingkat Kematangan III – Tahap 2 yang ada dengan status “Diterapkan Secara Menyeluruh”, dan
- Satu bentuk pengamanan Tingkat Kematangan III – Tahap 3 dengan status “Dalam Penerapan/Diterapkan Sebagian”, dan
- Sisa jumlah pengamanan Tingkat Kematangan III – Tahap 3 dengan status “Diterapkan Secara Menyeluruh.”
- Dua bentuk pengamanan Tingkat Kematangan IV – Tahap 3 dengan status “ Dalam Penerapan/Diterapkan Sebagian”, dan

- Sisa jumlah pengamanan Tingkat Kematangan IV – Tahap 3 yang ada dengan status “Dalam Perencanaan.”

Tingkat Kematangan IV : Mencapai Minimal

- Prasyarat Dasar Tingkat Kematangan III+; dan
- Seluruh bentuk pengamanan Tingkat Kematangan IV – Tahap 3 dengan status “Diterapkan Secara Menyeluruh.”

Tingkat Kematangan IV+: Mencapai Minimal

- Mencapai Tingkat Kematangan IV; dan Satu bentuk pengamanan Tingkat Kematangan V – Tahap 3 dengan status “Dalam Penerapan /Diterapkan Sebagian.”

Tingkat Kematangan V: Mecapai Minimal

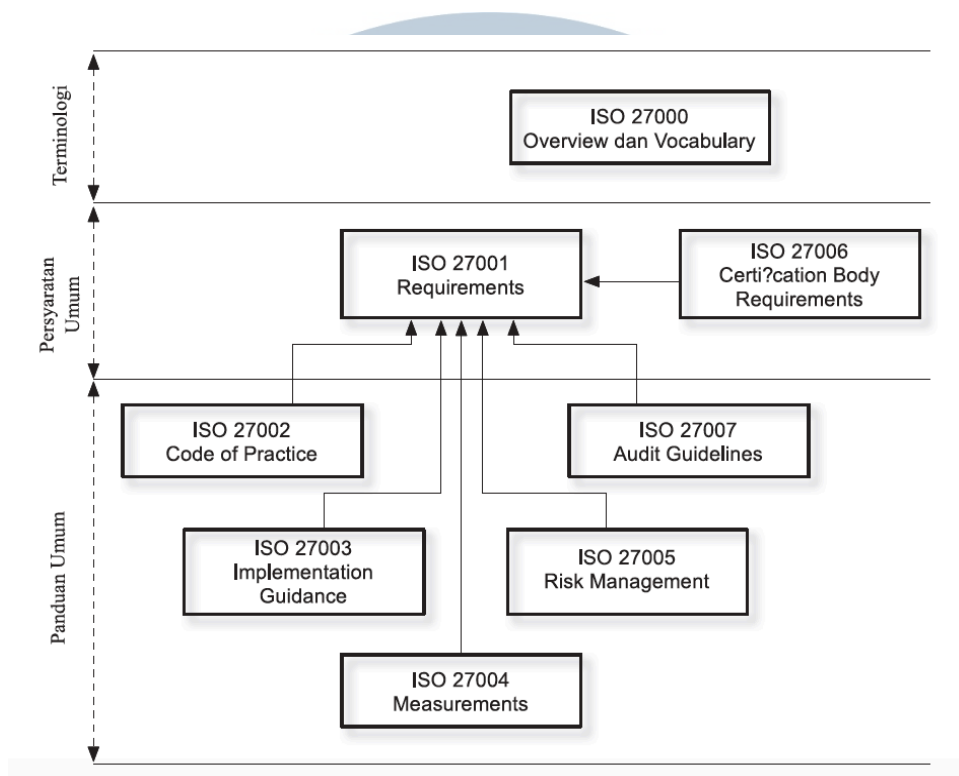
- Mencapai Tingkat Kematangan IV; dan
- Seluruh bentuk pengamanan Tingkat Kematangan V – Tahap 3 dengan status “Diterapkan Secara Menyeluruh.”

2.6. Sistem Manajemen Keamanan Informasi

2.6.1. ISO/IEC 27001 ISMS – *Overview and Vocabulary*

Standar yang sudah mengalami revisi hingga edisi tahun 2014, memuat prinsip-prinsip dasar *Information Security Management System* (Sistem Manajemen Keamanan Informasi – SMKI), definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga SMKI, baik yang telah diterbitkan maupun sedang dalam tahap pengembangan.

Hubungan antar standar keluarga ISO 27000 dapat digambarkan sebagai berikut:



Gambar 2.14 Hubungan Antara Keluarga ISO

2.6.2. ISO/IEC 27001 - Persyaratan SMKI

ISO/IEC 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (*review*), pemeliharaan dan peningkatan suatu SMKI.

Pendekatan proses mendorong pengguna menekankan pentingnya:

- a) Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi
- b) Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan
- c) Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
- d) Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.

Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ini mengadopsi "*Plan-Do-Check-Act*" (PDCA) model, yang digunakan untuk mengatur semua proses SMKI. Penerapan model PDCA juga akan mencerminkan prinsip-prinsip sebagaimana diatur dalam Pedoman OECD (2002) yang mengatur keamanan sistem informasi dan jaringan. Standar ini memberikan model untuk menerapkan prinsip-prinsip dalam pedoman yang mengatur penilaian risiko, desain keamanan dan implementasi, manajemen keamanan dan penilaian ulang (Anggi Anugraha Putra1), 2016).

2.6.3. ISO/IEC 27002 – *Code of Practice for ISMS*

ISO/IEC 27002 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk- bentuk kontrol yang disajikan

seluruhnya menyangkut 14 area pengamanan sebagaimana ditetapkan dalam ISO/IEC 27001 ISO/IEC 27002 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil kajian risiko yang telah dilakukannya. Pengguna juga dapat memilih kontrol di luar daftar kontrol yang dimuat standar ini sepanjang sasaran kontrolnya dipenuhi.

2.6.4. ISO/IEC 27003 -*Information security management system implementation guidance*

Tujuan dari ISO/IEC 27003 adalah untuk memberikan panduan bagi perancangan dan penerapan SMKI agar memenuhi persyaratan ISO 27001. Standar ini menjelaskan proses pembangunan SMKI meliputi persiapan, perancangan dan penyusunan / pengembangan SMKI yang digambarkan sebagai suatu kegiatan proyek. Sebagai kegiatan proyek, tahapan utama yang dijelaskan dalam standar ini meliputi

- Mendapatkan persetujuan manajemen untuk memulai proyek SMKI
- Mendefinisikan ruang lingkup, batasan dan kebijakan SMKI
- Melakukan analisis persyaratan SMKI
- Melakukan kajian risiko dan rencana penanggulangan risiko
- Merancang SMKI
- Perencanaan penerapan SMKI

Standar ini diterbitkan pada bulan Januari 2010.

2.6.5. ISO/IEC 27004 - *Information security management measurement*

Standar ini menyediakan panduan penyusunan dan penggunaan teknik pengukuran untuk mengkaji efektivitas penerapan SMKI dan kontrol sebagaimana dipersyaratkan ISO/IEC 27001. Standar ini juga organisasi dalam mengukur ketercapaian sasaran keamanan yang ditetapkan.

Standar ini mencakup bagian utama sebagai berikut:

- Penjelasan tentang pengukuran keamanan informasi;
- Tanggung jawab manajemen;
- Pengembangan metode pengukuran;
- Pengukuran operasi;
- Analisis data dan pelaporan hasil pengukuran;
- Evaluasi dan perbaikan Program Pengukuran Keamanan Informasi.

Standar ini diterbitkan bulan Desember 2009.

2.6.6. ISO/IEC 27005 - *Information security risk management*

Standar ini menyediakan panduan bagi kegiatan manajemen risiko keamanan informasi dalam suatu organisasi, khususnya dalam rangka mendukung persyaratan-persyaratan SMKI sebagaimana didefinisikan oleh ISO/IEC 27001.

Standar ini diterbitkan pada bulan Juni 2008.

2.6.7. ISO/IEC 27006 - *Requirements for bodies providing audit and certification of information security management systems.*

Standar ini menetapkan persyaratan dan memberikan panduan bagi

organisasi yang memiliki kewenangan untuk melakukan audit dan sertifikasi sistem manajemen keamanan informasi (SMKI). Standar ini utamanya dimaksudkan untuk mendukung proses akreditasi Badan Sertifikasi ISO/IEC 27001 oleh Komite Akreditasi dari negara masing-masing.

2.7. ISO/IEC 27001 : 2013

ISO 27001:2013 merupakan susunan secara adopsi identik terhadap standar ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*. 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.

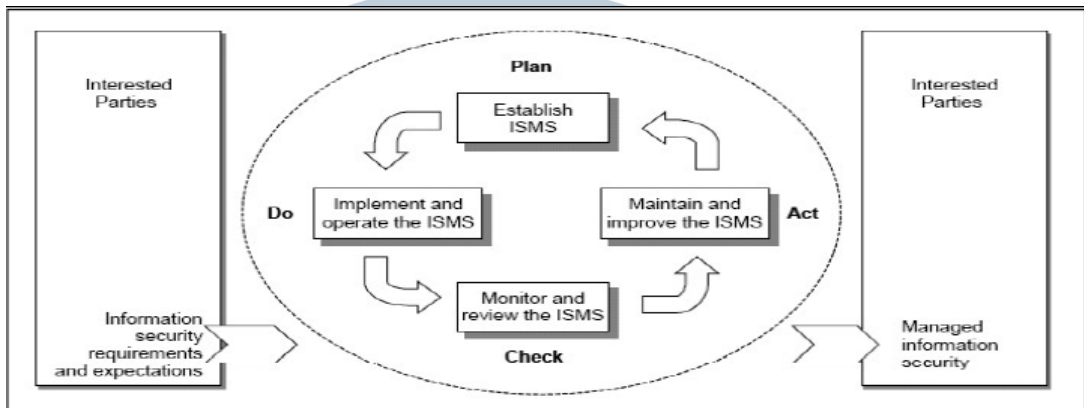
ISO 27001 digunakan sebagai ikon sertifikasi ISO 27001. ISO 27001 merupakan dokumen standar sistem manajemen keamanan informasi (SMKI) atau *Information Security Management System (ISMS)* yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah instansi atau perusahaan dalam usaha mereka mengimplementasikan konsep-konsep keamanan informasi di perusahaan.

Struktur dan konsep dari ISO 27001 :2013 *Information technology – Security techniques – Information security management system – Requirement* (ISO/IEC 27001 , 2013)

0. *Introduction*
1. *Scope*
2. *Normative Reference*
3. *Terms and Conditions*
4. *Context of the organization*
5. *Leadership*
6. *Planning*
7. *Support*
8. *Operation*
9. *Performance Evaluation*
10. *Improvement*

Annex A – Controls objectives and controls atau yang dikenal ISO 27002

Standar SNI ISO/IEC 27001:2009 mengadopsi model metode “*Plan-Do-Check-Act*” (PDCA) yang diterapkan untuk membentuk seluruh proses SMKI. Gambar dibawah ini memperlihatkan persyaratan keamanan informasi dan harapan dari pihak terkait menjadi masukan bagi SMKI, serta melalui tindakan dan proses yang diperlukan akan menghasilkan keluaran keamanan informasi yang memenuhi persyaratan dan harapan tersebut.

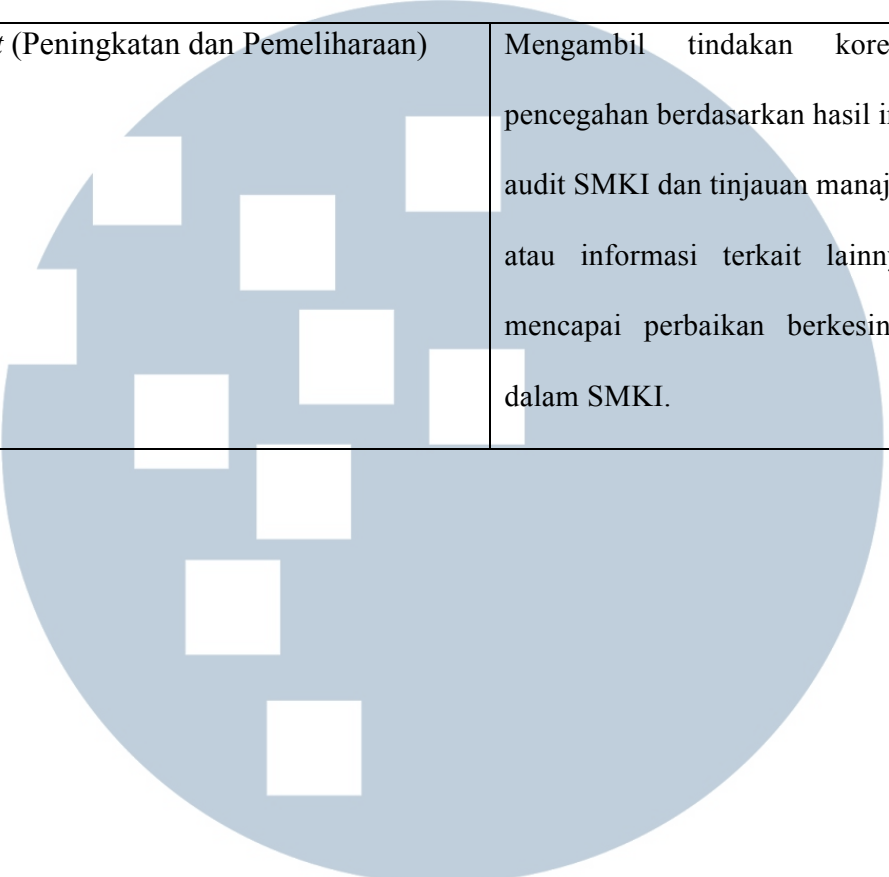


Gambar 2.15 Model PDCA

Untuk penjelasan model PDCA akan dijelaskan pada tabel dibawah ini:

Tabel 2.1 Penjelasan Model PDCA

| | |
|---|---|
| <i>Plan</i> (Penetapan SMKI) | Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran perusahaan secara keseluruhan. |
| <i>Do</i> (Penerapan dan Pengoperasian SMKI) | Menerapkan dan mengoperasikan kebijakan pengendalian, proses dan prosedur SMKI. |
| <i>Check</i> (Pemantauan dan Pengkajian SMKI) | Mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian. |

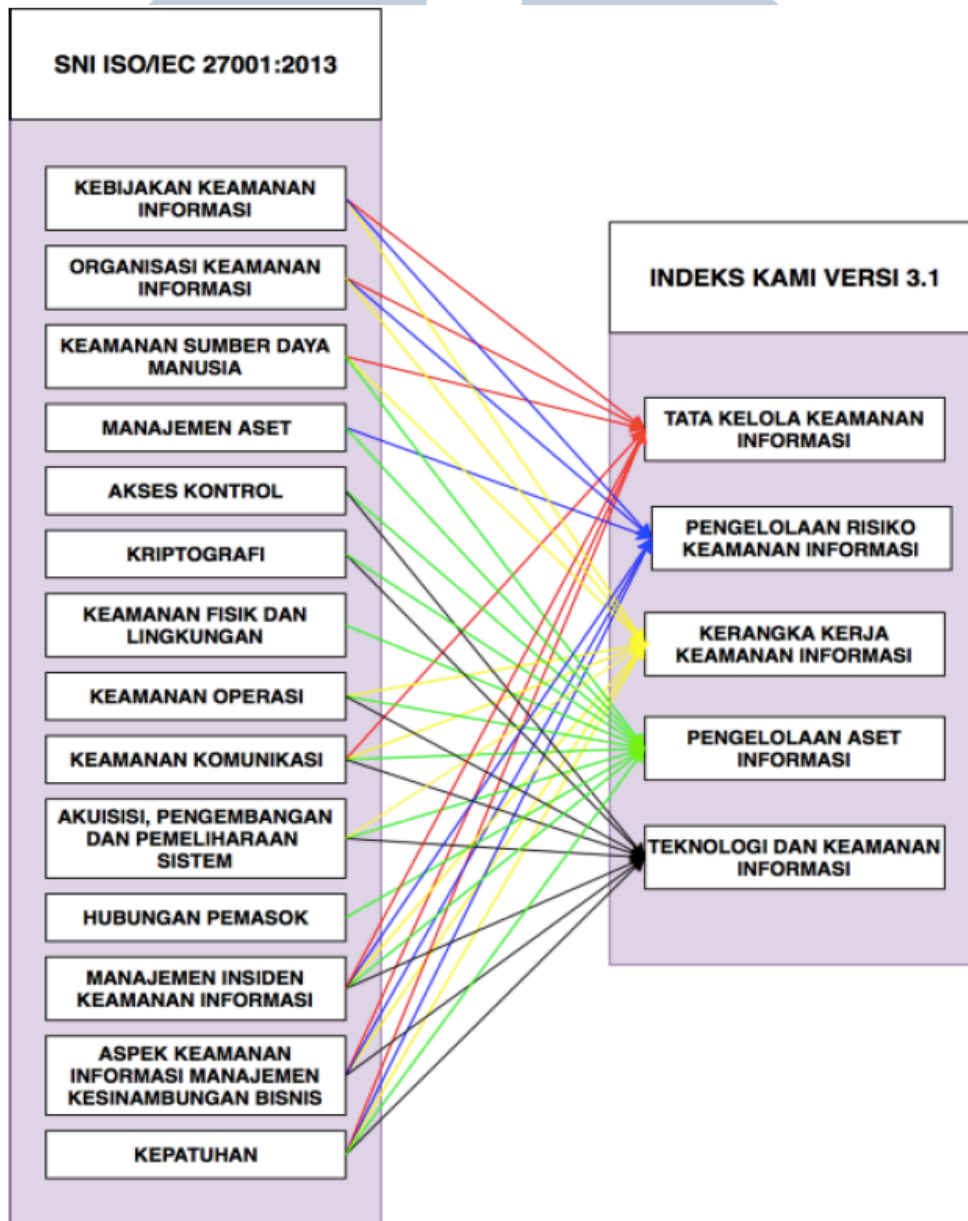


| | |
|---|---|
| <i>Act</i> (Peningkatan dan Pemeliharaan) | Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI. |
|---|---|

UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

2.8 Keterkaitan Indeks KAMI dengan ISO 27001 : 2013



Gambar 2.16 Korelasi Indeks KAMI & ISO 27001 : 2013

Sumber : Panduan Indeks KAMI (DISKOMINFO)

Gambar 2.16 diatas ini menggambarkan korelasi Indeks KAMI dengan klausul ISO 27001 : 2013. Area yang digunakan dalam Indeks KAMI untuk mengevaluasi atau mengukur tingkat kematangan SMKI instansi merangkul dari

14 sasaran pengendalian yang ada I ISO 27001:2013 ke dalam 5 area evaluasi. 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 dilkauan instansi dan yang ke dua adalah mengukur 5 area Kematangan Keamanan Informasi. Berikut ini merupakan penjelasan pengelompokan keterkaitan Indeks KAMI dengan ISO 27001:2013

1. Area Tata Kelola Keamanan Informasi


- Kebijakan Keamanan Informasi
- Organisasi Keamanan Informasi
- Keamanan Sumber Data Manusia
- Keamanan Komunikasi
- Manajemen Insiden Keamanan Informasi
- Aspek Keamanan Informasi Manajemen Kesiambungan
- Kepatuhan

2. Area Pengelolaan Risiko Keamanan Informasi

- Kebijakan Keamanan Informasi
- Organisasi Keamanan Informasi
- Manajemen Aset
- Manajemen Insiden Keamanan Informasi
- Aspek Keamanan Informasi Manajemen Kesiambungan Bisnis
- Kepatuhan

3. Area Kerangka Kerja Keamanan Informasi

- Kebijakan Keamanan Informasi
 - Organisasi Keamanan Informasi
 - Keamanan sumber Daya Manusia
 - Keamanan Operasi
 - Keamanan Komunikasi
 - Akuisi, Pengembangan dan Pemeliharaan Sistem
 - Manajemen Insiden Keamanan Informasi
 - Aspek Keamanan Informasi Manajemen Kesenambungan Bisnis
 - Kepatuhan
4. Area Pengelolaan Aset Informasi-
- Keamanan Sumber Daya Manusia
 - Manajemen Aset
 - Akses Kontrol
 - Kriptografi
 - Keamanan Fisik dan Lingkungan
 - Keamanan Operasi
 - Akusi, Pengembangan dan Pemeliharaan Sistem
 - Hubungan Pemasok
 - Manajemen Insiden Keamanan Informasi
 - Kepatuhan
5. Area Teknologi dan Keamanan Informasi
- Akses Kontrol
 - Kriptografi

- 
- Keamanan Operasi
 - Keamanan Komunikasi
 - Akuisi, Pengembangan dan Pemeliharaan Sistem
 - Hubungan Pemasok
 - Manajemen Insiden Keamanan Informasi
 - Aspek Keamanan Informasi Manajemen Kesiambungan Bisnis
 - Kepatuhan

UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA