ISSN : 2580-1503

KONSEP DAN STRATEGI EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) DAN EVALUASI KESADARAN KEAMANAN INFORMASI PADA PENGGUNA

Darmawan Setiya Budi [1)], **Avinanta Tarigan** [2)]

[1)]*Magister Teknik Informatika Universitas Amikom* [2)] *Fakultas Ilmu Komputer Universitas Gunadarma*
[1)] *Jl. Ring Road Utara, Condong Catur, Sleman 55283* [2)] *Jl. Margonda Raya 100, Depok 16424*
Email: darmawan.setiyabudi@gmail.com[1)], avinanta@staff.gunadarma.ac.id[2)]

Abstrak

Evaluasi menggunakan Indeks KAMI bertujuan untuk mengetahui tingkat kesiapan dan kematangan keamanan informasi pada suatu organisasi, sehingga dapat dirumuskan strategi dan penerapan keamanan informasi yang lebih baik dalam organisasi. Indeks KAMI terkini adalah Indeks KAMI versi 3.1 yang berbasis pada ISO 27001:2013.

Adapun evaluasi menggunakan HAIS-Q bertujuan untuk mengetahui kesadaran keamanan informasi pada pengguna berdasarkan aspek knowledge, attitude dan behaviour (KAB Model). Evaluasi kepada manusia (people) menjadi begitu penting, karena manusia merupakan pengguna teknologi informasi sekaligus rantai terlemah dalam keamanan informasi.

Penelitian ini merupakan studi pustaka yang bertujuan untuk merumuskan strategi evaluasi manajemen keamanan informasi dan kesadaran keamanan informasi pada pengguna, berikut konsep yang mendukungnya. Konsep dan strategi ini, diharapkan dapat memberikan pemahaman dan acuan dalam pelaksanaan evaluasi manajemen keamanan informasi dan evaluasi kesadaran keamanan informasi pada pengguna.

Kata kunci: *Information Security Management System, Indeks KAMI, Information Security Awareness.*

1. Pendahuluan

Saat ini, kita berada di dalam dunia yang saling terhubung dengan memanfaatkan teknologi dan internet yang terus tumbuh dan berkembang secara cepat. Tiap individu atau organisasi hampir tidak mungkin beraktivitas secara terpisah tanpa ketergantungan terhadap pihak lain. Seringkali suatu sistem atau proses bisnis melakukan pengumpulan, pengolahan, bahkan berbagi data terkait dengan informasi keuangan, produk, operasional, pelanggan hingga data karyawan dengan mitra, pemasok dan distributor[16].

Menurut Eloff dan Von Solms, seluruh organisasi tergantung pada sumber daya teknologi informasi yang dimilikinya. Pereira dan Santos berpendapat bahwa sumber daya teknologi informasi tidak hanya diperuntukkan bagi kelangsungan hidup organisasi, tetapi juga untuk pertumbuhan dan ekspansi organisasi didalam pasar global yang begitu kompetitif. Adapun Thomson dan Von Solms menyatakan bahwa penggunaan teknologi informasi juga membawa serta risiko yang signifikan sebagai bagian dari sifat yang dimilikinya[14].

Oleh karena itu, keamanan informasi perlu dikelola dan dikendalikan dengan baik sebagai perlindungan terhadap informasi dari berbagai ancaman. Hal ini dilakukan untuk memastikan kelangsungan bisnis, meminimalkan risiko bisnis, juga memaksimalkan pengembalian investasi dan peluang bisnis[14].

2. Metode Penelitian

2.1 Studi Pustaka

Studi pustaka dilakukan dengan mengkaji buku, jurnal ilmiah, makalah penelitian dan berbagai dokumen terkait dengan keamanan informasi secara umum dan lebih khusus terkait Indeks KAMI dan kesadaran keamanan informasi pada pengguna.

2.2 Pengumpulan Data

Pengumpulan data dilakukan melalui:

1. Studi dokumentasi bertujuan untuk mengetahui dan memahami manajemen keamanan informasi secara tertulis dari berbagai dokumen, meliputi: kebijakan, prosedur, panduan kerja, instruksi kerja, *minutes of meeting* dan dokumen lainnya.
2. Wawancara, yang bertujuan untuk mengetahui dan memahami manajemen keamanan informasi dari pimpinan atau pihak yang bertanggung jawab, meliputi aspek: dukungan pimpinan, arahan, penerapan dan berbagai aspek lainnya.
3. Observasi, bertujuan untuk mengetahui dan memahami manajemen keamanan informasi melalui pengamatan keseharian terkait aktivitas dilingkungan organisasi.
4. Kuisioner, bertujuan untuk mengetahui dan memahami kesadaran keamanan pengguna melalui berbagai pertanyaan yang diajukan dalam kuisioner.

ISSN : 2580-1503

2.3 Konsep Evaluasi SMKI Menggunakan Indeks KAMI dan Kesadaran Keamanan Informasi Pada Pengguna

Konsep evaluasi manajemen keamanan informasi menggunakan Indeks KAMI dan evaluasi kesadaran keamanan informasi pada pengguna dibahas pada bagian ini, termasuk didalamnya pembahasan kuisioner Indeks KAMI dan kuisioner kesadaran keamanan informasi pada pengguna.

2.4 Strategi Evaluasi SMKI Menggunakan Indeks KAMI dan Kesadaran Keamanan Informasi Pada Pengguna

Adapun pada bagian ini dibahas strategi implementasi evaluasi manajemen keamanan informasi menggunakan Indeks KAMI dan evaluasi kesadaran keamanan informasi pada pengguna, termasuk didalamnya tahapan implementasi dan waktu pelaksanaan.

3. Tinjauan Pustaka

3.1 Keamanan Informasi dan Manajemen Keamanan Informasi

Informasi adalah hal yang vital bagi setiap bisnis atau organisasi. Menurut Paulsen dan Toth, ancaman *(threat)* dalam keamanan informasi adalah sesuatu yang dapat mempengaruhi informasi yang diperlukan untuk menjalankan bisnis. Ancaman tersebut dapat mempengaruhi sebagian dari bisnis atau bahkan dapat menyebabkan bisnis berhenti secara total. Ancaman tersebut bisa datang dari manusia atau alam, baik secara disengaja ataupun tidak[3].

Paulsen dan Toth menyatakan bahwa keamanan informasi merupakan perlindungan terhadap sistem informasi dan seluruh informasi yang terkandung di dalamnya dari akses, penggunaan, pengungkapan, gangguan, pengubahan atau perusakan oleh yang tidak berhak[3]. Adapun pendapat Whitman dan Mattord, keamanan informasi adalah perlindungan atas kerahasiaan, keutuhan dan ketersediaan terhadap informasi dan aset, baik dalam proses penyimpanan, pengolahan ataupun transmisi melalui penerapan kebijakan, pendidikan, pelatihan dan kesadaran ataupun aspek teknologi[10].

Sari dan Candiwan menyatakan bahwa penerapan pengelolaan keamanan informasi di dalam organisasi harus memperhatikan tiga komponen, yaitu: (1) kerahasiaan informasi, informasi yang sensitif dilindungi dari intersepsi dan pengungkapan yang tidak berhak, (2) integritas, setiap informasi harus terjamin keakuratan dan kelengkapannya, (3) ketersediaan, informasi dan layanan vital harus selalu tersedia saat diperlukan[1].

Menurut Whitman dan Mattord, prinsip di dalam manajemen teknologi informasi adalah menitikberatkan kepada efektivitas dan efisiensi pengolahan informasi. Dalam pelaksanaannya manajemen keamanan informasi memperhatikan prinsip 6P, yaitu: *planning, policy, program, protection, people* dan *project*[9].

3.2 Sistem Manajemen Keamanan Informasi

Menurut Carlson, Sistem Manajemen Keamanan Informasi (SMKI) adalah proses penerapan manajemen risiko yang bertujuan untuk melindungi kerahasiaan, keutuhan dan ketersediaan informasi. SMKI menyediakan berbagai prasyarat yang berkaitan dengan pengelolaan keamanan informasi secara keseluruhan. Aspek dalam SMKI meliputi: *risk management, total quality management, a monitoring and reporting model, a structured approach* dan *an extensible framework*[12].

Adapun Disterer berpendapat, diperlukan standar keamanan yang dapat digunakan sebagai pedoman atau kerangka kerja dalam mengembangkan dan memelihara Sistem Manajemen Keamanan Informasi (SMKI) yang memadai. SMKI diperlukan karena meningkatnya pelanggaran terhadap privasi dan keamanan, praktik akuntansi yang tidak tepat dan semakin maraknya serangan terhadap TI di masyarakat[4]. Dalam sebuah SMKI terdapat beberapa komponen utama, yaitu: *management principles, resources, personnel* dan *information security process*[12].

3.3 ISO 27001 Sistem Manajemen Keamanan Informasi

ISO 27001 merupakan standar keamanan informasi yang terbitkan oleh *The International Organization for Standardization* (ISO) dan *The Electrotechnical Commission* (IEC) yang dipergunakan membantu organisasi dalam mengamankan aset informasi. ISO 27001 menjelaskan berbagai prasyarat bagi penetapan, penerapan, pelaksanaan, pemantauan, peninjauan ulang, pemeliharaan dan pendokumentasian Sistem Manajemen Keamanan Informasi (SMKI)[2].

ISO 27001 bersifat independen terhadap produk teknologi informasi, menggunakan pendekatan manajemen berbasis risiko dan dirancang untuk menjamin agar kontrol keamanan yang ada, mampu melindungi aset informasi dari berbagai risiko dan memberikan keyakinan tingkat keamanan bagi pihak yang berkepentingan[7].

Dalam penetapan, penerapan, pelaksanaan, pemantauan, peninjauan ulang, pemeliharaan dan peningkatan SMKI dalam suatu organisasi, ISO 27001 menggunakan suatu model yang dikenal dengan nama *"Plan, Do, Check, Act"* (PDCA). Dimana *plan* adalah menetapkan SMKI, *do* adalah menerapkan dan melaksanakan SMKI. Sedangkan c*heck* adalah memantau dan meninjau ulang SMKI, adapun act adalah memelihara dan meningkatkan SMKI. Saat ini, ISO 27001:2013 merupakan revisi terbaru dari standar SMKI yang diluncurkan pada Oktober 2013. Pada ISO 27001:2013 terdapat 14 area pengamanan *(main clauses)* dan 114 kontrol *(control)* keamanan informasi[2].

3.4 Indeks Keamanan Informasi (KAMI)

Indeks KAMI merupakan suatu media evaluasi terhadap tingkat kesiapan dan kematangan keamanan informasi berdasarkan ISO 27001. Evaluasi tidak ditujukan untuk

ISSN : 2580-1503

menganalisis kelayakan atau efektivitas pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan 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 ISO 27001[7].

Evaluasi yang diterapkan dalam Indeks KAMI didesain untuk dapat dipergunakan oleh organisasi dari berbagai tingkatan, ukuran, maupun kepentingan penggunaan TIK. Evaluasi indeks KAMI mencakup enam area, meliputi: kategori sistem elektronik, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi dan teknologi dan keamanan informasi[7].

Adapun dalam identifikasi tingkat kematangan penerapan pengamanan yang terdapat dalam keseluruhan klausul dan kontrol yang ada, mengacu kepada tingkatan kematangan yang didefinisikan dalam CMMI *(Capability Maturity Model for Integration)*[7].

3.5 Manusia Dalam Rantai Keamanan Informasi

Menurut Von Solms dan Cervone, untuk meminimalkan risiko pelanggaran terhadap keamanan informasi, maka sangat penting bagi suatu organisasi untuk menerapkan rencana atau strategi keamanan informasi. Bagi Namjoo, pencegahan yang dilakukan setelah terjadinya suatu pelanggaran keamanan informasi, bisa menjadi sangat terlambat[6].

Whitman dan Mattord menyampaikan bahwa manusia adalah titik terlemah dalam keamanan informasi. Suatu organisasi bisa saja memiliki teknologi terbaik, menggunakan perlindungan *firewall, intrusion detection system* (IDS), sistem biometrik dan lain sebagainya, tetapi karyawan yang tidak dicurigai dapat membobol sistem tanpa diduga[10]. Adapun Harris dan Maymi menyatakan bahwa keamanan suatu organisasi tergantung pada teknologi dan manusia. Manusia merupakan titik terlemah dalam rantai keamanan dan seringkali menyebabkan pelanggaran keamanan dan kebocoran terhadap sistem. Jika pengguna dapat memahami sistem dengan baik, maka insiden keamanan yang terjadi dapat diminimalkan. Terdapat berbagai cara untuk mengeksploitasi manusia sebagai titik terlemah dalam rantai keamanan, tetapi secara umum hanya terdapat tiga serangan utama yang umum dilakukan, yaitu: *social engineering, social network* dan *weak password*[13].

3.6 Kesadaran Keamanan Informasi Pengguna

Kesadaran keamanan informasi adalah suatu tingkat yang menunjukkan pemahaman publik atau individu terhadap keamanan informasi, tanggung jawab setiap individu dan bertindak sesuai dengan pemahaman dan tanggung jawab tersebut[15]. Sedangkan Bulgurcu berpendapat bahwa kesadaran keamanan informasi adalah pengetahuan karyawan tentang konsep keamanan informasi dan kesadarannya terhadap rencana keamanan informasi dan berbagai parameter yang telah ditetapkan oleh organisasi[6].

Dalam penelitiannya Dzazali menyimpulkan bahwa faktor pengguna harus diperhitungkan dalam keamanan informasi. Kebijakan atau kontrol menjadi tidak berguna jika pengguna tidak mengetahui risiko keamanan dan kebijakan yang ada[6]. Sebesar apapun investasi perangkat keras dan lunak yang ditanamkan, akan menjadi tidak berarti karena karyawan yang tidak terlatih dan tidak memiliki kesadaran keamanan informasi menjadi vektor dari serangan siber[11]. Keterampilan dan kesadaran yang kurang atau tidak memadai dapat menyebabkan kesalahan yang disengaja ataupun tidak terkait dengan keamanan[8].

Whitman dan Mattord menyatakan bahwa kesalahan atau kegagalan yang disebabkan manusia, dapat dihindari dengan pelatihan, aktivitas kesadaran dan penerapan kontrol[10]. Sedangkan pengguna komputer dengan pengetahuan dan pemahaman yang memadai tentang konsep keamanan informasi, akan menunjukkan sikap dan perilaku yang lebih positif terhadap keamanan informasi[8]. Adapun pernyataan Knapp, terdapat hubungan positif dan langsung antara kesadaran keamanan informasi dan tindakan pencegahan dalam peningkatan kinerja keamanan. Dan Bulgurcu dalam penelitiannya menunjukkan bahwa keamanan informasi secara positif dapat mempengaruhi sikap karyawan dan mendorong kepatuhan[6].

3.7 Evaluasi Kesadaran Keamanan Informasi Pengguna

Kesadaran keamanan informasi merupakan suatu proses yang bersifat dinamis terkait dengan tantangan dan risiko yang terus berubah, sehingga kesadaran terhadap keamanan informasi harus diukur dan dikelola sesuai dengan perubahan dan perkembangan risiko. Kesadaran keamanan informasi juga harus dilakukan secara terus-menerus, berkesinambungan dan menjadi bagian dari budaya organisasi atau perusahaan. Adapun Schlienger dan Teufel menyatakan bahwa tujuan yang diharapkan dari kesadaran keamanan informasi, yaitu: pengguna "menjadi sadar", kemudian "tetap sadar" dan akhirnya "sadar" terhadap keamanan informasi[5].

Untuk mengetahui tingkat kesadaran keamanan informasi pengguna, Kruger dan Kearney membangun suatu model yang dapat dipergunakan sebagai media pengukuran kesadaran keamanan informasi. Pengukuran tersebut dilakukan pada tiga aspek, meliputi: pengetahuan *(knowledge)*, sikap *(attitude)* dan perilaku *(behaviour)*. Berdasarkan tiga aspek dimensi yang telah ditetapkan, dibagi kembali aspek tersebut menjadi enam area fokus. Setiap fokus yang ada, dibagi menjadi beberapa faktor dan kemudian dibagi kembali menjadi beberapa sub bagian. Model ini dikenal dengan nama KAB *(Knowledge-Attitude-Behaviour)* Model[5].

ISSN : 2580-1503

4. Pembahasan

4.1 Konsep Evaluasi Indeks KAMI

Indeks KAMI dipublikasikan pertama kali oleh Kementrian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) pada tahun 2011. Saat ini, Indeks KAMI telah mencapai versi 3.1 yang mengacu kepada ISO 27001:2013. Evaluasi dilakukan pada kategoi sistem elektronik dan lima area keamanan informasi.

4.1.1 Kategori Sistem Informasi

Bagian kategori sistem informasi bertujuan untuk mengevaluasi tingkat atau kategori sistem elektronik yang digunakan dalam organisasi. Terdapat 10 pertanyaan pada bagian ini, sesuai tabel 1.

Tabel 1. Pertanyaan Kategori Sistem Elektronik[7]

Kategori Sistem Elektronik	
No	**Karakteristik Instansi**
1	Nilai investasi sistem elektronik yang terpasang
2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik
3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu
4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik
5	Jumlah pengguna Sistem Elektronik
6	Data pribadi yang dikelola Sistem Elektronik
7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi
8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi
9	Dampak dari kegagalan Sistem Elektronik
10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme)

Adapun kategori sistem elektronik sendiri dibagi menjadi tiga, yaitu: rendah, tinggi atau strategis. Kategori tersebut diperoleh dari penilaian yang dilakukan pada tabel 1. Rentang kategori sistem elektronik, terdapat pada tabel 2.

Tabel 2. Kategori Sistem Elektronik[7]

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

Penentuan status kesiapan organisasi dalam SMKI dipengaruhi oleh kategori sistem elektronik. Sistem elektronik yang memiliki kategori strategis memiliki rentang nilai kesiapan yang lebih tinggi. Hal ini berarti, bahwa setiap prasyarat atau komponen Indeks KAMI harus dipenuhi secara lebih baik. Tingkat kesiapan SMKI bagi setiap kategori Sistem Elektronik (SE) terdapat pada tabel 3.

Tabel 3. Kategori SE dan Status Kesiapan[7]

Kategori SE	Skor Akhir	Status Kesiapan
Rendah	0 - 174	Tidak Layak
	175 - 312	Perlu Perbaikan
	313 - 535	Cukup
	536 - 645	Baik
Tinggi	0 - 272	Tidak Layak
	273 - 455	Perlu Perbaikan
	456 - 583	Cukup
	584 - 645	Baik
Strategis	0 - 333	Tidak Layak
	334 - 535	Perlu Perbaikan
	536 - 609	Cukup
	610 - 645	Baik

4.1.2 Tata Kelola Keamanan Informasi

Bagian tata kelola keamanan informasi bertujuan untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/ fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Terdapat 22 pertanyaan terkait tata kelola keamanana informasi sesuai tabel 4.

Tabel 4. Pertanyaan Tata Kelola Keamanan Informasi[7]

Tata Kelola Keamanan Informasi	
No	**Fungsi/Instansi Keamanan Informasi**
1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?
2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?
3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?
4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?
5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?
6	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?
7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi

ISSN : 2580-1503

	dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?
8	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?
9	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?
10	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?
11	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?
12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?
13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?
14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?
15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?
16	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?
17	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?
18	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?
19	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?
20	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?
21	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?
22	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?

4.1.3 Pengelolaan Risiko Keamanan Informasi

Bagian pengelolaan risiko keamanan informasi bertujuan untuk mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Terdapat 16 pertanyaan terkait pengelolaan risiko keamanan informasi sesuai tabel 5.

Tabel 5. Pertanyaan Pengelolaan Risiko Keamanan Informasi[7]

Pengelolaan Risiko Keamanan Informasi	
No	**Kajian Risiko Keamanan Informasi**
1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
2	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?
3	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?
5	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?
6	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset

ISSN : 2580-1503

	utama/penting dan proses kerja utama yang menggunakan aset tersebut?
7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?
8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?
9	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?
10	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?
11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektivitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?
12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?
13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektivitasnya?
14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?
15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektivitasnya?
16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan?

4.1.4 Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian kerangka kerja pengelolaan keamanan informasi bertujuan untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Terdapat 29 pertanyaan kerangka kerja pengelolaan keamanan informasi sesuai tabel 6.

Tabel 6. Pertanyaan Kerangka Kerja Pengelolaan Keamanan Informasi[7]

Kerangka Kerja Pengelolaan Keamanan Informasi	
No	**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**
1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?
2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?
3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?
4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?
5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?
6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?
7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?
8	Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?
9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekuensi dari kondisi ini?
10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya?
11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?

ISSN : 2580-1503

12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?
13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?
14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (compensating control) dan jadwal penyelesaiannya?
15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?
16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?
17	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?
18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?
19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?
	Pengelolaan Strategi dan Program Keamanan Informasi
20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?
21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?
22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?
23	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?
24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?
25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?
26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?
27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?
28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?
29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?

4.1.5 Pengelolaan Aset Informasi

Bagian kerangka kerja pengelolaan aset informasi bertujuan untuk mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Terdapat 38 pertanyaan terkait pengelolaan aset informasi sesuai tabel 7.

Tabel 7. Pertanyaan Pengelolaan Aset Informasi[7]

Pengelolaan Aset Informasi	
No	**Pengelolaan Aset Informasi**
1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)
2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?
3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?
4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi

ISSN : 2580-1503

	dan matrix yang merekam alokasi akses tersebut?
5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?
6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?
7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?
Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda
9	Tata tertib penggunaan komputer, email, internet dan intranet
10	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI
11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi
12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
13	Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya
14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
18	Prosedur back-up dan ujicoba pengembalian data (restore) secara berkala
19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
20	Proses pengecekan latar belakang SDM
21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
22	Prosedur penghancuran data/aset yang sudah tidak diperlukan
23	Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidak sesuaian (non-conformity) terhadap kebijakan yang berlaku
24	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya
25	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?
26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?
27	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?
	Pengamanan Fisik
28	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?
29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?
30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?
31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?
32	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?
33	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)
34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?
35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?
36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?
37	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)

ISSN : 2580-1503

38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?

4.1.6 Teknologi dan Keamanan Informasi

Bagian teknologi dan keamanan informasi bertujuan untuk mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Terdapat 26 pertanyaan terkait teknologi dan keamanan informasi sesuai tabel 8.

Tabel 8. Pertanyaan Teknologi dan Keamanan Informasi[7]

Teknologi dan Keamanan Informasi	
No	**Pengamanan Teknologi**
1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?
2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?
3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?
4	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?
5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?
6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?
7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?
8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?
9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?
10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?
11	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?
12	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?
13	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?
14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?
15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?
16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses?
17	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?
18	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?
19	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?
20	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?
21	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?
22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?
23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?
24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?
25	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?
26	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?

4.1.7 Penilaian dan Pembobotan

Pada bagian kategori sistem elektronik, tersedia opsi jawaban untuk dipilih *(multiple choice)*. Pemilihan jawaban harus mengacu pada kondisi organisasi terkini. Nilai yang diberikan untuk setiap pertanyaan, minimal

ISSN : 2580-1503

adalah 1 dan maksimal 5 dengan nilai total minimal 10 dan maksimal 50. Nilai total tersebut dipergunakan untuk mengetahui kategori sistem elektronik sesuai penjelasan sebelumnya.

Adapun pada bagian tata kelola, pengelolaan risiko, kerangka kerja pengelolaan, pengelolaan aset, dan teknologi dan keamanan informasi, pertanyaan dibagi menjadi beberapa kategori, yaitu kategori 1 hingga kategori 3. Sedangkan setiap kategori memiliki bobot nilai yang berbeda sesuai dengan status pengamanan yang diterapkan pada organisasi. Adapun detil status pengamanan dan kategori pengamanan berikut pembobotan tiap kategori, terdapat pada tabel 9.

Tabel 9. Status dan Kategori Pengamanan[7]

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

4.2 Konsep Evaluasi Kesadaran Keamanan Informasi Pada Pengguna

Evaluasi kesadaran keamanan informasi pada pengguna dilakukan dengan menggunakan metode evaluasi *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang dikembangkan oleh Parson, McCormac, Butavicius, Pattinson dan Jerram dengan berbasis KAB Model yang dicetuskan Kruger dan Kearney.

Pada HAIS-Q, aspek pengetahuan, sikap dan perilaku, dirumuskan secara lebih spesifik sesuai dengan evaluasi yang dilakukan. Pada topik kesadaran keamanan informasi, aspek pengetahuan *(knowledge)* adalah pengetahuan pengguna terhadap kebijakan dan prosedur *(policy and procedures)* terkait dengan keamanan informasi. Sedangkan aspek sikap *(attitude)* adalah sikap pengguna terhadap kebijakan dan prosedur keamanan informasi. Adapun aspek perilaku *(behaviour)* adalah perilaku pengguna dalam menggunakan komputer kerja[8].

Sedangkan pertanyaan yang diajukan terkait dengan kesadaran keamanan informasi pada pengguna dapat dilihat pada tabel 10.

Tabel 10. Pertanyaan Kesadaran Keamanan Informasi Pada Pengguna[8]

Evaluasi Kesadaran Keamanan Informasi Pada Pengguna	
No	**Manajemen Kata Sandi *(Password)***
1	Mengunci komputer kerja
2	Berbagi kata sandi
	Penggunaan Email
3	Penerusan surel *(forwarding emails)*
4	Membuka lampiran surel
5	Tingkat tanggung jawab TI
	Penggunaan Internet
6	Instalasi perangkat lunak tidak resmi
7	Akses laman mencurigakan
	Penggunaan Media Sosial
8	Waktu kerja yang digunakan ber-media sosial
9	Konsekuensi penggunaan media sosial
	Pelaporan Insiden
10	Melaporkan individu yang membahayakan
11	Melaporkan perilaku buruk rekan kerja
12	Melaporkan seluruh insiden keamanan informasi
	Mobile Computing
13	Pengamanan fisik perangkat elektronik perorangan
14	Pengiriman informasi sensitif melalui jaringan *mobile*
15	Membuka surel kerja melalui jaringan publik
	Penanganan Informasi
16	Pemusnahan dokumen sensitif
17	Penggunaan perangkat DVD atau USB
18	Meninggalkan informasi sensitif secara tidak aman

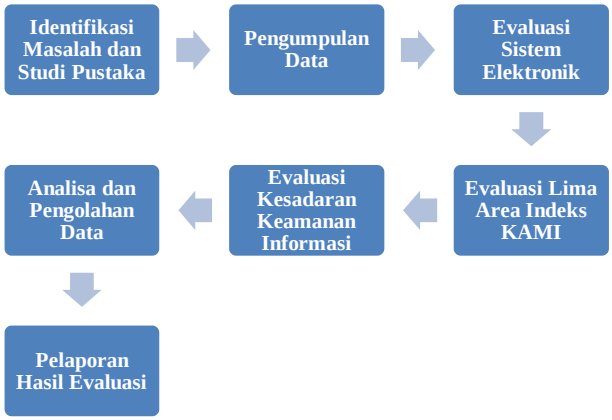
4.3 Strategi Evaluasi SMKI Menggunakan Indeks KAMI dan Kesadaran Keamanan Informasi Pada Pengguna

Adapun strategi pelaksanaan evaluasi secara umum terdapat pada gambar 1. Sedangkan aktivitas pada setiap tahapan evaluasi sebagai berikut:

1. Identifikasi masalah didapatkan dengan mempelajari organisasi obyek evaluasi. Hal tersebut dapat dilakukan dengan mempelajari proses bisnis, struktur organisasi dan hal terkait lainnya. Juga dilakukan studi pustaka terkait dengan media evaluasi, meliputi: dokumen ISO 27001, dokumen Indeks KAMI dan konsep atau model kesadaran keamanan informasi pada pengguna.
2. Pengumpulan data dilakukan dengan wawancara, pengamatan dilapangan dan kuisioner yang telah ditentukan.
3. Evaluasi sistem elektronik dilakukan dengan melakukan pemetaan *(mapping)* antara data yang dikumpulkan dengan Indeks KAMI.
4. Evaluasi lima area keamanan informasi juga dilakukan dengan melakukan pemetaan data yang didapatkan dengan Indeks KAMI.
5. Evaluasi kesadaran keamanan informasi pada pengguna dilakukan dengan menggunakan HAIS-Q.
6. Analisa data dilakukan untuk mendapatkan tingkat tingkat kritikalitas sistem elektronik dan tingkat kematangan pada lima area keamanan informasi pada Indeks KAMI. Hal ini mencerminkan kesiapan organisasi terkait SMKI. Selain itu, didapatkan persentase kesadaran keamanan informasi pada pengguna berdasarkan komponen yang ditetapkan dari HAIS-Q yang berbasis KAB Model.

ISSN : 2580-1503

7. Pelaporan merupakan hasil dari evaluasi yang dilakukan berikut berbagai rekomendasi yang diberikan untuk perbaikan dan meningkatkan kesiapan organisasi terkait SMKI berdasarkan Indeks KAMI dan peningkatan kesadaran terhadap keamanan informasi pada pengguna.



Gambar 1. Tahapan Implementasi Evaluasi

Berdasarkan tahapan yang telah ditentukan, estimasi waktu yang diperlukan untuk aktivitas tersebut dapat diperkirakan pada tabel 11.

Tabel 11. Estimasi Waktu Evaluasi

No	Tahapan	Minggu									
		1	2	3	4	5	6	7	8	9	10
1	Identifikasi Masalah dan Studi Pustaka										
2	Pengumpulan Data										
3	Evaluasi Sistem Elektronik										
4	Evaluasi Lima Area Indeks KAMI										
5	Evaluasi Kesadaran Keamanan Informasi										
6	Analisa dan Pengolahan Data										
7	Pelaporan Hasil Evaluasi										

3. Kesimpulan

Seluruh organisasi memiliki ketergantungan terhadap sumber daya teknologi informasi yang dimilikinya untuk dapat tetap hidup, terus berkembang dan berkompetisi dipasar global. Selain berbagai manfaat besar yang diberikan, teknologi informasi juga memiliki risiko bawaan yang sangat signifikan. Untuk meminimalkan risiko yang ada dan memberikan perlindungan terhadap berbagai ancaman, maka keamanan informasi harus dikelola dan dikendalikan dengan baik, termasuk didalamnya adalah *people, process* dan *technology*.

Indeks KAMI merupakan suatu media evaluasi untuk mengetahui tingkat kesiapan dan kematangan keamanan informasi pada suatu organisasi yang dikembangkan berdasarkan ISO 27001. Hasil yang diberikan oleh Indeks KAMI, dapat memberikan gambaran kepada manajemen organisasi untuk penyusunan strategi dan penerapan keamanan informasi yang lebih baik dalam organisasi.

Adapun metode HAIS-Q yang dikembangkan dari KAB Model, merupakan salah satu media evaluasi untuk mengetahui kesadaran keamanan informasi pada pengguna berdasarkan aspek *knowledge attitude* dan *behaviour*. Evaluasi kepada manusia *(people)* menjadi begitu penting, karena manusia merupakan pengguna teknologi informasi sekaligus rantai terlemah dalam keamanan informasi.

Evaluasi SMKI menggunakan Indeks KAMI dan evaluasi kesadaran keamanan informasi pada pengguna, dapat dilakukan secara bersamaan, berdasarkan berbagai kajian dan diskusi yang telah dibahas. Mengacu pada tahapan yang telah disusun, evaluasi SMKI dan kesadaran keamanan informasi dapat dilakukan dengan estimasi waktu selama sepuluh minggu.

Daftar Pustaka

[1] Candiwan, "Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia", *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security*, Kuala Lumpur, Malaysia, 2014.

[2] Candiwan, M.Y.D. Beninda, Y. Priyadi, "Analysis of Information Security Audit Using ISO 27001:2013 & ISO 27002:2013 at IT Division-X Company, In Bandung, Indonesia", *International Journal of Basic and Applied Science*, Vol. 04, No. 04, pp. 77-88, April 2016.

[3] C. Paulsen, P.Toth, *Small Business Information Security: The Fundamentals*, NISTIR 7621 Revision 1, National Institute of Standard and Technology (NIST) U.S. Department of Commerce, Maryland, 2016.

[4] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management", *Journal of Information Security*, 4, 92-10, 2013.

[5] H.A. Kruger, W.D. Kearney, "A Prototype for Assessing Information Security Awareness", *Computer & Security 25*, 289-296, 2006.

[6] H. Chan, S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector", *International Journal of Computer Applications (0975-8887)*, Volume 60-No.10, December 2012.

[7] Kominfo, *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*, Edisi 2.0, Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika RI, Jakarta, 2011.

[8] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, C. Jerram, "A Study of Information Security Awareness In Australian Government Organizations", *Information Management Computer Security 22(4)*, 334-345, 2014.

[9] M.E. Whitman, H.J. Mattord, *Management of Information Security*, Fourth Edition, Cengage Learning, Boston, 2013.

[10] M.E. Whitman, H.J. Mattord, *Principles of Information Security*, Fifth Edition, Cengage Learning, Boston, 2014.

ISSN : 2580-1503

[11] N. Badie, A.H. Lashkari, "A New Evaluation Criteria For Effective Security Awareness In Computer Risk Management Based On AHP". *J. Basic Appl. Sci. Res. 2(9)*, 9331-9347, 2012.
[12] S. Al-Dhahri, M. Al-Sarti, A.A. Aziz, "Information Security Management System", *International Journal of Computer Applications (0975-8887)*, Volume 158-No 7, January 2017.
[13] S. Harris, F. Maymi, *CISSP All-in-One Exam Guide*, Seventh Edition, McGraw-Hill Education, New York, 2016.
[14] Sheikhpour, R., Modiri, N., 2012, An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.
[15] Information Security Forum (ISF). 2002. Effective Security Awareness Workshop Report. Diakses pada 24 Maret 2018 dari https://www.igt.hscic.gov.uk/Knowledgebase/Kb/ISF%20documents/Effective%20Security%20Awareness%2022-04-02.pdf.
[16] Telstra, 26 September 2017, Telstra Cyber Security Report 2017, https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf